KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GİZLİ GÖRÜNTÜ PAYLAŞIM ŞEMALARININ İYİLEŞTİRİLMESİ VE GEOMETRİ TABANLI YENİ BİR YÖNTEMİN TASARIMI

DOKTORA TEZİ

Bil. Yük. Müh. Güzin ULUTAŞ

OCAK 2012
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GİZLİ GÖRÜNTÜ PAYLAŞIM ŞEMALARININ İYİLEŞTİRİLMESİ VE GEOMETRİ TABANLI YENİ BİR YÖNTEMİN TASARIMI

Bilgisayar Yük. Müh. Güzin ULUTAŞ

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"DOKTOR (BİLGİSAYAR MÜHENDİSLİĞİ)"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 26.12.2011
Tezin Savunma Tarihi : 17.01.2012

Tez Danışmanı : Prof. Dr. Vasif V. NABİYEV

Trabzon 2012

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Ana Bilim Dalında

Güzin ULUTAŞ Tarafından Hazırlanan

GİZLİ GÖRÜNTÜ PAYLAŞIM ŞEMALARININ İYİLEŞTİRİLMESİ VE GEOMETRİ TABANLI YENİ BİR YÖNTEMİN TASARIMI

başlıklı bu çalışma, Enstitü Yönetim Kurulunun 27 / 12 / 2011 gün ve 1435 sayılı kararıyla oluşturulan jüri tarafından yapılan sınavda

DOKTORA TEZİ

olarak kabul edilmiştir.

Jüri Üyeleri

Başkan : Prof. Dr. Şeref SAĞIROĞLU .....

Üye : Prof. Dr. Vasif V. NABİYEV .....

Üye : Prof. Dr. Erhan COŞKUN .....

Üye : Doç. Dr. Cemal KÖSE .....

Üye : Yrd. Doç. Dr. Hüseyin PEHLİVAN .....

Prof. Dr. Sadettin KORKMAZ

Enstitü Müdürü

ÖNSÖZ

Ağ üzerinden gerçekleştirilen gizli görüntü iletiminde hataya karşı toleransın sağlanması ya da kişiye güven yerine gruba güven mekanizmasının uygulanması gerektiği durumlarda, sır paylaşım şemalarının kullanımı gereksinimleri karşılayacaktır. Ancak mevcut paylaşım şemalarının halen iyileştirilmesi gereken problemleri mevcuttur. Bu tez çalışmasında var olan gizli görüntü paylaşım şemalarındaki problemlerin iyileştirilmesine çalışılmış ve var olan sır paylaşım yöntemlerini kullanmayan yeni bir geometri tabanlı şemanın tasarımı gerçekleştirilmiştir.

Çalışmalarımda danışmanlığımı üstlenip ilgisini, desteğini ve tecrübelerini esirgemeyen sayın Prof. Dr. Vasif V. NABİYEV'e sonsuz teşekkürlerimi bir borç bilirim. Doktora süresince fikirlerine başvurduğum jüri üyelerine ayrıca teşekkür ederim. Doktora eğitimimin başlamasında ve her aşamasında yanımda olan eşime, hoşgörülerinden ötürü sevgili aileme çok teşekkür ederim.

Güzin ULUTAŞ
Trabzon 2012

TEZ BEYANNAMESİ

Doktora Tezi olarak sunduğum "Gizli Görüntü Paylaşım Şemalarının İyileştirilmesi ve Geometri Tabanlı Yeni Bir Yöntemin Tasarımı" başlıklı bu çalışmayı baştan sona kadar danışmanım Prof. Dr. Vasif V. NABİYEV'ın sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuarlarda yaptığımı/yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim. 14/02/2012

Güzin ULUTAŞ

İÇİNDEKİLER

Sayfa No

Doktora Tezi

ÖZET

GİZLİ GÖRÜNTÜ PAYLAŞIM ŞEMALARININ İYİLEŞTİRİLMESİ VE GEOMETRİ TABANLI YENİ BİR YÖNTEMİN TASARIMI

Güzin ULUTAŞ

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Danışman: Prof. Dr. Vasif V. NABİYEV
2012, 196 Sayfa, 12 Ek Sayfa

Çalışma kapsamında gizli görüntü paylaşımı alanındaki problemler irdelenmiş ve bu sorunlara çözüm getirecek şekilde yeni görüntü paylaşım şemalarının tasarlanması gerçekleştirilmiştir. Üretilen stego görüntülerin PSNR değerinin iyileştirilmesi, stego görüntüleri doğrulamada kullanılan bit sayısının görüntü kalitesini bozmadan artırılması, pay görüntülerini saklamada kullanılan örten görüntü büyüklüğünün küçültülmesi, gizli görüntünün yeniden yapılandırılmasının ardından örten görüntülerin tekrar elde edilmesi, örten ve gizli görüntü büyüklüğüne bağlı olarak adaptif doğrulama tekniklerinin geliştirilmesi problemlerine çözüm getiren yeni gizli görüntü paylaşım şemalarının tasarımı yapılmıştır. Gizli görüntü olarak medikal görüntülerin seçilmesi durumu çalışma kapsamında tasarlanan yeni bir paylaşım şeması ile ayrıca değerlendirilmiştir. Önerilen gizli görüntü paylaşım şeması, literatürdeki medikal görüntü güvenliğini sağlayan çalışmalardan farklı olarak; Medikal görüntü güvenliğini, elektronik hasta kaydı iletimini ve gruba güven mekanizmasını bir arada sunmaktadır. Tez çalışmasında önerilen ve Morley'in üçgen teoremini kullanan geometri tabanlı bir diğer gizli görüntü paylaşım şeması, literatürde ilk olarak, pay görüntülerinin bozulması durumunda dahi gizli görüntüyü yeniden yapılandırabilme yeteneğine sahiptir. Önerilen gizli görüntü paylaşım şemalarından elde edilen sonuçların literatürdeki benzer çalışmalarla kıyaslaması gerçekleştirilerek üstünlükleri ortaya konmuştur.

Anahtar Kelimeler: Sır paylaşımı, Gizli görüntü paylaşımı, Steganografi, Morley'in üçgen teoremi.

PhD. Thesis

SUMMARY

IMPROVEMENTS IN SECRET IMAGE SHARING SCHEMES AND THE DESIGN OF A NEW GEOMETRY BASED TECHNIQUE

Güzin ULUTAŞ

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering Graduate Program
Supervisor: Prof. Dr. Vasif V. NABİYEV
2012, 196 Pages, 12 Pages Appendix

Secret image sharing problems are investigated in this thesis and new schemes are proposed to overcome these. Proposed schemes are designed to deal with problems such as improving PSNR of shares, increasing number of authentication bits without degrading share quality, reducing cover image size to hide shares, recovering cover images after the reconstruction of secret image and make use of adaptive authentication depending on both cover and secret images. A new secret image sharing scheme for medical images is also considered and developed. Proposed medical image sharing scheme not only deals with security of secret image but also handles electronic patient record and introduces trust mechanism to a group of shareholders different from similar studies reported in the literature. Another secret image sharing scheme based on the Morley's triangle theorem is proposed to recover the secret image even if shares are distorted.

Results are compared with similar studies reported in the literature to reveal the strengths of proposed secret image sharing schemes.

Keywords: Secret sharing, Secret image sharing, Steganography, Morley's triangle theorem.

ŞEKİLLER DİZİNİ

Sayfa No

TABLOLAR DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

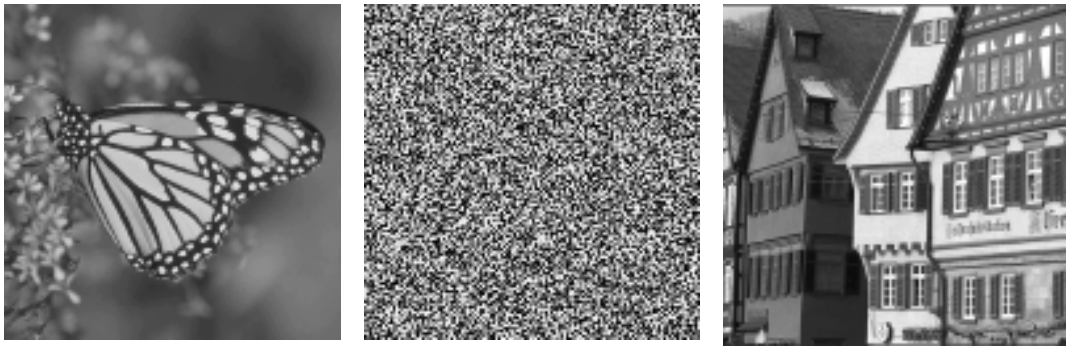
BBPS	: Bozulduğu belirlenen piksel sayısı
BPCS	: Bit düzeyinde karmaşıklık ayrıştırması(Bit plane complexity segmentation)
BPS	: Bozulmuş piksel sayısı
CRT	: Çinli kalan teoremi (Chinese Remainder Theorem)
DCT	: Ayrık kosinüs dönüşümü (Discrete Cosine Transform)
DO	: Doğrulama oranı
EMD	: Değişim yönünü kullanma (Exploiting modification direction)
FIPS	: Federe bilgi işleme standartları (Federal information processing standarts)
GF	: Galois cismi (Galois Field)
GSP	: Görsel sır paylaşımı (Visual secret sharing)
HMAC	: Özüt fonksiyonuna dayanan mesaj doğrulama kodu (Hash based message authentication code)
KK	: Kuadratik kalan (Quadratic residue)
KKO	: Kuadratik kalan olmayan(Quadratic non-residue)
KPS	: Kullanılan örten piksel sayısı
KS	: Karakter sayısı
LSB	: En anlamsız bit (Least significant bit)
MD5	: Mesaj özütü 5 (Message Digest 5)
NIST	: Ulusal standart ve teknoloji enstitüsü (National institute of standarts and technology)
OGSP	: Olasılıklı görsel sır paylaşma şeması (Probabilistic visual secret sharing)
OPAP	: En etkin piksel ayarlama süreci (Optimal pixel adjustment process)
PBGK	: Piksel başına düşen gömme kapasitesi
PSNR	: Tepe sinyal gürültü oranı (Peak to signal noise ratio)
PVD	: Piksel değer farklılıkları (Pixel value differencing)
RSA	: Rivest Shamir Adleman (Rivest Shamir Adleman)
SPIHT	: Hiyerarşik ağaçlarda küme bölütleme (Set Partitioning in Hierarchical Trees)
TPS	: Örten görüntüdeki toplam piksel sayısı
VQ	: Vektör kuantalama (Vector quantization)
WPSNR	: Ağrlıklı tepe sinyal gürültü oranı (Weighted PSNR)

1. GENEL BİLGİLER

1.1. Giriş

Internet üzerinden gizli görüntülerin iletimi esnasında veri güvenliğinin sağlanması son yıllarda araştırmacılar tarafından rağbet gören bir konu haline gelmiştir. Aktarılmak istenen görüntünün siyasi, askeri veya tıbbi önem taşıması durumunda, kötü niyetli kişiler tarafından görüntülenmesine engel olmak amacıyla, araştırmacılar tarafından farklı yöntemler uygulanmıştır [1-25]. Kriptografi ve steganografi gizli görüntü güvenliğini sağlamada kullanılan iki yaygın tekniktir [1, 2].

Kriptografinin kullanılması durumunda gizli görüntü taraflar arasında iletilmeden önce paylaşılan bir anahtar değeri ile şifrelenmektedir. Şekil 1.1'de verilen gizli görüntünün, kullanılan simetrik şifreleme algoritması sonucunda Şekil 1.1(a)'de verilen şifreli görüntüye dönüştürüldüğü görülmektedir. Şifrelenmiş görüntülerin ağ üzerinden iletimi esnasındaki en büyük problemlerden biri gürültü benzeri yapılarının kötü niyetli kişilerin dikkatini çekecek olmasıdır. Bu problemin üzerinden gelebilmek amacıyla araştırmacılar steganografinin kullanımını önermiştir [9-25]. Eski bir yunanca kelime olan ve "Saklı Yazma" anlamına gelen steganografi gizli veriyi dikkat çekmeyen bir ortam içerisine saklar. Örten ortam olarak adlandırılan ve gizli veriyi barındırmada kullanılan ortam görüntü, ses ya da video dosyası olabilir. Şekil 1.1(b)'de gizli görüntünün örten ortam içerisine saklanması durumunda üretilen stego ortam verilmiştir.



(a) (b) (c)

Şekil 1.1. (a)128×128 büyüklüğündeki gizli görüntü (b) Şifreli görüntü (c) 256×256 büyüklüğündeki stego görüntü

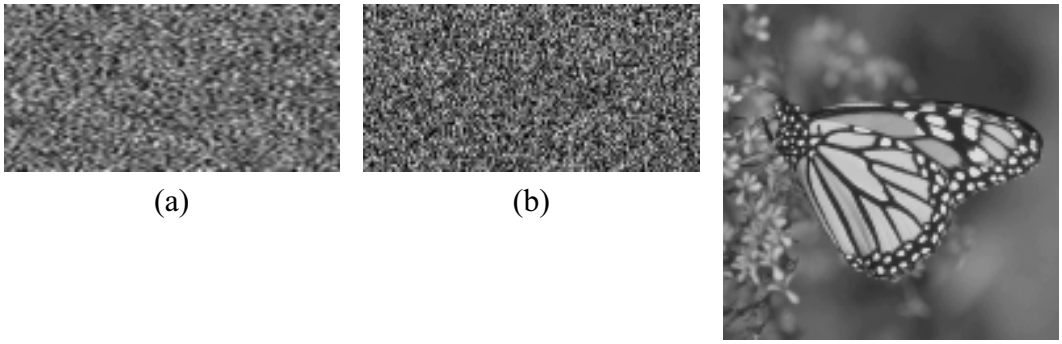
Şekil 1.1(a) ve Şekil 1.1(b)'de verilen her iki teknik gizli görüntü güvenliğini sağlasa dahi etkilendikleri ortak sorunlar vardır. Sorunlardan biri şifreli resmin ya da stego ortamın kaybolması durumunda gizli görüntünün yeniden yapılandırılamayacak şekilde kaybolmasıdır. Bir diğer sorun ise gizli görüntünün iletimi esnasında karşıdaki kişiye güven problemidir. Askeri haritalar ya da ticari önem taşıyan görüntüler gibi bazı verilerin, ancak birden fazla kişinin bir araya gelmesi durumunda yeniden elde edilmesi istenir. Örneğin bir bankanın kasasına giriş için kullanılan şifre görüntüsünün ancak banka yöneticilerinin hepsinin bir araya gelmesi durumunda elde edilmesi istenen bir gizlilik politikası olabilir. Birden fazla kişiye güven gerektiren böyle durumlarda steganografi veya kriptografi kullanılamamaktadır.

Naor ve Shamir 1994 yılındaki çalışmalarında, Görsel Sır Paylaşım (GSP-Visual Secret Sharing) şeması olarak adlandırılan ve yukarıda bahsi geçen probleme çözüm getiren yeni bir teknik önermiştir [3]. Bu şema için paylaşılan sır gizli bir görüntüdür (el yazısı notları, yazıcı çıktıları, resimler gibi). Bu yeni sır paylaşım tekniğinin en önemli özelliği, başka bir hesaplamaya ihtiyaç duymaksızın insan görme sistemini, gizli veriyi ortaya çıkarmada kullanmasıdır. Geleneksel şifreleme tekniklerinin, şifre çözme için gerektirdiği karmaşık hesaplamalar yeni alanda yer almamaktadır. *(k, n)* GSP şeması için, sır sahibi olan kişi, gizli görüntüden görsel şifreleme tekniklerini kullanarak *n* tane anlamsız pay oluşturur ve sırı paylaşacağı gruptaki alıcıların her birine bir adet pay gönderir. Paylar; aslında anlam ifade etmeyen gürültü benzeri görüntülerdir. Gizli görüntünün ortaya çıkarılabilmesi için en az *k* adet kişinin kendi paylarını asetat üzerine basmaları ve bu slaytları tam olarak üst üste getirmeleri gerekmektedir. Gizli veri, görsel şifreleme teknikleri kullanılarak paylara dağıtıldığı için, kötü amaçlı kişiler herhangi tek bir paydan gizli görüntüyü elde edemeyecektir. Naor ve Shamir tarafından önerilen bu şemayı (GSP) geliştirmek amacı ile araştırmacılar çeşitli yaklaşımlar önermiştir. İletilen sır sayısının artırılması, pay görüntülerindeki karşıtlığın iyileştirilmesi, iletilen sır görüntülerinin renkli olarak tanımlanabilmesi, pay görüntülerindeki genişleme oranının iyileştirilmesi, genişleme oranını azaltmak için önerilen Olasılıklı Görsel Sır Paylaşım Şeması (OGSP-Probabilistic Visual Secret Sharing) şemaları ve üretilen pay görüntülerindeki rasgeleliğin sağlanması çalışmaların hedefini teşkil etmiştir [40-57].

GSP şemalarının en büyük problemi genişleme oranı ve yeniden elde edilen gizli görüntüdeki düşük karşıtlıktır. Gizli görüntünün yeniden elde edilmesi aşaması her ne

kadar sayısal bir hesaplama gerektirmese dahi pratik anlamda kullanımı zordur. Tüm bu nedenlerle 2002 yılında Thien ve Lin tarafından, Gizli Görüntü Paylaşımı olarak adlandırılan yeni bir teknik önerilmiştir [4]. Bu teknik Shamir'in 1979 yılında önermiş olduğu (k, n) eşik şeması yönteminin görüntülere uyarlanmış halidir [5]. Gizli görüntü katılımcılar arasında pay görüntülerine bölünürken, her pay görüntüsü orijinal gizli görüntünün $1/k$'sı büyüklüğündedir. En az k tane katılımcının bir araya gelmesi durumunda gizli görüntü hatasız olarak yeniden yapılandırılacaktır. GSP şemalarından farklı olarak, gizli görüntünün yeniden elde edilmesi aşamasında matematiksel işlemlerin kullanımını gerektirir. Yalnız GSP şemalarında gizli görüntünün hatasız olarak yeniden yapılandırılabilmesi söz konusu değildir.

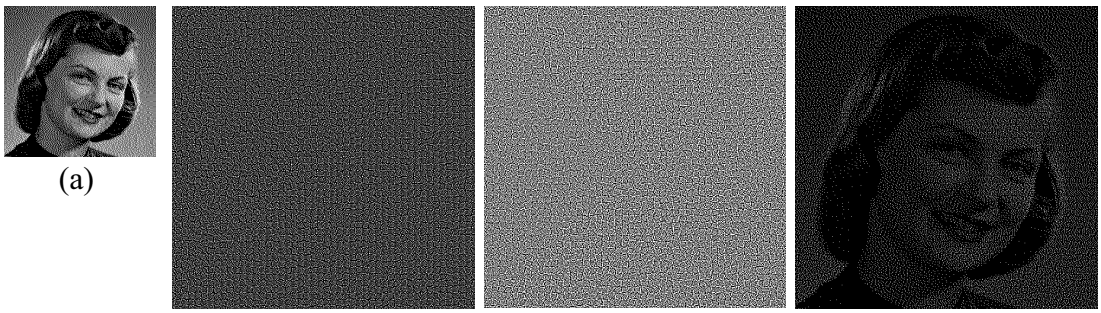
Şekil 1.2(a)-(b)'de gizli görüntünün (2, 2) gizli görüntü paylaşım şeması kullanılarak paylaştırılması sonucu elde edilen pay görüntüleri verilmektedir. Şekil 1.2(c)'de ise bu iki pay görüntüsü kullanılarak elde edilen yeniden yapılandırılan gizli görüntü verilmiştir. Pay görüntü büyüklükleri şekilden de gözlemlenebileceği gibi gizli görüntünün yarısı kadardır. Şekil 1.2(c)'de elde edilen görüntü orijinal gizli görüntü ile birebir aynıdır.



(a) (b) (c)

Şekil 1.2. (a)-(b) (2, 2) şemasının üretmiş olduğu pay görüntüleri (c) Yeniden yapılandırılan gizli görüntü

Şekil 1.3. (b)-(c)'de, Şekil 1.3.(a)'da verilen gizli görüntünün (2, 2) GSP şeması ile paylaştırılması sonucu elde edilen pay görüntüleri gösterilmiştir. Her iki pay görüntüsünün asetatlara basılarak üst üste getirilmesi durumunda elde edilen yeniden yapılandırılan gizli görüntü Şekil 1.3(d)'de yer almaktadır. Elde edilen gizli görüntü, şekilden de gözlemlenebileceği gibi düşük karşıtlık değerine sahiptir. Aynı zamanda kodlama sonucu elde edilen pay görüntüleri, gizli görüntünün en ve boy yönünde iki katı kadardır.



(a) (b) (c) (d)

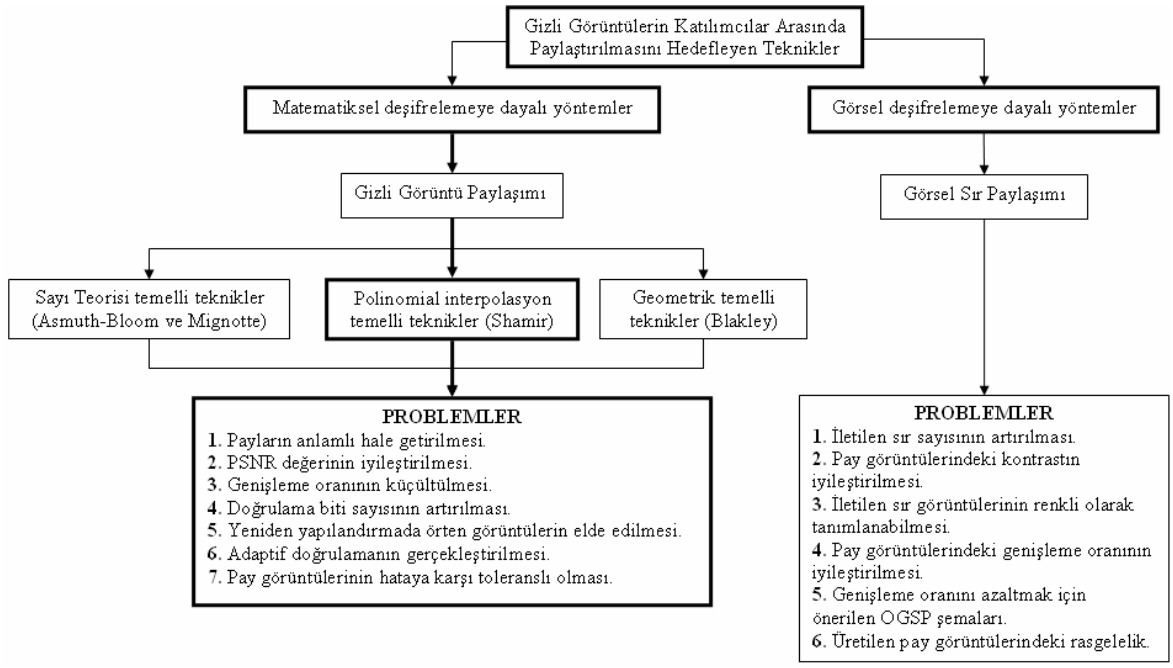
Şekil 1.3. (a) 128×128 büyüklüğünde gizli görüntü (b)-(c) 256×256 büyüklüğündeki pay görüntüleri (d) 256×256 büyüklüğündeki yeniden yapılandırılan görüntü

Şekil 1.4'te genel olarak gizli görüntü paylaşımı problemi için literatürde var olan çalışmaların gruplaması gerçekleştirilmiştir. Literatürdeki gizli görüntü paylaşım şemaları var olan eşik şemalarını kullanmaktadır. Shamir'in polinomial yaklaşımı bu alanda genel olarak kullanılan teknik olmuştur. Yapılan bazı çalışmalar Blakley'in geometri tabanlı eşik şeması yöntemini ve sayı teorisine dayanan şemaları da gizli görüntü paylaşımı alanında kullanmıştır [6-8]. Gerek GSP gerekse gizli görüntü paylaşımı alanındaki ihtiyaçlar da ilgili şekilde vurgulanmıştır. Depolama gereksinimleri, yeniden yapılandırılan gizli görüntünün doğruluğu ve yönetilebilirliğinin kolaylığı nedeni ile son yıllarda gizli görüntü paylaşımının kullanımı diğer yönteme kıyasla daha çok yaygınlık kazanmıştır.

Gizli görüntü paylaşımını Shamir'in yöntemi ile gerçekleştiren 2002 yılındaki ilk çalışmanın ardından, araştırmacılar çeşitli hedefleri gerçekleştirmeye çalışan yeni gizli görüntü paylaşım şemaları önermişlerdir. Yeni önerilen gizli görüntü paylaşım şemalarının hedefleri kısaca aşağıdaki şekilde özetlenebilir:

1. Üretilen gürültü benzeri pay görüntülerinin steganografik yöntemlerle saklanması.
2. Üretilen pay görüntülerinin örten ortamlar içerisine saklanması sonucu elde edilen stego görüntülerin PSNR değerinin iyileştirilmesi.
3. Stego görüntülerde meydana gelen genişleme oranının küçültülmesi.
4. Stego görüntüleri onaylamada kullanılan doğrulama bit sayısının PSNR değerini de bozmayacak şekilde artırılması.

5. Üretilen stego görüntülerden yeniden yapılandırma aşamasında örten görüntülerin elde edilmesi.
6. Gizli görüntü büyüklüğü ve stego görüntü büyüklüğüne bağlı olarak adaptif doğrulamanın gerçekleştirilmesi.
7. Üretilen pay görüntülerinin hataya karşı toleranslı hale getirilmesi.



Şekil 1.4. Gizli görüntülerin iletiminde kullanılan yöntemlerin sınıflandırılması

Bu tez çalışmasında gizlilik gerektiren görüntülerin (askeri, medikal vb.) güvenliğini sağlayabilmek için, verilen amaçlar doğrultusunda literatürde var olan yöntemlere kıyasla daha iyi sonuçlar üreten yeni gizli görüntü paylaşım tekniklerinin önerilmesi ve eşik şemalarına dayanan gizli görüntü paylaşım şemalarının performans değerlendirilmesinin gerçekleştirilmesi veya varolan sorunların giderilmesi hedeflenmiştir. Aynı zamanda literatürdeki eşik şemalarını kullanan görüntü paylaşım şemalarında olmayan "Pay görüntüsünde meydana gelecek bozulmalarda dahi gizli görüntüyü belirli bir oranda yeniden yapılandırabilme özelliğine sahip", yeni bir geometri tabanlı gizli görüntü paylaşım şemasının tasarlanması ve gerçekleştirilmesi amaçlanmıştır.

Tez kapsamında Blakley'in yöntemine dayanan şemalardaki pay görüntüsünün rasgeleliği probleminin üstesinden gelinmiş ve Shamir tabanlı yöntemlere kıyasla genişleme oranı açısından dört kat iyileştirme sağlanmıştır. Shamir tabanlı yöntemlerdeki

PSNR değerini iyileştirebilmek ve doğrulama bit sayısını artırabilmek amacıyla, pay değerlerinin ifade edilmesi esnasında yeni bir aralıklandırma prosedürü kullanılmıştır. Pay değerlerini temsil etmede kullanılan bit sayısı optimum olarak seçilmiş böylece PSNR değerini kötüleştirmeden maksimum doğrulama yeteneğinin kazandırılması hedeflenmiştir. Adaptif doğrulamayı sağlayabilmek için önerilen yöntem, örten görüntü ve gizli görüntü büyüklüğüne bağlı olarak blok büyüklüğünü belirlemekte ve değişen blok büyüklükleri için değişen sayıda doğrulama biti kullanmaktadır. Doğrulama bitinin örten blok büyüklüğüne bağlı olarak değiştirilmesi, yöntemin doğrulama yeteneğini iyileştirmiştir. Aynı zamanda Eslami'nin çalışmasındaki zincir doğrulama tekniğindeki problemler tespit edilmiş ve önerilen yeni doğrulama tekniği ile problemin üstesinden gelinmiştir. Gizli görüntü paylaşım şemalarındaki geri döndürülebilirliği sağlamak amacıyla (stego görüntülerden örten görüntülerin elde edilmesi) önerilen yöntem, EMD (Exploiting Modification Direction) denklemini görüntü paylaşımında kullanılacak şekilde adapte etmiştir. Aynı zamanda modulo operatörünün de yöntem tarafından uyarlanması ile yeni bir şemanın tasarımı gerçekleştirilmiştir. Literatürde var olan çalışmaların örten piksel parlaklık değerine bağımlı olduğunu tespit eden çalışma, PSNR değeri açısından başarılı sonuçlar üretmektedir. Gizli görüntünün medikal görüntü olması durumu değerlendirilmiş ve literatürde ilk kez hem medikal görüntü güvenliğini sağlayan hem de elektronik hasta kayıt bilgisini gizleyen yeni bir çalışma tez kapsamında önerilmiştir. Shamir'in, Blakley'in, Asmuth-Bloom'un ve Mignotte'nin eşik şemalarını kullanan gizli görüntü paylaşım şemaları tasarlanmış ve hedefler doğrultusundaki performans değerlendirmeleri yapılmıştır. Ayrıca var olan paylaşım tekniklerinde, pay görüntülerinin bozulması durumunda, gizli görüntünün yeniden yapılandırılmayacak şekilde bozulduğu ortaya konmuştur. Gerek var olan eşik şemalarını kullanmayan gerekse bozulmalara karşı dayanıklı olan yeni bir geometri tabanlı gizli görüntü paylaşım şemasının tasarımı gerçekleştirilmiştir.

İlerleyen bölümlerde veri güvenliğinin sağlanması için kullanılan steganografiden bahsedilecek ve bu alandaki çeşitli çalışmalar incelenecektir. Ardından sır paylaşım şemalarını oluşturan temel unsurlar ortaya konup, eşik şemalarının detayları üzerinde durulacaktır. Son olarak gizli görüntü paylaşım şemalarının, iyileştirme sağladıkları hedefler doğrultusunda gruplaması gerçekleştirilecektir. Her grupta yer alan temel çalışmalar ilgili bölümlerde detayları ile beraber yer alacaktır.

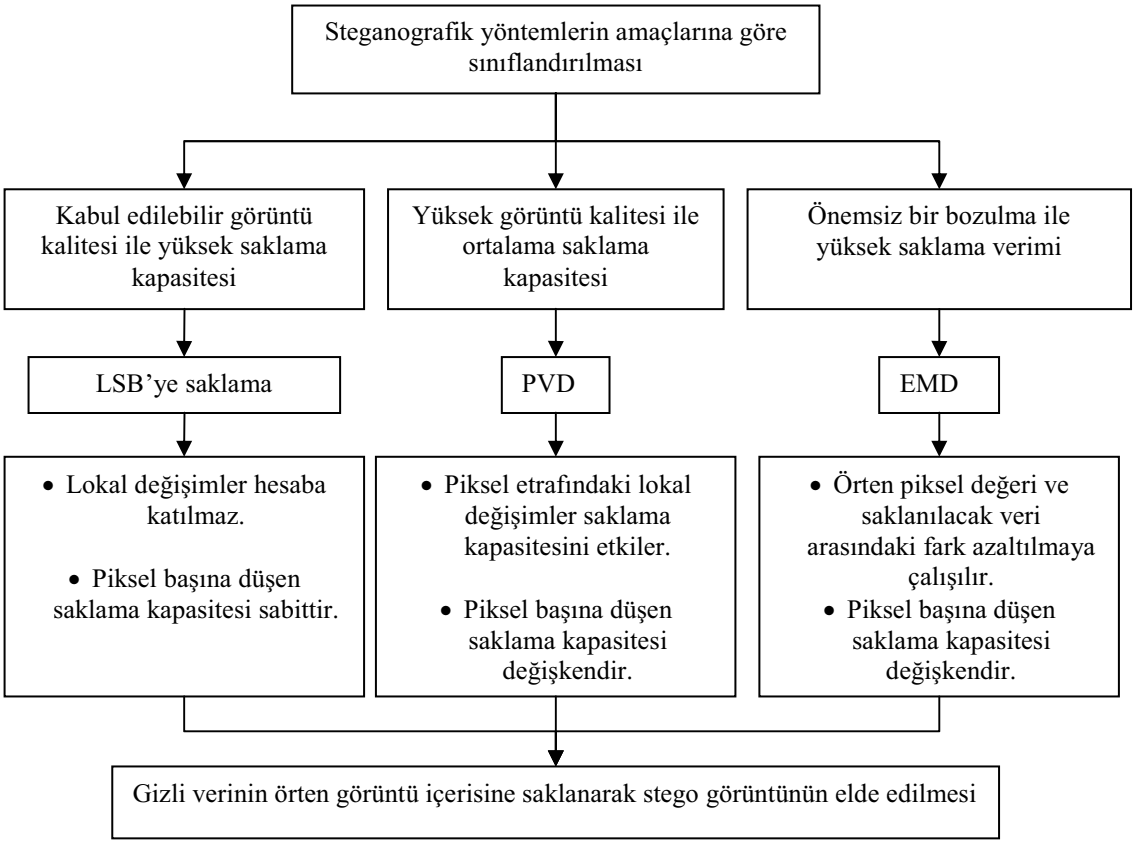
1.2. Steganografi

Steganografi, taraflar arasında iletilen verinin güvenliğini sağlamak amacıyla gizli veriyi farklı bir sayısal ortam içerisine saklamada kullanılan tekniktir. Veri güvenliğini sağlamadaki yaklaşımlardan diğeri olan kriptografi ise, gizli veriyi kullanılan matematiksel transformasyon yoluyla okunamayan bir hale dönüştürme sanatıdır [1, 2]. Şifreli sayısal ortamın rasgelelik içeriyor olması, veri haberleşmesinin kötü niyetli kullanıcıların ilgisini çekme olasılığını yükseltmektedir. Bu açıdan bakıldığında, gizli veriyi; resim, video ya da ses dosyası gibi olağan sayısal ortamlar içerisine saklayan steganografi, veri güvenliğinin sağlanmasında daha etkin olmaktadır.

Steganografik tekniklerin gizli veriyi saklamada kullandıkları sayısal veri "örten ortam", saklama işleminin ardından oluşan sayısal veri ise "stego ortam" olarak adlandırılmaktadır. Örten ortam olarak kullanılan sayısal dosya ses, video ya da görüntü dosyası olabilir. Fakat son yıllarda literatürde yapılan çalışmalarda ağırlıklı olarak görüntü dosyaları örten ortam olarak kullanılmakta ve önerilen teknikler gizli veriyi görüntü dosyaları içerisine saklamaktadır. Saklama ardından oluşan stego görüntünün görsel kalitesi ve örten ortam içerisine saklanabilen veri miktarı, steganografik tekniklerin karşılaştırılmasında araştırmacılar tarafından kullanılmaktadır. Saklanabilen veri miktarındaki artış, stego ortamın görsel kalitesindeki düşüşü beraberinde getirmektedir. Tekniklerin karşılaştırılmasında kullanılan bu iki parametre arasında bir denge bulabilmek yöntemin uygulanabilirliği açısından önemlidir. Örten görüntü ve stego görüntü arasındaki farkların karelerinin toplamı, veri saklama sonrasında oluşan bozulma oranı hakkında bilgi vermektedir. PSNR (Peak to Signal Noise Ratio) olarak adlandırılan ve ifadesi (1.1)'de verilen oran, araştırmacılar tarafından steganografik tekniklerin karşılaştırılmasında kullanılmaktadır. İfade de $N \times M$ büyüklüğündeki örten ve stego görüntüler sırasıyla C ve ST ile gösterilmektedir.

$$PSNR = 10 \times \log_{10} \frac{(255)^2}{MSE} \, dB$$
$$MSE = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \left(C_{ij} - ST_{ij} \right)^2 \tag{1.1}$$

Gri seviye bir görüntüye veri saklama sonrasındaki piksel parlaklık değerlerindeki değişimin, insan gözü tarafından ayırt edilebilirliğinin düşük olması, yapılan çalışmalarda örten ortam olarak gri seviye resimlerin kullanılmasına sebebiyet vermiştir. Saklama algoritmasının tasarlanmasında, insan görme sisteminin duyarlılığının hesaba katılmasına bağlı olarak, literatürde önerilen yöntemler üç gruba ayrılmaktadır [21]. (1) Kabul edilebilir görüntü kalitesi ile yüksek saklama kapasitesi, (2) Yüksek görüntü kalitesi ile ortalama saklama kapasitesi, (3) Önemsiz bir bozulma ile yüksek saklama verimliliği. Şekil 1.5'te amaçları doğrultusunda steganografik yöntemlerin sınıflandırılması gösterilmiştir.



Şekil 1.5. Steganografik yöntemlerin amaçları doğrultusunda sınıflandırılması

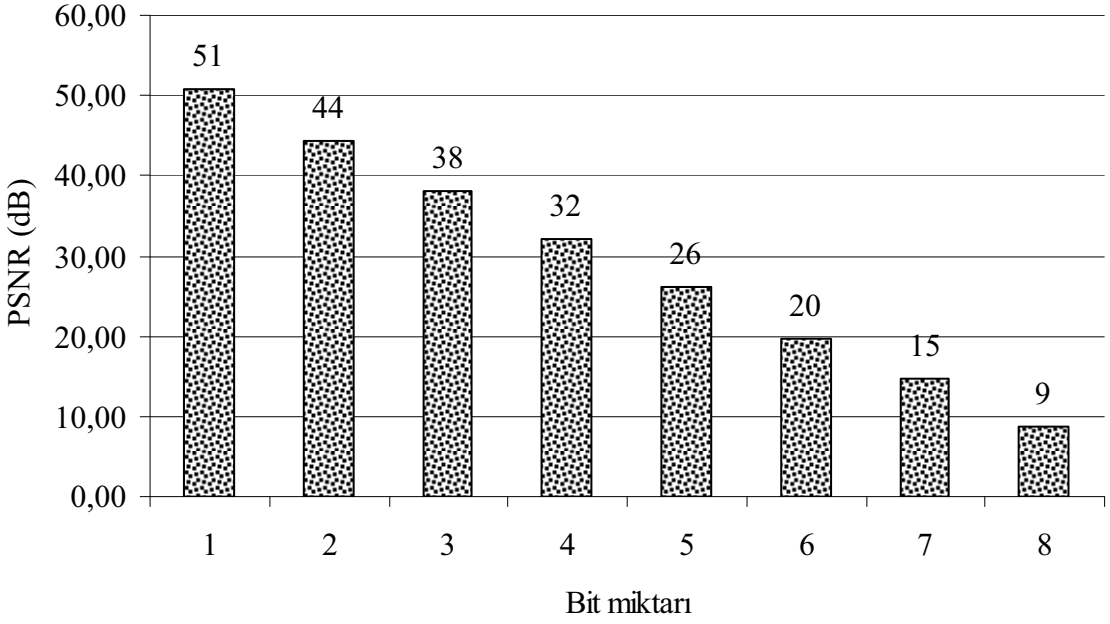
İlk grupta yer alan tekniklerde, saklama kapasitesinin kestiriminde kullanılan mekanizma, görüntüdeki yerel dokuları hesaba katmaz. Örten görüntüdeki her pikselin saklama kapasitesi, keskin ya da yumuşak geçişli bir bölgede olmasına bakılmaksızın, aynıdır. Bu gruptaki bilinen en genel saklama prosedürü en anlamsız bite yerleştirme (LSB

– Least Significant Bit Embedding) yöntemidir. Örten görüntüdeki piksel parlaklık değerlerinin en anlamsız bitleri, gizli veriyi saklamada kullanılmaktadır. İlk grupta yer alan teknikler aynı zamanda LSB şemaları olarak da adlandırılabilir. Bit düzeyinde yapılan değişimler insan gözünün fark edemeyeceği ölçekte olmaktadır. Yapılan bazı çalışmalarda LSB yaklaşımları üç boyutlu modeller, dokümanlar ve ikili görüntülere de uygulanmıştır [23-25]. Bugüne kadar, birçok çalışma yüksek saklama kapasitesi sunan LSB şemalarındaki görüntü kalitesinin iyileştirilebilmesini hedeflemiştir. Piksel parlaklık değerlerinin en anlamsız üç bitinin kullanımı, görsel açıdan fark edilmemeyi sağlarken, en yüksek saklama kapasitesini sunmaktadır. Son üç bitin veri saklamada kullanılması durumunda elde edilen görüntünün PSNR değeri yaklaşık olarak 38 dB civarındadır. Saklama kapasitesi açısından bakıldığında, bu gruptaki teknikler diğer yöntemlere nazaran daha fazla bilgi saklayabilmektedir. Şekil 1.6'da, kullanılan en anlamsız bit sayısına bağlı olarak üretilen stego görüntünün PSNR değerindeki değişim örneği verilmiştir. Hesaplanan değerler, gizli görüntünün bütün piksellerine rasgele veri saklanması durumunda ölçülen PSNR değerleridir. Ortalama PSNR değerinin elde edilebilmesi için, 100 saklama işleminin sonucu değerlendirilmiştir.

Thien ve Lin, 2003 yılında yapmış oldukları çalışmada, modulo operatörünü kullanarak yeni bir saklama yöntemi önermişlerdir [9]. Yöntem $[0, m)$ aralığındaki verileri saklama esnasında, klasik LSB'ye gömme prosedürüne göre daha iyi sonuçlar üretmektedir. Saklama ve saklanan veriyi çıkarma aşamalarında işlem karmaşıklığı açısından klasik LSB kadar basit olan yöntem, aynı zamanda yüksek saklama kapasitesine de sahiptir. 512×512 boyutlarındaki bir örten görüntü içerisine, 256×512 ya da 256×256 büyüklüğünde gizli görüntü saklanabilmektedir. Yöntem aynı zamanda piksel başına düşen değişim oranının $\lceil (m-1)/2 \rceil$'den az olduğunu göstermiştir.

Chan ve Cheng, OPAP (Optimal Pixel Adjustment Process-En etkin piksel ayarlama süreci) olarak adlandırılan yeni bir yöntemi 2004 yılında yaptıkları çalışmada önermişlerdir [10]. Çalışmaları örten görüntü ve klasik LSB'ye saklama yöntemi sonucu elde edilen stego görüntüyü aynı anda değerlendirmektedir. Klasik LSB'ye gömme işlemi ardından üretilen stego görüntü OPAP prosedüründen geçirildikten sonra, içerisinde sakladığı bilgiler değişmemesine rağmen, daha yüksek PSNR değerine sahip olmaktadır. Elde etmiş oldukları deneysel sonuçlar OPAP prosedürü tarafından işleme konulan stego görüntünün PSNR değerinin, klasik LSB sonucu elde edilen stego görüntüye kıyasla, $[0-3]$ dB

arasında arttığını göstermektedir. Klasik LSB yönteminde yalnızca 1 bitin veri saklamada kullanılması durumunda, OPAP prosedürünün uygulanmasının ardından, stego görüntünün PSNR değerinde bir değişim gözlemlenmemektedir. Fakat son iki bitin veri saklamada kullanılması durumunda, OPAP ardından oluşan görüntünün PSNR değeri 2 dB civarında artış göstermiştir. Her ne kadar önerilen yöntem, saklama sonrası oluşan stego görüntünün yeniden bir işleme tabi tutulmasını gerektirse de görsel kalitedeki iyileşim yadsınamayacak ölçüdedir.



Şekil 1.6. Kodlamada kullanılan bit miktarına bağlı olarak PSNR değişimi

2005 yılında yapılan bir çalışma, gizli görüntüyü örten görüntü içerisine saklarken modulo operatöründen faydalanmıştır [11]. Algoritmada kullanılan eşik değeri aynı zamanda yöntemin gizli görüntünün ne kadar bitini saklayabileceği hakkında da bilgi vermektedir. Diğer yöntemlere kıyasla yardımcı bir tabloya ihtiyaç duymazken, yüksek saklama kapasitesi sağlayabilmesi önemli bir avantaj olarak sunulmuştur. Elde edilen deneysel sonuçlarda vurgulandığı gibi, 256×256 büyüklüğündeki gizli görüntünün 512×512 büyüklüğündeki örten görüntüye saklanması durumunda üretilen stego görüntülerin PSNR değerleri, diğer yöntemlere kıyasla belirgin bir şekilde yüksektir.

2005 yılında Wu ve arkadaşları klasik LSB yöntemine ve 2003 yılında önerilen PVD (Pixel Value Differencing-Piksel Değer Farklılıkları) yöntemine dayanan yeni bir yöntem önermişlerdir [12]. PVD yönteminden faydalanılarak, iki komşu pikselden bir fark değeri

üretilmektedir. Küçük fark değerleri örten görüntüde değişimin az olduğu bölgelere, büyük fark değerleri ise değişimin yüksek olduğu köşeli bölgelere saklanmaktadır. OPAP'ın kullanıldığı yönteme kıyasla, stego görüntülerde iyi bir görsel kalite sunarken daha yüksek miktarda veri saklayabilmektedir. Yöntem esas olarak, saklanacak bit sayısını artırmayı hedeflemektedir.

İkinci gruptaki teknikler, Adaptif Steganografi Şemaları olarak adlandırılmaktadır. Bu grupta yer alan teknikler bir pikselin saklama kapasitesini tahmin ederken, komşu piksellerdeki parlaklık değişimlerini göz önüne almaktadır. Adaptif şemalar, saklama kapasitesine karar verirken, görüntüdeki lokal dokuyu ve insan görme sistemini hesaba katmaktadır. Adaptif steganografik şemalar, örten görüntüde, karmaşıklığı yüksek olan bölgelere daha çok gizli veri saklamaya çalışırken, karmaşıklığın az olduğu bölgelere daha az veri gömmeyi amaçlamaktadır. Böylece oluşan stego ortamdaki bozulmanın insan gözü tarafından ayırt edilmesinin engellenmesi hedeflenmiştir. LSB tabanlı şemaların sunduğu yüksek saklama kapasitesi, ikinci grupta yer alan adaptif şemalar için bir hedef olmamaktadır. Adaptif şemaların oluşturduğu stego görüntülerdeki bozulmaların, saklama işlemi lokal bölgelerdeki karmaşıklıklara uygun olarak gerçekleştirildiğinden, insan gözü tarafından ayırt edilmesi daha güçtür.

Gizli mesajı gri seviye örten görüntü içerisine saklamak için 2003 yılında önerilen PVD yöntemi, örten görüntüyü örtüşmeyen ikili piksel gruplarına ayırmaktadır [13]. Saklama algoritması tarafından her bloktaki piksel değerleri kullanılarak fark değeri hesaplanır. Bütün mümkün olabilir fark değerleri aralıklar halinde sınıflandırılmaktadır. Aralıkların belirlenmesi, insan görme sisteminin gri seviye değerlerin değişimine olan duyarlılığının karakteristiğine bağlı olarak, yapılmıştır. Fark değeri, karşılık düşecek gizli veriyi temsil edecek ve insan gözü tarafından en az fark edilecek şekilde, yeni bir değerle değiştirilmektedir. Bir piksel çiftinin saklayabilecek olduğu bit miktarı, fark değerinin karşılık düştüğü aralığın genişliği ile belirlenmektedir. Önerilen metot, klasik LSB yöntemine nazaran, daha az fark edilebilir stego görüntüler üretmektedir. Stego görüntüye saklanan gizli mesaj, orijinal örten görüntüye ihtiyaç duymaksızın tekrar elde edilebilmektedir. Deneysel sonuçlarda önerilen yöntemin istatistiksel ataklara karşı dayanıklılığı gösterilmiştir.

Chang ve Tseng'in 2004 yılında yapmış oldukları çalışmada, saklama kapasitesini artırmak ve aynı zamanda stego görüntü kalitesini iyileştirmek için yan bilgisi kullanılmaktadır [14]. Önerilen yöntem komşu pikseller arasındaki korelasyon bilgisini

kullanarak, bölgenin yumuşak ya da sert geçişli bir bölge olup olmadığına karar vermektedir. Değişimin sert olduğu bir bölgede bulunan piksel, yumuşak geçişli bölgede yer alan piksele göre daha fazla veri saklayabilir. 2-yanlı, 3-yanlı ve 4-yanlı olarak adlandırılan üç farklı yöntemin kullanımı araştırmacılar tarafından önerilmektedir. Elde edilen deneysel sonuçlar, yöntemin belirgin bir bozulma yapmaksızın daha fazla sayıda bit saklayabildiğini göstermektedir. Bunun yanında, saklanan veri, orijinal örten görüntüye ihtiyaç duymaksızın stego görüntüden elde edilebilmektedir.

Zhang ve Wang, 2005 yılında çoklu taban sistemini ve insan görme sisteminin hassasiyetini kullanan yeni bir yöntem önermiştir [15]. Saklanacak olan veri, çoklu taban kullanan sayı sistemine çevrilir. Örten görüntüdeki piksel değerlerindeki lokal değişimlerin derecesi sayı tabanlarını belirlemede kullanılmaktadır. Karmaşıklığın çok olduğu bölgelerdeki pikseller daha çok veri saklayabilmektedir. Önerilen adaptif yaklaşımın, PVD yöntemine kıyasla, daha yüksek PSNR değerleri ürettiği deneysel sonuçlarda gösterilmiştir.

2008 yılında Wang ve arkadaşlarının önermiş olduğu yöntem, insan gözüyle bozulmanın fark edilemeyeceği stego görüntülerin üretimini amaçlamaktadır [16]. Bunun yanında, yöntem sınır dışına düşme probleminden kaçınmak için PVD yöntemini ve modulo operatörünü kullanmıştır. PVD yöntemi kullanılarak resimdeki ikili piksel gruplarından fark bilgileri üretilmektedir. İkili piksel gruplarının saklama kapasitesi, fark değeri ile ilişkilidir. İki pikselin kalanları modulo operatörü kullanılarak hesaplanmakta ve ardından gizli veri iki piksele, kalan değerlerini değiştirerek kodlanmaktadır. Aynı zamanda, kalanların değişimi esnasında, stego görüntünün daha az bozulmasını saklayabilmek amacıyla da yeni bir yaklaşım önermişlerdir. Deneysel sonuçlar yöntemin istatistiksel ataklara karşı dayanıklı olduğunu göstermektedir. Yöntemin saklama kapasitesi açısından PVD ile denk olmasına rağmen, daha yüksek PSNR değerlerine sahip olduğu sonuçlarda vurgulanmıştır.

Gelişmiş saklama kapasitesi ve daha yüksek PSNR değerleri üreten, PVD yaklaşımına dayalı bir diğer adaptif steganografik yöntem 2008 yılında Yang ve arkadaşları tarafından önerilmiştir [17]. Yöntem, iki piksel arasındaki fark değerini, gruba kaç bit verinin saklanabileceğini belirlemede kullanmaktadır. Kenar bilgisi taşıyan bölgelerdeki piksellerin saklamada kullanılan son k biti, yumuşak geçişli bölgelerdeki piksellere nazaran daha fazladır. Fark değer aralıkları adaptif olarak alçak, orta ve yüksek olarak seviyelendirilmiştir. İkili gruplardaki bütün piksellerin son k bitleri LSB yöntemi ile

veri saklamada kullanılmaktadır. Fakat hangi grubun son kaç bitinin saklamada kullanılacağı, fark değerinin karşılık düştüğü seviyeye bağlı olarak adaptif olarak belirlenmektedir. Saklama işleminin ardından yeniden hızalandırma prosedürü, gizli verinin çıkartılması aşamasındaki bozulmalara engel olabilmek amacıyla uygulanmaktadır. Wu ve arkadaşlarının çalışmasına kıyasla daha yüksek PSNR ve saklama kapasitesine sahip bir metottur.

Yüksek saklama verimliliğini sağlamaya çalışan üçüncü gruptaki çalışmalar ise, az miktarda verinin gömülmesi esnasında, görüntüde meydana gelen bozulmaların en aza indirgenmesini hedeflemektedir. Bu çalışmalarda, piksel başına düşen gömme kapasitesi 2 bit ya da daha azdır. Zhang ve Wang yapmış oldukları çalışmada saklama verimini, saklanan bit miktarı ile saklama işleminin sebep olduğu bozulma enerjisi arasındaki oran olarak vermiştir [18]. Mielikainen önermiş olduğu yöntemde iki piksele iki bit saklayacak şekilde ikili bir fonksiyonun kullanımını önermektedir [19]. Çalışmada piksel başına düşen bit miktarı 1 olarak ölçülmüştür. Piksel başına düşen beklenilen ortama kareler toplamı 0.375 ve saklama verimi $8/3$ olarak rapor edilmiştir. Hesaplanan değer yalnızca bir biti saklamada kullanan LSB tabanlı bir çalışmadan (piksel başına beklenilen ortalama kareler toplamı 0.5, saklama verimi 2.0) daha yüksek saklama verimine sahiptir. Zhang ve Wang, 2006 yılında, değişim yönünü kullanarak yeni bir saklama algoritması önererek, önceki çalışmalara kıyasla daha iyi sonuçlar elde etmektedir [20].

[19]'daki çalışma, LSB'ye saklama yönteminde, örten görüntüye bir ekleneceğimi yoksa bir çıkartılacağının mı tamamen rasgele belirlendiğinin üzerine vurgu yapmaktadır. Yöntem iki örten görüntü piksel değerini parametre olarak alan ikili bir fonksiyon kullanmaktadır. Saklama prosedürü ikili piksel grupları üzerinde işlem yapmaktadır. Birinci pikselin LSB değeri bir bit bilgi taşırken, iki piksel değerinin fonksiyon sonucu da bir bit değer taşımaktadır. Böylece yöntem, LSB'ye saklama yöntemi ile (son bir bitin saklama için kullanılması durumunda) aynı saklama kapasitesine sahip olmuştur. Fakat saklama esnasında örten görüntüde meydana gelecek değişimleri en aza indirgediği için daha yüksek PSNR değerlerine sahiptir. Aynı zamanda deneysel sonuçlar, yöntemin istatistiksel ataklara karşı dayanıklı olduğunu da göstermektedir.

[18]'deki çalışmada, örten görüntüde saklama esnasında oluşabilecek değişimlerin azaltılması ve böylece stego görüntülerin PSNR değerinin artırılması hedeflemektedir. Blok tabanlı kodlama yaklaşımlarından farklı olarak, her gizli veri biti, örten görüntü bitleri tarafından temsil edilmektedir. Aynı zamanda, örten piksel bitindeki değişim, birden

çok gizli veri bitini temsil edebilir. Deneysel sonuçlar yöntemin, örten görüntü piksel değerlerindeki değişimi azalttığı için, güvenilir olduğunu göstermektedir. Önerilen kodlama tekniğinin diğer veri saklama yaklaşımları ile kullanılabileceğine çalışmada vurgu yapılmaktadır.

Veri saklama alanındaki EMD (Exploiting Modification Direction, Değişim Yönünü Kullanma) olarak adlandırılan bir diğer yöntem, $(2n+1)$sayı sistemindeki gizli verinin n örten piksel ile beraber temsil edilebileceğini göstermiştir [20]. Gizli veri, n pikselden herhangi birinin parlaklık değerinin bir artırılması ya da bir azaltılması ile temsil edilebilmektedir. Başka bir deyişle n piksel üzerinde gerçekleştirilebilecek $(2n+1)$ değişim ile $(2n+1)$ tabanındaki tüm sayılar ifade edilmektedir. Her iki yöndeki değişimde tam anlamıyla kullanılabildiği için, önceki yöntemlere kıyasla yüksek saklama kapasitesine sahiptir.

Üç alt gruptaki steganografik teknikler içerisinden literatürde en çok ilgi gören OPAP, PVD ve EMD yöntemlerinin detayları ilerleyen bölümlerde sırasıyla verilmiştir.

1.2.1. OPAP Yöntemi ile Veri Saklama

Chan ve Cheng önermiş oldukları çalışmada LSB'ye saklama yönteminin kullanımı ile üretilen stego görüntülerin görsel kalitesini iyileştirmeyi hedeflemiştir [10]. LSB'ye saklama yöntemi ile üretilen stego görüntüler, saklama işleminin ardından, önerilen OPAP yöntemi ile ek bir işleme tabi tutulmaktadır. Elde edilen deneysel sonuçlar, OPAP kullanımı ardından üretilen stego görüntünün görsel kalitesinde önemli bir iyileşme olduğunu ortaya koymaktadır. Prosedüre ilişkin detaylar aşağıda verilmiştir. OPAP prosedürünün temeli Chan ve Cheng'in 2001'deki çalışmalarına dayanmaktadır [22]. Algoritma süresince kullanılacak bazı semboller ve tanımları aşağıda verilmiştir:

C Örten görüntü.

C' LSB'ye saklama yöntemi ile elde edilen stego görüntü.

C'' OPAP uygulanmasının ardından elde edilen stego görüntü.

p_i C ile gösterilen örten görüntüdeki *i*'inci piksel.

p_i' C' ile gösterilen stego görüntüdeki *i*'inci piksel.

p_i'' C'' ile gösterilen stego görüntüdeki *i*'inci piksel.

Örten görüntü ve stego görüntü pikseli arasındaki hata oranı, $\delta_i = p_i^{'} - p_i$ şeklinde olsun. $p_i^{'}$ değeri, p_i ile gösterilen örten görüntü piksel parlaklık değerinin son *k* bitinin gizli veri bit değerleri ile doğrudan yer değiştirilmesi ile elde edilmektedir. Bu nedenle örten görüntü ve stego görüntü pikselleri arasındaki hata oranını gösteren δ_i değeri (1.2) ile gösterilen aralıkta yer almaktadır.

$$-2^k < \delta_i < 2^k \tag{1.2}$$

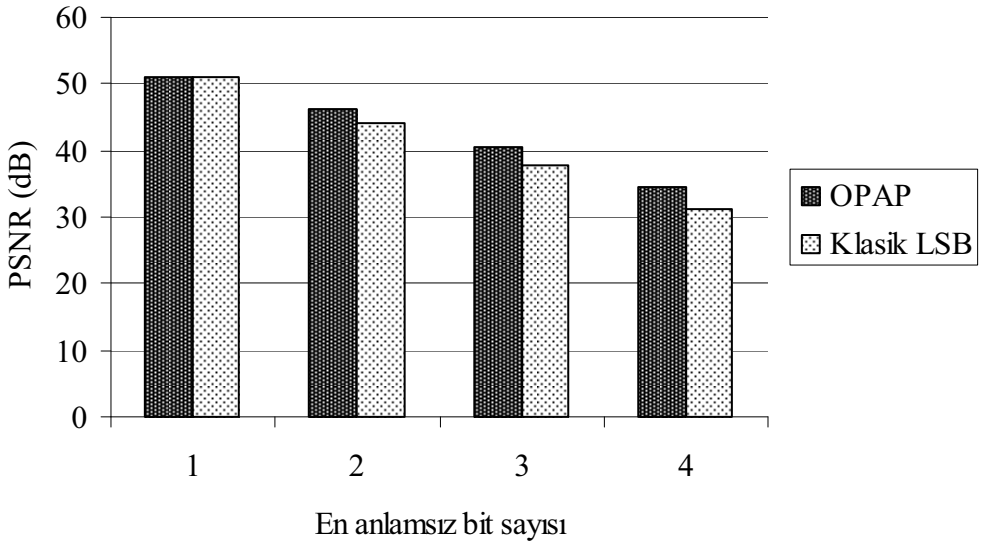
Hata oranı δ_i'nin karşı düştüğü aralık aşağıda verilmiş olan üç alt parçaya ayrılmaktadır.

Aralık I : $2^{k-1} < \delta_i < 2^k$ Aralık II : $-2^{k-1} \le \delta_i \le 2^{k-1}$ Aralık III : $-2^k < \delta_i < -2^{k-1}$

Hata oranının karşılık düştüğü aralığa ve $p_i^{'}$ ile gösterilen stego pikselin değerine bağlı olarak, OPAP prosedürü yeni stego piksel değerini (1.3)'te verilmiş olan kurallar yardımıyla belirler. Verilen adımların, karşılık düşen tüm stego piksellere uygulanması sonucu elde edilen stego görüntüdeki hata oranı LSB ile elde edilen stego görüntüye kıyasla daha az olacaktır. OPAP işlemi sonucunda elde edilen ikinci stego görüntü aynı zamanda gizli veriyi de içermektedir. Önerilen yöntemin araştırmacılar tarafından elde edilen deneysel sonuçlarında, LSB'ye gömme işlemi esnasında bir bitin kullanılması durumunda, OPAP prosedürünün görsel kalite açısından katkı sağlamadığını göstermektedir.

$$\begin{aligned}
&\left(2^{k-1} < \delta_i < 2^k\right) \wedge \left(p_i^{'} \ge 2^k\right) \Rightarrow p_i^{''} = p_i^{'} - 2^k \\
&\left(2^{k-1} < \delta_i < 2^k\right) \wedge \sim \left(p_i^{'} \ge 2^k\right) \Rightarrow p_i^{''} = p_i^{'} \\
&\left(-2^{k-1} \le \delta_i \le 2^{k-1}\right) \Rightarrow p_i^{''} = p_i^{'} \\
&\left(-2^k < \delta_i < -2^{k-1}\right) \wedge \left(p_i^{'} < 256 - 2^k\right) \Rightarrow p_i^{''} = p_i^{'} + 2^k \\
&\left(-2^k < \delta_i < -2^{k-1}\right) \wedge \sim \left(p_i^{'} < 256 - 2^k\right) \Rightarrow p_i^{''} = p_i^{'}
\end{aligned} \tag{1.3}$$

Fakat son iki bitin saklamada kullanılması durumunda elde edilen PSNR değerlerinde yaklaşık 2 dB civarında iyileşme gözlemlenmektedir. Şekil 1.7'de örten görüntü piksellerinin son kaç bitinin veri taşımada kullanıldığına bağlı olarak, üretilen stego görüntülerin PSNR değerinin karşılaştırmalı grafiği verilmiştir. Şekilden de gözlemlenebileceği gibi, bit sayısı arttıkça OPAP işlemi üretmiş olduğu PSNR değerleri açısından daha başarılı sonuçlar vermektedir.



Şekil 1.7. OPAP yönteminde kullanılan bit miktarına bağlı olarak PSNR değişimi

1.2.2. PVD Yöntemi ile Veri Saklama

Wu ve Tsai, 2003'deki çalışmalarında gizli mesajları gri seviye görüntüler içerisine saklamada kullanılacak yeni bir yöntem önermişlerdir [13]. Gizli mesajın saklanması aşamasında ilk olarak örten görüntü ikili piksel gruplarına parçalanmaktadır. Her bloktaki piksellerin arasındaki fark değeri hesaplanmakta ve hesaplanan fark değerleri önceden belirlenen aralıklara karşı düşürülmektedir. Aralıklar, insan görme sisteminin gri seviye bir görüntüdeki yumuşak ve sert geçişlere olan tepkisi göz önüne alınarak belirlenmektedir. İki piksel arasındaki fark değeri, gizli mesajın bir kısmını ifade edecek şekilde önerilen algoritma tarafından değiştirilmektedir. O anki piksel bloğuna gömülebilecek olan bit miktarı, fark değerinin karşılık düştüğü aralığın genişliğine göre belirlenmektedir. Önerilen yöntem değişimin aralık dışına çıkmasına engel olacak şekilde tasarlanmıştır. PVD yöntemi sonucu üretilen stego görüntüler, klasik LSB'ye saklama yöntemine kıyasla daha

iyi sonuçlar üretmektedir. Stego görüntü içerisinde saklı olan mesaj, orijinal örten görüntüye ihtiyaç duymaksızın alıcı tarafta elde edilebilmektedir. Deneysel sonuçlarda aynı zamanda yöntemin istatistiksek ataklara karşı dayanıklı olduğu gösterilmiştir.

Önerilen yöntem örten görüntü olarak 256 seviyeli gri görüntüleri kullanmaktadır. Örtüşmeyen ikili piksel gruplarının her biri için fark değeri *d* hesaplanır. Örten görüntünün ikili bloklara ayrılması esnasında, soldan sağa - yukarıdan aşağıya tarama yöntemi kullanılmaktadır. İşlem görecek olan gruptaki piksellerin gri seviye parlaklık değerleri (p_i, p_{i+1}) ile gösterilsin. *d* ile gösterilen fark değeri $p_{i+1} - p_i$ ifadesi yardımıyla hesaplanır. Hesaplanan fark değeri $[-255, 255]$ aralığında bir değere sahip olacaktır. Çalışmada, fark değerinin simetri gereği $[0, 255]$ aralığında değiştiği varsayılarak, $R_i, i = 1, 2, \cdots, n$ ile gösterilen alt aralıklara parçalanmıştır. Alt aralıklar 1 ile *n* arasındaki indis değerleri ile temsil edilmektedir. R_i ile ifade edilen alt aralığın alt ve üst değerleri I_i ve u_i ile gösterilsin. Bu durumda *i* ile gösterilen aralığın genişliği $u_i - I_i + 1$ olarak hesaplanmaktadır. Önerilen yöntemde aralıkların genişlikleri 2'nin katı olacak şekilde, insan görme sistemine duyarlı olarak seçilir. Yumuşak geçişli blokları temsil eden fark değerlerinin yer aldığı alt aralıklar daha küçük seçilirken, kenar bilgilerinin olduğu blokları temsil eden fark değerlerinin karşı düştüğü alt aralıklar ise yöntem tarafından daha geniş olarak belirlenir. *k* indisi ile gösterilen aralığa düşen fark değerinin *k* indisine sahip olduğu söylenmektedir. Belirli bir alt aralıktaki tüm değerler yeterince birbirine yakındır. Böylece aynı alt aralıktaki bir değerin yine aynı alt aralıktaki başka bir değerle yer değişmesi durumunda, parlaklık seviyesindeki değişim insan gözü tarafından ayırt edilemeyecektir. Önerilen yöntem, gizli veriyi ilgili bloktaki piksellere, fark değerini aynı alt aralıkta başka bir fark değeri ile değiştirerek kodlamaktadır. Böylece kodlanmış veriyi içeren ikili piksel grubunun yeni fark değeri aynı alt aralık içerisinde kalmakta ve aynı zamanda gizli veriyi barındırmaktadır.

Yöntem tarafından gizli mesaj bit dizisi olarak kabul edilmektedir. İki pikselden oluşan örten görüntü bloğu *B*'nin indeks değeri *k* iken, piksel değerleri arasındaki fark *d* ile gösterilsin. İlgili bloğa saklanabilecek bit miktarı $n = \log_2(u_k - I_k + 1)$ ifadesi ile belirlenir. Gizli mesajdan alınan ve *n* bitten oluşan alt dizi *S*'nin değeri, *b* ile gösterilsin. O anki blok için hesaplanan yeni fark değeri d', (1.4)'ün kullanımı ile hesaplanır.

$$d' = \begin{cases} I_k + b & d \geq 0 \quad için \\ -(I_k + b) & d < 0 \quad için \end{cases} \tag{1.4}$$

b değeri $[0,(u_k - I_k))$aralığında değişim gösterdiği için $d' \in [I_k, u_k)$ olacaktır. d ile gösterilen fark değerinin d' ile değiştirilmesi insan gözü tarafından fark edilemeyecek ölçüdedir. Ardından d' yi kullanarak yapılan ters hesaplama sonucu o anki stego piksel parlaklık değerleri $\left(p_i{}', p_{i+1}{}' \right)$ olarak elde edilir.

Orijinal (p_i, p_{i+1}) değerleri kullanılarak, yeni stego piksel değerleri $\left(p_i{}', p_{i+1}{}' \right)$, (1.5)'te tanımlı fonksiyon yardımı ile hesaplanmaktadır.

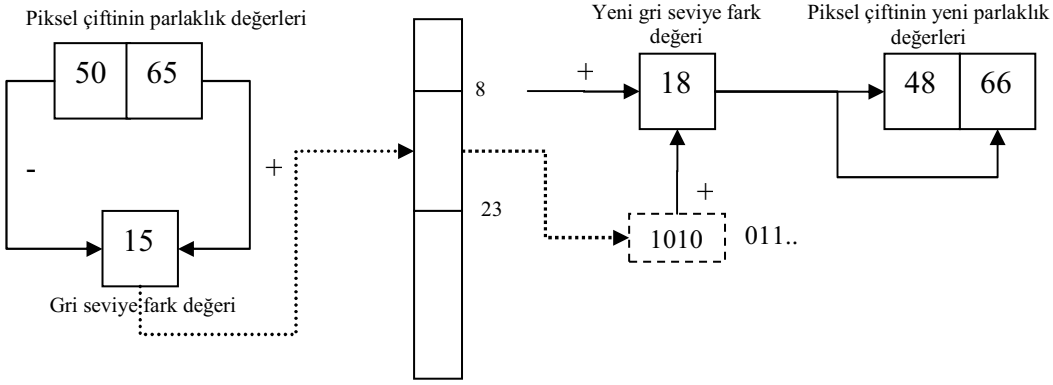
$$f((p_i, p_{i+1}), m) = \begin{cases} (p_i - \lceil m/2 \rceil, p_i + \lfloor m/2 \rfloor) & d \quad tek\ sayı\ ise \\ (p_i - \lfloor m/2 \rfloor, p_i + \lceil m/2 \rceil) & d \quad çift\ sayı\ ise \end{cases} \tag{1.5}$$
$$m = d' - d$$

Veri gömme işleminin nasıl gerçekleştirildiğini gösterebilmek amacıyla verilen örnek Şekil 1.8'de verilmiştir. İşlem görmekte olan ikili piksel bloğundaki parlaklık değerleri $(50, 65)$ olsun. Hesaplanan fark değeri 15, 8 ile 23 arasındaki aralığa karşı düşmektedir. Aralığın genişliği $16 = 2^4$ olacak şekilde belirlenmiştir. Böylece bu aralıktaki fark değeri, 4 bit veriyi kodlamada kullanılabilecektir. Gizli verinin saklanacak olan o anki 4 bit değeri 1010 olsun. İkili formdaki bit dizisinin onluk düzendeki karşılığı olan 10 değeri b ile gösterilsin. Bu değer, aralığın alt sınır değerine eklenir ve yeni fark değeri olan $d' = 18$ olarak hesaplanır. (1.5)'te verilen fonksiyon, karşılık düşen stego piksel değerlerini oluşturmakta kullanılmaktadır.

Saklanan verinin yeniden elde edilmesi aşamasında (1.6)'daki ifadeden yararlanılmaktadır. d^* değeri, o anki stego bloktaki (iki pikselden oluşan) piksel parlaklık değerlerinin farkını gösterir.

$$b = \begin{cases} d^* - I_k & d^* \geq 0 \quad için \\ -d^* - I_k & d^* < 0 \quad için \end{cases} \tag{1.6}$$

Stego görüntüden gizli mesajın elde edilmesi aşamasında, orijinal örten görüntüye ihtiyaç duyulmamaktadır. Deneysel sonuçlarda, kullanılan farklı alt aralıklar için elde edilen taşıma kapasitesi ve PSNR değerleri rapor edilmiştir. Aynı zamanda yöntemin istatistiksel ataklara karşı dayanıklılığı da gösterilmiştir.



Şekil 1.8. PVD yöntemi kullanılarak gerçekleşen veri saklama işleminin gösterimi

1.2.3. EMD Yöntemi ile Veri Saklama

Zhang ve Wang, 2006'da yapmış oldukları çalışmada, gizli veriyi temsil eden rakamların $(2n+1)$ sayı sisteminde olması durumunda, n tane örten görüntü pikselinin saklamada kullanan yeni bir yöntem önermiştir [20]. Saklama esnasında n örten pikselden yalnız biri ya bir artırılacak ya da bir azaltılacaktır. n pikselden oluşan bir grup için, $2n$ farklı değişim mümkündür. Eğer piksellerin değiştirilmeme durumu da göz önüne alınırsa, n pikselden oluşan bir grup için, artı bir ya da eksi bir değişimle, $2n+1$ farklı durum oluşturulabilir.

Verinin saklanmasından önce, gizli mesaj $(2n+1)$ sayı sistemine çevrilir. Eğer gizli mesaj ikilik tabanda ise, L bitten oluşan parçalara ayrılır. Her bir parçanın onluk değeri $(2n+1)$'lik sistemdeki K adet sayı tarafından temsil edilir. (1.7)'de L değerinin ifadesi verilmiştir.

$$L = \lfloor K \cdot \log_2(2n+1) \rfloor \tag{1.7}$$

Gizli mesajdan alınan bit dizisinin (1101 0110 1001) olması durumunda, 5'lik

sistemde gizli mesaj (23 11 14) şeklinde ifade edilebilir. Bu durumda *L*=4 ve *K*=2 olarak hesaplanır.

Önerilen yöntem *n* örten görüntü pikselini, $(2n+1)$ sistemindeki bir sayıyı saklamada kullanacaktır. Gruptaki tek bir pikselin artırılması ya da azaltılması gizli sayınının ifade edilmesi için yeterli olmaktadır. Örten görüntü piksel değerleri *n* pikselden oluşan gruplara ayrılır. Bir gruptaki piksel parlaklık değerleri $p_1, p_2, \cdots, p_n$ ile gösterilsin. $(2n+1)$ tabanında ağırlıklandırılmış toplamı ifade eden f fonksiyonu (1.8)'de verilmektedir.

$$f(p_1, p_2, \cdots, p_n) = \left[\sum_{i=1}^{n} (p_i \cdot i) \right] \mod (2n+1) \tag{1.8}$$

Gizli verideki sayı değeri *d*'nin hesaplanan *f* değerine eşit olması durumunda, piksel grubunda herhangi bir değişiklik yapılmasına ihtiyaç duyulmaz. $d \neq f$ olması durumunda $s = d - f \bmod(2n+1)$ değeri hesaplanır. Eğer *s* değeri *n*'den büyük değilse, p_s değeri bir artırılır. Aksi takdirde p_{2n+1-s} değeri bir azaltılır. *n*=4 olarak belirlenen bir sistemde o anki işlem görecek olan piksel bloğu [137 139 141 140] parlaklık değerlerine sahip olsun. Saklanmak istenen 9'luk sistemdeki gizli rakam değeri ise 4 olarak verilsin. Bu durumda f değeri 3 ve *s* değeri 1 olarak hesaplanmaktadır. Saklama işleminin ardından elde edilen stego blok [138 139 141 140] şeklinde olur. Saklanacak olan verinin 0 olması durumunda, *s* değeri 6 olarak hesaplanır ve bloktaki üçüncü piksel 1 azaltılarak kodlama gerçekleştirilir [137 139 140 140].

Alıcı tarafta, (1.8)'de verilmiş olan ve saklama esnasında kullanılan fonksiyonun stego piksel blokları üzerinde uygulanması sonucu gizli veri elde edilmektedir. Çalışmada verilen deneysel sonuçlar, yöntemin benzer yöntemlere kıyasla, daha yüksek bir saklama verimi sunduğunu göstermiştir.

Literatürde veri güvenliğini sağlamada kullanılan steganografik yöntemlerin sahip olduğu en önemli eksiklik, üretilen stego görüntünün tek bir ortamda tutuluyor olmasıdır. Stego ortamın kaybolması ya da ağ üzerinden iletimi esnasında tahrip olması durumunda gizli veri yeniden yapılandırılamayacak şekilde kaybolur. Stego görüntünün birden fazla kopyasının tutulması ise korunması gereken veri miktarını artıracağı için güvenliği tehlikeye atacaktır. Bu nedenle son yıllarda veri güvenliğinin ve hataya karşı toleransın

sağlanması için sır paylaşım şemaları kullanılmaktadır. Aynı zamanda sır paylaşım şemaları kişiye güven yerine gruba güven mekanizmasının uygulanmasını da olanaklı kılmaktadır. Bir sonraki bölümde sır paylaşım şemalarının temel özelliklerinden ve farklı türlerinden bahsedilecektir.

1.3. Sır Paylaşım Şemaları

Gizli veriyi *n* katılımcı arasında paylaştırmada kullanılan sır paylaşım metotları, kişiye güven yerine gruba güven prensibine dayanmaktadır. Katılımcı sayısının en az iki olmak zorunda olduğu şemalarda, ancak kurallara göre belirlenen önceden tanımlı yetkili grupların bir araya gelmesi sonucu gizli veri yeniden yapılandırılabilmektedir.

Sır paylaşım şemaları paylaştırma ve yeniden yapılandırma olarak isimlendirilen iki alt algoritmadan oluşmaktadır. Sır paylaşma şemalarında, gizli verinin paylaştırılması ve dağıtılmasından sorumlu olan kişi dağıtıcı olarak adlandırılır. Dağıtıcı tarafından uygulanan paylaştırma algoritması, gizli veriyi herhangi bilgi içermeyecek şekilde pay olarak adlandırılan alt parçalara ayırmaktan sorumludur. Yeniden yapılandırma aşamasında, önceden belirlenen yetkili grupların katılımcılarının, pay değerlerini bir araya getirmesi sonucu gizli veri yeniden elde edilmektedir. Gizli verinin yeniden yapılandırılabilmesi için yetkili grupların kümesi erişim yapısı olarak adlandırılır ve Γ ile gösterilir.

Shamir ve Blakley, 1979 yılında ayrı zamanlarda eşik tabanlı sır paylaşım şemalarını önermiştir [5, 6]. (*k*, *n*) eşik şeması olarak da adlandırılan yöntemler, gizli verinin *n* kişinin arasında paylaştırılmasına dayanmaktadır. Gizli verinin yeniden yapılandırılabilmesi için en az *k* tane katılımcının bir araya gelmesi gerekmektedir. *k*-1 ya da daha az sayıda katılımcı gizli veri hakkında herhangi bir bilgi açığa çıkarmamaktadır.

Sır paylaşım şemalarının gerçekleştirilmesindeki önemli konulardan biri katılımcılara dağıtılacak olan pay değerlerinin büyüklüğüdür. Çünkü bir sistemin güvenliği gizli tutması gereken bilgi miktarı arttıkça azalmaktadır. Bu nedenle pay değerlerinin büyüklüğü sır paylaşım şemalarının tasarımındaki anahtar noktalardan biridir. Sır paylaşımındaki önemli parametrelerden biri ortalama bilgi oranı ρ, katılımcılara gönderilecek olan pay büyüklüklerinin gizli verinin büyüklüğüne oranı olarak hesaplanmaktadır. Sır paylaşım şemalarında, pay bilgileri, hiçbir zaman gizli veriden küçük olamaz. Bu nedenle bilgi oranı

değerinin birden küçük olmayacağı söylenebilir. Literatürde bilgi oranı 1'e eşit olan sır paylaşım şemaları ideal olarak adlandırılmaktadır.

