KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ÇOK PARÇALI SIR PAYLAŞIM ŞEMALARI VE UYGULAMALARI

YÜKSEK LİSANS TEZİ

Katira SOLEYMAN ZADEH

TEMMUZ 2012
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ÇOK PARÇALI SIR PAYLAŞIM ŞEMALARI VE UYGULAMALARI

Katira SOLEYMAN ZADEH

Karadeniz Teknik Üniversitesi Fen Bilimler Enstitüsüne
"BİLGİSAYAR YÜKSEK MÜHENDİSLİĞİ"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 03.07.2012
Tezin Savunma Tarihi : 24.07.2012

Tez Danışmanı : Prof.Dr. Vasif V.NABİYEV

Trabzon 2012

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalında

Katira SOLEYMAN ZADEH tarafından hazırlanan

ÇOK PARÇALI SIR PAYLAŞIM ŞEMALARI VE UYGULAMALARI

başlıklı bu çalışma, Enstitü Yönetim Kurulunun 03/07/2012 gün ve 1464 sayılı kararıyla oluşturulan jüri tarafından yapılan sınavda

YÜKSEK LİSANS TEZİ

olarak kabul edilmiştir.

Jüri Üyeleri

Başkan : Prof.Dr. Vasif V.NABİYEV …...……

Üye : Doç. Dr. İsmail KAYA …...……

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

Prof. Dr. Sadettin KORKMAZ

Enstitü Müdürü

ÖNSÖZ

"Çok Parçalı Sır Paylaşım Şemaları Ve Uygulamaları" çalışma, Karadeniz Teknik Üniversitesi, Fen Bilimler Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans Tezi olarak hazırlanmıştır.

Çalışmalarımda bilgileri, tecrübeleri, önerileriyle destekleyen danışmanım sayın Prof. Dr. Vasif V. NABİYEV'e sonsuz teşekkürlerimi arz ederim. Ayrıca destek ve yardımlarını esirgemeyen saygıdeğer Yrd. Doç. Dr. Güzin ULUTAŞ, Arş.gör. Selda BAYRAK, Arş.gör. Çiğdem GÜNGÖR'e ve eğitim süresince yardımları geçen tüm arkadaşlarıma teşekkürlerimi sunarım.

Hayatımın her bir adımında destekleriyle her zaman yanımda olan saygıdeğer babam ve sevgili anneme saygılarımı ve teşekkürlerimi arz ederim. Yüksek lisans eğitim aşamasında yanımda olan, görüşleri ve yardımlarıyla desteklediği eşime teşekkür ederim. Beni hayata bağlayan Bil.Müh.Somaye SOLEYMAN ZADEH'ye sonsuz teşekkürlerimi sunarım.

Katira SOLEYMAN ZADEH
Trabzon 2012

TEZ BEYANNAMESİ

Yüksek Lisans Tezi olarak sunduğum "Çok Parçalı Sır Paylaşım Şemaları Ve Uygulamaları" başlıklı bu çalışmayı baştan sona kadar danışmanım Prof. Dr. Vasif V. NABİYEV'ın sorumluluğunda tamamladığım, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuarlarda yaptığımı/yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma suresince bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksini ortaya çıkması durumunda her turlu yasal sonucu kabul ettiğimi beyan ederim. 03/07/2012

Katira SOLEYMAN ZADEH

İÇİNDEKİLER

Sayfa No

Yüksek Lisans Tezi

ÖZET

ÇOK PARÇALI SIR PAYLAŞIM ŞEMALARI VE UYGULAMALARI

Katira SOLEYMAN ZADEH

Karadeniz Teknik Üniversitesi
Fen Bilimler Enstitüsüne
Bilgisayar Mühendisliği Anabilim Dalı
Danışmanı: Prof.Dr. Vasif V.NABİYEV
2012, 70Sayfa, 2 Ek Sayfa

Geleneksel sır paylaşım şemalarında tüm katılımcılar genelde aynı yetkiye sahiptirler, ancak bazı durumlarda katılımcılar yetkilerine göre parçalara bölünebilirler. Bu tez çalışmasında, genelleştirilmiş çok parçalı erişim yapıları ve bunlar için önerilen sır paylaşım şemalarının tasarlanması gerçekleştirilmiştir. Hiyerarşik erişim yapısı için, geometri tabanlı mükemmel ideal sır paylaşım şeması önerilmiştir. Bölütlenmiş erişim yapısında, bölümlerdeki katılımcılar hiyerarşik düzenlenerek yeni bir iç içe bölütlenmiş erişim yapısı ve bu erişim yapısı için mükemmel ideal olan sır paylaşım şeması önerilmiştir. Çok parçalı sır paylaşım şemaları gizli görüntü paylaşımı gibi bazı uygulamalarda kullanılmıştır. Bu çalışmada yeni bir hiyerarşik gizli görüntü paylaşım şeması önerilmiştir. Önerilen şemada pay görüntülerin büyüklüğü gizli görüntünün boyutu kadardır. Tez çalışmasında tanımlanan iç içe bölütlenmiş erişim yapısı için gizli görüntü paylaşım şeması önerilmiştir. Önerilen tüm gizli görüntü paylaşım şemalarda PSNR değeri sonsuz olarak belirlenmiştir.

Anahtar Kelimeler: Sır paylaşım şeması, Hiyerarşik erişim yapısı, İç içe bölütlenmiş erişim yapısı, Gizli görüntü paylaşımı

Master Thesis

SUMMARY

MULTIPARTITE SECRET SHARING SCHEMES AND APPLICATIONS

Katira SOLEYMAN ZADEH

Karadeniz Technical University
The Graduate School of Natural And Applied Sciences
Computer Engineering Graduate Program
Supervisor: Prof.Dr. Vasif V.NABİYEV
2012, 70Pages, 2 Pages Appendix

In the traditional secret sharing schemes, all participants are equal in terms of privileges but in special situations participants may not be equal. In this work we consider generalized access structures and linear secret sharing schemes for their realization. We studied hierarchical access structure to propose new geometry based secret sharing scheme. Nested compartment access structure is considered where a hierarchical is defined within compartment. Also a perfect ideal secret sharing scheme for nested compartment accesses structure is proposed. Proposed schemes are ideal and perfect. Hierarchical and nested compartment image secret sharing schemes is considered. In proposed schemes size of shared images is equal to secret image and PSNR in these schemes is infinite.

KeyWords: Secret sharing scheme, Hierarchical access structure, Nested compartment access structure, Image secret sharing scheme

ŞEKİLLER DİZİN

Sayfa No

TABLOLAR DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

GF	: Galois alanı (Galois field)
PSNR	:Tepe sinyal gürültü oranı (Peak to signal noise ratio)
GSP	: Görsel sır paylaşım şeması
EBOB	: En Büyük Ortak Bölen
ECC	: Error correction code

1.GENEL BİLGİLER

1.1.Giriş

Sayısal bağlantılar, internet aracığıyla elektronik verilerin iletimi, elektronik ticaret gibi global faaliyetler, askeri görüntüler gibi hassas bilgilerin kullanımı ve benzeri konular, hızlı bir şekilde hayatımızın bütün yönlerinde yaygınlaşmaktadır. Bu bilgilerin güvenliğinin sağlanması oldukça kritik ve önemli bir konudur. Verilerin gizliliğini sağlama prosedürleri, kriptografinin esasını teşkil eden kavramlardandır.

Sır paylaşım şeması, sadece bir kişiye güven olmadığı durumlarda kullanılmaktadır. Sır paylaşım şeması önemli bilgileri taşıyan gizli verilerde, birden fazla kişinin bir araya gelmesi durumunda yeniden elde edilmesi istenir. Sır paylaşım şeması, bir bankanın kasasının erişiminin kontrolü, bir nükleer füzenin ateşlenmesinin izninin verilmesi gibi örnek durumlarda uygulanabilmektedir. Örneğin bir nükleer bombanın ateşlenme onayı için, birkaç kişinin bir araya gelmesi durumunda onay verilmesi mümkün olacaktır.

Sır paylaşım şeması ilk olarak 1979 yılında Shamir[1] ve Blakley[2] tarafından önerilmiştir. İlk önerilen sır paylaşım şemalarında, sırrı yeniden elde etmek için önemli olan sadece katılımcıların sayısıdır. Bu şemalara eşik sır paylaşım şeması denilir ve (t, n) ile gösterilir. Shamir ve Blakley'in şemaları birbirinden oldukça farklıdır. Shamir'in şemasının yapısı polinomial interpolasyona ve Blakley'inki ise sonlu geometriye dayanmaktadır. Bunların önerdikleri şemalardan sonra başka şemalar ortaya çıkmıştır. Mignotte[3] ve Asmuth-Bloom[4] sır paylaşım şemalarını Çinli kalan teoremine dayanarak önermişler.

Sır paylaşım şeması iki temel aşamadan oluşur. İlk aşamada, dağıtıcı sırrı paylaştırma algoritmasıyla paylara böler ve bu payların her biri, bir katılımcıya dağıtılır. İkinci aşamada, katılımcılardan oluşan yetkili altkümenin kendi paylarını birleştirmesi ile sır yeniden elde edilir. Katılımcıların yetkili altkümesine, erişim yapısı denilir ve Γile gösterilir. Γ'da olan her bir altküme, sırrı kendi paylarından elde edebilmektedir ve Γ'da olamayan her bir altküme, sırla ilgili hiçbir bilgiyi ortaya çıkaramamaktadır. Eğer Γ'da olamayan yetkisiz altkümeler, sırla ilgili hiçbir bilgiye erişemezlerse, bu durumda sır

paylaşım şemasına mükemmel denir. Bilgi oranı sır paylaşım şemasının verimliliğinin ölçümü olarak tanımlanır ve pay boyutu, sır boyutunun oranı olarak tanımlanır. Eğer sır paylaşım şeması mükemmelse ve bilgi oranı bütün paylar için 1'e eşitse, bu durumda sır paylaşım şeması idealdir.

Ito, Saito, Nishizaki[5] monoton erişim yapısı için, mükemmel sır paylaşım şeması olduğunu ispatlamışlar. Ancak bu metotla elde edilen şemalar aslında ideal değildirler. Burada payların boyutu katılımcıların miktarına göre üstel biçimde büyümektedir. Aslında her tür erişim yapısı için, ideal sır paylaşım şeması bulmak mümkün olamamakta ve bazı durumlarda payların boyutunun sırra göre daha büyük olması gerekmektedir. Benaloh[6] bazı monoton erişim yapıları için ideal sır paylaşım şemasının olmadığını ispatlamıştır.

Sır paylaşım şemasında genel erişim yapısı için pay boyutunun optimize edilmesi çözülememiş problemlerdendir ve pay boyutunun üst ve alt sınırının arasında büyük bir boşluk var olmaktadır. Csirmaz[7]'ın yaptığı çalışmalarına göre bazı durumlarda payların boyutunun sırrın boyutuna göre çok daha büyük olması gerekir. Karnin ve arkadaşları[8]'nın ispatlarına göre, mükemmel eşik sır paylaşım şemalarında, payların boyutunun en az sırrın boyutu kadar olması gerekmektedir. Böylece, her verilen erişim yapısı için verimli ve ideal bir sır paylaşım şemasının bulunmasını beklenemez.

Gerçek hayattaki uygulamaların çoğunda, erişim yapıları, eşik erişim yapısı gibi sade değildir. Bu uygulamalar birçok senaryo için kullanışlıdır. Son yıllarda genelleştirilmiş geleneksel eşik erişim yapıları üzerinde araştırmalar yapılmaktadır. Uygulamalara ilişkin çok parçalı erişim yapıları daha çok ilgi görmüştür[9-14].

Çok parçalı erişim yapılarında, katılımcılar kümesi birkaç parçaya bölünür ve aynı parçada olan tüm katılımcılar aynı rolleri üstlenir. Çok parçalı sır paylaşım şeması, eşik sır paylaşım şemalarının genelleştirilmiş halidir. Katılımcıların tümü, eşik erişim yapılarında aynı seviyededirler oysa çok parçalı erişim yapılarında, katılımcılar farklı sınıflara, örneğin hiyerarşik organizasyonlara dağıtılmışlardır.

Her verilen erişim yapısı için, verimli bir sır paylaşım şemasının inşa edilmesi zordur, bundan dolayı, ideal erişim yapısı birkaç belli yapılar için araştırılmıştır ve bu yapılar için sır paylaşım şemaları önerilmiştir. Sır paylaşım şemasının erişim yapısı, eşik erişim yapısından farklı olarak, ilk Shamir tarafından önerilmiştir. Bu şemaya ağırlıklı eşik sır paylaşım şeması denir. Bu şemada her katılımcıya bir ağırlık verilmektedir ve bu bir pozitif tamsayıdır. Eğer ağırlık toplamı belli bir eşik değerinden büyük olursa, bu küme yetkili kümedir ve gizli veriyi yeniden elde edebilmektedir. Shamir'in tanımladığı yapı

çok basittir: bir eşik şeması alınır ve her katılımcıya ağırlığı miktarında pay verilir, ancak bu şema ideal değildir. Kothari[15] ideal hiyerarşik sır paylaşım şemalarının yapılandırmasını ortaya koymuştur. Simmons[16] tarafından çok seviyeli ve bölütlenmiş erişim yapıları için araştırmalar yapılmıştır. Simmons, Blakley'in geometri tabanlı metodunu genelleştirerek, bu erişim yapıları için, sır paylaşım şeması önermiştir. Çok seviyeli erişim yapıları hiyerarşik organizasyonlar için uygundur, oysaki bölütlenmiş erişim yapıları farklı parçalardan oluşan bölümlerin yapılandırılmasıdır. Simmons'un çok seviyeli ve bölütlenmiş erişim yapıları için, ideal sır paylaşım şemasının olması ihtimali Brickell[17] tarafından ispatlanmıştır. Brickell, ideal sır paylaşım şemasının kurulması için, lineer cebire dayanan yeni bir metot tanımlamıştır. Bu metot, ideal sır paylaşım şemasının, sonraki yapılarında kullanılmıştır.