Literatürde araştırmacılar tarafından (*k*, *n*) eşik şemalarından farklı olarak birçok yeni sır paylaşım tekniği önerilmiştir [28-39]. Fakat tez çalışmasının temelini oluşturan Gizli Görüntü Paylaşım Şemalarında etkin olarak eşik şemalarının kullanımı tercih edildiğinden dolayı, bu bölümde, var olan eşik şemalarının detaylarından bahsedilecektir.

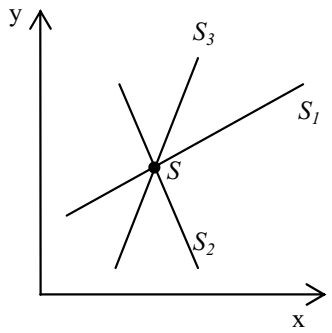
1.3.1. (*k*, *n*) Eşik Şemaları

Sır paylaşım şemaları ilk olarak 1979 yılında Shamir ve Blakley tarafından önerilmiştir. Önerilen sır paylaşım metotları, (*k*, *n*) eşik şeması özelliği taşımaktadır. Bu çalışmaların ardından sayı teorisine dayanan ve Çinli Kalan Teoremini (ÇKT) kullanan eşik şeması yöntemleri, Asmuth-Bloom ve Mignotte tarafından 1983 yılında ortaya konmuştur. Bahsi geçen eşik şemalarına ilişkin detaylar aşağıda verilmektedir.

1.3.1.1. Blakley'in Geometri Tabanlı Eşik Şeması

Blakley'in önermiş olduğu sır paylaşım şemasında, gizli veri GF_q^k vektör uzayında bir elemandır. Katılımcılara dağıtılacak olan paylar ise gizli veriyi barındıran (*k*-1) boyutlu hiper düzlemlerdir $\left\{(x_1,\cdots,x_k)\in GF_q^k \middle| \alpha_1\cdot x_1+\cdots+\alpha_k\cdot x_k=\beta\right\}$. $\alpha_1,\cdots,\alpha_k,\beta$ değerleri GF_q alanının elemanlarıdır ve pay değerlerini tanımlamada kullanılır. Gizli veri herhangi *k* payın kesişmesi sonucu yeniden yapılandırılmaktadır. Şekil 1.9'da (2, 3) eşik şemasının geometrik anlamı gösterilmiştir. Böyle bir şema için katılımcılara gönderilecek olan pay değerleri iki boyutlu uzaydaki doğru denklemleri ile ifade edilir. Dağıtıcı kişi tarafından, gizli verinin temsil ettiği noktayı kesen *n* adet doğru denklemi üretilir. Verilen örnek için *S* ile gösterilen noktayı kesen üç farklı doğru oluşturulmuştur. Doğruları ifade eden katsayılar ise katılımcılara pay değeri olarak gönderilir. Herhangi iki kişinin bir araya gelmesi ile iki doğrunun kesiştirilmesi sonucu gizli veri yeniden yapılandırılır. Blakley'in önermiş olduğu şema mükemmel sır paylaşım şeması özelliği taşımamaktadır. Çünkü *k* katılımcıdan daha az kişinin bir araya gelmesi, gizli verinin üzerinde yer aldığı doğru denkleminin elde edilmesine sebep olmaktadır. Fakat gizli verinin, bir noktanın yalnız tek

bir koordinatı olarak seçilmesi durumunda, bilgi oranı etkilense dahi şema mükemmel hale getirilebilir. Verilen örnekte bir katılımcı, gizli verinin, kendi pay değerinin göstermiş olduğu doğru üzerindeki bir nokta olduğunu bilmektedir.



Şekil 1.9. Blakley'in (2, 3) eşik şeması

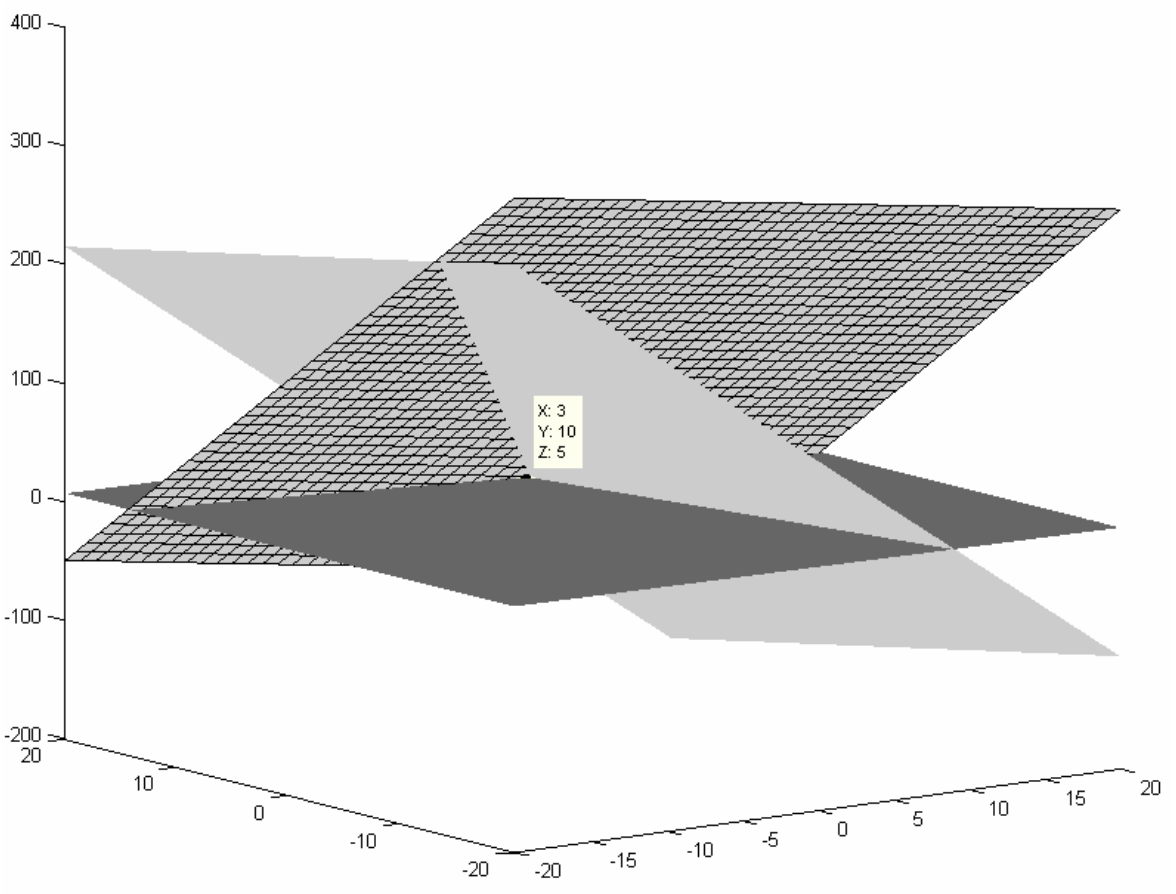
Örnek: Blakley'in yöntemi kullanılarak paylaştırılacak olan gizli veri üç boyutlu uzaydaki (3, 10, 5) koordinatları ile gösterilen nokta olsun. (3, 3) şeması kullanılarak gizli verinin dağıtılabilmesi için $3\alpha_1 + 10\alpha_2 + 5\alpha_3 = \beta$ denklik ifadesi üretilir. İfadeyi sağlayacak olan 3 farklı değerler kümesi $(\alpha_1, \alpha_2, \alpha_3, \beta)$ katılımcılara gönderilecek pay değerlerini oluşturur.

Pay değerleri sırasıyla (2, 10, 1, 111), (10, 2, 1, 55), (1, 0, 10, 53) şeklinde olsun. Üretilen bu değerler Şekil 1.10'da gösterildiği gibi üç boyutlu uzaydaki düzlemlere karşı düşmektedir. Herhangi üç katılımcının bir araya gelmesi, ilgili yüzeylerin kesişimi olan ve (3, 10, 5) ile gösterilen noktanın (gizli verinin) yeniden yapılandırılmasını sağlar. Yeniden yapılandırma işleminin matematiksel olarak ifadesi ise, (1.9)'da verilen denklik sistemi ile gösterilmektedir. Üç katılımcıdan elde edilen pay değerleri kullanılarak elde edilen sistemin çözümü, gizli veriyi temsil eden noktanın koordinatlarını vermektedir.

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 & 10 & 1 \\ 10 & 2 & 1 \\ 1 & 0 & 10 \end{bmatrix}^{-1} \times \begin{bmatrix} 111 \\ 55 \\ 53 \end{bmatrix} = \begin{bmatrix} 3 \\ 10 \\ 5 \end{bmatrix} \tag{1.9}$$

Şekilden de gözlemlenebileceği gibi herhangi iki katılımcının bir araya gelmesi durumunda gizli verinin üzerinde bulunduğu doğru denklemi elde edilebilmektedir. Blakley'in yöntemi, Shamir'in yöntemine nazaran, gizli veri hakkında daha fazla bilgi

açığa çıkarmaktadır. Blakley'in şeması ile ilgili bir diğer problem ise üretilen pay değerinin büyüklüğüdür. Örnekte verilen şemada, üç değer ile temsil edilen gizli veriyi temsil etmek için dört değerden oluşan paylar üretilmektedir.



Şekil 1.10. (3, 10, 5) ile ifade edilen gizli verinin üç katılımcı arasında (3, 3) şeması kullanılarak paylaştırılması sonucu elde edilen yüzeyler

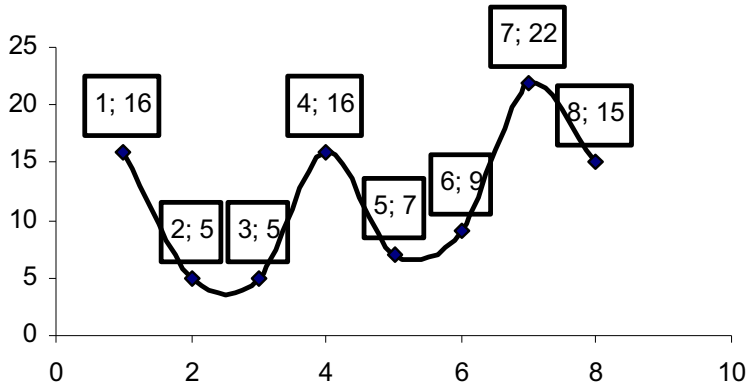
1.3.1.2. Shamir'in Polinomial Tabanlı Eşik Şeması

Shamir tarafından önerilen eşik şeması yöntemi, polinomial interpolasyona dayanır [5]. Verilen herhangi k adet noktanın $(x_1, y_1)\cdots(x_k, y_k)$, $x_i \neq x_j, 1 \leq i < j \leq k$ koşulunu sağlamak şartıyla, üzerinden geçtiği k-1 dereceden yalnızca bir $P(x)$ polinomu vardır. Shamir'in yöntemine göre gizli veri S, k-1 dereceden ve pozitif tamsayıların alanında bir polinomun sabit katsayısı olarak belirlenir. Polinom ifadesi (1.10)'da verilmektedir. Seçilecek olan gizli verinin tanımlı olması gerektiği aralık p değeri ile belirlenir,

$s \in (0,\ p-1]$. Seçilecek olan p değeri asal sayı olmak zorundadır. Geri dönüş esnasında tek bir çözüm elde edilmesi ihtimalini kesinleştirmek için p değerinin asal olarak seçilme zorunluluğu vardır. Polinoma ilişkin katsayı değerleri, $(a_1, a_2, \cdots, a_k)$, rasgele belirlenir.

$$P(x) = \left(S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}\right) \bmod p \tag{1.10}$$

$I_1, \cdots, I_n$ olarak gösterilen pay değerleri polinomun farklı x değerlerinde üretmiş olduğu y değerlerinden oluşmaktadır, $I_i = P(x_i), 1 \le i \le n$. Seçilen x değerlerinin birbirinden farklı olması gerekmektedir. Gizli verinin 7 olması ve eşik şemasının (3, 8) olması durumunda yapılandırılacak olan polinom $f(x) = \left(7 + 19x + 21x^2\right) \bmod 31$ şeklindedir. Polinom ikinci dereceden olup, sabit terim hariç diğer katsayıları rasgele seçilmiştir. Polinom tanımlamasında kullanılan asal değer ise, gizli verinin tanımlı olduğu aralığı kapsayacak en büyük asal sayı değeridir. Verilen örnek şema için Shamir'in şemasının geometrik anlamı Şekil 1.11'de verilmektedir.



Şekil 1.11. Shamir'in yönteminin (3, 8) şeması için gösterimi

A ile gösterilen grup için herhangi k tane pay değeri $\{I_i | i \in A\}, |A| = k$, (1.11)'de verildiği üzere Lagrange'ın interpolasyon yöntemi yardımıyla, gizli verinin yeniden yapılandırılmasında kullanılmaktadır.

$$S = \sum_{i \in A} \left(I_i \cdot \prod_{j \in A - \{i\}} \frac{x_j}{x_j - x_i} \right) \tag{1.11}$$

Lagrange'ın interpolasyonundan farklı olarak, lineer denklik sistem çözümlerinden de gizli verinin elde edilmesinde faydalanılabilir. Polinomun $P(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$ ile gösterilmesi durumunda, bir araya gelen herhangi *k* adet pay değeri $I_{i_1}, \cdots, I_{i_k}$, (1.12)'de verilen denklik sistemi yardımıyla gizli verinin yeniden yapılandırılmasında kullanılmaktadır.

$$\begin{cases} a_0 + a_1 x_{i_1} + \cdots + a_{k-1} x_{i_1}^{k-1} = I_{i_1} \\ \vdots \\ a_0 + a_1 x_{i_k}^{1} + \cdots + a_{k-1} x_{i_k}^{k-1} = I_{i_1} \end{cases} \tag{1.12}$$

Verilen sistem, *k* adet denklem, *k* adet bilinmeyen $(a_{k-1}, \cdots, a_1, a_0)$ ve tek bir çözüme sahiptir. Sistemin determinantı sıfır olmayan Vandermonde matrisin determinantı olduğu için, tek bir çözüme sahiptir. Shamir'in şeması mükemmeldir, çünkü herhangi *k*-1 ya da daha az değer kullanılarak polinom kestirilemez. *k*-1 adet pay değerinin olması durumunda, oluşan denklik sistemi (1.13)'te verilmiştir. Herhangi a_0 değeri için sistem farklı çözümlere sahiptir.

$$\begin{cases} a_1 x_{i_1} + \cdots + a_{k-1} x_{i_1}^{k-1} = I_{i_1} - a_0 \\ \vdots \\ a_1 x_{i_k}^{1} + \cdots + a_{k-1} x_{i_k}^{k-1} = I_{i_1} - a_0 \end{cases} \tag{1.13}$$

Örnek. Gizli veri olarak verilen 10 sayısının (3, 5) eşik şeması kullanılarak paylaştırılması için, sabit terim hariç diğer katsayıları rasgele belirlenen $P(x) = 2x^2 + 7x + 10$ polinomu Z_{11} alanında tanımlı olsun.

Polinom kullanılarak beş katılımcı için hesaplanan pay değerleri $I_1 = P(1) = 8, I_2 = P(2) = 10, I_3 = P(3) = 5$ ve $I_4 = P(4) = 4, I_5 = P(5) = 7$ olarak hesaplanır. Yeniden yapılandırma esnasında birinci, ikinci ve dördüncü katılımcıların bir araya gelmesi sonucu Lagrange'ın interpolasyonu yardımıyla elde edilen ifade (1.14)'te verilmiştir. Verilen ifadenin hesaplanması durumunda gizli veri 10 yeniden yapılandırılır.

$$8 \cdot \frac{2}{2-1} \cdot \frac{4}{4-1} + 10 \cdot \frac{1}{1-2} \cdot \frac{4}{4-2} + 4 \cdot \frac{1}{1-4} \cdot \frac{2}{2-4} = 10 \tag{1.14}$$

Shamir'in yöntemine göre, üretilen pay değerlerinin büyüklüğü, gizli verinin büyüklüğünü aşmaz. Aynı zamanda yöntem dinamik özelliğe sahiptir. *k* değerini sabit tutmak koşuluyla, yeni pay değerleri, var olanları etkilemeden üretilebilir. Aynı zamanda gizli verinin değişmesine ihtiyaç duyulmadan, pay değerleri değiştirilebilir.

1.3.1.3. Mignotte'nin Sayı Teorisine Dayanan Eşik Şeması

Mignotte, önermiş olduğu sır paylaşma yönteminde, Mignotte'nin sırası olarak adlandırılan sıralı tamsayıları kullanmıştır [8]. (*k*, *n*) eşik şeması için birbirleri arasında asal olan *n* tamsayı $p_1 < p_2 < \cdots < p_n$ (1.15)'teki koşulu sağlayacak şekilde belirlenir.

$$\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i \tag{1.15}$$

Gizli veri *S,* $\beta < S < \alpha$ aralığında bir sayı olmak zorundadır. α değeri en küçük *k* sayının çarpımına karşı düşerken $\alpha = \prod_{i=1}^{k} p_i$, β değeri en büyük *k*-1 sayının çarpımına eş değerdir $\beta = \prod_{i=0}^{k-2} p_{n-i}$. Pay değerleri $I_i = S \bmod p_i, 1 \le i \le n$ denklik ifadesi yardımıyla belirlenir. Yeniden yapılandırma esnasında herhangi *k* adet pay değerinin bir araya gelmesi, gizli verinin yeniden yapılandırılması için yeterli olmaktadır. (1.16)'da verilen denklik sisteminin çözümünde ÇKT kullanılır. ÇKT teoreminin uygulanmasına ilişkin detaylar Ek 1'de verilmektedir.

$$\begin{cases} x \equiv I_{i_1} \bmod p_{i_1} \\ \quad \vdots \\ x \equiv I_{i_k} \bmod p_{i_k} \end{cases} \tag{1.16}$$

Gizli veri $S < \alpha$ olduğu için, $Z_{p_{i_1} \cdots p_{i_k}}$'de tanımlıdır. Yalnızca *k*-1 pay değerinin yeniden yapılandırmada kullanılması durumunda $I_{i_1}, \cdots, I_{i_{k-1}}$, elde edilen denklik ifadesi

$S \equiv x_0 \bmod p_{i_1} \cdots p_{i_{k-1}}$ şeklinde olur. x_0 değeri $\bmod p_{i_1} \cdots p_{i_{k-1}}$ tabanındaki tek çözümdür.

Örnek. Gizli veri olarak seçilen 615 değeri (3, 5) şeması kullanılarak katılımcılar arasında paylaştırılacak olsun. Her katılımcı ile ilişkilendirilmiş modulo değerleri sırasıyla 10, 14, 18, 22 ve 26 olarak belirlenmiştir. Seçilen taban değerleri aynı zamanda Mignotte'nin koşulunu da sağlamaktadır. Katılımcılara gönderilecek pay değerleri, taban değerleri kullanılarak, sırasıyla 5, 13, 3, 21 ve 17 olarak hesaplanır. Yeniden yapılandırma aşamasında, ilk üç katılımcının bir araya geldiği varsayılsın. Aşağıda verilen denklik sisteminin ÇKT ile çözülmesi sonucunda gizli veri yeniden yapılandırılır.

$$\begin{cases} x \equiv 5 \bmod 10 \\ x \equiv 13 \bmod 14 \\ x \equiv 3 \bmod 18 \end{cases} \tag{1.17}$$

1.3.1.4. Asmuth-Bloom'un Sayı Teorisine Dayanan Eşik Şeması

Asmuth ve Bloom'un 1983'de önerdiği eşik şeması yöntemi de, özel sıralı tamsayıların kullanımına dayanır [7]. Aralarında asal n+1 asal sayı $p_0, p_1 < p_2 < \cdots < p_n$ (1.18)'de verilen koşulu sağlayacak şekilde seçilmektedir.

$$p_0 \cdot \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i \tag{1.18}$$

Katılımcıların kendileri ile ilişkili asal değerleri bilmesi, şemanın düzgün çalışabilmesi için gereklidir. Gizli veri S, Z_{p_0} kümesinin bir elemanı olmak zorundadır. Katılımcılara gönderilecek olan pay değerleri $I_i = (S + \alpha \cdot p_0) \bmod p_i, 1 \le i \le n$ denklik ifadesi kullanılarak hesaplanır. Şemanın rasgeleliğini sağlayan α değeri $S + \alpha \cdot p_0 \in Z_{p_1 \cdots p_k}$ şartını sağlayacak şekilde seçilir. Yeniden yapılandırma esnasında, herhangi k tane pay değeri, ÇKT yardımıyla gizli verinin elde edilmesinde kullanılmaktadır.

Örnek. (3, 4) eşik şeması kullanılarak gizli veri 2'nin katılımcılar arasında paylaştırılabilmesi için öncelikle Asmuth-Bloom özel sıralı sayılarının elde edilmesi

gerekir [37]. Seçilen sayıların sırasıyla 3, 11, 13, 17 ve 19 olması durumunda (1.19)'da verilen koşulun sağlandığı gözlemlenir $3 \cdot 17 \cdot 19 < 11 \cdot 13 \cdot 17$. Ardından pay değerlerinin oluşturulması için gerekli olan $S + p_0 \cdot \alpha = 2 + 3 \cdot 51 = 155$ değeri hesaplanır. Örnekte şemanın rasgeleliğini sağlayan α değeri 51 olarak seçilmiştir. $(p_1 \cdots p_4)$ değerleri kullanılarak üretilen pay değerleri sırasıyla $(1, 12, 2, 3)$ olmaktadır. İlk üç katılımcının yeniden yapılandırma için bir araya gelmesi durumunda (1.19)'da verilen denklik sistemi elde edilir.

$$\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv 12 \bmod 13 \\ x \equiv 2 \bmod 17 \end{cases} \tag{1.19}$$

Denklik sistemini çözümünde $M = 11 \cdot 13 \cdot 17 = 2431$ ve M_1, M_2, M_3 değerleri sırasıyla 221, 187, 143 olarak hesaplanır. M_1, M_2, M_3 değerlerine karşılık düşen modulo taban değerleri kullanılarak çarpmaya göre tersleri bulunur $M_1^{-1} = 1, M_2^{-1} = 8, M_3^{-1} = 5$. Denklik sisteminin çözümü olan x değeri $(1 \cdot 221 \cdot 1 + 12 \cdot 187 \cdot 8 + 2 \cdot 143 \cdot 5) \bmod 2431 = 155$, gizli veri S değeri ise $155 \bmod 3 \equiv 2$ olarak hesaplanır.

1.4. Gizli Görüntülerin Paylaşımında Kullanılan Teknikler

Günümüzde ticari ya da askeri birçok uygulama, gizlilik gerektiren görüntülerin ağ üzerinden iletimini ve depolanmasını gerektirmektedir. Bu nedenle veri güvenliğinin nasıl sağlanacağı, araştırmacılar tarafından çözüm getirilmeye çalışılan önemli bir konu olmuştur. Son yıllarda önerilen bazı tekniklerle gizli görüntülerin güvenliğinin sağlanması amaçlanmıştır. Steganografi ve kriptografi literatürde sıklıkla kullanılan iki tekniktir. Steganografi gizli görüntüyü ilgi çekmeyecek şekilde farklı bir örten ortam içerisine saklarken, kriptografi gizli görüntüyü anlamsız ve gürültü niteliği taşıyan görüntüye çevirmektedir. Her iki yöntemde de karşılaşılan iki problem mevcuttur:

- Saklanan ya da şifrelenen verinin tek bir ortamda tutulması, stego ya da şifreli ortamın herhangi bir şekilde bozulması durumunda gizli verinin yeniden yapılandırılamayacak şekilde tahrip olmasına sebep olmaktadır.

Stego ortamın ya da şifreli ortamın birden çok kopyasının tutulması, bozulma ya da kaybolma problemlerinin üstesinden gelebilmek için önerilebilir. Fakat bu durum da, gizlilik gerektiren veri miktarını artırmak, güvenliği daha da çok tehlikeye atacaktır.

- Kriptografi ve steganografi, tek kişiye güven prensibine dayanır. Gizli verinin ancak belirli sayıda kullanıcının bir araya gelmesi durumunda yapılandırılmasını her iki yöntemde desteklememektedir.

Bu nedenle son yıllarda gruba güven mekanizmasının uygulanabildiği ve hataya karşı toleransın sağlandığı Görsel Sır Paylaşımı ve Gizli Görüntü Paylaşımı şemalarının kullanımı ağırlık kazanmıştır. İlerleyen bölümlerde her iki yöntem de detayları ile irdelenecektir.

1.4.1. Görsel Sır Paylaşımı

SP yöntemini temel alan ve daha yeni bir yöntem olan GSP, Naor ve Shamir tarafından 1994 yılında önerilmiştir [3]. Bu şema için paylaşılan sır gizli bir görüntüdür (el yazısı notları, yazıcı çıktıları, resimler gibi). GSP'nin en önemli özelliği, başka bir hesaplamaya ihtiyaç duymaksızın insan görme sistemini, gizli veriyi ortaya çıkarmada kullanmasıdır. Geleneksel şifreleme tekniklerinin, şifre çözme için gerektirdiği kompleks hesaplamalar bu yeni alanda yer almamaktadır. (k, n) GSP şeması için, sır sahibi olan kişi, gizli görüntüden görsel şifreleme tekniklerini kullanarak n tane anlamsız pay oluşturur ve sırrı paylaşacağı guruptaki alıcıların her birine bir adet pay gönderir. Paylar aslında anlam ifade etmeyen gürültü görünümündeki görüntülerdir. Gizli görüntünün ortaya çıkarılabilmesi için en az k adet kişinin kendi paylarını asetat üzerine basmaları ve bu asetatları tam olarak üst üste getirmeleri gerekmektedir. Gizli veri, görsel şifreleme teknikleri kullanılarak paylara dağıtıldığı için, kötü amaçlı kişiler herhangi k-1 ya da daha az paydan gizli görüntü hakkında herhangi bir bilgi elde edemez.

Naor ve Shamir tarafından önerilen bu şemanın farklı problemlerini iyileştirmeye çalışan birçok çalışma mevcuttur [40-58]. Bazı çalışmalar, paylaşılacak olan görüntünün yalnızca siyah beyaz resim olmak yerine, gri seviye veya renkli resim olabileceğini göstermiştir [40-42]. Paylaşılacak olan gizli görüntü sayısının artırılması ise yine ilgi çeken bir diğer konu olmuştur [43-48]. Görsel şifrelemenin doğası gereği oluşan kontrast problemlerinin giderilmeye çalışılması çözülmeye çalışılan problemler arasındadır [49-52].

Tanımı gereği görsel şifrelemede, sır olarak paylaşılacak olan görüntüdeki bir piksel, paylarda birden çok alt piksel ile temsil edilmektedir. Böyle bir kodlama tekniği ise görüntü boyutlarının belirli bir oranda genişlemesine neden olmaktadır. Genişleme faktörü olarak adlandırılan bu büyüme oranı, depolama gereksinimleri ve bant genişliğinin kullanımı açısından olumsuz etkilere sahiptir. Yapılan birçok çalışma ile bu oranın küçültülmesi amaçlanmıştır [53-58].

(k, n) GSP şemasında orijinal görüntünün siyah ve beyaz piksellerden oluştuğu varsayılır. Orijinal görüntüdeki her bir piksel, paylarda *m* adet alt piksele kodlanır. GSP şeması $n \times m$ büyüklüğündeki mantıksal *S* matrisi ($S = \lfloor s_{ij} \rfloor$) tarafından tanımlanır. Eğer *i.* paydaki *j.* alt piksel siyah ise $s_{ij} = 1$, aksi takdirde $s_{ij} = 0$'dır. $i_1, i_2, \ldots, i_k$ ile gösterilen payların alt pikselleri uygun bir şekilde örtüşecek şekilde üst üste getirildiğinde gizli veri ortaya çıkacaktır. *S* matrisindeki satırların OR'lanması sonucu oluşan vektörün Hamming ağırlığı, ilgili pikselin insan görme sistemi tarafından nasıl algılanacağını göstermektedir. Siyah ve beyazı ayırt etmek için sabit bir eşik değeri olsun ve *d* ($1 \le d \le m$) ile gösterilsin. Resmin görünebilirliği açısından, α ile gösterilen kontrastın sıfırdan büyük olması gerekir. İlgili piksel için belirlenen *S* matrisinin satırlarının OR'lanması sonucu oluşan $1 \times m$'lik vektör *V* ile gösterilsin. Bu durumda eğer $H(V) \ge d$ ise, yeniden yapılandırılan piksel insan görme sistemi tarafından siyah, eğer $H(V) \le d - \alpha m$ ise beyaz olarak algılanacaktır.

Tanım 1. *(k, n)* GSP şeması, B_0 ve B_1 ile gösterilen $n \times m$ büyüklüğündeki mantıksal matrislerden oluşan iki küme ile temsil edilir. Beyaz bir piksel paylaşılacağı zaman kişi B_0 mantıksal matrisinin satırlarından birini rasgele olarak seçer ve ilgili paya yerleştirir. Siyah bir piksel paylaşılacağında ise B_1 matrisinden seçilen rasgele bir satır ilgili payı kodlamada kullanılmaktadır. B_0 veya B_1 matris kümelerinden rasgele seçilen bir matris, *n* tane paydaki *m* adet alt pikselin gri seviyesini belirlemeye yardımcı olur. Naor ve Shamir'in tanımı gereği, bir GSP şeması ancak aşağıdaki koşulları sağladığı takdirde geçerlidir.

1. B_0 veya B_1 kümelerinden seçilen herhangi bir matrisin, *n* tane satırının herhangi *k* tanesinin OR'lanması sonucu oluşan vektörün (*V*), seçildiği kümeye bağlı olarak şu koşulları sağlaması gerekir. B_0'dan seçilen bir matris için $H(V) \le d - \alpha m$ veya B_1'den seçilen matris için $H(V) \ge d$ olmalıdır.

2. $\{1,2,\ldots,n\}$'nin herhangi alt kümeleri $\{i_1,i_2,\ldots,i_q\}(q<k)$ için, B_0 ve B_1 matrislerinin içermiş olduğu matrislerin sıklığı eşit olmalıdır.

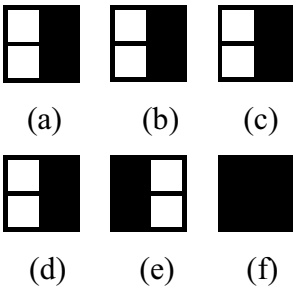
İlk parametre kontrast olarak adlandırılırken, ikinci parametre şemanın güvenliğini garanti eder. İkinci koşul sayesinde, *k* adetten az sayıda payın üst üste getirilmesi ile gizli verinin elde edilemeyeceği garanti edilir.

(k, n) GSP şemalarının nasıl gerçekleştirildiğini göstermek amacıyla, (2, 2) durumu bir örnek ile açıklanacaktır. B_0 ve B_1 matrisleri (1.20)'deki gibi tanımlansın.

$$B_0=\left\{\begin{matrix}\textit{kolonların permütasyonu ile}\\ \textit{elde edilen tüm matrisler}\end{matrix}\begin{pmatrix}1&0&1&0\\1&0&1&0\end{pmatrix}\right\}$$
$$B_1=\left\{\begin{matrix}\textit{kolonların permütasyonu ile}\\ \textit{elde edilen tüm matrisler}\end{matrix}\begin{pmatrix}1&0&1&0\\0&1&0&1\end{pmatrix}\right\} \qquad (1.20)$$

B_0 ve B_1 kümelerini oluşturan matrislerin satırlarının görünme olasılıkları birbirlerine eşittir. Bu da belirli bir örüntünün belirli bir renge ait olduğu bilgisinin gizli görüntüyü ele geçirmeye çalışan saldırganlar tarafından çıkarılmasına engel olmaktadır. Permütasyon işleminin gerçekleştirileceği matrislerden de anlaşılacağı üzere, B_0 kümesini oluşturan herhangi bir matrisin satırlarının OR'lanması sonucu oluşan vektörün Hamming uzaklığı *2* iken (beyaz pikseli temsil eder), B_1 kümesindeki bir matris için hesaplanan Hamming uzaklık 4 olacaktır. Aradaki fark, insan gözünün siyah ve beyaz arasında ayrım yapmasını sağlayacak karşıtlığı oluşturmaktadır.

Kodlama işlemi esnasında, gizli görüntüdeki beyaz pikselin kodlanması için B_0 kümesinden rastgele bir matris seçilir (R_0). Birinci payda karşı düşen alt piksel grubunun içeriği R_0'ın birinci satırı tarafından belirlenirken, ikinci paya karşı düşen piksel grubu ikinci satır tarafından oluşturulur. Benzer şekilde siyah pikselin kodlanması için kullanılacak olan matris ise B_1 kümesindeki matrisler arasından seçilir. Görüntüdeki tüm siyah ve beyaz pikseller için bahsedilen kodlama gerçekleştirildiğinde, sırrı paylaşacak olan kişilere dağıtılacak olan paylar oluşturulmuş olmaktadır. Açıklanan kodlama işlemine ilişkin bir örnek Şekil 1.12'de verilmektedir.



Şekil 1.12. (a)-(b) Beyaz pikselin kodlanmasında kullanılan pay değerleri (c) Yeniden yapılandırılan beyaz pikselin temsili (d)-(e) Siyah pikselin kodlanmasında kullanılan pay değerleri (f) Yeniden yapılandırılan siyah pikselin temsili

Gizli görüntüdeki her bir pikselin, paylarda kaç alt piksel ile temsil edileceği GSP şemalarının oluşturulmasındaki parametrelerden biridir. Verilen örnekte bu değer 2 olarak seçilebileceği halde resmin en boy oranında bozulmaya neden olmaması için her iki doğrultuda da 2 olacak şekilde yani 4 olarak belirlenmiştir. Şemanın karşıtlığını belirten α değeri, kodlanmış beyaz piksel ile siyah pikselin Hamming uzaklıkları arasındaki farktır. α değerinin büyük olması, tekrar yapılandırılan resmin karşıtlığını, bir başka deyişle görünebilirliğini iyileştirir. Verilen bu örnekte α değeri ikidir.

2004 yılında Yang tarafından olasılıklı görsel sır paylaşma olarak adlandırılan yeni bir yöntem önerilmiştir [53]. Yeni yöntemin ürettiği payların büyüklüğü, geleneksel yöntemlerden farklı olarak, paylaşılacak olan gizli görüntü ile aynı kalmaktadır. Üretilen payların boyutlarının, gizli görüntü ile aynı kalması, saklama kapasitesi açısından önemli ölçüde kazançları da beraberinde getirmektedir. Şema beyaz piksellerin siyah ve beyaz bölgede görünme sıklığını, insan gözünün siyah ve beyazı ayırt etmesini sağlayacak şekilde kullanmaktadır. Yang, çalışmasında vermiş olduğu tanım bağıntıları ile (2, 2), (2, *n*), (*k*, *k*) ve (*k*, *n*) şemalarının nasıl oluşturulabileceğini göstermiştir.

Olasıklı yöntemi geleneksel yöntemden ayıran en önemli fark, kodlanacak olan görüntüdeki pikseli birden çok alt pikselle paylarda temsil etmek yerine tek bir piksel ile kodlamaktır. Orijinal görüntünün yeniden yapılandırılması için gereken yalnızca *(k, n)* şeması için en az *k* adet payın üst üste getirilmesidir. Bu da geleneksel yöntemdeki OR'lanma işlemine karşı düşer. Geleneksel yöntem beyaz pikseli temsil etmek için $x_0 B y_0 S$ (x_0 adet beyaz, y_0 adet siyah), siyah pikseli temsil etmek için ise $x_1 B y_1 S$ kullanır.

Bir pikselin kaç alt pikselle temsil edildiği *m* ile gösterilecek olursa, $x_0 + y_0 = x_1 + y_1 = m$ olmaktadır. OGSP şemalarında ise *m* değeri 1'e eşittir.

OGSP şemaları özellikle depolama gereksinimlerinin ve bant genişliğinin etkin kullanılmasında öneme sahiptir. Gizli görüntünün yeniden yapılandırılmasında, GSP şemalarında olduğu gibi herhangi bir matematiksel işleme ihtiyaç duymamaktadır.

Bir sonraki bölümde, gizli görüntünün yeniden yapılandırılmasında matematiksel işlemlerden faydalanan gizli görüntü paylaşımı yönteminden bahsedilecektir.

1.4.2. Gizli Görüntü Paylaşımı

1994 yılında önerilen ve detayları önceki bölümde verilmiş olan GSP şemalarında bazı problemler mevcuttur. Yeniden yapılandırılan gizli görüntüdeki kontrast kaybı, üretilen pay görüntülerinin gizli görüntünün en ve boy yönünde iki katı olması, renkli görüntülerin paylaşımına destek vermemesi, bahsi geçen yöntemin belli başlı problemleri olarak verilebilir.

Thien ve Lin, 2002'deki çalışmalarında gizli görüntülerin ağ üzerinden iletimi için, "Gizli görüntü paylaşımı" (Secret Image Sharing) olarak adlandırılan, yeni bir yöntem önermişlerdir [4]. Bu yöntem; steganografi, kriptografi veya görsel sır paylaşımı kullanılması durumunda oluşan problemlerin üstesinden gelmektedir. Görsel sır paylaşımından farklı olarak, gizli görüntünün yeniden yapılandırılabilmesi için matematiksel işlemlere gerekmektedir.

Gizli görüntü paylaşımında, gizli görüntü *n* katılımcı arasında, Shamir'in önermiş olduğu Sır Paylaşma şeması kullanılarak paylaştırılmaktadır. Paylaştırma algoritmasının ardından, her katılımcı gürültüye benzer pay görüntülerine sahip olur. Pay görüntüleri tamamen gürültü benzeri olup, gizli görüntü hakkında herhangi bir bilgi açığa çıkarmaz. Katılımcılardan *k* tanesinin bir araya gelmesi gizli görüntünün yeniden yapılandırılması için yeterli olmaktadır. Böylece bazı pay görüntülerinin bozulması ya da kaybolmasında dahi, en az *k* tane görüntünün hatasız olması durumunda, önerilen yöntem gizli veriyi yeniden yapılandırabilmektedir. 2002'deki bu çalışmanın ardından gizli görüntü paylaşımı literatürde irdelenen ve var olan eksikliklerinin üstesinden gelinmeye çalışılan bir konu halini almıştır. "Gizli Görüntü Paylaşımı" yönteminde var olan bazı eksiklikler aşağıdaki şekildedir.

- Gizli görüntülerin, $[0, 255]$ aralığında parlaklık değerlerine sahip piksellerden oluşan gri seviye görüntüler olduğu varsayılmaktadır. Gizli görüntü paylaşımında kullanılan Shamir'in polinom ifadesindeki asal modulo değeri, $[0, 255]$ aralığındaki en büyük asal sayı değeri olan 251 seçilmiştir. 255'ten büyük ilk asal değerin kullanılmamasının sebebi, gri seviye görüntünün bit derinliğinin artırılmasının depolama gereksinimlerini kötü yönde etkileyecek olmasıdır. Seçilen modulo değerinden dolayı, Shamir'in polinomundaki katsayı değerlerini belirleyecek olan gizli görüntü piksel değerleri $[0, 250]$ aralığında olmak zorundadır. Bu nedenle gizli görüntünün paylaştırılmasından önce $[251, 255]$ aralığındaki gizli görüntü piksel parlaklık değerleri 250'ye ötelenmektedir. Bu da yeniden yapılandırma aşamasında tekrar oluşturulan gizli görüntünün belirli bir oranda bozulmuş olmasına sebep olur.
- Üretilen pay görüntülerinin gürültü şeklinde olması, kötü niyetli kişilerin ilgisini çekeceği için sistem güvenliğini tehlikeye atmaktadır.
- Katılımcılara gönderilen pay görüntülerinin, araya giren kötü niyetli bir kişi tarafından bozulmaya uğradığının tespiti mümkün değildir.

Literatürde gizli görüntü paylaşma şemaları üzerine yapılan çalışmalar, aşağıda verilmiş olan alt alanlara ayrılabilir.

- Steganografi tabanlı ve doğrulama mekanizmalı teknikler: Pay görüntülerinin anlamlı hale gelebilmesi için steganografik yöntemleri ve üretilen stego pay görüntülerinin katılımcılar tarafından onaylanması için doğrulama yöntemleri kullanan tekniklerdir [59-72]. Literatürdeki çalışmaların önemli bir kısmı üretilen pay görüntülerinin steganografi yardımıyla anlamlı hale getirilmesi ve pay değerlerini taşıyan stego görüntüleri doğrulamada kullanılan mekanizmaların iyileştirilmesini hedeflemektedir. Üretilen stego görüntülerin iyileşme oranları PSNR değeri ile ölçülmektedir. Doğrulama oranını iyileştirmek için, kullanılan doğrulama biti sayısının artırılması, PSNR oranının düşmesine sebep olmaktadır. Bu nedenle stego görüntü kalitesi ve doğrulama mekanizmasının etkinliği arasında ters bir orantı mevcuttur. Araştırmacılar her iki parametreyi de aynı anda olabildiğince iyileştirmeyi hedeflemektedir.

- Geri döndürülebilir gizli görüntü paylaşma teknikleri: Pay değerlerini taşıyan stego görüntüler kullanılarak gizli görüntü yapılandırıldıktan sonra, orijinal örten görüntüleri yeniden elde etmeye çalışan tekniklerdir. Katılımcılara gönderilen örten

görüntülerin askeri harita gibi önem arz eden görüntüler olması durumunda, gizli görüntünün yeniden yapılandırılmasının ardından, örten görüntünün stego görüntülerden elde edilmesi bir gerekliliktir. Son yıllarda yapılan bazı çalışmalarda gizli görüntü paylaşım şemalarına geri döndürülebilirlik özelliği kazandırılmaya çalışılmıştır [73-77].

- Kandırılmayı engelleyen gizli görüntü paylaşma teknikleri*:* Araya giren kötü niyetli bir kişinin pay görüntüsünü farklı bir görüntü ile değiştirmesine engel olmaya çalışan tekniklerdir. Kötü niyetli bir katılımcının sunmuş olduğu yalancı pay değerleri ile beraber diğer katılımcıları kandırması mümkündür [78]. Bu gibi atakları engelleyebilmek amacıyla son yıllara yapılan çalışmalar sır paylaşım şemalarına farklı özellikler eklemeye çalışmışlardır [79-85]. Önerilen yöntemler kendi içlerinde iki alt kategoride incelenebilir: Hile tespiti ya da Hilecinin tespiti. Birinci grupta yer alan çalışmalar gizli verinin yeniden yapılandırılması esnasında, katılımcıların kendi aralarında bir hileci olup olmadığını tespit edebilmelerini sağlar [79-80]. İkinci grup çalışmalar ise hilecinin tespitini olanaklı kılmaktadır [81-85].

- Diğer sır paylaşım tekniklerini kullanan gizli görüntü paylaşım teknikleri: Geometrik tabanlı ya da sayı teorisine dayalı sır paylaşma yöntemlerini, gizli görüntü paylaşımında kullanan tekniklerdir. Literatürde gizli görüntülerin paylaşımında kullanılmak için ağırlıklı olarak seçilen sır paylaşma tekniği Shamir'in polinomial yaklaşımı olmuştur. Fakat yapılan bazı çalışmalar, sayı teorisine veya geometri tabanlı yöntemlere dayanan sır paylaşma tekniklerinin de, gizli görüntü paylaşımında kullanılması için çeşitli yöntemler önermiştir [86-90].

- Kademeli gizli görüntü paylaşım teknikleri: Gizli görüntüyü kademeli yani katılımcı sayısına bağlı olarak yeniden yapılandıran çalışmalardır. *k* tane pay görüntüsünün bir araya gelmesi sonucu gizli görüntüyü belirli bir oranda yeniden yapılandıran bu teknikler, ardından gelen pay görüntülerini yeniden yapılandırılan gizli görüntünün kalitesinin artırmada kullanır [91-100].

- Pay büyüklüğü kısıtlamalı gizli görüntü paylaşım teknikleri: Gizli görüntü paylaşım şemalarında oluşturulan pay görüntülerinin büyüklüğü depolama gereksinimleri ve bant genişliği açısından problem oluşturabilmektedir. Bu alandaki çalışmalar, pay görüntü büyüklüğünü küçülterek, yöntemin kullanacak olduğu örten görüntü büyüklüğünü azaltmayı ve dolayısıyla depolama gereksinimleri ve bant genişliği açısından iyileşme sağlamayı hedeflemektedir [101-105].

- Kullanıcı dostu gizli görüntü paylaşma teknikleri: Görüntü paylaşım şemaları son yıllarda bazı çalışmalarda gizli olmayan görüntülerin paylaşımı amacıylada kullanılmak istenmiştir [106-111]. Böyle bir durumda üretilen pay görüntülerinin gürültü şeklinde olması, yönetilebilirlik açısından problemler teşkil etmektedir. Kullanıcı dostu görüntü paylaşım şemalarının üretmiş olduğu pay görüntüleri, paylaştırılan görüntünün daha düşük kalitedeki versiyonlarıdır.
- Çoklu gizli görüntü paylaşım teknikleri: Birden çok gizli görüntünün aynı anda paylaşımını gerçekleştiren tekniklerdir [112-119]. Bir tane gizli görüntünün paylaşımı esnasında kullanılan bilgiden daha fazlasını gerektirmeden, daha fazla sayıda gizli görüntü paylaşabilen bu şemalar pratik kullanımda oldukça etkindir.

Gizli görüntü paylaşımı alanında verilmiş olan alt alanlarda tez kapsamında gerçekleştirilen çalışmalar ve elde edilen sonuçlardan ilerleyen bölümlerde bahsedilecektir.

2. YAPILAN ÇALIŞMALAR

Günümüzde internet üzerinden gerçekleştirilen veri haberleşmesindeki artış ve beraberinde kablosuz aygıtların maliyetindeki düşüş, veri güvenliği probleminin önem kazanmasına sebep olmuştur. Askeri önem taşıyan haritalar, ticari bilgi içeren ya da önemli kişilere ait medikal görüntüler gibi gizlilik gerektiren sayısal verilerin internet üzerinden iletimi esnasında kötü niyetli kullanıcılardan korunması literatürde önem gören bir konudur. Sayısal veri güvenliğinin sağlanması amacıyla yapılan çalışmalarda kriptografi ve steganografi kullanılmaktadır. Kriptografi anahtar olarak adlandırılan sayısal veriyi kullanarak, gizli veriyi şifreli veri biçimine dönüştürmektedir. Dönüşüm esnasında kullanılan yöntemler matematiksel işlemlerden oluşur. Alıcı tarafta ters dönüşüm fonksiyonları kullanılarak gizli verinin yeniden elde edilmesi hedeflenmektedir. Diğer yöntem olan steganografi ise örten ortam olarak adlandırılan herhangi bir görüntü, ses ya da video dosyasını gizli verinin saklanmasında kullanmaktadır. Saklama işleminin ardından üretilen ortam stego ortam olarak adlandırılmaktadır. Her iki yöntemdeki en büyük problem üretilen ortamların (şifreli ya da stego ortam) tek bir ortam olmasıdır. Stego ortamın ya da şifreli ortamın kötü niyetli kişiler tarafından tahrip edilmesi ya da iletim esnasında bozulması durumunda, gizli veri yeniden yapılandırılamayacak şekilde bozulacaktır. Buradan yola çıkarak iki yöntemi veri güvenliğini sağlamada kullanan tekniklerin, hataya karşı toleranssız olduğu söylenebilir.

Son yıllarda özellikle gizli görüntülerin iletimi esnasında Sır Paylaşma tekniklerini kullanan yöntemler popülerlik kazanmıştır. Önerilen yöntemlerin hataya ya da tahribe karşı toleranslı olması, steganografi veya kriptografi tabanlı yöntemlere nazaran daha ön plana çıkmalarını sağlamıştır. Aynı zamanda Sır Paylaşımına dayalı yöntemler, gizli verinin kişiler arasında paylaştırılabilmesini ve ancak belirli sayıda katılımcının bir araya gelmesi durumunda gizli verinin yeniden yapılandırılabilmesini olanaklı kılmaktadır. Diğer iki teknikte ise alıcı taraf tek bir kişidir ve tek kişiye güven prensibi yöntemlerin uygulanmasında geçerlidir.

Gizli görüntü paylaşım şemaları iki alt algoritmadan oluşmaktadır: Paylaştırma ve Yeniden Yapılandırma. Paylaştırma algoritması gizli veriyi n katılımcı arasında paylaştırır. Katılımcılara gönderilen bilgiler, gürültü özelliği taşıyan ve gizli görüntünün $1/k$'sı

büyüklüğündeki pay görüntüleridir. Pay görüntüleri gizli görüntü hakkında herhangi bir bilgi içermezken, ancak *k* tanesinin bir araya gelmesi sonucu gizli veri yeniden yapılandırılır. *k*-1 ya da daha az pay görüntüsü gizli görüntü hakkında herhangi bir bilgi açığa çıkarmaz. Literatürde yer alan çalışmalar gizli görüntü paylaşım şemalarının iyileştirilmesini hedeflemiştir. İyileştirilmeye çalışılan unsurlar birkaç başlık altında toplanabilir:

- Üretilen pay görüntülerinin gürültü şeklinde olması kötü niyetli kişilerin ilgisini çekeceği için, steganografinin gizli görüntü paylaşım teknikleri ile kullanımı önerilmiştir. Üretilen pay görüntüleri, örten görüntüler içerisine saklanmaktadır. Pay görüntülerinin saklanması esnasında stego görüntülerde meydana gelen bozulmaların aza indirgenmesi ve PSNR'nin iyileştirilmesi hedefler arasında yer almaktadır.
- Pay görüntülerinin saklanabilmesi için, seçilen örten görüntülerin genişleme olarak adlandırılan oranda büyük olması gerekmektedir. Genişleme oranının küçülmesi, gerek bant genişliği gerekse depolama gereksinimleri açısından önemli bir unsurdur.
- Stego görüntülerin katılımcılar tarafından değiştirilmediğini ya da iletim esnasında bozulmadığını ispatlamak amacıyla doğrulama bitlerinin kullanılması gerekir. Doğrulama bitlerinin sayısındaki artış yöntemi diğer yöntemlere kıyasla daha güvenilir hale getirmektedir. Yalnız doğrulama bitlerinin sayısındaki artışın, stego görüntü kalitesinde azalmaya sebep olacağı unutulmaması gereken bir unsurdur.
- Gizli görüntünün yeniden yapılandırılmasının ardından, stego görüntüler kullanılarak örten görüntülerin elde edilmesi literatürdeki çalışmaların hedefleri arasında yer alır. Böylece gizli görüntü paylaşım şemalarına geri döndürülebilirlik özelliği kazandırılmış olmaktadır.

Gizli görüntü paylaşım şemalarında, literatürdeki araştırmacılar tarafından üzerinde durulan unsurların iyileştirilmesi ve sorunlarının giderilmesi tez kapsamında yapılan çalışmaların hedefini teşkil etmiştir. Genel bilgiler kısmında verilen "Steganografi ve Doğrulama mekanizmalı yöntemler", "Diğer sır paylaşım tekniklerini kullanan yöntemler" ve "Geri döndürülebilir gizli görüntü paylaşım teknikleri" irdelenerek verilen hedefler doğrultusunda iyileşme sağlayacak yeni gizli görüntü paylaşım şemaları önerilmiştir.

Tez kapsamında yapılan çalışmalar aşağıda maddeler halinde verilmektedir.

1. Blakley'in geometrik tabanlı yöntemi kullanılarak önerilen gizli görüntü paylaşım şeması, literatürdeki genişleme oranı problemine çözüm getirmektedir. Shamir tabanlı yöntemlerde genişleme oranı 4 olarak rapor edilirken, önerilen yöntem bu değeri 1'e indirmeyi başarmıştır.

2. Önerilen yeni bir kodlama tekniği ile pay değerlerinin temsili için gerekli bit sayısı azaltılmış, böylece doğrulama bit sayısı artırılarak, PSNR değeri açısından ve doğrulama yeteneği açısından literatürdeki yöntemlere kıyasla daha üstün yeni bir gizli görüntü paylaşım şeması önerilmiştir.

3. Gizli görüntü büyüklüğü ve örten görüntü büyüklüğüne bağlı olarak doğrulama yeteneğini adaptif olarak değiştirebilen yeni bir yöntemin tasarımı gerçekleştirilmiştir. Önerilen yöntem, literatürde yer alan Eslami'nin adaptif çalışmasına kıyasla gerek doğrulama gerekse PSNR açısından daha başarılıdır.

4. Geri döndürülebilir gizli görüntü paylaşım şemalarındaki piksel parlaklık aralığına bağlılık (gri seviye ya da siyah-beyaz örten görüntü seçilmesi durumu) problemine vurgu yapılan çalışmada, EMD yönteminde kullanılan denklem ifadesinin probleme uyarlaması gerçekleştirilmiştir. Modulo operatörü ile beraber EMD'yi kullanan yöntem, literatürdeki problemleri ortadan kaldırarak, PSNR açısından daha başarılı sonuçlar üretmiştir.

5. Paylaşım esnasında kullanılacak olan gizli görüntünün medikal görüntü olması durumu değerlendirilmiştir. Literatürde yer alan medikal görüntü güvenliğini sağlayan çalışmalardan farklı olarak, ilk kez hem görüntü güvenliğini sağlayan hem de elektronik hasta kaydının iletimini gerçekleştiren yeni bir yöntem önerilmiştir.

6. Literatürde var olan gizli görüntü paylaşım şemalarının var olan eşik şemalarını (Shamir ve Blakley) kullandığına vurgu yapılarak, yeni bir geometrik tabanlı gizli görüntü paylaşım şeması önerilmiştir. Yeni önerilen şema görüntülerin paylaşımı için Morley'in üçgen teoreminden faydalanmaktadır.

7. Sayı teorisine dayalı yöntemlerin gizli görüntü paylaşımı alanında kullanılması durumunda, Shamir tabanlı yöntemlere kıyasla avantaj sağlanıp sağlanamayacağını test etmek amacıyla, gizli görüntü paylaşım şemalarının tasarlanması gerçekleştirilmiştir.

Çalışmaların detaylarından bahsedilmeden önce içerikleri hakkında verilen genel bilgiler aşağıdaki şekildedir.

İlk önerilen şemada Blakley'in yöntemi ve steganografi kullanılarak gizli görüntü paylaşımı gerçekleştirilmiştir. Üretilen pay görüntülerini anlamlı görüntüler içerisine saklayan literatürdeki ilk geometrik tabanlı gizli görüntü paylaşım yöntemidir. Önerilen yöntemin var olan tekniklere kıyasla genişleme oranı açısından 4 kat iyileşme sağladığı gözlemlenmiştir. Aynı zamanda üretilen stego görüntülerin PSNR değerinin $k > 3$ için diğer yöntemlere kıyasla daha yüksek olduğu yine deneysel sonuçlardan görülmektedir.

Çalışma kapsamında önerilen bir diğer şema stego görüntülerin PSNR değerini iyileştirirken, doğrulama oranını da yükseltmeyi hedeflemiştir. Gizli görüntü paylaşım şemasında kullanılan polinomial ifade değiştirilerek, üretilecek olan pay değerinin daha dar bir aralıkta ifade edilmesi sağlanmıştır. Böylece pay değerlerini saklamada kullanılan bit sayısı azalırken, doğrulama da kullanılan bit sayısı 3'e çıkartılmıştır. Gizli görüntü piksel değerlerinin polinoma yerleştirilmesi esnasında seviyelendirme yönteminin kullanılması önerilmiştir. Elde edilen deneysel sonuçlarda bu alanda yapılan çalışmalara kıyasla, önerilen yöntemin PSNR değeri ve doğrulama oranı açısından daha başarılı olduğu gösterilmiştir.

Dinamik olarak doğrulama biti sayısına karar veren diğer bir çalışmada, Eslami ve arkadaşlarının yöntemindeki aksaklıklar ortaya koyularak, EMD yöntemine dayalı yeni bir gizli görüntü paylaşım şeması önerilmiştir. Yöntemin Eslami'nin yöntemine kıyasla daha başarılı sonuçlar ürettiği deneysel sonuçlarda gözlemlenmiştir. Eslami'nin çalışmasındaki zincir probleminin üstesinden gelinerek hem doğrulamada kullanılan bit sayısı artırılmış hem de PSNR değeri kabul edilebilir değerlerde tutulmuştur.

Tez kapsamında gerçekleştirilen ve literatürdeki geri döndürülebilir gizli görüntü paylaşım tekniklerindeki önemli problemlere vurgu yapan çalışmada, örten görüntülerin histogramının şemaların üretmiş olduğu stego görüntü PSNR değerleri üzerinde önemli etkilere neden olduğu ortaya konmuştur. Önerilen geri döndürülebilir gizli görüntü paylaşım tekniği örten görüntünün siyah-beyaz olması durumunda dahi yaklaşık olarak 43 dB PSNR'ye sahip stego görüntüler üretebilmektedir. EMD yönteminde kullanılan denklem ifadesini değiştirerek gizli görüntü paylaşım şemalarına adapte eden çalışmanın, diğer yöntemlere kıyasla daha üstün sonuçlar verdiği deneysel sonuçlarda gözlemlenmiştir.

Önerilen şemaların dışında, medikal görüntü güvenliğinin sağlanmasında sır paylaşım şemalarının kullanımının pratik anlamda değer taşıyacağı çalışma kapsamında tespit edilmiş ve uygulaması gerçekleştirilmiştir. Literatürde var olan teknikler damgalama, steganografi ve kriptografiyi medikal görüntü güvenliğini sağlamada kullanmıştır.

Önerilen tekniklerin en önemli dezavantajı medikal görüntü güvenliğini ve elektronik hasta kayıt bilgisinin iletimini aynı anda sağlayamamasıdır. Bunun dışında medikal görüntüsü internet üzerinden transfer edilecek olan kişinin askeri ya da devlet düzeyinde önem taşıyan biri olması durumunda, var olan çalışmalardaki tek kişiye güven politikası belirgin problemlere yol açacaktır. Çalışma kapsamında önerilen sır paylaşma yöntemi ile önemli kişilere ait medikal görüntülerin ve elektronik hasta kayıt bilgisinin önceden belirlenen taraflar arasında paylaşımı gerçekleştirilmiştir. Medikal görüntü güvenliğinde gereken unsurların tek bir yöntemde karşılanıyor olması, tekniğin literatürdeki önemini artırmaktadır.

Tez çalışmasında ayrıca düzlem geometrisindeki Morley'in üçgen teoremini kullanan yeni bir geometri tabanlı gizli görüntü paylaşım tekniği önerilmiştir. Literatürde var olan ve eşik şemalarının kullanımına dayanan gizli görüntü paylaşım şemalarından farklı olarak, yeni bir gizli görüntü paylaşım şemasının oluşturulması hedeflenmiştir. Morley'in üçgeninin kenar bilgisi ve x eksenine göre yönlenimi gizli verinin kodlanmasında kullanılmaktadır. Morley'in üçgeni kullanılarak üretilen dış üçgen ise katılımcılara gönderilecek pay bilgilerini oluşturmaktadır.

Son olarak yapılan çalışmalar kısmında gizli görüntü paylaşımı alanında sayı teorisine dayalı eşik şemalarının performanslarını görebilmek ve diğer şemalarla kıyaslayabilmek amacıyla, Asmuth-Bloom ve Mignotte şemalarını kullanan gizli görüntü paylaşım şemaları gerçekleştirilmiştir.

Bu tez çalışması süresince yapılan çalışmalar Matlab simülasyon ortamı kullanılarak denenmiş ve önerilen teknikler hazır paketler olmaksızın kodlanarak gerçeklenmiştir. Maddeler halinde verilmiş olan çalışmaların detayları sırasıyla ilerleyen bölümlerde verilmektedir.

2.1. Geometri Tabanlı Gizli Görüntü Paylaşım Şeması

Gizli görüntülerin paylaşımında Shamir'in polinomial tabanlı yaklaşımını ya da ÇKT tabanlı eşik şeması yöntemlerini kullanan birçok çalışma literatürde mevcuttur. Son yıllarda yapılan birkaç çalışmada geometri tabanlı sır paylaşım şeması olan Blakley'in yöntemi gizli görüntü paylaşımında kullanılmıştır. 2008 yılında Chen ve arkadaşları ve Tso ayrı zamanlarda Blakley'in yöntemini gizli görüntü paylaşma alanına adapte etmeye çalışmıştır [86, 87]. Chen ve arkadaşlarının çalışmasında, gizli görüntü büyüklüğü ile aynı

büyüklükte pay görüntüleri üretilmiştir. Tso'nun yönteminde ise, pay görüntü büyüklüklerinin yani genişleme oranının küçüldüğüne vurgu yapılmıştır. Fakat her iki yöntemde de üretilen pay görüntüleri gürültü şeklindedir. Son yıllarda yapılan birçok çalışma, gürültü şeklindeki pay görüntülerinin kötü niyetli kişilerin ilgisini çekeceğini vurgulamıştır. Bu nedenle gizli görüntü paylaşma alanında, pay görüntülerinin anlamlı hale getirilmesi önemli bir konu olmaktadır.

Bu çalışmada geometrik tabanlı sır paylaşım şemasını steganografi ile beraber kullanan yeni bir gizli görüntü paylaşma yöntemi önerilmiştir [145]. Literatürde önceden yapılan ve Blakley'in şemasını kullanan çalışmalar gürültü şeklinde pay görüntüleri üretir. Aynı zamanda Shamir'in yaklaşımını kullanan çalışmalardan farklı olarak önerilen yöntem genişleme oranını 4'ten 1'e indirerek gerek örten görüntülerin iletim zamanı gerekse depolama gereksinimleri açısından iyileştirme sağlamıştır.

Önerilen gizli görüntü paylaşma şeması iki alt bölümden oluşur. İlk bölümde anlatılacak olan ve gizli görüntünün n katılımcı arasında paylaştırılması için kullanılacak algoritma "paylaştırma algoritması" olarak adlandırılır. İkinci bölümde, katılımcılardan herhangi k tanesinin bir araya gelmesi sonucu gizli görüntünün elde edilmesi için uygulanan "yeniden yapılandırma" algoritması verilmiştir. Dağıtıcı, paylaştırma algoritmasında kullanılacak olan eşik şemasını belirlemek amacıyla (k, n) değerlerini seçer. n değeri gizli görüntünün paylaştırılacak olduğu kişi sayısını gösterirken, k değeri gizli görüntünün yeniden yapılandırılması için gerekli olan minimum kişi sayısını ifade etmektedir. Eğer k ya da daha fazla katılımcı bir araya gelirse gizli görüntü yeniden yapılandırılmaktadır. Her bir katılımcı kendi ile ilişkilendirilmiş ve gizli görüntüye ait bilgi taşıyan, "*pay*" olarak adlandırılan parçayı sayısal görüntü biçiminde alır. Paylaştırma algoritması aynı zamanda pay bilgilerini örten görüntülere saklayabilmek için steganografi kullanmaktadır. Böylece rasgele gürültü şeklindeki pay bilgileri, kötü niyetli kişilerin dikkatini çekmeden, doğal görünümlü örten görüntülere saklanır. Bu nedenle dağıtıcı paylaştırma algoritmasının icrasından önce n adet gri seviye örten görüntü resmi seçer.

Önerilen paylaştırma algoritması Blakley'in yöntemini gizli görüntünün paylaştırılması için kullanır. Blakley'e göre gizli veri k boyutlu uzayda bir noktadır. $1\times k$ büyüklüğündeki bir vektör k boyutlu uzaydaki noktayı ve dolayısıyla gizli veriyi temsil eder. Fakat önerilen yöntemde gizli veri $N\times M$ boyutlarındaki dijital bir resimdir. Bu nedenle gizli görüntü k adet pikselden oluşan gruplara parçalanır. Her grup k boyutlu uzaydaki bir noktayı ifade etmektedir.

k adet pikselden oluşan grup tarafından belirlenen noktayı kesen *n* farklı hiper düzlem denklemi *n* tane örten görüntüde karşılık düşen *k* adet piksel grubuna gömülür. Sonuç olarak *k*'lık piksel grubundan elde edilen bilgi, yine *k* adet pikselden oluşan örten görüntülerdeki piksel gruplarına yerleştirilmektedir. Üretilen pay görüntü büyüklüğü, gizli görüntü büyüklüğüne eş değer olur. Buradan yola çıkarak genişleme oranının önerilen yöntem için 1 olduğu söylenmektedir. Önerilen paylaştırma algoritmasının detayları aşağıdaki şekildedir.

Gizli görüntü üst üste örtüşmeyen *k* adet pikselden oluşan gruplara parçalanmaktadır. Her grup *k* boyutlu uzayda bir nokta tanımlar, $x=(x_1, x_2, \cdots, x_k)$. Karşılık düşen pay bilgilerinin oluşturulması için, bu noktayı kesen ve *k* adet katsayıya sahip hiper düzlem denklemleri oluşturulur. Düzlemin katsayıları $(a_1, a_2, \cdots, a_k)$ ve *B* sabit terimi hiper düzlem denklemini tanımlar. Katsayı değerleri o anki işlem görmekte olan örten görüntünün piksel grubundaki değerlerden alınırken, (2.1)'in kullanımı ile üretilen *B* değeri, yine aynı gruptaki piksellerin en anlamsız hanelerine steganografinin kullanımı ile kodlanır.

$$(a_1 x_1 + a_2 x_2 + \cdots + a_k x_k) \bmod 251 \equiv B \tag{2.1}$$

B değerinin kodlanması ile değiştirilen örten görüntüler, paylaştırma algoritmasının sonucunda katılımcılara dağıtılacak olan stego görüntüleri oluşturur. Örten görüntülerde meydana gelen bozulmalar insan gözünün ayırt edemeyeceği ölçüdedir. Blakley'in şeması tarafından kullanılan hiper düzlem denklemi (2.1)'deki gibi değiştirilmiştir. Bunun sebebi kullanılan gizli görüntünün parlaklık değerlerinin gri seviye olmasıdır. Aynı zamanda asal modulo tabanının kullanılması, yeniden yapılandırma aşamasında biricik sonucun elde edilmesini garantileyecektir. Başka bir deyişle, yeniden yapılandırma aşamasında lineer denklik sisteminin çözümünün tek olacağı, modulo işleminde asal bir sayının kullanımı ile garantilenir. 251 değeri, gri seviye bir resimdeki piksellerin parlaklık aralığındaki $[0-255]$ en büyük asal sayı değeridir.

$(a_1, a_2, \cdots, a_k)$ değerleri örten görüntülerde karşılık düşen *k*'lık piksel grubundaki piksel parlaklık değerlerinden elde edilir. Aynı zamanda bu pikseller, üretilecek olan *B* değerini saklamak için de kullanılacaktır. *B* değerinin temsilinde $\lceil \log_2 251 \rceil = 8$ bit yeterli olmaktadır. Geriye kalan 8×*k*-8 bit değeri, $(a_1, a_2, \cdots, a_k)$'nın değerlerini belirlemektedir.

Piksel grubundaki k adet değerden düzlem denkleminin katsayılarının elde edilmesi için aşağıdaki yöntem kullanılabilir. Öncelikle B değerinin, k'lık gruptaki piksellerin son kaç bitlerine gömüleceğini belirlemek için (2.2)'de verilen kümeden faydalanılır. Küme elemanları sırasıyla piksellerin son kaç bitinin B değerini depolamada kullanılacağını belirtmektedir.

$$B = \left\{ b_i \,\middle|\, b_i = \left\lceil \frac{l_i}{u_i} \right\rceil, i \in \{0, \cdots, k-1\} \right\}, \tag{2.2}$$

Bu ifadede ki l_i ve u_i değerleri (2.3)'teki gibi tanımlanır.

$$\begin{aligned} &U = \{u_i \mid u_i = k - i, i \in \{0, \cdots, k-1\}\}, \\ &l_0 = 8 \qquad L = \left\{ l_i \,\middle|\, l_i = l_{i-1} - \left\lceil \frac{l_{i-1}}{u_{i-1}} \right\rceil, i \in \{1, \cdots, k-1\} \right\}, \end{aligned} \tag{2.3}$$

k tane pikselden oluşan gruptaki piksellerin son kaç bitlerinin B değerini kodlamada kullanılacağı tespit edildikten sonra, (2.4) ile verilen denklem, hiper düzlemin katsayılarını belirler. İlgili örten görüntüdeki k adet piksel değeri $(c_1, c_2, \cdots, c_k)$ ile gösterilsin.

$$A = \left\{ a_i \,\middle|\, a_i = \frac{\left(c_i \wedge \left(256 - 2^{b_{i-1}}\right)\right)}{2^{b_{i-1}}}, i \in \{1, \cdots, k\} \right\} \tag{2.4}$$

$(a_1, a_2, \cdots, a_k)$ değerlerinin karşılık düşen k'lık piksel grubunun kullanımı ile hesaplanması ve üretilen B değerinin aynı piksel grubuna steganografi kullanılarak gömülmesi işlemleri kısa bir örnek üzerinde gösterilecektir.

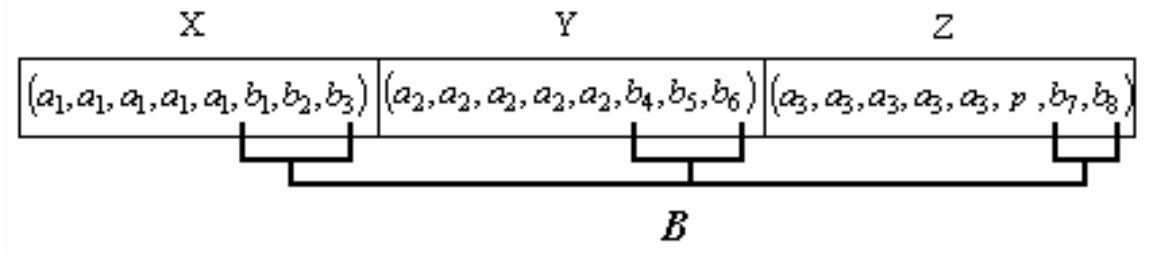
(3, n) eşik şeması için, bir örten görüntüdeki her bir k'lık piksel grubunun hangi bitlerinin, $(a_1, a_2, \cdots, a_k)$ değerlerini belirlemede kullanılacağı ve B değerini hangi bitlerin taşıyacağı Şekil 2.1'de verilmektedir.

Örten görüntüdeki 3 adet piksel değerinden, (X, Y, Z), pay bilgilerinin üretilmesinde faydalanılır. Hiper düzlem denklemindeki (a_1, a_2, a_3) değerlerini belirlemede kullanılacak olan bitler Şekil 2.1'de gösterilmiştir. Her üç pikselin sırasıyla ilk beş biti düzlem

katsayılarını belirler. Elde edilen katsayılar doğrultusunda oluşturulan denklem (2.5)'de verilmiştir.

$$\left(a_1 x_1 + a_2 x_2 + a_3 x_3\right) \bmod 251 \equiv B \tag{2.5}$$

Yukarıdaki denkliğin kullanımı ile hesaplanan B değeri, üç pikselin sırasıyla son üç, üç, iki bitine gömülür. Böylece (X, Y, Z)'nin en anlamlı bitleri hiper düzlemin katsayılarını belirlemede kullanılırken, en anlamsız bitleri ise hesaplanan B değerini saklamaya yardımcı olur. Piksellerin son kaç bitinin B'yi temsilde kullanılacağı (2.2)'in kullanımı ile elde edilir.



Şekil 2.1. Hiper denklem düzlemindeki a katsayılarını belirlemede ve hesaplanan B değerini saklamada kullanılacak bit pozisyonları

Son olarak, kötü niyetli kişilerin stego görüntüleri bozmasına engel olmak için yönteme bir doğrulama yetisi kazandırılacaktır. MD5 (Message Digest 5) olarak bilinen ve Ek 2'de detayları verilen özüt fonksiyonu, $H(\cdot)$, k adet piksel değeri içeren stego bloklar üzerinde uygulanır. Örnekteki (X, Y, Z) değerleri p ile gösterilen bit hariç birleştirilerek (2.6)'da görüldüğü gibi özüt fonksiyonuna tabi tutulur.

$$\begin{aligned} T &= H\left(X \| Y \| (Z - p)\right) \\ T &= \left\{ t_i \,\middle|\, i \in \{1, 2, \cdots, 128\}, t_i \in \{0, 1\} \right\} \end{aligned} \tag{2.6}$$

MD5 fonksiyonu, giriş ne olursa olsun 128 bit çıkış üreten tek yönlü bir fonksiyondur. Çıkışın (2.7)'deki gibi ikili bitler halinde XOR'lanması sonucu stego bloğa ilişkin özet bilgi üretilir ve ilgili bit değerine yerleştirilir.

$$p = ((((t_1 \oplus t_2) \oplus t_3) \oplus t_4) \cdots) \oplus t_{128} \tag{2.7}$$

Yukarıda örneklendirilerek anlatılan prosedür, *n* tane stego görüntünün oluşturulabilmesi için gizli görüntüdeki bütün *k*'lık piksel gruplarına uygulanmaktadır. Paylaştırma algoritması adımlar halinde aşağıdaki şekilde verilebilir:

Giriş : *S* ile gösterilen gizli görüntü ve *n* tane örten görüntü
Çıkış : *n* tane stego görüntü

Adım 1. Gizli görüntü *S* ve *n* tane örten görüntü *k* adet pikselden oluşan gruplara ayrılır. *S*'de oluşan her grup için aşağıdaki adımlar tekrarlanır.
Adım 2. O anki gruptaki *k* adet piksel, *k* boyutlu uzayda bir noktayı temsil etsin.
Adım 3. *n* tane örten görüntüde karşılık düşen *n* tane *k* piksellik grubu kullanarak *n* farklı hiper düzlem denklemini aşağıdaki adımları kullanarak belirle ve Adım 2'ye dön.
Adım 4. O anki örten görüntüdeki $(a_1, a_2, \cdots, a_k)$ değerlerini (2.4)'ü kullanarak belirle.
Adım 5. *B* değerini hesapla ve (2.2)'nin kullanımı ile o anki örten görüntüdeki piksel değerlerinin son bitlerine kodla.
Adım 6. Örten bloğa ilişkin doğrulama bit değerini (2.6) ve (2.7)'yi kullanarak hesapla ve bu değeri *p* ile gösterilen yere kodla.

Paylaştırma algoritmasına ilişkin yalancı kod ifadesi Ek 3'te verilmektedir. Önerilen yöntemin uygulanabilirliğini göstermek için (3, 5) eşik şeması örneği göz önüne alınabilir. Gizli görüntüye ilişkin ilk üç piksel değerinin sırasıyla $(110\ 24\ 72)$ olduğu varsayılsın. Beş adet örten görüntü, üçerli piksel gruplarına parçalanır. Örten görüntülere ilişkin ilk üç piksel değerleri sırasıyla $(57\ 99\ 220)$, $(85\ 100\ 23)$, $(150\ 100\ 150)$, $(199\ 223\ 223)$, $(12\ 33\ 15)$ şeklinde verilsin. Örten görüntülerdeki grupların her biri, üç boyutlu uzaydaki noktayı (gizli görüntünün ilk üç pikseli) kesen hiper düzlemleri belirlemede kullanılır. Birinci örten görüntü için, (a_1, a_2, a_3)'ün değerleri $(7\ 12\ 27)$ olarak hesaplanır ve elde edilen hiper düzlem denklemi $7x_1 + 12x_2 + 27x_3 \equiv B(\text{mod } 251)$ şeklindedir. Eğer gizli görüntüden alınan *x* değerleri hiper düzlem denklemine yerleştirilirse, $7 * 110 + 12 * 24 + 27 * 72 \equiv 241$ değeri hesaplanır. Elde edilen bu değerin ikili karşılığı ($241 = 11110001_2$) örten görüntü piksellerinde belirlenen bit pozisyonlarına yerleştirilir.

Saklama işlemi ardından değişen örten görüntü piksel değerleri (63 100 221) olmaktadır. Geri kalan örten görüntü piksel gruplarının, aynı yöntemin uygulanması sonucu değişmiş halleri sırasıyla (80 102 22), (145 100 150), (198 221 220) ve (15 33 14) şeklinde olur. Yukarıda verilen örnek, örten görüntü piksel parlaklık değerlerinin saklama işlemi ardından $[0-7]$ aralığında değiştiğini göstermiştir. Böyle bir değişim sonuçlarda da vurgulanacağı gibi insan gözü tarafından fark edilemez.

Yeniden yapılandırma algoritması, gizli görüntünün *k* ya da daha fazla katılımcının bir araya gelmesi sonucu yeniden yapılandırılmasını sağlar. Katılımcılardan elde edilen stego görüntülerden herhangi *k* tanesi, *k* adet pikselden oluşan gruplara bölünür. Karşılıklı gruplar üzerinde özüt fonksiyonu uygulanarak, stego görüntülerin kötü niyetli kişiler tarafından herhangi bir bozulmaya uğrayıp uğramadığı tespit edilmeye çalışılır. Ardından karşılıklı piksel grupları, hiper düzlemleri temsil eden lineer denklik sistemlerinin tespitinde kullanılır. Lineer denklik sisteminin çözümü o anki gizli görüntü piksel değerlerini oluşturur. Yeniden yapılandırma algoritması adımlar halinde aşağıdaki şekilde verilmektedir.

Adım 1. Dağıtıcının kullanmış olduğu (*k*, *n*) değerlerine göre, katılımcılardan herhangi *k* tanesinden gelen stego görüntüyü seç.

Adım 2. Her stego görüntüyü, *k* adet pikselden oluşan gruplara böl.