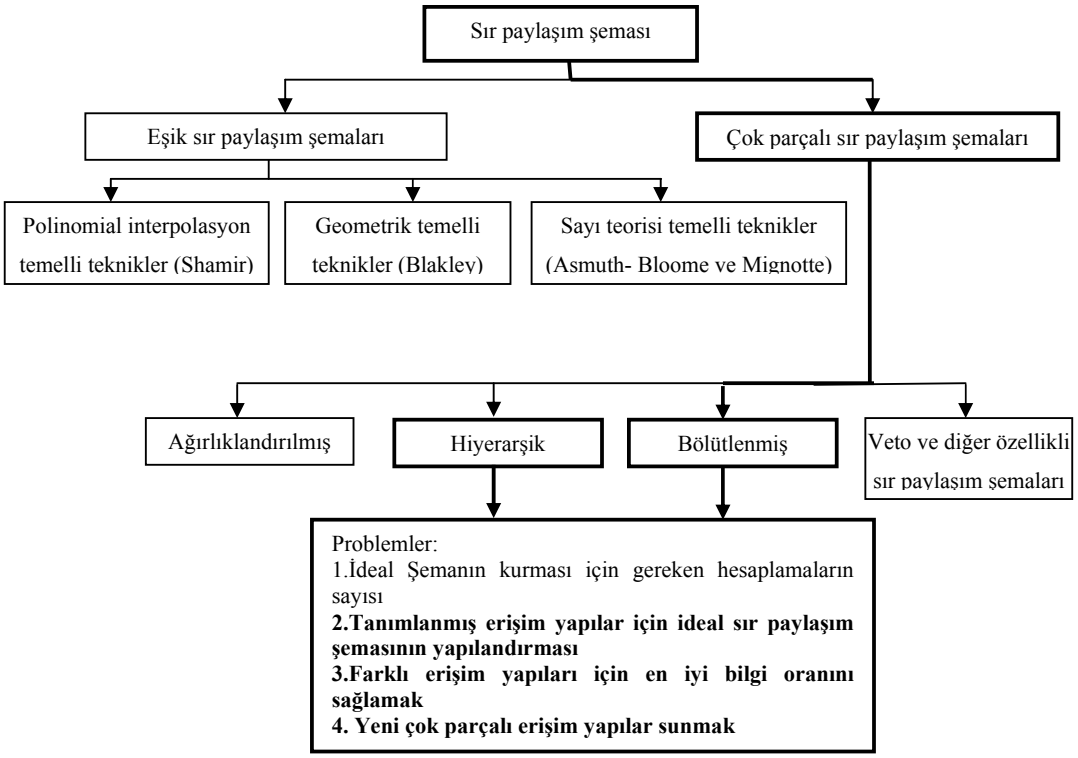
Tassa[18] hiyerarşik erişim yapısı için bir ideal sır paylaşım şeması önermiştir. Tassa'nın önerdiği yapı, Shamir'in eşik şemasının bir başka biçimi gibidir. Önerilen yapıda, payları belirlemek için bir rastgele polinomu kullanılır, fakat bazı payların miktarı polinomun türevinin miktarıdır. Türevin derecesi, katılımcıların hiyerarşik seviyelerine bağlıdır. Bu yüzden, sırrı elde etmek için Lagrange interpolasyonu yerine, Birkhoff interpolasyonu kullanılmaktadır. Belenkiy[19] çok seviyeli sır paylaşım şeması için, Birkhoff interpolasyonunun nasıl kullanıldığını göstermiştir.

m bölüm (veya seviyeden) ve m koşuldan oluşan, çok parçalı erişim yapılarında, Simmons'un tanımladığı ayırıcı hiyerarşik erişim yapısındaki katılımcılar kümesi, belirlenen m koşuldan, herhangi bir koşulu sağlarsa o zaman bu küme yetkili olmaktadır. Ama Tassa'nın önerdiği birleştirici hiyerarşik erişim yapısında, belirlenen m koşulun tümünün karşılanması gerekir.

K.Kaşkaloğlu[20] çalışmasında m bölümlü ve bunlar üzerinde belirli m koşul bulunan çok parçalı katılımcı kümesi için, tüm koşulların birden veya yalnızca herhangi birinin sağlandığı durumlar yerine, herhangi c tanesinin yeterli olma yaklaşımında, hem bölütlenmiş hem de hiyerarşik durumlarda ortaya çıkan genelleştirilmiş ara erişim yapılarını incelemiştir. Önerilen şemalar ideal değildir ancak mükemmellilik özelliğini sağlamıştır. Çalışmasının bir kısmında bölümler içinde başka bölümler olduğunu düşünerek iç içe çok parçalı erişim yapılar üzerinde araştırmalar yapmıştır.

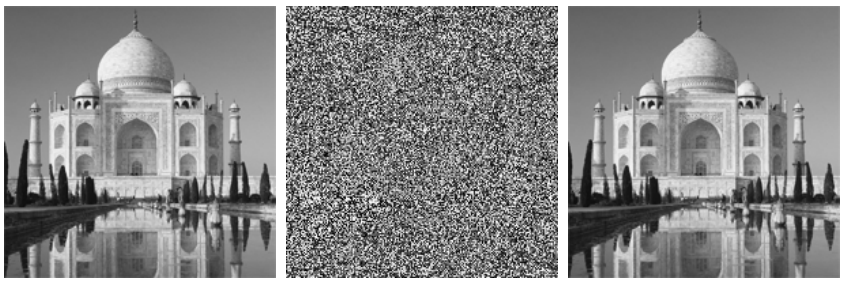
Şekil 1.1'de genel olarak sır paylaşım şemasının sınıflandırılması ve var olan problemleri gösterilmiştir. Tez çalışmada bazı genelleştirilmiş çok parçalı erişim yapıları için araştırmalar yapılmış ve bu erişim yapıları için ideal sır paylaşım şemalar önerilmiştir.

Tez çalışmasında yeni bir iç içe bölütlenmiş erişim yapısı tanımlanmıştır ve bu erişim yapısı için ideal sır paylaşım şeması önerilmiştir. Tanımlanan iç içe erişim yapısında her bölütlenmiş bölümlerin içindeki katılımcıların hiyerarşik düzenlendiği göz önüne alınmıştır. Tassa'nın tanımladığı birleştirici hiyerarşik erişim yapısı için yeni bir ideal sır paylaşım şeması önerilmiştir. Önerilen şemaların mükemmellik özelliği sağlanmıştır ve şemaların bilgi oranı bire eşittir, böylece şemalar idealdir.



Şekil 1.1. Sır paylaşım şemasının sınıflandırılması

Günümüzde, elektronik bilgiler, sayısal videolar, görüntüler, sesler ve metinler internet üzerinden paylaşılır ve iletiliyor. Bunların arasında, gizli veya önemli veriler taşıyan, askeri, ticari ve tıbbi görüntüler olabilmektedir. Bu görüntüleri korumak için, kriptografi sağlam ve güvenilir iletişim için, popüler ve gereken çözüm olmuştur. Kriptografide gizli görüntü bir anahtar değeri ile şifrelenir. Şekil 1.2'de gizli görüntü Pareek ve arkadaşları[21] önerdikleri kaos şifreleme algoritması kullanarak şifrelenmiş. Sekil 1.2(a)'da orijinal görüntü ve şekil 1.2(b)'de şifreli görüntü ve şekil 1.2(c)'de deşifre olunmuş gizli görüntüyü gösteriyor.

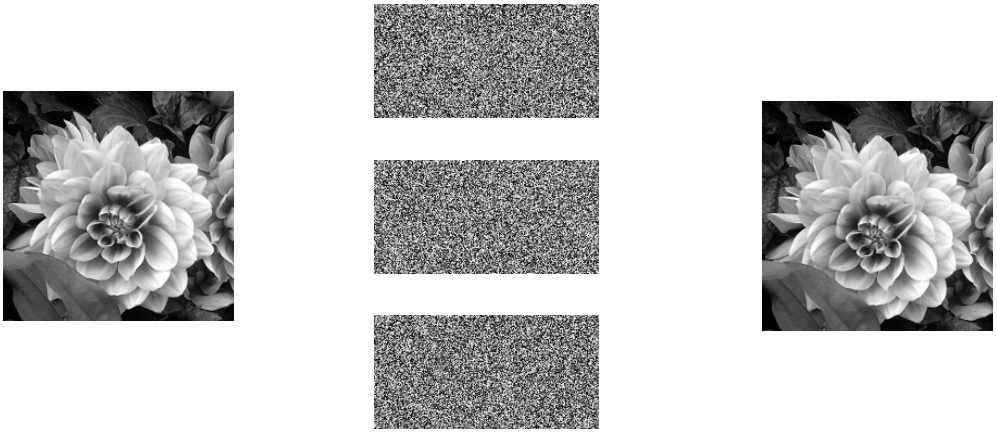


(a) (b) (c)

Şekil 1.2. (a) 210×210 orijinal görüntü (b) şifreli görüntü (c) deşifre olunmuş gizli görüntü

Gizli görüntülerin güvenliğini sağlanması için çalışmalar yapılmıştır. Tez kapsamındaki önerilen şemalar gizli görüntü üzerinde uygulanmıştır. İlk olarak 2002 yılında Thien ve Lin[22] tarafından önerilen, *(t,n)* gizli görüntü paylaşım şemasında, gizli görüntü *n* katılımcı arasında pay görüntülerine bölünür. Gizli görüntünün yeniden yapılandırması için, en az *t* tane katılımcı paylarının bir araya gelmesi gerekmektedir, *t* den az katılımcı olduğu durumunda, gizli görüntü elde edilmemektedir.

Şekil 1.3(a)'da, (2,3) gizli görüntü paylaşım şemasını kullanarak, pay görüntüleri şekil 1.2(b)'de gösterilmiştir ve şekil 1.2(c)'de iki pay görüntüyü kullanarak, gizli görüntü yeniden elde edilmiştir.



(a) (b) (c)

Şekil 1.3. (a) Gizli görüntü (b) (2,3) şemanın üremiş olduğu pay görüntüleri (c) Yeniden yapılandırılan gizli görüntü

Tez kapsamında yapılan çalışmalar aşağıda verilmiştir:

1- Var olan hiyerarşik erişim yapısı için yeni bir ideal geometrik sır paylaşım şeması önerilmiş ve şemanın mükemmel olması ispatlanmış.
2- Yeni bir iç içe bölütlenmiş erişim yapısı tanımlanmıştır. Var olan Shamir eşik şemasına dayanarak yeni bir ideal sır paylaşım şeması önerilmiştir. Şemanın mükemmellik özelliği sağlanmıştır.
3- Önerilen hiyerarşik sır paylaşım şemasını kullanarak, yeni bir gizli görüntü paylaşım şeması önerilmiştir.
4- Önerilen iç içe bölütlenmiş sır paylaşım şeması kullanarak, gizli görüntü üzerinde örneklendirilmiştir.
5- Ayrıca VeriMatrisi'nin güvenliğini sağlamak amacıyla, VeriMatrisler için sır paylaşım şeması uygulanmıştır.

İlerleyen bölümlerde sır paylaşım şemasında bahsedilecek, eşik şemalar ve çok parçalı şemalar detaylıca anlatılacaktır. Ardından erişim yapısının özellikleri bahsedilecek ve çok parçalı erişim yapılar tanımlanacaktır. Sır paylaşım şemasının araştırmalarının birisi olan, gizli görüntü paylaşım şemasın temeli anlatılacak. Ardından VeriMatrisler incelenecektir. Yapılan çalışmalar bölümünde, önerilen erişim yapıları detaylıca incelenmekte ve yeni sır paylaşım şeması açıklanmaktadır. Önerilen şemaların gizli görüntü üzerinde uygulamaları verilmektedir. Ayrıca sır paylaşım şemasının, VeriMatrisler üzerinde uygulamaları yer almaktadır.

1.2. Sır Paylaşım Şemaları

Sır paylaşım şeması, hassas bilgileri *n* katılımcı arasında paylaştırmak için bir metottur. Önceden belirlenen katılımcıların yetkili alt grupları bir araya gelerek, sır miktarı yeniden elde edilir. Örneğin önemli bir verinin erişimi için bir gizli anahtar gereklidir. Bu anahtarın kaybolması durumunda tüm önemli bilgiler erişilmez hale gelir ve eğer anahtar çalınırsa, o zaman gizli veri hırsızlar tarafından ifşa edilir. Bu tür problemleri önlemek için, gizli anahtar parçalara bölünür ve kişiler arasında dağıtılır. Böylece anahtarın bir parçasının kaybolması durumunda önceden belirlenen diğer yetkili kişilerin bir araya gelmesinde, gizli anahtar yeniden elde edilebilir. Gizli anahtarın bir parçasının çalınması durumunda ise parçaların gizli anahtarla ilgili, herhangi bilgi içermediğine göre gizli anahtar yeniden elde edilememektedir. Ödeme sistemi için gereken ana anahtar, kritik bir

faaliyet için gereken aktifleştirme kodu veya bir füzeyi ateşlemesi için gereken anahtar, bir banka kasasını açması gibi durumlar da sır paylaşım şemasına örnek olarak gösterilebilir.

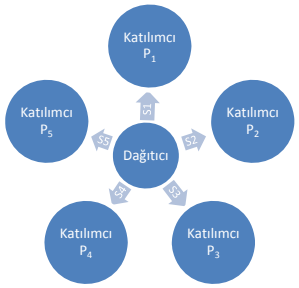
Sır paylaşım şemasında gizli veri *S*, paylaştırma algoritmasını kullanarak paylara bölündükten sonra, dağıtıcı tarafından katılımcılar arasında dağıtılır. Üretilen pay değerleri gizli veriyle ilgili herhangi bilgiyi içermemektedir. Önceden belirlenen yetkili katılımcılar, pay değerlerini bir araya getirerek gizli veri yeniden elde edilmektedir. Sır paylaşım şeması aşağıda verilen üç aşamadan oluşur:

1- Payların İnşa Etmesi

Bu aşamada gizli veri *S*,bir güvenilir kişi (dağıtıcı olarak adlandırılır) tarafından paylara, $s_1, \dots, s_n$ bolunur.

2- Payların Dağıtılması

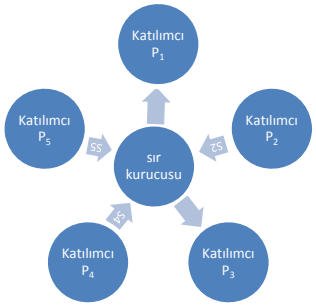
İlk aşamadaki üretilen paylar, *n* katılımcı arasında dağıtılır, şekil 1.4.



Şekil 1.4. Payların katılımcılar arasında dağıtılması

3- Sırrın yeniden elde edilmesi

Sırrı yeniden elde etme aşamasında, katılımcıların yetkili kümesi kendi paylarını birleştirerek, sır yeniden elde edilir, şekil1.5.



Şekil 1.5. Sırrın yeniden elde edilmesi

Sır paylaşım şemasının paylarının boyutuna göre genişleme faktörü ve bilgi oranı iki önemli parametre hesaplanmaktadır[23]. Denklem (1.1)'de verilen genişleme faktörü, tüm payların boyutunun katılımcı sayısına bölünmesine eşittir.

$$Ef = \frac{\sum_{i=1}^{|P|} |S_i|}{|P|} \tag{1.1}$$

$|S_i|$ i. payın bit boyutu, |P| katılımcı sayısıdır.

Diğer önemli parametre katılımcılara dağıtılacak olan pay değerlerinin büyüklüğüdür. Katılımcılara gönderilecek olan pay büyüklüklerinin gizli verinin büyüklüğüne oranı olarak hesaplanan parametre, bilgi oranı ρ_j denklem (1.2)'de gösterilmiştir.

$$\rho_j = \frac{|S|}{|S_j|} \tag{1.2}$$

ρ_j j. katılımcının bilgi oranıdır, |S| sırrın bit boyutu ve $|S_j|$ j. payının bit boyutudur.

Sır paylaşım şemasının bilgi oranı, katılımcıların bilgi oranlarının ortalaması alınarak (1.3)'deki denklemi kullanarak hesaplanır.

$$\rho = \frac{|S|}{Ef} = \frac{|P| \times |S|}{\sum_{i=1}^{|P|} |S_i|} \tag{1.3}$$

Bilgi oranı 1'e eşit olursa sır paylaşım şeması ideal denilir[17].

1.2.1. Erişim Yapısı

Sır paylaşım şemasının erişim yapısı, gizli veriyi yeniden elde etmek için tüm yetkili grupların kümesidir ve Γ ile gosterilir[5]. Yetkili kümelere sırrı yeniden elde etme yeteneğine sahipler.

$\mathcal{U} = \{u_1, u_2, \dots, u_n\}$, n katılımcının kümesi olsun. Gizli veri katılımcılar arasında dağıtılmıştır.

- Eğer $\mathcal{U}' \subset \mathcal{U}$ olursa ve gizli veriyi yeniden elde etme yeteneğine sahip ise o zaman bu kümeye yetkili küme denir böylece ulaşabilme özelliği sağlanmıştır.
- Eğer$\mathcal{U}' \subset \mathcal{U}$ olursa ve gizli veriyi yeniden elde etme yeteneğine sahip değilse o zaman bu kümeye yetkisiz küme denir böylece mükemmellilik özelliği sağlanmıştır.

Tanım 1.1: $\Gamma \subseteq 2^{\mathcal{U}}$ erişim yapısı olarak tanımlanır. Eğer katılımcı kümesinin altkümesi, $A \in \Gamma$ ise o halde A yetkili altkümedir ve gizli veriyi hesaplayabilmektedir.

Tanım 1.2:*A* ve *B* katılımcı kümesinin iki altkümesi olsun. Eğer $A \in \Gamma$ ise ve $A \subseteq B$ olursa, o halde $B \in \Gamma$'dir, böylece erişim yapısı monotondur.

Monoton erişim yapısında minimum boyutta olan yetkili kümelerin eşitsiz tek topluma sahip olmasıdır. Yani eğer $A \in \Gamma$, Γ'nın minimum kümesi ve $A' \in \Gamma$, $A' \subseteq A$ olursa , o zaman $A' = A$dır.

İlerleyen bölümlerde literatürde önerilen eşik ve çok parçalı erişim yapılar için önerilen sır paylaşım şemalar hakkında bilgiler verilecektir.

1.2.2. *(t,n)* Eşik Sır Paylaşım Şemaları

Bir *(t,n)*eşik şeması, bir gizli paylaşım şemasıdır ki, *S* sırrı *n* katılımcı arasında dağıtılır. Bu şemalarda sırrı yeniden elde etmek için en az *t* katılımcının bir araya gelmesi gereklidir ve herhangi *t-1* veya daha az katılımcı sırrı yeniden elde edemezler. Eşik erişim yapısı $\Gamma = \{A \subseteq \mathcal{U} \mid |A| \geq t\}$ dir ve buna (t,$|\mathcal{U}|$) eşik erişim yapısı denir. Eşik sır paylaşım şeması ilk olarak Shamir ve Blakley tarafından 1979'da önerilmiştir. Shamir'in şeması polinomialinterpolasyona dayalıdır ve Blakley'in ki ise geometriye dayanmaktadır. Bu çalışmaların ardından, 1983 yılında, Asmuth-Bloom ve Mignotte tarafından önerilmiş olan eşik sır paylaşım şemaları için ise Çinli kalan teoremi kullanılmıştır.

1.2.2.1. Shamir Sır Paylaşım Şeması

1979 yılında Shamir[1] tarafından tanımlanan temel eşik sır paylaşım şeması, Lagrange'ın polinomial interpolasyonuna dayanmaktadır. Shamir'in*(t,n)* eşik yönteminin tek değişkenli polinomu $(t-1)$ derecedendir. Polinom denklemi (1.4)'de verilmektedir.

$$p(x) = \sum_{i=0}^{t-1} a_i x^i \pmod{q} \tag{1.4}$$

Burada gizli veri $a_0 = S$dır ve $a_1, \dots, a_{t-1}$ ler rastgele seçilen tamsayılardır. Gizli veriyi, n katılımcı arasında paylaştırmak için, n tane farklı $x_1, \dots, x_n$ rasgele tamsayılar belirlenir ve j. katılımcıya verilen pay değeri denklem (1.5)'deki gibi elde edilmektedir.

$$p_j(x_j) = \sum_{i=0}^{t-1} a_i x_j^i \pmod{q} \tag{1.5}$$

$a_1, \dots, a_{t-1}$rastgele seçilen parametreler ve gizli veri, $[0, q)$ aralığında olmalıdır. Yeniden yapılandırma aşamasında tek bir çözüm elde edilmesi için q değerinin asal olması gerekmektedir. Polinomun tanımlanmasında kullanılan asal değer, gizli verinin tanımlı olduğu aralığı kapsayacak en büyük asal sayı değeridir. Örneğin, gri seviyesinde olan bir gizli görüntünün piksel değerleri $[0,255]$aralığındadır ve bu aralıkta olan en büyük asal değer 251 seçilmelidir.

Yeniden yapılandırma aşamasında en az t tane pay değeri bir araya gelerek, gizli veri S, Lagrange interpolasyonu hesaplayarak elde edilmektedir. Lagrange[24]denklemi (1.6)'da verilmiştir.

$$p(x) = \sum_{i=1}^{t} \left(p_i(x_i) \prod_{1 \le j \le t, i \ne j} \frac{x - x_j}{x_i - x_j} \right) (\mathrm{mod}\, q) \tag{1.6}$$

Sadece gizli veriyi hesaplanması için (1.6)'da verilen denklemi sadeleştirilerek, (1.7)'deki verilen denklem kullanılmaktadır.

$$c_i = \prod_{1\le j\le t, i\ne j} \frac{x_j}{x_j - x_i} \quad S = a_0 = \sum_{i=1}^{t} c_i\, p(x_i) (\mathrm{mod}\, q) \tag{1.7}$$

Örnek 1.1:$S = 23$ gizli veri olacak şekilde (3,4) eşik sır paylaşım şeması GF(29) üzerinden farz edelim. Eğer $a_1 = 12$, $a_2 = 7$ olursa, aşağıdaki ikinci dereceden polinom tanımlanır:

$f(x) = 23 + 12x + 7x^2$

Pay değerleri dört katılımcı için

$f(2) = v_1 = 17$, $f(3) = v_2 = 6$, $f(1) = v_3 = 13$, $f(5) = v_4 = 26$

olarak hesaplanır. Sırrı yeniden elde etmek için her bir dört katılımcıdan üç katılımcının bir araya gelmesi gerekir. Örnek olarak,s_1, s_2, s_4 pay değerlerinden, S sırrı aşağıda verilen şekilde elde edilebilir:

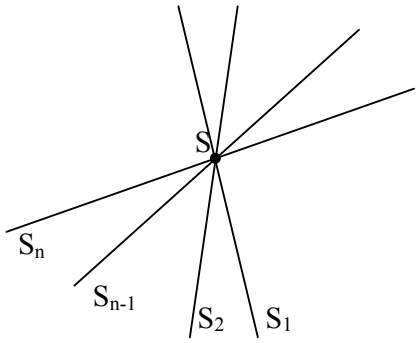
$$S = 17\frac{3}{3-2}\frac{5}{5-2} + 6\frac{2}{2-3}\frac{5}{5-3} + 26\frac{2}{2-5}\frac{3}{3-5} = 85 - 30 + 26 = 81\ mod\ 29$$
$$= 23$$

1.2.2.2. Blakley Sır Paylaşım Şeması

Blakley[2] polinomial interpolasyon yerine, t boyutlu uzaydaki hiper düzlemlere dayanan geometriyi kullanmaktadır. (t, n)eşik şemasını uygulamak için, n katılımcının her birine, GF(q) sonlu alan üzerinde *t* boyutlu uzayda bir hiper düzlem denklemi verilir. Hiper düzlemler $a_1x_1 + \cdots + a_tx_t = b$ şeklinde olan denklemin tanımlanmaktadır. $x = (x_1, \ldots, x_t)$değerleri pay değerlerini tanımlamada kullanılır. Her bir hiper düzlem belli bir noktadan geçmektedir. Hiper düzlemlerin kesişme noktaları, sır olarak tanımlanmaktadır. t katılımcının bir araya gelmesiyle, sırrı yeniden elde etmek için denklem sistemi çözülmesi gerekmektedir.

Şekil 1.6.'da Blakley sır paylaşım şemasının bir örneğinin gerçekleştirilmesi gösterilmiştir. Burada $t = 2$'dir, yani her hiper düzlem denklemi bir doğru denklemiyle

ifade edilir. *n* sayıda katılımcı için, dağıtıcı tarafından gizli verinin temsil ettiği noktayı kesen *n* adet doğru denklemi üretilir. Herhangi *t* sayıda katılımcının doğrusunun kesiştirilmesi sonucu gizli veri yeniden elde edilmektedir.



Şekil 1.6. Blakley sır paylaşım şeması,$t = 2$

Örnek 1.2:Blakley'in yöntemine göre, gizli veri üç boyutlu uzayda bir noktanın koordinatlarıyla (2,4,9) olarak verilsin. (3,4) şeması için $2x_1 + 4x_2 + 9x_3 = b$ denklemi GF(11) alan üzerinde üretilir. Her bir katılımcıya gönderilecek olan 4 farklı değerler kümesi (x_1, x_2, x_3, b) pay değerlerini oluşturur. Pay değerleri aşağıda ki şekilde hesaplanarak elde edilir.

$$\left(\begin{bmatrix} 2 & 3 & 1 \\ 3 & 2 & 6 \\ 4 & 2 & 1 \\ 5 & 1 & 10 \end{bmatrix} \times \begin{bmatrix} 2 \\ 4 \\ 9 \end{bmatrix}\right)\%11 = \begin{bmatrix} 3 \\ 2 \\ 3 \\ 5 \end{bmatrix}$$

Pay değerleri sırasıyla (2,3,1,3), (3,2,6,2), (4,2,1,3), (5,1,10,5) olacaktır. Bu katılımcılardan herhangi üç katılımcı bir araya gelerek, düzlemlerinin kesişme noktası olan (2,4,9) yeniden elde edilir. Gizli veri aşağıda ki sistemi çözerek yeniden elde edilir.

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \left(\begin{bmatrix} 2 & 3 & 1 \\ 4 & 2 & 1 \\ 5 & 1 & 10 \end{bmatrix}^{-1} \times \begin{bmatrix} 3 \\ 3 \\ 5 \end{bmatrix}\right)\%11 = \begin{bmatrix} 2 \\ 4 \\ 9 \end{bmatrix}$$

1.2.2.3. Çinli Kalan Teoremine Dayalı Sır Paylaşım Şemaları

Çinli kalan teoremine göre (1.8)'deki denklem sistemi verilsin:

$$\begin{aligned} x &\equiv a_1 \bmod p_1 \\ x &\equiv a_2 \bmod p_2 \\ &\vdots \\ x &\equiv a_n \bmod p_n \end{aligned} \tag{1.8}$$

Taban değerleri $p_1, p_2, \dots, p_n$ arasında asal olsun yani $\text{ebob}(p_i, p_j) = 1, i \neq j$

$P = \prod_{i=1}^{n} p_i$

Tüm $i \in \mathbb{N}$ $(1 \leq i \leq n)$ için y_i bir tamsayı olsun ki

$y_i \cdot \frac{P}{p_i} \equiv 1 \; mod \; p_i$

Burada oluşacak tek çözüm $x_0 = \sum_{i=1}^{n} a_i y_i \frac{P}{p_i}$ ve$x \equiv x_0 \; (mod \; P)$Şeklinde elde edilebilir.

Örnek 1.3. Örneğin aşağıdaki sistemi ele alırsak,

$$\begin{aligned} x &\equiv 4 \; mod \; 5 \\ x &\equiv 5 \; mod \; 7 \\ x &\equiv 8 \; mod \; 11 \end{aligned}$$

$P = 5 \times 7 \times 11 = 385$, $n_1 = \frac{P}{p_1} = 77$, $n_2 = 55$, $n_3 = 35$

y_i ler aşağıdaki gibi bulunur:

$77 \; y_1 \equiv 1 \; (mod \; 5) 55 \; y_2 \equiv 1 \; (mod \; 7) 35 \; y_3 \equiv 1 \; (mod 11)$

$$y_1 = 3 \, , \qquad y_2 = 6 \, , \qquad y_3 = 6$$

$$x = (3 \times 4 \times 77 + 5 \times 6 \times 55 + 6 \times 8 \times 35)\ mod\ 385 = 19\ (mod\ 385)$$

x değeri 19 olarak hesaplanır.

1.2.3.3.1.Mignotte'nin Şeması

Mignotte'nin eşik sır paylaşım şeması, Mignotte'nin sırası olarak adlandırılan sıralı tamsayıları kullanmıştır. (t, n)eşik şeması için Mignotte'nin sırası, aralarında asal olan tamsayılar $m_1 < m_2 < \cdots < m_n$ sırasıdır ve (1.9)'daki koşulu sağlayacak şekilde belirlenir.

$$\prod_{i=0}^{t-2} m_{n-i} < \prod_{i=1}^{t} m_i \qquad (1.9)$$

(1.9)'da verilen denkleme (1.10)'da verilen denkleme eşittir.

$$max_{1 \le i_1 \le \cdots \le i_{t-1} \le n}(m_{i_1} m_{i_2} \ldots m_{i_{t-1}}) < min_{1 \le i_1 \le \cdots \le i_t \le n}(m_{i_1} m_{i_2} \ldots m_{i_t}) \qquad (1.10)$$

(t, n) Mignotte'nin sır paylaşım şeması aşağıdaki adımları halinde verilmektedir:

- Gizli veri *S*, $\beta < S < \alpha$ koşulu sağlanacak şekilde rastgele tamsayı olarak seçilir. $\alpha = \prod_{i=1}^{t} m_ive\beta = \prod_{i=0}^{t-2} m_{n-i}$ dir.
- Pay değeri $s_i = S\ mod\ m_i$, $1 \le i \le n$ denklik ifadesi yardımıyla belirlenir.
- Herhangi t adet pay değeri $s_{i_1}, \ldots, s_{i_t}$ ele alınır, Çinli Kalan Teoremi kullanılarak, (1.11)'daki denklik sisteminin tek çözümü olarak yeniden gizli veri *S*, elde edilir.

$$\begin{aligned} x &\equiv s_{i_1} \bmod m_{i_1} \\ &\vdots \\ x &\equiv s_{i_t} \bmod m_{i_t} \end{aligned} \qquad (1.11)$$

Yeniden yapılandırma aşamasında ,sadece t-1 pay değerinden $s_{i_1}, \ldots, s_{i_{t-1}}$, elde edilen denklik ifadesi $S \equiv x_0 \; mod \; m_{i_1} \ldots m_{i_{t-1}}$şeklinde olur. $x_0$değerimod$m_{i_1} \ldots m_{i_{t-1}}$tabanındaki tek çözümdür.