Adım 3. Örten görüntülerdeki karşılıklı piksel grupları için aşağıdaki adımları tekrarla.

Adım 4. O anki örten gruptaki *p* değerini belirle.

Adım 5. Alt piksel grubunun *p* hariç tüm bitlerine (2.6)'yı uygula. Elde edilen sonucu Adım 4'te elde edilen değerle kıyasla. Eğer değerler aynıysa blok doğrulanmıştır ve algoritma Adım 6'dan devam edebilir. Aksi takdirde ilgili bloğu doğrulanmadığını gösterecek şekilde siyaha çevir.

Adım 6. O anki piksel grubundan, $(a_1, a_2, \cdots, a_k)$ ve *B* değerlerini çıkart.

Adım 7. Adım 4 ve Adım 6 arasındaki ifadelerin uygulanması sonucu (2.8)'deki gibi *k* adet lineer bağımsız denklem elde edilir. Lineer denklik sistemini, Matris tersleme yöntemini kullanarak hesapla.

$$\begin{aligned} (a_1x_1 + a_2x_2 + \cdots + a_kx_k) \bmod 251 &\equiv b_1 \\ (a_{k+1}x_{k+1} + a_{k+2}x_{k+2} + \cdots + a_{k+k}x_{k+k}) \bmod 251 &\equiv b_2 \\ \vdots &\vdots \\ (a_{k(k-1)+1}x_{k(k-1)+1} + \cdots + a_{k(k-1)+k}x_{k(k-1)+k}) \bmod 251 &\equiv b_k \end{aligned} \tag{2.8}$$

Verilmiş olan algoritmanın uygulanabilirliği basit bir örnek üzerinde gösterilebilir. Paylaştırma algoritmasındaki (3, 5) eşik şeması örneği sonucu elde edilen stego görüntülerden herhangi üç tanesi kullanılarak sır yeniden yapılandırılmak istenmektedir. Beş tane katılımcıdan herhangi üç tanesinin bir araya gelmesi sonucu elde edilen lineer denklem sistemi (2.9) ile verilmiştir.

$$\left(\begin{bmatrix} 10 & 12 & 2 \\ 18 & 12 & 18 \\ 24 & 27 & 27 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 26 \\ 50 \\ 212 \end{bmatrix} \right) \bmod 251 \tag{2.9}$$

İkinci, üçüncü ve dördüncü stego görüntülerin seçilmesi durumunda elde edilen denklik sistemidir. Matris tersleme işlemi, bu lineer denklik sistemine çözüm getirmek için kullanılır. Çözümün ara adımları ve sonuç (2.10)'da verilmiştir.

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 10 & 12 & 2 \\ 18 & 12 & 18 \\ 24 & 27 & 27 \end{bmatrix}^{-1} \begin{bmatrix} 26 \\ 50 \\ 212 \end{bmatrix} = \begin{bmatrix} 24708 \\ 20606 \\ 58806 \end{bmatrix} \bmod 251 \equiv \begin{bmatrix} 110 \\ 24 \\ 72 \end{bmatrix} \tag{2.10}$$

Üç tane stego görüntünün bütün piksel grupları (her biri üç pikselden oluşan gruplar) yukarıda ifade edilen işleme tabi tutulduğu takdirde gizli görüntü yeniden yapılandırılır.

Bu çalışmada geometrik tabanlı yeni bir gizli görüntü paylaşma şeması önerilmiştir. Şema polinomial tabanlı gizli görüntü paylaşma şemalarından farklı olarak, Blakley'in geometrik tabanlı şemasını gizli görüntü paylaşımında kullanmaktadır. Var olan geometrik tabanlı gizli görüntü paylaşma şemaları ile üretilen pay görüntüleri gürültü şeklinde olup kötü niyetli kişilerin ilgisini çekebilir. Aynı zamanda bu şemalarda stego görüntülerin doğruluğunun testi de yapılmamaktadır. Çalışmada steganografi kullanılarak üretilen pay görüntüleri anlamlı örten görüntülere saklanmıştır. MD5 özüt fonksiyonu kullanılarak da stego görüntülerinin bütünlüğünün testi yapılmıştır.

Yöntem, polinomial tabanlı yöntemlere göre depolama ihtiyaçları, stego görüntülerin iletimi için gerekli bant genişliği ve iletim zamanı değerlendirmesi açısından daha başarılı sonuçlar vermiştir. Genişleme oranı diğer yöntemlere kıyasla $1/4$ oranında azaltılmıştır. Aynı zamanda üretilen stego görüntülerin PSNR değerleri k'nın ikiden büyük olduğu

durumlarda “Bulgular ve İrdeleme” bölümünde görüleceği gibi diğer yöntemlerden daha iyi sonuç vermektedir.

2.2. Steganografi Tabanlı ve Doğrulama Mekanizmalı Şema

Son yıllarda yapılan çalışmalarda Shamir’in yöntemi ve steganografi beraber kullanılarak gizli görüntülerin *n* kişi arasında paylaştırılması amaçlanmaktadır. Aynı zamanda üretilen pay görüntüleri steganografi yardımıyla anlamlı görüntüler içerisine saklanır. Araştırmacılar tarafından steganografi tabanlı ve doğrulama mekanizmalı şemalardaki esasta iki unsurun geliştirilmesi hedeflenmektedir:

- Pay görüntüleri saklandıktan sonra oluşan stego görüntülerin PSNR değerlerinin iyileştirilmesi.
- Stego görüntüleri doğrulamada kullanılan bit sayısının artırılması.

Yöntemler üretilen pay değerlerini örten görüntülere saklarken en basit steganografi tekniklerinden biri olan LSB’ye saklama tekniğini kullanmaktadır [59-72]. Üretilen pay değerlerinin $[0-250]$ aralığında olması, kodlama esnasında 8 bitin kullanımını gerektirir. Gizli görüntüdeki bir pikseli kodlamak için örten görüntüdeki 2×2’lik piksel bloğunun kullanıldığı düşünülürse, 4 pikselin son iki biti pay değerini saklar. Son hanelerdeki diğer bitlerden ise doğrulama bitlerinin saklanması esnasında faydalanılır. 2004’te Lin’in yapmış olduğu çalışma doğrulama için fazladan bir bit kullanmıştır [59]. Doğrulama bitinin elde edilebilmesi için eşitlik (parity) doğrulama yöntemi örten blok üzerinde uygulanmaktadır. Böylelikle örten bloğun karşılık düşen piksellerinin sırasıyla (3, 2, 2, 2) biti pay değerini ve doğrulama bitini barındırır. 2007 yılında Yang vd.’nin yapmış olduğu çalışmada eşitlik doğrulama biti yerine anahtarlı özüt fonksiyonlarının kullanımı önerilmiştir [62]. Aynı zamanda pay değerlerinin üretimi esnasında GF(2^8) kullanmaları, gizli görüntüdeki $[251-255]$ arasındaki piksel değerlerinin bozulmasına engel olmuştur. LSB’ye saklama prosedüründe kullandıkları bit düzeninin farklı olması sayesinde stego görüntülerin PSNR’sini 2004’deki yönteme kıyasla geliştirmişlerdir. 2008 yılında Chang vd.’nin önermiş olduğu çalışmada, doğrulama bitlerinin sayısı 4’e çıkarılmıştır [63]. Doğrulama bitlerinin üretiminde Çinli kalan teoreminden faydalanmışlardır. Yalnız örten bloğun toplam 12 bitinin LSB’ye saklama esnasında değişmesinden dolayı stego görüntülerin PSNR değeri diğer yöntemlere kıyasla daha düşük olmuştur. 2009 yılında, Wu vd.’nin

önermiş olduğu çalışma stego görüntülerin PSNR değerini iyileştirmeyi amaçlamıştır [65]. 2007 yılında Yang vd. tarafından yapılmış çalışmaya kıyasla PSNR değerinde 0.4 dB artış elde etmişlerdir.

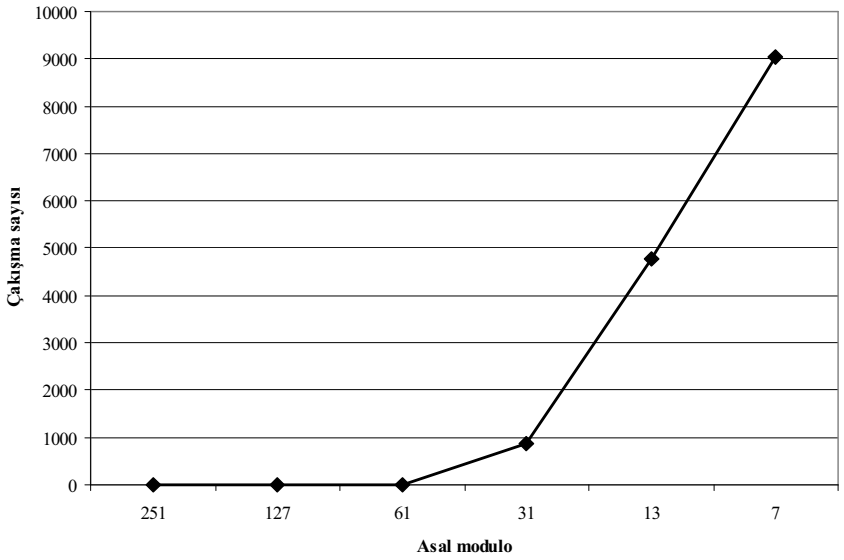
Bu alanda yapılan çalışmalardan da gözlemlenebileceği gibi, yöntemler stego görüntülerin doğrulama yeteneğini iyileştirirken, PSNR değerinden ödün vermektedir. Tez kapsamında gerçekleştirilen çalışmada, pay değerlerini ifade ederken farklı bir kodlama tekniğinin kullanımı önerilmiş ve bu sayede hem doğrulamada kullanılan bit sayısının artırılması hem de stego görüntülerin PSNR değerinin iyileştirilmesi amaçlanmıştır [146]. Sonuçlar kısmında da gözlemlenebileceği gibi, stego görüntülerin PSNR değerleri diğer yöntemlere kıyasla 1.2 dB artmaktadır. Aynı zamanda yöntemin yalancı stego blokları yakalayabilme olasılığı 0.875 olarak rapor edilmiştir. Doğrulama amacıyla örten blokta üç bit kullanılmaktadır. Önerilmiş olan tekniğe ilişkin detaylar ilerleyen kısımda verilmektedir.

Önerilen yöntem paylaştırma ve saklama, yeniden yapılandırma olarak adlandırılan iki alt algoritmadan oluşur. Paylaştırma ve saklama prosedürü tarafından gizli görüntü n katılımcı arasında paylaştırılır. Kullanıcı tarafından seçilen örten görüntüler, gürültü şeklindeki pay bilgilerini kötü niyetli kullanıcılardan saklamak amacıyla kullanılır. Dağıtıcı, D, n katılımcı için n farklı örten görüntü seçmek zorundadır. Dağıtıcı, sır paylaştırma algoritmasını gizli görüntü ve n örten görüntü üzerinde gerçekleştiren kişidir.

$N \times M$ büyüklüğündeki gizli görüntünün her pikseli sırasıyla işlem görür ve üretilen pay değerleri örten görüntülerde karşılık düşen 2×2'lik piksel bloklarına yerleştirilir. Gizli piksel değeri, oluşturulacak olan polinomun sabit katsayı değerlerini belirlerken kullanılır. Her pikselin 8 bit ile temsil edildiği gri seviye resimlerde, piksel parlaklık değerleri $[0-255]$ aralığındadır. 2004'teki çalışmada, paylaştırma algoritmasından önce, parlaklık değeri 251 ve yukarısında olan gizli piksel değerleri 250'ye ötelenmektedir [59]. Gizli görüntü piksel değerlerinin belirli bir aralıkta olması zorunlu olduğu için, bu aralık dışında kalan piksel değerlerinin alt değere (250) ötelenmesi, Lin ve Tsai'nin çalışmalarında bir acizlik olarak rapor edilmiştir [62]. Shamir'in yaklaşımından kaynaklanan böyle bir bozulma, gizli görüntünün askeri bir bilgi taşıması durumunda, tolere edilemeyebilir.

Önerilen yöntem piksel parlaklık aralığını alt alanlara bölerek, ötelemeden kaynaklanan gizli piksel parlaklık değerlerinin bozulmasına engel olmayı ve stego görüntülerin görsel kalitesini iyileştirmeyi hedeflemektedir. Böylece, Shamir'in polinomu ile kullanılacak olan asal sayı değeri 251'den küçük bir değer olarak seçilebilir. Polinom

ile kullanılacak olan asal sayı değerinin daha küçük seçilmesi, pay bilgilerini kodlamada daha az sayıda bitin kullanılacağı gerçeğini beraberinde getirir. Önerilen yöntem 31 değerini asal modulo değeri olarak belirlemiştir. 31'den daha küçük asal sayı değerlerinin seçilmesi, farklı örten bloklardan aynı x değerlerinin elde edilme olasılığını artırmaktadır. Şekil 2.2'de, (3, 4) eşik şeması için farklı asal sayı değerleri kullanılması durumundaki çakışma sayıları değerlendirilmiştir. Modulo işlemi ilk üç asal sayı değeri için (251, 127 ve 61), x değerlerinin limitli aralığından dolayı çakışmaya sebep olmaz. Fakat, bu değerler pay değerlerini kodlamada kullanılacak olan bit sayısını artırır. Yöntemin 31 değerini seçmesi, çakışmaların sebep olduğu görüntüdeki bozulmaların, pay değerlerini daha az sayıda bit kullanarak temsil edilmesi ile tolere edilmesinden kaynaklanmaktadır. Pay değerlerini temsil etmekte kullanılan bit sayısı ile çakışma sayısı arasında ters bir ilişki mevcuttur.



Şekil 2.2. Farklı asal modulo değerleri için çakışma miktarları

Seçilen asal sayı değeri üretilen pay değerlerinin örten bloklara kodlanmasında, diğer yöntemlerden farklı olarak 8 bit yerine 5 bit'in kullanımına neden olur. Kodlama esnasında kullanılan bit sayısının azalması daha az değişime uğramış stego görüntülerin oluşmasını, böylelikle PSNR değerinin iyileşmesini sağlar. Diğer yandan, pay değerlerini kodlamada kullanılan bit sayısının azalması, doğrulama için kullanılacak bit sayısının artırılabilmesini

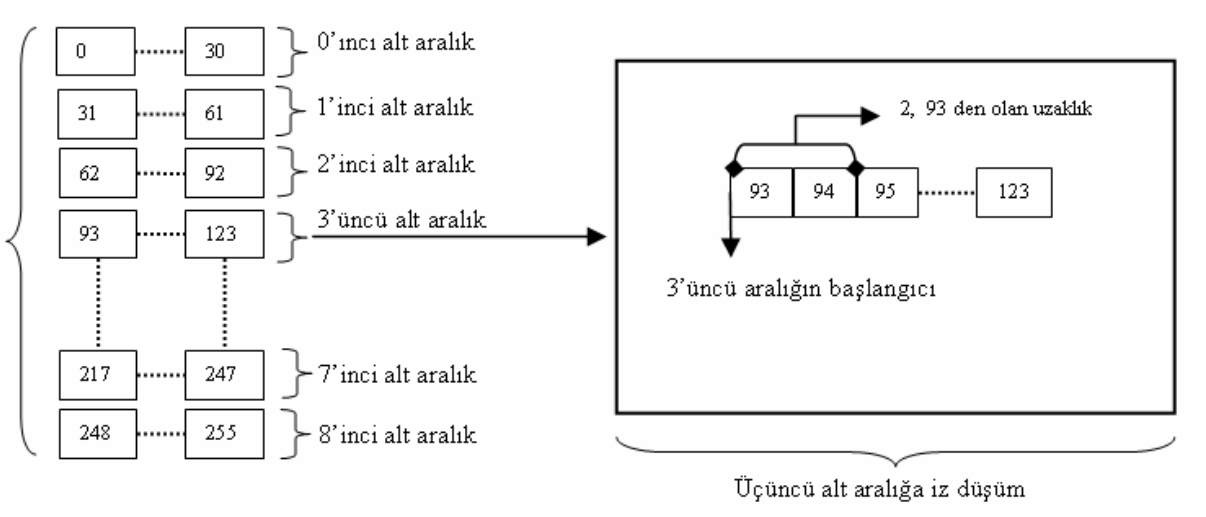
olanaklı kılar. Stego görüntülerin PSNR değerini iyileştirirken aynı zamanda doğrulama yeteneğini artıran yöntemin detayları aşağıda verilmiştir.

Yöntem tarafından piksel parlaklık değer aralığı birbiriyle örtüşmeyen 9 alt aralığa bölünmektedir, $\{[0-30],[31-61],\cdots,[217-247],[248-255]\}$. Her gizli görüntü pikseli, kodlama esnasında bu alt aralıklardan birine karşı düşürülür ve iki değer ile ifade edilir. Bunlardan ilki pikselin karşı düştüğü alt aralık hakkında bilgi veren ve 0 ile 8 arasında değer alan alt aralık indeksidir. İkincisi ise belirlenen alt aralıktaki başlangıca göre pozisyonu gösterir ve 0 ile 30 arasında değer alır. $N \times M$ büyüklüğündeki P ile gösterilen gizli görüntüden alınan *i*'inci satır *j*'inci sütundaki piksel değeri p_{ij} ile gösterilsin. Piksel değerinin karşılık düştüğü alt alan basit bir işlemle hesaplanabilir, $\lfloor p_{ij}/31 \rfloor$. Bu aralığın başlangıcından itibaren olan ofset değeri ise $(p_{ij} \bmod 31)$ ile belirlenir. Böylece, her bir piksel parlaklık değeri iki sayı ile temsil edilmiş olur, $(\lfloor p_{ij}/31 \rfloor, p_{ij} \bmod 31)$. Gizli görüntü pikselini temsil eden sayılar, polinomun ilk iki katsayısına kodlanırken, geriye kalan *k*-2 adet katsayı değeri $[0-30]$ aralığındaki sayılardan rasgele olarak belirlenir. Asal modül değeri 31 olarak seçildiği için, polinomdan üretilen değerlerin temsilinde 5 bit yeterli olacaktır. 95 değerini taşıyan gizli görüntü pikselinin, $p_{ij} = 95$, alt aralıklara karşı düşürülmesinde kullanılan yöntemin görsel ifadesi Şekil 2.3'te verilmiştir. Gizli piksel değeri, üçüncü ($\lfloor 95/31 \rfloor = 3$) alt aralıktaki baştan ikinci ($95 \bmod 31 \equiv 2$) değer olarak ifade edilebilir. Böylece önerilen algoritmaya göre 95 değerine sahip piksel değeri $(3, 2)$ ile temsil edilir. Herhangi gizli piksel değerini temsil etmekte kullanılan iki değer (r_1, r_2) ile gösterilsin. Bu durumda paylaştırma algoritması tarafından kullanılacak olan polinom (2.11)'de verilmiştir.

$$q(x) = \left(r_1 + r_2 x + c_2 x^2 + c_3 x^3 \cdots + c_{k-1} x^{k-1}\right) \bmod 31 \tag{2.11}$$

Polinomun ilk ikisi hariç diğer katsayıları $[0-30]$ aralığındaki sayılar arasından rasgele olarak belirlenir. Her gizli piksel değeri *k* ile gösterilen örten görüntüde 2 × 2'lik bir örten bloğa karşı düşmektedir, $k = \{1, \cdots, n\}$. Gizli görüntünün *i*'inci satır ve *j*'inci sütununda yer alan piksel değerinin, p_{ij}, *k*'ıncı örten görüntüde karşılık düştüğü blok B_k^{ij} ile gösterilsin. Her 2 × 2 'lik örten bloğun ilk pikselinin en anlamlı 6 biti, (2.11) ile verilen

polinomun değerlendirilmesi aşamasında *x* değeri olarak kullanılır. Polinomdan elde edilen $q(x)$ değeri üç parçaya bölünür. Her parça sırasıyla 2, 2, 1 bit'ten oluşmaktadır. Bu parçalar o anki örten bloğun üç piksel değerine saklanır. *n* örten görüntüdeki karşılıklı örten bloklardan aynı şekilde yararlanılmaktadır.



Şekil 2.3. $p_{ij} = 95$ değerinin alt aralıklara karşı düşürülmesi

Şekil 2.4'te *k*'ıncı örten görüntünün kullanımı ile elde edilen stego blok görüntüsü verilmiştir. Örten blok, pay bilgilerinin saklanmasının ardından stego blok olarak adlandırılmaktadır.

X_k^{ij} $(x_1\ x_2 \cdots x_6\ s_1\ s_2)$	V_k^{jj} $(v_1\ v_2 \cdots v_6\ s_3\ s_4)$
W_k^{ij} $(w_1\ w_2 \cdots w_6\ a_1\ s_5)$	Z_k^{ij} $(z_1\ z_2 \cdots z_6\ a_2\ a_3)$

Şekil 2.4. 2×2 pikselden oluşan stego blok görüntüsü

B_k^{ij} ile gösterilen örten bloğun ilk pikseli olan X_k^{ij}'nın en anlamlı 6 bitinin $(x_1, x_2, \cdots, x_6)$ onluk düzendeki değeri, (2.11)'deki polinomda *x* değeri olarak kullanılır ve

S_k^{ij} ile gösterilen pay değeri üretilir. S_k^{ij} ile ifade edilen pay değerinin ikilik düzendeki karşılığı $(s_1 s_2 \cdots s_5)$ ile gösterilsin. *k*'ıncı örten görüntüde karşılık düşen piksel bloğunun B_k^{ij}, $(x_7 x_8 v_7 v_8 w_8)$ ile ifade edilen bit değerlerinin, sırasıyla $(s_1 s_2 \cdots s_5)$ bit değerleri ile değiştirilmesi sonucu, pay değerini saklama işlemi gerçekleştirilmiş olur.

Önerilen yöntemde NIST'in FIPS198 standardına uyan HMAC özüt fonksiyonunu gizli anahtar değeri olan *K* ile kullanmıştır, $H_K(\cdot)$. Stego bloğun 3-bit doğrulama bitleri $(a_1 a_2 a_3)$ hariç olan 29 bitlik kısmı, bloğun indeks değeri $i * j \in [1, M \times N]$ ve stego görüntünün tanımlayıcı numarası $I_{ID}^{(ij)}$, özüt fonksiyonuna parametre olarak verilir. (2.12)'de ifadesi verilen özüt fonksiyonu geriye 160 bit değer döndürmektedir, $G = \{g_i \mid i \in \{1, 2, \cdots, 160\}\}$.

$$G = H_K\left(\left(B_k^{ij} - \left(\{a_1, a_2, a_3\}\right)\right) \| i * j \| I_{ID}^{(ij)}\right) \tag{2.12}$$

3 bitlik doğrulama dizisi $(a_1 a_2 a_3)$, 160 bitlik özüt fonksiyonu sonucu üzerinde basit bir XOR işleminin (2.13)'teki gibi uygulanması ile elde edilir.

$$(a_1 a_2 a_3) = (g_1\ g_2\ g_3) \oplus \cdots \oplus (g_{157}\ g_{158}\ g_{159}) \oplus (g_{160}\ 11) \tag{2.13}$$

Sonuç olarak örten bloğun $(w_7 z_7 z_8)$ ile gösterilen bitleri, stego blok için hesaplanan doğrulama bitleri ile yer değiştirilir, $(a_1 a_2 a_3)$. Yukarıda tanımlanan prosedür gizli görüntünün bütün pikselleri için, pay değerlerini ve doğrulama bitlerini üretmek ve karşılık düşen örten bloklara saklamak için uygulanır. Pay değerlerinin üretilmesi ve karşılık düşen örten bloklara yerleştirilmesi, stego bloklardan doğrulama bitlerinin elde edilmesi ve saklanmasını özetleyen algoritmanın adımları aşağıda verilmiştir. Yalancı kod ifadesi ise Ek 4'te mevcuttur. Gizli görüntü büyüklüğünün $N \times M$ ve örten görüntü büyüklerinin $2N \times 2M$ olduğu varsayılmıştır. (Algoritmanın dördüncü adımında kullanılan ve $\wedge$ ile gösterilen işaret, bit düzeyindeki AND'leme işlemine karşılık düşmektedir)

Paylaştırma ve Saklama Prosedürü

1. Dağıtıcı, *D,* gizli görüntüyü piksellere böler, $p_{11}, p_{12}, \cdots, p_{MN}$.

2. Aşağıdaki adımları $i = 1, 2, \cdots, M$ için tekrarla.

3. Aşağıdaki adımları $j = 1, 2, \cdots, N$ için tekrarla.

3.1. O anki gizli piksel değerini temsil eden (r_1, r_2) değerini, $(\lfloor p_{ij}/31 \rfloor, p_{ij} \bmod 31)$ olarak hesapla.

3.2. $q(x) = (r_1 + r_2 x + c_2 x^2 + \cdots + c_{k-1} x^{k-1}) \bmod 31$ şeklindeki (*k*-1). dereceden $q(x)$ polinomunu yapılandır.

4. Aşağıdaki adımları $t = 1, 2, \cdots, n$ için tekrarla.

4.1. *t* inci örten görüntüde, p_{ij} 'ye karşılık düşen örten blok B_t^{ij} olsun.

4.2. B_t^{ij} ile gösterilen örten bloğun ilk piksel değerini al, $X_t^{ij} = B_t^{ij}(1,1)$.

4.3. Polinomun o anki örten görüntü için giriş parametresi olan değeri hesapla, $x_t = \lfloor (X_t^{ij} \wedge 252)/4 \rfloor$.

4.4. $q(x_t)$'nin hesaplanması ile 5 bit lik pay bilgisini, $S_t^{ij} = (s_1 s_2 s_3 s_4 s_5)$ elde et.

4.5. $(s_1 s_2 s_3 s_4 s_5)$ ile gösterilen 5 bitlik pay bilgisini, o anki örten bloğun B_t^{ij} üç piksel değerine, $X_t^{ij}\ V_t^{ij}\ W_t^{ij}$, yerleştir.

4.6. O anki stego bloğu kullanarak özüt bit dizisi olan *G*'yi (2.12) yardımıyla hesapla.

4.7. 3 bitlik doğrulama dizisini oluştur, $(a_1 a_2 a_3)$.

4.8. Karşılık düşen örten bloğun $(w_7 z_7 z_8)$ ile gösterilen bitlerini $(a_1 a_2 a_3)$ ile yer değiştir.

Önerilen algoritmaya bakarak, sonuçta üretilecek olan stego görüntülerin kalitesinde ve stego görüntülerin doğrulama oranında iyileşme olacağı söylenebilir. Gizli piksel değerleri, $[0-30]$ aralığındaki iki sayı ile ifade edilmektedir. Böylece Shamir'in polinomunda belirlenen asal modulo değeri 31 olarak seçilebilmiştir. Polinomun kullanımı ile üretilen pay değerleri ise 5 bit olmaktadır. Pay bilgisini ifade etmede kullandığı bit sayısının daha az olması, literatürdeki diğer yöntemlere kıyasla üretecek olduğu stego görüntülerin PSNR değerlerinin daha iyi olacağı gerçeğini beraberinde getirmektedir.

Doğrulama oranının iyileşmesi ise kullanılan bit sayısı ile ilişkilidir. Her stego blok üç doğrulama biti içermektedir. Bu da algoritmanın bozulmuş bir stego bloğu tespit

edilebilme olasılığını $7/8$ olarak belirler ve bu değer literatürdeki diğer üç çalışmadan daha yüksektir [59, 62, 65].

Yeniden yapılandırma ve doğrulama aşamasında algoritma tarafından en az k tane katılımcının, gizli görüntüyü yeniden yapılandırmak üzere bir araya getirildiği varsayımı yapılmaktadır. Paylar, içerisindeki bilgiler yeniden yapılandırmada kullanılmadan önce, herhangi bir bozulmaya uğrayıp uğramadığının tespiti için doğrulanmalıdır. Yöntemin bu fazında iki prosedür eş zamanda kullanılır. İlk prosedür stego görüntünün herhangi bir şekilde bozulmadığını doğrularken, diğeri doğrulamanın gerçeklenmesi durumunda gizli veriyi yeniden yapılandırmaktadır. İkinci prosedürde Lagrange'ın interpolasyon tekniğinden gizli görüntünün elde edilmesinde faydalanılır.

$2N\times 2M$ büyüklüğünde stego görüntülere sahip n katılımcıdan herhangi k tanesinin görüntüsü, S ile gösterilen gizli görüntüyü yeniden yapılandırabilmek için toplanmış olsun, $(ST_1, ST_2, \cdots, ST_k)$. Her stego görüntü kendi içinde 2×2'lik bloklara bölünür. Her pay (stego) görüntüsündeki toplam 2×2'lik blok sayısının t olduğu varsayılsın. ST_k^i, k'ıncı stego görüntüdeki i'inci bloğu gösterir. Bu bloktaki dört piksel değeri $(X_k^i V_k^i W_k^i Z_k^i)$ şeklindedir. İlk önce doğrulayan daha sonra gizli veriyi elde eden algoritmanın adımları yalancı kodla beraber aşağıdaki şekilde verilmiştir.

1. $i = 1, 2, \cdots, t$ için aşağıdaki adımları tekrarla.

2. $j = 1, 2, \cdots, k$ için Adım 3 ve Adım 5 arasını tekrarla.

3. Doğrulama bit dizisini $(d_1 d_2 d_3)$ o anki stego blok ST_j^i için aşağıdaki ifadeyi kullanarak hesapla.

$$G_j = H_K\left(\left(ST_j^i - \left(\{a_1, a_2, a_3\}\right)\right) \| b \| I_{ID}^{(j)}\right), \quad b = \left\lceil \frac{i}{M} \right\rceil * \left(i - \left(\left\lceil \frac{i}{M} \right\rceil - 1 \right) * M \right)$$

4. Stego bloktaki doğrulama bit dizisini elde et $(a_1 a_2 a_3)$.

5. Eğer hesaplanan değer $(d_1 d_2 d_3)$ çıkartılan bit dizisine $(a_1 a_2 a_3)$ eşitse, blok doğrulanır ve adım 2'ye dönülür. Aksi takdirde blok bozulmuş olarak işaretlenir ve Adım 1'e dönülür.

6. k stego görüntüdeki i inci bloklar doğrulandıktan sonra kontrol *yeniden yapılandırma* prosedürüne geçer. k bloktan elde edilen ilk 5 bit değerleri $q(x)$ Lagrange'ın interpolasyonun da kullanılır ve gizli piksel değeri elde edilir.

Yukarıdaki algoritmada adım 3 ile adım 5 arasında verilmiş olan doğrulama prosedürü, k stego görüntüdeki karşılıklı stego blokların doğrulamasını yapmaktadır. Bütün

bloklar doğrulanmadığı müddetçe, gizli piksel değeri yeniden yapılandırılmaz ve gizli piksel değeri bozulmuş olarak işaretlenir. *k* stego görüntüdeki bütün bloklar benzer mantıkla işlem görür.

Doğrulama mekanizması için özüt fonksiyonu tarafından oluşturulan üç bitlik doğrulama dizisi kullanılır. Böylece, her stego bloktaki bozulma $7/8$ olasılıkla tespit edilir. Literatürdeki diğer çalışmalarda bu değer $1/2$ olarak rapor edilmiştir. Bu doğrultuda, diğer yöntemlerle kıyaslandığında önerilen yöntemin bozulmuş stego blok ataklarına karşı daha hassas olduğu söylenebilir. *k'*dan az stego görüntünün toplanması durumunda gizli görüntü hakkında herhangi bir bilgi edinilemez. Yöntem gereği en az *k* adet pay görüntüsünün bir araya gelmesi şarttır.

Sonuç olarak, giriş kısmında vurgu yapıldığı gibi, steganografi kullanan gizli görüntü paylaşım tekniklerinde araştırmacılar tarafından geliştirilmeye çalışılan metriklerden ikisi: üretilen stego görüntülerin PSNR değerinin artırılması ve stego görüntüleri doğrulama mekanizmasının iyileştirilmesidir. Bu çalışmada önerilen yöntemle beraber her iki metrik de iyileştirilmeye çalışılmıştır. Önerilen yöntem $[0-255]$ aralığında tanımlı piksel parlaklık değerlerini 31 değerden oluşan 9 alt alana karşı düşürmektedir. Her bir gizli görüntü pikseli iki sayı ile temsil edilir: Ait olduğu alt alanın indis değeri ve bu alt alanda başlangıca göre konumu. Örneğin 95 parlaklık değerine sahip bir piksel $(3, 2) = 31 \times 3 + 2$ ile temsil edilmektedir. Bu anlamda her piksel değerinin $[0-30]$ aralığındaki iki sayı ile temsil edildiği söylenir. Shamir'in yönteminde kullanılan asal modulo değeri yöntem tarafından 31 olarak belirlenmiştir. Bundan dolayı üretilen pay değerleri 5 bit ile temsil edilebilir. Yöntem aynı zamanda stego blokları doğrulamak için, özüt fonksiyonu sonucunda üretilen 3 doğrulama bitini kullanmaktadır. 2×2'lik örten bloktaki toplam 32 bitin 8 biti pay değerlerini ve doğrulama bitlerini taşımak için kullanılır. Daha az sayıda biti veri taşıma için kullandığından dolayı, önerilen yöntem literatürdeki diğer çalışmalara kıyasla daha yüksek PSNR değerleri üretmektedir. Stego görüntülerin PSNR değerleri, "Bulgular ve İrdeleme kısmında" gözlemlenebileceği gibi, Wu'nun 2009'da önermiş olduğu yönteme kıyasla 1.2 dB iyileşmiştir. Yöntem kötü niyetli kullanıcılara karşı daha dayanıklı hale getirilmiştir. Diğer yandan, yöntemin doğrulama mekanizması da Wu'nun önermiş olduğu yönteme kıyasla daha iyidir. Wu'nun yöntemi 2 × 2'lik bloğun doğrulamasında 1 bit kullanırken, önerilen yöntem 3 doğrulama biti kullanmaktadır. Literatürdeki diğer çalışmaların bozulmuş bir stego bloğu tespit edebilme olasılığı 0.51

olarak rapor edilirken, önerilen yöntem için bu değer 0.875 olarak ölçülmüştür. Yöntem, deneysel sonuçlarda vurgulandığı gibi, literatürdeki diğer yöntemlere kıyasla daha yüksek PSNR değerine ve geliştirilmiş bir doğrulama mekanizmasına sahiptir. Shamir'in polinomunda daha küçük asal sayı değerlerinin kullanımı, x değerlerinde çakışmaya sebep olmuştur. Şekil 2.2'de seçilen farklı asal sayı değerleri için yöntemin üretmiş olduğu çakışma miktarları verilmiştir. Çakışmaları engellemek için x değerlerinin değiştirilmesi, örten görüntüdeki en anlamlı 6 hanede değişime sebep olur. Çalışmada, doğrulama mekanizmasını iyileştirilirken, çakışmalardan kaynaklanan bozulma minimum düzeyde tutulmaya çalışılmıştır. Önerilen yöntem pay değerlerini farklı bir biçimde temsil ederek, doğrulama mekanizması için kullanılacak olan bit sayısını artırmaktadır.

2.3. EMD'ye Dayanan Geri Döndürülebilir Gizli Görüntü Paylaşım Şeması

Gizli görüntü paylaşımı alanında pay görüntülerinin örten görüntülerin içerisine saklanması sistem güvenliği açısından önemlidir. Saklama esnasında kullanılan örten görüntülerin medikal, askeri ya da sanatsal bir görüntü olması durumunda örten görüntülerin stego görüntüler kullanılarak yeniden yapılandırılabilmesi önem taşımaktadır. Steganografi tabanlı ve doğrulama mekanizmalı gizli görüntü paylaşım şemalarından farklı olarak Lin vd., 2009'da yapmış oldukları çalışmada örten görüntülerin, stego görüntülerden tekrar elde edilmesinin önemine vurgu yaptılar [73]. Çalışmalarında modulo operatörü pay değerlerinin örten görüntülere saklanması esnasında kullanıldı. Saklama esnasında kullanılan algoritma Thien ve Lin'in, 2003'teki çalışmasında tanımlanmaktadır [9]. k=4 için önermiş oldukları şemanın üretmiş olduğu stego görüntülerin PSNR değeri yaklaşık olarak 43 dB civarındadır. Yöntemlerini aynı zamanda siyah beyaz görüntüler üzerinde de test etmişler ve 38 dB PSNR'ye sahip stego görüntüler üretmişlerdir. Saklama esnasında kullandıkları algoritmadan dolayı yöntemleri alttan ve üstten taşma durumları ile karşılaşmaktadır. Stego ve örten görüntü pikselleri arasındaki piksel parlaklık değeri farklılıkları gri seviye örten görüntüler için $[-3, 3]$ aralığında değişir. Değişim aralığı siyah beyaz pikselleri olan örten görüntülerin kullanılması durumunda ise $[-6, 6]$ olmaktadır. Alttan ve üstten taşma durumlarından dolayı, önermiş oldukları yöntem siyah beyaz piksel sayısı fazla olan resimlerde daha düşük PSNR değerlerine sahiptir.

[74]'teki çalışma, [73]'teki çalışmanın taşıma kapasitesini iyileştirmeyi hedeflemektedir. Gri seviye örten görüntülerin kullanılması durumunda üretmiş oldukları stego görüntüler yaklaşık olarak 40 dB PSNR'ye sahiptir. Fakat önermiş oldukları yöntem siyah beyaz örten görüntüleri kapsamamaktadır. Taşıma kapasitesinde gösterdikleri artışa rağmen üretmiş oldukları PSNR değerleri düşüktür. Stego ve örten görüntü pikselleri arasında fark aralığı $[-6,6]$ olarak tespit edilmiştir. Yöntem gizli veriyi m tabanında temsil etmektedir. Bu nedenle $[\lfloor 255/m \rfloor \times m, 255]$ değer aralığındaki pikseller yöntem tarafından kullanılamamaktadır. [73]'teki çalışma pay değerlerinin saklanması esnasında geleneksel LSB'ye saklama tekniğinden farklı olarak, [9]'daki çalışmada tanımlanan steganografik yöntemden faydalanmaktadır. Fakat modulo işleminin alttan ve üstten taşmalara sebebiyet veriyor olması, siyah beyaz örten görüntüler için üretilen stego görüntülerin PSNR değerinin düşük olmasına sebep olacaktır. Diğer yandan [74]'teki çalışmada kullanılan saklama yöntemi ise örten görüntülerdeki beyaz piksellerin kodlamada kullanılamamasına sebep olmaktadır. Bu durumda siyah beyaz görüntüler ya da tram görüntülerin örten ortam olarak kullanılması olanaksız hale gelmektedir.

Çalışma kapsamında önerilen yöntem [20]'deki çalışmada yer alan EMD'yi oluşturulan özel denklem ifadesini uyarlayarak pay değerlerinin saklanmasını gerçekleştirmiştir. Oluşturulan denklem ifadesinin kullanımı ile yöntem literatürdeki çalışmalardan farklı olarak örten görüntü piksel değerlerinden bağımsız, yüksek PSNR değerlerine sahip stego görüntüler üretebilmektedir. Yöntem tamamen siyah beyaz piksellerden oluşan örten ortamların kullanılması durumunda dahi yaklaşık 43 dB PSNR değerine sahip stego görüntüler üretmektedir. Seçilen örten görüntünün gri seviye olması durumunda bu değer 47 dB seviyesine yükselmektedir. Gri seviye ve siyah-beyaz örten görüntüler için, stego ve örten görüntü piksel parlaklık değerleri arasındaki fark aralığı sırasıyla $[-2,2]$ ve $[-4,4]$ şeklindedir. Fark aralıklarının diğer yöntemlere kıyasla küçülmesinin doğal sonucu olarak, önerilen yöntem daha yüksek PSNR değerlerine sahiptir. Aynı zamanda gizli görüntünün yapılandırılmasının ardından, stego görüntülerden tekrar örten görüntülerin elde edilmesi geri döndürülebilir özelliğinin bir kanıtıdır. Yeniden yapılandırma esnasında modulo operatörünün önerilen şekilde kullanımı ile örten piksel değerleri yeniden elde edilebilmektedir. Yönteme ilişkin detaylar aşağıdaki şekildedir.

2006'da önerilen EMD metodu $f_e = (c_{11} + 2 \cdot c_{12}) \bmod 5$ ile gösterilen yerleştirme fonksiyonunu $[0-4]$ arasındaki gizli değerleri iki örten piksele saklamak için

kullanmaktadır. Fonksiyonun sonucunun gizli değeri verebilmesi için yalnız bir örten piksel değerinin değiştirilmesi yeterlidir. Örten pikseller için değişim aralığı $[-1,1]$ olarak verilmektedir. Lee vd., 2007'deki çalışmada $f_e = (c_{11} + 3 \cdot c_{12}) \bmod 8$ olarak verilen yerleştirme fonksiyonunun $[-1,1]$ aralığındaki değişimle $[0,7]$ aralığındaki gizli verileri kodlayabildiğini göstermiştir [152]. Bu yöntem EMD'den farklı olarak aynı anda iki örten piksel değerinin değişimine izin vermektedir. Lee vd.'nin metodundaki değişim aralığının $[-2,2]$ olarak değiştirilmesi durumunda kodlayabilecek olduğu değer aralığı $[0,15]$ olmaktadır. Çalışmada önermiş olduğumuz yöntem birazdan anlatılacağı gibi $[0,16]$ arasındaki değerleri saklamaya ihtiyaç duymaktadır. Bu nedenle üretilen pay değerlerini saklayabilecek şekilde çalışma kapsamında (2.14)'teki yerleştirme fonksiyonunun kullanımı önerilmiştir.

$$f(g_1, g_2) = (g_1 \cdot 1 + g_2 \cdot 4) \bmod 17 \tag{2.14}$$

Aslında önerilen fonksiyonun kullanımı ile $[0,19]$ aralığındaki değerler, örten piksellerdeki $[-2,2]$ değişim ile kodlanabilmektedir. Yalnız önerilen paylaştırma fonksiyonu, 17 değerini modulo olarak kullandığı için, pay değerleri $[17,19]$ aralığındaki değerleri taşımayacaktır. Çalışma kapsamında önerilen yöntem paylaştırma ve yeniden yapılandırma alt algoritmalarına sahiptir. Paylaştırma algoritması Shamir'in sır paylaşma şemasını gizli veriyi *n* kişi arasında paylaştırmak için kullanmaktadır. Gizli veri $[0,255]$ aralığındaki piksel parlaklık değerlerine sahip gri seviye bir görüntüdür. Dağıtıcı paylaştırma algoritması için *C* ile gösterilen gri seviye bir örten görüntü seçer. Örten görüntü, katılımcılara gönderilen ve pay değerlerini barındıran *n* farklı stego görüntünün üretimi için kullanılmaktadır. *N*×*M* büyüklüğündeki *T* ile gösterilen gizli görüntü $T = \{t_{uv} | t_{uv} \in [0,255], u = \{1 \cdots N\}, v = \{1 \cdots M\}\}$ şeklinde ifade edilsin. Paylaştırma algoritması gizli görüntüyü *S* ile gösterilen vektöre çevirmektedir $S = \{s_i | s_i \in [0,16], i = 1, 2, \cdots, (N \cdot M \cdot \lceil \log_{17} 255 \rceil)\}$. Vektörün sıralı ikilileri (s_i, s_{i+1}), aslında gizli görüntüdeki piksel değerinin 17 tabanındaki gösterimidir ve (2.15)'in kullanımı ile hesaplanır.

$$
\begin{aligned}
s_i &= \left(t_{uv} - t_{uv} \bmod 17\right)/17 \\
s_{i+1} &= t_{uv} \bmod 17 \\
i &= \left(2 \cdot v - 1\right) + \left(u - 1\right) \cdot M \cdot 2
\end{aligned}
\tag{2.15}
$$

[73]'teki çalışmada gizli görüntü 7 tabanına çevrilmektedir. Bu durumda gizli görüntü piksel değerleri $[0, 7]$ aralığındaki üç sayı ile temsil edilir. [74]'teki çalışma ise kendi yöntemlerinin farklı taban değerleri kullanılması durumunda üretmiş olduğu PSNR değerlerini rapor etmiştir. Sonuçlarında taban değeri olarak 7'yi kullanmanın kendi yöntemlerinin üretmiş olduğu stego görüntülerin PSNR değerini iyileştirdiğine vurgu yapmışlardır. Önermiş olduğumuz yöntemin taban değeri olarak 7'yi belirlemesi durumunda, S ile gösterilen vektörün uzunluğu $N \cdot M \cdot 3$ olacaktır. Vektörün büyüklüğündeki artış ise pay değerlerinin saklanabilmesi için daha büyük örten görüntülerin seçilmesini gerektirir. Shamir'in polinomu asal bir değer gerektirdiği için ve gizli piksel değerini iki sayı ile temsil eden ilk asal değer 17 olduğu için, önerilen yöntem gizli piksel değerlerinin ifade edileceği taban değeri olarak 17'yi seçmiştir. Üretilen S vektörünün büyüklüğü $N \cdot M \cdot 3$ yerine $N \cdot M \cdot 2$ olmaktadır.

Bu sayede t_{uv} ile gösterilen gizli piksel değerleri S vektörünün karşılık düşen iki eleman değeri (s_i, s_{i+1}) ile temsil edilir. Örneğin gizli görüntüdeki piksel değerlerinin $(125, 215)$ olması durumunda, S vektörünün karşılık düşen elemanları $((7, 6); (12, 11))$ şeklinde hesaplanır.

Paylaştırma algoritması S vektörünü her biri k-2 elemandan oluşan bölümlere ayırır. $N \cdot M$ büyüklüğündeki gizli görüntü için, toplamda üretilen bölüm sayısı $(N \cdot M \cdot 2)/(k - 2)$ olmaktadır. Her bölüm Shamir'in polinomunu yapılandırmakta kullanılır. Polinomun ilk k-2 katsayısı o an işlem görmekte olan bölümden gelmektedir. Diğer iki katsayı değeri ise pay değerlerinin saklanması esnasında kullanılacak olan iki örten piksel değeri hakkında bilgi içerir. Shamir'in polinomunun n farklı x değeri için üretmiş olduğu değerler pay değerlerini oluşturur. Paylaştırma algoritmasının saklama prosedürü pay değerlerini iki örten piksel değerine kodlamakta ve stego piksel değerlerini elde etmektedir. Buradan yola çıkarak örten görüntü büyülüğünün $(N \cdot M \cdot 4)/(k - 2)$'den büyük olması gerektiği söylenmektedir.

Gizli görüntüdeki her bir bölüme uygulanması gereken işlemler aşağıdaki şekilde özetlenebilir. O an paylaştırılmakta olan bölümün ilk bölüm olduğu varsayılsın. Shamir'in

polinomunun ilk *k*-2 katsayısı o anki bölümün değerleri $(s_1, s_2, \cdots, s_{k-2})$ kullanılarak (2.16)'daki gibi belirlenir. Vektör *S*'nin elemanları, ya da başka bir deyişle polinom tarafından paylaştırılacak olan gizli değerler $[0, 16]$ aralığında olduğu için asal sayı değeri olarak 17 seçilmiştir.

$$F(x) = \left(s_1 + s_2 x + \cdots + s_{k-2} x^{k-3} + p_1 x^{k-2} + p_2 x^{k-1}\right) \bmod 17 \tag{2.16}$$

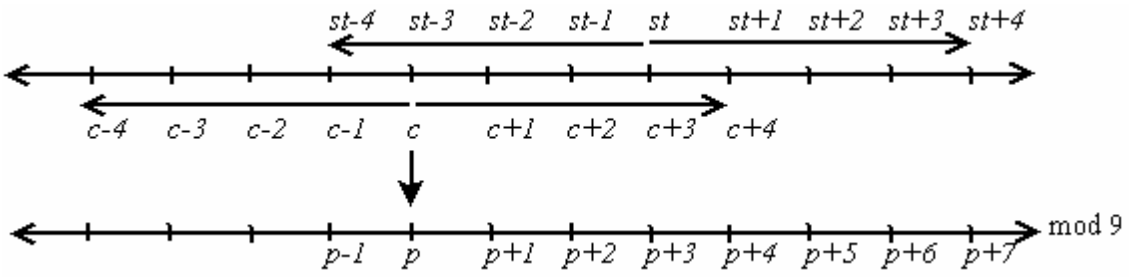
$F(x_k)$ ile gösterilen pay değerini saklamada kullanılacak olan karşılık düşen iki piksel değeri (c_{11}, c_{12}) ile gösterilsin. Polinomda verilen p_1 ve p_2 değerleri (2.17)'nin kullanımı ile hesaplanır.

$$p_1 = c_{11} \bmod 9 \quad p_2 = c_{12} \bmod 9 \tag{2.17}$$

Polinomun (p_1, p_2) ile gösterilen son iki katsayı değeri, yeniden yapılandırma aşamasında stego piksel değerlerinden örten piksel değerlerinin elde edilmesi için kullanılır. Stego piksel değerleri ve örten piksel değerleri arasındaki fark $[-4, 4]$ aralığındadır. *k*'ıncı pay görüntüsündeki ilk stego piksel değeri st_{11}^k ile gösterilsin. Bu piksel değeri saklama prosedürü tarafından c_{11} ile gösterilen örten piksel değerinin $[-4, 4]$ aralığındaki değerlerden biri ile ötelenmesi sonucu elde edilmektedir. Böylece katılımcılar örten piksel değerinin $[st_{11}^k - 4, st_{11}^k + 4]$ aralığında olduğunu yeniden yapılandırma algoritması esnasında bilmektedir. Bu aralık 9 sıralı sayıdan oluşur. Önerilen yöntem bu aralıktaki sayıların modulo 9 tabanında biricik kalana sahip olduğu gerçeğinden faydalanmaktadır. Böylece örten piksel değerleri kullanılarak Şekil 2.5'te görüldüğü gibi stego piksel değerleri elde edilebilmektedir. st_{11}^k ve c_{11} gösterimlerindeki alt ve üst indisler şekildeki anlaşılabilirliği artırabilmek amacıyla göz ardı edilmiştir.

Paylaştırma algoritması *n* farklı pay değerini farklı x_l değerlerini $l = 1, 2, \cdots, k, \cdots, n$ kullanarak, $(x_l, F(x_l))$ çiftleri şeklinde hesaplar. $(F(x_1), F(x_2), \cdots, F(x_n))$ ile gösterilen pay değerleri karşılık düşen stego görüntü piksel değerlerine, örten piksel değerleri kullanılarak kodlanır. Önerilen yöntem tek bir örten görüntüyü *n* farklı stego görüntü $(st^1, st^2, \cdots, st^n)$ üretmek için kullanır. Birinci bölüm için üretilen pay değerlerinin kodlanması sonucu

oluşan *k*'ıncı stego görüntüdeki piksel değerleri $\left(st_{11}^{k}, st_{12}^{k}\right)$ ile gösterilsin. Stego piksel değerlerinin oluşturulması için kullanılan örten piksel değerleri $\left(c_{11}, c_{12}\right)$'dir. (2.14)'te verilen yerleştirme fonksiyonu o anki örten piksel grubu $\left(c_{11}, c_{12}\right)$ üzerinde $f_e\left(c_{11}, c_{12}\right) = \left(c_{11} + 4 \cdot c_{12}\right) \bmod 17$ şeklinde uygulanır.



Şekil 2.5. Örten piksel değerlerinin elde edilebilmesinde kullanılan $\left(p_1, p_2\right)$'nin hesaplanması

Yerleştirme fonksiyonunun üretmiş olduğu değer $F\left(x_k\right)$ değeri ile karşılaştırılır. Eğer eşitlerse $\left(F\left(X_k\right) = f_e\left(c_{11}, c_{12}\right)\right)$, örten piksel değerlerini değiştirmeye ihtiyaç yoktur. Böylece *k* ile gösterilen stego görüntüdeki karşılık düşen piksel değerleri örten piksel değerlerine eşit olur $\left(st_{11}^{k}, st_{12}^{k}\right) = \left(c_{11}, c_{12}\right)$. Aksi takdirde örten piksel değerleri, fonksiyon sonucu $f_e\left(c_{11}, c_{12}\right)$, pay değeri $F\left(x_k\right)$'ye eşit olacak şekilde değiştirilir. Saklama prosedürü her örten piksel değer için değişim aralığını ayrı olarak $\left(x_1, x_2\right)$ ve $\left(y_1, y_2\right)$ şeklinde belirler. Saklama prosedürü *k*'ıncı stego görüntüdeki karşılık düşen piksel değerlerini $\left(st_{11}^{k}, st_{12}^{k}\right)$; pay değeri $F\left(x_k\right)$, örten piksel değerleri $\left(c_{11}, c_{12}\right)$ ve yerleştirme fonksiyon sonucunu $f_e\left(c_{11}, c_{12}\right)$ kullanarak aşağıdaki şekilde hesaplar. Adımları verilen algoritma, vektör'ün ilk bölümünden üretilen pay değerlerinin saklanması sonucu oluşacak olan *n* stego piksel grubunun değerini hesaplamaktadır $\left(st_{11}^{k}, st_{12}^{k}\right), k = 1 \cdots n$.

Saklama Prosedürü

1. O anki örten piksel grubu için, (2.14)'in kullanımı ile yerleştirme fonksiyonu sonucu hesaplanır.

2. (2.18)'i kullanarak her örten piksel değeri için değişim aralıkları belirlenir.

$$
\begin{aligned}
&(c_{11} \geq 254) \Rightarrow \quad x_1 = -4 \quad x_2 = 0 \\
&(c_{12} \geq 254) \Rightarrow \quad y_1 = -4 \quad y_2 = 0 \\
&(c_{11} \leq 1) \Rightarrow \quad x_1 = 0 \quad x_2 = 4 \\
&(c_{12} \leq 1) \Rightarrow \quad y_1 = 0 \quad y_2 = 4 \\
&(2 \leq c_{11} \leq 253) \Rightarrow \quad x_1 = -2 \quad x_2 = 2 \\
&(2 \leq c_{12} \leq 253) \Rightarrow \quad y_1 = -2 \quad y_2 = 2
\end{aligned}
\tag{2.18}
$$

3. $k = 1 \cdots n$ için aşağıdaki adımlar tekrarlanır.

4. $f_e(c_{11}, c_{12}) = F(x_k)$ kontrolü yapılır.

4.1. Eğer eşitlik varsa örten piksel değerlerinde herhangi bir değişikliğe ihtiyaç duyulmaz. O anki stego bloğun piksel değerleri $(st_{11}^k, st_{12}^k) = (c_{11}, c_{12})$ olarak belirlenir.

4.2. Aksi takdirde aşağıdaki adımlar uygulanır.

4.2.1. $X = x_1$'den x_2'ye kadar aşağıdaki adımları tekrarla.

4.2.2. $Y = y_1$'den y_2'ye kadar aşağıdaki adımları tekrarla.

4.2.3. b'nin değerini $b = (X + 4 \cdot Y)$ifadesini kullanarak hesapla.

4.2.4. $(b + f_e(c_{11}, c_{12}))\bmod 17 = F(x_k)$ eşitliği sağlanıyorsa, o anki stego bloktaki piksel değerlerini $(st_{11}^k, st_{12}^k) = (c_{11} + X, c_{12} + Y)$ olarak belirle ve adım 2'ye geri dön.

Yalancı kod ifadesi Ek 5'te verilen algoritmanın icrası sonucu oluşan n tane stego görüntü $(st^1, st^2, \cdots, st^n)$, C ile gösterilen örten görüntünün bir benzeridir. Paylaştırma algoritması alttan ve üstten taşma durumlarını saklama prosedürü boyunca kontrol etmektedir. O anki örten piksel değerleri kullanılarak değişim aralıkları da adaptif olarak belirlenmektedir. Bir stego piksel değeri ile bir örten piksel değeri arasındaki mutlak fark en fazla 4 olabilir. En büyük fark değeri örten piksel değerinin alttan taşma veya üstten taşma sınırına yakın olması durumunda oluşur $(c_{ij} \leq 2 \vee c_{ij} \geq 254)$.

Yöntemin uygulanabilirliğini göstermek ve anlaşılabilirliğini kolaylaştırmak amacıyla iki örnek verilmiştir. Her iki örnekte (4, 5) sır paylaşma şemasını kullanmaktadır. Gizli veri değeri 202 iken, örten piksel değerleri birinci ve ikinci örnek için sırasıyla $(193, 199)$ ve $(255, 255)$ olarak seçilmiştir. İkinci örnek yöntemin üstten taşma sınırına yakın durumlardaki testini sağlar. Beş katılımcı için belirlenen seri sayılar $x_k = k \quad k = 1, 2, \cdots, 5$ olarak seçilmiştir.

Örnek. Gizli veri değeri 202 iki elemanlı S vektörüne dönüştürülür $S = \langle 11, 15 \rangle$. Vektör k-2=2 elemandan oluşan bölümlere ayrılır. Vektörün büyüklüğünden dolayı $(11, 15)$ içeriğine sahip bir bölüm oluşur. Örten piksellerin modulo 9 tabanındaki kalanları (2.17)'nin kullanımı ile p_1=4 ve p_2=1 olarak hesaplanır. Ardından Shamir'in polinomu $F(x) = (11 + 15x + 4x^2 + x^3) \bmod 17$ şeklinde yapılandırılır. Katılımcılara gönderilecek olan pay değerleri kendi seri numaralarının kullanımı ile sırasıyla 14, 14, 0, 12 ve 5 olarak hesaplanır. İlk pay değerinin, karşılık düşen örten piksel değerleri kullanılarak, stego piksel değerlerinin oluşturulmasındaki kullanımı gösterilmektedir. Her iki örten piksel için değişim aralığı, örten piksel değerleri sınırlara yakın olmadığı için $[-2, 2]$ olarak belirlenir. Önerilen yöntem, birinci ve ikinci örten piksel değerlerinin sırasıyla iki ve bir azaltılması durumunda yerleştirme fonksiyonu f_e'nin pay değerini üreteceğini fark etmektedir. Böylece ilk stego görüntüdeki karşılık düşen piksel değerleri $(191, 198)$ olarak belirlenir. Pay değeri 14, yeniden yapılandırma esnasında stego piksel değerleri üzerinde yerleştirme fonksiyonunun uygulanması sonucu $f_e = (191 + 4 \cdot 198) \bmod 17 \equiv 14$ şeklinde elde edilecektir. Diğer dört stego görüntüdeki piksel değerleri ise sırasıyla (191, 198), (194, 198), (193, 197) ve (191, 200) olarak hesaplanır. Örten piksel parlaklık değerleri sınır değerlerine yakın olmadığı için, örten ve stego piksel değerleri arasındaki mutlak fark ikiyi aşmayacaktır.

Örnek. (255 mod 9) değeri 3 olduğundan dolayı, p_1 ve p_2 değerleri 3 olarak hesaplanır. Shamir'in polinomu $F(x) = (11 + 15x + 3x^2 + 3x^3) \bmod 17$ şeklinde oluşturulur. Katılımcılar için üretilecek olan pay değerleri kendi seri numaralarının kullanımı ile 15, 9, 11, 5 ve 9 olarak hesaplanmaktadır. O anki örten blok üzerinde yerleştirme fonksiyonunun gerçekleştirilmesi durumunda $f_e = (255 + 4 \cdot 255) \bmod 17 \equiv 0$ değeri elde edilir. Her iki örten piksel değeri için değişim aralığı algoritma tarafından $[-4, 0]$ olarak seçilecektir. Çünkü üst sınırda olan piksel parlaklık değerlerini artırmak mümkün olmaz. O anki örten bloktaki ilk pikselin değerinin iki azaltılması durumunda, birinci pay değeri olan 15, yerleştirme fonksiyonunun sonucu olarak elde edilir. Böylece ilk stego görüntüdeki karşılık düşen stego piksel değerleri $(253, 255)$ olarak belirlenir. Bu değerlerin kullanımı ile yeniden yapılandırma aşamasında $f_e = (253 + 4 \cdot 255) \bmod 17 \equiv 15$ pay değeri elde edilecektir. Diğer dört stego görüntüdeki piksel parlaklık değerleri sırasıyla algoritma tarafından (255, 253), (253, 254), (255, 252) ve (255, 253) olarak hesaplanır. Örten ve

stego piksel değerleri arasındaki en büyük fark üçüncü stego görüntüde 3 olarak görülmüştür. Sınır değerlerine yakın örten piksel değerleri daha büyük bir değişime neden olmaktadır.

Yeniden yapılandırma algoritması gizli görüntünün elde edilebilmesi için, en az *k* katılımcıdaki stego görüntülerin bir araya gelmesini gerektirir. Paylaştırma algoritması süresince kullanılan örten görüntü de, algoritma tarafından yeniden yapılandırılmaktadır. Yeniden yapılandırma algoritması stego görüntüleri sıralı iki piksel içeren gruplara ayırır. Paylaştırma adımında kullanılan yerleştirme fonksiyonu f_e, her bölüm üzerinde uygulanarak $(F(x_1), F(x_2),\cdots,F(x_k))$ ile gösterilen pay değerleri elde edilir. Lagrange'ın interpolasyon tekniği Shamir tarafından önerildiği gibi *k* ayrı noktadan polinomun tahmini için kullanılır. Polinomun ilk *k*-2 katsayı değeri karşılık düşen gizli piksel değerinin 17 tabanındaki ifadesidir. Son iki katsayı ise yeniden yapılandırma algoritması tarafından örten piksel değerinin elde edilmesinde kullanılır.

Herhangi *k* tane katılımcının kendi stego görüntüleri ile bir araya geldiği varsayılsın $(st^1, st^2, \cdots, st^k)$. Her stego görüntü iki pikselden oluşan bölümlere ayrılır. Yerleştirme fonksiyonu f_e bütün bölümler üzerinde uygulanmaktadır. Paylaştırma algoritması *NM* büyüklüğündeki gizli görüntü için örten görüntü büyüklüğünün en az $((4NM)/(k-2))$ olmasını gerektirmektedir. Örneğin eşik değeri *k*'nın 4 seçilmesi durumunda örten görüntü büyüklüğü en az 2*NM* olmak zorundadır. *k* stego görüntüdeki karşılık düşen bölümlerden, (2.19)'daki ifadenin yardımı ile pay değerlerinin elde edilmesinde faydalanılır.

$$F(x_k) = \left(st_{ij}^k + 4 \cdot st_{ij+1}^k\right) \bmod 17 \tag{2.19}$$

Pay değerleri Lagrange'ın metodu aracılığıyla polinomun interpolasyonunda kullanılır. İnterpolasyon tekniği *k* farklı nokta üzerinde $((x_1, F(x_1)),(x_2, F(x_2))\cdots,(x_k, F(x_k)))$ uygulanır ve (2.20)'deki ifade elde edilir.

$$F(x) = (s_1 + s_2 + \cdots + s_{k-2} + p_1 + p_2) \bmod 17 \tag{2.20}$$

Polinomun ilk *k*-2 katsayısı gizli vektör *S*'nin karşılık düşen değerlerini oluşturmaktadır. Son iki katsayı ise karşılık düşen örten piksel değerlerinin yeniden

yapılandırılmasında kullanılır. Aşağıda verilen "*ortaya çıkarma*" prosedürü (p_1, p_2) değerlerinin kullanımı ile örten piksel değerlerinin yeniden yapılandırılmasını sağlamaktadır. *k*'ıncı stego görüntünün örten piksel değerlerini yeniden yapılandırmada kullanıldığı varsayılsın. Bu durumda kullanılacak bölüm (st_{11}^k, st_{12}^k) olarak gösterilir. c_{11} ve c_{12} ile gösterilen örten piksel değerleri sırasıyla st_{11}^k ve st_{12}^k'nin kullanımı ile yeniden yapılandırılır. İlk örten piksel değerinin c_{11} yeniden elde edilmesi için gerçeklenen işlemler adımlar halinde verilecektir. Aynı işlemlerin uygulanması ile c_{12} değeri de benzer şekilde elde edilebilir. Aşağıda verilmiş olan algoritmada kullanılan (p_1, p_2) değerleri (2.20)'nin kullanımı ile elde edilmiştir.

1. O anki stego piksel için kontrol aralığı $[b_1, b_2]$'yi belirle.

$(st_{11}^k \le 3) \Rightarrow b_1 = 0, b_2 = st_{11}^k + 4$

$(st_{11}^k \ge 252) \Rightarrow b_1 = st_{11}^k - 4, b_2 = 255$

$(4 < st_{11}^k < 252) \Rightarrow b_1 = st_{11}^k - 4, b_2 = st_{11}^k + 4$

2. $b = b_1 \cdots b_2$ için aşağıdaki adımları tekrarla.

2.1. $b \bmod 9 = p_1$ eşitliğini kontrol et.

2.1.1. Eğer doğruysa yeniden yapılandırılan örten görüntüdeki piksel değeri c_{11}'i b olarak belirle.

2.1.2. Aksi takdirde adım 2'ye dön.

Yukarıda adımları verilen prosedür $[b_1, b_2]$ aralığındaki değerleri test ederek, modulo 9 tabanında p_1 kalanını veren değeri bulmaya çalışır. Aynı adımların st_{12}^k üzerinde p_2'nin yardımıyla uygulanması sonucu ise c_{12} değeri elde edilecektir. Sonuç olarak o anki stego blok için, örten blok değerleri yeniden hesaplanmış olur.

Yeniden yapılandırma algoritması, stego görüntüdeki her bölüme uygulanır. *S* vektörü, gizli piksel değerlerinin 17 tabanındaki gösterimini içerecek şekilde yapılandırılır. Vektör iki elemandan oluşan gruplar halinde değerlendirilir. Her grup karşılık düşen gizli piksel değerinin 17 tabanındaki temsilidir. Bu durumda gizli görüntünün ilk piksel değeri $(s_1 \cdot 17 + s_2)$'nin kullanımı ile hesaplanır.

Yeniden yapılandırma algoritmasının adımları aşağıdaki şekildedir.

1. Dağıtıcı *k* katılımcıdan *k* stego görüntüyü elde eder $\left(st^1, st^2, \cdots, st^k\right)$.

2. Her stego görüntü iki pikselden oluşan bölümlere ayrılır.

3. Stego görüntünün karşılık düşen bölümleri için aşağıdaki adımlar tekrarlanır.

3.1. (2.19)'un kullanımı ile stego görüntülerdeki karşılıklı bölümlerden $F(x_1), F(x_2), \cdots, F(x_k)$ ile gösterilen pay değerleri elde edilir.

3.2. Pay değerleri Lagrange'ın tekniği yardımıyla polinomun interpolasyonunda (2.20)'deki gibi kullanılır.

3.3. Polinomun ilk *k*-2 katsayısı *S* vektörünün karşılık düşen elemanlarını oluşturur. Son iki katsayı ise "ortaya çıkarma" prosedürü aracılığıyla örten piksel değerlerinin belirlenmesinde kullanılır.

4. Adım 3'te oluşturulan *S* vektörü iki elemandan oluşan gruplara ayrılır. Her grup $s_i \cdot 17 + s_{i+1}$ ifadesi yardımıyla o an karşılık düşen gizli görüntü piksel değerinin yapılandırılmasında kullanılır.

Paylaştırma algoritmasında verilen örnek, yeniden yapılandırma algoritmasının da işleyişini göstermek amacıyla kullanılacaktır. Stego piksel değerleri (191,198), (191,198), (194, 198), (193, 197) ve (191, 200) şeklindedir. Dağıtıcı tarafından yeniden yapılandırma esnasında herhangi 4 tanesi elde edilir.

Örnek. Stego görüntüler arasında (191, 198), (194, 198), (193, 197) ve (191, 200) değerleri seçilmiş olsun. Her stego görüntü sıralı iki piksel grupları şeklinde ayrılır. Pay değerleri (2.19)'un kullanımı ile elde edilir.

İkinci stego görüntü için pay değeri yerleştirme fonksiyonunun kullanımı ile $F(x_2) = f_e(191, 198) = (191 + 4 \cdot 198) \bmod 17 \equiv 14$ şeklinde hesaplanır. Diğer pay değerleri sırasıyla $F(x_3) = 0, F(x_4) = 12, F(x_5) = 5$ şeklinde elde edilir. Lagrange'ın interpolasyon tekniği kullanılarak polinom ifadesi $F(x) = \left(11 + 15x + 4x^2 + 1x^3\right) \bmod 17$ şeklinde oluşturulur. İlk iki katsayı *S* vektöründeki o anki elemanları tanımlar. Son iki katsayı (p_1, p_2) ise karşılık düşen örten piksel değerlerinin elde edilmesinde kullanılır. Herhangi bir stego görüntüden elde edilen grup, örten görüntü piksellerinin elde edilmesi için yeterli olur. İlk grubun kullanıldığı varsayılarak, ilk piksel değeri için kontrol aralığı $[187, 195]$ olarak belirlensin. İkinci stego piksel için belirlenen aralık $[194, 202]$ şeklinde olur. Her iki kontrol aralığı örten piksel değerlerinin elde edilmesinde kullanılır.

İlk kontrol aralığındaki sayılar modulo 9 tabanında sırasıyla $(7, 8, 0, 1, 2, 3, 4, 5, 6)$ kalanlarına sahiptir. p_1 değeri ise Shamir'in polinomunda 4 olarak belirlenmiştir. Bu aralıkta kalanı 4'e eşit olan sayı 193 olarak belirlenir. 193 sayısının modulo 9 tabanındaki kalanı 4'tür ve aynı zamanda karşılık düşen örten pikselin parlaklık değeridir. İkinci kontrol aralığı da ikinci örten piksel değerini ortaya çıkarmada kullanılır. İkinci aralıktaki sayılar sırasıyla modulo 9 tabanında $(5, 6, 7, 8, 0, 1, 2, 3, 4)$ kalanlarına sahiptir. Bu aralıktaki sayılar içerisinde modulo 9 tabanında p_2=1 kalanını veren sayı 199'dur. Bu nedenle karşılık düşen örten piksel parlaklık değeri 199 olarak belirlenir. *S* vektöründeki elemanlar kullanılarak ise $(11 \cdot 17 + 15) = 202$ gizli veri elde edilmektedir.

Çalışma kapsamında, gizli görüntü paylaşımı alanındaki önemli alt alanlardan biri olan, geri döndürülebilir gizli görüntü paylaşım şemalarına iyileştirme sağlanmıştır. [73]'teki çalışma örten görüntüleri parlaklık seviyelerinden bağımsız olarak kullanmaktadır. Yalnız üretmiş oldukları stego görüntülerin PSNR değerleri, örten görüntünün parlaklık değişiminden etkilenmektedir. Gri seviye örten görüntüler için stego görüntü PSNR değeri 43 dB civarında iken, bu değer siyah-beyaz görüntülerle 38 dB civarına düşmektedir. [74]'teki çalışma ise taşıma kapasitesini iyileştirmesine rağmen siyah-beyaz örten görüntüleri desteklememektedir. Gri seviye örten görüntüler için üretmiş olduğu stego görüntülerin PSNR değeri ise 40 dB civarındadır. Önermiş olduğumuz yöntemle beraber gri seviye ve siyah-beyaz örten görüntülerin kullanılması durumunda üretilecek olan stego görüntülerin PSNR değerlerinde iyileştirme sağlanmıştır. Yöntem paylaştırma esnasında EMD yöntemini ve modulo operatörünü kullanmaktadır. Gri seviye örten görüntüler için PSNR değeri 47 dB civarlarında hesaplanırken, siyah-beyaz görüntülerde bu değer 43 dB olarak elde edilmiştir. Böylece önerilen yöntemin literatürdeki diğer yöntemlere kıyasla daha yüksek PSNR değerlerine sahip olduğu söylenebilir.

2. 4. Adaptif Doğrulama Yeteneğine Sahip Gizli Görüntü Paylaşım Şeması

Gizli görüntü paylaşım şemalarında, pay görüntülerinin anlamlı örten görüntülere saklanması sonucu üretilen stego görüntülerde değişim olup olmadığı doğrulama bitleri aracılığıyla kontrol edilmektedir. Literatürde var olan yöntemler, saklanmak istenen gizli görüntünün büyüklüğüne bakmaksızın, her bir pay değerini örten görüntüdeki 2×2'lik

örten bloklara yerleştirmektedir. Örten bloklar aynı zamanda önceden belirlenen miktardaki doğrulama bitini de içerir. Gizli görüntü büyüklüğüne bağlı olarak örten görüntülerde kodlama esnasında hiç kullanılmayan bölgeler oluşabilmektedir. Eslami ve Ahmadabadi, 2011'deki çalışmalarında örten görüntünün bütün kapasitesinin, pay değerlerini ve doğrulama bitlerini saklayacak şekilde kullanılmasını önermiştir [68]. Örten blokların büyüklüğü, örten görüntü büyüklüğü ve gizli görüntü büyüklüğüne göre dinamik olarak belirlenmektedir. Aynı zamanda doğrulama amacıyla da dört bit kullandıkları için bozulmuş bir stego bloğu tespit edebilme olasılıklarını $15/16 \cong 0{,}93$ olarak rapor etmektedirler. Yalnız doğrulama bitlerinin üretimi esnasında kullanmış oldukları zincir yapısı önemli bir probleme sahiptir. Stego bloklardan birinin iletim esnasında bozulması durumunda, geriye kalan stego bloklar herhangi bir problem olmasa dahi doğrulanamamakta ve bozuk olarak değerlendirilmektedir. Buna paralel olarak stego bloklara karşılık düşen gizli piksel değerleri yapılandırılamamaktadır. Önerdikleri yöntemdeki diğer bir dezavantaj ise blok başına kullandıkları bit sayısının sabit olmasıdır. Blok büyüklüğüne bakmaksızın kullanılan doğrulama biti sayısı dört olarak kalmaktadır.

Tez kapsamında gerçekleştirilen çalışmada örten blok büyüklüğü arttıkça kullanılan doğrulama biti sayısını artırarak, doğrulama oranını iyileştiren yeni bir adaptif doğrulama yeteneğine sahip gizli görüntü paylaşım şeması önerilmiştir. Üretilen pay değerlerinin dinamik büyüklükteki bloklara yerleştirilmesi esnasında [152]'de önerilen 8 tabanındaki EMD metodu kullanılmıştır. Örten bloğun büyüklüğü paylaştırma algoritmasının doğrulama gücünü belirlemektedir. Küçük büyüklükteki bloklar için 4 doğrulama biti kullanılırken, bu değer blok boyu büyüdükçe artmaktadır. Yöntem işlem görmekte olan bloğun doğrulamasını, bir sonraki blokta yer alan doğrulama dizisi yardımıyla gerçekleştirmektedir. Böylece herhangi değiştirilmiş bir stego blok yalnızca kendisinden bir önceki bloğu etkilerken, kendinden sonraki blokların doğrulama prosedürünü engellemeyecektir. Örneğin üçüncü stego bloğun değişmiş olması durumunda, yalnızca ikinci ve üçüncü stego bloklar değişmiş olarak varsayılacaktır. Önerilen yöntem değişen stego bloktan sonraki tüm stego blokları sorunsuz bir şekilde doğrulayabilmektedir. Eslami'nin yönteminde ise bozulan bir stego bloktan sonraki tüm bloklarda doğrulama mekanizması çalışmamaktadır. Yöntem aynı zamanda blok büyüklüğün 8'den büyük olduğu tüm durumlarda 48 dB'den yüksek PSNR'ye sahip stego görüntüler üretmektedir. Algoritmanın detayları aşağıda verilmiştir.

Önerilen yöntem öncelikle gizli görüntüyü *n* pay görüntüsüne parçalamakta, ardından da *n* örten görüntü içerisine saklamaktadır. Gizli görüntü, *k*-1 dereceden ve $F(x)$ ile gösterilen Shamir'in polinomunu yapılandırmak için kullanılacak olan, *k* pikselden oluşan alt bölümlere ayrılmaktadır. Polinomun katılımcılarla ilişkilendirilmiş farklı x_i, $i = 1 \cdots n$ değerleri için üretmiş olduğu değerler pay bilgilerini oluşturur. O anki bloğa ilişkin üretilen pay değerleri ve bir önceki stego blok için hesaplanan doğrulama bitleri, karşılık düşen örten bloğa saklanmaktadır. Doğrulama bitleri, stego görüntülerde meydana gelen değişimlerin tespit edilebilmesini sağlamaktadır.

Gri seviye gizli görüntü *S*, $S = \left\{ s_{ij} \middle| s_{ij} \in [0-255], 1 \le i \le S_N, 1 \le j \le S_M \right\}$ ile gösterilsin. Gizli görüntü *k* pikselden oluşan alt gruplara ayrılmaktadır. İlk bölüm $(s_1, s_2, \cdots, s_k)$ kullanılarak oluşturulan (*k*-1) dereceden polinom ifadesi (2.21)'de verilmiştir.

$$F(x) = \left(s_1 + s_2 x + s_3 x^2 + \cdots + s_k x^{k-1}\right) \bmod 257 \tag{2.21}$$

8 bit gri seviye gizli görüntüdeki piksel değer aralığını kapsayabilen ilk asal sayı değeri 257 olduğu için Shamir'in polinom ifadesindeki taban değeri de 257 olarak seçilmiştir. Pay değerleri, polinomun farklı x_i değerleri için ürettiği değerler kullanılarak oluşturulur. Ardından üretilen pay değerleri $F(x_1), F(x_2), \cdots, F(x_n)$, (2.22) ile tanımlı *L* büyüklüğündeki örten bloklara kodlanmaktadır. Örten blok büyüklüğü *L*; gizli görüntü büyüklüğüne, örten görüntü büyüklüğüne ve eşik değerine bağlı olarak hesaplanır. (3, *n*) eşik şemasının seçilmesi durumunda $C_N \times C_M$ büyüklüğündeki bir örten görüntü için seçilecek olan örten blok büyüklüğünün $C_N \cdot C_M \ge 3 \cdot S_N \cdot S_M$ koşulunu sağlaması gerekir.

$$L = \left\lfloor (C_N \cdot C_M \cdot k) / (S_N \cdot S_M) \right\rfloor \tag{2.22}$$

Üretilen pay değerleri belirlenen örten blok büyüklüğüne bağlı olarak m_s tabanına çevrilmektedir. (2.23) ile verilen koşulu sağlayan en küçük m_s değeri seçilmelidir.

$$L-2 \geq 2\left\lceil \log_{m_S} 255 \right\rceil \quad , \quad m_S \in \{8,16\} \tag{2.23}$$

(2.23)'deki ifadenin yardımıyla *L*=6 değeri için seçilecek olan m_S değeri 16 olarak hesaplanır. Bu durumda pay değerleri 16 tabanına çevrilir ve örten bloğun $2 \cdot \lceil \log_{16} 255 \rceil = 4$ piksel değeri, EMD yardımıyla pay değerlerinin saklanması için kullanılır. Üretilen $[0-(m_s-1)]$ aralığındaki pay değerleri, $\left\lceil \log_{m_s} 255 \right\rceil$ adet sayı ile temsil edilir. Önerilen yöntem örten bloğun $2 \cdot \left\lceil \log_{m_s} 255 \right\rceil$ adet pikselini pay değerlerini saklamada kullanırken, geri kalan pikseller ise doğrulama değerini kodlamak için kullanılmaktadır.