Örnek 1.4: Mignotte'nin (3,5) eşik şeması kullanarak, $S = 135$ gizli veriyi katılımcılar arasında paylaştırılır. Her katılımcıya karşılıklı olan, Mignotte'nin koşullunu sağlayarak, modül değerleri sırasıyla 7,11,13,17,19 olsun. Katılımcılara gönderilecek olan pay değerleri

$$\begin{cases} s_1 = 135 \bmod 7 = 2 \\ s_2 = 135 \bmod 11 = 3 \\ s_3 = 135 \bmod 13 = 5 \\ s_4 = 135 \bmod 17 = 16 \\ s_5 = 135 \bmod 19 = 2 \end{cases}$$

olarak hesaplanır. Yeniden yapılandırma aşamasında, en az üç katılımcının bir araya gelmesi gerekir. $s_2 = 3, s_3 = 5, s_4 = 16$pay değerleri seçilir. Çinli kalan teoremi kullanarak, aşağıda verilen denklik sisteminin çözülmesi sonucu gizli veri yeniden elde edilir.

$$\begin{cases} S \equiv 3 \bmod 11 \\ S \equiv 5 \bmod 13 \\ S \equiv 16 \bmod 17 \end{cases}$$

$$S = (221 \times 3 \times 1 + 187 \times 5 \times 8 + 143 \times 16 \times 5) \bmod 2431 = 19583 \bmod 2431 = 135$$

1.2.2.3.2. Asmuth-Bloom'un Şeması

Asmuth-Bloomeşik sır paylaşım şeması, Mignotte sır paylaşım şemasına benzer niteliktedir ve bu yöntemde de, özel sıralı tamsayılar (aralarında asal olan $m_0 < m_1 < \cdots < m_n$) kullanılmaktadır. Sıra tamsayılar (1.12)'deki koşulu sağlayacak şekilde seçilmektedir.

$$m_0 \cdot \prod_{i=0}^{t-2} m_{n-i} < \prod_{i=1}^{t} m_i \qquad (1.12)$$

Genelde m_0, sır olarak saklanır ve $m_1, \dots, m_n$ aleni olarak belli olur. Asmuth-Bloom sır paylaşım şeması aşağıdaki adımları halinde verilmektedir:

- Gizli veri S , $\mathbb{Z}_{m_0}$ kümesinin bir elemanı olarak seçilir.
- y , $y = S + A.m_0$denkleminden hesaplanır. Burada A bir rastgele sayıdır ve $y \in \mathbb{Z}_{m_{1\dots m_t}}$'dir.
- Pay değerleri olan s_i'ler , $s_i = y \, mod \, m_i$, $1 \le i \le n$ denkleminden hesaplanır.
- Herhangi t tane pay değeri $s_{i_1}, \dots, s_{i_t}$ele alınarak, gizli veri S, $S = x_0 \, mod \, m_0$ denklemi sayesinde elde edilir. x_0 verisi farklı standart Çinli kalan teoremi kullanılarak, (1.13)'deki denklik sisteminden, $m_{i_1} \dots m_{i_t}$modülünün tek çözümü olarak hesaplanır.

$$\begin{aligned} x &\equiv d_{i_1} \bmod m_{i_1} \\ &\vdots \\ x &\equiv d_{i_t} \bmod m_{i_t} \end{aligned} \qquad (1.13)$$

1.2.3. Çok Parçalı Erişim Yapıları

(t, n)eşik sır paylaşım şemasında tüm katılımcılar aynı yetkiye sahiptirler. Ama gerçek hayatta katılımcılar her zaman aynı seviyede olamayıp ve bazı katılımcılar diğerlerinden daha güçlüdürler. Örneğin çok parçalı erişim yapıları, ağırlıklandırılmış, hiyerarşik, bölütlenmiş, üç parçalı gibi şemalara sınıflandırılmıştır. İlerleyen bölümlerde çok parçalı erişim yapılar hakkında bilgiler verilecektir.

1.2.3.1.Ağırlıklandırılmış Eşik Sır Paylaşım Şeması

Ağırlıklandırılmış eşik şeması ilk olarak Shamir tarafından önerilmiştir. Bu şemalarda katılımcılar aynı seviyede değiller. Ağırlıklandırılmış eşik şemalarında her bir katılımcıya pozitif bir ağırlık verilir. Gizli verinin yeniden yapılandırılması için bir araya gelen katılımcıların ağırlıklarının toplamı belli bir eşik değerini geçmelidir. Örnek olarak,

bir şirketteki gizli veri pay sahipleri arasında bölünür; fakat her bir pay sahibi şirketteki konumlarına göre farklı miktarlarda pay alır. Ağırlıklandırılmış eşik erişim yapısı aşağıdaki ifadeyle tanımlanmaktadır:

Tanım 1.3: $n \geq 2$ katılımcı olsun ve her katılımcının ağırlık miktarı, $\omega = (\omega_1, \dots, \omega_n)$ sıralı pozitif tamsayılar şeklinde olsun. Eşik miktarı w, $2 \leq w \leq \sum_{i=1}^{n} \omega_i$ eşitsizliğini sağlayacak şekilde bir pozitif tamsayı olsun. (ω, w, n) ağırlıklandırılmış eşik erişim yapısı (1.14)'de verilmiştir:

$$\Gamma = \left\{ A \in \mathcal{P}\left(\{1,2,\dots,n\}\right) \mid \sum_{i \in A} \omega_i \geq w \right\} \tag{1.14}$$

Eğer katılımcıların ağırlıkları 1'e eşit olursa $\omega_1 = \cdots = \omega_n = 1$ ve eşik değeri $w = t$ olursa geleneksel (t, n) eşik sır paylaşım şeması olur.

1.2.3.2 Hiyerarşik Sır Paylaşım Şeması

Hiyerarşik sır paylaşım şemasında, katılımcılar kümesi yetkilerine göre hiyerarşik olarak $L_0, L_2, \dots, L_m$ seviyeleri arasında bölünür. L_0en yüksek seviye ve L_m en alçak seviyeyi gösterir.t_j, $0 \leq i \leq m$, her seviyenin eşik değerini gösterir. Bu eşik değerlermonoton artan tamsayıların sırası, $t_0 < t_1 < t_2 < \cdots < t_m$, şeklinde düşünülebilir. Simmons ve Brickell birbirinden bağımsız olarak ayırıcı hiyerarşik eşik erişim yapısını önermişler:

Tanım 1.4: $U = \cup_{i=0}^{m} U_i$, $U_i \cap U_j = \phi$, $0 \leq i < j \leq m$, m seviyeye bolunmuş olan, n katılımcının kümesi olsun. $t = \{t_i\}_{i=0}^{m}$ monoton artan tamsayıların sırası olsun. Ayırıcı hiyerarşik eşik erişim yapısı (1.15)'de verilen ifadeyle tanımlanmıştır:

$$\Gamma = \left\{ A \subset U : \left| A \cap \left(\bigcup_{j=0}^{i} U_i \right) \right| \geq t_i, \exists i \in \{0,1,\dots,m\} \right\} \tag{1.15}$$

(1.15)'de tanımlanan hiyerarşik erişim yapısı için, Simmons'un tarafından önerilen sır paylaşım şeması, Blakley'nin önerdiği geometri yapısına dayanmaktadır. Ancak bu şema ideal değildir. Brickell aynı problem için iki şema önermiştir. Ghodosi ve

arkadaşları[25] bir başka ideal şema önermiştir. Bu şema Shamir'in eşik sır paylaşım şemasının genişletilmesi esasına dayanmaktadır.

Ayrıcı *(t,n)* hiyerarşik eşik erişim yapısının tanımlanmasına göre düşük seviyeye ait olan katılımcılar, yüksek seviyede ki olan katılımcıların yerine geçebilirler. Böylece paylaştırılan gizli değeri, herhangi ilgili büyük gruplardan oluşan düşük seviyedeki katılımcıların pay miktarından yeniden elde edilebilir. T.Tassa'nın ayrıcı hiyerarşik erişim yapısına kısıtlayıcı şartlar eklemiştir. Tanımlan yeni yapı birleştirici hiyerarşik erişim yapısı olarak adlandırılmıştır.

Bu yapıda düşük seviyeye ait olan katılımcılar yüksek seviyede olan katılımcıların yerine geçemezler ve gizli veriyi yeniden elde etmek için yüksek seviyeden katılan katılımcıların sayısı en az o seviyenin eşik miktarı kadar olması gerekir. Birleştirici hiyerarşik erişim yapısı tanım 1.5'de verilmektedir.

Tanım 1.5: $U = \cup_{i=0}^{m} U_i$, $U_i \cap U_j = \phi$, $0 \le i < j \le m$, m seviyeye bölünmüş olan, n katılımcının kümesi olsun. $t = \{t_i\}_{i=0}^{m}$, $0 < t_1 < \cdots < t_m$, monoton artan tamsayıların sırası olsun. Birleştirici hiyerarşik erişim yapısı (1.16)'da verilen ifadeyle tanımlanmıştır:

$$\Gamma = \left\{ A \subset U : \left| A \cap \left(\bigcup_{j=0}^{i} U_i \right) \right| \ge t_i, \forall i \in \{0,1,\ldots,m\} \right\} \tag{1.16}$$

Tassa'nın sır paylaşım şeması ise Brikhoff interpolasyonuna dayanmaktadır. Tassa'nın önerdiği yeni şema düşük seviyelerdeki katılımcılara daha küçük paylar üretmek için polinomların türevini almaktır. Tassa'nın önerdiği yapısında Shamir interpolasyon yapısı gibi bir P(x) polinomu tanımlanır ve gizli veri bu polinomun katsayısı olarak belirlenir. i seviyesinde olan katılımcılara, $P^i(x)$ polinomuna eşit olan pay değeri veriliyor. Daha önemli olan katılımcılara $P(x)$ polinomunun düşük türevi verilir, çünkü daha duşuk türev, daha yukarı türevlere göre daha çok bilgi taşımaktadır. Yetkili katılımcılar kümesi bir araya gelerek, Brikhoffinterpolasyonunu çözerek, sırrı yeniden elde edebilirler.

1.2.3.3. Bölütlenmiş Sır Paylaşım Şeması

Bölütlenmiş sır paylaşım şemasında, katılımcılar kümesi kendi ile ilişkin m bölümlere ayrılır. Her bir bölüm için bir eşik değeri, $t_i \in \mathbb{N}, 1 \leq i \leq m$ ve bir genel eşik değeri t vardır. Her bir bölümden katılan katılımcıların sayısı o bölümün eşik değerine eşit ya da daha büyükse ve toplam katılımcı sayısının genel eşik miktarına eşit ya da daha büyük olursa gizli veri yeniden elde edilebilmektedir. Bölütlenmiş sır paylaşım şeması ilk Simmons[16] tarafından tartışılmış ve ideal sır paylaşım şeması, Brickell tarafından önerilmiştir. Brickell'in[17] yapısına göre, gizli veri, m parçaya ayrılır ve kısmi sır değeri her bölümün katılımcıları arasında paylaştırılır. Yeniden yapılandırma esnasında gizli veri m bölümden elde edilen kısmi sır miktarlarının birleştirilmesiyle elde edilir. Brickell'in erişim yapısı (1.6)'da verilen ifadeyle tanımlanmaktadır.

Tanım 1.6 : $\mathcal{C} = \{C_1, C_2, \dots, C_m\}$, n katılımcının ($U = \{1,2, \dots, n\}$) bölümleridir. $C_i \cap C_j = \emptyset, 1 \leq i < j \leq m$. $t_i \in \mathbb{N}, 1 \leq i \leq m$, C_i bölümünün eşik miktarı ve $t \in \mathbb{N}$ genel eşik miktarıdır ve $t \geq \sum_{j=1}^{m} t_j$ dir.Bölütlenmiş erişim yapısı (1.17)'de verilen ifadeyle gösterilmektedir.

$$\Gamma = \{\mathcal{V} \subseteq \mathcal{U} : \exists \mathcal{W} \subseteq \mathcal{V} \text{ oyle ki } |\mathcal{W} \cap \mathcal{C}_i| \geq t_i, 1 \leq i \leq m \text{ ve } |\mathcal{W}| = t\} \quad (1.17)$$

Tassa ve Dyn[14] tanım 1.6'daki erişim yapısında bazı değişiklikler yaparak, yeni bir bölütlenmiş erişim yapısı önermiştir. Tassa'nın önerdiği erişim yapısına göre yetkili altkümenin boyutu en az eşik değerinin miktarı kadar olmalıdır, fakat her bölümden katılan katılımcı sayısına bir sınır getirmiştir. Tassa'nın sunduğu erişim yapısı aşağıda verilen ifadeyle tanımlamaktadır:

$$\Gamma = \{\mathcal{V} \subseteq \mathcal{U} : \exists \mathcal{W} \subseteq \mathcal{V} \text{ oyle ki } |\mathcal{W} \cap \mathcal{C}_i| \leq s_i \ , 1 \leq i \leq m \text{ ve } |\mathcal{W}| = s\} \quad (1.18)$$

Burada $s_i, s \in \mathbb{N}$ ve $s \leq \sum_{i=1}^{m} s_i$ olmaktadır. Tassa önerdiği erişim yapısına üst sınır bölütlenmiş erişim yapısı ve Simmon'un önerdiği erişim yapısına ise alt sınır bölütlenmiş erişim yapısı adını vermiştir.

Tassa ve Dyn tanımladıkları erişim yapısı için bir sır paylaşım şeması önermişler, bu şema iki değişkenli interpolasyona dayanmaktadır.

1.2.4. Veto Özellikli Sır Paylaşım Şeması

Geleneksel (t, n) eşik sır paylaşım şemalarında, katılımcılardan t kadar kişi, onay vermeye karar verirlerse, sır yeniden elde edilir[26]. Ancak bazı uygulamalarda yetkili katılımcıların bir kısmına onay vermeme yetkisi verilir. Böylece *t* katılımcının sırrı elde etmesi bu grubun onay verme kararına bağlıdır. Onay verme yetkisinin olması veto olarak tanımlanır.

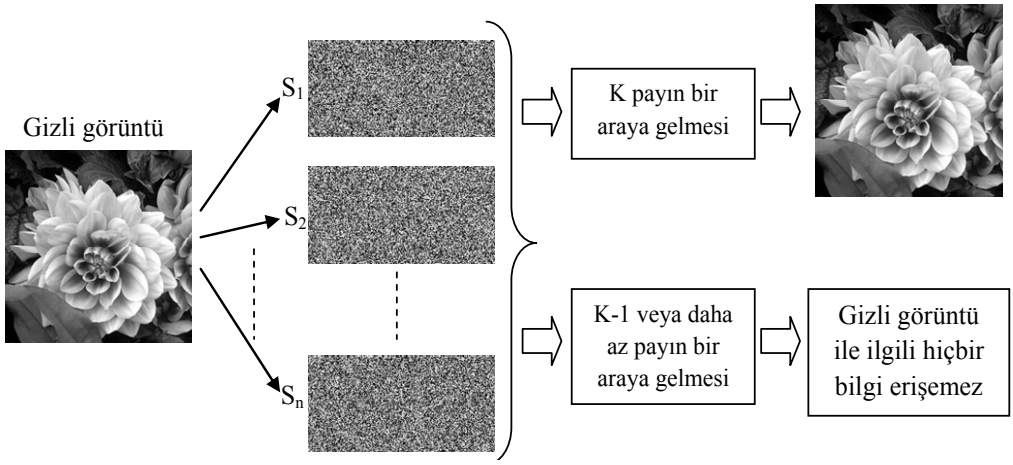
1.3. Gizli Görüntü Paylaşım Şeması

İnternet insanların dünyanın her bir tarafından birbirleriyle iletişim kurmasına olanak sağlayan bir açık erişim evrensel ağdır. İnternet üzerinden iletilen bilgiler gizli tıbbi görüntüler, askeri belgeler, Data Matris barkodlar gibi gizli görüntüler olabilir. Bu tür görüntülerin gizliliğinin sağlanması, araştırmacılar tarafından önemli bir konu haline gelmiştir. Gizli görüntünün güvenliğinin sağlanması için görsel sır paylaşım şeması(GSP) ve gizli görüntü paylaşım şeması gibi yöntemler önerilmiştir. Gizli görüntü paylaşım şeması, tek bir kişiye güven yerin, gruba güven prensibine dayanmaktadır.

Naor ve Shamir[27] tarafından önerilmiş olan görsel sır paylaşım şemasında sır gizli bir görüntüdür. Bu şemada gizli görüntü, gölge adı verilen birkaç gurultulu görünüme sahip n parçaya ayrılır. (t,n) görsel sır paylaşım şemasında gizli görüntü dağıtıcı tarafından görsel şifreleme algoritması kullanılarak *n* tane gurultulu pay oluşturulur ve her katılımcıya bir pay verilir. Gizli görüntünün yeniden oluşturulması için en az t sayıda katılımcının kendi paylarını üst üste koymaları gerekir. Eğer GSP şemasında, gizli görüntüyü yeniden elde etmek için bir araya gelen katılımcı sayısı, t den az olursa gizli görüntü hakkında hiçbir bilgiye erişilemez. Bu teknikte bazı problemlerle karşılaşılmıştır. Örneğin, payların boyutu gizli görüntün boyunun iki katıdır, bu yüzden yeniden yapılandırılan gizli görüntünün, orijinal görüntüye kıyaslanması durumunda kontrast kaybı oluşmaktadır.

(t,n) Gizli görüntü paylaşım şemaları Paylaştırma ve Yeniden Yapılandırma adı verilen iki alt algoritmadan oluşur. Gizli görüntü *S*, paylaştırma algoritmasını kullanarak *t* adet pay görüntülerine bölünür ve dağıtıcı tarafından *n* katılımcıya dağıtılır. Yeniden yapılandırma aşamasında ise t veya daha fazla katılımcı bir araya gelerek gizli görüntü

yeniden elde edilir. Ancak *t-1* ya da daha az pay görüntüsü gizli görüntü hakkında hiçbir bilgi vermez. Şekil 1.7'de gizli görüntü paylaşım şeması gösterilmiştir.



Şekil 1.7. Gizli Görüntü Paylaşım Şeması

PSNR değeri görüntülerin birbirleriyle olan benzerliğini karşılaştırmak için kullanılmaktadır. Yüksek PSNR değeri yeniden elde edilen görüntün kontrast kaybının daha düşük olduğunu gösterir. Eğer PSNR değeri sonsuzsa bu durumda orijinal görüntü ve yeniden elde edilen görüntün arasında hiçbir fark yoktur. Bir $M \times N$ büyüklüğündeki görüntü için PSNR oranı denklem (1.19)'da verilmiştir.

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad (dB)$$

$$MSE = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(X_{ij} - X_{ij}^{'})^2 \tag{1.19}$$

X_{ij}veX'_{ij} sırasıyla gizli görüntü ve yeniden elde edilen görüntün piksel değerlerini göstermektedir. 8 bitlik görüntülerin maksimum parlaklık değeri 255 dir.

Thien ve Lin[22] 2002 yılında, ilk olarak gizli görüntü paylaşımı için yeni bir yöntem önermişlerdir. Bu yöntem GSP şemalarından farklıdır. Önerdikleri yöntemde, gizli görüntünün yeniden elde edilmesi için matematiksel işlemler kullanılmışlardır. Bu yöntemde gizli görüntü Shamir'in sır paylaşım şeması kullanılarak, *n* tane parçaya bölünür. Paylaştırma sonrası dağıtıcı tarafından her katılımcıya gurultu benzeri bir pay

görüntüsü verilir. Pay görüntülerin boyutu, gizli görüntü boyutundan daha küçük olur ve gizli görüntü hakkında hiçbir bilgi açığa çıkarmamaktadır. Pay görüntülerin *t* tanesi bir araya gelerek gizli görüntü yeniden elde edilmektedir. Thien ve Lin'in çalışması ardından Gizli görüntü paylaşım şemaları araştırmacılar tarafından pek çok ilgi görmüştür[28-33].

Gizli görüntü paylaşım şemalarında en çok Shamir'in sır paylaşım şeması kullanılmıştır, ancak bazı yapılarda, sayı teorisine dayanarak Mignotte ve Ashmuth-Bloom'un şemaları veya Balkley'in geometrik şeması kullanılmıştır.

Gizli görüntü paylaşım şemasında gri seviyesinde olan görüntünün piksel değerleri [0,255] aralığındadır[22]. Paylaştırma aşamasında kullanılan polinom ifadesindeki asal modül değeri bu aralığın en büyük asal değeri 251, seçilir. Asal değerin seçilmesinin nedeni yeniden yapılandırma aşamasında tek bir çözüm elde edilmesidir. Ancak 251 değeri asal değeri olarak seçildiğine göre, gizli görüntünün piksel değerleri [0,250] aralığında olmak zorundadır. Böylece gizli görüntün [251,255] aralığındaki piksel değerleri 250 ye ötelenmektedir. Bu da yeniden yapılandırma aşamasında gizli görüntüde piksel parlaklık kaybına neden olur.

Bai[34] renkli görüntü üzerinde yaptığı çalışmasında Shamir'in sır paylaşım şemasını ve matris izdüşümü yöntemlerini kullanmıştır. Herhangi t sayıda pay görüntüsü bir araya gelerek, gizli görüntü kayıpsız olarak yeniden yapılandırılır. Bu yöntemde veri kaybı önlenmiştir.

Tso ve arkadaşları [35]gri gizli görüntüler üzerinde *(n,n)* sır paylaşım şemasını kullanmışlardır. Bu yöntemde n tane pay görüntüsünü oluşturmak için, dönüştürme işleminde bir çizelge kullanılmıştır. Bu yöntemde yeni yapılandırma aşamasında gizli görüntü kayıpsız olarak yeniden elde edilir.

Lukac ve arkadaşları[36], 2004 yılında her pikseli için *B* bit kullanarak kodlanılan görüntünü için sır paylaşım şeması önerilmiştir. Bu şema Shamir in yöntemini kullanmaktadır. Pay görüntülerin boyutu gizli görüntünün iki katı olarak belirlenmiştir.

Chen ve Fu[37], 2008 de gizli görüntü paylaşımında Blakley'nin sır paylaşım şemasını kullanmışlardır. Bu çalışmada *(t,n)* gizli görüntü paylaşım için *n* tane pay görüntü üretilir ve katılımcılar arasında dağıtılır. Paylaştırma algoritmasında gizli görüntü, *t* adet pikselden oluşan bölümlere ayrılır. Her bölüm*t* boyutlu uzayda bir noktayı $x = (x_1, x_2, \dots, x_t)$, temsil eder. Rastgele *n* tane farklı çözüm seti $(a_1, a_2, \dots, a_k, b)$ seçildikten sonra, $a_1x_1 + a_2x_2 + \cdots + a_kx_k = b$ hiper düzlemi oluşturulur. Çözüm seti katılımcılara dağıtılacak olan pay değerini oluşturmaktadır. Üretilen pay görüntülerin boyutu gizli

görüntünün boyutu kadardır. Yeniden yapılandırma aşamasında ise en az *t* sayısı kadar pay görüntü bir araya gelerek gizli görüntünü elde edilir. Her pay görüntüsü *t* adet pikselden oluşan bölümlere ayrılır ve bu değerler kullanılarak hiper düzlem denklemini oluşturan $(t+1)$ değer elde edilmektedir. *t*farklı görüntüden alınan, farklı hiper düzlem denklemlerinin kesiştirilmesi sonucu üretilen nokta, *t* gizli görüntü piksel değerini oluşturur. Yeniden yapılandırılan gizli görüntü kayıpsızdır.

Tso[38] 2008 yılında Blakley'in sır paylaşım şemasını kullanarak gizli görüntü paylaşım şemasını önermiştir. Bu yöntemde gizli görüntü paylaştırılmadan önce bir b katsayısı kullanarak kuantalanmaktadır. Kuantalanan görüntü permutasiyon fonksiyonuyla karıştırıldıktan sonra, *t* adet pikselden $(a_1, a_2, \dots, a_t)$ oluşan bölümlere ayrılır. Her bir bölüm için $(s_n + a_1x_1 + a_2x_2 + \cdots + a_{t-1}x_{t-1}) mod\ q = b$ hiper düzlemi oluşturulur. Burada $q = [255/b]$ olarak tanımlanır. Dağıtıcı tarafından rastgele seçilen $x_1, x_2, \dots, x_{t-1}$ değerleri kullanılarak katılımcılara dağıtılacak olan pay değerleri, $s_1, s_2, \dots, s_n$ oluşturulur. Oluşan pay görüntülerinin boyutu, gizli görüntü boyutuyla aynıdır. Gizli görüntünün yeniden yapılandırılmasında, *t* katılımcı pay görüntülerini bir araya getirir ve paylaşım algoritmasının ters işlemler uygulanır. Bu yöntemde yeniden elde edilen gizli görüntüde belli oranda kayıplar oluşur.

Ulutaş ve arkadaşları[39] çalışmalarında Tso'nun önerdiği gizli görüntü paylaşımının yeniden elde dilen görüntünün bozulmasını önlemek için geometrik tabanlı bir yöntem önermişlerdir. Burada pay görüntülerin büyüklüğü, 1/t oranında küçüktür. Bu yöntemde gizli görüntünün yeniden yapılandırmasında PSNR değeri sonsuzdur.

Gizli görüntü paylaşım çalışmalarının çoğunda, geleneksel *(t,n)* eşik sır paylaşım şemalar kullanılmaktadır. Ancak, 2011 yılında ilk olarak Guo ve arkadaşları[40], Tassa'nın önermiş olduğu hiyerarşik sır paylaşım şemasını kullanarak, hiyerarşik gizli görüntü paylaşım şemasını önermiştir. Guo'nun yönteminde, (t,n) hiyerarşik sır paylaşım şemasına göre (t-1) dereceden olan $F(x) = s_0 + s_1x + \cdots + s_{t-1}x^{t-1} \bmod p$ polinomu üretilir($s_0, s_1, s_2, \dots, s_{t-1}$ gizli görüntününpiksel değerleridir). En yüksek seviye için (t-1) dereceden olan $F(x)$ polinomu kullanılır. i.seviye için kullanılacak polinom için, $F(x)$ polinomun (t_{i-1}) turevi alınır, $(t_{-1} = 0)$. Her katılımcı için, *x* rastgele değerleri seçildikten sonra pay görüntüleri her seviye için üretilir. Pay görüntüleri dağıtıcı tarafından örten görüntüler içinde gömülür. Örneğin, hiyerarşik sır paylaşım şeması üç seviyeden oluşmaktadır, $U = U_0 \cup U_1 \cup U_2$. Gereken eşik değeri sırasıyla $t_0 = 2, t_1 = 4$ ve $t_2 = 7$ olsun. Burada gizli görüntüyü yeniden elde etmek için, gereken pay görüntüsü

en az 7 tane olmalıdır ve bu görüntülerin en az 2si birinci seviyeden, en az 4u $(U_0 \cup U_1)$ seviyesinden olması gerekmektedir. Örnekte $t = 7$ olduğundan 6.dereceden olan polinom $F(x) = s_0 + s_1 x + \cdots + s_6 x^6 \bmod p$ uretilir. Pay görüntüleri üretmek için Dağıtıcı tarafından her seviyede $F(x)$ in (t_{i-1}).dereceden turevi alınır. Birinci seviye için $F(x)$'i kullanılarak o seviyenin pay görüntüleri üretilir. İkinci seviyede ise, $t_0 = 2$ olduğu için $F(x)$'in ikinci dereceden türevi pay görüntülerini üretmek için kullanılır. Üçüncü seviye için, $t_1 = 4$ olduğundan $F(x)$'in dördüncü türevi alınır.

Yeniden yapılandırma aşamasında hiyerarşik eşik erişim yapısı oluşturarak gizli görüntü yeniden elde edilir. Bu çalışmada, pay görüntüleri hiyerarşik eşik değerini sağlamazsa, gizligörüntü tam elde edilememektedir. Ancak bu şemada, gizli görüntüyü yeniden elde etme aşamasında, üst seviyenin katılımcılarının pay görüntüsü olmazsa gizli görüntü az çok belirlenebilir ve bu durum gizli ve önemli görüntüler için uygun olmamaktadır. Bu çalışmada yeniden elde edilen gizli görüntüsünün PSNR değeri sonsuz olarak elde edilmiştir.

1.4. Barkodlar

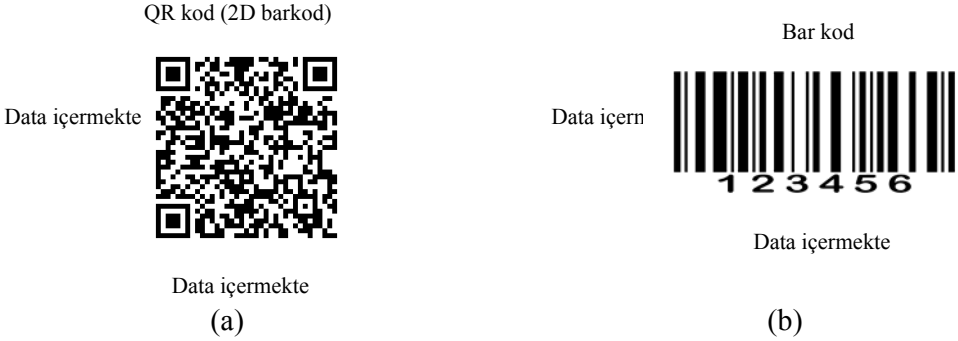
Barkod günümüzde ürünler hakkında bilgileri içeren 1 boyutlu(1B) veya 2 boyutlu(2B) verilerin, görsel özellikli makineler tarafından okunabilmesi için çeşitli kodlama yöntemidir. Günümüzde hiçbir ürün kalite veya miktarına rağmen barkodsuz değildir. Barkodların kimyasal ve biyomedikal analizlerinin araçlarında idari, dosyalarda, ilaç paketlerinde, şahsi kartlarda ve dokümanlarda, posta ve benzeri gibi uygulamalarda kullanımı giderek artmaktadır. Ürün üzerine barkodların basılması veya barkodların okunması için ek işleme, donanım cihazlarına gerek yoktur. Üründeki barkodlar optik makineler yardımıyla veya mobil cihazlar tarafından okunmaktadır. Örneğin, barkod bilgileri cep telefonlar üzerinden okunabilinir.