Paylaştırma algoritması $F(x_1), F(x_2), \cdots, F(x_n)$ ile gösterilen pay değerlerini (2.23) tarafından belirlenen m_s tabanına çevirir. Pay değerini temsil etmekte kullanılan bir sayı örten blokta karşılık düşen iki veya üç ikili piksel değerine, değiştirilen EMD metodu yardımıyla kodlanır. Karşılık düşen pikseller üzerinde uygulanan yerleştirme fonksiyonu sonucunun pay değerini temsil eden sayıya karşı düşmesi durumunda herhangi bir değişim yapılmaz. Aksi takdirde örten bloktaki piksel değerleri, yerleştirme fonksiyonu sonucu pay sayısını verecek şekilde değiştirilecektir. Önerilen yöntem yerleştirme fonksiyonunda kullanılacak modulo değerini m_s olarak seçer. Örten görüntü *L* pikselden oluşan bloklara ayrılır. *k*'ıncı örten görüntü C^k'daki bloklar $C_1^k C_2^k \cdots C_{\lfloor C_N C_M / L \rfloor}^k$ ile gösterilmektedir. C_i^k bloğundaki pikseller $c_{i1}^k c_{i2}^k \cdots c_{iL}^k$ şeklinde verilsin. *k* ile gösterilen örten görüntüdeki *i* ile gösterilen grubun ilk iki piksel değerine $\left(c_{i1}^k, c_{i2}^k\right)$, pay sayısını saklamada kullanılacak olan yerleştirme fonksiyonu (2.24)'te verilmiştir. Yerleştirme fonksiyonunda kullanılacak olan değişim aralığı $[-a, a]$ ise, m_s'nin kullanımı ile (2.24)'teki şekilde belirlenmektedir.

$$\begin{aligned} f_e &= \left(c_{i1}^k + 3c_{i2}^k\right) \bmod m_s \\ m_s &= 8 \Rightarrow a = 1 \\ m_s &= 16 \Rightarrow a = 2 \end{aligned} \tag{2.24}$$

Üretilen pay değerleri $F(x_1), F(x_2), \cdots, F(x_n)$, m_s tabanına çevrilir. m_s tabanındaki pay değeri $F(x_k)$'nın gösterimi $\left(sd_1 \cdots sd_{\lceil \log_{m_S} 255 \rceil}\right)_{m_S}$ şeklindedir. *k*'ıncı örten görüntüde *i* ile

gösterilen gruptaki C_i^k karşılık düşen pikseller, (2.24) ile verilen yerleştirme fonksiyonun kullanımı ile değiştirilir. Pay değerinin m_s tabanındaki temsilindeki ilk sayı, örten bloğun ilk iki piksel değerine kodlanmaktadır. Aynı şekilde örten bloğun üçüncü ve dördüncü piksel değerleri, ikinci pay sayısını temsil etmekte kullanılacaktır.

Paylaştırma algoritması *i* ile gösterilen örten bloktaki ilk iki piksel için yerleştirme fonksiyonunu $f_e = \left(c_{i1}^k + 3c_{i2}^k\right) \bmod m_s$ hesaplar. Bu piksel değerleri $[-a, a]$ aralığı kullanılarak, yerleştirme fonksiyonu sonucu sd_1'i verecek şekilde değiştirilir. Değişimden sonra örten bloğa karşı düşen stego blok elde edilmektedir. Diğer pay sayıları olan (sd_2, sd_3) ise örten bloktaki sıralı ikili piksellere $\left(c_{i3}^k c_{i4}^k\right), \left(c_{i5}^k c_{i6}^k\right)$ kodlanmaktadır.

Yukarıda anlatılan adımların uygulanması ile o anki örten blok, pay değerinin m_s tabanındaki temsilini içerecek şekilde değiştirilir. Literatürdeki yöntemlerin çoğu pay değerini saklama esnasında basit LSB'ye yerleştirme teknikleri kullanmaktadır. Pay değerinin yerleştirilmesinin ardından, o anki blok için doğrulama bitleri hesaplanır ve önceden belirlenen pozisyonlara yerleştirilir. Önerilen yöntem pay değerini temsil eden sayıların kodlanması esnasında değiştirilmiş EMD yöntemini kullanmaktadır. EMD yöntemi ile kodlamanın gerçekleştirilmesi, örten bloktaki piksellerin kaç bitinin değişerek stego piksellerin oluştuğunun belirlenmesini olanaksız kılmaktadır. Önerilen yöntem o anki blokla ilişkili doğrulama bitlerinin yerleştirileceği pozisyonları belirlemekle ilgilenmeyecektir. Bu nedenle o anki bloğun doğrulama değeri, pay değerinin saklanmasının ardından hesaplanır ve bir sonraki bloğa yerleştirilir. Sonuç olarak her örten blok önceki bloğa ait doğrulama değerini içermektedir.

Doğrulama değerini taşıyacak piksel sayısı paylaştırma algoritması tarafından belirlenir. Pay değerini saklamada kullanılacak olan piksel sayısı, $CP_S = \lceil \log_{m_S} 255 \rceil$ ile gösterilsin. Doğrulama değerini kodlamada kullanılacak olan örten piksel sayısı ise CP_A olsun. CP_A değeri, örten blok büyüklüğü L ve CP_S'nin kullanımı ile (2.25)'teki gibi belirlenir. CP_A aynı zamanda, doğrulama değerinin dönüştürülecek olduğu taban değerini gösteren m_A'nın belirlenmesinde kullanılır.

$$\begin{aligned} CP_A &= \lfloor (L - 2 \cdot CP_S)/2 \rfloor = 1 \Rightarrow m_A = 16 \\ CP_A &= \lfloor (L - 2 \cdot CP_S)/2 \rfloor \geq 2 \Rightarrow m_A = 8 \end{aligned} \tag{2.25}$$

Paylaştırma algoritması, yöntemin doğrulama kabiliyetini L ve CP_A değerlerini kullanarak belirler. Önerilen yöntemin hesaplayacak olduğu doğrulama değeri $\left[0-\left(m_A{}^{(CP_A)}-1\right)\right]$ aralığındadır. Örten blok büyüklüğü arttıkça yöntemin doğrulama yeteneği iyileşir. Örten blok büyüklüğünün 10 olarak belirlenmesi durumunda doğrulama değeri 6 bit ile temsil edilmektedir. Örten blok büyüklüğünün 12 olması durumunda ise bu değer $[0-511]$ aralığında olacak yani doğrulama değeri 12 bit ile temsil edilecektir.

Paylaştırma algoritması o anki stego bloğun doğrulama değerini CP_A ve m_A değerlerini kullanarak hesaplar. k ile gösterilen stego görüntüdeki i'inci blok ST_i^k ile gösterilsin. Anahtarlı özüt fonksiyonu $H(\cdot)$ o anki blok üzerinde uygulanmaktadır. Özüt fonksiyonunun sonucu kendi içerisinde b bitlik değer üretecek şekilde (2.26) yardımıyla XOR'lanır.

$$R=\left\langle H\left(ST_i^k\right)\right\rangle_b,\quad b=\left\lceil \log_2 m_A^{CP_A}\right\rceil \tag{2.26}$$

R ile gösterilen o anki stego bloğun doğrulama değeri bir sonraki örten bloğa yerleştirilir. Doğrulama değeri m_A tabanı kullanılarak $r_1\cdots r_{CP_A}$ ile gösterilen doğrulama sayılarına dönüştürülmektedir. Değiştirilen EMD metodu doğrulama sayılarının gömülmesinde kullanılır. Her doğrulama sayısı örten bloğun sıralı ikili piksel değerlerine yerleştirilmektedir. Doğrulama sayısını yerleştirmede kullanılacak olan o anki örten piksel değerleri $\left(c^k_{i(j+2L-2)},c^k_{i(j+2L-1)}\right)$ olsun. Doğrulama sayılarını kodlamada kullanılacak olan ve (2.27) ile verilen yerleştirme fonksiyonunun faydalanacak olduğu modulo değeri m_A olarak seçilmektedir.

$$\begin{aligned} &f_e=\left(c^k_{i(j+2L-2)}+3c^k_{i(j+2L-1)}\right)\bmod m_A\\ &m_A=8\ \Rightarrow a=1\\ &m_A=16\Rightarrow a=2 \end{aligned} \tag{2.27}$$

Önerilen yöntem o anki blok için hesaplamış olduğu doğrulama değerini bir sonraki bloğa yerleştirir. Yeniden yapılandırma algoritması boyunca, bir stego blok kendinden sonraki blokta yer alan doğrulama değeri kullanılarak değerlendirilmektedir. Böyle bir doğrulama mekanizması yönteme adaptif doğrulama yeteneği kazandırmaktadır.

Eslami'nin metodu ise önceki bloktan yeniden yapılandırılan pay değerinin kullanımı ile o anki bloğu doğrular. Böylece değiştirilen bir bloğu yakalama olasılıklarının $1/4 \cdot 1/4 = 1/16$ olduğunu iddia etmektedirler. Her ne kadar yöntemleri diğer yöntemlere kıyasla geliştirilmiş bir doğrulama yeteneğine sahip olsa da bazı problemleri mevcuttur. Eğer önceki blokta herhangi bir değişim olduysa, o anki bloğun doğrulaması uygun bir şekilde yapılamayacak ve bu domino etkisi tüm blokları etkileyecektir. Böylece bozulan bir bloğun ardından gelen stego bloklar doğru bir şekilde yapılandırılamamakta ve gizli görüntü yeniden elde edilememektedir. Herhangi bir stego bloktaki bozulma geriye kalan tüm blokların reddedilmesine sebep olmaktadır. Önerilen yöntem ise blokları kendi içlerinde doğrulamakta ve yalnızca değiştirilen bloğu reddetmektedir. Bu da hatanın yayılmasına engel olmaktadır.

Adımları aşağıda gösterilen paylaştırma algoritmasının yalancı kod ifadesi Ek 6'da verilmektedir.

1. Aşağıda verilen adımlar $(N \cdot M)/k$ kere tekrarlanır.

1.1. Gizli görüntüde henüz işlem görmemiş k pikseli kullanarak bölüm bilgisini oluştur.

1.2. Elde edilen bölüm (2.21)'deki ifade yardımı ile polinomu oluşturmada kullanılır.

1.3. Polinom farklı x değerleri için değerlendirilerek pay değerlerinin $F(x_1) \cdots F(x_n)$ elde edilmesinde kullanılır.

1.4. $1 \le i \le n$ aralığı için aşağıdaki adımlar tekrarlanır.

1.4.1. O anki pay değeri $F(x_i)$, m_s tabanına çevrilir $\left(sd_1 \cdots sd_{\lceil \log_{m_S} 255 \rceil}\right)_{m_S}$.

1.4.2. i ile gösterilen örten görüntüdeki L pikselden oluşan j'inci blok elde edilir $\left(c_{j1}^i, c_{j2}^i, \cdots, c_{jL}^i\right)$.

1.4.3. Pay sayıları (2.24)'teki ifade kullanılarak örten bloğa yerleştirilir.

1.4.4. O anki blok için doğrulama değeri (2.26) ifadesi kullanılarak hesaplanır.

1.4.5. Hesaplanan doğrulama değerini m_A tabanına çevrilir.

1.4.6. j+1 ile gösterilen örten bloğun son $2 \cdot CP_A$ byte'ı doğrulama sayılarını yerleştirmek için kullanılır.

Gizli verinin n katılımcının arasında paylaştırılmasının ardından, herhangi k ya da daha fazla sayıda pay görüntüsünün bir araya gelmesi durumunda gizli görüntü yeniden yapılandırılabilir. Yeniden yapılandırma algoritması stego görüntüleri öncelikle bloklara

böler. O anki stego blok için hesaplanan doğrulama değeri, bir sonraki bloğa paylaştırma adımında yerleştirilmiş olan doğrulama değeri ile karşılaştırılır. Eğer elde edilen ve çıkartılan doğrulama değerleri eşit ise stego bloğun herhangi bir değişikliğe uğramadığı onaylanmaktadır. Aksi takdirde gizli görüntüde karşılık düşen k adet piksel değeri değiştirilmiş olarak işaretlenir. Stego bloğun doğrulanmasının ardından, bloğa yerleştirilmiş olan pay değeri elde edilir. Karşılıklı k stego bloktan (hepsinin doğrulanması durumunda) elde edilen pay değerleri, Lagrange'ın interpolasyonu yardımıyla Shamir'in polinomunun tahmin edilmesi için kullanılır. Üretilen polinomda yer alan k adet katsayı, gizli görüntünün karşılık düşen piksel parlaklık değerleridir.

k adet stego görüntü $ST^1, ST^2, \cdots, ST^k$ ile gösterilmiş olsun. Yeniden yapılandırma süresince stego görüntüler L adet pikselden oluşan gruplara ayrılmaktadır. $N \times M$ büyüklüğündeki bir stego görüntü için toplam $\lfloor NM/L \rfloor$ adet blok elde edilir. k ile gösterilen stego görüntüdeki bloklar $ST_1^k, ST_2^k, \cdots, ST_{\lfloor NM/L \rfloor}^k$ ile gösterilsin. Her stego blok L adet piksel değerine sahiptir. Yeniden yapılandırma algoritması o anki blok üzerinde doğrulama değerini hesaplayarak stego bloğu doğrulamaya çalışır. Esas doğrulama değeri ise paylaştırma algoritması esnasında bir sonraki stego bloğa yerleştirilmiştir. Bir sonraki stego bloğun son CP_A piksel değeri, o anki bloğun doğrulama değerini barındırır. k ile gösterilen stego görüntüdeki i-1'inci blok $st_{i-11}^k \cdots st_{i-1L}^k$ ile gösterilsin. i-1'inci blok için hesaplanan ve paylaştırma esnasında i'inci bloğa yerleştirilen doğrulama değeri (2.28)'in kullanımı ile hesaplanır.

$$a_{(i-1)t}^k = \left(st_{i(L-2CP_A+2(t-1)+1)}^k + 3 \cdot st_{i(L-2CP_A+2t)}^k \right) \bmod m_A \quad t = 1 \cdots CP_A \tag{2.28}$$

i-1'inci blok için elde edilen doğrulama değeri m_A tabanındadır ve $a_{(i-1)1}^k a_{(i-1)2}^k \cdots a_{(i-1)CP_A}^k$ ile temsil edilmektedir. Elde edilen sayılar kullanılarak onluk tabandaki doğrulama değeri (2.29)'un kullanımı ile ortaya çıkar.

$$A_{i-1} = a_{(i-1)1}^k \cdot m_A^{(CP_A-1)} + \cdots + a_{(i-1)CP_A}^k \tag{2.29}$$

Dağıtıcı aynı zamanda i-1'inci blok için doğrulama değerini bir kez daha (2.30) ifadesi yardımıyla hesaplar.

$$R_{i-1} = \left\langle H\left(ST_{i-1}^{k}\right)\right\rangle_{b}, \quad b = \left\lceil \log_2 m_A^{CP_A} \right\rceil \tag{2.30}$$

Eğer hesaplanan R_{i-1} değeri ile çıkartılan A_{i-1} değerleri eşit ise o anki stego blok doğrulanmış demektir. Aksi takdirde yeniden yapılandırılan gizli görüntüdeki karşılık düşen *k* adet piksel değeri bozuk olarak işaretlenir. Doğrulanmanın ardından stego bloğa yerleştirilmiş olan pay değeri elde edilir. *i*-1'inci stego bloğa yerleştirilmiş olan m_s tabanındaki pay sayıları (2.31)'in kullanımı ile elde edilir.

$$sd_{(i-1)t}^{k} = \left(st_{(i-1)(2(t-1)+1)}^{k} + 3 \cdot st_{(i-1)(2t)}^{k}\right) \bmod m_S \quad t = 1 \cdots CP_S \tag{2.31}$$

m_S tabanındaki pay sayıları onluk düzene (2.32)'deki şekilde dönüştürülür.

$$F\left(x_k\right) = sd_{(i-1)1}^{k} \cdot m_S^{(CP_S-1)} + \cdots + sd_{(i-1)t}^{k} \tag{2.32}$$

Diğer *k*-1 doğrulanmış stego bloktan elde edilen pay değerleri $F\left(x_1\right) \cdots F\left(x_{k-1}\right)$, Lagrange'ın interpolasyonunda kullanılarak polinom elde edilir. Yeniden yapılandırılan gizli görüntünün karşılık düşen *k* pikseli, belirlenen polinomun katsayı değerleridir. Yeniden yapılandırma algoritmasının adımları aşağıdaki şekilde verilmiştir.

1. Gizli görüntünün yeniden yapılandırılması için *k* adet stego görüntü elde edilir $ST^1, ST^2, \cdots, ST^k$.

2. Stego görüntüler *L* pikselden oluşan bloklara ayrılır.

3. Aşağıda verilen adımlar $1 \le i \le \lfloor NM/L \rfloor$ için tekrarlanır.

3.1. *k* stego görüntüden karşılık düşen *i*'inci stego bloklar elde edilir $ST_i^1, ST_i^2, \cdots, ST_i^k$.

3.2. Aşağıda verilen adımlar $1 \le j \le k$ için tekrarlanır.

3.2.1. Bir sonraki stego bloktan ST_{i+1}^{j} yerleştirilmiş olan doğrulama değeri (2.28) ve (2.29)'un kullanımı ile elde edilir.

3.2.2. ST_i^j için o anki doğrulama değeri (2.30) yardımıyla hesaplanır.

3.2.3. Eğer çıkartılan doğrulama değeri hesaplanan doğrulama değerine eşit ise 3.2.5'e dönülür.

3.2.4. Yeniden yapılandırılan gizli görüntüde karşılık düşen k adet piksel değeri değiştirilmiş olarak işaretlenir ve adım 3'e geri dönülür.

3.2.5. (2.31) ve (2.32)'nin kullanımı ile pay değeri $F(x_j)$ elde edilir.

3.3. Elde edilen pay değerleri üzerinde Lagrange'ın interpolasyonu uygulanarak Shamir'in polinom ifadesi elde edilir. Polinomun k adet katsayı değeri yeniden yapılandırılan görüntünün piksel parlaklık değerlerini oluşturur.

Bu çalışma kapsamında Eslami vd.'nin 2011'de önermiş olduğu çalışmada yer alan bazı problemler tespit edilmiş ve yeni bir adaptif doğrulama yeteneğine sahip gizli görüntü paylaşma şeması önerilmiştir. Eslami vd.'nin yöntemi doğrulama biti sayısını artırabilmek amacıyla zincir mekanizmasını kullanmaktadır [68]. Algoritmanın çalışma prensibi gereği, herhangi bir stego bloğun değiştirilmiş olması durumunda geri kalan stego bloklar doğrulanamamaktadır. Önerilen yöntem blok büyüklüğüne bağlı olarak yöntemin doğrulama yeteneğini adapte etmekte ve bozulan bir stego bloğun yalnız kendisini etkilemesini sağlamaktadır. Blok büyüklüğünün 8 ve daha fazla olması durumunda, üretilen stego görüntülerin PSNR değerlerinin 48 dB civarında olduğu gözlemlenmiştir.

2.5. Medikal Görüntü Örneğinde Bilgi Güvenliğinin Sağlanmasında Yeni Bir Yaklaşım

Ağ kullanımının giderek artması ile beraber medikal bilgilerin bilgisayarlar arasında transferi ve işlenmesi genel bir kullanım alanı bulmuştur. Medikal görüntüler ve hastalarla ilişkili kayıtlar; güvenilir depolama ve kolay erişilebilirlik açısından medikal veri tabanı sistemlerinde tutulmaktadır. Tele tanı koyma, tele konsültasyon gibi bazı medikal uygulamalar bilginin güvensiz bir ortam olan Internet üzerinden transferini gerektirmektedir. Medikal görüntülerin bütünlüğünün ve gizliliğinin korunması, hastaların medikal kayıtlarının yönetiminde karşılaşılan en büyük problemlerden biri olmuştur. Gizliliğin sağlanması, medikal görüntünün iletim esnasında doğrulanmamış kişiler tarafından görüntülenmesine engel olunmasını sağlayan bir servistir. Bütünlüğün korunması ise medikal görüntünün iletimi esnasında herhangi bir şekilde değiştirilmediğini garantileyecektir. Literatürde yer alan yöntemler medikal görüntü paylaşımındaki farklı gereksinimlerin (gizlilik, doğrulama, elektronik hasta kaydı saklama) üzerinde durmuş ve önerdikleri yöntemlerle problemleri ortadan kaldırmaya çalışmışlardır. Medikal görüntülerin güvenli paylaşımı için tanımlanacak olan bir metot bazı gereksinimleri

karşılayabilmelidir. Elektronik hasta kayıtları, depolama gereksinimlerini ve ağ genişliğini olumlu yönde kullanabilmek amacıyla medikal görüntüler içerisine saklanabilmeli, paylaşılan medikal görüntü doğal bir görüntü olarak gözükmeli ve kötü niyetli kişilerin ilgisini çekmemelidir. Siyasi liderlerin veya üst düzeydeki askeri yöneticilerin hastalıklarına teşhis koyulması esnasında, tüm medikal kayıtları tek bir kişinin görüntüleyebilmesine izin verilmemeli ve alıcı taraf kendisine gelen medikal görüntünün iletim esnasında değiştirilmediğini garantilemelidir.

Literatürdeki çalışmaların bazıları steganografiyi elektronik hasta kayıt bilgisini medikal görüntülerin içine saklamada kullanmıştır. Diğer bazı çalışmalar ise medikal görüntülerin gizliliğini sağlayabilmek amacıyla kriptografik yöntemlerden yararlanmaktadır. Medikal görüntülerin doğrulanması ise yine araştırmacılar tarafından damgalama yöntemlerinin kullanılmasıyla çözüm aranmaya çalışılan bir diğer problem olmuştur. Önerilen yöntem medikal görüntülerin ve elektronik hasta kayıtlarının iletimi için verilmiş olan gereksinimlerin tümünü sağlayan ve Shamir'in sır paylaşma şemasına dayandırılan yeni bir metottur.

Medikal görüntü güvenliğinin sağlanması alalında yapılan bazı çalışmalar, görüntünün bütünlüğünü ve gizliliğini sağlamak ve aynı zamanda elektronik hasta kaydını görüntüler içerisine saklayabilmek amacıyla damgalama yöntemlerinin kullanımını önermiştir [120-136]. Shih ve arkadaşları damga ve metin bilgisini medikal görüntünün ilgi alanının etrafına genetik algoritma kullanarak gömmüştür [120]. Woo ve arkadaşları ise çoklu damgalama yöntemini medikal görüntülerin bütünlüğünü doğrulayabilmek amacıyla kullanmıştır [121]. Zhou ve arkadaşları LSB'ye saklama tekniğini, üretmiş oldukları sayısal imzayı ve elektronik hasta kaydını saklamada kullanmıştır [122]. Aynı işaret görüntüsü içerisine farklı ebatlardaki hasta kayıt bilgisini saklayabilmek amacıyla yeni bir veri saklama yöntemi Chao ve arkadaşları tarafından önerilmiştir [123]. İşaret görüntüsü, hasta kaydının orijinini doğrulamak amacıyla, hastaneye ilişkin bir logo görüntüsü olabilir. Luo ve arkadaşlarının yöntemi, yüksek saklama oranı ve örten ortamı hatasız geri yapılandırabilme özellikleri ile diğer çalışmalardan farklılık göstermektedir [124]. Dalgacık dönüşümü ve çoklu damgalamaya dayanan bir diğer yaklaşım ise Giakoumaki ve arkadaşları tarafından önerilmiştir [125]. Doğrulama için doktorun sayısal imzası, hastanın kişisel bilgisi ve kırılgan damga aynı anda kullanılmıştır. Chen ve arkadaşları medikal görüntülerin bütünlüğünü koruma için medikal görüntünün ilgi bölgesi üzerinde MD5 fonksiyonu yardımıyla bir özet bilgi üretmiştir [126]. Elde edilen özet, hasta kayıt bilgisi

ile beraber medikal görüntünün ilgi dışı alanlarına gömülmüştür. Acharya ve arkadaşları ise hasta kayıt bilgisinin JPEG sıkıştırma esnasında medikal görüntüler içerisine serpiştirmesini gerçekleştirerek, depolama gereksinimlerinin iyileştirilmesini amaçlamıştır [124]. Nayak ve arkadaşları medikal görüntülerin hasta kayıt bilgileri ile beraber güvenli iletimini sağlayabilmek amacıyla hata düzeltme kodlarını kullanmıştır [128]. Hasta kayıt bilgisi hata düzeltme teknikleri ile beraber kodlanmış ve böylece iletim esnasındaki gürültü oluşumlarına dayanıklılığı sağlanmıştır. Srinivasan ve arkadaşları BPCS (Bit plane complexity segmentation, Bit düzleminde karmaşıklık ayrıştırması) steganografik yöntemini, hasta kayıtlarını renkli medikal görüntüler içerisine saklamada kullanmıştır [129]. Anand ve arkadaşları ise hasta kayıt dosyasını log fonksiyonu ile beraber şifrelemiş ve uzaysal domen steganografik yöntem kullanarak medikal görüntüye gömmüşlerdir [130]. Önerdikleri teknik, hızlı koşma zamanı ile acil tanı gerektiren durumlarda kullanım açısından etkindir.

Coatrieux vd. yapmış olduğu çalışmada medikal görüntü güvenliğinde damgalamanın tamamlayıcı rolünü incelemiştir [131]. Çalışmalarında medikal bilgi sistemleri arasında izlenebilirliğin ve doğrulamanın damgalama yöntemleri ile gerçekleştirilebileceğini göstermiştir. [132]'deki çalışmada bilginin doğru hastaya ait olduğunun ve doğru kaynaktan çıktığının ispatının medikal görüntü güvenliği alanındaki iki büyük problem olduğunu ortaya koymuştur. Navas vd. 2008 yılındaki çalışmasında dalgacık dönüşümü tabanlı geri döndürülebilir bir steganografik yöntemle medikal görüntü güvenliğini sağlamıştır [133]. Hasta kaydının şifrelemesini yaparak daha ileri bir güvenlik mekanizması sağlamaya çalışmışlardır. Acharya vd. hasta bilgisini medikal görüntülerle serpiştirerek depolama açısından iyileştirme sağlamayı amaçlamıştır [134]. Grafiksel sinyaller medikal görüntüyle serpiştirilmiştir. Kallel vd. önermiş olduğu projede pratisyenlerin erken teşhis koyabilmek amacıyla tele komünikasyon teknolojilerini kullanabileceğini ortaya koymuştur [135]. Bütünlük doğrulama kontrolü için geri döndürülebilir steganografiyi kullanmışlar ve saklama işleminden sonra medikal görüntünün kalitesini değerlendirmişlerdir. Memon vd. önermiş olduğu yöntemde damga bilgisini ilgi alanı dışındaki bölgelere gömmüştür [136]. Gömülecek olan bilgi aynı zamanda önceden şifrelenmiştir. Hu vd. yapmış olduğu çalışmada yeni bir e-sağlık güvenlik alt yapısı önermiştir [137]. Oturum tabanlı bir mekanizma yerine kontrat uyumlu bir mekanizmanın kullanılabileceğini göstermiştir. Damgalamadan farklı olarak medikal görüntülerin iletiminde son yıllarda yapılan çalışmalarda steganografi ve kriptografi de

kullanılmaktadır. Steganografi hasta kayıt bilgisini medikal görüntü içerisine saklarken, kriptografi medikal görüntülerin gizliliğini sağlar [129, 138-142]. Lou ve arkadaşları uzaysal domendeki çok katmanlı veri gizleme yöntemini, hasta kayıt bilgisini medikal görüntü içerisine saklamak için önermişlerdir [141]. Hu ve arkadaşları ise piksel tabanlı ve kaotik şifrelemeye dayanan bir yöntemle medikal görüntünün gizliliğini sağlamaya çalışmışlardır [142]. Önerdikleri yöntem, medikal görüntüyü gürültü benzeri şifreli görüntüye çevirmektedir. Medikal görüntülerin güvenliğinin sağlanmasında, güvenli depolama ve ağ üzerinden iletimi iki önemli husustur. Bununla birlikte, alıcı taraf hastaya ait bilgiyi kopyalayabilir ve hastanın izni dışında dağıtabilir. Siyasi bir lider ya da askeri bir kişinin medikal bilgisinin bu şekilde yayılması ülke politikaları açısından önemli problemlere sebep olabilir. Li ve arkadaşları böyle bir probleme yapmış oldukları çalışmada vurgu yapmışlardır [140]. Medikal görüntü tanılamada kullanılmadan önce, klinisyen kendi damga anahtarını kullanarak görüntüyü deşifrelemelidir. Damga anahtarları önceden üçüncü bir kurum tarafından dağıtılmak zorundadır. Fakat önermiş oldukları yöntem hasta kayıt bilgisinin saklanmasına ilişkin herhangi bir işlem yapmamaktadır.

Bahsi geçen yöntemler farklı gereksinimler için tasarlanmıştır. Lou vd. steganografi ile hasta kayıt bilgilerini medikal görüntüler içerisine saklamıştır [141]. Bütünlüğün doğrulanması ve medikal görüntülerin gizliliği, çalışmalarında değerlendirilmemiştir. Hu, medikal görüntüyü kriptografik yöntemler yardımıyla gürültü benzeri bir görüntüye çevirmiş ve gizliliği sağlamıştır. Fakat, hasta kayıt bilgisinin saklanması değerlendirilmediği gibi, gürültü benzeri görüntülerin kötü niyetli kişilerin ilgisini çekeceği konusuna vurgu yapılmamıştır. Li çalışmasında, medikal görüntülerin izinsiz dağıtılması problemi üzerinde durmuştur [140]. Fakat önerdikleri yöntemde kullanılan genel görüntü, medikal bir görüntünün iletilmeye çalışıldığını ortaya koymaktadır. Aynı zamanda hasta kayıt bilgisinin saklanması yaptıkları çalışmada değerlendirilmemiştir. 2005 yılında, Ho ve arkadaşları medikal görüntüleri doğrulamada nazik damgalama yöntemi kullanmıştır [138]. Üretilen damgalanmış medikal görüntü düşük PSNR değerine sahiptir ve hasta kayıt bilgisinin saklanması hesaba katılmamıştır. Nayak ve arkadaşları geri döndürülebilir steganografiyi hasta kayıt bilgilerini saklamada kullanmıştır [139]. Fakat önermiş oldukları yöntem, medikal görüntülerin gizliliğini ve doğrulamasını gerçekleştirmemektedir. Bunun yanında gömebildikleri karakter miktarı da sınırlıdır. Önermiş olduğumuz yöntem kullanılarak, medikal görüntülerin *n* kişinin arasında paylaştırılması gerçekleştirilmiştir.

Üretilen pay görüntüleri steganografi kullanılarak anlamlı görüntüler içerisine saklanmıştır. Aynı zamanda hasta kayıt bilgisi de Shamir'in polinomundaki katsayılar kullanılarak pay görüntülerinin içerisine yerleştirilmiştir. Herhangi k tane doktorun bir araya gelmesi sonucu gizli medikal görüntü ve hasta kayıt bilgisi yeniden yapılandırılabilmektedir. Tez kapsamında, literatürdeki çalışmalardan farklı olarak, giriş bölümünde verilmiş olan gereksinimlerin hepsini aynı anda sağlayabilen yeni bir medikal görüntü paylaşma metodu önerilmektedir [147]. Önerilen yöntem "Parçalama" ve "Ortaya Çıkarma" olarak adlandırılan iki alt algoritmadan oluşmaktadır. Parçalama algoritması kendi içerisinde 4 prosedürü barındırmaktadır. "İlk değer verme" olarak adlandırılan ilk prosedür, katılımcılarla ilişkilendirilecek olan x değerlerinin belirlenmesini sağlar. Böylece, her bir katılımcıya özgü x değerinin belirlenmesi ve güvenli olmayan bir ağ üzerinden iletilmesi gibi problemlerden kaçınılmış olunur. "Paylaştırma" olarak adlandırılan ikinci prosedür, medikal görüntüyü ve hasta kayıt bilgisini pay görüntülerine ayırır. Saklanabilecek hasta kayıt bilgisinin uzunluğu, seçilen medikal görüntünün bit derinliğine ve büyüklüğüne bağlıdır. Paylaştırma adımında Shamir'in yöntemi kullanıldığı için, pay görüntüleri gürültüye benzerdir. Bu nedenle, "Saklama" olarak adlandırılan üçüncü prosedür, üretilen pay görüntülerini OPAP tekniğini kullanarak örten görüntülere saklar. "Koruma" olarak adlandırılan dördüncü prosedür ise her bir katılımcı için sertifika üretecektir.

Herhangi k ya da daha fazla sayıdaki doktorun kendilerindeki pay görüntülerini birleştirmesi sonucu, medikal görüntü ve hasta kayıt bilgisi yeniden yapılandırılabilir. "Ortaya Çıkarma" algoritması iki alt prosedürden oluşur: "Doğrulama" ve "Yeniden Yapılandırma". Doğrulama prosedürü, pay görüntülerinin bütünlüğünü kontrol eder. Doğrulama prosedürünün, pay görüntülerini onaylamasının ardından, "Yeniden Yapılandırma" prosedürü Lagrange kullanarak medikal görüntüyü ve hasta kayıt bilgilerini ortaya çıkarır.

2.5.1. Parçalama Algoritması

Parçalama algoritması dört alt prosedürden oluşur: "İlk değer verme", "Paylaştırma", "Saklama", "Koruma". Alt prosedürlerin gerçekleştirme adımları detayları ile beraber verilmiştir.

2.5.1.1. İlk Değer Verme Prosedürü

"Paylaştırma" prosedüründe kullanılacak olan Shamir'in paylaştırma algoritması, dağıtıcı ve katılımcılar arasında pay görüntülerin transferinden önce bazı haberleşmeler gerektirir [83]. Dağıtıcı, her katılımcıya özgü ve farklı bir x değeri belirlemek zorundadır. Dağıtıcı ve katılımcılar arasında x değerlerinin paylaşılabilmesi için güvenli bir ağ ortamına ihtiyaç vardır. Zhao ve arkadaşları 2009'da yapmış oldukları çalışmada, dağıtıcı ve katılımcılar arasındaki güvenli olmayan ağ için bir metot önermişlerdir [83]. Katılımcılar kendilerine özgü "Sır" olarak adlandırılan gizli bir değer seçer. Her katılımcı yalnızca kendi sırrını bilir ve diğer katılımcıların sırları hakkında herhangi bir bilgi elde edememelidir. Sır değerleri dağıtıcı tarafından doğrudan olmayan bir yolla x değerlerinin belirlenmesinde kullanılır. Eğer sistem, sır değerlerinin gizliliğini sağlarsa, aynı zamanda üretilen x değerlerinin de güvenilirliğini sağlamış demektir. Kötü niyetli bir kullanıcı herhangi k tane pay görüntüsünü toplamış olsa bile, Lagrange'ın interpolasyonunu kullanabilmek için aynı zamanda görüntülerle ilişkili x değerlerini de bilmelidir. Aksi takdirde, interpolasyon yöntemi gizli medikal görüntüyü elde etmede kullanılamayacaktır. Lagrange'ın yöntemi, polinomu tahmin edebilmek için x değerlerini de gerektirir fakat pay görüntüleri yalnızca F(x) değerlerini içerir.

Zhao'nun metodu aynı zamanda katılımcılarla ilişkilendirilmiş x değerlerinin biricik olduğunu ve yalnızca dağıtıcı tarafından bilindiğini garantiler. x değerlerinin her katılımcı için ayrı olması, pay görüntülerinin de birbirinden farklı olacağının ispatıdır. Önerilen yöntem iki sebepten dolayı Zhao'nun metodunu kullanmaktadır. İlk sebep, her katılımcıya özgü bir x değeri oluşturabilmektir. İkinci olarak, katılımcılar tarafından seçilen rasgele değerler güvensiz ağ ortamı üzerinden iletilir. Fakat x değerleri katılımcı ve dağıtıcı taraflarında yeniden hesaplanır. Böylece ağ üzerinden x değerlerinin iletimi problemi ortadan kaldırılmış olacaktır. Kötü niyetli bir kullanıcı elde ettiği k adet pay görüntüsü ile beraber gizli görüntüyü yeniden yapılandırabilmesi için aynı zamanda x değerlerine de ihtiyacı vardır. "İlk Değer Verme" prosedürüne ilişkin detaylar aşağıdaki şekildedir.

- Dağıtıcı *D, p* ve *q* olarak adlandırılan ve $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$ koşullarını sağlayan iki büyük asal sayı belirler. Ardından N değerini $N = pq$ olarak belirler.
- D, p ve q ile aralarında asal olan bir g sayısı seçer, $g \in \left[N^{1/2}, N\right]$. D belirlemiş olduğu $\{g, N\}$değerlerini genel olarak duyurur.

- Her bir katılımcı kendine ait bir sır değeri belirler, $s_i \in [2, N]$. Ardından $R_i = g^{s_i} \bmod N$ değerini hesaplar.
- Her katılımcı bir önceki adımda hesaplamış olduğu R_i değerini *D*'ye gönderir. *D*, katılımcılardan gelen herhangi iki değerin aynı olmadığından emin olmalıdır $R_i \neq R_j$. Aksi takdirde ilgili katılımcıların yeni bir sır değerini seçmesini ister.
- *D*, $s_0 \in [2, N]$ koşulunu sağlayacak şekilde rasgele bir sır değeri belirler. Bu değer $(p-1)$ ve $(q-1)$ değerleri ile aralarında asal olmak zorundadır. Ardından $R_0 = g^{s_0} \bmod N$ değerini hesaplayarak genel olarak yayınlar.
- *D,* her katılımcı için $x_i = R_i^{s_0} \bmod N, \quad i = 1, 2, \cdots, N$ değerini hesaplar.

Bütün katılımcılar kendilerine ait bir sır değeri belirler s_i ve adım 3'de kendi sır değerlerini kullanarak R_i değerini hesaplarlar. Dağıtıcı, altıncı adımda R_i değerlerini kullanarak her katılımcı için bir *x* değeri hesaplar. Katılımcı, dağıtıcının kendisi ile ilişkilendirmiş olduğu *x* değerini, kendi sır değerini ve genel olarak bilinen R_0 değerini kullanarak hesaplayabilir $x_i = R_0^{s_i} \bmod N$. Böylece, yöntem *x* değerlerini güvensiz bir kanal üzerinden iletmeden her iki tarafta ayrı olarak hesaplanmasını olanaklı kılar. Aynı zamanda *D* dördüncü adımda her katılımcı için ayrı bir pay görüntüsü oluşturulacağını garanti eder. "İlk Değer Verme" prosedürü, yöntemin aşağıda verilmiş olan özellikleri kazanmasını sağlayacaktır.

- Biricik *x* değerlerinin kullanılmasıyla biricik pay görüntüleri oluşturulmaktadır.
- Paylaştırma prosedüründen önce *x* değerleri, taraflar arasında güvensiz bir ağ bağlantısı kullanılmadan hesaplanmaktadır.
- Kötü niyetli bir kişi ağ üzerinden *k* adet pay görüntüsünü elde etse bile gizli görüntüyü, *x* değerlerini bilmediği için yeniden yapılandıramaz.

2.5.1.2. Paylaştırma Prosedürü

Medikal görüntü ve elektronik hasta kaydı bu prosedürde katılımcılar arasında paylaştırılmaktadır. Doğal görüntülü pay görüntüleri, medikal görüntü ve elektronik hasta kayıtlarının gizliliğini sağlayacaktır. Metot aynı zamanda yerleşik doğrulama kabiliyetine sahiptir. Medikal görüntü ve hasta kaydı, herhangi *k* görüntüde bir bozulma olması

durumunda yeniden yapılandırılamaz. Literatürdeki önceki çalışmalar; gizlilik, bütünlük ve "hasta kayıt saklama" gibi medikal görüntülerin iletimindeki istenilen özellikleri bir arada sağlayamazken, önerilen yöntemle tüm bu hedefler tek bir yerde sağlanabilmiştir.

W×*H* büyüklüğündeki *b*-bit derinliğindeki (2^b gri seviye göstermektedir) medikal görüntü M ile gösterilsin $M = \left\{ m_i \middle| m_i \in \left[0 - \left(2^b - 1\right)\right], i = 1, 2, \cdots, W \times H \right\}$. Medikal görüntüdeki bütün piksel değerleri 251 tabanına çevrilir. Çünkü Shamir'in polinomunda kullanılacak olan asal değer 251 olarak seçilecektir. Medikal görüntü, paylaştırma algoritması tarafından piksel piksel işlem görür.

Varsayalım ki medikal görüntü *M*'de o an işlem görecek olan piksel m_i ile elektronik hasta kayıt bilgisi $E = \left\{ e_i \middle| e_i \in [0, 251), i = 1, 2, \cdots, L \right\}$ ile gösterilsin. Elektronik hasta kayıt bilgisinin uzunluğunun *L* olduğu ve kayıttaki her bir eleman ASCII bir karaktere karşılık düştüğü kabul edilmiştir. Medikal görüntüdeki her bir piksel değeri pay görüntülerindeki bir piksele karşı düşmektedir. Böylece pay görüntüleri ile medikal görüntülerinin büyüklüklerinin eşit olduğu söylenebilir. (2.33)'te verilen *(k*-1*)* dereceden polinom medikal görüntü piksel değeri m_i için pay değerlerinin belirlenmesinde kullanılır. Medikal görüntünün her bir piksel değeri 251 tabanına çevrilir. *b* bit derinliğindeki piksel değerinin 251 tabanındaki gösterimi $\left(m_{i1}, m_{i2}, \cdots, m_{i\left\lceil \log_{251} 2^b \right\rceil} \right)$ şeklindedir. Shamir'in iki veya daha fazla sayıdaki katsayısı, bit derinliğine bağlı olarak, medikal görüntü piksel değeri olan m_i değerini temsil edecektir. Polinomun ilk iki katsayısı en azından 8-bit, 10-bit veya 12-bit derinliğindeki tıbbi görüntüleri temsil etmek için yeterli olacaktır. *b* bit derinliğindeki medikal bir görüntünün piksellerini temsil etmek için $\left(\left\lceil \log_{251} 2^b \right\rceil\right)$ sayıda katsayı yeterli olacaktır. Başka bir deyişle, medikal görüntünün piksel derinliği aynı zamanda kullanılacak olan eşik değeri *k*'yıda belirleyecektir $k > \left\lceil \log_{251} 2^b \right\rceil$ .Shamir'in polinomu, 12 bit derinlikteki gizli medikal görüntünün paylaştırılması için (2.33)'teki gibi yapılandırılır.

$$F(x) = \left(m_{i1} + m_{i2} x + e_i x^2 + e_{i+1} x^3 + \cdots + e_{i+k-3} x^{k-1} \right) \bmod 251 \qquad (2.33)$$

Medikal görüntüden alınan bir piksel değeri ve elektronik hasta kaydı polinomun katsayıları olarak kullanılır $\left(m_{i1}, m_{i2}, e_i, e_{i+1}, \cdots, e_{i+k-3} \right)$. Medikal görüntünün 12 bit

derinlikte olduğu düşünülürse, polinomun ilk iki katsayısı piksel değerini kodlamada kullanılacaktır. Algoritma ilk prosedürden elde edilen farklı *x* değerlerini kullanarak polinomu hesaplar ve *n* tane $(x_i, F(x_i))$ çifti elde eder. $F(x_i)$ değeri, *i* ile gösterilen pay görüntüsündeki karşılık düşen parlaklık değeridir. Her katılımcı yeniden yapılandırma aşamasında kendisine karşı düşen *x* değerini tekrar hesaplayacaktır. Medikal görüntünün bütün piksel değerleri ve aynı zamanda hasta kaydındaki karakter değerleri, pay görüntülerinin oluşturulması esnasında kullanılmıştır. Pay görüntülerinin gizliliği bir sonraki prosedürde steganografi kullanılarak sağlanacaktır.

2.5.1.3. Saklama Prosedürü

Steganografi pay görüntülerini anlamlı örten görüntüler içerisine saklamak için kullanılır. Dağıtıcı (*k*, *n*) eşik şeması için *n* adet doğal görünümlü $2W \times 2H$ ebatlarında örten görüntü seçer. Saklama işlemi esnasında pay görüntüleri piksel düzeyinde işlem görmektedir. *i* inci pay görüntüsündeki pikseller (2.34) ile gösterilsin.

$$SH^i = \left\{ sh_j^i \middle| j = 1, 2, \cdots, W \times H, sh_j^i \in [0,251) \right\} \tag{2.34}$$

*i'*inci pay görüntüsünü saklamada kullanılacak olan örten görüntü C^i ile gösterilsin. Pay görüntüsündeki piksel değerleri, örten görüntüde karşılık düşen 2×2 büyüklüğündeki örten blok olarak adlandırılan piksellere saklanır. Böylece bloktaki piksellerin son iki bit değerleri pay değerlerini taşımada kullanılır. Önerilen yöntem stego görüntülerdeki bozulmayı azaltmak amacıyla, saklama işlemi esnasında OPAP yöntemini kullanmaktadır [9]. Varsayalım ki *i*'inci örten görüntüdeki *j*'inci piksel için karşılık düşen örten blok C_j^i olsun. Karşılık düşen bloktaki 4 piksel değeri sırasıyla (a, b, c, d) ile gösterilsin. Önerilen yöntem sh_j^i değerini sırasıyla (a, b, c, d) piksellerini OPAP'ı kullanarak saklamaktadır. Metot öncelikle sh_j^i değerini 2 bit'ten oluşan dört parçaya ayırır. Ardından her iki bitlik değeri karşılık düşen piksel değerine saklar. Yerleştirme işleminin ardından oluşan yeni bloktaki piksel değerleri (a', b', c', d') ile gösterilsin. Örten bloktaki pikseller için, $(\delta_a, \delta_b, \delta_c, \delta_d)$ ile gösterilen saklama hatası (2.35)'in kullanımıyla hesaplanır.

$$\delta_a = a' - a,\ \delta_b = b' - b,\ \delta_c = c' - c,\ \delta_d = d' - d \tag{2.35}$$

a ile gösterilen piksel için saklama hatası (2.36) ile verilen aralıklardan birine düşmektedir.

$$\begin{aligned} &2^{2-1} < \delta_a < 2^2 \\ &-2^{2-1} \le \delta_a \le 2^{2-1} \\ &-2^2 < \delta_a < -2^{2-1} \end{aligned} \tag{2.36}$$

OPAP, a' değerini aralığa bağlı olarak değiştirir ve yeni a'' değerini (2.37)'deki gibi elde eder.

$$\begin{aligned} &\left(2^{2-1} < \delta_a < 2^2\right) \wedge \left(a' \ge 2^2\right) \ \Rightarrow\ a'' = a' - 2^2 \\ &\left(2^{2-1} < \delta_a < 2^2\right) \wedge \sim \left(a' \ge 2^2\right) \ \Rightarrow\ a'' = a' \\ &\left(-2^{2-1} \le \delta_a \le 2^{2-1}\right) \ \Rightarrow\ a'' = a' \\ &\left(-2^2 < \delta_a < -2^{2-1}\right) \wedge \left(a' < 256 - 2^2\right) \ \Rightarrow\ a'' = a' + 2^2 \\ &\left(-2^2 < \delta_a < -2^{2-1}\right) \wedge \sim \left(a' < 256 - 2^2\right) \ \Rightarrow\ a'' = a' \end{aligned} \tag{2.37}$$

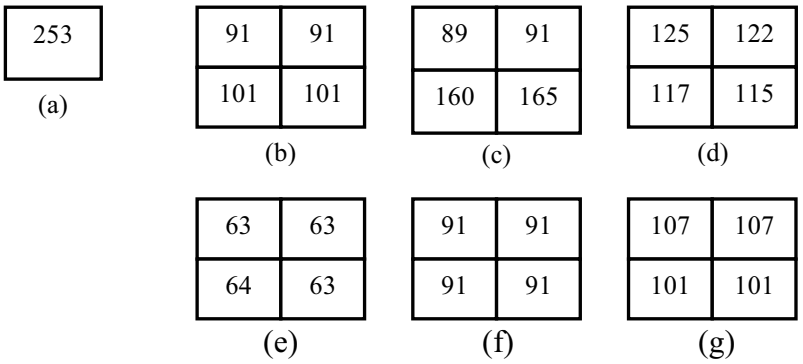
*a'*nın yeni değeri OPAP'ın kullanımıyla a'' olarak değiştirilir. Örten bloktaki diğer piksellerde, yukarıda verilen prosedür kullanılarak, stego piksellere dönüştürülür. *i*'inci pay görüntüsündeki piksel değeri, *i*'inci örten görüntüde karşılık düşen örten blok içerisine saklanır ve doğal görünümlü stego görüntüler elde edilir. Paylaştırılan medikal görüntü en az *k* tane doktorun bir araya gelmesi sonucu yeniden yapılandırılabilecektir. Paylaştırma ve saklama prosedürlerinin yalancı kod şeklinde gösterimi Ek 7'de verilmektedir.

Örnek. (*k, n*) = (4, 6) olarak kabul edilsin. Şekil 2.6(a) ve Şekil 2.6(b)-2.6(g) 8 bit derinlikteki gizli görüntünün piksel değerlerini ve karşılık düşen 6 adet örten görüntüdeki piksel değerlerini vermektedir. Elektronik hasta kaydından alınan bir kısım bilgi "disease" şeklinde olsun. Bu durumda Shamir'in polinomu gizli piksel değeri 253 için (2.38)'daki gibi yapılandırılacaktır.

$$F(x) = \left(1 + 2x + 100x^2 + 105x^3\right) \bmod 251 \tag{2.38}$$

Polinomun ilk iki katsayısı 253 parlaklık değerine sahip gizli görüntü pikselini temsil eder. Diğer iki katsayı ise hasta kaydındaki karşılık düşen karakterler olan ‘d’ ve ‘i’ yi temsil etmektedir. İlk değer verme prosedüründe x_i değerlerinin (2.39)’daki gibi belirlendiği varsayılsın.

$$X = \{x_i = i | i = 1, 2, \cdots, n\} \tag{2.39}$$



Şekil 2.6(a) Gizli piksel değeri (b)-(g) Altı örten blok piksel değerleri

Paylaştırma prosedürü $F(x_i)$ değerlerini sırasıyla 208, 241, 228, 46, 74 ve 189 olarak hesaplar. Ardından saklama prosedürü hesaplanan pay değerlerini örten bloklara OPAP yöntemini kullanarak yerleştirmek için kullanılacaktır. Saklama prosedürünün adımları ilk örten blok için anlatılacak olsa da diğer x_i değerleri için uygulanacak olan adımlar aynıdır. İlk pay değeri olan 208’in ikili temsili $(11010000)_2$ şeklindedir. Birinci örten bloktaki dört pikselin son iki bitleri pay değerini taşıyacak şekilde LSB kodlama ile değiştirilir. Saklama işleminin ardından (a', b', c', d') ile gösterilen örten bloğun yeni piksel değerleri (91, 89, 100, 100) şeklinde olur. Örten bloktaki pikseller için $(\delta_a, \delta_b, \delta_c, \delta_d)$ ile gösterilen saklama hataları (0, -2, -1, -1) olarak hesaplanır. (2.37)’de verilen kurallar göz önüne alındığında, örten bloğun yeni piksel parlaklık değerleri (91, 89, 100, 100) şeklindedir. Böylece gizli görüntü piksel değeri ve elektronik hasta kayıt karakterleri ilgili örten bloktaki dört adet piksel değerine saklanmıştır. Hasta kaydındaki geriye kalan beş karakter, o anki örten bloğu takip eden diğer üç örten bloğa kodlanır.

2.5.1.4. Koruma Prosedürü

Parçalama algoritmasının son prosedürü olan "Koruma", pay doğrulamayı sağlamak amacıyla kullanılmaktadır. Dağıtıcı [73]'teki çalışmaya benzer olarak bütün katılımcılar için bir sertifika oluşturur. Sertifikalar, pay görüntülerinde bir değişim olup olmadığının tespiti için kullanılmaktadır. 128 bit çıkışı olan MD5 özüt fonksiyonu, pay görüntülerindeki değişimi tespit edebilmek amacıyla kullanılır. Karşılık düşen x değerleri ile birleştirilmiş olan pay görüntüleri özüt fonksiyonunun girişini oluşturur. "Koruma" prosedürü KK yaklaşımını kullanmaktadır. İlk prosedürde seçilmiş olan N değerinden aynı zamanda bu aşamada da faydalanılır. a sayısı n tabanında herhangi bir sayının karesine denk ise, a sayısı n tabanında KK'dır denir ve $x^2 \equiv a \pmod{n}$ ile gösterilir. Aksi takdirde a sayısı n tabanında kuadratik kalan değildir (KKO) denir. Bu tanımdan faydalanarak, N sayısı iki asal sayının çarpımı olduğu için, a sayısı için aşağıda verilen dört durum söz konusudur.

Durum 1. a sayısı, p ve q tabanında KK'dır.

Durum 2. a sayısı p tabanında KK, fakat q tabanında KKO'dır.

Durum 3. a sayısı p tabanında KKO iken q tabanında KK'dır.

Durum 4. a hem p hem de q tabanında KKO'dır.

KKp ve KKOp, sırasıyla p tabanındaki kuadratik rezidü olan ve olmayan sayıların kümesini göstersin. (2.40)'ta verilmiş olan ve $(\alpha, \beta, \gamma, \delta)$ ile gösterilen dört parametre değeri, herhangi bir sayıyı, hem p hem de q tabanında KK yapabilmek için kullanılacaktır.

$$\begin{array}{ll} \alpha \in KKp \cap KKq & \beta \in KKp \cap KKOq \\ \gamma \in KKOp \cap KKq & \delta \in KKOp \cap KKOq \end{array} \tag{2.40}$$

a ile gösterilen herhangi bir değer, $(\alpha, \beta, \gamma, \delta)$ parametrelerinden uygun olanı ile çarpılarak hem p hem de q tabanında KK yapılabilir. Eğer a sayısı her iki tabanda KK ise, aynı zamanda N tabanında da KK olacaktır. Koruma prosedüründe kullanılan adımlar aşağıdaki şekilde verilmiştir.

- Dağıtıcı (2.40)'ı kullanarak $(\alpha, \beta, \gamma, \delta)$ değerlerini üretir. Ardından $(\alpha^{-1}, \beta^{-1}, \gamma^{-1}, \delta^{-1}, N)$ değerlerini genel olarak yayınlar.

- Dağıtıcı, $k = 1, 2, \cdots, n$ için $h_k = H\left(ST^k \| x_k\right)$ değerlerini MD5 fonksiyonunu kullanarak hesaplar.
- Dağıtıcı (2.41)'i kullanarak h'_k değerini hesaplar.

$$h'_k = \begin{cases} h_k \times \alpha, & id_k = 1 \quad \forall h_k \in KKp \cap KKq \\ h_k \times \beta, & id_k = 2 \quad \forall h_k \in KKp \cap KKOq \\ h_k \times \gamma, & id_k = 3 \quad \forall h_k \in KKOp \cap KKq \\ h_k \times \delta, & id_k = 4 \quad \forall h_k \in KKOp \cap KKOq \end{cases} \tag{2.41}$$

- Dağıtıcı k'ıncı katılımcı için sertifika değerini $Sert_k = \left(\left((h'_k)^{1/2} \bmod N\right) \| \, id_k \| b\right)$ olarak hesaplar. b değeri medikal görüntünün bit derinliğini göstermektedir.

Her katılımcı için oluşturulan sertifika değeri, pay görüntüsü ve katılımcıya özgü x değeri hakkında bilgi içermektedir. Böylece, katılımcılar yeniden yapılandırma aşamasında, pay görüntüsünün iletimi esnasında meydana gelen herhangi bir değişikliği fark edebilecek hale gelir. Önerile yöntem Lin ve arkadaşlarının 2009'daki çalışmalarında güvenlik amacıyla kullanılmaktadır [73].

Literatürdeki gizli görüntü paylaşımı alanındaki diğer çalışmalar blok tabanlı doğrulama prensibinden faydalanmaktadır. Pay görüntüsündeki her bir blok doğrulama bitleri içermektedir ve yeniden yapılandırma aşamasında onaylanmak zorundadır. böyle bir doğrulama mekanizması, medikal görüntülerdeki görüntü boyutunun büyüklüğü göz önüne alınırsa, zamansal açıdan problemlere sebep olacaktır. Önerilen yöntem doğrulamayı blok düzeyinde yapmak yerine bütün bir pay görüntüsünden elde ettiği sertifikalar aracılığıyla yapmaktadır.

2.5.2. Ortaya Çıkarma Algoritması

Ortaya çıkarma algoritması iki alt prosedürden oluşmaktadır: "Doğrulama" ve "Yeniden Yapılandırma". İlk prosedür pay görüntülerini doğrulamayı amaçlamaktadır. Katılımcılardan toplanan sertifikalar pay görüntülerinin bütünlüğünü onaylamada kullanılır. Herhangi bir değişimin fark edilmesi durumunda, ortaya çıkarma algoritması durdurulur. Aksi takdirde yeniden yapılandırma prosedürü medikal görüntüyü ve

elektronik hasta kaydını elde etmede kullanılır. Alt prosedürlere ilişkin detaylı açıklama aşağıda verilmiştir.

2.5.2.1. Doğrulama Prosedürü

Katılımcılar kendilerine gelen stego görüntüleri, sertifikalarını kullanarak doğrulayabilmektedir. Sertifika pay görüntüsü ve katılımcının x değeri hakkında özet bir bilgi içermektedir. Yeniden yapılandırma prosedürü ancak katılımcıların pay görüntülerinin doğrulanmasından sonra başlayacaktır. Doğrulama prosedürünün adımları aşağıda sırasıyla verilmiştir.

- Sertifikadan id_k ve b değerleri çıkartılır.
- id_k değerine göre $\left(\alpha^{-1}, \beta^{-1}, \gamma^{-1}, \delta^{-1}\right)$ değerleri arasından λ_k belirlenir.
- $h_k'' = \left((h_k')^{1/2} \bmod N\right)^2$ değeri hesaplanır.
- $\hat{h}_k = h_k'' \times \lambda_k \bmod N$ değeri hesaplanır.
- $H\left(ST^k \| x_k\right)$ değeri hesaplanır ve $\hat{h}_k$ ile kıyaslanır. Eğer değerler birbirine eşitse stego görüntü doğrulanır. Aksi takdirde iletim esnasında değiştirildiği varsayılır.

Doğrulama prosedürü, sertifikaları kullanarak yeniden yapılandırma adımından önce stego görüntüleri doğrular. Önerilen yöntemde böyle bir doğrulama mekanizması kullanılmamış olsaydı, yeniden yapılandırılan gizli medikal görüntü bozuk piksel alanları içerebilirdi. Bozuk olan bölgeler insan gözüyle ayırt edilemeyebilir ve hekimi yanlış teşhis koymaya yönlendirebilirdi.

2.5.2.2. Yeniden Yapılandırma Prosedürü

Katılımcılar bu aşamada kendilerine ait olan stego görüntüleri, medikal görüntüyü ve elektronik hasta kaydını elde edebilmek için bir araya getirirler. Herhangi k tane stego görüntü, gizli verileri elde edebilmek için yeterli olacaktır. Stego görüntülerde karşılıklı 2×2 büyüklüğündeki piksel bloklarından $((x_1, F(x_1)), (x_2, F(x_2)), \ldots, (x_k, F(x_k)))$ değerleri elde edilir. Bu çiftler Lagrange'ın interpolasyon yöntemi yardımıyla polinomun yeniden

yapılandırılmasında kullanılmaktadır. Polinomun katsayı değerleri medikal görüntü piksel değerleri ve elektronik hasta kaydındaki karakterler hakkında bilgi içerir. Algoritmanın detayları aşağıda verilmiştir.

Katılımcılar, stego görüntülerin bloklara ayrılmasından önce kendilerine ait x_i değerlerini belirlemelidir. "İlk Değer Verme" prosedüründe dağıtıcı ve katılımcı tarafından bilinen değerler her katılımcı için x_i değerinin hesaplanmasında kullanılmaktadır. Dağıtıcı tarafından herkese duyurulan R_0 değeri ve katılımcılar tarafından belirlenen rasgele s_i değeri, x_i değerlerinin hesaplanmasında faydalanılır. Her katılımcı kendisine ait x_i değerini (2.42)'yi kullanarak hesaplar.

$$x_i = R_0^{s_i} \bmod N \tag{2.42}$$

x_i değerleri, Lagrange'ın interpolasyonu yardımıyla gizli görüntü piksel değerlerini yapılandırır. Bu adımdan sonra, stego görüntü dört piksellik gruplara ayrıştırılır. $\left(ST^1, ST^2, \cdots, ST^k\right)$ ile gösterilen k adet stego görüntü medikal görüntüyü yeniden yapılandırılmak için kullanılsın. k adet stego görüntüden elde edilen karşılıklı stego bloklar, yeniden yapılandırılan gizli görüntüdeki karşılık düşen piksel değerlerini yapılandırmaktadır. *i*'inci stego görüntüdeki bir stego blok Şekil 2.7'de verilmiştir. Verilen bloktaki piksel değerleri $\left(a^i, b^i, c^i, d^i\right)$ ile gösterilsin. Dağıtıcı tarafından saklama prosedürü esnasında OPAP kullanılarak ilgili piksellere $F\left(x_i\right)$ değeri yerleştirilmiştir. (2.43) ile verilen ifade o anki stego bloğu kullanarak $F\left(x_i\right)$ değerini elde eder.

$$F\left(x_i\right) = \left(a^i \bmod 4\right)\cdot 64 + \left(b^i \bmod 4\right)\cdot 16 + \left(c^i \bmod 4\right)\cdot 4 + \left(d^i \bmod 4\right) \tag{2.43}$$

Diğer stego görüntülerdeki stego bloklar da, karşılık düşen $F\left(x_1\right), F\left(x_2\right), \ldots, F\left(x_k\right)$ değerlerine ulaşmada kullanılır. x_i değerleri (2.39) ile verilen ifadenin kullanımı ile elde edilir. Ardından $\left(\left(x_1, F\left(x_1\right)\right), \left(x_2, F\left(x_2\right)\right), \ldots, \left(x_k, F\left(x_k\right)\right)\right)$ çiftleri Lagrange'ın interpolasyonu yardımıyla polinom katsayılarını belirlemede kullanılır. Oluşturulan polinomun ilk

$y = \left(\left\lceil \log_{251} 2^b \right\rceil \right)$ katsayısı $s_1, \ldots, s_y$ ile gösterilsin. Karşılık düşen gizli piksel değeri m_i (2.44)'ün yardımıyla hesaplanır.

$$m_i = \left(s_1 \cdot 251^{y-1} + s_2 \cdot 251^{y-2} \ldots + s_y \right) \tag{2.44}$$

Katılımcılar, *b* değerini doğrulama prosedürü esnasında sertifikadan elde etmektedir. Polinomun geri kalan katsayıları ise hasta kayıt bilgisindeki karakterlerin oluşturulmasında kullanılır. Yapılanan polinomun her bir katsayısı hasta kayıt bilgisindeki bir karaktere karşılık düşer. Yeniden yapılandırma prosedürü *k* stego görüntüdeki bütün stego bloklar işlem görünceye kadar tekrarlanmaktadır. Yukarıda anlatılan adımlar karşılıklı *k* stego blokların tümüne aynen uygulanır. Ortaya çıkarma algoritmasının sonucunda gerek medikal görüntü gerekse elektronik hasta kaydı elde edilir. Lagrange'ın interpolasyonu, *k* adet pay görüntüsünden elde edilen stego blokların iletim esnasında bozulmaya uğraması durumunda, polinomu doğru bir şekilde yeniden yapılandıramaz. Böylece, hekimlerin stego görüntüler üzerinde meydana gelen değişimleri fark etmeleri kolay olacaktır.

$a_1^i a_2^i \cdots a_7^i a_8^i$	$b_1^i b_2^i \cdots b_7^i b_8^i$
$c_1^i c_2^i \cdots c_7^i c_8^i$	$d_1^i d_2^i \cdots d_7^i d_8^i$

Şekil 2.7. 2×2 stego blok görüntüsü

Çalışmada, hekimler arasında gizlilik gerektiren medikal görüntülerin paylaşımında Shamir'in sır paylaşma şeması kullanılmıştır. Medikal bilginin ancak belirli sayıda hekimin bir araya gelmesi sonucu konsültasyon için kullanılması sağlanmıştır. *N* hekim medikal bilgiyi ve elektronik hasta kaydını paylaşmaktadır. Her bir hekim normal görünümlü stego görüntüler alırken, medikal görüntü ve hasta kaydı en az *k* tane hekimin bir araya gelmesi sonucu elde edilebilmektedir. Böylece konsültasyondan önce, sağlık durumu ülke politikaları açısından önemli bir kişiye ait medikal görüntü hakkında tek bir kişi bilgi sahibi olamaz. Gruba güven prensipleri yöntem tarafından uygulanmıştır.

Bunun yanında metot, literatürdeki çalışmalardan farklı olarak; elektronik hasta kaydı saklama, gizlilik ve doğrulama gibi üç servisi bir arada sunmaktadır. Diğer

çalışmalar ilgili servislerden yalnız birini iyileştirmeyi amaçlamışlardır. Shamir'in şemasında kullanılan polinom katsayıları, hasta kayıt bilgisi ve medikal görüntünün tek bir ortamda saklanabilmesini olanaklı kılmıştır. Hasta kaydı için taşıma kapasitesi, diğer yöntemlerle kıyaslandığında üstünlük göstermektedir. Diğer yandan yeniden yapılandırılan medikal görüntü herhangi bir bozulmaya uğramaz. Ağ üzerinden iletilen pay görüntüleri steganografi kullanılarak doğal görünümlü görüntüler içerisine saklanmıştır. Stego görüntülerin PSNR değerini iyileştirebilmek amacıyla OPAP kullanılmaktadır. Metot, stego görüntülerin doğrulamasında sertifikalardan yararlanılır. Önerilen medikal görüntü paylaşım şeması gizlilik, doğrulama ve hasta kaydı barındırma gibi servisleri tek bir yöntem içerisinde sağlamayı başarmıştır.

2.6. Morley'in Teoremine Dayanan (3, 3) Gizli Görüntü Paylaşım Şeması

Gizli görüntü paylaşımı ile uğraşan çalışmalarda iyileştirilmesi hedeflenen belirli unsurlar vardır: depolama gereksinimleri, iletim zamanı, anlamlı paylar, payların doğrulanması ve kandırılmaların engellenmesi. Literatürdeki bu unsurların düzeltilmesini hedefleyen gizli görüntü paylaşım şemaları ise Shamir'in ya da Blakley'in yöntemini temel almaktadır. Bu çalışmada Morley'in teoremine dayanan yeni bir gizli görüntü paylaşım tekniği önerilmiştir [148]. Teoreme göre, herhangi bir üçgenin komşu açılarının üçe bölenlerinin kesişimi olan üç nokta bir eşkenar üçgen tanımlayacaktır. Oluşan eşkenar üçgen Morley üçgeni olarak adlandırılmaktadır. Yöntem tarafından Morley üçgeninin kenar ve x eksenine göre olan yönlenim bilgisi, gizli görüntü piksel değerlerini kodlamada kullanılacaktır. Morley üçgeni temel alınarak oluşturulan dış üçgenin köşe nokta koordinatları ise katılımcılara gönderilecek olan pay değerleridir. Dış üçgenin her üç noktası bilinmeden Morley üçgenini yapılandırmak mümkün olmayacaktır.

2.6.1. Morley'in Teoremi

ABC kenarları a, b, c ile gösterilen ve iç açıları sırasıyla 3α, 3β, 3γ olan herhangi bir üçgeni temsil etsin. Şekil 2.8'de verildiği gibi ΔABC ile gösterilen üçgenin içerisinde yer alan Morley üçgeni XYZ, dış üçgenin üçe bölenlerinin kesişiminden oluşur. Teorem ilk

olarak 1899 yılında Frank Morley tarafından ispatlanmıştır. Bu çalışmada ise 1997'de Roy tarafından verilen ispattan bahsedilecektir [143]. İspat, bazı kritik ve kesin açıların belirlenmesi temeline dayanmaktadır. $\angle AXZ$ ve $\angle BXY$ sırasıyla θ, μ açıları ile temsil edilsin. İspatın gerçekleşmesi için gereken $\theta = \pi/3 + \beta$ ve $\mu = \pi/3 + \alpha$ eşitliklerinin doğruluğunu göstermektir. Böylece $\angle ZXY$ açısı $\pi/3$ olarak hesaplanacaktır. Benzer şekilde Morley üçgeninin ΔXYZ diğer açıları da hesaplanabilir.

İspatın ilk aşaması $f(\theta) = f(\pi/3 + \beta)$ olduğunu göstermektir. f ile gösterilen fonksiyonun ifadesi (2.45)'te verilmiştir.

$$f(t) = \sin t / \sin(t + \alpha) \quad 0 < t < \pi - \alpha \tag{2.45}$$

ΔAXZ üçgeninin üzerinde sinüs kuralının uygulanması ile (2.46)'daki ifade elde edilir.

$$\frac{AZ}{\sin\theta} = \frac{AX}{\sin(\theta + \alpha)} \Rightarrow f(\theta) = \frac{AZ}{AX} \tag{2.46}$$

Benzer şekilde ΔAZC üzerinde de (2.47)'de verildiği gibi benzer şekilde sinüs kuralı uygulanır.

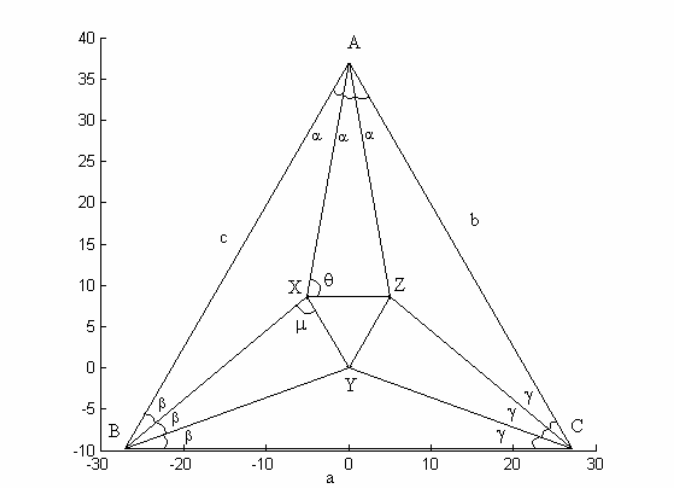
$$\frac{AZ}{\sin\gamma} = \frac{b}{\sin(2\pi/3 + \beta)} = \frac{b}{\sin(\pi/3 - \beta)} \tag{2.47}$$

$3\alpha + 3\beta + 3\gamma = \pi$ olduğundan dolayı $\angle AZC$, $\pi - (\alpha + \gamma) = 2\pi/3 + \beta$ olarak hesaplansın. Sinüs kuralının kullanımı ile (2.48)'deki ifade elde edilir.

$$\frac{AX}{\sin\beta} = \frac{c}{\sin(\pi/3 - \gamma)} \tag{2.48}$$

(2.47) ve (2.48)'in kullanımı ile $f(\theta)$ fonksiyonu (2.49)'daki gibi tanımlanır.

$$f(\theta)=\frac{b\sin\gamma\sin(\pi/3-\gamma)}{c\sin\beta\sin(\pi/3-\beta)} \tag{2.49}$$



Şekil 2.8. Morley'in Teoremi

$t=\pi/3+\beta\Rightarrow\sin(t+\alpha)=\sin(\pi/3+\gamma)$ ifadesinden yola çıkarak $f(\pi/3+\beta)$, $\frac{\sin(\pi/3+\beta)}{\sin(\pi/3+\gamma)}$ olarak tanımlanır. Sinüs kuralının ΔABC ile gösterilen dış üçgen üzerinde uygulanması sonucunda $b\sin 3\gamma=c\sin 3\beta$ eşitliği elde edilir. Eşitlikten (2.50) ile verilen ifadenin elde edilmesinde faydalanılır.

$$\begin{aligned}&4b\sin\left(\frac{\pi}{3}+\gamma\right)\sin\left(\frac{\pi}{3}-\gamma\right)\sin\gamma=4c\sin\left(\frac{\pi}{3}+\beta\right)\sin\left(\frac{\pi}{3}-\beta\right)\sin\beta\\&\frac{\sin(\pi/3+\beta)}{\sin(\pi/3+\gamma)}=\frac{b\sin\gamma\sin(\pi/3-\gamma)}{c\sin\beta\sin(\pi/3-\beta)}\end{aligned} \tag{2.50}$$

Bu ifadeden yola çıkarak $f\left(\frac{\pi}{3}+\beta\right)=\frac{b\sin\gamma\sin(\pi/3-\gamma)}{c\sin\beta\sin(\pi/3-\beta)}=f(\theta)$ eşitliği yazılır. Buradan da $\theta=\frac{\pi}{3}+\beta$ olduğu görülmektedir.

2.6.2. Önerilen Paylaştırma Algoritması

Paylaştırma algoritması D ile gösterilen gizli görüntüyü Morley'in teoremini kullanarak (S_1, S_2, S_3) ile gösterilen üç pay görüntüsüne parçalamaktadır. Gizli görüntü ve pay görüntüleri piksel parlaklık değerleri $[0, 255]$ aralığında değişen gri seviye görüntülerdir. $M \times N$ büyüklüğündeki gizli görüntü $D = \{ d_i \mid i = 1, 2, \ldots, (M \times N) \}$ ile gösterilsin. Algoritma, gizli görüntünün iki pikselden oluşan alt birimleri üzerinde işlem yapmaktadır. Sıralı iki pikselden oluşan ve U^j ile gösterilen gruplar (2.51)'deki gibi belirlenir.

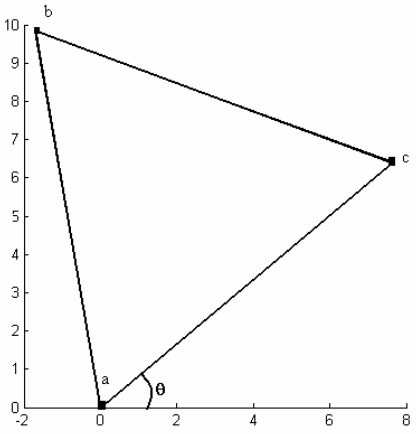
$$U = \{ U^j \mid j = 1, 2, \cdots, (M \cdot N)/2 \}$$
$$U^j = (d_i, d_{i+1}), \; j = \left\lfloor \frac{i+1}{2} \right\rfloor \tag{2.51}$$

U^j grubunun elemanları sırasıyla U_1^j, U_2^j şeklinde referanslanmaktadır. Grup elemanları, Morley'in teoremindeki iç üçgeni oluşturmak için kullanılır. Grubun ilk elemanı U_1^j, iç üçgenin kenar uzunluğunu temsil ederken, diğer elemanı üçgenin x ekseni ile yaptığı açıyı belirlemektedir. İşlem görmekte olan grup U^k ile gösterilsin. Bu durumda s ile gösterilen kenar uzunluğu ve yönlenim açısı θ, (2.52)'deki ifadenin kullanımı ile hesaplanır.

$$s = U_1^k + sbt, \; \theta = U_2^k \tag{2.52}$$

Kenar ve açı değerleri için değişim aralıkları, gri seviye görüntülerdeki piksel parlaklık değişim aralığı $[0 - 255]$ olduğu için sırasıyla $s \in [sbt - (255 + sbt)]$ ve $\theta \in [0 - 255]$ şeklindedir. sbt ile gösterilen sabit terim, gizli görüntüdeki siyah pikseller olması durumunda, anlamsız kenar bilgilerinin oluşmasına engellemek amacıyla kullanılmıştır. Diğer yandan üçgenin yönlenimini gösteren açı değerinin siyah piksellerden dolayı 0 olması, herhangi bir probleme sebep olmamaktadır. Morley'in teoremindeki iç üçgen; kenar uzunluğu ve yönlenim açısı bilgileri yardımıyla Şekil 2.9'daki gibi yapılandırılır.

Üçgenin bir köşesi şekilden de gözlemlenebileceği gibi başlangıç noktasına konumlandırılmıştır. Gizli görüntüdeki sıralı iki piksel parlaklık değerinin (10, 40) olması durumunda (a, b, c) köşeleri ile tanımlanan üçgen Şekil 2.9'da verilmiştir. Kenar uzunluğu 10 olan eş kenar üçgenin $|ac|$ kenarı şekilden de gözlemlenebileceği gibi *x* ekseni ile θ=40° açı yapmaktadır. Bir sonraki aşama Δabc ile gösterilen üçgenin kenarlarını taban alan ve taban açıları sırasıyla (x, y, z) olan ikizkenar üçgenlerin yapılandırılmasıdır. İkizkenar üçgenler için seçilecek olan taban açı değerlerinin toplamı 120°'ye eşit olmak zorundadır. Seçilecek olan taban açı değerleri $[0^\circ - 60^\circ]$ aralığındadır. Seçilecek olan rasgele taban açı değerleri aynı (s, θ) değerleri için bile farklı dış üçgenlerin oluşumunu sağlar. Dış üçgenin köşe noktalarının koordinatları ise pay görüntülerinde karşılık düşen piksel parlaklık değerlerini oluşturur. Gizli görüntü paylaşım şemaları pay görüntülerindeki rasgeleliği sağlamak amacıyla paylaştırma algoritmasından önce karıştırma algoritmaları kullanmaktadır. Oysa önerilen yöntem, ikizkenar üçgenleri yapılandırırken taban açılarını rasgele seçmesi sayesinde karıştırma algoritmalarına ihtiyaç duymamaktadır.



Şekil 2.9. Kenar uzunluğu 10 ve yönlenim açısı 40°olan Morley'in iç üçgeninin yapılandırılması

Taban açıları (x, y, z) olan üç ikizkenar üçgenin yapılandırılması paylaştırma algoritmasının bir sonraki adımı olmaktadır. Bir nokta etrafında başka bir noktanın döndürülmesi prensibi kullanılarak ikizkenar üçgenler yapılandırılır. İç üçgenin *a* ve *c* noktaları, taban kenarı $|ac|$ ve taban açıları *y* olan ikizkenar üçgenin yapılandırılmasında kullanılır. Her iki noktadan biri diğerinin etrafında döndürülmektedir. İlk varsayım *a*

noktası etrafında *c* noktasının –*y*° döndürülmesidir. Ardından *c* noktası etrafında *a* noktası *y*° döndürülür. *c* ve *a* noktalarının koordinatları sırasıyla (c_x, c_y), (a_x, a_y) ile gösterilsin. İlk varsayımdaki dönüşüm işlemine ait matematiksel ifade (2.53)'te verilmiştir. (Nc_x, Nc_y) koordinatları *c* noktasının *a* noktası etrafında –*y*° döndürülmesi sonucu elde edilen yeni noktanın koordinat değerleridir. Aynı şekilde *a* noktasının döndürme işleminden sonraki yeni koordinatları (Na_x, Na_y) olarak hesaplanır.

$$\begin{aligned} Nc_x &= (c_x - a_x)Cos(-x) - (c_y - a_y) * Sin(-x) \\ Nc_y &= (c_x - a_x)Cos(-x) + (c_y - a_y) * Sin(-x) \end{aligned} \tag{2.53}$$

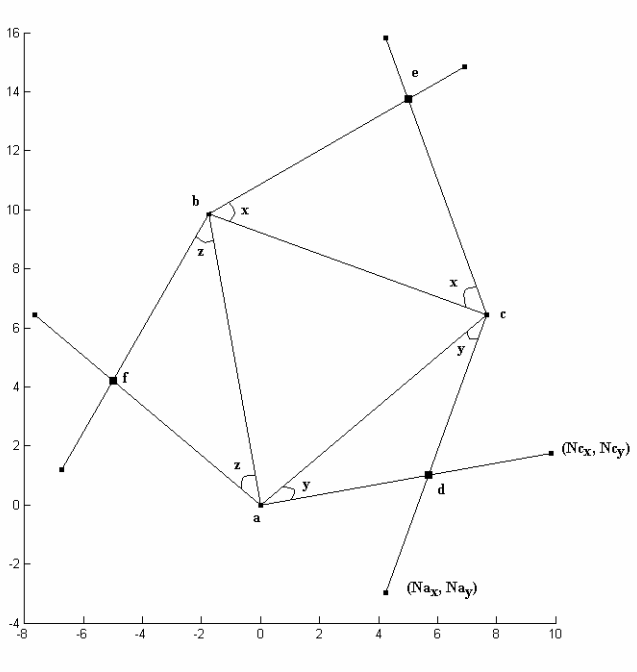
(Na_x, Na_y) ve (Nc_x, Nc_y) noktaları kullanılarak iki doğru belirlenir. (Na_x, Na_y) ve (c_x, c_y), (Nc_x, Nc_y) ve (a_x, a_y) noktalarından geçen doğrular oluşturulur. Bu iki doğrunun kesişim noktası ise Şekil 2.10'da görüldüğü gibi ikizkenar üçgenin *d* ile gösterilen tepe noktasını verecektir.

Diğer ikizkenar üçgenler de yukarıda anlatıldığı gibi yapılandırılmaktadır. Bu üçgenlerin tepe noktaları da sırasıyla *e* ve *f* olarak gösterilsin. İkizkenar üçgenlerin kenarlarının kesişinceye kadar uzatılması dış üçgenin oluşturulmasındaki son adım olmaktadır. Dış üçgenin köşe noktaları sırasıyla $(|be|, |ad|)$, $(|ec|, |af|)$ ve $(|bf|, |cd|)$ ile verilen doğruların kesiştirilmesi sonucu (2.54)'deki gibi elde edilir.

$$\begin{aligned} (A_x, A_y) &= (\,|be| \cap |ad|\,) \\ (B_x, B_y) &= (\,|ec| \cap |af|\,) \\ (C_x, C_y) &= (\,|bf| \cap |cd|\,) \end{aligned} \tag{2.54}$$

Dış üçgenin köşe koordinatları Şekil 2.11'de gösterildiği gibi (A_x, A_y), (B_x, B_y) ve (C_x, C_y) olarak bulunur. Şekilden de gözlemlenebileceği gibi dış üçgenin köşe noktaları koordinat düzleminde birinci bölgede olmayabilir. İlk bölge haricindeki diğer bölgelerde negatif değerler mevcuttur. Bu nedenle dış üçgenin yapılandırılmasının ardından birinci bölgeye transferi gerekmektedir. Dış üçgenin koordinatlarının birinci bölgeye transferi için kullanılan ifade (2.55)'te verilmiştir. min() fonksiyonu argümanlarının en küçüğünü döndürmektedir.

$$x^*_{\min} = \min\left(A_x, B_x, C_x\right)$$
$$y^*_{\min} = \min\left(A_y, B_y, C_y\right) \tag{2.55}$$
$$x^*_{\min} < 0 \Rightarrow \begin{cases} A_x = A_x + \left|x^*_{\min}\right| \\ B_x = B_x + \left|x^*_{\min}\right| \\ C_x = C_x + \left|x^*_{\min}\right| \end{cases} y^*_{\min} < 0 \Rightarrow \begin{cases} A_y = A_y + \left|y^*_{\min}\right| \\ B_y = B_y + \left|y^*_{\min}\right| \\ C_y = C_y + \left|y^*_{\min}\right| \end{cases}$$

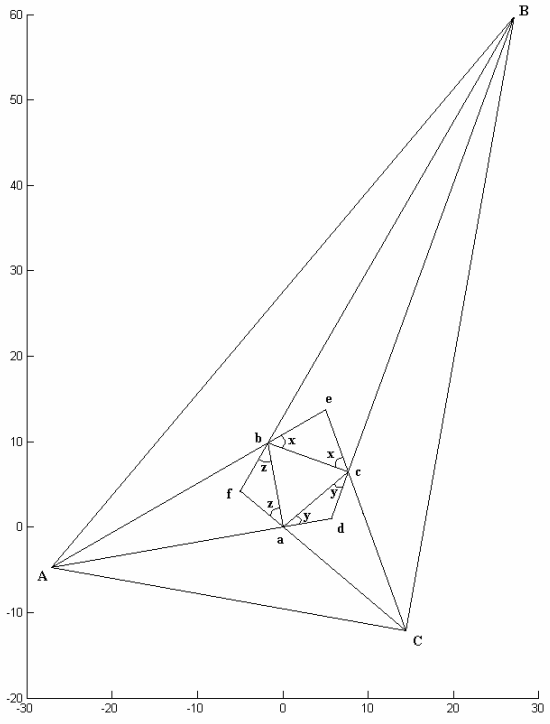


Şekil 2.10. İkizkenar üçgenlerin tepe noktalarının belirlenmesi

Kullanılan öteleme fonksiyonu ile beraber her ne kadar üçgen birinci bölgeye taşınmış olsa da, bazı köşeler *x* veya *y* ekseni üzerinde olabilir. Bu nedenle yöntem ötelemeden sonra rasgeleliğin sağlanması ve siyah değerine sahip pay piksellerinin çok fazla sayıda oluşumuna engel olmak amacıyla, rasgele bir öteleme kullanılmasını önermiştir. Her iki yönde $\left(r_x, r_y\right)$ parametreleri kullanılarak (2.56)'da verildiği gibi rasgele bir öteleme gerçekleştirilmektedir.

$$r_x = \left\lfloor \frac{x^*_{\min} + x^*_{\max}}{2} \right\rfloor \quad r_y = \left\lfloor \frac{y^*_{\min} + y^*_{\max}}{2} \right\rfloor \tag{2.56}$$

Böylece işlem görmekte olan ikili gizli piksel grubu için U^k, üretilen dış üçgenin köşe noktalarının koordinatları katılımcılara gönderilecek olan pay görüntülerin piksel parlaklık değerlerini oluşturur. 8 bit derinlikteki gizli görüntü için 256 mümkün kenar uzunluğu ve yine 256 mümkün açı kombinasyonu pay görüntü derinliğini belirlemede kullanılır. Ötelemede kullanılan sabit terimin 5 olarak seçilmesi durumunda, üretilen dış üçgenlerin köşe noktalarının koordinatlarının $[0-2048]$ aralığında değişim gösterdiği gözlemlenmiştir. Üçgen köşe koordinatlarını temsil etmede kullanılan 22 bit değer algoritma tarafından üç parçaya bölünmektedir. Dış üçgenin köşe noktası *A*, 11 bit iki sayı (A_x, A_y) ile temsil edilir. Her bir sayı 8 ve 3 bitten oluşan iki kısma ayrılmaktadır. Oluşan dört alt bölme kullanılarak üretilen *R, G, B* değerleri, (2.57)'deki ifade yardımıyla hesaplanır. Dış üçgenin diğer kenarları da aynı şekilde üç adet 8 bitlik sayı ile temsil edilerek karşılık düşen pay görüntüsünün piksel parlaklık değeri oluşturulur.



Şekil 2.11. Belirlenen dış üçgen ve koordinatları

İfadeden de gözlemlenebileceği gibi gizli görüntüdeki iki adet piksel değeri, pay görüntüsündeki pikselin üç kanalındaki parlaklık değeri ile temsil edilmektedir. *N*×*M*

büyüklüğündeki bir gizli görüntü için üretilen renkli pay görüntülerinin büyüklüğü $(N \times M/2)$ olmaktadır. (2.57)'deki ifadede yer alan '$\wedge$' ve '<<' sembolleri sırasıyla bit düzeyinde "AND" ve "Kaydırma" işlemlerine karşı düşmektedir.

$$\begin{aligned} R &= \lfloor A_x/8 \rfloor \\ G &= \lfloor A_y/8 \rfloor \\ B &= \left((A_x \wedge 7) << 3\right) \vee \left(A_y \wedge 7\right) \end{aligned} \tag{2.57}$$

Paylaştırma algoritmasını kısaca özetlemek gerekirse: gizli görüntü öncelikle iki pikselden oluşan gruplara bölünür. Bir sonraki aşamada sıradaki iki piksel parlaklık değeri kullanılarak oluşturulan Morley'in üçgeninin kenarlarında rasgele seçilen (x, y, z) taban açıları ile ikizkenar üçgenler oluşturulmaktadır. Taban açıları $[0^\circ - 60^\circ]$ aralığında rasgele olarak seçilir. Ardından dış üçgen ikizkenar üçgenlerin kenar bilgileri kullanılarak oluşturulur. Dış üçgen, negatif koordinatları engellemek amacıyla koordinat düzleminde birinci bölgeye ötelenmektedir. Üçgenin köşe koordinatları ise üretilecek pay görüntülerinin karşılık düşen piksel parlaklık değerlerini oluşturmaktadır. Önerilen yöntemin paylaştırma algoritmasına ait kaynak kod Ek 8'de verilmektedir.

2.6.3. Önerilen Yeniden Yapılandırma Algoritması

Katılımcılardan elde edilen pay görüntüleri gizli görüntüyü elde etmede kullanılır. Pay görüntüleri yeniden yapılandırma esnasında elde edilen 1×1 büyüklüğündeki karşılıklı bloklar dış üçgenin yapılandırılmasında kullanılır. Dış üçgenin köşe noktaları kenarları oluşturmaktadır. Kenarların eğim bilgisi kullanılarak iç açılar elde edilir ve içteki Morley üçgeni yapılandırılır. Morley üçgeninin kenar bilgisi ve x eksenine göre yönlenimi, yeniden yapılandırılan gizli görüntünün karşılık düşen piksel değerlerini oluşturmaktadır. Katılımcılardan elde edilen ve SH^1, SH^2, SH^3 ile gösterilen pay görüntüleri (2.58)'de verilmiştir.

$$SH^k = \left\{ SH_{ij}^k \;\middle|\; i \in \{1 \cdots N\}, j \in \left\{1 \cdots \frac{M}{2}\right\}, k = [1-3] \right\} \tag{2.58}$$

Her pay piksel değeri üç kanal bilgisinden oluşmaktadır. Pay görüntülerindeki karşılık düşen piksel parlaklık değerleri dış üçgenin köşe noktalarını belirler. İlk pay görüntüsünde *m* ile gösterilen pay değeri (2.59)'da verilmiştir. Pay değeri üç kanaldaki değerler kullanılarak yapılandırılır.

$$sh_m^1 = \left\{ sh_{m1}^1, sh_{m2}^1, sh_{m3}^1, m = \left\{1 \cdots N \times M/2\right\}\right\} \tag{2.59}$$

Diğer pay görüntülerinden elde edilen renkli piksel parlaklık değerleri sh_m^2, sh_m^3 ile gösterilsin. Bu piksellerden elde edilen değerler ise dış üçgenin diğer köşelerinin elde edilmesinde kullanılmaktadır. A ile gösterilen köşenin koordinatları $\left(A_x, A_y\right)$, ilk pay görüntüsünden elde edilen kanal renk bilgilerinin $sh_{m1}^1, sh_{m2}^1, sh_{m3}^1$ kullanımı ile (2.60)'taki gibi hesaplanır.

$$\begin{aligned} A_x &= \left(sh_{m1}^1 << 3\right) \vee \left(sh_{m3}^1 >> 3\right) \\ A_y &= \left(sh_{m2}^1 << 3\right) \vee \left(sh_{m3}^1 \wedge 7\right) \end{aligned} \tag{2.60}$$

>> ve $\vee$ işaretleri sırasıyla sağa kaydırma ve bit düzeyine OR'lama işlemlerine karşı düşmektedir. Dış üçgenin diğer köşeleri de iki ve üçüncü pay görüntülerinden gelen değerlerin kullanımı ile hesaplanır. Dış üçgenin elde edilen üç köşe bilgisi kenarları tanımlamaktadır. Üç kenarın eğim bilgisi iç açıların hesaplanmasını sağlar. slp_1, slp_2, slp_3 ile gösterilen eğim bilgileri (2.61)'deki ifadenin kullanımı ile elde edilir.

$$\begin{aligned} slp_1 &= \left(C_y - A_y\right) / \left(C_x - A_x\right) \\ slp_2 &= \left(B_y - A_y\right) / \left(B_x - A_x\right) \\ slp_3 &= \left(C_y - B_y\right) / \left(C_x - B_x\right) \end{aligned} \tag{2.61}$$

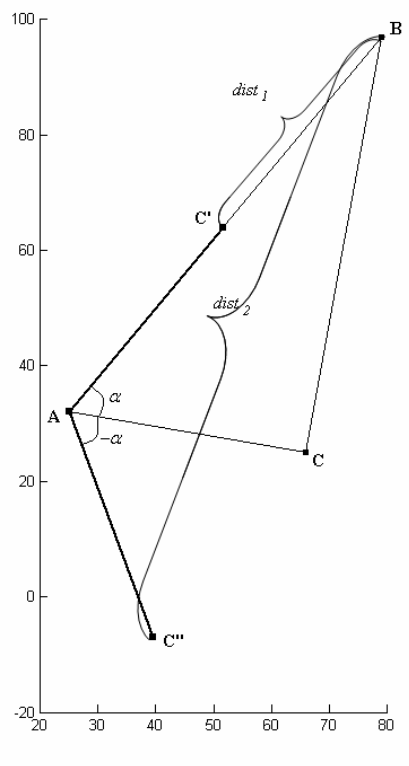
Yeniden yapılandırma sürecindeki bir sonraki aşama iç açıların üç eşit parçaya bölünmesi olduğu için, açıların doğru bir şekilde tespiti önem kazanmaktadır. Kenarların eğimi iç açıların belirlenmesinde kullanılır. α ile gösterilen iç açılardan bir tanesi (2.62)'deki ifade yardımıyla hesaplanır.

$$
\begin{aligned}
&slp_1 \cdot slp_2 = -1 \Rightarrow \alpha = 90 \\
&(slp_1 = \infty) \vee (slp_1 = -\infty) \Rightarrow \alpha = \arctan(180/(slp_2 \cdot \pi)) \\
&(slp_2 = \infty) \vee (slp_2 = -\infty) \Rightarrow \alpha = \arctan(180/(slp_1 \cdot \pi)) \\
&slp_2 > slp_1 \Rightarrow \alpha = \arctan\left(((slp_2 - slp_1)/(1 + slp_1 \cdot slp_2)) \cdot \frac{180}{\pi} \right) \\
&slp_1 > slp_2 \Rightarrow \alpha = \arctan\left(((slp_1 - slp_2)/(1 + slp_1 \cdot slp_2)) \cdot \frac{180}{\pi} \right)
\end{aligned}
\tag{2.62}
$$

Dış üçgenin diğer açıları olan β, γ'da benzer şekilde hesaplanır. (slp_1, slp_3) ve (slp_2, slp_3) değerleri sırasıyla ilgili açı değerlerinin hesaplanmasında kullanılır. Yeniden yapılandırma sürecinde bir sonraki aşama olarak (α, β, γ) ile gösterilen iç açılar üç eşit parçaya ayrılmaktadır. Döndürme transformasyonu açının üç eşit parçaya bölünmesinde kullanılır. Algoritmanın işleyişini göstermek amacıyla α açısı üç eşit parçaya bölünmektedir. Anlatılan adımlar diğer açılar için de geçerlidir. $|AC|$ ve $|AB|$ arasındaki açı α olsun. *C* köşesi *A* etrafında $\alpha/3$ ve $2\alpha/3$ derece döndürülerek açının üçe bölme işlemi gerçekleştirilir. Yalnız dönme işleminin saat yönünde mi yoksa saatin ters yönünde mi olacağı basit bir yöntem ile belirlenir. *C* noktasının *A* noktası etrafında saat yönünde ve saate ters yönde α kadar döndürülmesi sonucu elde edilen noktalar Şekil 2.12'de görüldüğü gibi sırasıyla C'' ve C' olsun. Üretilen noktaların *B* kenarına olan uzaklığını gösteren $dist_1$ ve $dist_2$, (2.63)'teki ifade yardımıyla hesaplanır.

$$
\begin{aligned}
dist_1 &= \sqrt{(B_y - C'_y)^2 + (B_x - C'_x)^2} \\
dist_2 &= \sqrt{(B_y - C''_y)^2 + (B_x - C''_x)^2}
\end{aligned}
\tag{2.63}
$$

B noktasına olan uzaklıklar, açının bölünmesi işleminde kullanılacak olan döndürme işleminin yönünü belirlemektedir. $dist_1 < dist_2$ olması durumunda saat yönünde dönüş işlemi gerçekleştirilecekken, aksi takdirde saat yönünün tersi kullanılır. Dönme yönü belirlendikten sonra, *C* noktası *A* etrafında $\alpha/3$ ve $2\alpha/3$ derece döndürülür. Döndürme işleminin ardından elde edilen yeni noktalar Şekil 2.13'te gösterildiği gibi C^1 ve C^2 olsun. (A, C^1) ve (A, C^2) ikilisi, α açısını üçe bölen ve t_{AC^1}, t_{AC^2} ile gösterilen doğrulardır. Diğer açıları üç eşit açıya bölen dört doğru ise $t_{BA^1}, t_{BA^2}, t_{CB^1}, t_{CB^2}$ ile gösterilsin.

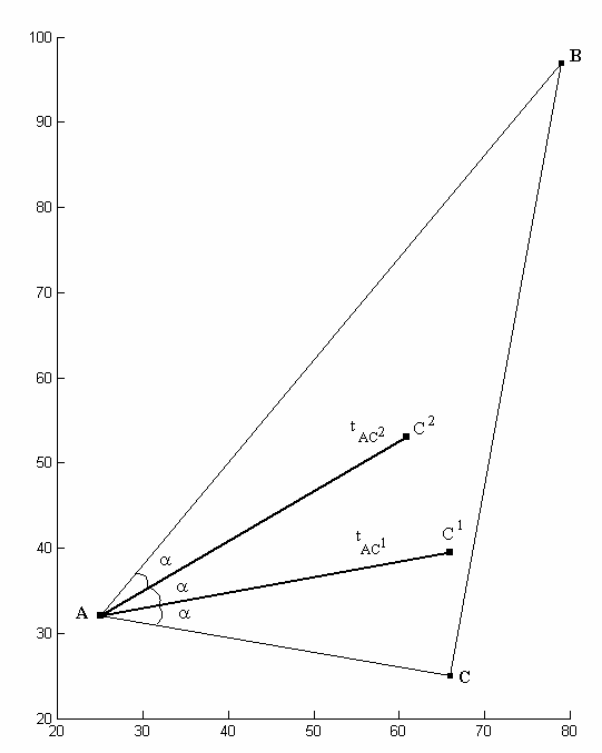


Şekil 2.12. B ve (C', C'')noktaları arasındaki uzaklıklar

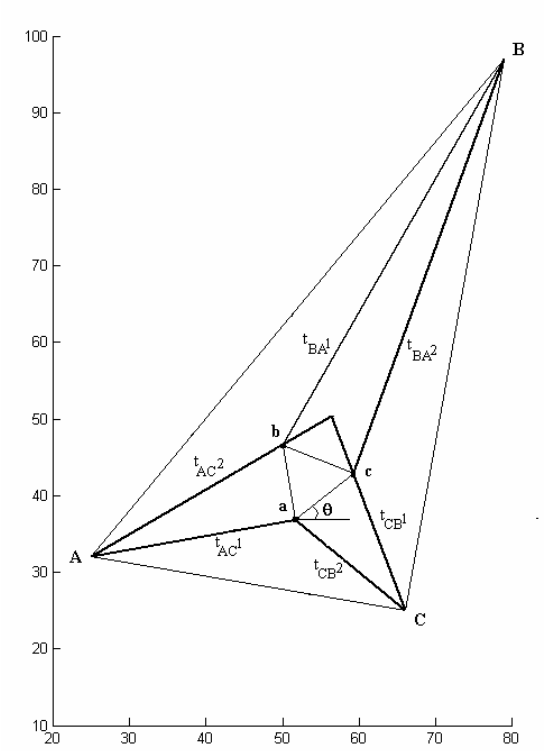
Morley'in üçgeni elde edilen bu doğruların doğru bir şekilde kesiştirilmesi ile elde edilecektir. a, b ve c, sırasıyla AB, BC ve AC kenarlarına yakın doğruların kesişim noktaları olsun. (2.64) ile verilen ifade Morley üçgeninin köşe noktalarını belirlemede kullanılır.

$$a = t_{AC^1} \cap t_{CB^2} \;\; b = t_{AC^2} \cap t_{BA^1} \;\; c = t_{CB^1} \cap t_{BA^2} \tag{2.64}$$

Şekil 2.14'te yeniden yapılandırılan Morley üçgeni gösterilmiştir. Morley üçgeninin köşeleri kullanılarak, üçgenin kenar uzunluğu ve x eksenine göre yönlenimi belirlenir. Elde edilen değerler ise yeniden yapılandırılan gizli görüntünün karşılık düşen piksel parlaklık değerlerini oluşturur. Pay görüntülerinde karşılık düşen bloklar üzerinde yukarıda anlatılan adımlar uygulanarak gizli görüntünün piksel parlaklık değerleri oluşturulur. Morley'in teoremindeki dış üçgenin köşe noktaları pay görüntülerindeki piksel parlaklık değerlerini oluştururken, Morley'in üçgeninin kenar ve yönlenim bilgisi gizli piksel değerlerini kodlamada kullanılmaktadır.



Şekil 2.13. C^1 ve C^2 ile gösterilen yeni noktalar



Şekil 2.14. Yeniden yapılandırılan Morley üçgeni

Elde edilen deneysel sonuçlarda pay görüntülerinin gizli görüntü hakkında herhangi bir bilgi ortaya çıkarmadığı gözlemlenmiştir. Yuvarlama işlemlerinden dolayı meydana gelen yeniden yapılandırma hataları ise insan gözü tarafından ayırt edilemeyecek derecededir.

2.7. Sayı Teorisine Dayanan Gizli Görüntü Paylaşım Şemaları ile İlgili Yapılan Çalışmalar

Literatürde var olan çalışmalar ağırlıklı olarak Shamir'in yöntemini dayanmakla beraber Blakley'in yöntemi de son yıllarda yapılan birkaç çalışmada gizli görüntü paylaşımında kullanılmıştır. Eşik şemaları alanında 1983 yılında Asmuth-Bloom ve Mignotte tarafında ayrı zamanlarda önerilmiş olan ve ÇKT teoreminden faydalanan iki yöntemin bu alandaki etkinliği henüz araştırmacılar tarafından aktif olarak değerlendirilmemiştir. Bu nedenle yapılan çalışmada sayı teorisine dayanan bu iki yöntemin gizli görüntü paylaşımına uyarlanması ve diğer yöntemlere kıyasla gizli görüntü paylaşımında üstünlük sağlayıp sağlamayacağının tespit edilmesi hedeflenmiştir.

2.7.1. Asmuth-Bloom Yönteminin Steganografi ile Beraber Gizli Görüntü Paylaşımında Kullanımı

Bu çalışmada, Asmuth-Bloom'un sır paylaşma yöntemi, gizli görüntülerin paylaşımında ortaya çıkan rasgele değerli pay görüntülerin steganografi tekniği ile örten görüntüler içinde saklanması ilkesi kullanılarak geliştirilmiştir [149, 150]. Üretilen pay değerleri, en anlamsız haneye (LSB) saklama tekniği kullanılarak örten görüntüler içine saklanmaktadır. Örten görüntülerde pay görüntülerin saklanması sonucu oluşan bozulmayı belirleme amacı ile, PSNR ölçümü yapılmıştır. Deneysel sonuçlarda da vurgulandığı gibi, stego görüntüler 50 dB civarında PSNR'ye sahiptir. Buradan yola çıkarak, gerçekleştirilen saklama işleminin örten görüntü üzerinde insan gözüyle ayırt edilemeyecek kadar küçük bir değişime neden olduğu söylenebilir. Önerilen yöntem, literatürdeki sayı teorisine dayalı sır paylaşma yöntemlerini temel alan gizli görüntü paylaşma tekniklerinden farklı olarak, doğal görünümlü pay görüntüleri üretir. Kötü niyetli kişilere karşı pay görüntülerinin güvenliği steganografi tekniğinin kullanımı ile sağlanmaktadır.

Dağıtıcı gizli görüntüyü göndermek istediği n katılımcı için en çok n adet anlamlı görüntü belirler. Örten görüntü olarak da adlandırılan bu ortamlar, gizli görüntü paylaşma

şeması tarafından oluşturulacak olan pay görüntülerinin saklanmasında kullanılır. Paylaştırma algoritması, gizli görüntüyü, önerilen sır paylaşma şemasını kullanarak *n* adet pay görüntüsüne böler. Pay görüntüsü kendisi ile ilişkilendirilmiş örten görüntüye LSB kodlama tekniği kullanılarak saklanır. Steganografik tekniğin kullanımı ile üretilen stego görüntüler, katılımcılara gönderilir.

Yöntemin uygulanmasındaki ilk aşama, Asmuth-Bloom'un sır paylaşma şemasının kullanılmasıyla pay görüntülerinin elde edilmesidir. Gizli görüntünün, yan yana piksellerin oluşturduğu ikili gruplardan oluştuğu varsayılır. *W* adet satırdan ve *H* kadar sütundan oluşan gizli görüntü *P,* (2.65) ile gösterilsin.

$$P = \left\{ p_{ij} \middle|\ p_{ij} \in [0-255], 1 \le i \le W, 1 \le j \le H \right\} \tag{2.65}$$

Asmuth-Bloom'ın sır paylaşma şemasındaki ilk adım olan özel sıralı pozitif tamsayıların seçilmesi işlemi, piksel parlaklık değerleri de göz önünde tutularak gerçekleştirilir. Görüntüdeki piksel parlaklık değerlerinin $[0-255]$ aralığında olduğu düşünülürse, m_0 değeri 255'ten büyük ilk asal sayı olan 257 olarak belirlenir. (*k, n*) eşik şeması için, diğer modulo değerlerinin seçilmesinde (1.18)'deki ifadeden yararlanılır.

Seçilecek olan $m_i, i \in \{1 \cdots n\}$ değerleri $(257, 512]$ aralığındadır. Bu aralığın kullanılmasının sebebi pay görüntülere kodlanacak olan bilginin 9 bit ile sınırlanması içindir. Özel sıralı pozitif tamsayıların seçilmesinden sonra Asmuth-Bloom şemasının gerek koşullarından bir diğeri olan $(S + \alpha \cdot m_0) < m_1 \cdots m_k$ ifadesi de önerilen gizli görüntü paylaşma yöntemi tarafından sağlanmalıdır.

Önerilen yöntem, $(S + \alpha \cdot m_0) < m_1 \cdots m_k$ ifadesindeki *S* ve α değerlerini gizli görüntüdeki piksel parlaklık değerlerine karşı düşürür. Yalnız α değerinin rasgeleliği yöntemin güvenilirliği açısından önemlidir. Aksi takdirde *k*'dan az katılımcının bir araya gelmesi gizli görüntü hakkındaki bazı bilgileri açığa çıkartabilir. Bu nedenle α değeri gizli görüntüde temsil edecek olduğu piksel değerinin belirli bir sabit (*b*) ile çarpılması ile elde edilir. α'nın temsil edecek olduğu pikselden önceki iki piksel değerinin ortalamasının 3/2 katının *b* değeri olarak alınması önerilmiştir.

Böyle bir seçimin Asmuth-Bloom'un şemasının $(S + \alpha \cdot m_0) < p_1 \cdots p_k$ ifadesini ihlal etmeyeceği şu şekilde gösterilebilir. Şemadaki m_0'ın 257 olarak seçilmesi

durumunda, b değerini göz önüne alarak, $(S+\alpha\cdot m_0)<m_1\cdots m_k$ ifadesinin alabilecek olduğu en büyük değer (2.66)'deki gibi hesaplanır.

$$\left(255+257\cdot 255\cdot\left(\frac{255+255}{2}\right)\cdot\frac{3}{2}\right)\cong 25067393<m_1\cdot m_2\cdots m_k \tag{2.66}$$

(2.66)'da hesaplanan 25067393 ifadesi en az üç sayının, (m_i, m_{i+1}, m_{i+2}), çarpımından küçük olur. Bu durumda önerilen yöntemde, k'nın alabilecek olduğu en küçük değerin üç olma zorunluluğu vardır. m_i değerlerinin alabilecek olduğu en küçük değer $\sqrt[3]{25067393}\cong 293$ 'den büyük olmalıdır. m_0 değerinin 257 olarak belirlenmesi ve k değerinin üç ve üçten büyük olması durumunda diğer m_i değerleri $[293, 512)$ aralığından seçilir. Sonuç olarak S ve α'nın gizli görüntü piksel parlaklık değerlerini temsil edecek şekilde seçilmesi durumunda, Asmuth-Bloom'un sır paylaşma şemasındaki gerek koşulları ihlal etmeyecekleri söylenebilir. Sıralı pozitif tamsayıların belirlenmesinden sonra, işleme girecek olan gizli görüntü piksel grubu (p_{ij}, p_{ij+1}) ile gösterilsin. S ve α'nın değerleri (2.67)'deki ifade ile belirlenir.

$$\begin{aligned} S &= p_{ij} \\ b &= \frac{3}{2}\cdot\left(\frac{p_{ij-1}+p_{ij-2}}{2}\right) \\ \alpha &= b\cdot p_{ij+1} \end{aligned} \tag{2.67}$$

(2.67)'deki ifadenin kullanımı ile pay görüntülere yerleştirilecek olan piksel parlaklık değerleri (2.68)'deki gibi hesaplanır. n adet katılımcı için oluşturulacak olan pay görüntüleri $SH^m, m\in\{1\cdots n\}$ ile gösterilsin. Birinci katılımcı ile ilişkilendirilmiş olan pay görüntüsü SH^1 ile ifade edilir.

$$\begin{aligned} SH_{xy}^1 &= (S+m_0\cdot\alpha)\bmod m_1 \\ SH_{xy}^2 &= (S+m_0\cdot\alpha)\bmod m_2 \\ &\vdots \\ SH_{xy}^n &= (S+m_0\cdot\alpha)\bmod m_n \end{aligned} \tag{2.68}$$

SH_{xy}^{1}, gizli görüntüdeki ikili grubun, birinci katılımcı ile ilişkilendirilmiş olan modulo m_1'in kullanımı ile hesaplanan değeri gösterir.

Gizli görüntü sağdan sola ve yukarıdan aşağıya ikili piksel grupları halinde taranır ve her grup için (2.67) ve (2.68)'deki ifadelerin kullanımı ile *n* adet pay görüntüsüne bir piksel değeri kodlanır. Buradan yola çıkarak oluşturulan pay görüntülerinin, gizli görüntünün büyüklüğünün yarısı olacağı söylenebilir.

Paylaştırma algoritması, yukarıda ifade edildiği gibi, Asmuth-Bloom'un sır paylaşma şemasını kullanarak *n* adet pay görüntüsü elde eder. Pay görüntüleri gizli görüntünün büyüklüğünün yarısı kadardır. Her pay görüntüsü kendisi ile ilişkilendirilmiş olan örten görüntüye saklanır. *m*. pay görüntüsü ile ilişkilendirilmiş olan örten görüntü C^m ile gösterilsin. Örten görüntünün 2×2'lik örten bloklardan oluştuğu varsayılır. Şekil 2.15'te C^m'de *d*. satır ve *e*. sütundan itibaren yer alan örten blok görüntüsü verilmiştir. İlgili bloğun ilk pikselinin son üç biti ve diğer piksellerin son iki bitleri, karşı düşen pay görüntüsündeki değeri kodlamada kullanılır. Her bir pay görüntü büyüklüğünün $W(H/2)$ olduğu düşünülürse, pay görüntüsünü saklamak için kullanılacak örten görüntü büyüklüğünün en az $2WH$ olması gerekir.

SH_{xy}^{m} değerinin *m*. örten görüntüde, C^m, karşılık düştüğü bloktaki piksel parlaklık değerleri $(c_{de}, c_{de+1}, c_{d+1e}, c_{d+1e+1})$ olsun. Bu durumda pay görüntüsündeki değerin, örten bloğa kodlanması için kullanılan ifade (2.69)'da verilmiştir.

$$
\begin{aligned}
c_{de} &= ((c_{de} \wedge 248)) \vee ((SH_{xy}^{m} \wedge 448)/64) \\
c_{de+1} &= ((c_{de+1} \wedge 252)) \vee ((SH_{xy}^{m} \wedge 48)/16) \\
c_{d+1e} &= ((c_{d+1e} \wedge 252)) \vee ((SH_{xy}^{m} \wedge 12)/4) \\
c_{d+1e+1} &= ((c_{d+1e+1} \wedge 252)) \vee (SH_{xy}^{m} \wedge 3) \\
d &= (x-1) \times 2 + 1 \\
e &= (y-1) \times 2 + 1
\end{aligned}
\tag{2.69}
$$

İfadeden görüleceği gibi bloğun ilk pikselinin son üç bitine, 9 bitten oluşan SH_{xy}^{m} değerinin ilk üç biti kodlanmıştır. SH_{xy}^{m}'in 448 ile 'AND'lenmesi, ilk üç bit hariç tüm bitlerin sıfırlanmasını sağlar. Ardından gerçekleştirilen 64'e bölme işlemi ise, 'AND'lenme işleminden sonra elde edilen değerin 6 bit sağa kaydırılmasına karşı düşer. Böylelikle elde

edilen ilk üç bit ‘OR’ işlemi kullanarak bloktaki ilk pikselin son üç bitine kodlanır. İlgili pikselin son üç bitini ‘OR’ işleminden önce sıfırlayabilmek için, c_{de} değeri 248 ile ‘AND’ lenmiştir. Bloktaki diğer piksellerin son iki bitlerine de aynı teknik kullanılarak saklama işlemi gerçekleştirilmiştir.

Örten görüntüye pay görüntülerinin saklanmasının ardından oluşan görüntüler stego görüntü olarak adlandırılır. Stego görüntülerdeki değişim insan gözüyle ayırt edilemeyecek ölçüdedir. Stego görüntü ve kodlanmış örten görüntü aynı anlama gelmektedir. Bu nedenle stego görüntülerin temsilinde farklı bir isimlendirme kullanılmamıştır.

Gizli görüntünün yeniden yapılandırılabilmesi için *k* ya da daha fazla sayıda katılımcının bir araya gelmesi gerekir. Katılımcıların kendilerine ait stego görüntüyü yeniden yapılandırma algoritmasına koyması sonucu, gizli görüntü elde edilir. Aksi takdirde, gizli görüntü hakkında herhangi bir bilgi açığa çıkarılamaz.

Yeniden yapılandırma algoritması öncelikle, *k* tane katılımcıdan gelen görüntüler içerisindeki pay görüntülerini çıkartır. Kodlanmış örten görüntüler (stego görüntü) 2×2’lik bloklar halinde değerlendirilir. *m*. stego görüntüdeki *d*. satır ve *e*. sütundan başlayan örten blok, $\left(c_{de}, c_{de+1}, c_{d+1e}, c_{d+1e+1}\right)$ ile gösterilsin. Bu durumda *m*. pay görüntüsüne gömülmüş olan pay değeri (2.70) ile hesaplanır.

$$\begin{aligned} g &= \left(\left(\left(c_{de} \wedge 7\right) << 6\right) \vee \left(\left(c_{de+1} \wedge 3\right) << 4\right)\right) \vee \left(\left(c_{d+1e} \wedge 3\right) << 2\right)\right) \\ SH_{xy}^{m} &= g \vee \left(c_{d+1e+1} \wedge 3\right) \\ x &= \left(d+1\right)/2 \\ y &= \left(e+1\right)/2 \end{aligned} \tag{2.70}$$

k stego görüntüdeki tüm bloklar değerlendirilerek, *k* pay görüntüsündeki karşılık düşen piksel değerleri elde edilir. Elde edilen pay görüntülerindeki değerler bu aşamadan sonra Asmuth-Bloom sır paylaşma şemasının yeniden yapılandırma aşamasında kullanılır. *k* adet farklı pay görüntüsünün karşılıklı pozisyonlardaki değerleri, $SH_{xy}^{1}, SH_{xy}^{2}, \cdots, SH_{xy}^{k}$ ile gösterilsin. Pay görüntüleri ile ilişkilendirilmiş modulo değerleri de kullanılarak (2.71)’deki ifade elde edilir.

c_{de} $\left(c_{de}^{1} \cdots c_{de}^{6} c_{de}^{7} c_{de}^{8}\right)$	c_{de+1} $\left(c_{de+1}^{1} \cdots c_{de+1}^{7} c_{de+1}^{8}\right)$
c_{d+1e} $\left(c_{d+1e}^{1} \cdots c_{d+1e}^{8}\right)$	c_{d+1e+1} $\left(c_{d+1e+1}^{1} \cdots c_{d+1e+1}^{8}\right)$

Şekil 2.15. C^m'de d. satır ve e. sütundan itibaren yer alan örten blok görüntüsü

$$\begin{aligned} T &= SH_{xy}^{1} \bmod m_1 \\ T &= SH_{xy}^{2} \bmod m_2 \\ &\vdots \\ T &= SH_{xy}^{k} \bmod m_k \end{aligned} \tag{2.71}$$

Verilen denklik ifadeleri için ortak çözüm olan *T*, ÇKT teoreminin kullanımı ile hesaplanır. Bir önceki adımda bulunan gizli görüntü piksel çifti değerleri, paylaştırma algoritmasında verilen *b* değerini belirler. *T* değeri, (S, α) çiftinin hesaplanmasında (2.72)'de verildiği gibi kullanılır.

Elde edilen *s* ve α değerleri yapılandırılmakta olan gizli görüntünün sıralı piksel ikilisini oluşturur, (p_{ij}, p_{ij+1}). (p_{ij-1}, p_{ij-2})çifti bir önceki adımda hesaplanan gizli görüntü piksel parlaklık değerleridir. Pay görüntülerindeki karşılıklı piksel değerlerinin oluşturduğu denklem sistemlerinin (2.71)'de ifade edildiği gibi ÇKT ile çözülmesi sonucunda, gizli görüntü pikselleri yeniden yapılandırılır, (2.72). Pay görüntülerindeki karşılıklı piksel değerleri, gizli görüntüde komşu iki piksel parlak değerini oluşturur. Yeniden yapılandırılan gizli görüntü herhangi bir bozulmaya uğramaz.

Bu çalışmada Asmuth-Bloom'un sır paylaşma şemasını ve steganografiyi bir arada kullanan yeni bir gizli görüntü paylaşma şeması önerilmiştir. Üretilen pay görüntülerinin PSNR değerlerinin 50 dB civarında olması, örten görüntülerde saklama işlemi sonrasında meydana gelen bozulmanın gözle ayırt edilemeyecek ölçüde olduğunu gösterir. Asmuth-Bloom'un şemasında tanımlı α değerinin rasgeleliğinin artırılması aynı zamanda yöntemin güvenilirliğinin de bir ölçütüdür. Deneylerde *k*'dan az sayıda katılımcının bir araya gelmesi durumunda gizli görüntü hakkında bir bilgi elde edilemeyeceği de gösterilmiştir.

$$
\begin{aligned}
&S = T \bmod m_0 \\
&b = \frac{3}{2} \cdot \left(\frac{p_{ij-1} + p_{ij-2}}{2} \right) \\
&b \cdot \alpha = \left\lfloor \frac{T}{m_0} \right\rfloor \Rightarrow \alpha = \left\lfloor \frac{T}{m_0} \right\rfloor \Big/ b \\
&p_{ij} = S \quad p_{ij+1} = \alpha
\end{aligned}
\tag{2.72}
$$

2.7.2. Mignotte'nin Şemasına Dayanan Gizli Görüntü Paylaşma Şeması

ÇKT'ne dayalı Mignotte'nin eşik şeması ilk olarak 2008 yılında Shyu vd. tarafından gizli görüntülerin paylaşımı için kullanılmıştır [144]. Fakat önermiş oldukları yöntem, üretilen pay görüntülerinin gizli görüntü hakkında bilgi içermesine engel olabilmek için çekirdek değeri ve algoritması taraflar arasında önceden bilinen rasgele fonksiyon kullanmaktadır. Rasgele fonksiyon hem paylaştırma algoritmasında hem de yeniden yapılandırma algoritmasında kullanılacağı için her iki algoritma da aynı rasgele fonksiyonu aynı çekirdek değeri ile kullanmalıdır. Gizli verinin Mignotte tarafından belirlenen aralık içerisine düşmesi için kullandıkları öteleme parametresi sabittir ve aynı zamanda rasgele fonksiyonun çekirdek değeridir. Yöntem tarafından çekirdek değeri katılımcılar arasında paylaşılmak zorundadır. Ek bilgilerin gizli veri haberleşmesi öncesinde paylaşılacak olması yöntemin güvenilirliğini tehlikeye atarken bant genişliğinin gereksiz kullanımına yol açmaktadır. Çalışma kapsamında önerilmiş olan yöntem, yalnızca paylaştırma algoritmasında rasgele fonksiyonu kullanarak hem gizli verinin Mignotte aralığına düşmesini sağlamış hem de gizli verinin iletiminden önce ek haberleşmeye engel olmuştur [151].

Önerilen yöntem iki alt algoritmadan oluşmaktadır: Paylaştırma ve Yeniden Yapılandırma algoritmaları. Paylaştırma algoritması gizli görüntüyü *n* katılımcı arasında Mignotte'nin şemasını kullanarak dağıtmaktadır. Algoritmanın uygulanması sonucunda katılımcılara gürültü şeklindeki pay görüntüleri gönderilir. Pay görüntülerinin en az *k* tanesinin bir araya gelmesi gizli görüntünün yeniden yapılandırılabilmesi için gereklidir. *k*-1 ya da daha az pay görüntüsünün bir araya gelmesi sonucu gizli görüntü hakkında herhangi bir bilgi edinilemez. Paylaştırma algoritmasının katılımcılara dağıtacak olduğu gizli görüntü, her bir piksel değeri $[0-255]$ aralığında değişen gri seviye bir görüntü

olsun. Gizli görüntü büyüklüğünün $N \times M$ olduğu varsayılırsa, (2.73)'teki ifade gizli görüntünün temsilinde kullanılacaktır.

$$S = \left\{ s_{ij} \,\middle|\, s_{ij} \in [0-255],\, i \in \{1 \cdots N\},\, j \in \{1 \cdots M\} \right\} \tag{2.73}$$

Gizli görüntüdeki her piksel değeri, Mignotte'nin şeması tarafından dağıtılacak olan gizli veri olarak kabul edilir. Paylaştırma algoritmasının ilk adımı dağıtıcı tarafından belirlenen k ve n değerlerine bağlı olarak n tane birbiriyle asal pozitif tamsayıyı, $p_1 < p_2 < \cdots < p_n$, (1.15)'te verilen koşulu sağlayacak şekilde belirlemek olacaktır. Seçilen değerler $[0-255]$ aralığındaki sayılardan oluşur. Örneğin (3, 4) şeması için seçilecek olan değerler sırasıyla $(p_1,\, p_2,\, p_3,\, p_4) = (238,\, 249,\, 251,\, 253)$ şeklinde belirlenmektedir. Ardından Mignotte'nin şemasında da vurgulandığı gibi gizli verinin bulunması gereken aralığın alt sınırı α ve üst sınırı β değerleri (2.74)'ün kullanımıyla belirlenir.

$$\alpha = p_n \cdot p_{n-1} \cdots p_{n-k+2}, \quad \beta = p_1 \cdot p_2 \cdots p_k \tag{2.74}$$

Gizli görüntüdeki $[0-255]$ aralığındaki piksel değerleri, paylaştırma esnasında (α, β) aralığına haritalanmalıdır. Shyu vd.'nin yapmış olduğu çalışmada sabit bir öteleme değeri pikselleri tanımlı aralığa düşürmek için kullanılmıştır [144]. Bu durumda yeniden yapılandırma algoritmasında sabit değerin kullanılabilmesi için, pay görüntülerinin dağıtımından önce katılımcılar arasında paylaşılması gerekir. Bu da sistemin güvenliğini tehlikeye atacaktır. Önerilen yöntem piksellerin ilgili aralığa düşmesi için modulo işleminin özelliklerinden faydalanmaktadır. Böylece yeniden yapılandırma esnasında gizli verinin ötelenmemiş değerine ulaşabilmek için herhangi bir değerin önceden bilinmesine gerek olmayacaktır. Yöntem α ve β değerlerini kullanarak her bir piksel değerini (2.75)'teki gibi Mignotte'nin tanımlı aralığına öteler.

$$\begin{aligned} r &= \left\lfloor rand \cdot \left(\left\lfloor \frac{\beta}{255} \right\rfloor - \left\lfloor \frac{\alpha}{255} \right\rfloor - 1 \right) + \left\lfloor \frac{\alpha}{255} \right\rfloor \right\rfloor \\ s_{ij} &= s_{ij} + (255 \cdot r) \end{aligned} \tag{2.75}$$

İfade de kullanılan *rand*() fonksiyonu $[0-1]$ aralığında rasgele değerler üreten bir fonksiyondur. (2.75)'in kullanımı ile işlem görmekte olan gizli görüntü pikseli s_{ij}, tanımlı aralığın içine düşürülür. Yalnız burada dikkat edilmesi gereken nokta, ötelemede kullanılan bağıl konum değerinin 255'in katı şeklinde olmasıdır. Paylaştırılacak olan piksel değerinin (α, β) aralığına haritalanmasının ardından (2.76)'daki ifade kullanılarak, pay görüntülerinde karşılık düşen piksel değerleri oluşturulur. Pay görüntüleri, gizli görüntü ile aynı büyüklüktedir. Çünkü her bir gizli görüntü pikseli için karşılık düşen pay görüntüsünde bir piksel değeri kodlanacaktır. Pay görüntüleri $G^1, G^2, \cdots, G^n$ şeklinde gösterilecek olursa, *k*'ıncı pay görüntüsü (2.76)'deki gibi tanımlanabilir.

$$G_{ij}^k = \left\{ g_{ij}^k \in [0-255],\ i \in \{1 \cdots N\},\ j \in \{1 \cdots M\} \right\} \tag{2.76}$$

Gizli görüntü pikseline karşılık düşen pay görüntülerindeki piksel değerleri (2.77)'nin yardımıyla hesaplanır.

$$g_{ij}^t = s_{ij} \bmod p_t, \quad t \in \{1 \cdots k \cdots n\} \tag{2.77}$$

Gizli görüntüdeki tüm piksel değerleri için bahsi geçen adımların tekrarlanması sonucu, $N \times M$ büyüklüğündeki *n* adet pay görüntüsü elde edilir. Paylaştırma algoritması ek herhangi bir işleme ihtiyaç duymaksızın, (2.77)'nin kullanımı ile gizli görüntüdeki lineerliklerin pay görüntülerin de oluşumuna engel olmuştur. Yeniden yapılandırma algoritması en az *k* adet katılımcıdan elde edilen pay görüntülerini kullanarak gizli görüntüyü yeniden elde etmede kullanılan algoritmadır. Herhangi *k* adet katılımcıdan toplanan pay görüntüleri, $G^1, G^2, \cdots, G^k$ olsun. Pay görüntüleri piksel piksel değerlendirilerek gizli görüntü yeniden yapılandırılmaya çalışılacaktır. *i.* satır ve *j.* sütundaki gizli görüntü piksel değerinin yapılandırılması için uygulanan adımlar aşağıda sırasıyla verilmiştir. Pay görüntülerindeki bütün pikseller için aynı işlemlerin uygulanması sonucu, gizli görüntü yeniden yapılandırılacaktır. Kullanılan *çkt*() fonksiyonu iki parametre almaktadır. İlk parametre modulo tabanlarını verirken ikinci parametre karşılık düşen rezidüleri içermektedir. Verilmiş olan tabanlarda karşılık düşen rezidüleri üreten tek bir

çözüm vardır. *çkt* fonksiyonu bu eşsiz sayının bulunması için kullanılmaktadır. (2.78)'deki ifade *çkt*'nin kullanımıyla elde edilen çözümü göstermektedir.

$$c = çkt\left(\left[p_1 \; p_2 \cdots p_k\right], \left[g_{ij}^1 g_{ij}^2 \cdots g_{ij}^k\right]\right), \quad c \in (\alpha, \beta) \tag{2.78}$$

c ile gösterilen değer, yeniden yapılandırma algoritmasında (2.75) ile gösterilen ifadede hesaplanan ötelenmiş değerdir. (2.79)'un kullanımıyla orijinal gizli görüntü piksel değeri yeniden yapılandırılır.

$$s_{ij} = c - \left\lfloor \frac{c}{255} \right\rfloor \cdot 255 \tag{2.79}$$

255 değeri gizli görüntü piksel değerlerinin ve aynı zamanda pay görüntü piksel değerlerinin sahip olabileceği maksimum parlaklık değeridir. Önerilen algoritma modulo özelliğinden faydalanarak herhangi bir bağıl konum değerini önceden dağıtmaya ya da kullanılan rasgele fonksiyonun algoritmasını bilmeye ihtiyaç duymadan gizli görüntüyü yeniden yapılandırabilmektedir. Bu da sistemin güvenilirliğini iyileştirmektedir. Bu çalışmada Mignotte'nin 1983 yılında önermiş olduğu eşik şeması yönteminin gizli görüntülerin paylaşımında uygulaması gerçekleştirilmiştir. Shyu vd.'nin 2008'de yapmış olduğu çalışmadan farklı olarak görüntüdeki rasgeleliği sağlamak için ek fonksiyonların kullanımına ihtiyaç duyulmamaktadır. Shyu vd.'nin yönteminde, paylaştırma algoritmasında ve yeniden yapılandırma algoritmasında önceden bilinen ortak bir rasgele fonksiyon kullanılmaktadır. Rasgele fonksiyonun çekirdek parametresi aynı zamanda görüntülerdeki lineerliğin pay görüntülerinde oluşmasına engel olmak için öteleme parametresi olarak kullanılmaktadır. Kullanılan çekirdek değeri paylaştırma algoritmasından önce taraflar arasında dağıtılmak zorundadır. Bu da sistemin güvenilirliğini tehlikeye atmaktadır. Önerilen yöntem paylaştırma algoritmasında kullanmış olduğu rasgele fonksiyona yeniden yapılandırma esnasında ihtiyaç duymamaktadır. Böylece önceden herhangi bir bilginin paylaşımına ihtiyaç duymayan yöntem, sistemin güvenliğini artırmış ve bant genişliğinin gereksiz kullanımına engel olmuştur.

3. BULGULAR VE İRDELEME

Bu bölümde tez kapsamında gerçekleştirilen çalışmalara ait bulguların, literatürde var olan çalışmalara ait sonuçlarla kıyaslanması gerçekleştirilerek, önerilen yöntemlerin üstünlükleri ve getirdikleri dezavantajlar irdelenecektir. Yapılan çalışmalar kısmında üzerinde durulduğu gibi önerilen yöntemler, gizli görüntü paylaşımı alanındaki belirli problemlere çözüm getirmeyi hedeflemektedir. Çalışmalar tarafından iyileştirilmeye çalışılan unsurlar kısaca aşağıdaki şekilde özetlenebilir.

- Üretilen pay görüntülerinin anlamlı hale getirilmesi.
- Stego görüntülerin PSNR değerinin iyileştirilmesi.
- Örten görüntülerdeki genişleme oranının küçültülmesi.
- Stego görüntülerde kullanılan doğrulama biti sayısının, PSNR değerini etkilemeden artırılması.
- Yeniden yapılandırma esnasında stego görüntülerden, örten görüntülerin elde edilmesi.
- Yeniden yapılandırılan gizli görüntünün hatasız olarak elde edilmesi.

Literatürdeki çalışmalar çözüm getirdikleri probleme bağlı olarak, genel bilgiler kısmında da bahsedildiği gibi, belirli alt gruplara ayrılmaktadır. Bu nedenle tez kapsamında yapılan çalışmaları kendi alt alanlarında değerlendirmek daha uygun olacaktır. Ait oldukları alt alanlara bağlı olarak gerçekleştirilen çalışmalar ve üstünlükleri kısaca aşağıdaki şekilde özetlenebilir.

"Diğer sır paylaşım tekniklerini kullanan gizli görüntü paylaşım şemaları" alanında yapılan çalışma Blakley'in yöntemini, gizli görüntülerin paylaşımında kullanmaktadır. Önerilen yöntemin var olan yöntemlere göre üstünlüğüne vurgu yapıldıktan sonra, Shamir tabanlı yöntemlerle kıyaslaması gerçekleştirilmektedir. Bu çalışmada kullanılan örten görüntü büyüklüğü, Shamir tabanlı yöntemlere kıyasla $1/4$ oranında küçülmüştür. Ayrıca Blakley'in yöntemini kullanan diğer yöntemlerden farklı olarak, üretilen pay görüntüleri anlamlı hale getirilmiştir.

Bu alanda yapılan bir diğer çalışmada, Asmuth-Bloom ve Mignotte'nin sır paylaşım şemalarının gizli görüntü paylaşımı alanına uyarlanması ile elde edilen sonuçlar irdelenmektedir. Sayı teorisine dayalı yöntemlerin gizli görüntü paylaşımı alanında

kullanılması durumunda, Shamir tabanlı yöntemlere kıyasla sağladığı avantaj ve dezavantajların üzerinde durulmaktadır. Asmuth-Bloom sır paylaşım tekniği, tez kapsamında literatürde ilk olarak gizli görüntü paylaşımı alanında kullanılmıştır. Mignotte'nin eşik şemasını gizli görüntü paylaşımında kullanan, literatürde yer alan çalışmadaki problemlerin üzerinde durulmakta ve önerilen yöntemin üstünlükleri irdelenmektedir.

"Steganografi Tabanlı ve Doğrulama Mekanizmalı Teknikler" alanında yapılan çalışmanın sonuçları bu alandaki diğer çalışmalarla kıyaslanmaktadır. Performans değerlendirmesinde kullanılan unsurlar, stego görüntülerdeki PSNR değeri ve yöntemin stego görüntüleri doğrulama yeteneği hakkında bilgi veren Doğrulama Oranı (*DO*)'dır. Var olan çalışmaların rapor ettiği değerler ile önerilen yöntemin kıyaslanması gerçekleştirilmiş ve üstünlüklerine vurgu yapılmıştır. Elde edilen deneysel sonuçlarda işaretlediği gibi önerilen yöntem, stego görüntülerin PSNR değerini iyileştirirken, doğrulama biti sayısını da artırmaktadır. Yine aynı alanda, doğrulama biti sayısını adaptif olarak belirleyen yeni bir yöntem önerilmiştir. Bu çalışmanın benzer çalışmalarla kıyaslaması, doğrulama biti sayısına bağlı olarak üretilen PSNR değerlerinin karşılaştırılması ile gerçekleştirilmiştir. Aynı zamanda bozulan stego görüntünün doğrulanması esnasında *DO* değerleri ölçülerek, yöntemin üstünlüğüne vurgu yapılmaktadır. Var olan çalışmalardan farklı olarak doğrulama biti sayısını adaptif olarak belirlenmesinin, gizli görüntü paylaşımı alanına katkıları irdelenmiştir.

"Geri Döndürülebilir Gizli Görüntü Paylaşma Teknikleri" alanında yapılan çalışmanın üretmiş olduğu sonuçlar kendi alanındaki diğer çalışmalarla kıyaslanmaktadır. Karşılaştırmalar esnasında; Üretilen stego görüntülerin PSNR değerleri, veri saklama miktarına bağlı olarak üretilen PSNR değerleri, örten görüntü piksel parlaklık değer aralığına bağlı olarak üretilen fark değer aralıkları kullanılmaktadır. Yöntemin, alanındaki diğer çalışmalardan farklı olarak, örten görüntü piksel parlaklık değerine bağlı olmaksızın yüksek PSNR değerine sahip stego görüntüler üretebildiği gösterilmektedir.

Tez kapsamında yapılan bir diğer çalışmada, gizli görüntü olarak medikal görüntülerin seçilmesi durumunda önerilen gizli medikal görüntü paylaşım tekniğinin, var olan steganografi ve damgalama tabanlı gizlilik yöntemlerinden olan üstünlükleri verilmektedir. Elektronik hasta kaydının saklanmasını ve görüntü gizliliğini aynı anda sağlayan literatürdeki ilk çalışma olan yöntemin aynı zamanda grup tabanlı gizlilik ilkesini de sağladığı gösterilmektedir. Diğer yöntemlere kıyasla sağladığı üstünlükler ve görüntü

çözünürlüğünün yeniden yapılandırma algoritmasının çalışma süresine etkisi irdelenmektedir.

Son olarak, var olan eşik şemalarını kullanan gizli görüntü paylaşım şemalarından farklı yeni bir geometri tabanlı gizli görüntü paylaşım şemasının önerimi hedeflenmiştir. "Morley'in Teoremi" ne dayandırılan yeni gizli görüntü paylaşım yönteminin sonuçları değerlendirilmektedir. Önerilen yöntemin üretmiş olduğu pay görüntülerinin, gizli görüntü hakkında bilgi içermediği ve yeniden yapılandırılan gizli görüntünün yüksek PSNR değerine sahip olduğu gösterilmektedir. Aynı zamanda önerilen yöntemin var olan yöntemlere kıyasla irdelemesi gerçekleştirilmiştir. Morley'in teoremini kullanan yöntem, pay görüntüsünde meydana gelen bozulmalara rağmen, gizli görüntüyü insan gözünün ayırt edebileceği şekilde yeniden yapılandırabilmektedir. Literatürdeki çalışmalar, pay görüntülerinde meydana gelebilecek bozulmaları hesaba katmazken, önerilen yöntem ilk olarak pay görüntüsündeki çeşitli bozulmalara rağmen gizli görüntüyü yeniden yapılandırabilmektedir. Pay görüntüsündeki bozulmalara rağmen gizli görüntüyü yine de yapılandırabilen, literatürdeki ilk çalışma olma özelliğini taşımaktadır.

Literatürdeki çeşitli problemlere çözüm getirmek için önerilen tekniklerden elde edilen bulgular ve kendi alanlarındaki diğer çalışmalarla kıyaslanması sırasıyla ilerleyen bölümlerde verilmektedir.

3.1. Geometri Tabanlı Gizli Görüntü Paylaşım Şemasının Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Literatürde var olan gizli görüntü paylaşım şemaları çoğunlukla Shamir'in sır paylaşım yöntemini gizli görüntü paylaşımında kullanmaktadır. Bu çalışmalardan farklı olarak son yıllarda gerçekleştirilen iki çalışma Blakley'in sır paylaşım şemasını, gizli görüntü paylaşımı alanına uyarlamıştır [86, 87]. Önerilen her iki çalışmada bazı problemlerden etkilenmektedir. [86]'daki çalışmanın üretmiş olduğu pay görüntüleri gizli görüntü ile birebir aynı büyüklüktedir. Aynı zamanda üretilen pay görüntüleri gürültü özelliği taşımaktadır. Gürültü özelliği taşıyan pay görüntülerinin steganografi kullanılarak gizliliğinin sağlanması durumunda meydana gelecek değişim oranı 4 olacaktır. [87]'deki çalışmada ise pay görüntü büyüklüğünü küçültebilmek amacıyla, gizli görüntü piksel parlaklık aralığı daraltılmıştır. Önerilen yeniden yapılandırma algoritması, gizli görüntü piksel değerlerini belirlenen aralığa bağlı bir hata oranı ile yeniden elde etmektedir. Bu

nedenle seçilen değere bağlı olarak yeniden yapılandırılan gizli görüntü hatalar içermektedir. Diğer bir problem ise paylaştırma algoritmasından önce katılımcılara, yeniden yapılandırma esnasında kullanılacak x değerlerinin iletilmesinin zorunluluğudur. Önerilen yöntemin böyle bir iletişimin de veri güvenliğini sağlaması gerekmektedir. Bahsi geçen problemler göz önüne alınarak, Blakley'in şemasını kullanan yeni bir gizli görüntü paylaşım tekniği önerilmekte ve yönteme ilişkin detaylar yapılan çalışmalar kısmında verilmektedir. Önerilen şemanın etkinliğini gösterebilmek ve Shamir tabanlı yöntemlerle kıyaslamasını gerçekleştirebilmek amacıyla yapılan testler ve elde edilen deneysel sonuçlar aşağıda verilmektedir.

İlk deney olarak (3, 5) eşik şeması kullanılarak belirlenen gizli görüntünün beş katılımcı arasında paylaştırılması gerçekleştirilmiştir. Katılımcılardan ancak üç ya da daha fazlasının bir araya gelmesi durumunda gizli görüntü yeniden yapılandırılabilecektir. Deneylerde gizli görüntü olarak, USC-SIPI veritabanından alınan gri seviye test görüntüleri kullanılmıştır. Şekil 3.1'de 256×256 büyüklüğündeki gri seviye gizli görüntü verilmektedir.

Şekil 3.1. 256×256 büyüklüğündeki gri seviye gizli görüntü

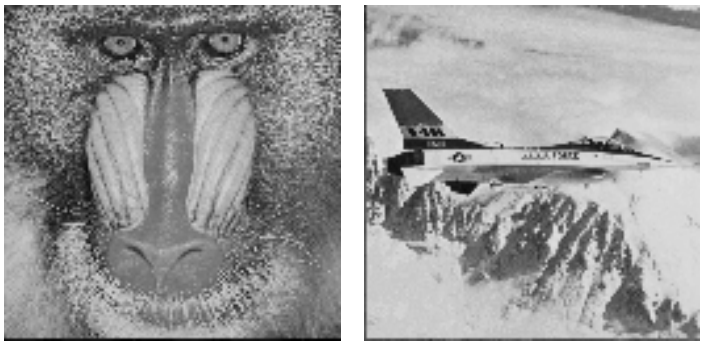
Üretilen pay değerlerinin saklanmasında, dağıtıcı tarafından kullanılacak olan örten görüntüler, gizli görüntü ile aynı büyüklükte ve gri seviye resimlerdir. Her biri 256×256 büyüklüğündeki, "Lake", "Lena", "Pepper", "Jet" ve "Baboon" isimli örten görüntüler Şekil 3.2'de gösterilmiştir. Paylaştırma algoritmasının icrası sonucu Şekil 3.1'de verilmiş olan gizli görüntü Blakley'in yöntemi kullanılarak pay değerlerine parçalanmakta ve üretilen pay değerleri de örten görüntülere saklanmaktadır. Saklama işlemi sonrası elde edilen ve katılımcılara gönderilecek olan pay görüntüleri stego görüntü olarak adlandırılır.

Şekil 3.3'te önerilen yöntemin uygulanması sonucu elde edilen stego görüntüler verilmektedir. Stego görüntülerdeki bozulma oranını tespit edebilmek amacıyla hesaplanan PSNR değerleri de bilgi olarak şekilde verilmiştir. PSNR değeri, iki resim (örten ve stego resim) arasındaki farklılığı tespit edebilmek amacıyla kullanılan bir orandır. Testlerde örten görüntü ve ilişkili stego görüntü arasındaki farklılığı tespit edebilmek amacıyla kullanılmıştır. Her iki görüntü arasında farklılık olmaması durumunda, PSNR değeri sonsuz olarak hesaplanır. Literatürdeki çalışmalarda 38dB ve üzerinde PSNR değerine sahip resimlerdeki değişimin insan gözü tarafından ayırt edilemeyeceği kabul edilmektedir.

Şekil 3.2. 256×256 büyüklüğündeki, "Lake", "Lena", "Pepper", "Baboon" ve "Jet" isimli örten görüntüler

Deneylerden de gözlemlenebileceği gibi gizli görüntü ve stego görüntüler aynı büyüklüktedir. Shamir'in yöntemini kullanarak gizli görüntü paylaşımını sağlayan literatürdeki diğer çalışmalarda ise genişleme oranı dört olarak rapor edilmektedir. Blakley'in sır paylaşma şemasını gizli görüntü paylaşımında kullanan, tez kapsamında önerilen yöntem için genişleme oranı birdir. Böyle bir iyileştirme depolama gereksinimleri ve stego görüntülerin internet üzerinden iletimi için gereken bant genişliği açısından iyileştirme sağlar. Pay görüntülerin iletim zamanı ve depolama ihtiyacı, gizli görüntü paylaştırma şemalarında iyileştirilmesi gereken parametreler arasında yer almaktadır.

38.74 dB 38.45 dB 38.32 dB



38.41 dB 38.17 dB

Şekil 3.3. Elde edilen stego görüntüler ve PSNR değerleri

Literatürde var olan ve Shamir'in yöntemine dayanan gizli görüntü paylaşım şemalarının performansları, önerilen Blakley tabanlı yöntemle kıyaslanmaktadır. Lin ve Tsai'nin, Yang ve arkadaşlarının ve önerilen yöntemin genişleme oranı açısından değerlendirmesi Tablo 3.1'de verilmektedir. Tabloda gösterilen yöntemlerden ilk ikisi polinomial tabanlı bir yaklaşım kullanırken, önerilen yöntem geometrik tabanlı bir yaklaşım olan Blakley'in yöntemini kullanmaktadır. Tablodan da görülebileceği gibi, diğer yöntemler gizli görüntüyü paylaştırabilmek için dört kat daha büyük örten görüntüler gerektirir. Bu da gerek depolama ihtiyaçları gerekse ağ bant genişliği açısından olumsuz etkilere sebep olmaktadır. İkinci deneyde ise önerilen yöntemin uygulanması sonucu elde edilen stego görüntülerin kalitesi diğer yöntemlerin sonuçları ile kıyaslanmıştır. Bu test için dört farklı eşik şeması kullanılmaktadır. Eşik şemalarındaki n değeri 5'e sabitlenmiş, k değeri ise iki ile beş aralığında değiştirilmiştir. Tablo 3.2'den de görüleceği gibi, diğer yöntemlerin PSNR değerleri beş farklı test için aynı kalmaktadır. Yöntemin üretmiş olduğu stego görüntülerin PSNR değeri üzerinde katılımcı sayısını gösteren n değerinin bir etkisi yoktur.

Önerilen yöntem (2, 5) şemasında diğer yöntemlere kıyasla daha kötü sonuç verirken, *k*'nın ikiden büyük olduğu durumlarda diğer yöntemlerden daha yüksek dB'lerde PSNR değerleri üretmektedir.

Tablo 3.1. Önerilen yöntemin genişleme oranı açısından kıyaslaması

	[59]	**[62]**	**Yöntem**
Örten görüntü büyüklüğü / Gizli görüntü büyüklüğü	4	4	1

Tablo 3.2. Önerilen yöntemin farklı eşik şemalarındaki stego görüntü PSNR değerlerinin diğer yöntemlerle kıyaslanması

(2, 5) şeması	**Lake**	**Lena**	**Pepper**	**Jet**	**Baboon**
[59]	38.49	38.6	38.29	38.35	37.71
[62]	40.97	41.1	40.66	40.15	40.06
Önerilen yöntem	28.4	28.37	28.85	28.38	28.69
(3, 5) şeması	**Lake**	**Lena**	**Pepper**	**Jet**	**Baboon**
[59]	38.49	38.6	38.29	38.35	37.71
[62]	40.97	41.1	40.66	40.15	40.06
Önerilen yöntem	38.74	38.45	38.32	38.41	38.17
(4, 5) şeması	**Lake**	**Lena**	**Pepper**	**Jet**	**Baboon**
[59]	38.49	38.6	38.29	38.35	37.71
[62]	40.97	41.1	40.66	40.15	40.06
Önerilen yöntem	41.58	41.8	41.9	41.16	41.95
(5, 5) şeması	**Lake**	**Lena**	**Pepper**	**Jet**	**Baboon**
[59]	38.49	38.6	38.29	38.35	37.71
[62]	40.97	41.1	40.66	40.15	40.06
Önerilen yöntem	45.45	45.07	44.88	44.95	44.65

Bu deneyde önerilen yöntemin diğer iki yöntemden farklı olarak *k*'nın ikiden büyük olduğu durumlarda daha yüksek PSNR değeri ürettiği görülmektedir. Yöntem aynı zamanda gerçek renkteki resimlerin gizli görüntü olarak paylaştırılabilmesini sağlayacak şekilde adapte edilebilir. Son olarak literatürdeki diğer geometrik tabanlı gizli görüntü paylaşma teknikleri ile önerilen yöntem kıyaslanmaktadır. Diğer yöntemlerin üretmiş

olduğu pay görüntüleri gürültü şeklindedir. Gürültü şeklindeki pay görüntüleri ise literatürdeki çalışmalarda vurgulandığı gibi kötü niyetli kişilerin ilgisini çekebilir. Bu çalışmada steganografi kullanarak üretilen pay görüntüleri örten görüntülere saklanmış ve yöntemin gizliliği artırılmıştır.

[86]'daki çalışmada üretilen pay görüntü büyüklükleri, gizli görüntü büyüklüğündedir. Gürültü özelliği taşıyan pay görüntülerinin, anlamlı hale getirilmesinin istenmesi durumunda seçilecek olan örten görüntü büyüklüğü, gizli görüntü büyüklüğünün dört katı olmak zorundadır. Oysa önerilen yöntem üretmiş olduğu pay değerlerini, gizli görüntü ile aynı büyüklükteki örten görüntülere saklayabilmektedir. [87]'deki çalışmada ise gizli görüntü paylaştırma adımından önce seçilen sabit bir değer ile kuantalanmaktadır. Kullanılan sabit değerin ve katılımcılarla ilişkilendirilen biricik x değerlerinin dağıtıcı ve taraflar arasında pay görüntülerinin iletiminden önce bilinme zorunluluğu yöntemin sorunları arasında yer almaktadır. Böyle bir haberleşme, sistem güvenliğini tehlikeye atan unsurlar arasındadır. Gizli görüntünün nicemlemesinde kullanılan sabit değerin 5 olarak seçilmesi durumunda yeniden yapılandırılan gizli görüntü yaklaşık olarak 45 dB PSNR'ye sahip olur. Bu bölümde önerilmiş olan Blakley tabanlı yöntem gizli görüntüyü hatasız olarak yapılandırırken, [87]'deki çalışmadaki piksel parlaklık aralığının daraltılmasında kaynaklanan bozulmalar yöntemin diğer bir acizliğidir. Bahsi geçen probleme [145]'teki çalışmamızda vurgu yapılmış ve yeniden yapılandırma hataları ortadan kaldırılmıştır.

Kısaca özetlenecek olursa Blakley'in yaklaşımını temel alan bu yöntem, Shamir tabanlı ve Blakley tabanlı yöntemlere kıyasla aşağıda verilmiş olan üstünlüklere sahiptir.

1. [59, 62]'deki çalışmaların gerektirdiği örten görüntü büyüklüğü, önerilen yöntemin gerektirdiği örten görüntü büyüklüğünün dört katı kadardır. Yöntem genişleme oranı açısından Shamir tabanlı yöntemlerden daha iyi sonuçlar üretmektedir.
2. Önerilen yöntemin üretmiş olduğu stego görüntülerin PSNR değerleri, k eşik değerinin artan değerleri için artış göstermektedir. Shamir tabanlı yöntemlerde ise k değerinden bağımsız olarak üretilen stego görüntülerin PSNR değerleri sabit kalmaktadır.
3. Blakley tabanlı [86]'daki yöntemden farklı olarak, önerilen yöntem, genişleme oranı açısından dört kat iyi sonuçlar vermektedir. Aynı zamanda üretmiş olduğu pay görüntüleri [86]'dan farklı olarak anlamlıdır.
4. Blakley tabanlı bir diğer yöntem olan [87]'deki çalışmada var olan, bazı sabit değerlerin pay görüntülerinin iletiminden önce paylaşılmasının zorunluluğu,

görüntünün nicemlemesinden kaynaklanan yeniden yapılandırılan gizli görüntüdeki bozulmalar ve pay görüntülerinin rasgeleliği problemlerinden etkilenmemektedir.

Blakley tabanlı bu yöntem literatürdeki genişleme oranı, pay görüntülerinin anlamlı hale getirilmesi ve gizli görüntünün hatasız olarak yeniden yapılandırılması problemlerine çözüm getirmektedir. Bir sonraki bölümde Shamir tabanlı ve "Steganografi tabanlı ve doğrulama mekanizmalı teknikler" alanındaki çalışmamızdan elde edilen deneysel sonuçlar ve kazanımlar verilecektir.

3.2. Steganografi Tabanlı ve Doğrulama Mekanizmalı Şemanın Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Gizli görüntü paylaşımındaki literatürdeki ilk çalışmanın ardından, 2004 yılında yapılan çalışmada pay görüntü güvenliğinin sağlanması için steganografi kullanılmıştır [4, 59]. Steganografiyi ilk kez görüntü paylaşımı ile beraber kullanan çalışma, aynı zamanda stego blokların katılımcılar tarafından doğrulanabilmesi için eşlik bitinin kullanımını önermiştir. Bu çalışmanın ardından, araştırmacılar üretilen stego görüntülerin PSNR değerini ve görüntü paylaşım şemalarının doğrulama yeteneğini iyileştirmeyi hedeflemiştir. Doğrulama yeteneğinin iyileştirilmesi kullanılan doğrulama biti sayısının artırılmasını gerektirirken, doğrulama biti sayısındaki artış stego görüntü kalitesini bozmaktadır. İyileştirilmeye çalışılan unsurlar arasındaki ters orantıya rağmen, her iki yönde de ilerleme kaydetme hedeflenmektedir.

Tez kapsamında önerilen yöntem, yapılan çalışmalar kısmında detayları verildiği gibi, gizli görüntü parlaklık aralığını seviyelendirmektedir. Yöntem, pay değerini temsil etmekte kullanılan bit sayısını azaltırken, doğrulama biti sayısını artırmaktadır. Pay değerini temsil eden bit sayısının azaltılması, polinomun x değerlerindeki çakışma oranını artıracağından, stego görüntü kalitesindeki azalmaya karşı düşmektedir. Yapılan çalışmalar kısmında elde edilen sonuçlarda, pay değerinin 5 bit olarak seçilmesi durumunda, çakışmalar ve stego görüntünün PSNR değeri arasında uygun bir denge sağlandığı rapor edilmiştir. Pay değerlerinin temsilinde kullanılan bit sayısındaki azalma, yöntemin doğrulama biti sayısını artırabilmesini sağlamaktadır. Önerilen yöntemin aynı alandaki diğer çalışmalar ile stego görüntülerin PSNR değeri ve doğrulama yeteneği açısından kıyaslaması aşağıdaki şekildedir.