Tek boyutlu barkodlar paralel çizgilerden oluşmaktadır. Bu çizgiler arasındaki mesafe, barkodun taşımış olduğu bilgiyi ifade eder. Code 39, Code 128, EAN-128 veya ISBN gibi barkodlar, 1B barkodlara örnek olarak verilebilir. Barkodların hata oranı düşüktür ve üretimi daha kolaydır. Ancak tek boyutlu barkodların veri taşıma kapasitesi azdır, bazı karakterleri ifade edememektedir. Örneğin, marketlerden gelen isteklerde barkodların daha çok bilgi taşıyabilmesi ve daha küçük alanda basılabilmesi gündeme gelmiştir. Küçük alanda çok miktarda bilgi içermesi, herhangi bir açıdan okunma imkânı,

barkodun 60%'ı bozulmuş olsa bile okunabilmesi, VeriMatris'in avantajlarındandır. Bu yüzden iki boyutlu barkodlar tanımlanmıştır. Şekil 1.8 de barkodların çeşitleri verilmiştir. Şekil 1.8(a)'da 1B barkodlar, şekil 1.8(b)'de 1B barkodların daha çok bilgi içermesi için, üst üste yığılmış barkodlar ve şekil 1.8(c)'de 2B barkod gösterilmiştir.

Şekil1.8. Barkod çeşitleri: (a) 1B barkodlar (b) Yığılmış barkod (c) 2B barkod (matris türü)

1B barkodlarda tek yönde veri kodlanırken, 2B barkodlarda iki yönde de veri kodlanmaktadır. Şekil 1.9'da barkodlarda kodlama yönleri gösterilmiştir.



Şekil 1.9. Barkodlarda kodlama yönleri (a) 2B barkodlar (b) 1B barkodlar

Veri kodlaması için tanımlanan 2B barkodların kapasitesi artmıştır, böylece daha çok veri kodlanmaktadır. Maxicode, QR kod, Datamatrix kod, PDF 417 gibi barkodlar, 2B barkodların örneklerindendir. Şekil 1.10'da 2B barkodların çeşitleri gösterilmiştir.

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

Şekil 1.10. (a) Maxi code (b) PDF 417 (c) QR code (d) Data Matris (e) AztecCode

İki boyutlu barkodlar birçok uygulamada kullanılmaktadır. Örneğin, Japonya'da Mcdonalds paketleri üzerinde QR kodları bulunmaktadır. Kullanıcı bu barkodu taradıktan sonra, Mcdonalds'n web sitesinden o ürün hakkındaki tüm bilgilere ulaşabilir.

Barkod bilgileri, cep telefonlarının açık kaynak yazılımları tarafından rahatça okunabilinir. Ancak barkodlar üzerinde taşınan bilgiler gizli bilgi olması durumu da mümkündür. Barkodlar üzerinde olan gizli bilgilerin gizliliğini sağlanması için araştırmalar yapılmıştır [41-44]. Örneğin, 2010 yılında Chuang ve arkadaşları[41]*(t,n)*Shamir'in sır paylaşım şemasını kullanarak gizli veriyi paylara bölüp QR kodları içerisinde gömmüşlerdir. Böylece en az *t* sayıda QR kodlarının bir araya gelmesi durumunda barkod üzerindeki gizli veri elde edilir. *t-1*veya daha az katılımcının bir araya gelmesi durumunda gizli veriyle ilgili hiçbir bilgiye ulaşılmaz.

1.4.1. VeriMatris

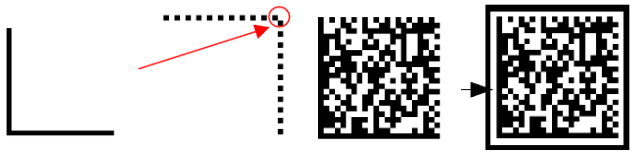
VeriMatrisi barkodları iki boyutlu barkod türüdür. Bu tür barkodlarda veri, iki dikey ve yatay yönde kodlanmaktadır. VeriMatris barkodları, makine, motor parçaları, cerrahi ve tıbbi enstrümanlarda kullanımları yaygındır. Örneğin, bu barkodlar posta servislerinde paket dağıtımı ve teslimatında yüksek verim elde etmek açısından kullanılmıştır. Mektuplar üzerinde kullanılan mektubun adresi, gönderici ve alıcının ismi ve benzeri bilgiler içeren VeriMatris barkodlar, makineyle üretilir ve paket üzerine basılır.

VeriMatris 80'lerin son yıllarında USA de ortaya çıkmıştır. VeriMatris'in iki çeşidi vardır. Birincisi, ECC 200 Reed-Solomon hata düzeltmesini[45]kullanmaktadır ve yeni uygulamalar için önerilmiştir. ECC 200 Data Matrisi, ASCII, ISO/IEC 646, C40, Text,X12, EDIFACT ve Base 256 gibi birçok kodlama yapılarını desteklemektedir. İkincisi ECC 000-140 gibi kapalı uygulamalarda kullanılmaktadır. Bu tür uygulamalarda

bir grup, sembollerin üretilmesini ve okunmasını kontrol eder. Ayrıca sistemin performansından sorumludur. Tez çalışmasında ECC200 VeriMatris kullanılmıştır.
ECC200 VeriMatris'in özellikleri aşağıda verilmiştir.

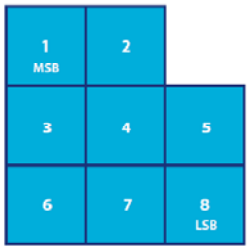
1. Kodlanabilir karakter kümesi
    a) ISO/IEC 646 US ulusal versiyonuna göre 0-127 arasındaki olan değerlerdir.
    b) ISO 8859-1 e göre 128-255 arasında olan değerlerdir. Bu değerlere genişletilmiş ASCII denilir.
2. Veri temsilciliği: karanlık modül, bir ve ışık modül, sıfırdır.
3. Modüllere göre sembol boyutu: ECC 200 (10×10 dan ta 144×144 sadece çift değerler), ECC 000-140(9×9 dan ta 49×49 ,sadece tek değerler)
4. Her sembol için veri karakterleri (ECC 200 olan maksimum sembol boyutu için):
    a) Alfa nümerik veri: 2335 karakter
    b) Sayısal veri: 3116 rakam
5. Seçilmiş hata düzeltme:
    a) ECC 200: Reed-Solomon hata düzeltme
    b) ECC 000-140: katlamalı hata düzeltmenin dört seviyesi
6. Kod turu: Matris
7. Yon belirleme bağımlılığı: var

Şekil 1.11 verimatris'in dört ana parçası gösterilmiştir. Şekil 1.11(a)'da VeriMatris'in hesaplama yönünü belirlemek için kullanılan Sabit sınır hattını göstermektedir. Şekil 1.11(b)'de satır ve sütun sayılarını gösteren açık sınır adlı verilen parça verilmiştir. ECC 200'de açık sınır parçasında üst sağ köşe beyazdır. Şekil 1.11(c)'de bilgilerin kodlanmış formunu içeren hafıza bölgesi gösterilmiştir. Şekil 1.11(d)'de belirgin bölge olarak adlandırılan parça gösterilmektedir. Bu parça, VeriMatris'inin etrafını çevreleyen boş bir bölgedir. Bu bölge ve yönlendirme amacı için kullanıldığından hiçbir bilgi içermez. Belirgin bölgenin eni bir satırdır.

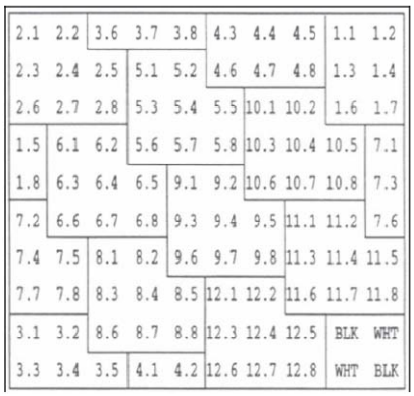


Şekil 1.11. VeriMatris'in ana parçaları (a) Sabit sınır hattı (b) Açık sınır (c) Hafıza bölgesi (d) belirgin bölge

VeriMatris barkodlarında her karakter sembolü, sekiz modülle temsil edilir ve şekil olarak karedir. Her modül bir bitle ifade edilir. Bir karakter sembolünü oluşturmak için, sekiz modülü soldan sağa doğru ve üstten aşağıya doğru sıralanır, şekil 1.12'de gösterilmiştir. Karakter sembolünün biçimi sınırlarında birbiriyle iç içe olamadığından dolayı, bazı karakter sembolü parçalara bölünmüştür. Bu biçimin yerleştirilmesi Standard ISO/IEC 16022 (F.3)'da tanımlanmıştır. 1.1, ilk kelime kodunun birinci bitine, 1.2 ilk kelime kodunun ikinci bitine, 1.3 ilk kelime kodunun uçuncu bitine karşılığıdır ve benzeri gibi.Şekil 1.13'de bir ECC 200 10 × 10 sembolü gosterilmiştir.



Şekil 1.12. LSB: en anlamsız bit, MSB: en anlamlı bit



Şekil 1.13. ECC 200 10 × 10 sembolü

2. YAPILAN ÇALIŞMALAR

Günümüzde askeri ve ticari belgelerin, tıbbi görüntülerin, nükleer bombanın ateşlenme onay anahtarı gibi verilerin, gizliliğinin sağlanması literatürde önem verilen konulardandır. Kriptografi ve steganografi gizli verilerin güvenliğini sağlamasında kullanılan iki yöntemdir. Kriptografi bir sayısal anahtarı kullanarak, gizli veriyi şifreler. Bu yöntemde gizli veriyi yeniden elde etmek için şifrelemenin tersi deşifreleme algoritması kullanılmaktadır. Diğer yöntemde ise örten ortam olarak adlandırılan herhangi bir görüntü ya da video dosyasını gizli verinin saklamasında kullanılmaktadır. Bu iki yöntemde tek bir kişiye güvenmeye dayanmaktadır. Böylece sırın kaybolması veya bozulması durumunda gizli veri yeniden elde edilmemektedir.

Son yıllarda gizli verinin güvenliğini sağlamak için sır paylaşım teknikleri kullanılmıştır. Sır paylaşım şemalarında, gizli veri kişiler arasında paylaştırılır ve ancak belli sayıda kişinin bir araya gelmesi durumunda gizli veri yeniden elde edilir. Sır paylaşım şemaları paylaştırma ve yeniden yapılandırma algoritmalarından oluşmaktadır. Paylaştırma algoritmasında gizli veri n katılımcı arasında paylaştırılır. *n* katılımcıdan, en az *t* sayısı kadar katılımcı bir araya gelerek sır yeniden elde edilebilir. Bu şema eşik sır paylaşım şeması olarak adlandırılır ve *(t,n)* ile gösterilir. Eşik şemaları, banka kasasının anahtarının paylaştırılması, nükleer silahların onaylanması, ticari belgelerin erişimi ve benzeri gibi uygulamalarda kullanmaktadır. Bu yöntemde bir kişi yerine gruba yetki vermesine dayanmaktadır. Böylece bazı payların kaybolması durumunda bile gizli veri belli sayıda kişinin bir araya gelmesi durumunda yeniden elde edilebilir.

Verilen örneklerin bazılarında, doğal olarak katılımcılar aynı yetkiye sahip değillerdir. Örneğin, banka senaryosunda kasanın anahtarının payları banka personelleri (banka memuru ve banka müdürü) arasında dağıtılır. Bankanın politikasına göre kasanın açılması için personellerden en az birisi banka müdürü olacak şekilde en az uç personel gerekir. Bu gibi durumlarda, çok parçalı sır paylaşım şemaları kullanılmaktadır.

Tez kapsamında yapılan çalışmalar aşağıda maddeler halinde verilmektedir.

1. Birleştirici ve ayrıcı hiyerarşik erişim yapısı için ideal sır paylaşım şeması önerilmektedir. İdeal ve mükemmelliği sağlanmış olan bu şema, Blakley'in geometri tabanlı yöntemine dayanmaktadır.

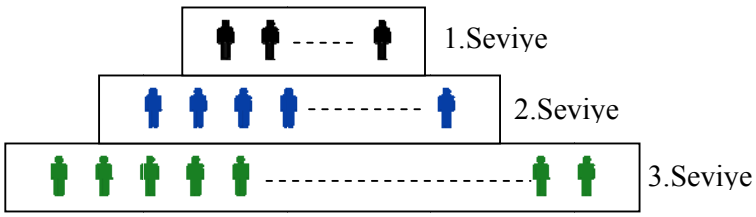
2. Yeni bir Birleştirici hiyerarşik gizli görüntü paylaşım şeması önerilmiştir. Bu şemada genişleme oranı $1/t$ dir. Ancak incelemelerine göre bu şema gizliliği sağlamamaktadır. Gizliliğin sağlanması için genişleme oranı $1/t$ye eşit olan şema önerilmiştir. Önerilen yöntemde XOR kullanarak bu problemin üstesinden gelmiştir.Önerilen tüm şemalarda PSNR değeri sonsuzdur.
3. Yeni bir iç içe bölütlenmiş erişim yapısı tanımlanmıştır. Bu erişim yapısı için, Shamir'in eşik şemasına dayanarak ideal ve mükemmel sır paylaşım şeması önerilmiştir.
4. Literatür taramalarına göre İlk kez iç içe bölütlenmiş gizli görüntü paylaşım şeması önerilmiştir. Bu şemada genişleme oranı 1'e eşittir.
5. Tez çalışmasında gizli veri Blakley'in sır paylaşım şeması kullanılarak paylara bölünür. Üretilen pay değerleri VeriMatrisi içinde saklanılır. Böylece VeriMatrisndeki gizlilik gerektiren verilerin güvenliği sağlanmıştır.

Tezde yapılan gizli görüntü sır paylaşım şemalar Borland C++ Builder ortamı kullanarak gerçeklenmiştir. Maddeler halinde verilmiş olan çalışmalar detayları ilerleyen bölümlerde verilmektedir.