Gizli görüntü paylaşma şemalarında iki önemli ölçüm parametresi, yöntemin diğer yöntemlere kıyasla üstünlüğünü göstermek amacıyla değerlendirilmiştir. İlk faktör stego görüntülerin görsel kalitesidir ve ölçülebilir bir değerdir. Gizli görüntü paylaşımı alanında çalışan araştırmacılar için, stego görüntülerin görsel kalitesinin iyileştirilmesi amaç olmaktadır. Daha yüksek PSNR değerleri, bozulmanın daha az gözlemlendiği stego görüntü demektir. Deneyler süresince kullanılan diğer bir ölçülebilir unsur ise önerilen yöntemin doğrulama kabiliyeti olmuştur. Bozulmuş bir stego bloğun yanlışlıkla doğrulanma olasılığı, önerilen yöntemin doğrulama metodunun etkinliği hakkında bilgi verir. Bütünlüğün doğrulanmasına ilişkin metrik [63]'teki çalışmada tanımlanmıştır. *DO* yanlış bir stego bloğun yakalanma olasılığını verir. Bozulmuş olan piksel sayısı *BPS* ile, bozulduğu belirlenen piksellerin sayısı *BBPS* ile gösterilirse, *DO* değeri (3.1) ile hesaplanır.

$$DO = \frac{BBPS}{BPS} \tag{3.1}$$

İlk olarak stego görüntülerin görsel kalitesi, örten görüntüdeki bozulma oranını tespit etmek amacıyla değerlendirilmiştir. Şekil 3.4'te gizli görüntü olarak kullanılacak 256 × 256 büyüklüğündeki gri seviye "girl" isimli test görüntüsü verilmektedir. Örten görüntü olarak ise "lighthouse", "chemical", "parrots" ve "houses" isimli test görüntüleri kullanılacaktır. Örten görüntüler 8 bit gri seviye olup 512 × 512 piksel büyüklüğündedir. (3, 4) eşik şeması, stego görüntülerin PSNR değerleri açısından önerilen yöntem ve diğer yöntemler arasında bir kıyaslama yapabilmek amacıyla kullanılmıştır. Şekil 3.5'te üretilen stego görüntüler ve onlarla ilişkili PSNR değerleri verilmiştir. Verilen PSNR değerlerinden de gözlemlenebileceği gibi, stego görüntülerdeki bozulma insan gözü tarafından fark edilememektedir. Yöntem, seçilen eşik değerinden bağımsız olarak, yaklaşık 43 dB PSNR değerine sahip stego görüntüler üretmektedir. Şekil 3.6'da ve Tablo 3.3'te PSNR değerleri açısından yöntemin diğer yöntemlerle kıyaslaması verilmiştir. Açıkça görüldüğü gibi yöntem diğer yöntemlere kıyasla daha yüksek PSNR değerlerine sahiptir. Bu da önerilen yöntemin diğer yöntemlerle karşılaştırıldığında, kötü niyetli kullanıcılara karşı daha dayanıklı olduğunu gösterir. Steganografi tabanlı diğer yöntemler, pay değerlerini ve doğrulama bitlerini kodlamak amacıyla, stego bloklarda, önerilen yönteme göre daha çok bozulmalara sebep olmaktadır. Bu nedenle de üretilen stego görüntülerin PSNR değerleri,

önerilen yönteme kıyasla daha düşük olmaktadır. Literatürdeki çalışmalar pay değerlerini temsil ederken, Shamir'in polinomunu yapılandırırken seçmiş oldukları asal değerden dolayı, 8 bit kullanmaktadır. Önerilen yöntem, asal değerini daha küçük seçerek ve gizli görüntü piksel değerlerini temsil etmede kullanmış olduğu teknikle pay değerini 5 bit ile temsil etmektedir. Pay değerini temsil etmede kullanılan bit sayısının azaltılması ise doğrudan stego görüntünün PSNR değerinin iyileşmesi ile ilişkilidir. Doğrulama esnasında kullanılan bit miktarı açısından bakıldığında, Chang vd.'nin 2008 yılında önermiş olduğu çalışma 4 doğrulama bitine sahip olmasına rağmen en düşük PSNR değerine sahiptir [63]. Önerilen yöntem PSNR açısından Chang vd.'nin yöntemine kıyasla 6 dB daha yüksektir. Wu vd., 2009 yılındaki çalışmasında örten görüntülerdeki bozulmayı azaltabilmek amacıyla OPAP denilen steganografi yöntemini pay değerlerini örten görüntülere gömme esnasında kullanmıştır [65]. Önerilen yöntem LSB'ye gömme tekniğini kullanmasına rağmen Wu vd.'nin yöntemine kıyasla daha yüksek PSNR değerlerine sahiptir. Wu vd.'nin yöntemi aynı zamanda doğrulama için yalnızca bir bit kullanmaktadır. Literatürde var olan yöntemlerdeki doğrulama mekanizmalarındaki en büyük dezavantaj, yanlış bir stego bloğun 0.5 olasılıkla doğrulanmasıdır. Önerilen yöntem ise doğrulama için 3 bit kullanmaktadır. Bu da bozulmuş bir stego bloğun yanlışlıkla doğrulanma olasılığını 0.125'e düşürmektedir. Böylece önerilen yöntem Wu vd.'nin yöntemine kıyasla PSNR değerinde 1.2 dB artış ve doğrulama mekanizması açısından da üstünlük sağlamaktadır. Lin ve Tsai'nin yöntemi eşlik bitini doğrulama amaçlı kullanmaktadır [59]. Yang vd. böyle bir doğrulama mekanizmasına ilişkin problemleri 2007'deki çalışmalarında rapor etmiştir [62]. Kullanmış oldukları 8 bit pay değeri ve 1 bit eşlik biti, 2×2'lik stego bloktaki 9 biti kodlamada kullanmaktadır. Bu nedenle önerilen yönteme kıyasla daha düşük PSNR değerine sahiptir. Kötü niyetli kişiler tarafından bilinçli bozulan stego bloklar, Yang vd.'nin çalışmasında da 0.5 olasılıkla doğru olarak kabul edilebilmektedir. Bu çalışmada da üretilen PSNR değerinin önerilen yöntemden daha düşük olduğu Şekil 3.6'dan gözlemlenebilmektedir. Yang vd.'nin çalışmasında stego blokta toplam 9 bit kodlamada kullanılmaktadır. Sonuç olarak önerilen yöntem PSNR açısından değerlendirildiğinde, bu alandaki diğer çalışmalara kıyasla Şekil 3.6'da görüldüğü gibi daha başarılıdır.

Şekil 3.4. “Girl” isimli 256×256 piksel büyüklüğündeki gri seviye gizli görüntü

(a) PSNR = 43.03 dB

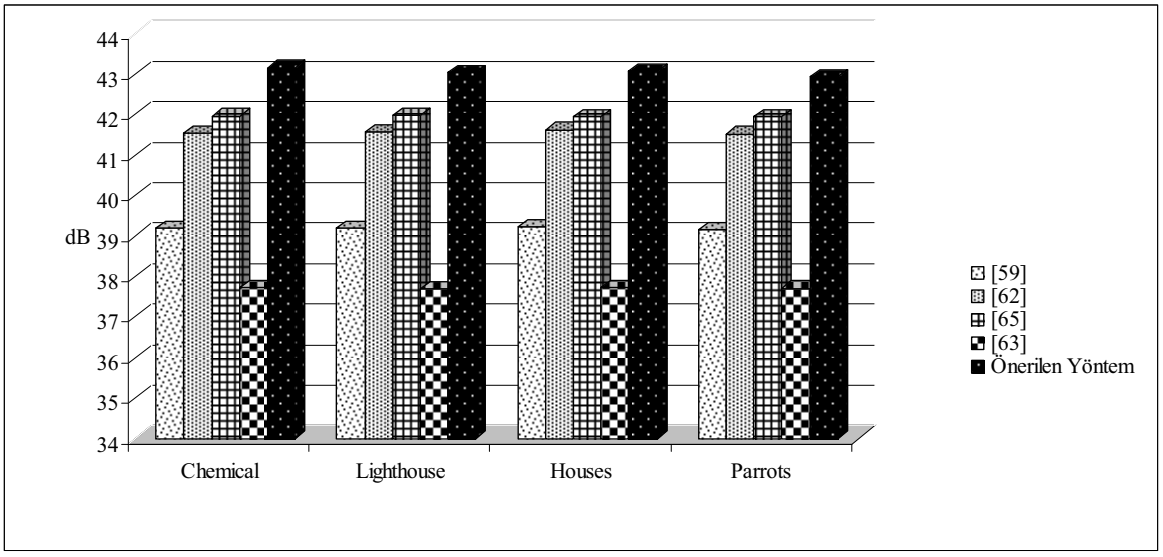
(b) PSNR= 43.15 dB

(c) PSNR= 42.94 dB

(d) PSNR = 43.07 dB

Şekil 3.5. (3, 4) eşik şeması için üretilen stego görüntüler ve PSNR değerleri

Steganografi tabanlı ve doğrulama mekanizmalı gizli görüntü paylaşım tekniklerindeki diğer bir başarı göstergesi ise kullanılan doğrulama biti sayısına bağlı olarak yöntemin üretmiş olduğu ve ifadesi (3.1)'de verilen doğrulama oranıdır. Önerilen yöntemin doğrulama yeteneğini gösterebilmek ve diğer yöntemlerle kıyaslamasını gerçekleştirebilmek amacıyla, deneylerde kullanılmak üzere, yalancı bir stego görüntü oluşturulmaktadır. "Pepper" isimli resim, "window" isimli stego görüntünün sol üst köşesine eklenerek Şekil 3.7(a)'da verilmiş olan bozulmuş stego görüntü elde edilmiştir. Şekil 3.7(b) ve Şekil 3.7(c)'de sırasıyla Wu vd.'nin 2009 yılında yapmış olduğu çalışmanın ve önerilen yöntemin bozulmuş stego blokları tespit edebilme oranını göstermektedir. Resimlerle beraber aynı zamanda yöntemlerin *DO* değerleri de verilmiştir. Wu'nun yöntemi için *DO* değeri 0.51 iken önerilen yöntem için 0.875 olmuştur. Buradan yola çıkarak önerilen yöntemin doğrulama mekanizmasının, Wu'nun yönteminden daha etkin olduğu söylenmektedir. Şekil 3.7(c)'den de gözlemlenebildiği gibi önerilen yöntem, diğer yönteme kıyasla yanlış bölgeleri daha doğru tahmin etmektedir. Tablo 3.3'te aynı zamanda diğer yöntemlerin de *DO* değerleri verilmektedir. Diğer yöntemler de, stego blokta yalnızca bir biti doğrulama amacıyla kullandıklarından dolayı Wu'nun yöntemi ile aynı sonucu üretmektedir.



Şekil 3.6. Önerilen yöntemin diğer yöntemlerle (3, 4) eşik şemasının kullanımı ile PSNR açısından kıyaslanması

Tablo 3.3. Önerilen yöntemin diğer yöntemlerle kıyaslaması

	[59]	**[62]**	**[63]**	**[65]**	**Yöntem**
Stego görüntülerin ortalama PSNR değeri	39.19	41.54	37.57	41.96	43.15
Doğrulama biti sayısı	1	1	4	1	3
DO (Bozulmuş bir stego bloğun tespit edilme olasılığı)	0.5	0.5	0.97	0.5	0.875

(a) Değiştirilmiş stego görüntü

(b) Wu'nun yöntemi

(c) Önerilen Yöntem

Şekil 3.7. Bozulmuş stego görüntü kullanılarak doğrulama açısından yöntemlerin kıyaslaması

Şu ana kadar verilmiş olan sonuçlar, önerilen yöntemin diğer yöntemlere kıyasla gerek stego görüntülerin görsel kalitesi gerekse bozulmuş olan stego blokların tespiti açısından diğer yöntemlere kıyasla daha iyi sonuçlar verdiğini göstermektedir.

Önerilen yöntem, Shamir'in polinom tabanlı yaklaşımındaki asal modulo değerini diğer yöntemlerden farklı biçimde 31 olarak belirlemiştir. Son kısımda böyle bir seçim yapılmasının sebepleri üzerinde durulacaktır. Önerilen yöntem örten görüntüyü 2×2 pikselden oluşan bloklara bölmektedir. Her bloktaki sol üst köşedeki pikselin en anlamlı 6 biti o anki polinomu değerlendirmede kullanılacak olan x değerini temsil etmektedir. Lagrange'ın interpolasyon yönteminin yeniden yapılandırma aşamasında kullanılabilmesi için, n örten bloktan elde edilen x değerlerinin $x_i, i = 1 \cdots n$ eşit olmaması gerekir. Eşit x değerlerinin üretimine sebep olan örten blokların ilk piksel değerleri, farklı x değerleri üretecek şekilde değiştirilmelidir.

Farklı örten bloklardan elde edilen aynı x değerlerinin sayısı ($N_{çakişma}$) ile gösterilsin. Çakışma sayısı iki faktörden etkilenmektedir. Bunlardan ilki x değerini temsil etmekte kullanılan bit sayısının azlığıdır. Yöntem x değerlerini belirlemek için 6 bit kullanmaktadır. Bit sayısının artırılması, çakışma sayısını azaltacaktır. Bunun dışında, eşit x değerlerinin olması aynı zamanda kullanılan örten görüntüler ile de doğrudan ilişkilidir. İlk faktörden kaynaklanan çakışma sayıları, farklı asal sayı değerleri için sabit kalmaktadır. Bu nedenle asal sayının seçiminde ilk faktör değerlendirilmemiştir.

İkinci faktör seçilecek olan asal sayı değeri ile doğrudan ilişkilidir. Seçilen asal sayı değeri küçüldükçe, herhangi iki ya da daha fazla örten görüntüden aynı x değerinin elde edilme olasılığı yani çakışma sayısı artacaktır. Çakışma meydana gelmesi durumunda ise, farklı x değerleri verecek şekilde örten blokların değiştirilmesi gerekir. Bu da üretilen stego görüntülerin görsel kalitesinin azalmasına sebep olacaktır. Yöntem tarafından kullanılacak olan asal sayı değeri, hem pay değerlerini daha az sayıda bit ile ifade edebilmeli hem de aynı zamanda çakışma sayısında artışa sebep olmamalıdır.

Yöntem tarafından seçilen 31 değeri yapılan çalışmalar kısmında vurgu yapıldığı gibi, çakışmalardan kaynaklanan resimdeki bozulmaları, pay değerlerini daha az sayıda bit ile temsil ederek dengelemektedir. Başka bir deyişle, pay değerlerini temsil etmekte kullanılan bit sayısı ile çakışma sayısı arasında ters bir ilişki mevcuttur. Stego bloktaki piksellerin son iki bitleri hem pay değerini hem de doğrulama bitlerini barındırmaktadır. Piksellerin son iki bitinin gömme amacı ile kullanılması ise stego görüntülerin PSNR değerinin yaklaşık 47 dB civarlarında çıkmasına sebep olur. Halbuki önerilen yöntemin

üretmiş olduğu stego görüntüler 43 dB PSNR'ye sahiptir. 43 dB PSNR elde edilmesinin sebebi, çakışmalar durumunda x değerini değiştirebilmek için örten bloğun ilk pikselinin en anlamlı hanelerinde yapılan değişimlerdir. Shamir'in polinomunda kullanılacak olan asal sayı değerinin 31 seçilmesi, yöntemi literatürdeki diğer çalışmalara kıyasla daha güvenilir kılmış ve stego görüntülerin PSNR değerinin iyileşmesine sebep olmuştur.

Çakışma sayısı aynı zamanda paylaştırma algoritmasının icra süresini de etkilemektedir. Çakışmaların çalışma zamanı üzerindeki etkisi, 256 × 256 boyutlarındaki gizli görüntü ve 512×512 boyutlarındaki örten görüntüler ile (3, 4) eşik şemasının kullanımı ile gerçekleştirilmiştir. Normal işlem zamanından ayrı olarak fazladan 182.7 msn, modulo işleminden kaynaklanan çakışmaların çözümü için algoritmaya ek bir yük getirmiştir. Böyle bir ek yük, gerek PSNR değerinin iyileşmesi gerekse iyileşen doğrulama mekanizması düşünüldüğünde azımsanacak bir küçüklüktedir. Bir sonraki kısımda, yapılan çalışmalar kapsamında, geri döndürülebilir gizli görüntü paylaşım teknikleri alanında gerçekleştirilen çalışmaya dair bulgular ve irdelemeler yer almaktadır.

3.3. EMD'ye Dayanan Geri Döndürülebilir Gizli Görüntü Paylaşım Şemasının Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Bu bölümde geri döndürülebilir gizli görüntü paylaşım teknikleri alanında gerçekleştirmiş olduğumuz ve detayları yapılan çalışmalar kısmında verilen yönteme ilişkin deneysel sonuçların irdelenmesi gerçekleştirilecektir. 2009 yılında ilk olarak Lin vd. tarafından gerçekleştirilen çalışma, yeniden yapılandırma algoritmasının ardından, örten görüntülerin stego görüntüler kullanılarak elde edilmesinin önemine vurgu yapmaktadır [73]. Bu çalışmanın ardından üretilen stego görüntülerin PSNR değerinin ve örten görüntülerin taşıma kapasitesinin iyileştirilmesi diğer araştırmacılar için hedef teşkil etmiştir. Fakat var olan çalışmalardaki en önemli problem, üretilen stego görüntülerin PSNR değerinin, örten görüntünün piksel parlaklık aralığından etkileniyor olmasıdır. Özellikle sınır değerlere yakın piksellerin fazla bulunduğu örten görüntülerin kullanılması durumunda düşük PSNR değerleri elde edilmektedir. Yapılan çalışmalar kısmında detaylarını vermiş olduğumuz yöntem, görüntünün dinamik aralığından bağımsız olarak, diğer çalışmalara kıyasla daha yüksek PSNR değerleri üretmektedir. Önerilen yöntemin testi için gerçekleştirilen deneyler ve sonuçların irdelenmesi ilerleyen kısımda verilmektedir. Yöntemin literatürde yer alan diğer çalışmalardan farklılığını gösterebilmek

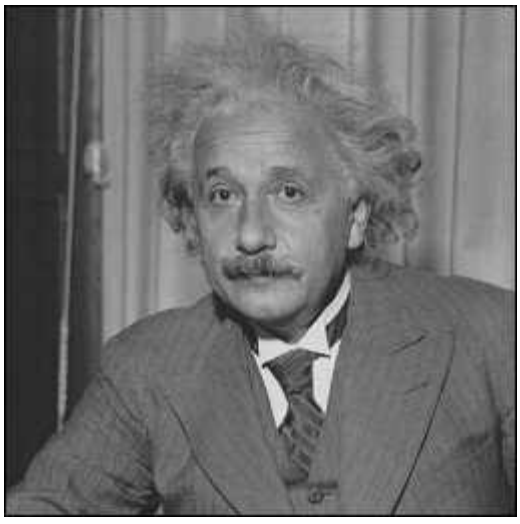
amacıyla, iki tür örten görüntü testler süresince kullanılmıştır: Gri seviye ve tramlanmış görüntüler. 512×512 piksel büyüklüğündeki on beş adet gri seviye görüntü ve onların tramlanmış versiyonları Şekil 3.8'de verilmektedir.

Şekil 3.8. Deneylerde kullanılan gri seviye ve tramlanmış test görüntüleri

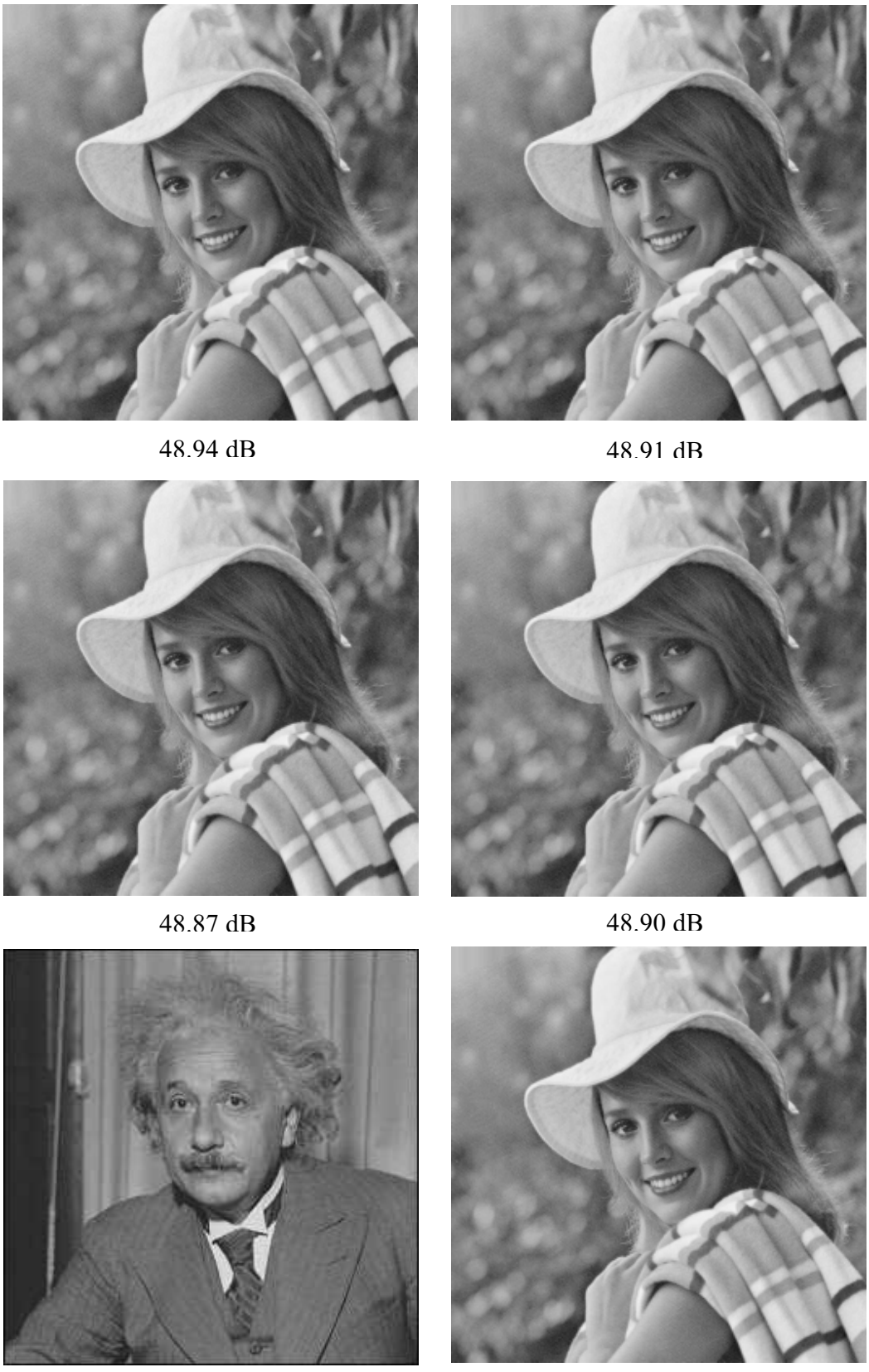
Şekil 3.9'da ise 256×256 büyüklüğündeki katılımcılar arasında paylaştırılacak olan gri seviye gizli görüntü gösterilmiştir. Önerilen yönteminin icrasının ardından oluşacak

olan stego görüntülerde meydana gelen bozulma oranı PSNR ile ölçülecektir. Yüksek PSNR değerleri stego görüntülerdeki bozulmanın insan gözü tarafından ayırt edilme olasılığının düşük olduğunun işaretçisidir.

Gerçekleştirilen ilk deneyde 8 bit gri seviye örten görüntü kullanılmaktadır. Algoritma tarafından üretilecek olan stego görüntülerin PSNR değerinin ölçülmesini amaçlayan bu test, (4, 4) sır paylaşımını gerçekleştirmektedir. Şekil 3.9'da verilen gizli görüntü önerilen yöntem tarafından dört katılımcı arasında paylaştırılır. Üretilen pay görüntüleri, örten görüntünün değiştirilmiş halleridir. Üretilen stego görüntüler ve karşılık düşen PSNR değerleri Şekil 3.10(a)-(d)'de verilmektedir. Şekilden de gözlemlenebileceği gibi üretilen stego görüntülerin ortalama PSNR değerleri 48 dB civarındadır. Şekil 3.10(e)'de ise yeniden yapılandırma algoritması tarafından elde edilen gizli görüntü verilmektedir. Dört katılımcının bir araya gelmesi durumunda elde edilen gizli görüntü sonsuz PSNR değerine sahiptir. PSNR değerinin sonsuz olarak hesaplanması, yeniden yapılandırılan gizli görüntünün hatasız olduğunun bir göstergesidir. Yeniden yapılandırma esnasında, yöntemin geri döndürülebilirlik özelliğinden dolayı, örten görüntüler stego görüntülerden elde edilebilmektedir. Sonsuz PSNR değerine sahip olan yeniden yapılandırılan örten görüntü Şekil 3.10(f)'de verilmiştir.



Şekil 3.9. 256×256 büyüklüğündeki gri seviye gizli görüntü



48.94 dB 48.91 dB

48.87 dB 48.90 dB

∞ dB ∞ dB

Şekil 3.10. (4, 4) şemasının uygulanması sonucu elde edilen stego görüntüler, yeniden yapılandırılan gizli ve örten görüntüler

Önerilen yöntem, 256×256 büyüklüğündeki gizli görüntünün *k*=4 eşik değeri kullanılarak paylaştırılması esnasında, örten görüntünün ancak $(256 \cdot 256 \cdot 4/2) = 256 \cdot 512$ adet pikselini kodlamada kullanmaktadır. Geriye kalan $(512 \cdot 512 - 256 \cdot 512) = 131072$ adet piksel değeri algoritma tarafından kodlama amacıyla kullanılmamaktadır. Gizli görüntü piksel sayısı ve örten görüntü piksel sayısı arasındaki ilişki (3.2)'de verilmektedir. Gizli ve örten görüntü büyüklükleri sırasıyla $N_T \times M_T$ ve $N_C \times M_C$ olarak verilsin.

$$\frac{N_T \cdot M_T \cdot 4}{(k-2)} \leq N_C.M_C \tag{3.2}$$

Paylaştırma algoritması tarafından kullanılan örten piksel sayısı *KPS* ile örten görüntüdeki toplam piksel miktarı ise *TP*S ile gösterilsin. Yöntem (3.3)'te tanımı verilen ve PSNR oranının değerlendirmede kullanılacak olan ve *kullanım oranı*(*ko*) olarak adlandırılan yeni bir metrik önermektedir. İlk deney için *ko* değeri 0.5 olarak seçilmiştir.

$$ko = \frac{KPS}{TPS}, \quad ko \in [0, 1] \tag{3.3}$$

En boy oranı 1 olarak gizli bir görüntünün maksimum genişlik ve yüksekliğinin, örten görüntü büyüklüğü $N_C \times M_C$, *k* ve *ko* cinsinden ifadesi (3.4)'te verilmektedir.

$$N_T = M_T = \sqrt{\frac{N_C.M_C \cdot (k-2) \cdot ko}{4}} \tag{3.4}$$

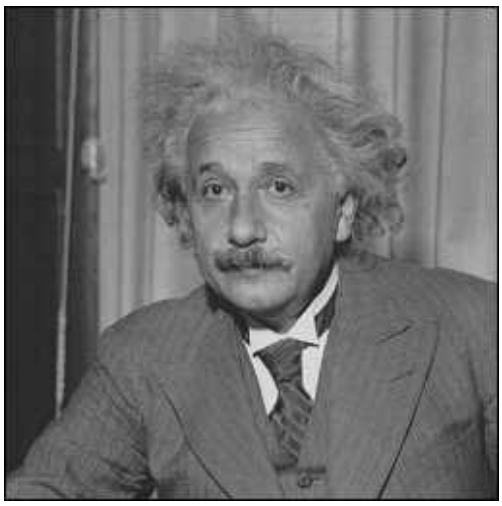
İkinci deneyde 512×512 büyüklüğündeki örten görüntüdeki bütün pikselleri kodlama için kullanabilmek amacıyla eşik değeri *k*=3 olarak belirlenmiştir. Bu durumda (3.4)'ü kullanarak gizli görüntü en ve boyunun $\lfloor \sqrt{(512 \cdot 512 \cdot (3-2) \cdot 1)/4} \rfloor = 256$ olması gerektiği hesaplanmaktadır. Şekil 3.9'da verilen 256×256 büyüklüğündeki gizli görüntü ikinci deneyde de gizli görüntü olarak kullanılmaktadır. (3, 4) eşik şemasının önerilen yöntem tarafından uygulanması sonucu elde edilen stego görüntüler ve üretilen PSNR değerleri Şekil 3.11(a)-(d)'de verilmektedir.

45.93 dB

45.95 dB

45.91 dB

45.92 dB



∞ dB

∞ dB

Şekil 3.11. *ko*=1 seçilmesi durumunda (3, 4) şemasının uygulanması sonucu elde edilen stego görüntüler, yeniden yapılandırılan gizli ve örten görüntüler

Gözlemlenebileceği gibi örten görüntü piksellerinin tümünün kodlamada kullanılması durumunda, üretilen stego görüntülerin ortalama PSNR değeri yaklaşık olarak 45.9 dB civarındadır. Sonsuz PSNR değerine sahip yeniden yapılandırılan örten görüntü ve gizli görüntü Şekil 3.11(e) ve 3.11(f)'de verilmiştir. Her iki deney de önerilen yöntemin iyileştirilmiş PSNR değerlerine sahip stego görüntüler ürettiğini göstermektedir.

İlk iki deneyde kullanılan gri seviye görüntünün tramlanmış hali üçüncü deneyde örten görüntü olarak kullanılacaktır. *ko* değerinin 1 olması durumunda (3, 4) sır paylaşım şemasının Şekil 3.9'da verilen gizli görüntüyü 512×512 piksel büyüklüğündeki iki parlaklık seviyesinden oluşan örten görüntüye yerleştirmesi esnasında yöntemin başarısı irdelenecektir. Paylaştırma sonrasında üretilen stego görüntüler ve PSNR değerleri Şekil 3.12(a)-(d)'de verilmektedir. Yeniden yapılandırılan gizli görüntü ve örten görüntüler sırasıyla 3.12(e) ve 3.12(f)'de yer almaktadır. Deney sonuçlarından da gözlemlenebileceği gibi üretilen stego görüntülerin ortalama PSNR değeri 41 dB civarındadır.

Diğer bir deney ise üretilen stego görüntülerdeki bozulmaların insan gözü tarafından ne kadar ayırt edilebileceğini test etmek amacıyla gerçekleştirilmiştir. Makoto tarafından 1998'de önerilen wPSNR (Weighted Peak to Signal Noise Ratio) oranı testte kullanılmaktadır [153]. Tablo 3.4'te, yöntemin 313×313 büyüklüğündeki gizli görüntüyü (4, *n*) eşik şemasını kullanarak paylaştırıyorken verilen farklı test örten görüntüleri için üretmiş olduğu değerler listelenmektedir. Dört stego görüntünün, gri seviye ve tram örten görüntülerin kullanılması durumunda, ortalama WPSNR değerleri sırasıyla 59.68 ve 57.75 dB şeklindedir. Gerçekleştirilen bir diğer deneyde ise önerilen yöntem literatürde bu alandaki diğer iki çalışma ile üretilen stego görüntülerin PSNR değeri açısından kıyaslanmaktadır.

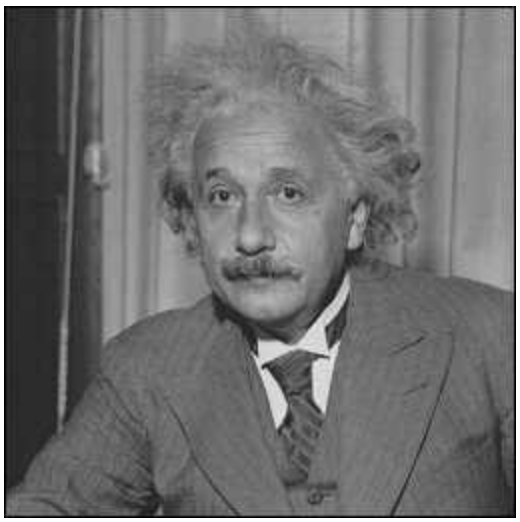
Gri seviye örten görüntüler ve onların tramlanmış halleri bütün metotların birbirlerine göre olan üstünlüklerini vurgulamak amacı ile kullanılmıştır. Literatürdeki yöntemlerin rapor ettikleri PSNR değerleri *ko*=0.75 için üretilmiştir. Bu nedenle önerilen yöntemin kıyaslanabilirliğini sağlamak amacı ile *ko* değerini 0.75 yapabilmek için 313×313 piksel büyüklüğündeki gizli görüntü, 512×512 büyüklüğündeki örten görüntü ve eşik değeri *k*=4 olarak seçilmiştir. Gizli görüntünün eni ve boyu (3.4)'ün kullanımı ile belirlenmektedir. Aynı *ko* değeri için önerilen yöntem, literatürdeki diğer yöntemlere kıyasla daha yüksek PSNR değerlerine sahiptir. Örten görüntü tramlanmış olsa dahi, üretilen stego görüntünün PSNR değeri 43 dB civarındadır.

41.57 dB

41.39 dB

41.41 dB

41.36 dB



∞ dB

∞ dB

Şekil 3.12. *ko*=1 ve tramlanmış örten görüntü seçilmesi durumunda elde edilen stego, yeniden yapılandırılan gizli ve örten görüntüler

Tablo 3.4. Önerilen yöntemin PSNR ve WPSNR değerleri

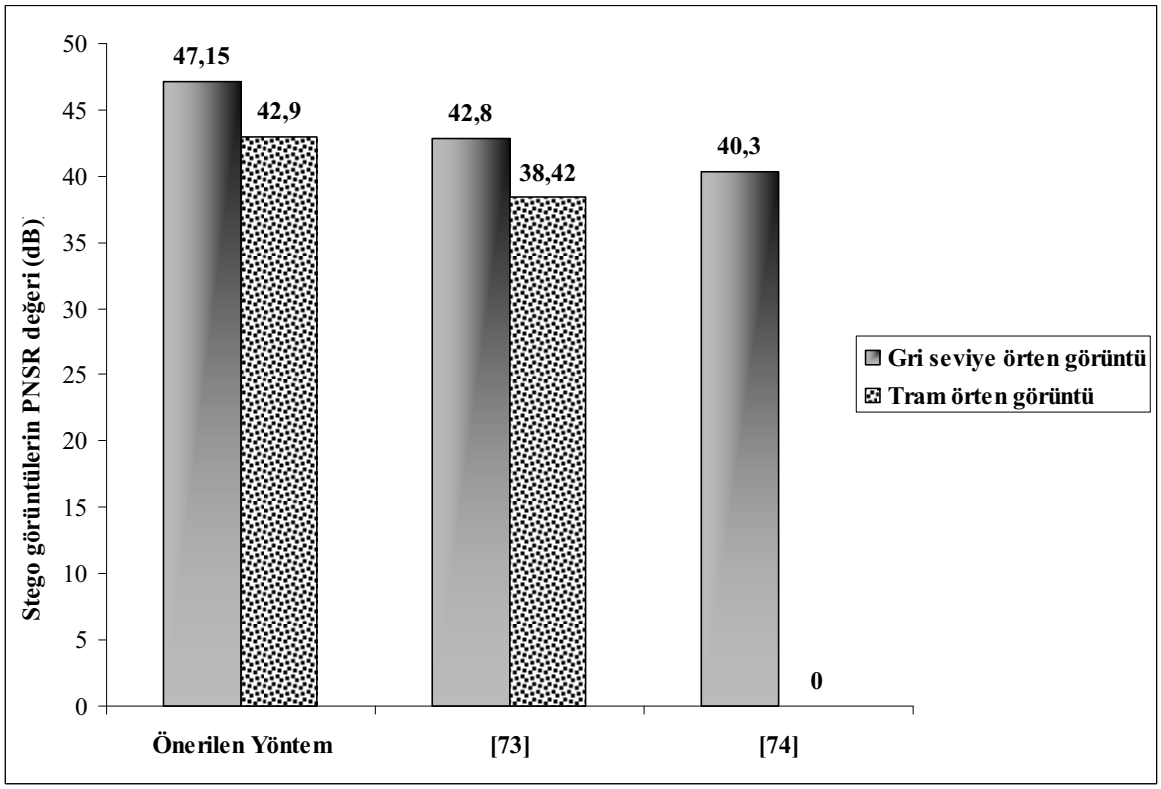
	Gri seviye örten görüntü		Tramlanmış örten görüntü	
Test Görüntüsü	**Ortalama wPSNR (dB)**	**Ortalama PSNR (dB)**	**Ortalama wPSNR (dB)**	**Ortalama PSNR (dB)**
Airplane	59.65	46.68	56.83	43.14
Cameraman	59.67	47.16	55.39	43.45
Clown	59.50	47.03	55.36	43.31
Couple	59.77	47.23	60.06	42.65
Elaine	59.69	46.81	58.89	42.77
Goldhill	59.70	46.56	58.58	42.85
House	59.81	46.82	58.26	42.81
Lena	59.67	46.55	59.00	42.73
Mandrill	59.65	46.57	59.91	42.68
Peppers	59.70	46.18	58.42	42.86
Sailboat	59.72	46.86	56.97	43.18
Splash	59.76	46.80	57.39	42.99
Tiffany	59.60	47.18	54.82	43.49
Einstein	59.60	47.14	59.52	42.7
Zelda	59.66	46.31	56.85	42.98
Ortalama	**59.68**	**46.79**	**57.75**	**42.97**

[73]'teki çalışmanın, tramlanmış örten görüntü kullanılması durumunda üretmiş olduğu stego görüntü PSNR değerleri 38 dB civarındadır. [74]'teki çalışma ise iki parlaklık değerine sahip örten görüntüleri desteklememektedir. Önerilen yöntem gri seviye örten görüntüler için de Şekil 3.13'te gösterildiği gibi daha yüksek PSNR değerlerine sahiptir.

Şekil 3.14, farklı *ko* değerleri için, her üç yöntemin PSNR değerlerini göstermektedir. Gri seviye örten görüntüler her üç yöntemin testi amacı ile kullanılmıştır. *ko* değerinin artışı ile beraber PSNR değerleri düşüş göstermektedir. Buna rağmen önerilen yöntem bütün *ko* değerleri için diğer yöntemlere kıyasla daha yüksek PSNR değerleri üretmektedir.

Son deney (3.5)'te tanımı verilen ve D ile gösterilen fark görüntüsünü kullanmaktadır. Örten görüntü ve stego görüntü piksel parlaklık değerleri arasındaki mutlak fark, fark görüntüsünün piksel değerlerini belirler.

$$D = \left\{ d_{ij} \;\middle|\; d_{ij} = \left| c_{ij} - st_{ij} \right| \right\} \tag{3.5}$$

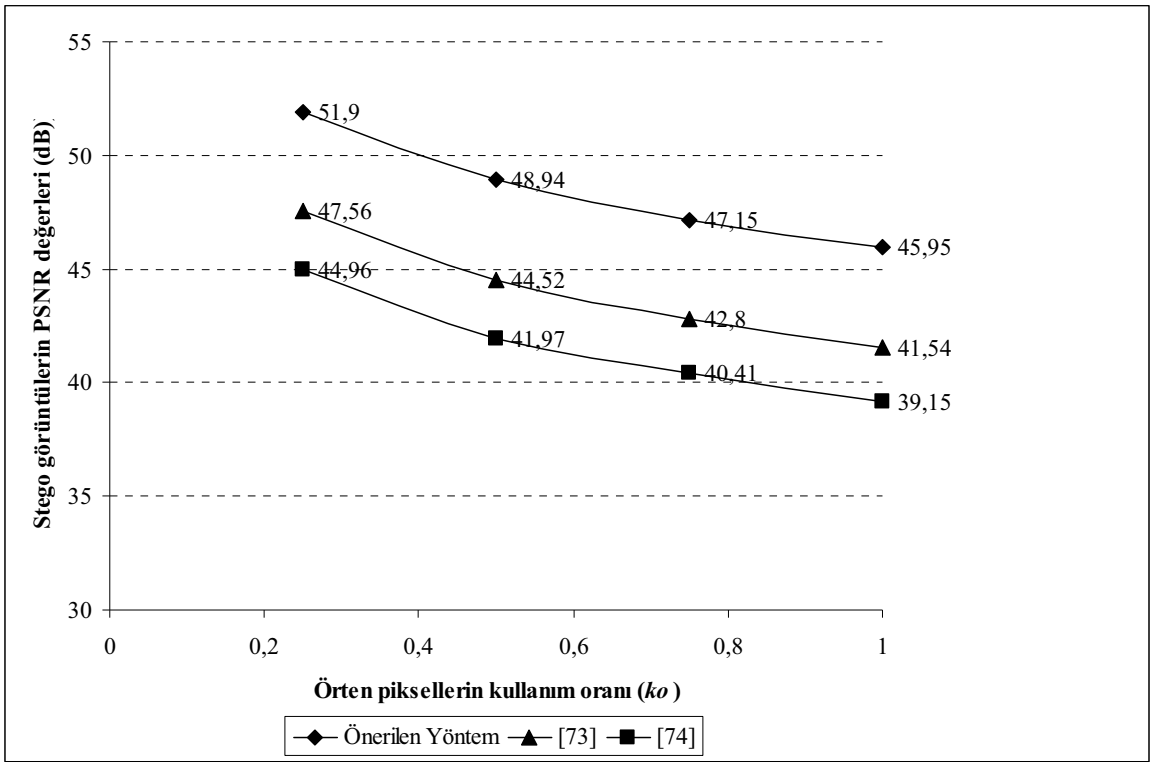


Şekil 3.13. *ko*=0.75 iken önerilen yöntem ve diğer çalışmaların üretmiş olduğu stego görüntülerin PSNR değerleri

Fark görüntüsü, örten görüntülerde meydana gelen değişimler hakkında bir fikir vermek için kullanılacaktır. Fark görüntüsünün parlaklık aralığı, kullanılan paylaştırma şeması ve örten görüntünün parlaklık aralığı ile ilişkilidir. Önerilen yöntem ve literatürdeki diğer çalışmalar farklı parlaklık aralıklarına sahip fark görüntüleri üretmektedir.

Fark görüntüsünün parlaklık aralığının daha dar olması, üretilecek olan stego görüntünün daha yüksek PSNR değerine sahip olacağını garantiler. Aralık genişledikçe, üretilen stego görüntünün PSNR değeri de düşecektir. Tablo 3.5, farklı parlaklık aralıklarına sahip örten görüntülerin kullanılması durumunda, literatürdeki çalışmaların ve

önerilen yöntemin üretmiş olduğu fark görüntülerinin parlaklık aralıklarını vermektedir. Önerilen yöntem gri seviye örten görüntüler için $[0, 2]$ parlaklık aralığına sahip fark görüntüleri üretmektedir. Diğer çalışmalar için fark görüntülerindeki parlaklık aralıkları daha geniştir. Bu da örten görüntü ve stego görüntüler arasındaki mutlak farkın daha büyük olduğunu göstermektedir. Önerilen yöntem, diğer yöntemlere kıyasla hem gri seviye hem de tramlanmış görüntüler için daha yüksek PSNR değerleri üretmektedir.



Şekil 3.14. Gri seviye örten görüntüler için her üç yöntemin farklı *ko* değerlerinde karşılaştırılması

Tablo 3.6 önerilen yöntemin, geri döndürülebilir özelliği taşıyan literatürdeki diğer yöntemlerle kıyaslamasını gerçekleştirmektedir. Tablodan da gözlemlenebileceği gibi, örten görüntülerde sırasıyla 4dB ve 7dB artış elde edilmiştir. [74]'teki çalışma tramlanmış görüntüleri desteklememektedir. [73]'teki çalışma ise tramlanmış örten görüntüler için, 38 dB PSNR'ye sahip stego görüntüler üretmektedir. Önerilen yöntem, örten görüntü piksel parlaklık aralığından bağımsız olarak, diğer yöntemlerden daha yüksek PSNR değerlerine sahip stego görüntüler üretmektedir.

Tablo 3.5. Fark görüntülerinin parlaklık aralıklarının kıyaslanması

	Fark görüntüsünün parlaklık aralığı	
	Gri seviye örten görüntü	**Tram örten görüntü**
Önerilen yöntem	$[0, 2]$	$[0, 4]$
[73]	$[0, 3]$	$[0, 6]$
[74]	$[0, 6]$	desteklenmiyor

Tablo 3.6. Önerilen yöntem ve diğer yöntemlerin özelliklerinin karşılaştırılması

	Gri seviye stego görüntü PSNR	**İkili stego görüntü PSNR**	**Kayıpsız gizli görüntü**	**Ek genişleme**	**Kayıpsız örten görüntü**	**Maksimum kapasite (piksel)**
[73]	43 dB	38 dB	E	H	E	$(k-3)\times N\times M/3$
[74]	40 dB	--	E	H	E	$(k-1)\times N\times M/3$
Önerilen Yöntem	47 dB	43 dB	E	H	E	$(k-2)\times N\times M/4$

Bir sonraki bölümde steganografi tabanlı ve doğrulama mekanizmalı tekniklerdeki doğrulama biti sayısının sabit olarak önceden belirlenmesine vurgu yapılacak ve [68]'deki çalışmanın sahip olduğu problemler tespit edilerek yeni bir gizli görüntü paylaşım yöntemi önerilecektir.

3.4. Adaptif Doğrulama Yeteneğine Sahip Gizli Görüntü Paylaşım Şemasının Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Steganografi tabanlı ve doğrulama mekanizmalı gizli görüntü paylaşım tekniklerindeki en büyük problem, gizli görüntü ve örten görüntü büyüklüğünü hesaba katmadan, stego blok büyüklüğünün sabit olarak 2×2 şeklinde seçilmesidir. Bu problem ilk olarak 2011 yılında Eslami ve Ahmedabadi tarafından yapılan çalışmada ortaya konmaktadır [68]. Yalnız önermiş oldukları yöntem, stego blokların büyüklüklerini adaptif olarak belirlemesine rağmen dinamik doğrulama yeteneğine sahip değildir. Yapılan çalışmalar kısmında vurgu yapıldığı gibi, çalışmalarındaki bir diğer önemli problem ise

kullandıkları zincir mekanizmasından kaynaklanmaktadır. Stego bloklardan birinde meydana gelen bozulma, geri kalan bloklarında hatalı olarak yorumlanmasına sebep olmaktadır. Yapılan çalışmalar kısmında detaylarını vermiş olduğumuz "Adaptif doğrulama yeteneğine sahip gizli görüntü paylaşım şeması" bahsi geçen problemlerin üzerinden gelmekte, gerek stego görüntülerin PSNR değeri gerekse doğrulama yeteneği açısından daha başarılı sonuçlar üretmektedir. Bu bölümde önerilen yöntemin kullanımı ile elde edilen deneysel sonuçlar verilecek ve irdelemesi gerçekleştirilecektir. Aynı zamanda diğer yöntemle olan farklılıklarına ve üstünlüklerine vurgu yapılacaktır.

Önerilen yöntemin diğer yöntemlerle kıyaslamasını gerçekleştirebilmek amacıyla bu alandaki çalışmalarda kullanılan iki parametre açısından irdelemeler gerçekleştirilmektedir. Üretilen stego görüntülerin PSNR değerinin karşılaştırılması ve yalancı bir stego bloğun tespit edilme olasılığı, kıyaslamalarda kullanılan parametrelerdir. Bu anlamda gerçekleştirilen ilk deneyde, önerilen yöntemin (2, 3) sır paylaşım şeması için üretmiş olduğu sonuçlar gözlemlenmektedir. Şekil 3.15(a)'da 256×256 büyüklüğündeki gri seviye "Jet" isimli test görüntüsü verilmektedir. Katılımcılara gönderilecek pay değerlerinin saklanmasında kullanılacak olan 512×512 büyüklüğündeki "Lena", "Lighthouse" ve "Parrots" isimli gri seviye örten görüntüler sırasıyla Şekil 3.15(b)-(d)'de yer almaktadır. Yöntem tarafından önerilen ve detayları yapılan çalışmalar kısmında verilmiş olan paylaştırma algoritması kullanılarak, gizli görüntü üç katılımcı arasında paylaştırılır. Pay değerlerinin, EMD metodunu kullanan gömme prosedürü yardımıyla örten görüntüler içerisine saklanmasının ardından elde edilen stego görüntüler sırasıyla Şekil 3.15(e)-(g)'de verilmektedir.

Örten görüntü ve stego görüntü arasındaki mutlak farkın küçük olması durumunda, insan gözü meydana gelen bozulmaları fark edememektedir. Stego görüntülerde meydana gelen bozulmaları ölçebilmek amacıyla PSNR değeri kullanılmıştır. Şekil 3.15'te üretilen stego görüntülerin ortalama PSNR değerleri 48.6 dB civarındadır. Bu deneyde kullanılan stego blokların büyüklüğü 8 olarak belirlenmiş ve bloğun büyüklüğünden dolayı kullanılan doğrulama biti sayısı 4 olarak seçilmiştir.

Gerçekleştirilen ikinci bir deneyde farklı blok büyüklükleri için üretilen stego görüntülerin PSNR değerleri ölçülmüştür. Tablo 3.7 blok büyüklüğüne bağlı olarak üretilen PSNR değerlerini rapor etmektedir. Açıkça gözlemlenebileceği gibi blok büyüklüğü arttıkça stego görüntü kalitesi iyileşmektedir. Blok büyüklüğü 8 ya da daha fazla olduğunda, üretilen stego görüntülerin PSNR değerleri 48 dB ve daha fazlası olarak

elde edilir. Yöntemin farklı blok büyüklükleri için üretmiş olduğu stego görüntülerin PSNR değerleri Şekil 3.16'da verilmektedir. Şekilden de gözlemlenebileceği gibi blok büyüklüğü 8 olarak seçilmiş iken, üretilen stego görüntülerin PSNR değeri yaklaşık olarak 48 dB civarındadır.

(a) Gizli görüntü

(b)

(c)

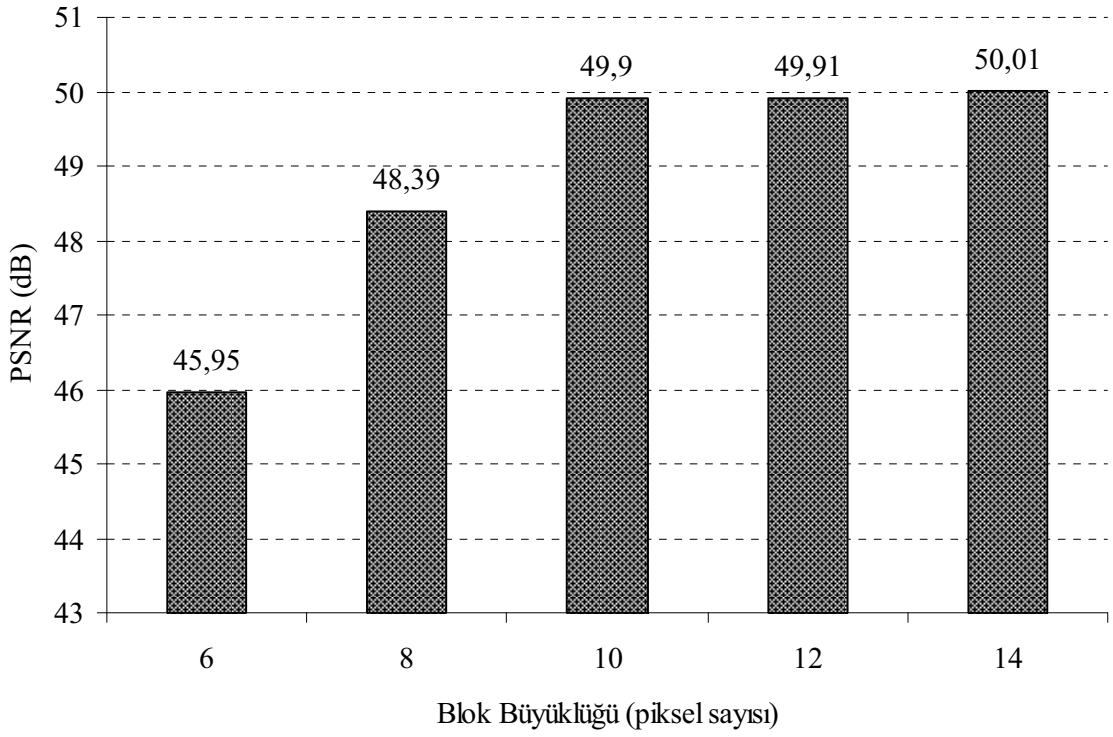
(d)

(e) 48.45 dB

(f) 48.62 dB

(g) 48.87 dB

Şekil 3.15 (a) 256×256 büyüklüğündeki gizli görüntü (b)-(d) 512×512 büyüklüğündeki örten görüntüler (e)-(g) PSNR değerleri ile verilen stego görüntüler



Şekil 3.16. Blok büyüklüğüne bağlı olarak üretilen stego görüntülerin PSNR değerleri

Tablo 3.7. Blok büyüklüğüne bağlı olarak önerilen yöntem ve [68]'deki çalışmanın kıyaslanması

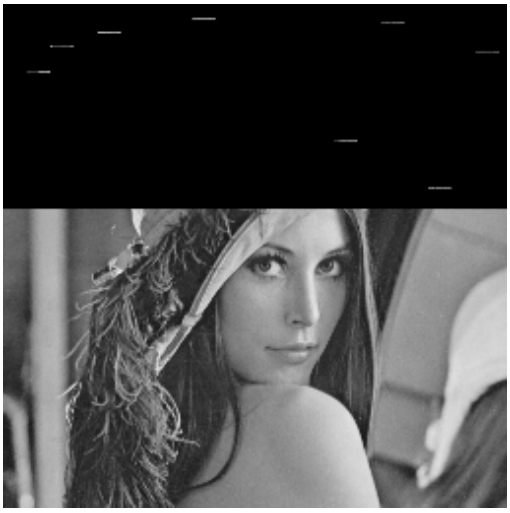
	Önerilen Yöntem			**Eslami vd.[68]**		
Blok büyüklüğü	**Doğrulama biti sayısı**	**Doğrulama Oranı (DR)**	**PSNR (dB)**	**Doğrulama biti sayısı**	**Doğrulama Oranı (DR)**	**PSNR (dB)**
6	4	0.94	45.95	4	0.94	45.60
8	4	0.94	48.39	4	0.94	48.03
10	6	0.98	49.90	4	0.94	50.69
12	9	0.998	49.91	4	0.94	51.47
14	12	0.999	50.01	4	0.94	52.10

Önerilen yöntemin doğrulama gücü de aynı zamanda yapılan testlerde gösterilmektedir. İlk olarak farklı blok büyüklüklerinde yöntemin doğrulama gücünü gösterebilmek amacıyla Şekil 3.17(a)'da gösterildiği gibi 208×512 büyüklüğündeki yalancı bir bölge, stego görüntünün üst kısmına yerleştirilerek yalancı stego görüntü elde edilir.

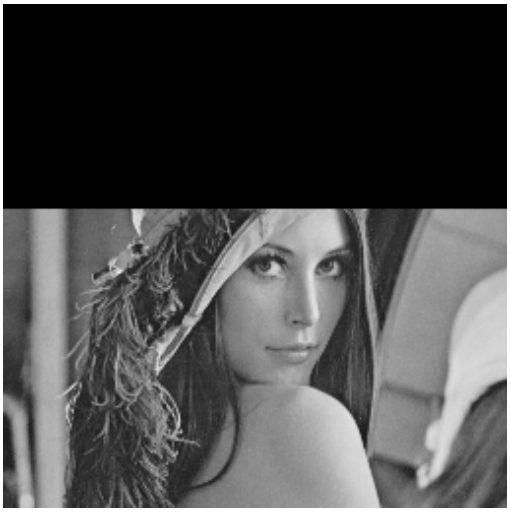
(a)

(b) *DO* = 0.93

(c) *DO* = 0.98



(d) *DO* = 0.99

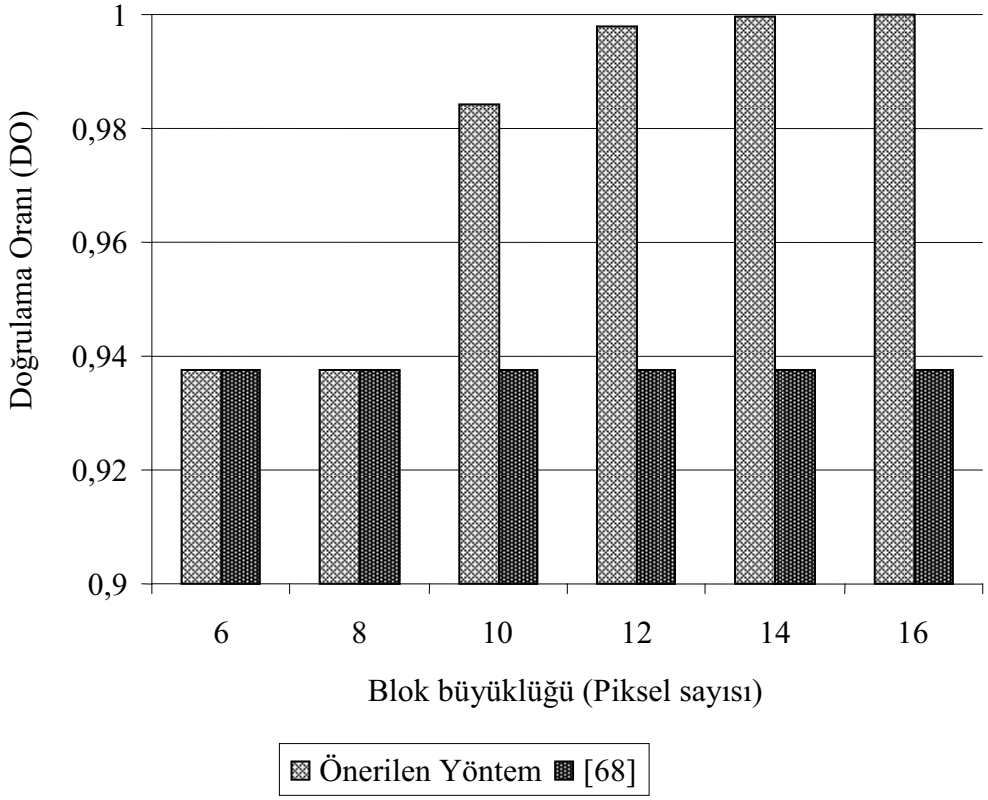


(e) *DO* = 1.0

Şekil 3.17. Farklı blok büyüklükleri için önerilen yöntemin doğrulama yeteneğinin ölçülmesi

Yeniden yapılandırma algoritması gizli görüntüyü elde etmeden önce stego görüntüleri doğrulamak zorundadır. Doğrulama prosedürünün başarısını göstermek amacıyla (3.1)'de tanımı verilen doğrulama oranı (*DO*) kullanılmıştır. Chang vd. tarafından 2008 yılındaki çalışmalarında tanımlanan bu oran $[0-1]$ aralığında değer almaktadır. Oranın herhangi bir doğrulama yöntemi için 0 olarak hesaplanması, yalancı stego piksellerin hepsinin yöntem tarafından yanlış bir şekilde doğru olarak yorumlandığı anlamını taşır. Gerçekleştirilen deneyde farklı blok büyüklükleri için (8, 10, 12 ve 14) yöntemin doğrulama yeteneği test edilmiştir. Seçilen blok büyüklüğü aynı zamanda blok başına kullanılacak olan doğrulama biti sayısını da belirler. Yöntem verilen blok büyüklükleri için sırasıyla 4, 6, 9 ve 12 biti doğrulama amacıyla kullanmaktadır. Doğrulama prosedürünün farklı blok büyüklükleri için üretmiş olduğu *DO* değerleri Şekil 3.17(b)-(e)'de verilmiştir. Blok başına dört doğrulama biti kullanıldığı zaman, yalancı stego pikseller 0.93 olasılıkla tespit edilmektedir. Blok büyüklüğünün artışı ile beraber doğrulama oranı da şekilden de gözlemlenebileceği gibi iyileşim gösterir. 9 bitin kullanılması durumunda doğrulama oranı yaklaşık olarak 0.99 civarındadır. Kullanılan bit sayısının 12 olması durumunda ise, yalancı bölge Şekil 3.17(e)'de görüldüğü gibi tam doğrulukla tespit edilir. Deneyde de vurgu yapıldığı gibi önerilen yöntem diğer yöntemlerden farklı biçimde, blok büyüklüğüne bağlı olarak kullandığı doğrulama biti sayısını adaptif olarak belirlemektedir.

Eslami vd.'nin önermiş olduğu yöntem blok büyüklüğünden bağımsız olarak doğrulama için 4 bit kullanır. Tablo 3.7, her iki yöntemin blok büyüklüğüne bağlı olarak doğrulama yeteneğini kıyaslamaktadır. Önerilen yöntemin doğrulama yeteneği adaptif olarak blok büyüklüğü arttıkça iyileşmektedir. Bununla birlikte Eslami vd.'nin yöntemi doğrulama oranı açısından blok büyüklüğünden bağımsız olarak sabit kalmaktadır. Blok büyüklüğünün 14 olması durumunda, önerilen yöntem 12 doğrulama bitinin kullanımı ile yaklaşık 50 dB PSNR'ye sahip stego görüntüler üretebilmektedir. Eslami vd.'nin yöntemi ise 4 doğrulama biti ile beraber 52 dB PSNR'ye sahip stego görüntüler oluşturur. Blok büyüklüğüne bağlı olarak her iki yöntemin üretmiş olduğu stego görüntülerin PSNR değerleri açısından kıyaslaması Şekil 3.18'de verilmiştir. Önerilen yöntemin doğrulama biti sayısını dinamik olarak belirlemesi, doğrulama ve görsel kalite arasındaki ayrıma kullanıcının karar verebilmesi açısından önem arz etmektedir.



Şekil 3.18. Blok büyüklüğü açısından her iki yöntemin doğrulama oranlarının kıyaslanması

Eslami vd.'nin yöntemlerindeki en belirgin problem, doğrulama prosedürlerinde önermiş oldukları zincir mekanizmasıdır. Yöntemleri, bir önceki blokta yeniden yapılandırılan pay değerinin bir sonraki blokta kullanılmasını gerektirmektedir. Bir önceki bloğun doğrulanmaması durumunda, işlem görmekte olan blok uygun bir şekilde doğrulanamayacaktır. Stego görüntünün doğrulanması esnasında, herhangi bir pikselde değişiklik olması durumunda, geri kalan pikseller değişmemiş olsa dahi doğrulanamaz. Stego görüntüdeki bir pikselde meydana gelen bozulma, geri kalan tüm piksellerin doğrulama prosedürü tarafından değiştirilmiş olarak yorumlanmasına sebep olur.

Şekil 3.19'da önerilen yöntemin ve Eslami vd.'nin yönteminin doğrulama prosedürlerinin sonuçları blok büyüklüğü 8 iken verilmiştir. Eslami vd.'nin çalışması stego görüntünün yalnızca üst tarafı değişmiş olsa dahi tüm stego görüntüyü değişmiş olarak algılamaktadır. Şekil 3.19(a)'da görüldüğü gibi, doğru olan stego bloklar bile yöntem tarafından değiştirilmiş olarak algılanmaktadır. Eslami'nin çalışmasının üretmiş olduğu *DO* değeri $512 \times 512 / 208 \times 512 \cong 2.4$ olarak hesaplanmaktadır. Oysaki *DO* değerinin 1'den

büyük olamayacağı bilinmektedir. Değiştirilmiş stego piksel sayısı 208×512 iken yöntemleri 512×512 adet pikseli değiştirilmiş olarak algılar. Önerilen yöntem ise Şekil 3.19(b)'de gözlemlenebileceği gibi değiştirilmiş stego blokları 0.93 olasılıkla tespit etmektedir. Değiştirilmeyen stego bloklar yöntem tarafından doğrulanmakta ve karşılık düşen gizli görüntüdeki piksel değerleri uygun olarak yeniden yapılandırılmaktadır. Fakat Eslami'nin yöntemi tek bir pikselde değişim olması durumunda, resmin geri kalanını doğrulayamamaktadır.

(a) (b)

Şekil 3.19. Önerilen yöntemin ve Eslami vd.'nin çalışmasının blok büyüklüğü 8 iken doğrulama yeteneklerinin karşılaştırılması

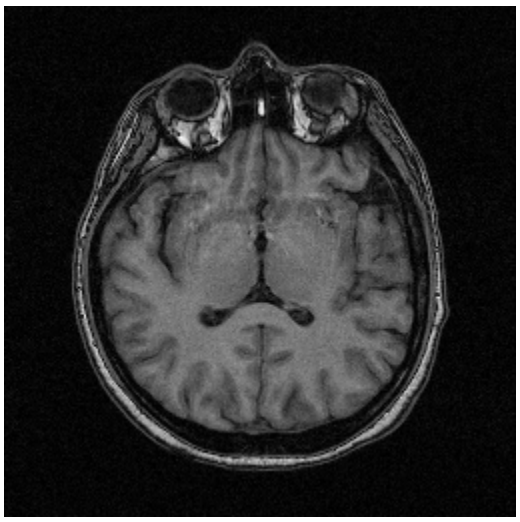
Bir sonraki bölümde gizli görüntünün medikal görüntü olarak seçilmesi durumunda önerilen gizli görüntü paylaşım şemasının irdelenmesi gerçekleştirilecek ve literatürdeki medikal görüntü güvenliğini sağlamaya çalışan yaklaşımlardan olan farklılıklar ve üstünlükler ortaya konacaktır.

3.5. Medikal Görüntü Güvenliğinin Sağlanmasında Önerilen Gizli Görüntü Paylaşım Şemasının Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Devlet politikaları açısından önem taşıyan kişilerin medikal görüntülerinin tek bir kişi tarafından gözlemlenmesi ve bilgi elde edilmesi çoğu zaman ülke güvenliği açısından istenmeyen bir durumdur. Önem taşıyan kişilere ait gizli medikal görüntülerin n kişi

arasında paylaştırılması ve ancak *k* tane hekimin bir araya gelmesi sonucu, konsültasyonun gerçekleştirilmesi, yapılan çalışmalar kısmında da bahsedildiği gibi tez çalışmasında önerilmiştir. Literatürde var olan yöntemler medikal görüntü güvenliğinin sağlanmasında, iki farklı unsuru iyileştirmeye çalışmaktadır: Görüntünün gizliliğinin sağlanması ve elektronik hasta kaydının gizli görüntü içerisine saklanması. Önerilen yöntem, var olan çalışmalardan farklı olarak her iki unsuru aynı anda sağlamakta ve tek kişiye güven yerine gruba güven prensibine dayanmaktadır. Elektronik hasta kaydını medikal görüntü ile beraber ileten, medikal görüntü gizliliğini sağlayan ve gruba güven prensibini gerçekleştiren literatürdeki ilk çalışma özelliğini taşımaktadır. Önerilen yöntemin kullanımı ile elde edilen deneysel sonuçlar ve irdelenmesi bu bölümde gerçekleştirilmektedir.

Deneylerin gerçekleştirilmesinde gizli medikal görüntü olarak Şekil 3.20(a)'da verilmiş olan 256×256 büyüklüğündeki 12 bit gri seviye manyetik rezonans (MR) görüntüsü kullanılmıştır. Şekil 3.20(b)'de ise medikal görüntü ile ilişkili elektronik hasta kayıt bilgisi yer almaktadır.



(a)

FARABI HASTANESİ
Hasta ismi: Ayse Gokturk
Dogum tarihi: 18-08-1980
Yas: 30
Adres: ---
Ağırlık: 60 kg.
Kan basıncı: Normal
Teşhis: Sara

(b)

Şekil 3.20 (a) 256×256 büyüklüğündeki gizli medikal görüntü (b)Elektronik hasta kaydı

(3, 4) gizli görüntü paylaşım şeması, medikal görüntünün dört hekim arasında paylaştırılması esnasında doğal görünümlü pay görüntülerinin oluşturulması için kullanılmaktadır. Konsültasyon için herhangi üç ya da dört doktorun bir araya gelmesi

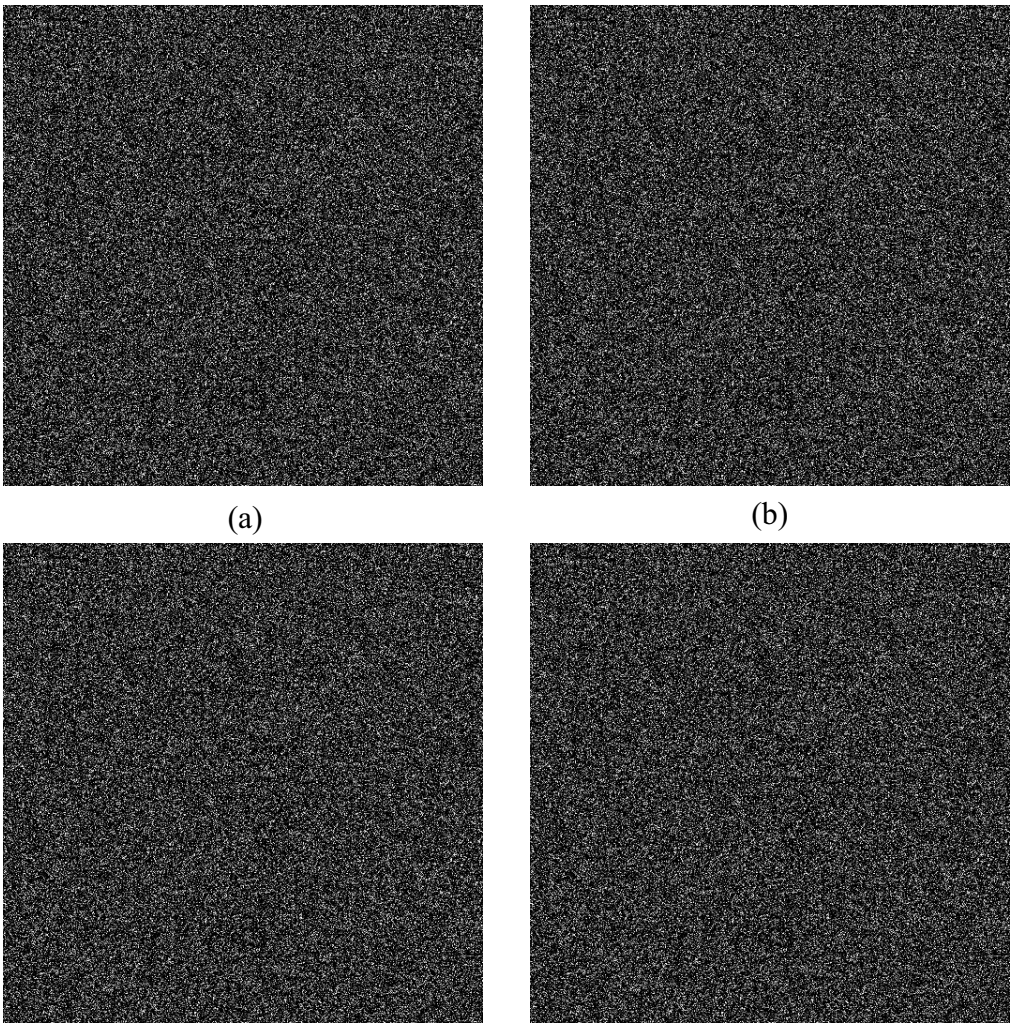
sonucunda ancak gizli medikal görüntü yeniden yapılandırılabilmektedir. Üçten daha az hekimin bir araya gelmesi durumunda, medikal görüntü ya da elektronik hasta kaydı hakkında herhangi bir bilgi elde edinilemez. Medikal görüntünün siyasi ya da askeri bir lidere ait olması durumunda, böyle bir güvenlik mekanizması önem arz etmektedir. Shamir'in şeması medikal kaydın incelenebilmesi için en az üç doktorun bir araya gelmesi zorunluluğunu gerektirir. İletim esnasında pay görüntülerinin kötü niyetli kişilerin ilgisini çekmemesi için dört adet doğal görünümlü görüntü seçilmektedir. Hu ve arkadaşlarının 2009'da yapmış oldukları çalışmada medikal görüntüden üretilen şifreli görüntü gürültü özelliği taşımaktadır [142].

Yüksek entropi ve gürültü benzeri görüntüler, şifrelemenin bir göstergesidir ve kötü niyetli kişilerin ilgisini çekmektedir. Önerilen yöntem, gürültü benzeri pay görüntülerini anlamlı örten görüntüler içerisine Steganografi kullanarak saklar. Böylece Hu vd.'nin metodundaki risk ortadan kaldırılmıştır. Yapılan çalışmalar kısmında anlatılan paylaştırma ve gömme algoritmaları dört adet gürültü benzeri pay görüntüsü üretir. Paylaştırma sonucu elde edilen pay görüntüleri Şekil 3.21'de verilmektedir.

Gömme prosedürü pay görüntülerini örten görüntüler içerisine saklar. OPAP metodu örten görüntülerdeki değişimi azaltmak amacıyla gömme işlemi esnasında kullanılmaktadır. Pay görüntüsünün her bir pikseli, örten görüntüdeki 2×2 büyüklüğündeki örten bloklara gömülür. Böylece medikal görüntünün boyutlarının $M \times N$ olması durumunda örten görüntünün en az $2N \times 2M$ büyüklüğünde olması gerekir. Şekil 3.22'de verilmiş olan 8 bit gri seviye, 512×512 büyüklüğündeki 'window', 'house', 'lighthouse' ve 'parrots' isimli test görüntüleri örten görüntü olarak seçilmiştir.

Stego görüntüler pay görüntülerinin örten görüntüler içerisine saklanması sonucunda oluşmaktadır. Stego görüntülerin görsel kalitesini test etmek amacıyla PSNR değeri kullanılmıştır. Şekil 3.23, yöntemin uygulanması sonucu elde edilen stego görüntüleri PSNR değerleri ile beraber vermektedir. Stego görüntüler için hesaplanan ortalama PSNR değerleri yaklaşık olarak 46.3 dB civarındadır. Gömme prosedürü geleneksel LSB'ye gömme tekniği kullansaydı ortalama PSNR değeri 44 dB civarlarında olurdu. OPAP metodunun kullanılması stego görüntülerin PSNR değerlerini iyileştirmiştir. Şekil 3.23'te verilmiş olan stego görüntüler dört hekim arasında dağıtılır.

Her hekim kendisi ile ilişkili bir pay görüntüsüne sahip olsa bile, hekimlerin herhangi biri hasta hakkında tüm bilgiye sahip olamaz. Hu vd.'nin metodu medikal görüntünün gizliliğini sağlayabilmek amacıyla karıştırma fonksiyonu kullanmıştır.



(a) (b)

(c) (d)

Şekil 3.21. Gizli görüntünün (3, 4) şeması kullanılarak paylaştırılması ve elektronik hasta kaydının saklanması sonucunda elde edilen pay görüntüleri

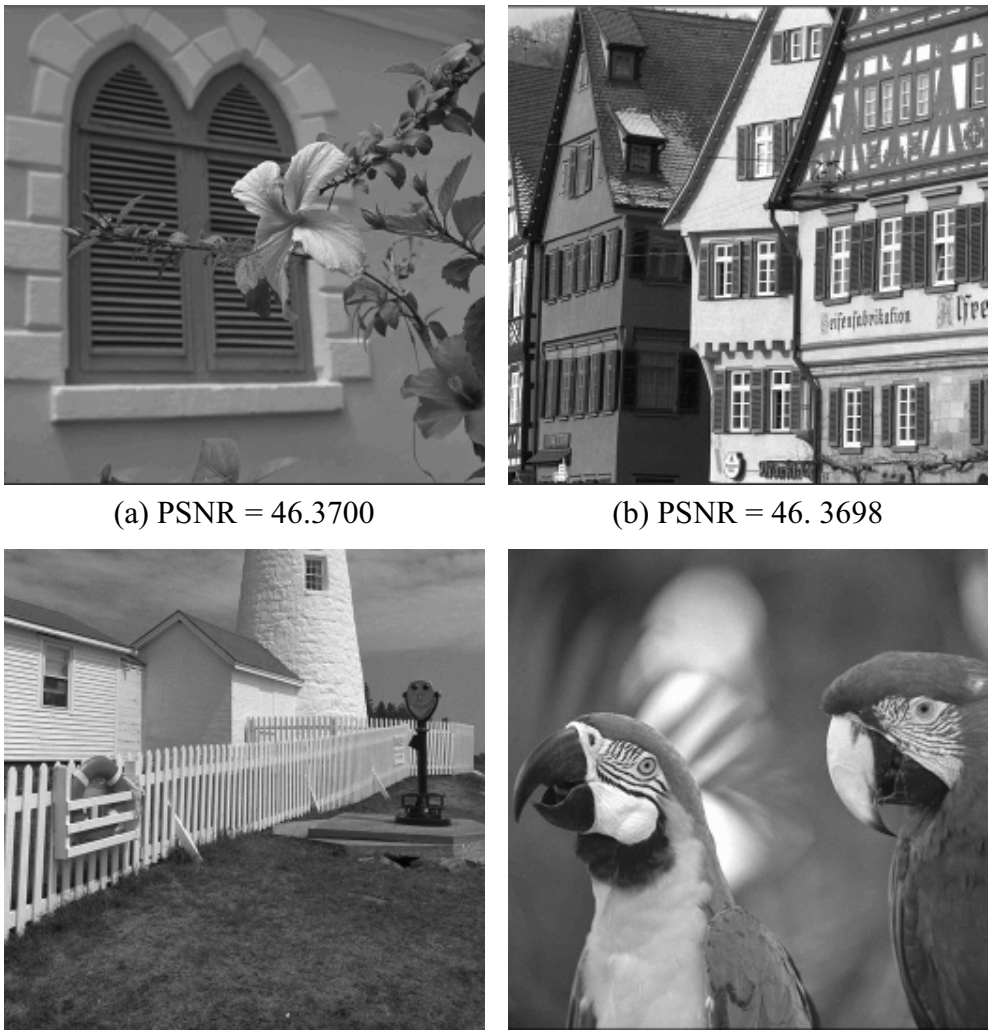
Fakat karıştırma fonksiyonu sonuçta gürültü şeklinde görüntüler üretmektedir. Ağ üzerinden gürültü benzeri görüntülerin iletimi kötü niyetli kişilerin ilgisini çekmektedir. Önerilen yöntem pay görüntülerini örten görüntüler içerisine saklamakta, stego görüntülerde herhangi bir değişim olması durumunda medikal görüntü veya hasta kaydı hakkında herhangi bir bilgi açığa çıkarmamaktadır. Diğer yandan, *n*-*k* pay bozulsa bile, gizli görüntü ve hasta kaydını bozulmayanları kullanarak elde etmek mümkün olacaktır. Bu da yöntemin aynı zamanda hata toleranslı olduğunu göstermektedir. Hu vd.'nin yöntemi yalnızca medikal görüntünün gizliliği ile ilgilenmiş, elektronik hasta kaydının iletimini tamamen göz ardı etmiştir. Yeniden yapılandırma prosedürü esnasında, önerilen yöntem medikal görüntü ve hasta kayıt bilgisini elde edebilmek amacıyla Lagrange'ın

interpolasyonunu kullanmaktadır. Medikal görüntü ve hasta kayıt bilgisini dört hekimden herhangi üç tanesinin bir araya gelmesi sonucunda elde edilebilecektir.

Şekil 3.22. Pay görüntülerinin saklanması için seçilen örten görüntüler

Ardından, elde edilen veriler kullanılarak hekimler konsültasyon yapabilir. Şekil 3.24(a) ve 3.24(b), yeniden yapılandırılan medikal görüntüyü ve hasta kayıt bilgisini göstermektedir. Önerilen yöntemin medikal görüntü ile iletebilecek olduğu hasta kayıt bilgisindeki karakter sayısı üç faktöre bağlıdır. Birinci faktör seçilen eşik değeri *k*'dır. Medikal görüntünün büyüklüğü ikinci faktördür. Son faktör ise medikal görüntünün bit derinliğidir. Hasta kaydının sahip olabileceği karakter sayısı (*KS*) her üç faktörden de etkilenmektedir. $N \times M$ büyüklüğündeki medikal görüntü için *KS* değeri (3.5)'te verilmiştir.

$$KS = \frac{(NM)}{k}\left(k - \left\lceil \log_{251} 2^{b} \right\rceil\right) \tag{3.5}$$



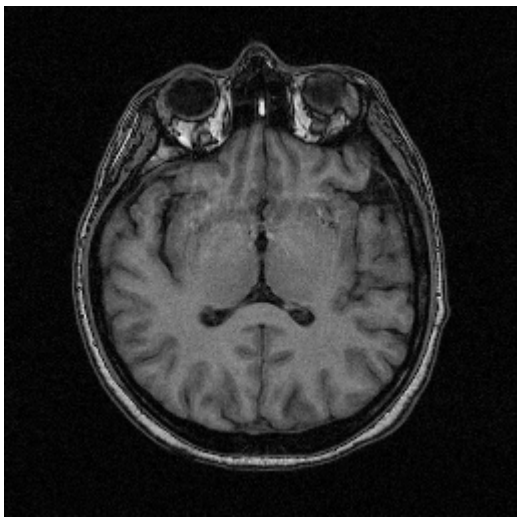
(a) PSNR = 46.3700 (b) PSNR = 46. 3698

(c) PSNR = 46.3702 (d) PSNR = 46.3691

Şekil 3.23. Gizli görüntü ve elektronik hasta kaydının paylaştırılması sonucu elde edilen stego görüntüler ve PSNR değerleri

Yapılan testte (3, 4) şeması ile birlikte kullanılan medikal görüntü 12 bit derinlikte 256×256 büyüklüğündeki bir MR görüntüsü olduğu için, Shamir'in polinomundaki ilk iki katsayı piksel değerini kodlamada kullanılmıştır. Üçüncü dereceden bir polinom kullanıldığından dolayı, geriye kalan katsayı hasta kaydındaki bir karakterlik bilgiyi kodlamaktadır. Böylece ilk deney için hesaplanan *KS* değeri 21845'dir. Nayak'ın 2009'daki çalışmasında elektronik hasta kaydını medikal görüntüye yerleştirmek için geri döndürülebilir steganografinin kullanılmasını önermiştir [139]. Medikal görüntü içerisine

gömülebilecek bit miktarı, medikal görüntünün histogramındaki zirve noktasındaki parlaklık değerine sahip piksel sayısı ile orantılıdır. Nayak'ın rapor ettiği değerlere göre aynı büyüklükteki medikal görüntüye saklayabilecek olduğu karakter sayısı 14510 olmaktadır. Önerilen yöntem Nayak vd.'nin metodu ile kıyaslanınca daha uzun hasta kayıt bilgisi saklayabilmektedir. Lou vd.'nin metodu hasta kayıt bilgisini saklayabilmek amacıyla çok seviyeli veri saklama yöntemini kullanmıştır. Birinci katman için saklayabilecekleri karakter sayısı 14863 olarak rapor edilmiştir [141]. Vurgu yapıldığı gibi önerilen yöntem diğer yöntemlere kıyasla daha uzun hasta kayıt bilgisi saklayabilmektedir.



FARABI HASTANESİ
Hasta ismi: Ayse Gokturk
Dogum tarihi: 18-08-1980
Yas: 30
Adres: ---
Ağırlık: 60 kg.
Kan basıncı: Normal
Teşhis: Sara

Şekil 3.24. Yeniden yapılandırılan gizli medikal görüntü ve elektronik hasta kaydı

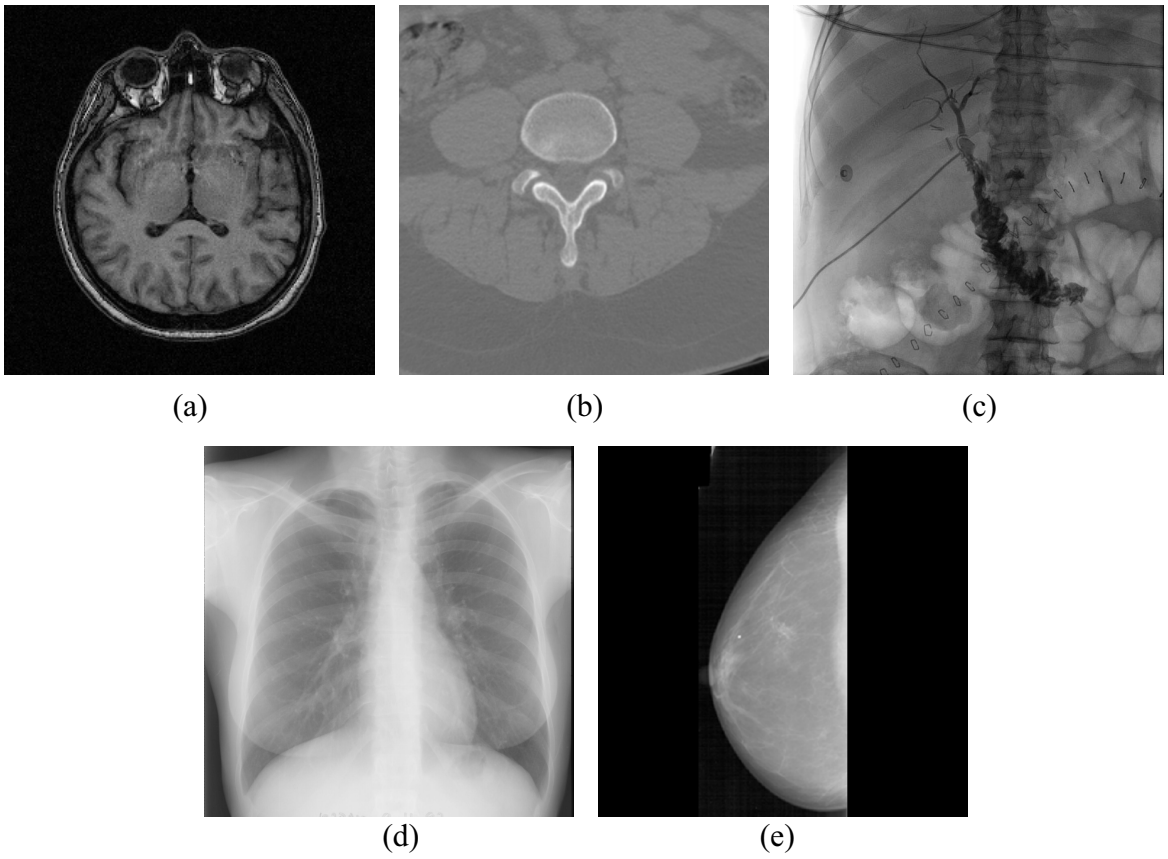
Medikal görüntülerin temsilinde farklı çözünürlükte resimler kullanılmaktadır. $M \times N \times b$ bit büyüklüğündeki iki boyutlu (2D) medikal görüntü, yükseklikte M piksele, genişlikte ise N piksele sahiptir. Görüntüleme için 2^b gri seviye kullanılmaktadır. Tablo 3.8 farklı medikal görüntüleme teknolojilerinde üretilen ortalama görüntü boyutlarını MB cinsinden vermektedir [154]. Medikal görüntünün bit derinliği ve çözünürlüğünün çalışma zamanı üzerine etkisi aşağıda incelenmiştir. Medikal görüntünün bit derinliği çalışma zamanını etkilemeyecektir. Bit derinliği dağıtıcının seçecek olduğu eşik değerinin alt sınırını belirlemektedir $k > \lceil \log_{251} 2^b \rceil$. (3.5)'te görüldüğü gibi bit derinliği aynı zamanda hasta kayıt bilgisindeki olabilecek karakter sayısını da etkilemektedir. 8, 10, 12 bit derinliğindeki medikal görüntüler Shamir'in polinomunun ilk iki katsayısının piksel temsilinde kullanılmasını gerektirir. Geriye kalan k-2 katsayı ise hasta kayıt karakterlerini

kodlamada kullanılır. Aynı şekilde 16 bit medikal görüntü polinomun ilk üç katsayısını piksel temsilinde kullanırken, eşik değerinin üçten büyük olması gerekmektedir. Yüksek bit derinlikleri Shamir'in polinomunda piksel değerini kodlamak için daha çok katsayının kullanılmasını gerektirir. Sonuç olarak, bit derinliği arttıkça polinomun daha az katsayısı hasta kayıt bilgisindeki karakterleri tutmak için kullanılır. Yeni bir ölçüm birimi olarak piksel başına düşen gömme kapasitesi ($PBGK = KS/NM = 1 - \lceil \log_{251} 2^b \rceil / k$) (3.5)'te verilen ifade kullanılarak türetilmiştir. Sabit bir k değeri için, piksel başına gömme kapasitesi bit derinliğinin artması ile beraber azalmaktadır. Örneğin 8, 10, 12 bit resimler için $PBGK$ değeri $1-\frac{2}{k}$ iken, 16 bit medikal görüntüler için bu değer $1-\frac{3}{k}$'ya düşmektedir.

Tablo 3.8. Farklı görüntüleme tekniklerindeki görüntü boyutları

Görüntüleme Türü	**Görüntü boyutu (piksel)**	**Gri Seviye (bit)**	**Ortalama büyüklük(Mbyte)**
(PET, SPECT)	128×128	12	1-2
MRI	256×256	12	8-20
Ultrason	512×512	8	5-10
CT	512×512	12	20-40
Spiral veya helikal CT	512×512	12	80-160
Dijital elektronik mikroskopi	512×512	8	Değişken
Dijital renkli mikroskopi	512×512	24	Değişken
Dijital anjiografi	512×512 veya 1024×1024	8	100-500
X-ray	2048×2048	12	8
CR	2048×2048	12	8
Mamografi	4096×4096	12	128 (4 görüntü)

Görüntü çözünürlüğünün koşma zamanı üzerine etkisi farklı görüntüleme teknikleri kullanılarak test edilmiştir. 12 bit 256×256 MR, 12 bit 512×512 Bilgisayarlı Tomografi (CT), 12 bit 1024×1024 Floroskopik görüntü, 12 bit 2048×2048 Bilgisayarlı Radyografi (CR) ve 12 bit 4096×4096 Mamografik görüntü koşma zamanı etkisini incelerken kullanılmıştır. Şekil 3.25'te kullanılacak olan test görüntüleri verilmiştir [155, 156]. Bütün çözünürlüklerdeki koşma zamanı ayrık k değerleri için Şekil 3.26'da gösterilmektedir.

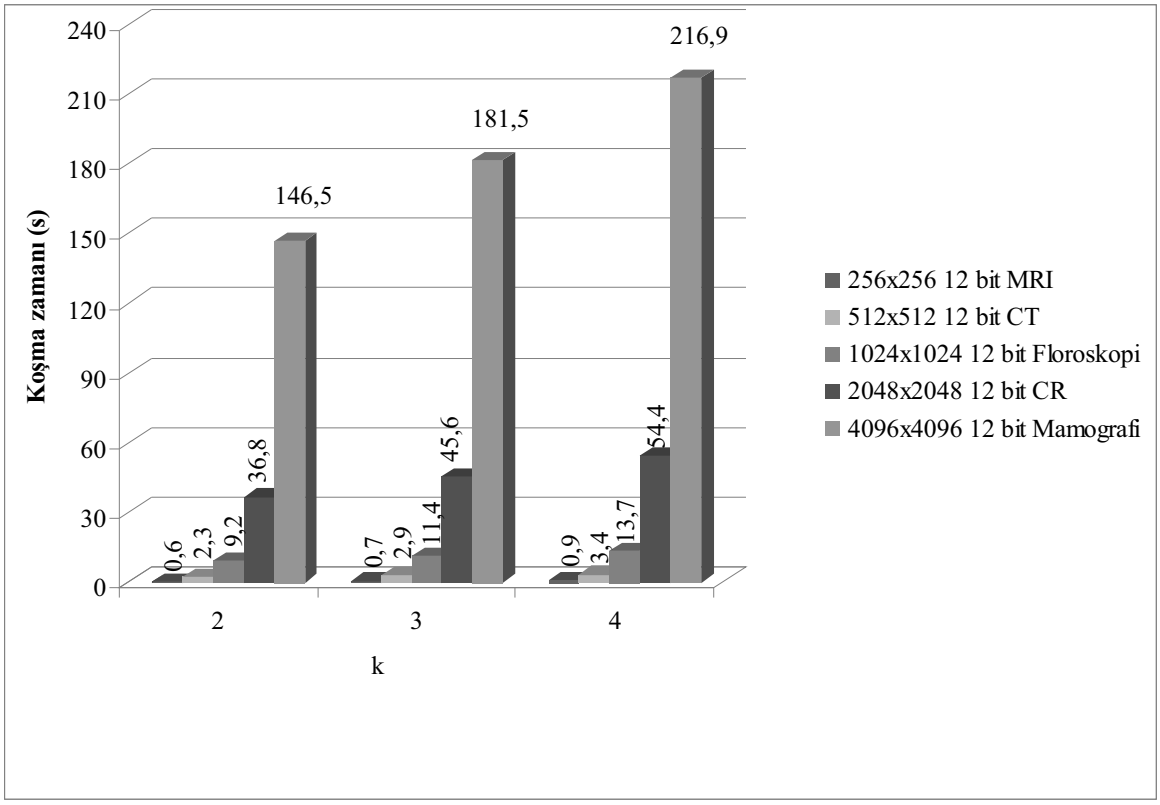


(a) (b) (c)

(d) (e)

Şekil 3.25. (a) 12 bit 256×256 MR (b) 12 bit 512×512 CT (c) 12 bit 1024×1024 Floroskopik görüntü (d) 12 bit 2048×2048 CR(e) 12 bit 4096×4096 Mamografik görüntü

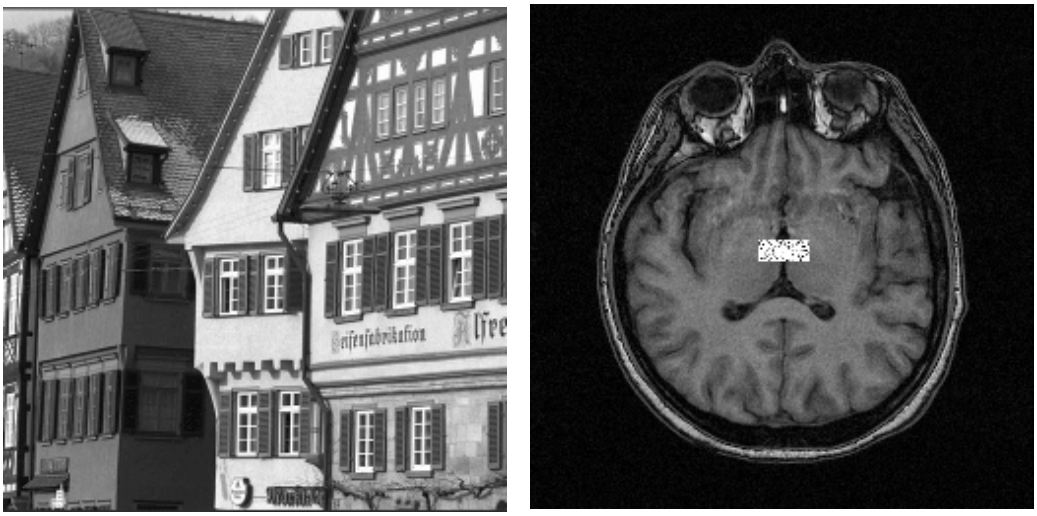
Grafikten lineer orantısal bir artış gözlemlenmektedir. Grafikten de görüldüğü gibi medikal görüntünün çözünürlüğü koşma zamanı üzerinde etkilidir. Aynı görüntü için daha büyük k değerlerinde de işlem zamanının arttığı gözlemlenmektedir. Çünkü polinomum belirlenmesinde kullanılan Lagrange interpolasyon yöntemi seçilen k değerine bağlıdır. Örneğin, yeniden yapılandırma algoritması 12 bit 2048×2048 CR görüntülerde k=3 değeri ile beraber 45.6 saniye koşarken, k=2 değeri için aynı süre 36.8 olarak ölçülmektedir. Önerilen yöntemin doğrulama yeteneğinin testi bu bölümdeki son deneydir. Medikal görüntülerin damgalanması literatürdeki çalışmalarda en çok tercih edilen yöntemdir. Ho ve arkadaşları 2005 yılında yapmış oldukları çalışmada nazik damgalama yöntemini doğrulama amaçlı kullanmışladır [138]. Nazik damgalama yöntemi, verinin bütünlüğünü garanti eder. Fakat damga bilgisi ile üretmiş oldukları medikal görüntüye ilişkin PSNR değeri çalışmalarında 40 dB olarak rapor edilmiştir. Bu da damganın çıkartılmasından sonra medikal görüntü de ciddi bir bozulma olduğunun göstergesidir.



Şekil 3.26. Farklı çözünürlüklerdeki ayrık *k* değerleri için koşma zamanı

Bunun yanında çalışmalarında, medikal görüntü içerisine hasta kayıt bilginsin saklanmasının üzerinde durmamışlardır. Önerilen yöntem medikal görüntülerin doğrulamasını iki faktör ile sağlamaktadır. Shamir'in yaklaşımı ve stego görüntüler hakkında özet bilgi içeren sertifikalar, önerilen yöntemin doğrulamada kullandığı mekanizmalardır. Lagrange'ın interpolasyon yöntemi herhangi bir bozulma durumunda polinomun yanlış katsayılarla yapılanmasını sağlayacak ve yeniden yapılandırılan görüntü de bozulmalara sebep olacaktır. Bu özellik yeniden yapılanan görüntüyü doğrulamada kullanılabilir. Şekil 3.27(a) ve 3.27(b)'de kısmi olarak değiştirilmiş bir pay görüntüsü ve üretilen yeniden yapılandırılmış görüntü verilmiştir. Yeniden yapılandırılan medikal görüntüdeki gürültülü alanlar, pay görüntülerinden birinde ağ üzerinden iletimi esnasında bozulma yaşandığını göstermektedir. İkinci faktör stego görüntüleri doğrulamada kullanılan sertifikalardır. Doğrulama prosedüründe, her katılımcı kendi pay görüntüsünü ve x_k değerini kullanarak özüt değerini hesaplamaktadır. Dağıtıcı da koruma prosedüründe hesaplamış olduğu değeri sertifika içerisine gömmüştür. Katılımcının doğrulama aşamasında hesapladığı değer ile sertifikadaki değer aynı ise stego görüntü doğrulanır.

Kötü niyetli bir kişi yalancı bir pay görüntüsünü yalancı bir sertifika ile beraber oluşturamaz, çünkü katılımcı ile ilişkilendirilmiş olan x_k değerini bilmemektedir.



(a) (b)

Şekil 3.27. Değiştirilen stego görüntü ve yeniden yapılandırılan medikal görüntü

Bir sonraki bölümde, var olan Shamir tabanlı gizli görüntü paylaşım şemalarından farklı olarak, yeni bir gizli görüntü paylaşım şemasının değerlendirilmesi ve elde edilen deneysel sonuçlar verilmektedir.

3.6. Morley'in Teoremine Dayanan Gizli Görüntü Paylaşım Şemasının Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

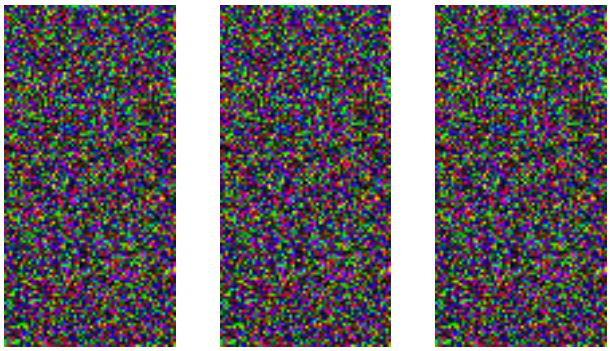
Literatürde var olan gizli görüntü paylaşım şemaları ağırlıklı olarak Shamir'in sır paylaşım yöntemini kullanmakla beraber, son yıllarda Blakley'in yaklaşımını tercih eden çalışmalarda mevcuttur. Gizli görüntü paylaşımında var olan eşik şemalarının kullanımı yazarlar tarafından tercih edilmektedir. Yapılan çalışmalar kısmında da bahsedildiği gibi, tez çalışmasında, Morley'in üçgen teoremini kullanarak gizli görüntülerin paylaşımını gerçekleştiren yeni bir teknik önerilmiştir. Morley'in üçgen teoremi, herhangi bir üçgenin üçe bölenlerinin kesişiminin eşkenar bir üçgen oluşturduğuna vurgu yapmaktadır. Oluşan eşkenar üçgenin kenar ve yönlenim bilgisinin gizli veriyi kodladığını varsayan çalışma, dış üçgenin koordinatlarını pay değeri olarak belirlemektedir. Önerilen ve var olan eşik şemalarından bağımsız olarak geometrik yöntemleri gizli görüntünün paylaştırılmasında

kullanan şemaya ilişkin deneysel sonuçlar ve gerçekleştirilen irdelemeler bu bölümde verilecektir. 128×128 büyüklüğündeki Şekil 3.28'de verilmiş olan gri seviye Lena görüntüsü gizli görüntü olarak kullanılmıştır. Önerilen yöntem gizli görüntüyü Morley teoremini kullanarak üç pay görüntüsüne parçalamaktadır. Gizli görüntü iki pikselden oluşan gruplara ayrılmakta ve üretilen pay değerleri, karşılık düşen pay görüntüsündeki renkli piksele kodlanmaktadır. Bu nedenle üretilen renkli pay görüntü büyüklüğü 128×64 olarak tespit edilmiştir. Önceki bölümde anlatıldığı gibi gizli görüntüdeki piksel grubu, Morley üçgenine ait kenar ve x eksenine göre yönlenim bilgisini içermektedir. Karşılık düşen pay görüntüdeki piksel değerleri ise, dış üçgenin köşe koordinatlarını barındırmaktadır. Böylece, pay görüntülerinden herhangi birinin tek başına bir anlam ifade etmeyeceği rahatlıkla söylenebilir. Bir adet pay görüntüsü dış üçgene ait tek bir köşe bilgisi içerirken, iki adet pay görüntüsü üçgene ait yalnızca bir kenarın bilinmesine sebep olacaktır. Kenar bilgisini kullanarak gizli veriyi barındıran Morley üçgenini yapılandırmak mümkün olmayacaktır. Önerilen yöntem gizli görüntünün yeniden yapılandırılabilmesi için her üç pay görüntüsünü de gerektirmektedir. İlk deneyde gizli görüntü üç katılımcı arasında paylaştırılmıştır. Üretilen 128×64 büyüklüğündeki pay görüntüleri Şekil 3.29'da verilmiştir. Pay görüntüleri gürültü özelliği taşımakta ve gizli görüntü hakkında herhangi bir bilgi içermemektedir. Ancak şekilde verilen üç pay görüntüsünün bir araya gelmesi sonucu gizli görüntü yeniden yapılandırılabilecektir. Yeniden yapılandırma sürecinde, pay görüntülerindeki piksel parlaklık değerleri Morley üçgenini yapılandırmada kullanılır.

Şekil 3.28. 128×128 büyüklüğünde gri seviye gizli görüntü

Fakat dış üçgenin köşe koordinatlarının reel olmasına rağmen paylaştırma sürecinde tamsayıya çevirmek için gerçekleştirilen yuvarlama işlemleri yeniden yapılandırılan gizli görüntüde bazı hataların oluşumuna sebep olmaktadır. Morley üçgenine ait kenar ve

yönlenim bilgisi ± 1 piksellik hatalarla elde edilebilir. Bu nedenle deneysel sonuçlarda elde edilen gizli görüntünün PSNR ölçümü gerçekleştirilmiştir.



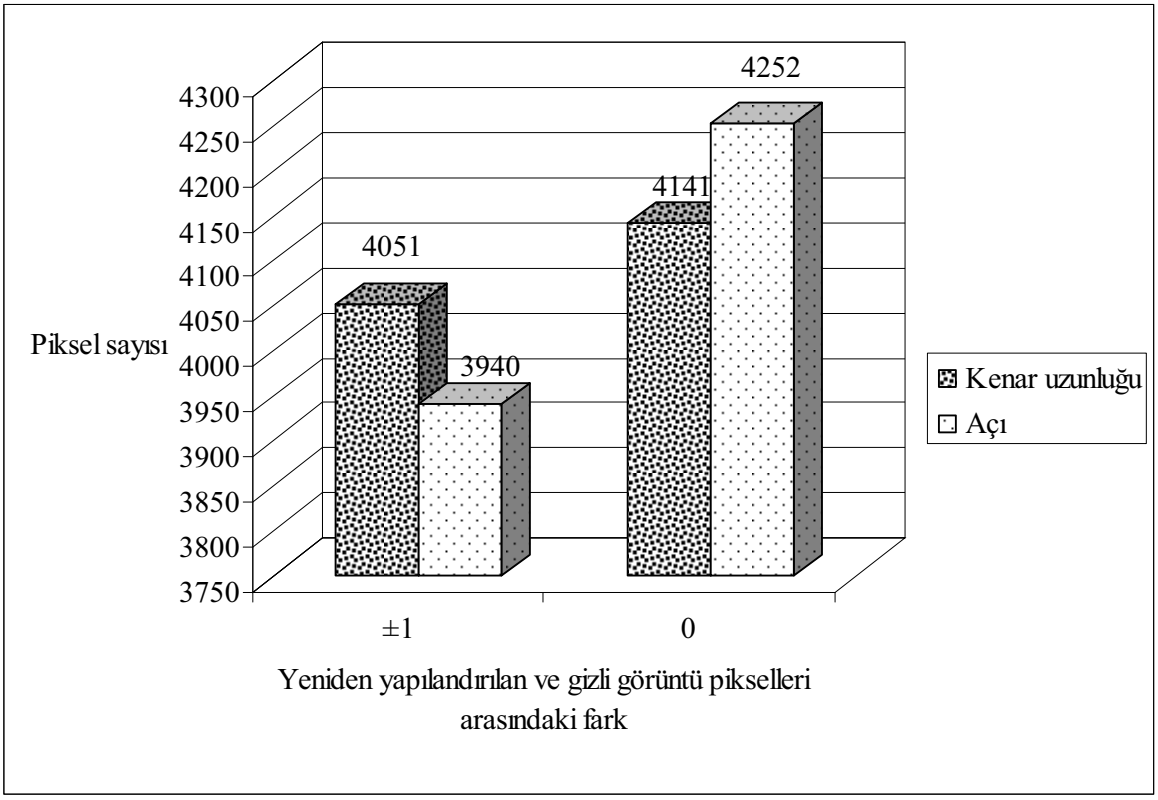
Şekil 3.29. 128×64 büyüklüğündeki pay görüntüleri

Gizli görüntü ve yeniden yapılandırılan gizli görüntü sırasıyla S, S' ile temsil edilmektedir. Yapılan testlerde yeniden yapılandırılan gizli görüntünün yaklaşık olarak 50.39 dB PSNR'ye sahip olduğu tespit edilmiştir. Literatürdeki çalışmalarda $[40, \infty)$ dB aralığında PSNR'ye sahip görüntülerin iyi bir görsel kaliteye sahip olduğuna vurgu yapılmaktadır. Böylece Şekil 3.30'da verilen yeniden yapılandırılan gizli görüntünün iyi bir görsel kaliteye sahip olduğu söylenebilir.

Diğer bir deney ise yeniden yapılandırma esnasında meydana gelen hata sayısını tespit etmek amacıyla gerçekleştirilmiştir. Şekil 3.31'den de gözlemlenebileceği gibi gizli görüntüdeki 128×128=16384 pikselin yarısı Morley üçgenlerinin kenar bilgisini taşırken diğer yarısı ise yönlenim bilgilerini içermektedir. Kenar bilgilerinin 4051 tanesi mutlak 1 farkla yapılandırılırken, açı bilgisinin 3940 tanesi mutlak 1 farkla elde edilmektedir.

Önerilen Morley tabanlı gizli görüntü paylaşım şemasını diğer yöntemlerden ayıran en önemli fark, pay görüntülerinde meydana gelen bozulmalara karşı yöntemin dayanıklı olmasıdır. Shamir'in eşik şemasını kullanan yöntemler, gizli görüntünün yeniden yapılandırılmasında, Lagrange'ın interpolasyonundan faydalanmaktadır. Gizli görüntü piksel parlaklık değerleri, yeniden yapılandırılacak polinomun katsayı değerlerinden elde edilir. Yeniden yapılandırmada kullanılan noktalardaki (pay değerlerinde karşılık düşen piksel parlaklık değerleri) bozulmalar, polinomun doğru bir şekilde yapılandırılamamasına neden olmaktadır.

Şekil 3.30. 50.39 dB PSNR'ye sahip yeniden yapılandırılan gizli görüntü



Şekil 3.31. Yeniden yapılandırma esnasında meydana gelen yuvarlama hataları

Hatalı olarak yapılandırılan polinom ise gizli görüntünün yeniden elde edilememesine sebebiyet vermektedir. Blakley'in şemasını kullanan gizli görüntü paylaşım şemaları da benzer problemlerden etkilenmektedir. Yeniden yapılandırma aşamasında lineer denklik sisteminin çözümünde, farklı pay görüntülerinden gelen değerleri kullanan şemalar, bozulmalara karşı dayanıklı değildir. Pay görüntülerinin herhangi bir şekilde bozulması, gürültüye maruz kalması durumunda gerek Shamir tabanlı gerekse Blakley

tabanlı yöntemler, gizli görüntüyü yeniden yapılandıramaz. Böyle bir durum, özellikle hataya karşı toleransı ile öne çıkan gizli görüntü paylaşım şemaları için bir zayıflık olarak rapor edilebilir. Önermiş olduğumuz Morley'in üçgen teoremini kullanan yöntem, gizli verinin temsilinde, dış üçgenin köşe koordinatlarından faydalanır. Üçgenin köşe noktalarındaki bozulmalar, içteki eşkenar üçgenin (gizli veriyi kodlamada kullanılan) yapılandırılmasında belirli oranda hatalara sebebiyet verse dahi, yeniden yapılandırılan gizli görüntü insan gözü tarafından fark edilebilmektedir. Pay görüntülerinde oluşacak olan hatalara karşı yöntemin dayanıklılığını göstermek amacıyla çeşitli testler gerçekleştirilmiştir. 128×128 büyüklüğündeki Şekil 3.32'de verilmekte olan "girl" isimli test görüntüsü, yöntemin hataya karşı toleransını gösteren deneylerde gizli görüntü olarak kullanılmıştır.

Şekil 3.32. 128×128 büyüklüğündeki test görüntüsü

Verilen görüntünün katılımcılar arasında paylaştırılmasının ardından oluşan pay görüntülerinden birinin JPEG atağına maruz kaldığı varsayılarak çeşitli sonuçlar elde edilmiştir. Öncelikle pay görüntüsü sırasıyla 20, 40, 60, 80, 100 JPEG kalitelerinde kaydedilmektedir. Farklı kalite faktörlerinde pay görüntüsünün sıkıştırılması, pay değerlerinde kayıplara sebep olmaktadır. Shamir ya da Blakley tabanlı yöntemlerde, pay görüntüsündeki böyle bir bozulma, gizli görüntünün yeniden yapılandırılamamasına sebep olmaktadır. Tarafımızdan önerilen yöntemin, pay görüntünün belirtilen kalite faktörlerinde sıkıştırılmasının ardından, üretecek olduğu yeniden yapılandırılmış gizli görüntüler Şekil 3.33'de verilmektedir. Şekil 3.33(a)'da verilen görüntü, pay görüntüsünün 20 kalite faktörü ile sıkıştırılmasının ardından üretilen yeniden yapılandırılmış görüntüdür. Şekil 3.33(e)'de ise pay görüntüsünün bozulmasında kullanılan kalite faktörü 100'dür. Sonuçlardan da gözlemlenebileceği gibi, önerilen yöntem, gizli görüntüyü insan gözünün ayırt edebileceği şekilde yeniden yapılandırmaktadır.


Kalite faktörü=20


Kalite faktörü=40

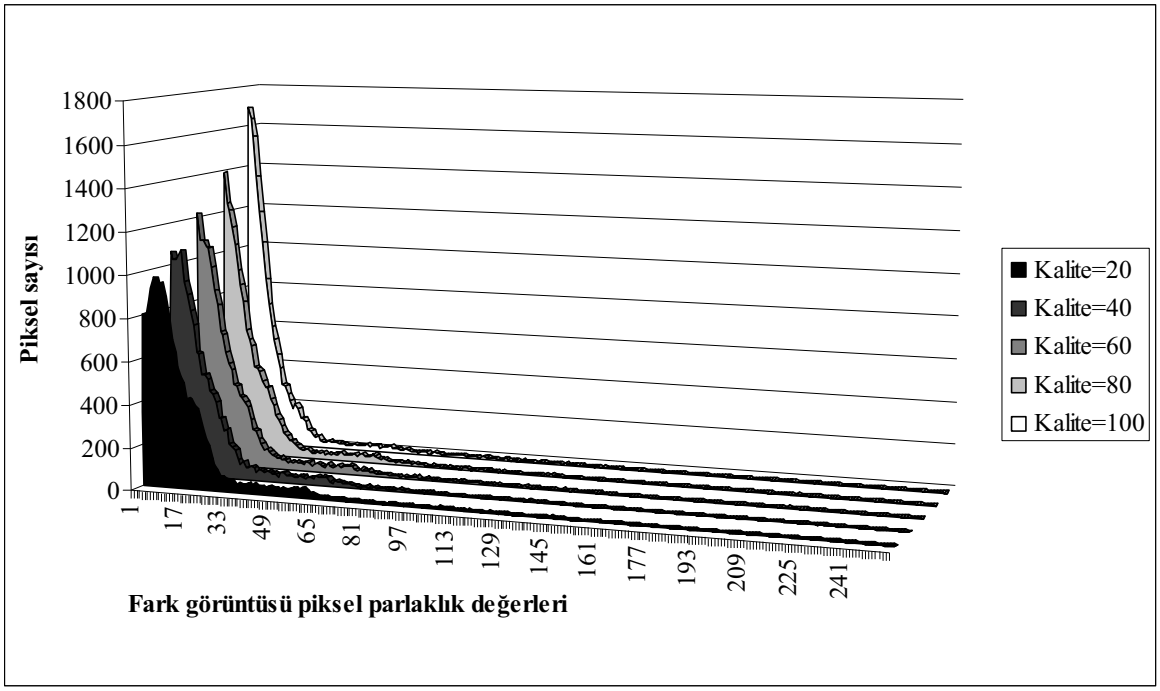

Kalite faktörü=60


Kalite faktörü=80

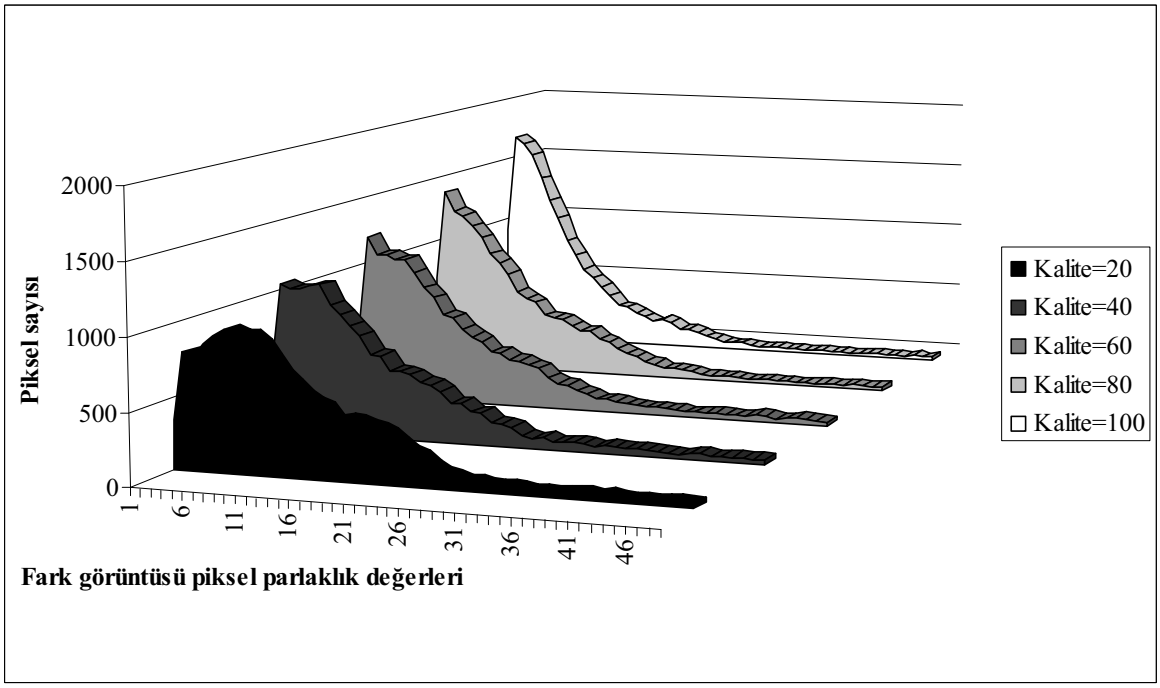

Kalite faktörü=100

Şekil 3.33. Pay görüntüsünün farklı kalite faktörleri kullanılarak sıkıştırılması sonucu elde edilen yeniden yapılandırılan gizli görüntü

Yeniden yapılandırılan gizli görüntü ve orijinal gizli görüntü arasındaki mutlak farkların oluşturduğu görüntü fark görüntüsü olarak adlandırılsın. Fark görüntüsünün histogramı, yöntemin, yeniden yapılandırma esnasındaki başarısı hakkında fikir verecektir. Farklı kalite faktörlerinde sıkıştırılmış pay görüntüleri kullanılarak elde edilen yeniden yapılandırılan görüntülerin oluşturduğu fark görüntülerinin histogramları Şekil 3.34'te verilmektedir. Şekilden de gözlemlenebileceği gibi, sıkıştırma oranı arttıkça, fark görüntüsündeki piksel parlaklık değerlerinin arttığı gözlemlenmektedir. Düşük sıkıştırma oranlarında ise, fark görüntüsündeki piksel parlaklık değerlerinin daha küçük olduğu söylenebilir. Fark görüntüsündeki piksel parlaklık değerlerinin küçük olması (0'a yakınlığı), yeniden yapılandırılan görüntünün, orijinal gizli görüntüye olan benzerliğinin göstergesidir. Şekilden de gözlemlenebileceği gibi, parlaklık değerleri ağırlıklı olarak $[0-20]$ aralığında yer almaktadır. Fark görüntüsünün histogramının incelenmesini kolaylaştırmak amacıyla, histogramın göstermiş olduğu parlaklık aralığı $[0-50]$ olarak değiştirilmiş ve elde edilen grafik Şekil 3.35'te verilmiştir.



Şekil 3.34. Fark görüntülerinin histogramları



Şekil 3.35. Fark görüntülerinin $[0-50]$ aralığındaki histogramlarının görüntülenmesi

Yöntemin hataya karşı dayanıklılığını göstermek için gerçekleştirilen diğer bir deneyde, pay görüntüsüne, farklı varyanslardaki (0.001, 0.004, 0.008) ortalama değeri 0

olan Gauss gürültüsü eklenmiştir. Bozulmuş olan pay görüntüsü kullanılarak elde edilen yeniden yapılandırılmış gizli görüntüler Şekil 3.36'da verilmektedir. Düşük varyanslı gürültünün eklenmesi sonucu oluşan pay görüntüsü kullanılarak yeniden yapılandırılan gizli görüntünün diğerlerine nazaran daha net olduğu insan gözü tarafından ayırt edilebilmektedir. Eklenen gürültünün varyansı artırıldıkça, yeniden yapılandırılan görüntünün görsel kalitesi, şekilden de gözlemlenebileceği gibi düşmektedir.

Varyans=0.001 Varyans=0.004 Varyans=0.008

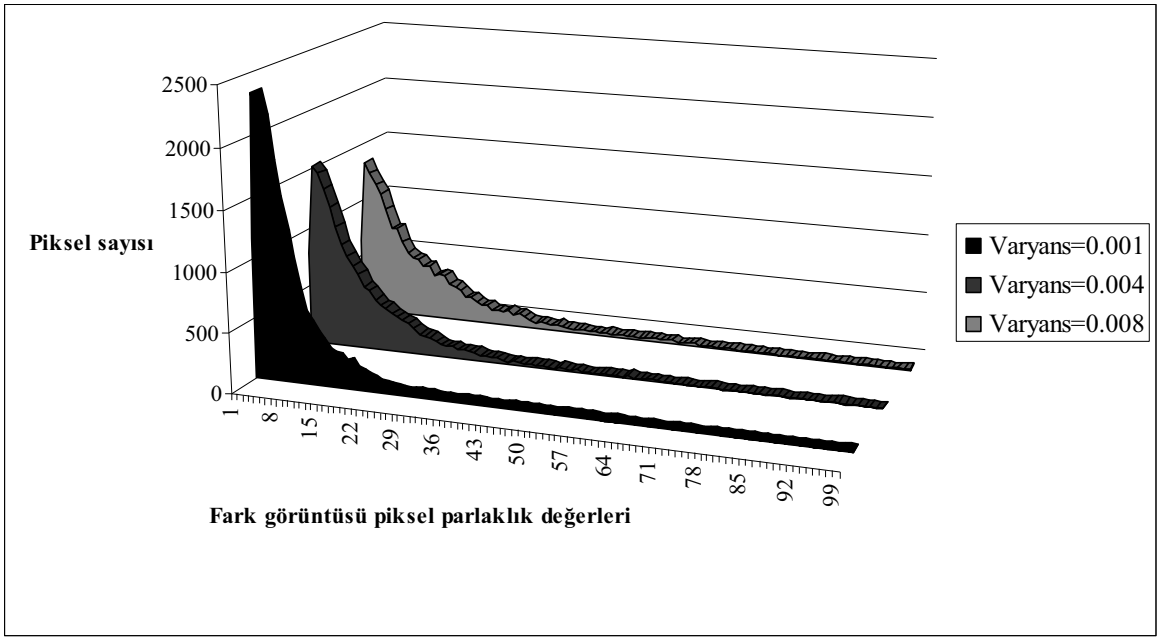
Şekil 3.36. Pay görüntüsüne farklı varyanslarda gürültü eklenmesi sonucu yeniden yapılandırılan gizli görüntüler

Yeniden yapılandırılan gizli görüntüler ve orijinal gizli görüntüden elde edilen fark görüntülerinin histogramları Şekil 3.37'de verilmektedir. Fark görüntülerinin histogramlarının daha belirgin bir şekilde gözlemlenebilmesi amacıyla parlaklık aralığı $[0-100]$ ile sınırlandırılmıştır.

Diğer bir testte, pay görüntüsü üzerinde damgalama yöntemlerinde kullanılan üç atak (bulanıklaştırma, yeniden boyutlandırma, histogram ayarlama) gerçekleştirilmiştir. Bulanıklaştırma için 3×3 büyüklüğünde maske kullanan ortalama filtresi uygulanmıştır. Pay görüntüsünün bulanıklaştırma operasyonunda sonra yeniden yapılandırma adımında kullanılması sonucu elde edilen yeniden yapılandırılan görüntü, Şekil 3.38(a)'da verilmiştir. Şekil 3.38(b) ve (c) ise sırasıyla, pay görüntüsü üzerinde yeniden boyutlandırma ve histogram ayarlama ataklarının uygulanması sonucu elde edilen gizli görüntüleri vermektedir.

Yeniden yapılandırmada, 128×64 büyüklüğündeki pay görüntüsü, 256×128 büyüklüğüne yeniden örneklenmekte ve ardından tekrar 128×64 büyüklüğüne

düşürülmektedir. Histogram ayarlamada kullanılan parametreler ise pay görüntüsüne özgü olarak [0 0.7] olarak seçilmiştir.



Şekil 3.37. Fark görüntülerinin $[0-100]$ aralığındaki histogramlarının görüntülenmesi

Sonuçlarda da vurgu yapıldığı gibi, önerilen gizli görüntü paylaşım tekniği, literatürde ilk olarak pay görüntüsündeki bozulmalara karşı dayanıklılık özelliği içermektedir.

(a) (b) (c)

Şekil 3.38. Pay görüntüsü üzerinde gerçekleştirilen (a) Bulanıklaştırma (b) Yeniden boyutlandırma (c) Histogram ayarlama ataklarından sonra elde edilen yeniden yapılandırılmış gizli görüntüler

Blakley ve Shamir tabanlı yöntemlerden farklı olarak, pay görüntüsündeki bozulmalara karşı dayanıklı olan yöntem, farklı atakların uygulanmasında dahi insan gözü tarafından fark edilebilir yeniden yapılandırılmış gizli görüntüler elde etmektedir. Bir sonraki bölümde sayı teorisine dayanan eşik şeması yöntemlerinin gizli görüntü paylaşımında kullanılmasının, Shamir veya Blakley tabanlı yöntemlere kıyasla sağlayacağı avantaj ve dezavantajlar değerlendirilecektir.

3.7. Sayı Teorisine Dayanan Gizli Görüntü Paylaşım Şemaları ile İlgili Yapılan Çalışmaların Değerlendirilmesi ve Elde Edilen Deneysel Sonuçlar

Sır paylaşım şemalarının ilk olarak [4]'teki çalışmada gizli görüntü paylaşımında kullanılmasının ardından gerçekleştirilen birçok çalışma ağırlıklı olarak Shamir'in yöntemini kullanmaktadır. Son yıllarda bazı çalışmalar Blakley'in yöntemini kullansalar dahi genel olarak bu alanda Shamir'in yöntemi öne çıkmaktadır. Sayı teorisine dayalı eşik şemalarının gizli görüntü paylaşımı alanında henüz kullanılmamış olması, bizi hangi eşik şemasının görüntü paylaşımında kullanımının gereksinimler açısından olumlu sonuçlar vereceğini araştırmaya yönlendirmiştir.

İlk olarak 2009 yılında gerçekleştirdiğimiz çalışmada Asmuth-Bloom sır paylaşım tekniğinin gizli görüntülerin paylaşımında kullanımı gerçekleştirilmiştir [149]. Bu çalışma sonucunda üretilen pay görüntüleri gürültü özelliği taşımaktadır. Sonraki yıllarda steganografi kullanılarak üretilen pay görüntülerinin anlamlı hale getirilmesi hedeflenmiştir [150]. Yapılan çalışmalar kısmında da detayları verilen gizli görüntü paylaşım şeması, Asmuth-Bloom sır paylaşım şemasını literatürde ilk olarak gizli görüntü paylaşımında kullanmıştır. Bu bölümde öncelikle önerilen gizli görüntü paylaşım şemasına ait sonuçlar verilecektir. Ardından gerçekleştirilen ve yine sayı teorisine dayanan Mignotte'nin eşik şemasını kullanan gizli görüntü paylaşım şemasından elde edilen sonuçlar da değerlendirilecektir [151]. Mignotte'nin şeması ilk olarak 2008 yılında Shyu vd. tarafından gizli görüntülerin paylaşımında kullanılmıştır. Yalnız önermiş oldukları yöntem, pay görüntülerinin gizli görüntü hakkında bilgi içermesine engel olabilmek amacı ile rasgele fonksiyon kullanmaktadır. Rasgele fonksiyonun çekirdek değerinin ise önceden taraflar arasında paylaşılması gerekmektedir. Gerek rasgele fonksiyonun algoritmasının gerekse çekirdek değerinin önceden taraflar arasında iletilecek olması yöntemi ataklara karşı aciz bırakmaktadır. Önermiş olduğumuz yöntem yeniden yapılandırma aşamasında

rasgele fonksiyona ihtiyaç duymayarak, paylaşma öncesinde herhangi bir veri haberleşmesi gerektirmemektedir. Shyu vd.'nin yöntemindeki acizlikleri ortadan kaldıran ve Mignotte'nin şemasını gizli görüntü paylaşımında kullanan şemaya ilişkin deneysel sonuçlar bu bölümde verilmektedir.

Asmuth-Bloom'un sır paylaşım şemasını ilk olarak gizli görüntü paylaşımında kullanan yöntemin sonuçlarını gösterebilmek amacıyla (3, 4) eşik şeması seçilmiştir. Paylaşım şemasında kullanılacak olan gizli görüntü, Şekil 3.32'de verilen, 128×128 büyüklüğündeki "girl" isimli gri seviye test görüntüsüdür. İlgili görüntünün dört katılımcı arasında paylaştırılacağı varsayılır. Bu nedenle dört katılımcı için de dört farklı ve doğal görünümlü örten görüntü seçilir. Seçilen örten görüntüler 256×256 büyüklüğündeki gri seviye test görüntüleridir. Şekil 3.39'da 256×256 büyüklüğündeki örten görüntü olarak kullanılan "lighthouse", "monarch", "clock" ve "oldhouse" görüntüleri verilmiştir.

Yöntemin (3, 4) eşik şeması için gerçeklenmesi sonucu elde edilen stego görüntüler Şekil 3.40'da yer almaktadır. Şekilden de görüleceği gibi, örten görüntülerde kodlama sonrası oluşan değişim insan gözünün ayırt edemeyeceği ölçüde küçüktür. Elde edilen PSNR değerleri yaklaşık olarak 50 dB'dir. Bu da örten görüntüdeki değişimin insan gözüyle ayırt edilemeyecek ölçüde küçük olduğunun bir göstergesidir. Örten görüntülerdeki 2×2 büyüklüğündeki bloklara saklanan pay değerleri 9 bit büyüklüğündedir. 2×2'lik blokların hepsinde 9 bit değişim gerçekleşseydi üretilen stego görüntülerin PSNR değerleri yaklaşık olarak 40 dB civarında olurdu. Elde edilen PSNR değerinin ise 50 dB civarında olması örten görüntüde kullanılmayan piksellerin olmasından kaynaklanmaktadır. Yöntem 128×128 büyüklüğündeki gizli görüntüden 128×64 adet 9 bit pay değeri üretmektedir. Pay değerlerinin her birinin 4 pikselden oluşan bloklara kodlanacak olduğu düşünülürse, örten görüntüdeki $(128\times128)\times4/2 = 128\times256$ adet piksel değeri saklama amacıyla kullanılmaktadır. Örten görüntünün yarısı pay değerlerini saklamada kullanılırken diğer yarısı veri içermemektedir. Örten görüntü büyüklüğünün 256×256 olarak seçilmesi Shamir tabanlı yöntemlerde kullanılan test görüntüleri ile kıyaslanabilirliğini sağlamaktır. Literatürde var olan yöntemler PSNR değerini rapor ederken doluluk oranını hesaba katmamaktadır. İlk olarak tarafımızdan önerilen ve ifadesi (3.3)'te verilen *ko*'nın kullanılması yöntemlerin kıyaslanabilirliği açısından daha etkin olacaktır. Asmuth-Bloom'un sır paylaşım şemasının gizli görüntü paylaşımına uygulanması esnasında, gizli görüntü pikselleri ikişerli gruplar şeklinde değerlendirilmiştir.

Gizli görüntü piksel parlaklık değerlerinin tüm aralığını kapsayabilecek şekilde şemanın gerektirdiği sıralı sayıların seçimi, ancak 9 bitlik sayılarla mümkün olmaktadır. Bu nedenle de her bir pay değeri 9 bit ile temsil edilir. Shamir tabanlı yöntemlerin üretmiş olduğu pay değerlerinin 8 bit olması stego görüntülerde meydana gelecek değişimleri azaltmaktadır.

Şekil 3.39. 256×256 büyüklüğündeki gri seviye örten görüntüler

[4]'teki çalışma Shamir'in sır paylaşım şemasını, gizli görüntülerin paylaşımına uygularken, gizli görüntüdeki her k adet pikselden bir pay değeri oluşturmaktadır. Üretilen pay görüntü büyüklüğü gizli görüntü büyüklüğünün $1/k$'sı kadar olsa dahi, üretilen pay değerleri gizli görüntü hakkında bilgi içermektedir. Buna engel olmak amacıyla yazarlar, pay görüntülerinin, iletimden önce anahtar değerine bağlı olarak karıştırılmasını önermişlerdir. Shamir'in polinomundaki katsayı değerlerinin tümü gizli görüntüden gelecek şekilde, (3, 4) şemasının gizli görüntü üzerinde uygulanması sonucu elde edilen 128×42 büyüklüğündeki pay görüntüleri Şekil 3.41'de verilmiştir. Şekilden de gözlemlenebileceği gibi üretilen pay görüntüleri, paylaştırma esnasında polinomun k adet katsayı değerinin gizli görüntüden alınması durumunda, gizli görüntü hakkında bilgi verebilmektedir. Bu çalışmanın ardından gelen ve pay görüntülerinin saklanmasında

steganografi kullanan çalışmalar, polinomun yalnızca sabit terimini gizli görüntü piksel değerini taşımada kullanmıştır.

PSNR = 51.4 dB

PSNR = 50.9 dB

PSNR = 50.8 dB

PSNR = 49.77 dB

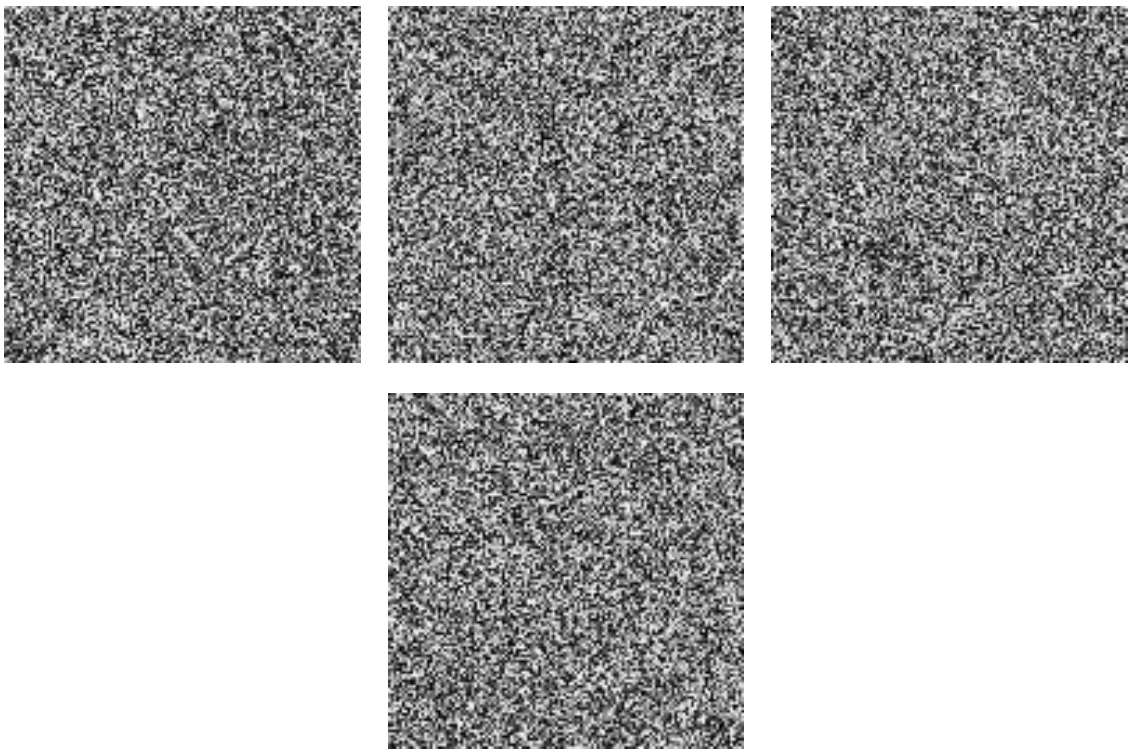
Şekil 3.40. 256×256 büyüklüğündeki stego görüntüler ve ilişkili PSNR değerleri

Şekil 3.41. [4]'teki şema kullanılarak gizli görüntünün paylaştırılması sonucu elde edilen pay görüntüleri

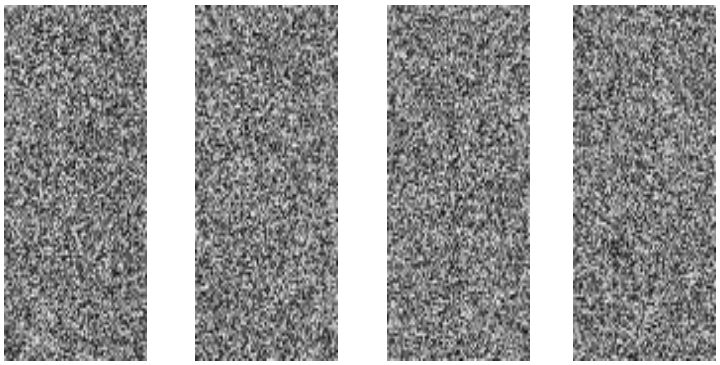
Bu durumda herhangi bir (k, n) eşik şeması için üretilen pay görüntü büyüklüğü, gizli görüntü büyüklüğü ile aynıdır. (3, 4) şeması için Shamir'in şemasının öngördüğü şekilde yalnızca sabit terimin gizli görüntü piksel değerini taşıması durumunda üretilen pay

görüntüleri Şekil 3.42'de verilmektedir. Şekilden de gözlemlenebileceği gibi, pay görüntü büyüklüğü, gizli görüntü büyüklüğü ile aynıdır ve gizli görüntü hakkında herhangi bir bilgi açığa çıkarmaz. Bu nedenle, polinomun yalnızca sabit terimini veri saklamada kullanan şemalar karıştırma fonksiyonuna ihtiyaç duymamaktadır. Üretilen pay görüntü büyüklüğü, polinom katsayı değerlerinin tümünü veri taşımada kullanan yöntemlere göre, daha büyüktür. Asmuth-Bloom yöntemini sır paylaşımında kullanan ve tarafımızdan önerilen yöntemin üretmiş olduğu pay görüntüleri ise Şekil 3.43'te verilmiştir. Üretilen pay görüntüleri eşik değeri k'dan bağımsız olarak orijinal gizli görüntü büyüklüğünün neredeyse yarısı $(9/16)(\cong 0.56)$ kadardır. Aynı zamanda herhangi bir karıştırma fonksiyonuna ihtiyaç duymadan pay görüntülerindeki rasgeleliği sağlamaktadır. 128×128 gizli görüntü için üretilen pay görüntüleri eşik değerinden bağımsız olarak 128×72 büyüklüğündedir.

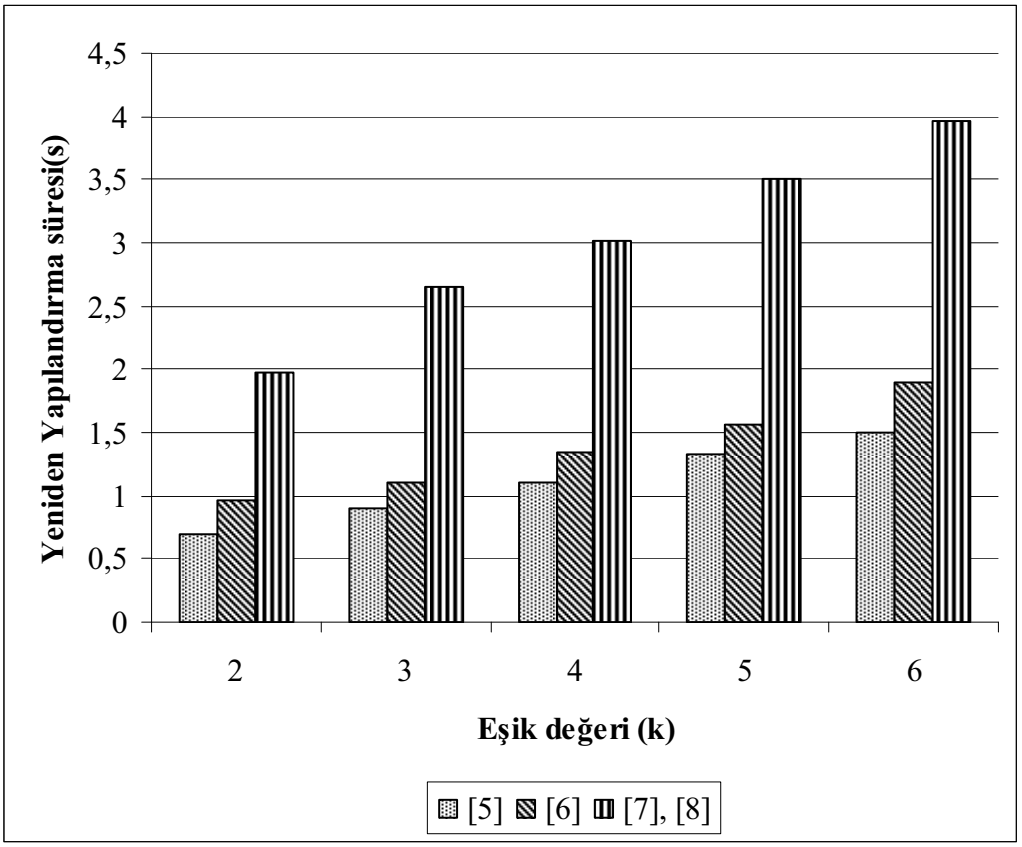
Shamir'in yöntemini kullanan gizli görüntü paylaşım şemaları ile Asmuth-Bloom'un eşik şeması kullanan yöntemler arasındaki en belirgin fark yeniden yapılandırma esnasında yaşanmaktadır. Shamir tabanlı yöntemler, yeniden yapılandırma esnasında Lagrange'ın interpolasyonunu kullanırken, önerilen yöntem ÇKT'ni kullanmaktadır.



Şekil 3.42. Shamir'in polinomundaki yalnızca sabit terimin gizli veri taşıması durumunda üretilen 128×128 büyüklüğündeki pay görüntüleri



Şekil 3.43. Önerilen yöntemin (3, 4) şeması için üretmiş olduğu 128×72 büyüklüğündeki pay görüntüleri



Şekil 3.44. Farklı eşik değerleri için Shamir, Blakley ve Asmuth-Bloom tabanlı gizli görüntü paylaşım şemalarının yeniden yapılandırma süreleri

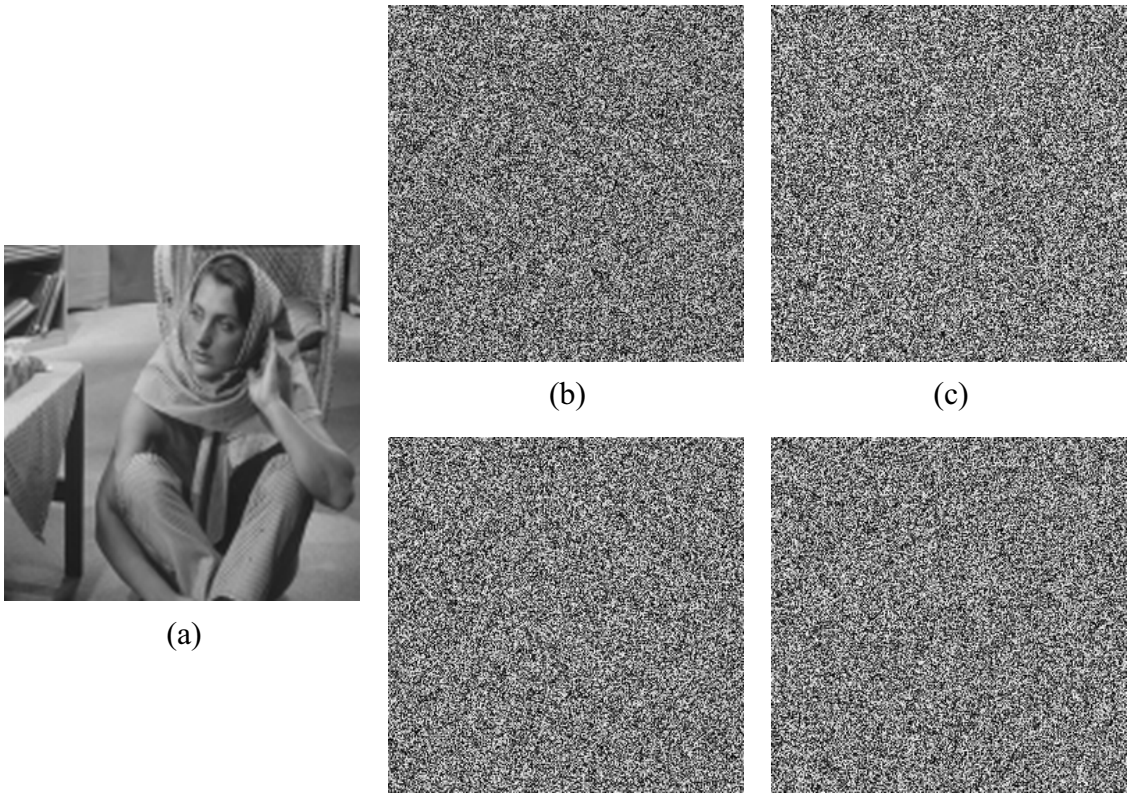
Asmuth-Bloom tabanlı bir yöntemin performans değerlendirmesini yapabilmek amacıyla 128×128 büyüklüğündeki gizli görüntü k=2, 3, 4, 5, 6 değerleri kullanılarak paylaştırılmıştır. Farklı eşik değerlerinde gerek Shamir ve Blakley tabanlı yöntemlerin

gerekse önerilen yöntemin yeniden yapılandırma süreleri ölçülmüştür. Testler sonucunda elde edilen değerler Şekil 3.44'te gösterilmektedir.

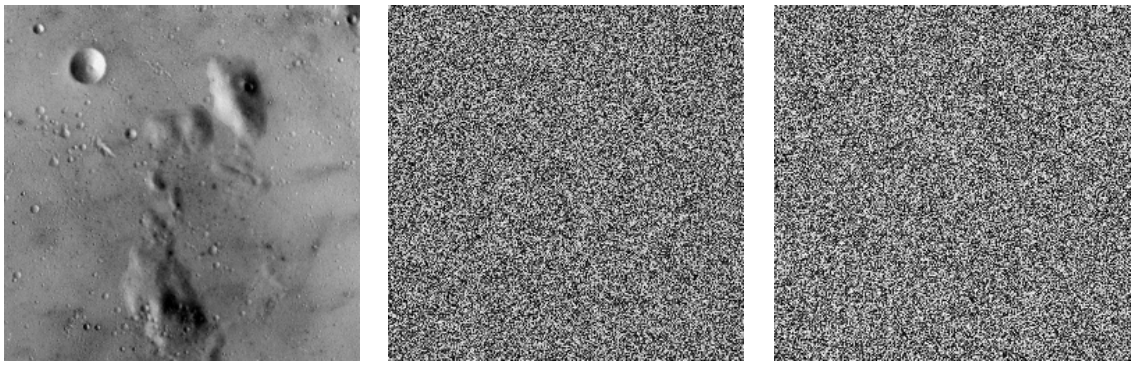
Şekilden de gözlemlenebileceği gibi hız açısından Shamir ve Blakley tabanlı yöntemler öne çıkmaktadır. Asmuth-Bloom sır paylaşım yönteminin gizli görüntü paylaşımında kullanımı, pay görüntülerinde karıştırma gerekmeksizin rasgeleliği sağlamasına rağmen işlem zamanı açısından olumlu sonuçlar vermemektedir.

Sayı teorisine dayalı bir diğer yöntem olan Mignotte eşik şemasının gizli görüntü paylaşımına uyarlanması tez kapsamında gerçekleştirilmiştir. [144]'teki çalışmadan farklı olarak yeniden yapılandırma esnasında rasgele fonksiyonuna ihtiyaç duymayan yöntem, gizliği iyileştirmektedir. Asmuth-Bloom ve Mignotte şemalarının, yeniden yapılandırma esnasındaki işlem zamanları neredeyse aynıdır. Bu nedenle de Şekil 3.44'e Mignotte'nin şemasını kullanan yöntemin yeniden yapılandırma süresi eklenmemiştir. Şekil 3.45(a)'da verilen gizli görüntünün Mignotte'nin yönteminin (3, 4) eşik şeması ile paylaştırılması sonucu elde edilen pay görüntüleri Şekil 3.45(b)-(e)'de verilmektedir. Pay görüntü büyüklükleri gizli görüntü ile aynı olup, karıştırma fonksiyonuna ihtiyaç duymadan rasgelelik içermektedir. Yöntemin, piksel parlaklık değerleri arasında benzerlik olan gizli görüntülerde dahi, ürettiği pay görüntülerinin rasgelelik içerdiğini göstermek amacıyla gerçekleştirilen diğer bir deneyin sonuçları Şekil 3.46'da verilmektedir.

Sonuç olarak önerilen sayı teorisine dayalı eşik şemalarını kullanan yöntemler tarafından üretilen pay görüntülerinin sıkıştırılabilirlik oranlarının düşüklüğü, yeniden yapılandırma esnasındaki yavaşlıkları göz önüne alınarak, tez süresince yapılan çalışmalarda ağırlıklı olarak Shamir ve Blakley'in eşik şemasını kullanan yeni yöntemlerin geliştirilmesine çaba sarf edilmiştir. Gerek Asmuth-Bloom gerekse Mignotte'nin şemasını kullanan tarafımızdan önerilen gizli görüntü paylaşım şemaları, pay değerlerinin ifade edilmesinde esnekliğe sahip değildir. Pay görüntülerinin sıkıştırılabilir özelliğinin azlığı, yönteme doğrulama yeteneğinin de eklenmesine engel olmaktadır. Asmuth-Bloom'u kullanan yöntem her ne kadar gizli görüntünün neredeyse yarısı büyüklüğünde pay görüntüsü üretse dahi, *ko* değeri hesaba katıldığında Shamir tabanlı yöntemlere nazaran daha düşük PSNR değerlerine sahip olacaktır. Gerek Mignotte tabanlı gerekse Asmuth-Bloom tabanlı yöntemlerin tercih edilmemesine sebep olarak pay görüntü büyüklükleri ve yeniden yapılandırma işlem süresi verilebilir.



Şekil 3.45. (a) 128×128 büyüklüğündeki gizli görüntü (b)-(e) (3, 4) şeması için üretilen 128×128 büyüklüğündeki pay görüntüleri



Şekil 3.46. (a) Gizli görüntü (b)-(c) (2,2) şeması ile (a)'da verilen gizli görüntünün paylaştırılması sonucu elde edilen pay görüntüleri

Tez çalışması kapsamında önerilen yöntemlerin kendi alt alanlarındaki çalışmalarla; stego görüntülerin PSNR değeri, pay görüntülerindeki genişleme oranı ve kullanılan doğrulama biti sayısı açısından kıyaslamaları Tablo 3.9'da verilmektedir. Tablodan da gözlemlenebileceği gibi önerilen yöntemler kendi alt alanlarındaki çalışmalara kıyasla

üstünlük göstermektedir. Steganografi tabanlı ve doğrulama mekanizmalı tekniklerde doğrulama biti sayısı artırılırken PSNR değerinin iyileştirilmesi hedeflenmektedir. [146]'daki yöntemin bu alandaki çalışmalarla kıyaslandığında daha yüksek PSNR değeri üretirken doğrulama biti sayısını da artırdığı gözlemlenmektedir. Adaptif doğrulama gerçekleştiren yöntem, benzer çalışma olan Eslami'nin yöntemine kıyasla, doğrulama biti sayısını adaptif olarak artırabilmektedir. Ayrıca Eslami'nin çalışmasının etkilenmiş olduğu zincirleme problemine karşı dayanıklıdır. Diğer sır paylaşım tekniklerini kullanan yöntemler içerisinde önerilen Blakley tabanlı yöntem üstünlükler içermektedir. Gerek anlamlı pay üretimi gerekse bu alandaki çalışmalarda doğrulama kullanan ilk yöntem olması üstünlüğü ortaya koymaktadır. Geri döndürülebilir yöntemler alanındaki çalışmalar içerisinde ise önerilen yöntem, örten görüntü parlaklık aralığından bağımsız olarak diğer yöntemlere kıyasla daha yüksek PSNR değerlerine sahiptir. Tablodan'da gözlemlenebileceği gibi önerilen yöntemler diğer çalışmalara kıyasla üstünlükler içermektedir.

Tablo 3.9. Önerilen yöntemlerin var olan çalışmalarla genel bir kıyaslaması

		PSNR (dB)	Genişleme oranı	Doğrulama bit sayısı
Steganografi Tabanlı ve Doğrulama mekanizmalı teknikler	[4]	--	$1/k$	Y
	[59]	39	1	1
	[62]	41	1	1
	[63]	37	$1/k$	4
	[146]	43	1	3
Adaptif Yöntemler	[68]	[45, 52]	$1/k$	4
	Yöntem 2.4	[45, 52]	$1/k$	Adaptif
Diğer Sır Paylaşım Tekniklerini Kullanan Yöntemler	[87]	--	1	Y
	[86]	--	$1/k$	Y
	[145]	[28, 51]	$1/k$	1
	[150]	42	$1/2$	Y
	[151]	--	1	Y
Geri Döndürülebilir Yöntemler	[73]	İki bit örten görüntü: 37.2 Sekiz bit örten görüntü: 41.5	$3/(k-3)$	Y
	[74]	İki bit örten görüntü: -- Sekiz bit örten görüntü: 39	$3/(k-1)$	Y
	Yöntem 2.3	İki bit örten görüntü: 41.4 Sekiz bit örten görüntü: 45.9	$4/(k-2)$	Y

4. SONUÇLAR

Ağ üzerinden gerçekleştirilen veri iletiminin artması, bilgi güvenliği problemini beraberinde getirmiştir. Güvenliğin sağlanmasında kullanımı yaygın teknikler olan steganografi ve kriptografi'nin etkilendiği en önemli problem, şifrelenen yada saklanan verinin tek bir ortamda (stego yada şifreli ortam) tutulmasıdır. Ortamın tahrip olması yada herhangi bir şekilde bozulması durumunda, gizli veri yeniden yapılandırılamaz. Her iki yöntemde tek kişiye güven prensibine dayanmaktadır. Gizli verinin ancak belirli sayıda kullanıcının bir araya gelmesi sonucu elde edilebilmesinin istendiği durumlar için farklı bir yöntemin kullanımı şarttır.

Hataya karşı toleransı sağlarken gruba güven mekanizmasını sunabilen sır paylaşım şemaları ilk olarak 2002 yılında, gizli görüntülerin iletiminde kullanılmıştır. Bu çalışmanın ardından literatürdeki çalışmalar, var olan gizli görüntü paylaşım şemalarının çeşitli problemlerini iyileştirmeye çalışmaktadır. Genişleme oranının küçültülmesi, üretilen stego görüntülerin PSNR değerinin iyileştirilmesi, stego görüntüleri doğrulamada kullanılan bit sayısının görüntü kalitesinden ödün vermeden artırılması, gizli görüntünün yeniden yapılandırılmasının ardından örten görüntülerin elde edilebilmesi ve adaptif doğrulamanın gerçekleştirilmesi, araştırmacılar tarafından iyileştirilmesi hedeflenen unsurlardır. Tez süresince hedefleri iyileştirmek doğrultusunda tasarlanan paylaşım şemalarından ve önerilen yeni geometri tabanlı şemadan elde edilen sonuçlar kısaca aşağıdaki şekilde özetlenebilir.

1) Örten görüntü büyüklüğü ve gizli görüntü büyüklüğü arasındaki oranı tanımlayan genişleme oranı, Shamir tabanlı yöntemler için 4 olarak rapor edilmektedir. Blakley'in yönteminin bu tez çalışmasında önerilen kodlama tekniği ile beraber kullanılması sonucu, genişleme oranı 1'e düşürülmüştür. Genişleme oranındaki dört kat iyileşme elde edilmesinin dışında, Blakley'e dayanan yöntem, eşik değerinin 3'den büyük olduğu durumlarda Shamir tabanlı yöntemlere nazaran daha yüksek PSNR değerine sahip stego görüntüler üretmektedir. Eşik değerinin 4 olarak seçilmesi durumunda, önerilen yöntem yaklaşık [0.5, 3] dB aralığında artış sağlamaktadır. Eşik değerinin 5 olarak seçilmesi durumunda ise artış [4, 7] dB aralığında değişmektedir. Yöntem özellikle eşik değerinin 3'ten büyük olduğu durumlarda başarı göstermektedir.