2.1. Hiyerarşik Erişim Yapısı

Hiyerarşik sır paylaşım şemasında, katılımcılar kümesi yetkilerine göre hiyerarşik olarak, $L_1, L_2, \dots, L_m$ seviyeleri arasında bölünür, şekil 2.1. L_1 en yüksek seviyeyi ve L_m ise en alçak seviyeyi gösterir. Her seviye için tanımlanan eşik değerleri, her seviye için bir koşul olduğunun farz edilirse, m seviye için m koşul var olmaktadır. Hiyerarşik erişim yapısının iki farklı erişim yapısı vardır, birleştirici ve ayrıcı. Birleştirici hiyerarşik erişim yapısında m koşulun sağlanması gerekir oysa ayrıcı hiyerarşik erişim yapısında m'nin herhangi bir koşulu sağlanması yeterlidir. Örneğin üniversitelerde, lisansüstüne başvurularda öğrenci adaylarından referans mektubu istenir. Referans mektuplarının en az ikisi Profesör olmak koşuluyla minimum 5 öğretim üyesinden istenmektedir. Bu senaryoda Profesörler en üst seviyede diğerleri ise ikinci seviyedendirler. Bu seviyeler için gereken eşik değerleri sırasıyla $t_0 = 2$ ve $t_1 = 5$tir. Birleştirici hiyerarşik erişim yapısında bir üst seviyenin pay değerleri, aşağı seviyedeki pay değerleri yerine geçebilir. Örneğin iki Profesör ve üç Yardımcı doçent, üç Profesör ve iki Yardımcı doçent, dört Profesör ve bir

Yardımcı doçent veya beş Profesörden oluşan tüm durumlar geçerlidir. Oysa ayrıcı hiyerarşik erişim yapısında bir alt seviyenin pay değerleri, üst seviyedeki pay değerleri yerine geçebilir. Örneğin iki Profesör ve üç Yardımcı doçent, bir Profesör ve dört Yardımcı doçent veya beş Yardımcı doçentten oluşan tüm durumlar geçerlidir. İlerleyen bölümlerde hiyerarşik erişim yapısının iki farklı erişim yapıları kısaca bilgilendirilmiş ardından hiyerarşik sır paylaşım şeması önerilmiştir.



Şekil 2.1. Hiyerarşik sır paylaşım şeması

2.1.1. Birleştirici Hiyerarşik Sır Paylaşım Şeması

Tassa'nın önerdiği birleştirici hiyerarşik erişim yapısını göz önüne alarak, bu yapı için Blakley'nin geometri şemasına dayanarak yeni bir ideal birleştiren hiyerarşik sır paylaşım şeması tanımlanmaktadır.

Tanım 2.1: $U = \cup_{i=0}^{m} U_i$, $U_i \cap U_j = \phi$, $0 \le i < j \le m$, m seviyeye bölünmüş olan, n katılımcının kümesi olsun. $t = \{t_i\}_{i=0}^{m}$, $0 < t_1 < \cdots < t_m$, monoton artan tamsayıların sırası olsun. Birleştirici hiyerarşik erişim yapısı (2.1)'de verilen ifadeyle tanımlanmaktadır.

$$\Gamma = \left\{ A \subset U : \left| A \cap \left(\bigcup_{j=0}^{i} U_i \right) \right| \ge t_i, \forall i \in \{0,1,\ldots,m\} \right\} \tag{2.1}$$

Gizli veri *S, GF(q)* vektör uzayında bir nokta olarak seçilir. Bu noktada kesişen *n*adet doğru için denklemler oluşturularak *n* katılımcı arasında dağıtılır. Paylaştırma algoritması aşağıdaki şekildedir.

Adım 1. Gizli veri *S*, GF(q) vektör uzayından, $(t-1)$ boyutlu uzayda bir noktanın tek bir koordinatı alınarak, $(a_0 = S, a_1, \ldots, a_{t-1})$ şeklinde seçilir.

Adım 2. Dağıtıcı tarafından , $(t-1)$ boyutlu hiper düzlem, $P(x)=\sum_{j=0}^{t-1} a_j \,.\, x$, $a_0 = S$ üretilir.

Adım3. i.seviyede olan $u \in \mathcal{U}_i$, $0 \le i \le m$, katılımcılar için, $P_i(x) = \sum_{j=t_{i-1}}^{t-1} a_j \,.\, x$ $(t_{-1}=0)$ hesaplanır.

Adım 4.$\mathcal{U}_i$ seviyesinde olan her u_{ij} katılımcı için $x=(x_{i,j},\dots,x_{i,t-t_{i-1}}) \in GF(q)$ kümesi rasgele seçilir ve $s_{i,j}=P_i(x_{i,j},\dots,x_{i,t-t_{i-1}})$ özel pay değerleri oluşturulur. Her katılımcıya sadece bu $s_{i,j}$ değeri verilir. $x$katsayısı dağıtıcı tarafından bilinen veridir.

Teorem 2.2: Tanım2.1'de önerilen birleştirici hiyerarşik sır paylaşım şeması mükemmel ve idealdir.

İspat:$A=\{u_0,\dots,u_{|A|}\} \subset U$ katılımcılar kümesi olsun ve bu kümenin katılımcıları hiyerarşik düzende olmaktadır. Her seviyeden katılan katılımcı sayısı $0 \le \alpha_0 \le \cdots \le \alpha_m = |A|$ olsun, yani:

$$
\begin{aligned}
&u_0,\dots,u_{\alpha_0} \in U_0\\
&u_{\alpha_0+1},\dots,u_{\alpha_l} \in U_1\\
&\vdots\\
&u_{\alpha_{l-1}+1},\dots,u_{\alpha_m} \in U_m
\end{aligned}
$$

Eğer $\alpha_i \ge t_i$, $\forall\, i: 0 \le i \le m$ için sağlanmış olursa bu durumda A yetkilidir ve gizli bilgi yeniden elde edilir. $a=(a_0=S,a_1,\dots,a_{t-1})$,$(t-1)$ boyutlu uzayda, $P(x)$'in katsayıları olarak düşünülür. Gizli veri bu noktanın ilk koordinatı olarak gösterilmiştir. Her seviye için, bu noktayı kesen, $t-t_{i-1}$ boyutlu hiper düzlem denklemi oluşturulur. Böylece en yüksek seviyede olan katılımcılar gizli veriyi, $a_0=S$barındıran hiper düzleme sahiptir. Diğer seviyeler için, $a_0=S$ içermeyen $t-t_{i-1}$ boyutlu hiper düzlem denklemi oluşturulmuştur yani noktanın daha az koordinat bilinmektedir. Her katılımcıya dağıtılan pay miktarı, $x.a=p(u)$ olarak tanımlanır.

Gizli veri,$a_0=S$, A kümesinde olan tüm katılımcılar kendi paylarını bir araya koyarak, (2.2)'de verilen doğrusal denklemin çözülmesiyle elde edilir:

$$\underbrace{\begin{bmatrix} x_{0,0,0} & x_{0,0,1} & x_{0,0,2} & \cdots & & \cdots & x_{0,0,t-t_{i-1}-1} \\ \vdots & & & & & & \\ x_{0,\alpha_0,0} & x_{0,\alpha_0,1} & x_{0,\alpha_0,2} & \cdots & & & x_{0,\alpha_0,t-t_{i-1}-1} \\ 0 & \cdots & 0 & x_{1,\alpha_0+1,0} & \cdots & \cdots & x_{1,\alpha_0+1,t-t_{i-1}-1} \\ \vdots & & & & & & \\ & & & x_{1,\alpha_1,0} & & & \\ \vdots & & & & & & \\ 0 & \cdots & \cdots & 0 & x_{m,\alpha_{m-1}+1,0} & \cdots & x_{m,\alpha_{m-1}+1,t-t_{i-1}-1} \\ \vdots & & & & & & \\ 0 & \cdots & \cdots & 0 & x_{m,\alpha_m,0} & \cdots & x_{m,\alpha_m,t-t_{i-1}-1} \end{bmatrix}^{-1}}_{M_A} \times \begin{bmatrix} b_0 \\ \vdots \\ b_{\alpha_0} \\ b_{\alpha_0+1} \\ \vdots \\ b_{\alpha_1} \\ \vdots \\ b_{\alpha_{m-1}+1} \\ \vdots \\ b_{\alpha_m} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ \\ \vdots \\ \\ \\ \\ a_{t-1} \end{bmatrix} \tag{2.2}$$

A en az yetkili küme olsun, yani $|A| = t$, bu durumda yeniden yapılandırma matrisi M_A , kare ve düzenlidir. Böylece *S* sırrı elde edilir. Eğer A minimum değilse, yani $|A| > t$, buradan bir $A_0 \subset A$ vardır ve $|A_0| = t$ yetkilidir. M_{A_0} , M_A nın alt matrisi olduğu için, düzenlidir, böylece $M_A a = b$ bağıntısının tek bir çözümü olmaktadır.

$A \notin$ Γyetkisiz küme olsun, yani *A* kümesinde olan katılımcılar kendi paylarını bir araya koyarak, gizli veriyle ilgili hiçbir bilgiye erişememektedir. Burada iki durum vardır: birincisi $|A| \neq t$ olursa, yeniden yapılandırma aşamasında, denklem sayısı ve bilinmeyen sayısı eşit olmayacaktır ve yeniden yapılandırma matrisi M_A kare olamadığı için, denklemin çözümü bulunmamaktadır. Böylece gizli veri elde edilemeyecektir. İkinci durumda, Eğer $|A| = t$ ise gizli veriyi elde etmek için katılan katılımcıların hiç birisi üst seviyeden değilse yeniden yapılandırma matrisi $M_A = 0$ olacaktır ve böylece gizli veri elde edilemeyecektir.

Bu şema idealdir, çünkü her katılımcı, $GF(q)$ alanından sadece bir pay değeri alır. Buradan bilgi oranı bire eşittir.

Örnek 2.1: Üç seviyeli bir hiyerarşik sır paylaşım şeması düşünülür. Katılımcılar kümesi $\mathcal{U} = \mathcal{U}_0 \cup \mathcal{U}_1 \cup \mathcal{U}_2$ dir ve $t = (t_0, t_1, t_2) = (2,4,7)$ eşik miktarlarıdır. Yani $A \subset U$ yetkili kümesidir. Burada gizli veriyi elde etmek için katılımcı sayısı en az 7 olması gerekir. bu yedi katılımcının , en az dört katılımcısı $\mathcal{U}_0 \cup \mathcal{U}_1$ den ve 2 katılımcı da $\mathcal{U}_0$dan olması gerekir. $t = t_2 = 7$olduğu için, dağıtıcı tarafından $t - 1 = 6$ boyutlu olan bir hiper düzlem, $P(x) = \sum_{j=0}^{6} a_j x_j$, $a_0 = S$, denklemi oluşturulur. Ayrıca her seviye $u \in \mathcal{U}_i$ katılımcılar için üretilen hiper düzlem denklemi aşağıdaki şekilde ifade edilir.

$$u \in \mathcal{U}_0, \quad P_0(x) = \sum_{j=0}^{6} a_j \,.\, x = (a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6).x$$
$$u \in \mathcal{U}_1\,, \quad P_1(x) = \sum_{j=2}^{6} a_j \,.\, x = (a_2 + a_3 + a_4 + a_5 + a_6).x$$
$$u \in \mathcal{U}_2\,, \quad P_2(x) = \sum_{j=4}^{6} a_j \,.\, x = (a_4 + a_5 + a_6).x$$

12 katılımcının olması durumunda, her katılımcıya $x_{i,j,z}$, $(0 \le i \le m\,,\ 0 \le j \le \alpha_i\,, 0 \le z \le t - t_{i-1})$ değeri verilir ve $M \times a = b$ denklik sistemi (2.3)'de verilen şekilde üretilir. Mdağıtıcı tarafından belirlenen çözüm dizisi, a bir noktanın koordinatları ve b üretilen pay değerleridir.

$$\begin{bmatrix} x_{0,0,0} & x_{0,0,1} & x_{0,0,2} & x_{0,0,3} & x_{0,0,4} & x_{0,0,5} & x_{0,0,6} \\ x_{0,1,0} & x_{0,1,1} & x_{0,1,2} & x_{0,1,3} & x_{0,1,4} & x_{0,1,5} & x_{0,1,6} \\ x_{0,2,0} & x_{0,2,1} & x_{0,2,2} & x_{0,2,3} & x_{0,2,4} & x_{0,2,5} & x_{0,2,6} \\ 0 & 0 & x_{1,3,0} & x_{1,3,1} & x_{1,3,2} & x_{1,3,3} & x_{1,3,4} \\ 0 & 0 & x_{1,4,0} & x_{1,4,1} & x_{1,4,2} & x_{1,4,3} & x_{1,4,4} \\ 0 & 0 & x_{1,5,0} & x_{1,5,1} & x_{1,5,2} & x_{1,5,3} & x_{1,5,4} \\ 0 & 0 & x_{1,6,0} & x_{1,6,1} & x_{1,6,2} & x_{1,6,3} & x_{1,6,4} \\ 0 & 0 & 0 & 0 & x_{2,7,0} & x_{2,7,1} & x_{2,7,2} \\ 0 & 0 & 0 & 0 & x_{2,8,0} & x_{2,8,1} & x_{2,8,2} \\ 0 & 0 & 0 & 0 & x_{2,9,0} & x_{2,9,1} & x_{2,9,2} \\ 0 & 0 & 0 & 0 & x_{2,10,0} & x_{2,10,1} & x_{2,10,2} \\ 0 & 0 & 0 & 0 & x_{2,11,0} & x_{2,11,1} & x_{2,11,2} \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \\ b_9 \\ b_{10} \\ b_{11} \end{bmatrix} \qquad (2.3)$$

Yeniden yapılandırma aşamasında, 7 katılımcının pay değerleri ele alınır ve yeniden yapılandırma matrisi oluşturulur. Denklik sisteminin çözümü $M^{-1} \times b = a$, (2.4)'de verilen ifadeyle gösterilmiştir.M^{-1}yeniden yapılandırma matrisi, b katılımcıların pay değerleri ve a yeniden yapılan gizli veridir.

$$\begin{bmatrix} x_{0,1,0} & x_{0,1,1} & x_{0,1,2} & x_{0,1,3} & x_{0,1,4} & x_{0,1,5} & x_{0,1,6} \\ x_{0,2,0} & x_{0,2,1} & x_{0,2,2} & x_{0,2,3} & x_{0,2,4} & x_{0,2,5} & x_{0,2,6} \\ 0 & 0 & x_{1,4,0} & x_{1,4,1} & x_{1,4,2} & x_{1,4,3} & x_{1,4,4} \\ 0 & 0 & x_{1,6,0} & x_{1,6,1} & x_{1,6,2} & x_{1,6,3} & x_{1,6,4} \\ 0 & 0 & 0 & 0 & x_{2,8,0} & x_{2,8,1} & x_{2,8,2} \\ 0 & 0 & 0 & 0 & x_{2,9,0} & x_{2,9,0} & x_{2,9,0} \\ 0 & 0 & 0 & 0 & x_{2,11,0} & x_{2,11,0} & x_{2,11,0} \end{bmatrix}^{-1} \times \begin{bmatrix} b_1 \\ b_2 \\ b_4 \\ b_6 \\ b_8 \\ b_9 \\ b_{11} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} \tag{2.4}$$

Örnek 2.2: Örnek 2.1'de gizli veri 6 boyutlu uzaydaki noktasının $(9,29,242,96,170,137,141)$, ilk koordinatının değeridir $s = 9$. Dağıtıcı tarafından belirlenen x değerleri, çözüm dizisini oluşturur. (2.5)'de verilen denklem sistemini hesaplayarak her katılımcıya bir pay değeri üretilip dağıtılır.