2) Stego görüntülerin kalitesini bozmadan doğrulamada kullanılan bit sayısını artırmayı hedefleyen yöntem, pay değer aralığını alt aralıklara bölerek, pay değerlerini temsil etmektedir. Pay değerini temsil eden bit sayısının azalması, yöntemin doğrulama biti sayısını artırabilmesini sağlamıştır. Böylece stego görüntü kalitesi etkilenmeden, doğrulama yeteneği diğer yöntemlere kıyasla artırılmıştır. Aynı zamanda pay değerlerinin saklanması esnasında OPAP yönteminin kullanılması, klasik LSB yöntemi kullanan yöntemlere kıyasla, daha yüksek PSNR'ye sahip stego görüntüler üretilebilmesini sağlamıştır. Literatürde ilk olarak Shamir'in polinomuna giriş olarak verilen x değer aralığının küçültülmesi durumunda oluşan çakışmaların stego görüntü kalitesine etkisi çalışma kapsamında değerlendirilmiştir. Önerilen yöntemin doğrulama oranı [59, 62, 65] çalışmalarına kıyasla yaklaşık olarak %60 iyileşme sağlamıştır. Stego görüntü kalitesi açısından bakıldığında, [59], [62], [63] ve [65]'deki çalışmalarda rapor edilen PSNR değerlerine kıyasla yaklaşık olarak sırasıyla 4, 2, 6 ve 1 dB artış sağlanmıştır.

3) Adaptif doğrulama gerçekleştiren diğer bir çalışma, doğrulama biti sayısını, gizli görüntü ve örten görüntü büyüklüğü ile eşik değerine bağlı olarak belirlemektedir. Yöntem literatürde adaptif olarak adlandırılan diğer bir çalışmadaki, zincirleme mekanizmasından kaynaklanan güçsüzlüğü ortaya koymaktadır. Pay değerlerinin ve doğrulama bitlerinin saklanması esnasında, dinamikliği sağlayabilmek amacıyla, klasik LSB'ye saklama yöntemi yerine EMD yöntemi kullanılmaktadır. Elde edilen sonuçlarda yöntemin [68]'de var olan zincirleme probleminden etkilenmediği gösterilmektedir. Aynı zamanda yöntemin doğrulama oranının blok büyüklüğü ile orantılı bir şekilde değiştiği gözlemlenmektedir. [68]'deki çalışma blok büyüklüğünden bağımsız olarak 0.94 doğrulama oranı sunarken, önerilen yöntem blok büyüklüğünün artışı ile beraber %100 doğrulama oranı sunabilmektedir. Blok büyüklüğü olarak 12 seçilmesi durumunda önerilen yöntemin %100 doğrulama oranına rağmen, [68]'deki çalışmadan, PSNR açısından yalnız 1.5 dB düşük PSNR'ye sahip stego görüntüler üretmesi başarılı olduğunun göstergesidir.

4) Geri döndürülebilir gizli görüntü paylaşımı alanında yapılan çalışmada, literatürde var olan çalışmalardaki problemleri giderecek yeni bir teknik önerilmiştir. EMD yönteminde kullanılan ifadenin uyarlanması gerçekleştirilmiş ve yeniden yapılandırma esnasında örten görüntü piksellerinin elde edilebilmesi amacıyla modulo operatöründen faydalanılmıştır. Aynı zamanda literatürde ilk olarak "kullanım oranı" olarak adlandırılan yeni bir metriğin kullanımı önerilmiştir. Elde edilen deneysel sonuçlarda, yöntemin siyah-beyaz örten görüntülerin kullanılmasında dahi, yüksek PSNR değerlerine sahip stego

görüntüler ürettiği gösterilmiştir. Var olan yöntemlerle önerilen yöntemin *ko* cinsinden kıyaslaması yapılmış ve yöntemin örten görüntü parlaklık aralığından bağımsız olarak yüksek PSNR değerleri ürettiği gözlemlenmiştir.

[73]'teki yönteme kıyasla, gri seviye örten görüntüler için stego görüntü kalitesi yaklaşık olarak 5 dB iyileşme göstermiştir. [74]'teki çalışmaya kıyasla bu iyileşim yaklaşık 7 dB civarındadır. Tramlanmış görüntüler için ise, önerilen yöntem [73]'teki çalışmada üretilen stego görüntülerden 4 dB fazla PSNR'ye sahip stego görüntüler üretmektedir. [74]'teki çalışma ise siyah beyaz görüntüleri desteklememektedir. [73]'teki yöntemin tramlanmış örten görüntü kullanılması durumunda üretmiş olduğu fark görüntüsünün parlaklık aralığı [0, 6] iken önerilen yöntemde bu değer [0, 4] şeklindedir. Fark görüntü histogramının daha dar bir bant içeriyor olması iyileşen PSNR'nin bir ispatıdır. Önerilen yöntem sonuçlardan da gözlemlenebileceği gibi, örten görüntü parlaklık aralığından bağımsız olarak yüksek PSNR'ye sahip stego görüntüler üretmektedir.

5) Paylaşılan görüntünün medikal görüntü olması durumu çalışma kapsamında değerlendirilmiştir. Medikal görüntü güvenliği alanında yapılan çalışmaların ayrı ayrı iyileştirmeye çalıştığı unsurlar (elektronik hasta kaydının iletimi, medikal görüntü güvenliğinin sağlanması, gruba güven prensibinin uygulanması) önerilen şema ile aynı anda gerçekleştirilebilmektedir. Bu bağlamda, bütün hedefleri tek bir yöntemle sağlayabilmesi açısından, literatürdeki ilk çalışma özelliği taşımaktadır. Medikal görüntünün özellikle siyasi yada askeri önem taşıyan birine ait olması durumunda, gruba güven mekanizması önem taşımaktadır. Aynı zamanda yöntem, var olan yöntemlerle kıyaslandığında, daha yüksek elektronik hasta kaydı saklama kapasitesine sahiptir.

(3, 4) şeması ve 256×256 büyüklüğündeki MR görüntüsü kullanılarak yapılan testte, önerilen yöntemin 21845 karakter saklayabildiği görülmüştür. Bu alandaki diğer iki çalışma olan [139, 141] ise aynı koşullarda sırasıyla 14510, 14863 karakter bilgisi saklayabilmektedir. Üretilen stego görüntülerin PSNR değeri yaklaşık olarak 46 dB civarındadır. Yöntemin yeniden yapılandırma süresi değerlendirildiğinde ise, medikal görüntü çözünürlüğünün artışı ile beraber, sürenin de lineer olarak artış gösterdiği gözlemlenmiştir. Eşik değeri 3 için 12 bit 2048×2048 büyüklüğündeki CR görüntülerde yapılandırma süresi 45.6 saniye iken, $k = 2$ için bu süre 36.8 olarak ölçülmektedir. Eşik değerine bağlı böyle bir değişim, interpolasyon ifadesinden kaynaklanmaktadır. Doğrulama için gerek sertifika gerekse Shamir'in yönteminden faydalanılması, yöntemin başarısını artırmaktadır. [138]'deki çalışma doğrulama için nazik damgalama kullanırken,

üretmiş olduğu stego görüntü kalitesi 40 dB civarındadır. Oysa önerilen yöntemin üretmiş olduğu stego görüntü kalitesi yaklaşık olarak 46 dB civarındadır.

6) Literatürde var olan gizli görüntü paylaşım şemaları çoğunlukla Shamir ve Blakley'in sır paylaşım şemalarından faydalanmaktadır. Her iki yöntemde, yeniden yapılandırma esnasında, en az k tane pay görüntüsünün hatasız olarak elde edilebilmesini gerektirir. Pay görüntülerinde meydana gelen değişme, gizli görüntüde karşılık düşen bölgelerin yapılandırılamamasına sebep olmaktadır. Literatürde ilk olarak var olan sır paylaşım şemalarını kullanmayan yeni bir geometri tabanlı gizli görüntü paylaşım şeması, tez kapsamında önerilmektedir. Morley'in üçgen teoremini gizli görüntü paylaşımında kullanan yöntem, pay görüntülerinde bozulma meydana gelse dahi, gizli görüntüyü yeniden yapılandırabilmektedir. Literatürde ilk kez pay görüntülerinin çeşitli ataklara maruz kalması durumunda, gizli görüntünün yeniden yapılandırılabilme oranı çalışma kapsamında değerlendirilmiştir. Elde edilen deneysel sonuçlarda, pay görüntüsündeki bozulmalara rağmen, gizli görüntünün insan gözü tarafından ayırt edilebildiğini göstermektedir. Yapılan testlerde bozulmanın belirlenmesinde insan görme sisteminden faydalanılmıştır.

7) Son olarak sayı teorisine dayalı yöntemlerin (Asmuth-Bloom ve Mignotte) gizli görüntü paylaşımında kullanılması durumunda, diğer yöntemlerle kıyaslaması gerçekleştirilmiştir. Bu bağlamda Asmuth-Bloom ve Mignotte'nin eşik şemalarının gizli görüntü paylaşımına uyarlaması gerçekleştirilmiştir. Elde edilen sonuçlarda gerek yeniden yapılandırma algoritmasının işlem zamanı gerekse üretilen pay görüntülerinin sıkıştırılabilirlik oranlarının küçük olması sebebi ile gizli görüntü paylaşımı alanında tercih edilmelerinin uygun olmayacağı kanaatine varılmıştır.

Tez çalışmasında gizli görüntü paylaşımı alanındaki problemlerin iyileştirilmesini hedefleyen yeni görüntü paylaşım tekniklerinin tasarımı gerçekleştirilmiştir. Ayrıca, eşik şemalarını kullanan gizli görüntü paylaşım şemalarından farklı olarak, Morley'in üçgen teoremine dayanan yeni bir görüntü paylaşım yöntemi tasarlanmıştır. Önerilen yöntem, literatürde ilk olarak, pay görüntülerinde bozulma meydana gelse dahi gizli görüntüyü belirli bir oranda yeniden yapılandırabilecek yeteneğe sahiptir. Çalışmalarımızda önerilen yaklaşımların uygulamaları MATLAB ortamında geliştirilmiş olup, çevrimiçi platformlara uyarlanabilir modülerliğe sahiptirler.

5. ÖNERİLER

Gizli görüntü paylaşımı özellikle 2002 yılından itibaren ilgi gören ve üzerinde araştırmalar yapılan bir konudur. Konunun, oldukça yeni olmasına rağmen yapılan çalışmalardaki yoğunluk, geliştirmelere ve yeniliklere açık olduğunun göstergesidir. Araştırmacılar çoğunlukla var olan sistemlerdeki problemlerin üzerine gitmeyi hedeflemektedir. Gürültü şeklindeki pay görüntülerinin örten görüntüler içerisine saklanması, üretilen stego görüntülerin kalitesini iyileştirme yönünde uğraş gerektirmektedir. Üretilen pay değerlerinin örten görüntülere saklanması esnasında LSB'ye saklama araştırmacılar tarafından yaygın olarak kullanılmaktadır. Farklı saklama tekniklerin kullanımının stego görüntünün PSNR değerini iyileştirmeye katkısı araştırmacılar tarafından incelenebilir.

Üretilen pay değer aralığının $[0-250]$ aralığında olması, örten görüntüde karşılık düşen bloktaki 8 bit değerinin saklamada kullanılacağını göstermektedir. Doğrulama için kullanılacak olan bit sayısının b ile gösterilmesi durumunda, değeri değişmesi gereken bit sayısı $8+b$ olacaktır. Böyle bir bozulmanın stego görüntü kalitesini etkilemesine engel olmak için örten blok büyüklüğünü artırmak gerekir. Boyut artışı ise depolama gereksinimleri ve bant genişliği açısından negatif etkiye sahiptir. Bu nedenle pay değerlerinin ifade edilmesinde kullanılan bit sayısının azaltılabilmesi araştırmacılar tarafından hedeflenebilir.

Stego bloklardaki doğrulama, ilgili bloğa yerleştirilen doğrulama bitleri ile sağlanmaktadır. Blok başına doğrulama kullanmak yerine, stego görüntünün tümü üzerinden geliştirilen bir doğrulama mekanizmasının, görüntü paylaşım şeması üzerine etkisi incelenebilir. İnceleme önerilen yöntemin gerek doğrulama yeteneği üzerine gerekse yeniden yapılandırma algoritmasının çalışma süresine etkisi göz önüne alınarak yapılabilir.

Shamir'in yöntemini kullanan görüntü paylaşım şemalarında seçilen x değerlerinin (karşılık düşen örten bloklardan elde edilen) aynı çıkması durumunda, ilgili örten bloğun değiştirilmesi gerekir. x değerinin en anlamlı beş bit kullanılarak elde edilmesi durumunda, böyle bir değişim stego görüntünün kalitesinde önemli düşüşlere sebep olur. Bu nedenle örten bloklardan elde edilecek x değerlerini belirlerken, çakışmayı engelleyecek şekilde dinamik bir stratejinin kullanımı denenebilir.

Yeniden yapılandırma esnasında örten görüntüleri elde eden yöntemlerde farklı katılımcılar için kullanılan örten görüntüler aynıdır. Yapılan çalışmalarda, yönteme geri döndürülebilirlik özelliğinin kazandırılabilmesi için, örten piksellere ait bilginin pay değerlerinde tutulması gerektiğine vurgu yapılmaktadır. Bu nedenle farklı örten görüntülerinin kullanılması durumunda, saklanması gereken bilgi sayısı artacaktır. Araştırmacılar Shamir'in polinomundaki katsayıları kullanarak, farklı örten görüntülerin kullanılabilmesini sağlamaya çalışabilir. Fakat bu durumda da yine de *n* farklı görüntünün kullanılabilmesi mümkün olmayacaktır. *n* farklı örten görüntünün kullanılması, sistemi güvenliğini artırabilir.

Adaptif doğrulama gerçekleştirilen yöntemlerde, doğrulama biti sayısı arttıkça, örten görüntünün saklayabildiği gizli görüntü büyüklüğü azalır. Bu nedenle adaptif doğrulama yöntemlerinde, pay değerinin ve doğrulama değerinin saklanması esnasında PVD yönteminin kullanılması denenebilir. Böylece daha az pikselle daha geniş aralıklardaki verinin temsili gerçekleştirilebilir.

Sayı teorisine dayanan ve Polinomial tabanlı yöntemlerin hibrit kullanımının, stego görüntü kalitesine iyileştirme sağlayıp sağlamayacağı gözlemlenebilir.

Geometri tabanlı yöntemlerde, stego görüntülerden elde edilen değerlerle oluşturulan X matrisinin determinantının 0 olma olasılığı, Shamir tabanlı yöntemlerdeki herhangi iki *x* değerinin aynı gelme olasılığına göre daha düşüktür. Örten blokların benzerlik karakteristiğine bağlı olarak, dinamik bir şekilde kullanılacak sır paylaşım şeması belirlenebilir.

Pay görüntülerinde meydana gelebilecek hatalar durumunda, gizli görüntünün karşılık düşen pikselleri yapılandırılamamaktadır. Lagrange'ın interpolasyonu ve lineer denklik sisteminin çözümü, bu şekildeki hataları tolere edemeyecektir. Bu nedenle görüntü paylaşımı esnasında, hatalara karşı daha az duyarlı yeniden yapılandırma mekanizmaları olan yöntemlerin önerilmesi avantaj sağlayabilir.

Morley'in üçgen teoremi kullanılarak önerilen şema, (*k*, *n*) eşik değerlerini destekleyecek şekilde genişletilebilir.

6. KAYNAKLAR

1. Wayner, P., Disappearing Cryptography, Second Edition, Morgan Kaufmann, San Francisco, 2002.

2. Forouzan, B., A., Cryptogaphy and Network Security, International Edition, Mc Graww Hill, Singapore, 2008.

3. Naor, M. ve Shamir, R., Visual Cryptography, Lecture Notes in Computer Science, 950 (1995) 1–12.

4. Thien, C. C. ve Lin, J. C., Secret Image Sharing., Computers and Graphics, 26 (2002) 765–770.

5. Shamir, A., How to Share a Secret, Communications ACM, 22 (1979) 612–613.

6. Blakley, G. R., Safeguarding Cryptographic Keys, National Computer Conference, Haziran 1979, New York, Bildiriler Kitabı, 313–317.

7. Asmuth, C. ve Bloom, J., A Modular Approach to Key Safeguarding, IEEE Transactions on Information Theory, 29 (1983) 208–210.

8. Mignotte, M., How to Share a Secret, Lecture Notes in Computer Science, 149 (1983) 371–375.

9. Thien, C. C. ve Lin, J. C., A Simple and High-Hiding Capacity Method for Hiding Digit-by-Digit Data in Images Based on Modulus Function, Pattern Recognition, 36 (2003) 2875–2881.

10. Chan, C. K. ve Cheng, L. M., Hiding Data in Images by Simple LSB Substitution, Pattern Recognition, 37 (2004) 469–474.

11. Wang, S. J., Steganography of Capacity Required Using Modulo Operator for Embedding Secret Image, Applied Mathematics and Computation, 164 (2005) 99–116.

12. Wu, H. C., Wu, N. I., Tsai, C. S. ve Hwang, M.S., Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods, IEE Proceedings of Vision Image and Signal Processing, 152 (2005) 611–615.

13. Wu, D. C. ve Tsai, W. H., A Steganographic Method for Images by Pixel-Value Differencing, Pattern Recognition Letters, 24 (2003) 1613–1626.

14. Chang, C. C. ve Tseng, H. W., A Steganographic Method for Digital Images Using Side Match, Pattern Recognition Letters, 25 (2004) 1431–1437.

15. Zhang, X. ve Wang, S., Steganography Using Multiple-Base Notational System and Human Vision Sensitivity, IEEE Signal Processing Letters, 12 (2005) 67-70.

16. Wang, C. M., Wu, N. I., Tsai, C. S. ve Hwang, M. S., A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Function, The Journal of Systems and Software, 81 (2008) 150-158.

17. Yang, C. H., Weng, C. Y., Wang, S. J. ve Sun, H. M., Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems, IEEE Transactions on Information Forensics and Security, 3 (2008) 488-497.

18. Zhang, X. ve Wang, S., Dynamical Running Coding in Digital Steganography, IEEE Signal Processing Letters, 13 (2006) 165-168.

19. Mielikainen, J., LSB Matching Revisited, IEEE Signal Processing Letters, 13 (2006) 285-287.

20. Zhang, X. ve Wang, S., Efficient Steganographic Embedding by Exploiting Modification Direction, IEEE Communications Letters, 10, 11 (2006) 781-783.

21. Lou, D. C., Wu, N. I., Wang, C. M., Lin, Z. H. ve Tsai, C. S., A Novel Adaptive Steganography Based on Local Complexity and Human Vision Sensitivity, Journal of Systems and Software, 83, 7 (2010) 1236-1248.

22. Chan, C. K. ve Cheng, L. M., Improved Hiding Data in Images by Optimal Moderately Significant-Bit Replacement, IEE Electron. Letters, 37, 16 (2001) 1017–1018.

23. Huang, N. C., Li, M. T. ve Wang, C. M., Toward Optimal Embedding Capacity for Permutation Steganography, IEEE Signal Processing Letters, 16, 9 (2009) 802-805.

24. Liu, T. Y. ve Tsai, W. H., A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique, IEEE Transactions on Information Forensics and Security, 2 (2007) 24-30.

25. Yang, H. ve Kot, A. C., Pattern-Based Data Hiding for Binary Image Authentication by Connectivity-Preserving, IEEE Transactions on Multimedia, 9 (2007) 475-486.

26. Ito, M., Saito, A. ve Nishizeki, T., Multiple Assignment Scheme for Sharing Secret, Journal of Cryptology, 6, 6 (1993) 15-20.

27. Benaloh, J. C. ve Leichter, J., Generalized Secret Sharing and Monotone Functions, Lecture Notes in Computer Science, 403 (1990) 27-35.

28. Karnin, E. D., Greene, J. W. ve Hellman, M. E., On Secret Sharing Systems, IEEE Transactions on Information Theory, 29, 1 (1983) 35–41.

29. Stinson, D. R., Decomposition Constructions for Secret-Sharing Schemes, IEEE Transactions on Information Theory, 40, 1 (1994) 118–125.

30. Beimel, A., Tassa, T. ve Weinreb, E., Characterizing ideal weighted threshold secret sharing, Journal on Discrete Mathematics, 22,1 (2008) 360–397.

31. Beimel, A. ve Weinreb, E., Monotone Circuits for Monotone Weighted Threshold Functions, Information Processing Letters, 97, 1 (2006) 12–18.

32. Morillo, P., Padr´o, C., S´aez, G. ve Villar, J. L., Weighted Threshold Secret Sharing Schemes, Information Processing Letters, 70, 5 (1999) 211–216.

33. Benaloh, J. ve Leichter, J., Generalized Secret Sharing and Monotone Functions, Lecture Notes in Computer Science, 403 (1989) 27–35.

34. Simmons, G. J., How to (Really) Share a Secret, Lecture Notes in Computer Science, 403 (1989) 390–448.

35. Brickell, E. F., Some Ideal Secret Sharing Schemes, Journal of Combinatorial Mathematics and Combinatorial Computing, 6 (1989) 105–113.

36. Ghodosi, H., Pieprzyk, J. ve Safavi-Naini, R., Secret Sharing in Multilevel and Compartmented Groups, Lecture Notes in Computer Science, 1438 (1998) 367–378.

37. http://en.wikipedia.org/wiki/Secret_sharing, 20 Mayıs 2009.

38. Lin, C., Harn, L., Ye, D., Ideal Perfect Multilevel Threshold Secret Sharing Scheme, Fifth International Conference on Information Assurance and Security, Ağustos 2009, Fuzhou, Bildiriler Kitabı, 118-121.

39. Brickell, E. F., Some Ideal Secret Sharing Schemes, Journal of Combinatorial Mathematics and Combinatorial Computing, 6 (1989) 105–113.

40. Hou, Y.C., Visual Cryptography for Color Images, Pattern Recognition, 36 (2003) 1619-1629.

41. Lin, C. C. ve Tsai, W. H., Visual Cryptography for Gray-Level Images by Dithering Techniques, Pattern Recognition Letters, 24 (2003) 349–358.

42. Shyu, S. J., Efficient Visual Secret Sharing Scheme for Color Images, Pattern Recognition, 39, 5 (2006) 866–880.

43. Wu, C. C. ve Chen, L. H., A Study on Visual Cryptography, Yüksek Lisans Tezi, Institute of Computer and Information Science, National Chiao Tung University, Taiwan,1998.

44. Wu, H. C. ve Chang, C. C., Sharing Visual Multi-Secrets Using Circle Shares, Computer Standards & Interfaces, 28, 1 (2005) 123–135.

45. Shyu, S. J., Huang, S. Y., Lee, Y. K. ve Wang, R. Z., Sharing Multiple Secrets in Visual Cryptography, Pattern Recognition, 40, 12 (2007) 3633-3651.

46. Ateniese, G., Blundo, C., De Santis, A. ve Stinson, D. R., Visual Cryptography for General Access Structures, Information and Computation, 129, 2 (1996) 86–106.

47. Stinson, D. R., An Introduction to Visual Cryptography, Public Key Solutions'97, Nisan 1997, Kanada, Bildiriler Kitabı, 28-30.

48. Verheul, E. R. ve Van Tilborg, H. C. A., Constructions and Properties of k Out of n Visual Secret Sharing Schemes, Designs, Codes and Cryptography, 11, 2 (1997) 179–196.

49. Blundo, C., De Santis, A. ve Stinson, D. R., On the Contrast in Visual Cryptography Schemes, Journal of Cryptology, 12 (1999) 261–289.

50. Hofmeister, T., Krause, M. ve Simon, H., Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography, Theoretical Computer Science, 1276 (1997) 176–185.

51. Cimato, S., De Prisco, R., De Santis, A., Colored Visual Cryptography Without Color Darkening, Theoretical Computer Science, 374 (2007) 261–276.

52. Ito, R., Kuwakado, H. ve Tanaka, H., Image Size Invariant Visual Cryptography, IEICE Transaction on Fundamentals, 10 (1999) 2172-2177.

53. Yang, C. N., New Visual Secret Sharing Schemes Using Probabilistic Method, Pattern Recognition Letters, 25, 4 (2004) 481–494.

54. Cimato, S., Prisco, R. D. ve De Santis, A., Probabilistic Visual Cryptography Schemes, The Compututer Journal, 49, 1 (2006) 97-107.

55. Wang, D., Zhang, L., Ma, N. ve Li, X., Two Secret Sharing Schemes Based on Boolean Operations, Pattern Recognition, 40 (2007) 2776-2785.

56. Ulutas, M., Yazici, R., Nabiyev, V. ve Ulutas, G., (2, 2)-Secret Sharing Scheme with Improved Share Randomness, International Symposium on Computer and Information Sciences, Ekim 2008, İstanbul, Bildiriler Kitabı, 1-5.

57. Ulutas, M., Nabiyev, V. ve Ulutas, G., A PVSS Scheme Based on Boolean Operations with Improved Contrast, International conference on Network and Service Security, Haziran 2009, Paris, Bildiriler Kitabı, 1-5.

58. Rabin, M., Digitalized Signatures and Public-Key Functions as Intractable as Factorization, MIT Laboratory for Computer Science, USA, 1979.

59. Lin, C. C. ve Tsai, W. H., Secret Image Sharing with Steganography and Authentication, Journal of Systems and Software, 73 (2004) 405–414.

60. Chang, C. C. , Chan, C. S. ve Fan, Y. H., A Secret Image Sharing Scheme Based on Vector Quantization Mechanism, Lecture Notes in Computer Science, 4096 (2006) 469-478.

61. Linde, Y., Buzo, A. ve Gray, R. M., An Algorithm for Vector Quantizer Design, IEEE Transactions on Communications, 28 (1980) 84-95.

62. Yang, C. N., Chen, T. S., Yu, K. H. ve Wang, C. C., Improvements of Image Sharing with Steganography and Authentication, Journal of Systems and Software, 80 (2007) 1070-1076.

63. Chang, C. C., Hsieh, Y. P. Ve Lin, C. H., Sharing Secrets in Stego Images with Authentication, Pattern Recognition, 41 (2008) 3130-3137.

64. Yang, C. N. ve Ciou, C. B., A Comment on Sharing Secrets in Stegoimages with Authentication, Pattern Recognition, 42 (2009) 1615-1619.

65. Wu, C. C., Hwang, M. S. ve Kao, S.-J., A New Approach to the Secret Image Sharing with Steganography and Authentication, Imaging Science Journal, 57 (2009) 140-151.

66. Huang, C. P., A New Sharing Secret Algorithm in Stego Images with Authentication, 7th International Conference on Information, Communications and Signal Processing, Aralık 2009, Macau, Bildiriler Kitabı, 1-5.

67. Eslami, Z., Razzaghi, S. H. ve Ahmadabadi, J. Z., Secret Image Sharing Based on Cellular Automata and Steganography, Pattern Recognition, 43 (2010) 397-404.

68. Eslami, Z. ve Ahmadabadi, J. Z., Secret Image Sharing with Authentication-Chaining and Dynamic embedding, Journalof Systems and Software, 84 (2011) 803-809.

69. Chang, C. C., Chen, Y. H. ve Wang, H. C., Meaningful Secret Sharing Technique with Authentication and Remedy Abilities, Information Sciences, 181 (2011) 3073-3084.

70. Wang, S. J., Lin, I.-S., Hsieh, Y. L. ve Weng, C. Y., Secret Sharing Systems with Authentication-Based Steganography, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Ağustos 2008, Washington, Bildiriler Kitabı, 1146-1149.

71. Wu, C. C., Kao, S. J., Kuo, W. C. ve Hwang, M. S., Enhance the Image Sharing with Steganography and Authentication, International Conference on Intelligent Information Hiding and Multimedia Processing, Ağustos 2008, Harbin, Bildiriler Kitabı, 1177-1181.

72. Li, P., Ma, P. ve Su, X., Image Secret Sharing and Hiding with Authentication, International Conference on Pervasive Computing Signal Processing and Applications, Eylül 2010, Harbin, Bildiriler Kitabı, 367-370.

73. Lin, P. Y., Lee, J. S. ve Chang, C. C., Distortion-Free Secret Image Sharing Mechanism Using Modulus Operator, Pattern Recognition, 42 (2009) 886-895.

74. Lin, P. Y. ve Chan, C. S., Invertible Secret Image Sharing with Steganography, Pattern Recognition Letters, 31, 13 (2010) 1887-1893.

75. Chang, C. C., Huang, Y. H. ve Liu, T. C., Reversible Secret Sharing with Distortion Control Mechanism, ICIC Express Letters, 1, 2 (2010) 163-167.

76. Zhou, M., Luo, H., Zhao, Z., Yu, F. X. ve Lu, Z. M., Reversible Secret Image Sharing in Diverse Camouflage Images, ICIC Express Letters, 5, 8 (2011) 2423-2428.

77. Guo, C., Wang, Z. H., Chang, C. C. ve Qin, C., A Secret Image Sharing Scheme with High Quality Shadows Based on Exploiting Modification Direction, Journal of Multimedia, 6, 4 (2011) 341-348.

78. Tompa, M. ve Woll, H., How to Share a Secret with Cheaters, Journal of Cryptology, 1, 2 (1988) 133–138.

79. Brickell, E.F. ve Stinson, D.R., The Detection of Cheaters in Threshold Schemes, Lectur Notes in Computer Science, 403 (1989) 564–577.

80. Wu, T.C. ve Wu, T.S., Cheating Detection and Cheater Identification in Secret Sharing Schemes, IEE Proc. Comput. Digit. Tech., 142, 5 (1995) 367–369.

81. Chang, C.C. ve Hwang, R.J., Efficient Cheater Identification Method for Threshold Schemes, IEE Computers and Digital Techiques, 144, 1 (1997) 23–27.

82. Hwang, R.J., Lee, W.B. ve Chang, C.C., A Concept of Designing Cheater Identification Methods for Secret Sharing, Journal of System and Software, 46, 1 (1999) 7–11.

83. Zhao, R., Zhao, J.J., Dai, F. ve Zhao, F.Q., A New Image Secret Sharing Scheme to Identify Cheaters, Computer Standarts and Interfaces, 31, 1 (2009) 252–257.

84. Hu, C.M. ve Tzeng, W.G., Cheating Prevention in Visual Cryptography, IEEE Transactions on Image Processing, 16, 1 (2007) 36–45.

85. Lin, P. Y. ve Chang, C. C., Cheating Resistance and Reversibility-Oriented Secret Sharing Mechanism, IET Information Security, 5, 2 (2011) 81-92.

86. Chen, C. C. ve Fu, W. Y., A Geometry Based Secret Image Sharing Approach, Journal of Information Science and Engineering, 24 (2008) 1567-1577.

87. Tso, H. K., Sharing Secret Images Using Blakley's Concept, Optical Engineering, 47, 7 (2008) 1-3.

88. Elsheh, E. ve Hamza, A. B., Secret Sharing Approaches for 3D Object Encryption, Expert Systems with Applications, 38, 11 (2011) 1906-13911.

89. Chen, C. C. ve Chang, C. C., Secret Image Sharing Using Quadratic Residues, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kasım 2007, Kaohsiung, Bildiriler Kitabı, 515-518.

90. Schneier B., Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Wiley, Ekim 1995.

91. Chen, S. K. ve Lin, J. C., Fault-Tolerant and Progressive Transmission of Images, Pattern Recognition, 38 (2005) 2466-2471.

92. Fang, W. P., Quality Controllable Progressive Secret Image Sharing- Discrete Cosine Transform Approach, International Journal of Education and Information Technolologies, 1, 1 (2007) 43- 47.

93. Kong, J., Zhang, Y., Meng, X., Zheng, Y. ve Lu, Y., A Scalable Secret Image Sharing Method Based on Discrete Wavelet Transform, Lecture Notes in Computer Science, 4688 (2007) 736-745.

94. Huang, C. P. ve Li, C. C., Secure and Progressive Image Transmission Through Shadows Generated by Multiwavelet Transform, International Conference on Wavelet Analysis and Pattern Recognition, Kasım 2007, Beijing, Bildiriler Kitabı, 1539-1544.

95. Huang, C. P., Hsieh, C. H. ve Huang, P. S., Progressive Sharing for a Secret Image, Journal of Systems and Software, 83 (2010) 517-527.

96. Wang, R. Z. ve Shyu, S.J., Scalable Secret Image Sharing, Signal Processing: Image Communication, 22 (2007) 363-373.

97. Lukac, R. ve Plataniotis, K.N., A Cost-Effective Encryption Scheme for Color Images, Real–Time Imag., 11, 5 (2005) 454–464.

98. Lin, Y. Y. ve Wang, R. Z., Scalable Secret Image Sharing with Smaller Shadow Images, IEEE Signal Processing Letters, 17, 3 (2010) 316-319.

99. Yang, C. N. ve Huang, S. M., Constructions and Properties of k out of n Scalable Secret Image Sharing, Optics Communications, 283 (2010) 1750-1762.

100. Yang, C. N. ve Chu, Y. Y., A General (k, n) Scalable Secret Image Sharing Scheme with the Smooth Scalability, Journal of Systems and Software, 84 (2011) 1726-1733.

101. Lin, C. C. ve Tsai, W. H., Secret Image Sharing with Capability of Share Data Reduction, Optical Engineering, 42, 8 (2003) 2340-2345.

102. Wu, Y. S., Thien, C. C. ve Lin, J. C., Sharing and Hiding Secret Images with Size Constraint, Pattern Recognition, 37 (2004) 1377-1385.

103. Wang, R. Z. ve Su, C. H., Secret Image Sharing with Smaller Shadow Images, Pattern Recognition Letters, 27 (2006) 551-555.

104. Chang, C. C., Lin, C. C., Lin, C.-H. ve Chen, Y.-H., A Novel Secret Image Sharing Scheme in Color Images Using Small Shadow Images, Information Sciences, 178 (2008) 2433-2447.

105. Chang, C.C. ve Wu, M.N., An Algorithm for Color Image Compression Based on Common Bitmap Block Truncation Coding, International Conference on Information Sciences, Mart 2002, North Carolina, Bildiriler Kitabı, 964–967.

106. Thien, C. C. ve Lin, J. C., An Image Sharing Method with User Friendly Shadow Images, IEEE Transactions on Circuits and Systems for Video Technology, 13, 12 (2003) 1161-1169.

107. Yang, C. N., Yu, K. H. ve Lukac R., User Friendly Image Sharing in Multimedia Database Using Polynomials with Different Primes, Lecture Notes in Computer Science, 4352, 2 (2007) 443-452.

108. Fang, W. P., Secret Image Sharing Safety, International Asia-Pacific Conference on Communications, Ekim 2008, Tokyo, Bildiriler Kitabı, 1-4.

109. Chao, K.Y. ve Lin, J.C., User-Friendly Sharing of Images: Progressive Approach Based on Modulus Operations, Journal of Electronic Imaging, 18 (2009) 1–9.

110. Wang, R. Z., Chien, Y. F. ve Lin, Y.-Y., Scalable User Friendly Image Sharing, Journal of Visual Communications and Image Representation, 21 (2010) 751-761.

111. Yang, C. N., Yu, K. H. ve Lukac, R., User-Friendly Image Sharing Using Polynomials with Different Primes, International Journal of Imaging Systems and Technology, 17 (2007) 40-47.

112. Tsai, C. S., Chang, C. C. ve Chen, T. S., Sharing Multiple Secrets in Digital Images, Journal of Systems and Software, 64 (2002) 163-170.

113. Feng, J. B., Wu, H. C., Tsai, C. S. ve Chu, Y. P., A New Multi-Secret Images Sharing Scheme Using Lagrange's Interpolation, Journal of systems and Software, 76 (2005) 327-339.

114. Alvarez, G., Encinas, L. H. ve Rey, A. M., A Multisecret Image Sharing Scheme for Color Images Based on Cellular Automata, Information Sciences, 178 (2002) 4382-4395.

115. Rishiwal, V., Kumar, H., Arya, K. V. ve Yadav, M., Multiple Secret Image Sharing Scheme, International Conference on Industrial and Information Systems, Aralık 2008, Kharagpur, Bildiriler Kitabı, 1-4.

116. Shyu, S. J. ve Chen, Y. R., On Secret Multiple Image Sharing, Workshop on Combinatorial Mathematics and Computation Theory, Nisan 2008, Taiwan, Bildiriler Kitabı, 1-6.

117. Lee, C. F. ve Juan, J. S. T., Multi-Secret Images Sharing Scheme with General Access Structure, 19th Cryptology Information Security Conference, Haziran 2009, Taiwan, Bildiriler Kitabı, 1-6.

118. Lin, Y. T., Juan, J. S. T. ve Wang, Y. C., A Secure and Efficient Multi Use Multi-Secret Images Sharing Scheme for General Access Structure, International Conference on Industrial Informatics, Temmuz 2010, Osaka, Bildiriler Kitabı, 437-442.

119. Hou, Z. ve Gao, H., Multi-secret Images Sharing Based on Matrix Multiplication, International Conference on Network Security, Wireless Communications and Trusted Computing, Nisan 2009, Wuhan, Bildiriler Kitabı I,184-187.

120. Shih, F. Y. ve Wu, Y. Ta , Robust Watermarking and Compression for Medical Images Based on Genetic Algorithms, Journal of Information Sciences, 175, 3 (2005) 200-216.

121. Woo, C. S., Du, J. ve Pham, B., Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images, Workshop on Digital Image Computing, 2005, Australia, Bildiriler Kitabı, 59-64.

122. Zhou, X. Q., Huang, H. K. ve Lou, S. L., Authenticity and Integrity of Digital Mammography Images, IEEE Transaction on Medical Imaging, 20, 8 (2001) 784–791.

123. Chao, H. M., Hsu, C. M. ve Miaou, S. G., A Data-Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records, IEEE Transactions on Information Technology in Biomedicine, 6, 1 (2002) 46-53.

124. Luo, X., Cheng, Q. ve Tan, J., A Lossless Data Embedding Scheme for Medical Images in Application of E-Diagnosis, 25th Annual International Conference of the Engineering in Medicine and Biology Society, Eylül 2003, Athena, Bildiriler Kitabı I, 852–855.

125. Giakoumaki, A., Pavlopoulos, S. ve Koutsouris, D., A Medical Image Watermarking Scheme Based on Wavelet Transform, 25th Annual International Conference of the Engineering in Medicine and Biology Society, Eylül 2003, Athena, Bildiriler Kitabı I, 856–859.

126. Cheng, S., Wu, Q., ve Castleman, K.R., Non-Ubiquitous Digital Watermarking for Record Indexing and Integrity Protection of Medical Images, International Conference on Image Processing, Eylül 2005, League, Bildiriler Kitabı II, 1062-1065.

127. Acharya, R., Niranjan, U.C., Iyengar, S.S., Kannathal, N. ve Min, L.C., Simultaneous Storage of Patient Information with Medical Images in the Frequency Domain, Computer Methods and Programs in Biomedicine, 76 (2004) 13-19.

128. Nayak, J., Bhat, P.S., Kumar, M.S. ve Acharya, R., Reliable Transmission and Storage of Medical Images with Patient Information Using Error Control Codes, India Annual Conference , Aralık 2004, Hindistan, Bildiriler Kitabı,147-150.

129. Srinivasan, Y., Nutter, B., Mitra, S., Phillips, B. ve Ferris, D., Secure Transmission of Medical Records Using High Capacity Steganography, IEEE Symposium on Computer Based Medical Systems, Haziran 2004, Lubbock, Bildiriler Kitabı, 122-127.

130. Anand, D. ve Niranjan, U.C., Watermarking Medical Images with Patient Information, 20th Annual International Conference of the Engineering in Medicine and Biology Society, Kasım 1998, Hong Kong, Bildiriler Kitabı II, 703–706.

131. Coatrieux, C.G., Lecornu, L., Roux, Ch. ve Sankur, B., A Review of Image Watermarking Applications in Healthcare, International Conference on Engineering in Medicine and Biology, Eylül 2006, New York, Bildiriler Kitabı I, 4691-4694.

132. Coatrieux, G., Quantin, C., Montagner, J., Fassa, M., Allaert, F.-A. ve Roux, C., Watermarking Medical Images with Anonymous Patient Identification to Verify Authenticity, Studies in Health Technology and Informatics, 136 (2008) 667-672.

133. Osman, N. A. A., Ibrahim, F., Abas, W. A. B. W., Rahman, H. S. A. ve Ting, H.-N., A Novel Technique for EPR Hiding in Medical Images for Telemedicine, International Conference on Biomedical Engineering, Haziran 2008, Kuala Lumpur, Bildiriler Kitabı I, 703-706.

134. Acharya, R. U., Bhat, P. S., Kumar, S. ve Min, L. C., Transmission and Storage of Medical Images with Patient Information, Computers in Biology and Medicine, 33 (2003) 303-310.

135. Kallel, I. F., Bouhlel, M. S., Lapayre, J. C. ve Garcia, E., Control of Dermatology Image Integrity Using Reversible Watermarking, International Journal of imaging systems and technology, 19, 1 (2009) 5-9.

136. Memon, N. A., Gilani, S. A. M. ve Ali, A., Watermarking of Chest CT Scan Medical Images for Content Authentication, International conference on Information and communication technologies, Ağustos 2009, Karachi, Bildiriler Kitabı, 175-180.

137. Hu, J., Chen, H. H. ve Hou, T. W., A Hybrid Public Key Infrastructure Solution for HIPAA Privacy/Security Regulations, Computer Standarts & Interfaces, 32 (2010) 274-280.

138. Ho, A. T. S., Zhu, X. ve Shen, J., Authentication of Biomedical Images Based on Zero Location Watermarking, Control, Automation, Robotics and Vision Conference, Aralık 2004, Kunming, Bildiriler Kitabı II, 973-976.

139. Nayak, J., Bhat, P. S., Rajendra, U., Acharya, M. ve Kumar, S., Efficient Storage and Transmission of Digital Fundus Images with Patient Information Using Reversible

Watermarking technique and error control codes, Journal of Medical Systems, 33 (2009) 163-171.

140. Li, M., Poovendran, R. ve Narayanan, S., Protecting Patient Privacy Against Unauthorized Release of Medical Images in a Group Communication Environment, Computerized Medical Imaging and Graphics, 29 (2005) 367-383.

141. Lou, D. C., Hu, M. C. ve Liu, J. L., Multiple Layer Data Hiding Scheme for Medical Images, Computer Standarts and Interfaces, 31 (2009) 329-335.

142. Hu, J. ve Han, F., A Pixel Based Scrambling Scheme for Digital Medical Images Protection, Journal of Network and Computer Applications, 32 (2009) 788-794.

143. Barbara, R., Two short proofs of Morley's Theorem, The Mathematical Gazette, 81, 492 (1997) 447-450.

144. Shyu, S. J. ve Chen, Y. R., Threshold Secret Image Sharing by Chinese Remainder Theorem, Asia-Pacific Services Computing Conference, Aralık 2008, Taoyuan, Bildiriler Kitabı, 1332-1337.

145. Ulutas, M., Nabiyev, V. ve Ulutas, G., Improvements in Geometry Based Secret Image Sharing Approach with Steganography, Mathematical Problems in Engineering, doi:10.1155/2009/187874.

146. Ulutas, M., Ulutas, G. ve Nabiyev. V., Secret Image Sharing with Enhanced Visual Quality and Authentication Mechanism, Imaging Science Journal, 59, 3 (2011) 154-165.

147. Ulutas, M., Ulutas, G. ve Nabiyev, V., Medical Image Security and EPR hiding using Shamir's secret sharing scheme, Journal of Systems and Software, 84, 3 (2011) 341-353.

148. Ulutas, G., Ulutas, M. ve Nabiyev, V., A new (3, 3) Secret Image Sharing Scheme based on Morley's Theorem, World Conference on Information Technology, Kasım 2011, Antalya, Bildiriler Kitabı, 1-5.

149. Ulutas, M., Nabiyev, V. ve Ulutas, G., A New Secret Image Sharing Technique Based On Asmuth Bloom's Scheme, Application on Information and Communication Technologies, Ekim 2009, Bakü, Bildiriler Kitabı,1-5.

150. Ulutas, M., Nabiyev, V. ve Ulutas, G., Asmuth-Bloom Yönteminin Steganografi ile Beraber Gizli Görüntü Paylaşımında Kullanımı, 4th International Information Security and Cryptology Conference, Mayıs 2010, Ankara, Bildiriler Kitabı, 1-6.

151. Ulutas, G., Ulutas, M. ve Nabiyev, V., Mignotte'nin Şemasına Dayanan Gizli Görüntü Paylaşma Şeması, Sinyal İşleme ve Uygulamaları, Nisan 2011, Antalya, Bildiriler Kitabı, 291-294.

152. Lee, C. F., Wang, Y. R. ve Chang, C. C., A Steganographic Method with High Embedding Capacity by Improving Exploiting Modification Direction, Intelligent Information Hiding and Multimedia Signal Processing Conference, Kasım 2007, Kaohsiung, Bildiriler Kitabı, 497-500.

153. Makoto, M., Objective picture quality scale (PQS) for image coding, IEEE Transactions on Communications, 46, 9 (1998) 1215–1226.

154. Robb, R. A., Biomedical Imaging, Visualization, and Analysis, Wiley-Liss, December 1999.

155. http://www.barre.nom.fr/medical/samples/ Medikal görüntüler. 21 Kasım 2010.

156. http://marathon.casee.usf.edu/mammography/database.html Mamogram görüntüleri. 22 Kasım 2010.

157. Rivest, R., "The MD4 Message Digest Algorithm", RFC 1320, MIT ve RSA Data Security, Inc., Nisan 1992.

7. EKLER

Ek-1. Çinli Kalan Teoremi

Herhangi bir sayının farklı modulo tabanlarındaki kalanları biliniyorsa ve taban değerleri aralarında asal ise, denklik sisteminin biricik çözümü, Çinli Kalan Teoremi (ÇKT) yardımı ile elde edilebilir. x sayısının $m_1, m_2, \cdots, m_k$ tabanlarındaki kalanlarını ifade eden denklik sistemi (E.1)'deki gibi verilmiş olsun.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \qquad \text{(E.1)}$$

ÇKT verilmiş olan denklik sisteminin, seçilen taban değerlerinin aralarında asal olması durumunda biricik bir çözümü olduğunu ifade eder. Seçilen x sayısı 3, 5 ve 7 tabanlarında sırasıyla 2, 3 ve 2 kalanlarını versin. Verilen değerler için çözüm üreten x değeri 23 olmaktadır. 23 değeri verilen tabanlarda karşılık düşen kalanları vermektedir. Biricik çözümün elde edilmesinde uygulanan adımlar aşağıdaki şekildedir.

1. Genel taban değerini gösteren M, $M = m_1 \times m_2 \times \ldots \times m_k$ ifadesi yardımıyla hesaplanır.
2. Her bir denklik için $M_1 = M/m_1, M_2 = M/m_2, \cdots, M_k = M/m_k$ değerleri elde edilir.
3. $M_1, M_2, \cdots, M_k$'nın çarpmaya karşı tersleri karşılık düşen taban değerleri $m_1, m_2, \cdots, m_k$ kullanılarak hesaplanır $M_1^{-1}, M_2^{-1}, \cdots, M_k^{-1}$.
4. Verilen denklik sistemleri için çözüm oluşturan x değeri, önceki adımlarda hesaplanan değerlerin kullanımı ile (E.2)'deki gibi hesaplanır.

$$x = \left(a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}\right) \bmod M \qquad \text{(E.2)}$$

Yukarıda verilmiş olan örnek için ÇKT'nin uygulanma aşamaları ve 23 olarak verilen çözümün elde edilmesi şu şekildedir:

1. $M = 3 \times 5 \times 7 = 105$
2. $M_1 = 105/3 = 35,\ M_2 = 105/5 = 21,\ M_3 = 105/7 = 15$
3. $M_1^{-1} = 2,\ M_2^{-1} = 1,\ M_3^{-1} = 1$
4. $x = \left(2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1\right) \bmod 105 = 23 \bmod 105$.

Ek-2. MD5 (Message Digest 5) Özüt Fonksiyonu

MD5 fonksiyonu girişten aldığı veri hakkında 128 bit uzunluğunda özet bilgi üreten ve detayları RFC 1321'de verilen özüt fonksiyonudur [157]. Birçok güvenlik uygulamasında yer alan MD5 fonksiyonu, 1991'de Ron Rivest tarafından önceki özüt fonksiyonu yerine (MD4) önerilmiştir. MD5 algoritması, MD4'e göre daha yavaştır.

Algoritma girişten gelen herhangi bir uzunluktaki veriyi, 512 bitten oluşan parçalara böler. Verinin 512'nin katı olmaması durumunda, ekleme (padding) işlemi gerçekleştirilir. Ekleme işleminde 448'in tam katı olacak şekilde, verinin sonuna eklenecek olan bit dizisindeki ilk değer 1'dir. Geriye kalan bit değerleri ise 0 olacaktır. Ardından verinin orijinal uzunluğunun 64 bitteki temsili eklenir.

MD5 fonksiyonu (A, B, C, D) ile isimlendirilen ve her biri 32 bit olan dört adet kaydedici kullanır. Kaydedicilere (E.3)'de verildiği gibi başlangıç değerleri atanır.

$$\begin{aligned} A &: 01 \quad 23 \quad 45 \quad 67 \\ B &: 89 \quad ab \quad cd \quad ef \\ C &: fe \quad dc \quad ba \quad 98 \\ D &: 76 \quad 54 \quad 32 \quad 10 \end{aligned} \tag{E.3}$$

Algoritmanın, mantıksal operatörleri kullanan ve F, G, H, I ile gösterilen dört adet yardımcı fonksiyonu vardır. İlgili fonksiyonlara ilişkin ifadeler (E.4)'te verilmektedir.

$$\begin{aligned} F(X,Y,Z) &= XY \vee (\overline{X})Z \\ G(X,Y,Z) &= XZ \vee Y(\overline{Z}) \\ H(X,Y,Z) &= X \oplus Y \oplus Z \\ I(X,Y,Z) &= Y \oplus (X \vee \overline{Z}) \end{aligned} \tag{E.4}$$

Girişten gelen veri 512 bit büyüklüğündeki bölümlere ayrılır. Her bir bölümün 16 adet 32 bit kelimeden oluştuğu varsayılır. Bir bölümdeki kelimeler $w[j], 0 \le j \le 15$ ile gösterilsin. Bölümün elemanları 64 kere çalışan bir döngü içerisinde kullanılmaktadır. Döngünün $[0-15], [16-31], [32-47], [48-63]$ değer aralıklarında kullanmış olduğu yardımcı fonksiyonlar sırasıyla F, G, H ve I şeklindedir. Algoritmaya ilişkin yalancı kod ifadesi aşağıda verilmiştir. ($a << b$) ifadesi, a ile gösterilen sayının b bit sola kaydırılması anlamını taşımaktadır. bol(x, y) fonksiyonu ise x girişindeki bit dizisini her biri y bitten oluşan parçalara ayırmaktadır. Giriş verisinin her 512 bitlik bölümü üzerinde hesaplanan özüt değeri, bir önceki bölümün çıkışına eklenmektedir. Sonuçta üretilen veri, yalancı kod ifadesinden de gözlemlenebileceği gibi 128 bit uzunluğundadır.

Ek-2'nin Devamı

```
var int[64] r, k
var int h0 := 0x67452301
var int h1 := 0xEFCDAB89
var int h2 := 0x98BADCFE
var int h3 := 0x10325476

r[ 0..15] := {7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22}
r[16..31] := {5,  9, 14, 20, 5,  9, 14, 20, 5,  9, 14, 20, 5,  9, 14, 20}
r[32..47] := {4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23}
r[48..63] := {6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21}
for i from 0 to 63
   k[i] := floor(abs(sin(i + 1)) × (2 pow 32))
end
// 512 bitlik her bir blok için aşağıdaki işlemler tekrarlanır
for i = 0 : blok_sayisi
   var int a := h0
   var int b := h1
   var int c := h2
   var int d := h3
      // İşlem görmekte olan bölüm 32 bitten oluşan 16 kelimeye ayrılır
   w = bol (blok(i), 16);
   for i = 0: 63
      if 0 ≤ i ≤ 15 then
         f := (b and c) or ((not b) and d)
         g := i
      else if 16 ≤ i ≤ 31
         f := (d and b) or ((not d) and c)
         g := (5×i + 1) mod 16
      else if 32 ≤ i ≤ 47
         f := b xor c xor d
         g := (3×i + 5) mod 16
      else if 48 ≤ i ≤ 63
         f := c xor (b or (not d))
         g := (7×i) mod 16
      temp := d
      d := c
      c := b
      b := b + ((a + f + k[i] + w[g]) << r[i])
      a := temp
   end
//O anki bölüm için hesaplanan özüt değeri geçici sonuca eklenir
   h0 := h0 + a
   h1 := h1 + b
   h2 := h2 + c
   h3 := h3 + d
end
```

Ek-3. Geometri Tabanlı Gizli Görüntü Paylaşım Şemasındaki Paylaştırma Algoritması

Bu bölümde, yapılan çalışmalar kısmında önerilmiş olan geometri tabanlı gizli görüntü paylaşım şemasındaki paylaştırma algoritmasının yalancı kod ile gösterimi verilmektedir. Algoritma, giriş olarak $N \times M$ büyüklüğünde S ile gösterilen gizli görüntü ve n adet $C_i, i = 1 \cdots n$ ile gösterilen örten görüntü almaktadır. Gizli görüntünün algoritma tarafından paylaştırılması ve saklanmasının ardından üretilen stego görüntüler ise $ST_i, i = 1 \cdots n$ ile verilmektedir. Yalancı kod ifadesinde kullanılan pow(x, y) fonksiyonu x sayısının y kuvvetini geri döndürmektedir. ceil(x) fonksiyonu ise, x sayısını kendisinden büyük ilk tamsayıya yuvarlamaktadır. Bit düzeyindeki OR ve AND işlemleri ise sırasıyla '$\vee$' ve '$\wedge$' sembolleri ile bit düzeyinde sağa kaydırma ise '>>' ile gösterilmektedir.

```
b = []; j = 1;
bit = 8;
for i = k : -1 : 1
  kalan = ceil (bit / i);
  b(j) = kalan;
  bit = bit – kalan;
  j = j + 1;
end

for i = 1 : N
  for j = 1 : M
          grup = S (i, j: j + k -1);
          for m = 1: n
                  orten_blok = C_m (i, j: j + k - 1);
                  a = [];
                  for x = 1: k
                          a (x) = (orten_blok(x) ∧ (256-pow(2, b(x)))) / pow(2, b(x));
                  end
                  B = 0;
                  for x = 1: k
                          B = B + a(x) * grup (x);
                  end
                  B = mod (B, 251);
                  temp = 0;
                  for x = 1: k
                          temp = temp + b(i);
                          deger = (B>>(8-temp)) ∧ (pow(2, b(x))-1);
                          temp2 = orten_blok(x) ∧ (256-(pow(2, b(x))));
                          temp2 = temp2 ∨ deger;
                          orten_blok (x) = temp2;
                  end
          ST_m (i, j: j + k - 1) = orten_blok;
          end
  end
end
```

Ek-4. Steganografi Tabanlı ve Doğrulama Mekanizmalı Şemadaki Paylaştırma Algoritması

Yapılan çalışmalar kısmında verilen yöntemin paylaştırma algoritmasının yalancı kod ifadesi bu bölümde verilmektedir. $N \times M$ büyüklüğündeki gizli görüntü S, $C_i, i = 1 \cdots n$ ile gösterilen örten görüntüler kullanılarak paylaştırılmakta ve $ST_i, i = 1 \cdots n$ stego görüntüleri elde edilmektedir. Yalancı kod ifadesinde kullanılan hash() fonksiyonu girişinden verilen verinin SHA(Secure Hash Algorithm) özüt fonksiyonu sonucunu üretmektedir. round(x) fonksiyonu x ile verilen sayıyı yuvarlamakta kullanılırken, floor(x) fonksiyonu x sayısından küçük ilk tamsayıyı geri döndürür. rand(1) fonksiyonu, [0-1] aralığında rasgele sayılar üretmede kullanılırken, xor(x, y) fonksiyonu iki sayının bit düzeyinde XOR işlemini gerçekleştirir. Paylaştırma algoritmasına ilişkin yalancı kod ifadesi aşağıdaki şekildedir.

```
for i = 1 : N
  for j = 1 : M
        katsayi (1) = floor (S(i, j) / 31);
        katsayi (2) = mod (S(i, j), 31);
        for t = 3: k
            katsayi (t) = round (rand(1) * 30);
        end
        for t = 1: n
            B = Cm ( ((i-1) * 2+1): ((i-1) * 2 + 2), ((j-1) * 2 + 1): ((j-1) * 2) + 2) );
            X = B(1, 1) >> 2;
            toplam = 0;
            for d = 1: k
                toplam = toplam + katsayi (d) * pow (x, d-1);
            end
            toplam = mod (toplam, 31);
            B (1, 1) = B (1, 1) ∧ 252;
            B (1, 1) = B (1, 1) ∨ (toplam >> 3);
            B (1, 2) = B (1, 2) ∧ 252;
            B (1, 2) = B (1, 2) ∨ ((toplam>>1) ∧3);
            B (2, 1) = B (2, 1) ∧ 254;
            B (2, 1) = B (2, 1) ∨ (toplam ∧ 1);
            G = hash (B); G(161) = 1; G(162) = 1;
            sayi = G(1) * 4 + G(2) * 2 + G(3);
            for d = 4: 3: 162
                temp = G(d) * 4 + G(d+1) * 2 + G(d+2);
                sayi = xor (sayi, temp);
            end
            B(2, 1) = B (2, 1) ∧ 253;
            B(2, 1) = B (2, 1) ∨ ((sayi ∧4)>>1);
            B(2, 2) = B (2, 2) ∧ 252;
            B(2, 2) = B (2, 2) ∨ (sayi ∧3);
            STm ( ((i-1) * 2+1): ((i-1) * 2 + 2), ((j-1) * 2 + 1): ((j-1) * 2) + 2) ) = B;
        end
  end
end
```

Ek-5. EMD'ye Dayanan Geri Döndürülebilir Gizli Görüntü Paylaşım Şemasındaki Paylaştırma Algoritması

Geri döndürülebilir gizli görüntü paylaşımı alanında gerçekleştirilen ve detayları yapılan çalışmalar kısmında verilen yöntemin paylaştırma ve saklama prosedürlerine ilişkin yalancı kod ifadesi bu bölümde verilmektedir. $N \times M$ büyüklüğündeki gizli görüntü T, C ile gösterilen $2N \times 2M$ büyüklüğündeki örten görüntü kullanılarak paylaştırılmakta ve $ST_i, i = 1 \cdots n$ stego görüntüleri elde edilmektedir.

```
m = 1;
for i = 1: N
    for j = 1: M
        S (m) = (t(i, j) – mod(t(i, j), 17)) / 17;
        S (m + 1) = mod (t(i, j+1), 17); m = m + 2;
    end
end
d = 1;
for i = 1: 2N
    for j = 1: 2M
        if (C(i, j) ≥ 254)                          x1 =  -4; x2 = 0; end
        if (C(i, j) ≤ 1)                            x1 =   0; x2 = 4; end
        if (C(i, j+1) ≥ 254)                        y1 = -4; y2 = 0; end
        if (C(i, j+1) ≤ 1)                          y1 =  0; y2 = 4; end
        if (C(i, j) ≥ 2) and (C(i, j) ≤ 253)        x1 = -2; x2 = 2; end
        if (C(i, j+1) ≥ 2) and (C(i, j+1) ≤ 253)    y1 = -2; y2 = 2; end
        f = mod (C(i, j) + 4 * C(i, j+1), 17);
        for m = 1: n
            toplam = 0; katsayi = S (d: d+k-3);
            katsayi (k-1) = mod (C(i, j), 9); katsayi (k) = mod (C(i, j+1), 9);
            for c = 1: k
                toplam = toplam + katsayi (c) * pow (m, c-1);
            end
            toplam = mod (toplam, 17);
            if f = toplam
                ST_m (i, j) = C(i, j); ST_m (i, j+1) = C(i, j+1);
            else
                for x = x1: x2
                    for y = y1: y2
                        b = x + 4 * y;
                        if (mod (b+f), 17)=toplam
                            ST_m (i, j: j+1) = [C(i, j) + x, C(i, j+1) + y];
                        end
                    end
                end
            end
            d = d + k - 2;
        end
    end
end
```

Ek-6. Adaptif Doğrulama Yeteneğine Sahip Gizli Görüntü Paylaşım Şemasındaki Paylaştırma Algoritması

Adaptif doğrulama yeteneğine sahip paylaştırma algoritmasının yalancı kod ifadesi aşağıda verilmektedir. $CN \times CM$ büyüklüğündeki örten görüntüler kullanılarak SN×SM büyüklüğündeki gizli görüntü, $ST_i, i = 1 \cdots n$ stego görüntülerine paylaştırılmaktadır. Yalancı kod ifadesinde kullanılan donustur(x, y) fonksiyonu, x ile verilen değerin y tabanındaki ifadesini geri döndürmektedir. emd (A[], x, y) fonksiyonu y sayısını A katsayılarına x tabanını kullanarak EMD yöntemi ile saklamakta ve katsayıların yeni değerlerini geri döndürmektedir. xor_grup (x, y) fonksiyonu x ile gösterilen bit dizisini kendi içerisinde y bitlik gruplar şeklinde XOR'layarak y bit sonuç geri döndürmektedir. logaritma(x, y) ise $\log_x y$ değerini üreten bir fonksiyondur.

```
L = floor ( (CN*CM*k) / (SN*SM) );
for ms = 8 : 8: 16
   if (L-2) ≥ (2*(logaritma (ms, 255)))
      CPS = ceil (logaritma (ms, 255));
      CPA = floor((L - 2*CPS)/2);
      if CPA = 1        ma = 16
      else              ma = 8
      end
      break
   end
end
cx = 1, cy = 1;
for i=1 : SN
   for j=1 : L : SM
      pay =  üret(S (i, j: j + k - 1), [1..n] );
      for t = 1 : n
         pay_rakam = donustur(pay(t), ms);
         B = Ct (cx, cy: cy + L - 1); ind = 1;
         for z = 1 : 2: 2*CPS
            B (z : z+1) = emd( B (z : z+1, ms, pay_rakam(ind));
            ind = ind + 1;
         end
         STt (cx, cy : cy + L - 1) = B;
         R = xor_grup (hash(B), ceil(logaritma(2, pow(ma,CPA))));
         r = donustur(R, ma);
         sonraki_B = Ct (cx, cy + L : cy + 2*L - 1); ind = 1;
         for z=1 : 2: 2*CPA
            sonraki_B (L-z+1 : L-z)= emd (sonraki_B(L-z+1 : L-z), ma, r(ind));
            ind = ind + 1;
         end
         STt (cx, cy + L : cy + 2*L - 1) = sonraki_B;
      end
      cy = cy + L;
   end
   cx = cx + 1;
end
```

Ek-7. Medikal Görüntü Örneğinde Bilgi Güvenliğinin Sağlanması Yaklaşımındaki Paylaştırma Algoritması

Medikal görüntü güvenliğini sağlamak için önerilen yöntemin, M ile gösterilen ve $H \times W$ büyüklüğünde olan gizli görüntüyü paylaştırma ve saklama esnasında kullanmış olduğu yalancı kod ifadesi aşağıda verilmektedir. Elektronik hasta kaydı ise E ile gösterilen dizi de tutulmaktadır. Algoritmanın çıkışında n adet ve $ST_i, i = 1 \cdots n$ ile gösterilen stego görüntü üretilmektedir.

```
y = 1;
for i = 1: H
  for j = 1: W
        piksel = M(i, j); temp = piksel; x = 1;
        while (temp > 0)
              sayi (x) = mod (temp, 251); temp = floor (temp / 251); x = x + 1;
        end
        x = x – 1;
        for d = 1: x
              medikal (d) = sayi (x – d + 1);
        end
        for d = x + 1: k
              medikal(d) = E(y); y = y + 1;
        end
        for m = 1: n
            B = Cm ( ((i-1) * 2+1): ((i-1) * 2 + 2), ((j-1) * 2 + 1): ((j-1) * 2) + 2) );
            a = B(1, 1); b = B(1, 2); c = B(2, 1); d = B(2, 2);
            toplam = 0;
            for d = 1: k
                toplam = toplam + medikal(d)*pow(xm, (d-1));
            end
            toplam = mod (toplam, 251);
            ay = (a ∧ 252) ∨ (toplam>>6);
            by = (b ∧ 252) ∨ ((toplam>>4) ∧ 3);
            cy = (c ∧ 252) ∨ ((toplam>>2) ∧ 3);
            dy = (d ∧ 252) ∨ (toplam ∧ 3);
            farka = ay – a; farkb = by – b; farkc = cy – c; farkd = dy – d;
            a = OPAP (farka, ay); b = OPAP (farkb, by);
            c = OPAP (farkc, cy); d = OPAP (farkd, dy);
            STm(((i-1) * 2+1):((i-1)* 2 + 2), ((j-1) * 2 + 1):((j-1) * 2)+2))=[a b; c d];
        end
  end
end
sonuc = function OPAP (fark, stego)
        if (fark>2) and (fark<4) and (stego ≥ 4) sonuc = stego-4; end;
        if (fark>2) and (fark<4) and (stego<4) sonuc = stego; end;
        if (fark ≥ -2) and (fark ≤ 2) sonuc = stego; end;
        if (fark>-4) and (fark<-2) and (stego<252) sonuc = stego+4; end;
        if (fark>-4) and (fark<-2) and (stego ≥ 252) sonuc = stego; end;
  return sonuc;
```

Ek-8. Morley'in Teoremine Dayanan (3, 3) Gizli Görüntü Paylaşım Şemasının Paylaştırma Prosedürü

Morley'in üçgen teoremini kullanan sır paylaşma şemasına ilişkin paylaştırma algoritmasının kaynak kodu aşağıda verilmektedir. Yöntem öncelikle gizli görüntüyü iki pikselden oluşan bölümlere ayırmaktadır. Her bir bölüm ise morley_aci fonksiyonu yardımıyla dış üçgenin belirlenmesinde kullanılır. Fonksiyonun geri dönüş değerleri olan, Morley'in dış üçgeninin köşe koordinatları ise katılımcılara gönderilecek pay değerlerini oluşturur. bol(x, y) fonksiyonu, toplam 22 bit olan x ve y koordinatlarını sırasıyla 8, 8 ve 6 bite bölerek geri döndürmektedir.

```
satir, sutun = 1;
for i=1: N
  for j = 1: 2: M-1
            kenar = S(i, j);
            aci = S(i, j + 1);

            kose = morley_aci (kenar, aci);

            gecici = bol (kose(1,1), kose(1, 2));
            pay1(satir, sutun,1:3) = gecici(1:3);

            gecici = bol (kose(2,1), kose(2, 2));
            pay2(satir, sutun,1:3) = gecici(1:3);

            gecici = bol (kose(3,1), kose(3, 2));
            pay3(satir, sutun,1:3) = gecici(1:3);

            sutun = sutun + 1;
  end
  sutun = 1;
  satir = satir + 1;
end

function sonuc = morley_aci (k, aci)
a = [0, 0];
b = [k*cos((60+aci)*pi/180) k*sin((60+aci)*pi/180)];
c = [k*cos(aci*pi/180) k*sin(aci*pi/180)];
aci1 = round (rand(1) * 50); aci2 = round (rand(1)*40); aci3 = 120 - (aci1 + aci2);

% d, e, f → ikizkenar üçgenlerin tepe noktalarıdır
r=k/(2*cos(aci1*pi/180));
d = [r*cos((60+aci1+aci)*pi/180) r*sin((60+aci1+aci)*pi/180)];

r = k/(2*cos(aci2*pi/180));
e=  [k*cos(aci*pi/180)+r*cos((120-aci2+aci)*pi/180)  k*sin(aci*pi/180)+r*sin((120-
aci2+aci)*pi/180)];
r = k/(2*cos(aci3*pi/180));
f = [r*cos((aci-aci3)*pi/180) r*sin((aci-aci3)*pi/180)];
```

Ek-8'in Devamı

```
if ((abs(b(1,1)-e(1,1)))==0)
   m_be = 0; b_be = b(1, 1); m_af = (a(1,2)-f(1,2)) / (a(1,1) - f(1,1));
   b_af = a(1,2)-m_af * a(1, 1); be = [0 b_be];
   af = [m_af b_af];
   k1_x = b(1,1);
   k1_y = be(1,1) * k1_x + be(1,2);
elseif ((abs(a(1,1)-f(1,1)))==0)
   m_be = (b(1,2)-e(1,2)) / (b(1,1) - e(1,1)); m_af = 0;
   b_be = b(1,2)-m_be * b(1, 1); b_af = a(1, 1);
   be = [m_be b_be]; af = [m_af b_af];
   k1_x = a(1,1);
   k1_y = be(1,1) * k1_x + be(1,2);
elseif ((abs(a(1,2)-f(1,2)))==0)
   m_be = (b(1,2)-e(1,2)) / (b(1,1) - e(1,1)); b_be = b(1,2)-m_be * b(1, 1);
   m_af = 0; b_af = a(1, 2); be = [m_be b_be];
   af = [m_af b_af]; k1_y = a(1,2);
   k1_x = (k1_y - be(1,2))/(be(1,1));
elseif ((abs(b(1,2)-e(1,2)))==0)
   m_af = (a(1,2)-f(1,2)) / (a(1,1) - f(1,1)); b_af = a(1,2)-m_af * a(1, 1);
   m_be = 0; b_be = b(1, 2);
   be = [m_be b_be]; af = [m_af b_af];
   k1_y = b(1,2); k1_x = (k1_y - af(1,2))/(af(1,1));
else
   m_be = (b(1,2)-e(1,2)) / (b(1,1) - e(1,1)); m_af = (a(1,2)-f(1,2)) / (a(1,1) - f(1,1));
   b_be = b(1,2)-m_be * b(1, 1); b_af = a(1,2)-m_af * a(1, 1);
   be = [m_be b_be]; af = [m_af b_af];
   k1_x = (af(1,2)-be(1,2))/(be(1,1)-af(1,1)); k1_y = be(1,1) * k1_x + be(1,2);
 end
if (abs(c(1,1)-f(1,1))) ==0
   m_cf = 0; cf = [0 c(1,1)];m_bd = (b(1,2)-d(1,2)) / (b(1,1) - d(1,1));
   b_bd = b(1,2)-m_bd * b(1, 1); bd = [m_bd b_bd];
   k2_x = c(1,1); k2_y = bd(1,1) * k2_x + bd(1,2);
elseif (abs(b(1,1)-d(1,1))) ==0
   m_bd = 0; bd = [0 b(1,1)]; m_cf = (c(1,2)-f(1,2)) / (c(1,1) - f(1,1));
   b_cf = c(1,2)-m_cf * c(1, 1); cf = [m_cf b_cf];
   k2_x = b(1,1); k2_y = cf(1,1) * k2_x + cf(1,2);
elseif ((abs(c(1,2)-f(1,2)))==0)
   m_bd = (b(1,2)-d(1,2)) / (b(1,1) - d(1,1)); b_bd = b(1,2)-m_bd * b(1, 1);
   m_cf = 0; b_cf = c(1, 2); bd = [m_bd b_bd];
   cf = [m_cf b_cf]; k2_y = c(1,2); k2_x = (k2_y - bd(1,2))/(bd(1,1));
elseif ((abs(b(1,2)-d(1,2)))==0)
   m_cf = (c(1,2)-f(1,2)) / (c(1,1) - f(1,1)); b_cf = c(1,2)-m_cf * c(1, 1);
   m_bd = 0; b_bd = b(1, 2);
   bd = [m_bd b_bd]; cf = [m_cf b_cf];
   k2_y = d(1,2); k2_x = (k2_y - cf(1,2))/(cf(1,1));
else
```

Ek-8'in Devamı

```
   m_cf = (c(1,2)-f(1,2)) / (c(1,1) - f(1,1)); b_cf = c(1,2)-m_cf * c(1, 1);
   cf = [m_cf b_cf]; m_bd = (b(1,2)-d(1,2)) / (b(1,1) - d(1,1));
   b_bd = b(1,2)-m_bd * b(1, 1); bd = [m_bd b_bd];
   k2_x = (cf(1,2)-bd(1,2))/(bd(1,1)-cf(1,1));
   k2_y = bd(1,1) * k2_x + bd(1,2);
 end

if (abs(c(1,1) - e(1,1))) == 0
   m_ce = 0; b_ce = c(1, 1); ce = [m_ce b_ce];
   m_ad = (a(1,2)-d(1,2)) / (a(1,1) - d(1,1)); b_ad = a(1,2)-m_ad * a(1, 1);
   ad = [m_ad b_ad]; k3_x = c(1,1); k3_y = ad(1,1) * k3_x + ad(1,2);
elseif (abs(a(1,1) - d(1,1))) == 0
   m_ce = (c(1,2)-e(1,2)) / (c(1,1) - e(1,1)); b_ce = c(1,2)-m_ce * c(1, 1);
   ce = [m_ce b_ce]; m_ad = 0; b_ad = a(1, 1);
   ad = [m_ad b_ad]; k3_x = a(1,1); k3_y = ad(1,1) * k3_x + ad(1,2);
elseif ((abs(c(1,2)-e(1,2)))==0)
   m_ad = (a(1,2)-d(1,2)) / (a(1,1) - d(1,1)); b_ad = a(1,2)-m_ad * d(1, 1);
   m_ce = 0; b_ce = c(1, 2);
   ad = [m_ad b_ad]; ce = [m_ce b_ce]; k3_y = c(1,2);
   k3_x = (k3_y - ad(1,2))/(ad(1,1));
elseif ((abs(a(1,2)-d(1,2)))==0)
   m_ce = (c(1,2)-e(1,2)) / (c(1,1) - e(1,1)); b_ce = c(1,2)-m_ce * c(1, 1);
   m_ad = 0; b_ad = d(1, 2); ad = [m_ad b_ad];
   ce = [m_ce b_ce]; k3_y = d(1,2);
   k3_x = (k3_y - ce(1,2))/(ce(1,1));
else
   m_ce = (c(1,2)-e(1,2)) / (c(1,1) - e(1,1)); b_ce = c(1,2)-m_ce * c(1, 1);
   ce = [m_ce b_ce]; m_ad = (a(1,2)-d(1,2)) / (a(1,1) - d(1,1));
   b_ad = a(1,2)-m_ad * a(1, 1); ad = [m_ad b_ad];
   k3_x = (ce(1,2)-ad(1,2))/(ad(1,1)-ce(1,1));
   k3_y = ad(1,1) * k3_x + ad(1,2);
end

x_deger = min([k1_x k2_x k3_x]);
 y_deger = min([k1_y k2_y k3_y]);

% I. bölgeye öteleme
if x_deger<0
  x_deger=abs(x_deger);
  k1_x=k1_x+x_deger; k2_x=k2_x+x_deger;k3_x=k3_x+x_deger;
end
if y_deger<0
  y_deger=abs(y_deger);
  k1_y=k1_y+y_deger; k2_y=k2_y+y_deger;k3_y=k3_y+y_deger;
end
x_deger = floor((min([k1_x k2_x k3_x])+max([k1_x k2_x k3_x]))/5);
y_deger = floor((min([k1_y k2_y k3_y])+max([k1_x k2_x k3_x]))/5);
```

Ek-8'in Devamı

```
ekstra_x = x_deger;
ekstra_y = y_deger;
ekstra_x = double(round(rand(1)*ekstra_x));
ekstra_y = double(round(rand(1)*ekstra_y));
k1_x=k1_x+ekstra_x; k2_x=k2_x+ekstra_x;k3_x=k3_x+ekstra_x;
k1_y=k1_y+ekstra_y; k2_y=k2_y+ekstra_y;k3_y=k3_y+ekstra_y;
sonuc = round([k1_x k1_y;k2_x k2_y;k3_x k3_y]);
end

function sonuc = bol_color(piksel1, piksel2, bit)
a = bitshift(piksel1,-3);
b = bitshift(piksel2,-3);
ilkuc = bitand(piksel1,7);
sonuc = bitand(piksel2,7);
c = ilkuc * 8 + sonuc;
sonuc=  [a b c];
end
```

ÖZGEÇMİŞ

Güzin ULUTAŞ; 1980 yılında Trabzon'da doğdu. İlk ve orta öğrenimini Trabzon'da tamamladı. 1998 yılında Fatih Süper Lisesi'nden mezun oldu. 1998 yılında, ÖSYS ile yerleştirildiği Karadeniz Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü'nü 2002 yılında bölüm üçüncüsü derecesi ile bitirdi. 2004 yılında aynı bölümde yüksek lisansını tamamladı. 2007 yılında Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı'nda doktora çalışmalarına başladı. 2002-2004 yıllarında KTÜ Bilgisayar Mühendisliği Bölümünde Fen bilimlerine bağlı Araştırma Görevlisi, 2005-2009 yıllarında OMÜ Bilgisayar Mühendisliği Bölümünde Dekanlığa bağlı Araştırma Görevlisi olarak görev yaptı. 2009 yılında Öğretim Görevlisi olarak atandığı KTÜ Bilgisayar Mühendisliği Bölümünde halen çalışmaya devam etmektedir. Doktora çalışması esnasında, KTÜ BAP destekli 2010.112.009.1 numaralı projede araştırmacı statüsünde görev aldı. Yabancı dil olarak İngilizce bilmektedir. Başlıca yayınları aşağıda verilmiştir.

Ulutas, M., Nabiyev, V. ve **Ulutas, G.**, "Improvements in Geometry Based Secret Image Sharing Approach with Steganography", Mathematical Problems in Engineering, Kasım 2009, doi:10.1155/2009/187874.

Ulutas, M., **Ulutas, G.** ve Nabiyev. V., "Secret Image Sharing with Enhanced Visual Quality and Authentication Mechanism", Imaging Science Journal, 59, 3 (2011) 154-165.

Ulutas, M., **Ulutas, G.** ve Nabiyev, V., "Medical Image Security and EPR hiding using Shamir's secret sharing scheme", Journal of Systems and Software, 84, 3 (2011) 341-353.