$$\left[\begin{array}{ccccccc} 2 & 3 & 5 & 7 & 2 & 1 & 4 \\ 1 & 5 & 2 & 3 & 6 & 7 & 2 \\ 2 & 3 & 1 & 4 & 5 & 3 & 1 \\ \hline 0 & 0 & 2 & 1 & 3 & 1 & 4 \\ 0 & 0 & 4 & 5 & 7 & 1 & 2 \\ 0 & 0 & 1 & 2 & 3 & 5 & 4 \\ 0 & 0 & 3 & 2 & 1 & 4 & 5 \\ \hline 0 & 0 & 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & 3 & 1 & 7 \\ 0 & 0 & 0 & 0 & 4 & 1 & 2 \\ 0 & 0 & 0 & 0 & 6 & 5 & 1 \\ 0 & 0 & 0 & 0 & 2 & 6 & 7 \end{array}\right] \times \begin{bmatrix} 9 \\ 29 \\ 242 \\ 96 \\ 170 \\ 137 \\ 141 \end{bmatrix} = \begin{bmatrix} 16 \\ 175 \\ 125 \\ 34 \\ 45 \\ 185 \\ 82 \\ 228 \\ 128 \\ 95 \\ 89 \\ 141 \end{bmatrix} \tag{2.5}$$

Yeniden yapılandırmada aşamasında 7 katılımcının pay değerleri hiyerarşik eşik koşulunu sağlayacak şekilde bir araya gelmesi gerekmektedir. Bu durumda eşik değeri (2,4,7) olduğuna göre, birinci seviyeden (175,125), ikinci seviyeden (45,82), üçüncü seviyeden (128,95,141) pay değerleri ele alınır. Gizli veri $S = 9$, (2.6)'da verilen denklem sistemini hesaplayarak elde edilir.

$$\begin{bmatrix} 143 & 180 & 71 & 1 & 126 & 193 & 54 \\ 72 & 215 & 0 & 215 & 246 & 173 & 181 \\ 0 & 0 & 179 & 180 & 42 & 208 & 185 \\ 0 & 0 & 108 & 107 & 45 & 237 & 31 \\ 0 & 0 & 0 & 0 & 120 & 164 & 120 \\ 0 & 0 & 0 & 0 & 74 & 83 & 225 \\ 0 & 0 & 0 & 0 & 225 & 133 & 24 \end{bmatrix} \times \begin{bmatrix} 175 \\ 125 \\ 45 \\ 82 \\ 128 \\ 95 \\ 141 \end{bmatrix} = \begin{bmatrix} 9 \\ 29 \\ 242 \\ 96 \\ 170 \\ 137 \\ 141 \end{bmatrix} \quad (2.6)$$

Örnek 2.3: örnek 2.2'de yeniden yapılandırma aşamasında, gizli veriyi yeniden elde etmek için m koşulun sağlanması gerekir aksi takdirde gizli veri yeniden elde edilemez. Örneğim eğer birinci seviyeden katılımcı olmazsa bu durumda gizli veri elde edilemez. İkinci seviyeden (45,82), üçüncü seviyeden (128,95,141) pay değerleri ele alınır. (2.7)'de verilen denklik sisteminin çözümü bu durumu gösterir.

$$\begin{bmatrix} 179 & 180 & 42 & 208 & 185 \\ 108 & 107 & 45 & 237 & 31 \\ 0 & 0 & 120 & 164 & 120 \\ 0 & 0 & 74 & 83 & 225 \\ 0 & 0 & 225 & 133 & 24 \end{bmatrix} \times \begin{bmatrix} 45 \\ 82 \\ 128 \\ 95 \\ 141 \end{bmatrix} = \begin{bmatrix} 242 \\ 96 \\ 170 \\ 137 \\ 141 \end{bmatrix} \quad (2.7)$$

2.1.2. Ayrıcı Hiyerarşik Sır Paylaşım Şeması

Simmons'unönerdiği ayrıcı hiyerarşik erişim yapısında seviyeler için belirlenen koşulların birisi sağlandığı takdirde gizli veri elde edilir.

Tez çalışmasında önerilen (t,n) birleştirici hiyerarşik sır paylaşım şemasında bazı değişiklikler yaparak, yeni bir ideal sır paylaşım şeması önerilmiştir. Bu değişiklikler orijinal şemada gizli veri a_0'a eşittir ama yeni şemada gizli veri a noktasının son koordinatıa_{t-1} olarak alınır. Bir diğeri ise daha önemli olan seviyeler için a noktasının daha az koordinatları verilir. Ayrıcı hiyerarşik sır paylaştırma algoritması aşağıdaki verilmiştir.

Adım 1. Gizli veri *S*, GF(q) vektör uzayından, bir noktanın sadece tek bir koordinatı alınarak, $(a_0, a_1, \dots, a_{t-1} = S)$ seçilir.

Adım 2. Dağıtıcı tarafından rastgele $t-1$ boyutlu hiper düzlem $P(x)=\sum_{j=0}^{t-1} a_j . x$, $a_{t-1}=S$ üretilir.

Adım 3.i. seviyede olan $u \in \mathcal{U}_i$, $0 \leq i \leq m$, katılımcılar için, $P_i(x)=\sum_{j=t-t_i}^{t-1} a_j x_j$, $t_{-1}=0$'ın polinomu üretilir.

Adım 4.$\mathcal{U}_i$ seviyesinde olan her u_{ij} katılımcı için $x=(x_{i,j,0},\ldots,x_{i,})\in GF(q)$ kümesi verilir ve $s_{i,j}=P_i(x_{t_{i-1},j},\ldots,x_{t-1,j})$ özel pay değeri üretilir. Her katılımcıya sadece $s_{i,j}$ pay değeri verilir. $x$katsayısı dağıtıcı tarafından bilinen değerdir.

Örnek 2.4: Hiyerarşik olarak üç seviyeden oluşan bir $\mathcal{U}=\mathcal{U}_0 \cup \mathcal{U}_1 \cup \mathcal{U}_2$ katılımcı kümesi ele alınır. $t=(t_0,t_1,t_2)=(2,4,7)$eşik miktarları olsun. Bu durumda $\mathcal{U}_2$ seviyesinden katılan katılımcı sayısı en az 7 veya $\mathcal{U}_1$ seviyesinden en az 4 katılımcı veya $\mathcal{U}_0$ seviyesinden en az 2 katılımcı olursa gizli veri S yeniden elde edilebilir. $t=t_2=7$olduğu için, dağıtıcı 6 boyutlu hiper düzlemi $P(x)=\sum_{j=0}^{6} a_j . x$, $a_6=S$ denklemini üretir. Ayrıca her seviye $u \in \mathcal{U}_i$ katılımcılar için üretilen hiper düzlem denklemi aşağıdaki şekilde ifade edilir.

$$u \in \mathcal{U}_0,\ P_0(x)=\sum_{j=5}^{6} a_j . x=(a_5+a_6).x$$
$$u \in \mathcal{U}_1\ , P_1(x)=\sum_{j=3}^{6} a_j . x=(a_3+a_4+a_5+a_6).x$$
$$u \in \mathcal{U}_2\ , P_2(x)=\sum_{j=0}^{6} a_j . x=(a_0+a_1+a_2+a_3+a_4+a_5+a_6).x$$

payı alınır.

12 katılımcının olması farzıyla, her katılımcıya $x_{i,j,z}$, $(0 \leq i \leq m\ ,\ 0 \leq j \leq \alpha_i\ , 0 \leq z \leq t-t_{i-1})$ değeri verilir ve $M \times a=b$ denklik sistemi (2.8)'de verilen şekilde üretilir. Mdağıtıcı tarafından belirlenen çözüm dizisi, a bir noktanın koordinatları ve b üretilen pay değerleridir.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & x_{0,0,0} & x_{0,0,1} \\ 0 & 0 & 0 & 0 & 0 & x_{0,1,0} & x_{0,1,1} \\ 0 & 0 & 0 & 0 & 0 & x_{0,2,0} & x_{0,2,1} \\ 0 & 0 & 0 & x_{1,3,0} & x_{1,3,1} & x_{1,3,2} & x_{1,3,3} \\ 0 & 0 & 0 & x_{1,4,1} & x_{1,4,2} & x_{1,4,3} & x_{1,4,4} \\ 0 & 0 & 0 & x_{1,5,1} & x_{1,5,2} & x_{1,5,3} & x_{1,5,4} \\ 0 & 0 & 0 & x_{1,6,1} & x_{1,6,2} & x_{1,6,3} & x_{1,6,4} \\ x_{2,7,0} & x_{2,7,1} & x_{2,7,2} & x_{2,7,3} & x_{2,7,4} & x_{2,7,5} & x_{2,7,6} \\ x_{2,8,0} & x_{2,8,1} & x_{2,8,2} & x_{2,8,3} & x_{2,8,4} & x_{2,8,5} & x_{2,8,6} \\ x_{2,9,0} & x_{2,9,1} & x_{2,9,2} & x_{2,9,3} & x_{2,9,4} & x_{2,9,5} & x_{2,9,6} \\ x_{2,10,0} & x_{2,10,1} & x_{2,10,2} & x_{2,10,3} & x_{2,10,4} & x_{2,10,5} & x_{2,10,6} \\ x_{2,11,0} & x_{2,11,1} & x_{2,11,2} & x_{2,11,3} & x_{2,11,4} & x_{2,11,5} & x_{2,11,6} \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \\ b_9 \\ b_{10} \\ b_{11} \end{bmatrix} \quad (2.8)$$

Yeniden yapılandırma aşamasında, 7 katılımcının pay değerleri ele alınır ve yeniden yapılandırma matrisi oluşturulur. Denklik sisteminin çözümü $M^{-1} \times b = a$, (2.9)'da verilen ifadeyle gösterilmiştir.M^{-1}yeniden yapılandırma matrisi, b katılımcıların pay değerleri ve a yeniden yapılan gizli veridir.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & x_{0,1,0} & x_{0,1,1} \\ 0 & 0 & 0 & 0 & 0 & x_{0,2,0} & x_{0,2,1} \\ 0 & 0 & 0 & x_{1,4,1} & x_{1,4,2} & x_{1,4,3} & x_{1,4,4} \\ 0 & 0 & 0 & x_{1,6,1} & x_{1,6,2} & x_{1,6,3} & x_{1,6,4} \\ x_{2,8,0} & x_{2,8,1} & x_{2,8,2} & x_{2,8,3} & x_{2,8,4} & x_{2,8,5} & x_{2,8,6} \\ x_{2,9,0} & x_{2,9,1} & x_{2,9,2} & x_{2,9,3} & x_{2,9,4} & x_{2,9,5} & x_{2,9,6} \\ x_{2,11,0} & x_{2,11,1} & x_{2,11,2} & x_{2,11,3} & x_{2,11,4} & x_{2,11,5} & x_{2,11,6} \end{bmatrix}^{-1} \times \begin{bmatrix} b_1 \\ b_2 \\ b_4 \\ b_6 \\ b_8 \\ b_9 \\ b_{11} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} \quad (2.9)$$

Örnek 2.5: Örnek 2.4'de gizli veri 6 boyutlu uzaydaki noktasının (9,29,242,96,170,137,141), ilk koordinatının değeridir $S = 141$. Dağıtıcı tarafından belirlenen *x* değerleri, çözüm dizisini oluşturur. (2.10)'da verilen denklem sistemini hesaplayarak her katılımcıya bir pay değeri üretilip dağıtılır.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 1 & 3 & 5 & 6 \\ 0 & 0 & 0 & 2 & 4 & 3 & 1 \\ 0 & 0 & 0 & 5 & 2 & 6 & 3 \\ 0 & 0 & 0 & 1 & 3 & 2 & 1 \\ \hline 2 & 3 & 5 & 7 & 2 & 1 & 4 \\ 1 & 5 & 2 & 3 & 6 & 7 & 2 \\ 2 & 3 & 1 & 4 & 5 & 3 & 1 \\ 6 & 5 & 2 & 1 & 3 & 1 & 5 \\ 3 & 2 & 1 & 4 & 1 & 2 & 3 \end{bmatrix} \times \begin{bmatrix} 9 \\ 29 \\ 242 \\ 96 \\ 170 \\ 137 \\ 141 \end{bmatrix} = \begin{bmatrix} 58 \\ 77 \\ 168 \\ 129 \\ 169 \\ 57 \\ 17 \\ 16 \\ 175 \\ 125 \\ 123 \\ 72 \end{bmatrix} \quad (2.10)$$

Yeniden yapılandırmada aşamasında 7 katılımcının pay değerleri hiyerarşik eşik koşulunu sağlayacak şekilde bir araya gelmesi gerekmektedir. Bu durumda eşik değeri (2,4,7) olduğuna göre, birinci seviyeden (58,77), ikinci seviyeden (129,57), üçüncü seviyeden (16,175,123) pay değerleri ele alınır. Gizli veri $S = 141$, (2.11)'de verilen denklem sistemini hesaplayarak elde edilir.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 4 & 2 \\ \hline 0 & 0 & 0 & 1 & 3 & 5 & 6 \\ 0 & 0 & 0 & 5 & 2 & 6 & 3 \\ \hline 2 & 3 & 5 & 7 & 2 & 1 & 4 \\ 1 & 5 & 2 & 3 & 6 & 7 & 2 \\ 6 & 5 & 2 & 1 & 3 & 1 & 5 \end{bmatrix}^{-1} \times \begin{bmatrix} 58 \\ 77 \\ 129 \\ 57 \\ 16 \\ 175 \\ 123 \end{bmatrix} = \begin{bmatrix} 9 \\ 29 \\ 242 \\ 96 \\ 170 \\ 137 \\ 141 \end{bmatrix} \quad (2.11)$$

Ayrıcı hiyerarşik sır paylaşım şemasında alt seviyede olan katılımcılar üst seviyedeki katılımcılar yerine geçebilirler. Bu durumda gizli veri yeniden elde edilmektedir. Bu durum örnek 2.6ve örnek 2.7'de açıklanmıştır.

Örnek 2.6: Örnek 2.5'de yeniden yapılandırma aşamasında, sırrı yeniden elde etmek için herhangi bir m koşulun birisi sağlanması yeterlidir. Örneğin katılan katılımcı sadece en üst seviyeden olursa ve katılımcı sayısı en az o seviyenin eşik değerini sağlarsa gizli veri yeniden elde edilir. Birinci seviyeden katılan katılımcı sayısı o seviyenin eşik

değeri $t_0 = 2$ dir. İki katılımcının pay değerleri (58,77) ele alınır. Gizli veri $S = 141$, (2.12)'de verilen denklem sistemini hesaplayarak elde edilir.

$$\begin{bmatrix} 1 & 3 \\ 4 & 2 \end{bmatrix}^{-1} \times \begin{bmatrix} 58 \\ 77 \end{bmatrix} = \begin{bmatrix} 137 \\ 141 \end{bmatrix} \tag{2.12}$$

Örnek 2.7:. Gizli veriyi elde etmek için katılan katılımcıların hiçbirisi birinci seviyeden değiller. İkinci seviyeden katılan katılımcıların pay değerleri (169,57,17) ve üçüncü seviyenin katılımcılarının pay değerleri (175,125,123,72) olursa, gizli veri $S = 141$, (2.13)'de verilen denklem sistemini hesaplayarak elde edilir.

$$\left[\begin{array}{ccccccc} 0 & 0 & 0 & 2 & 4 & 3 & 1 \\ 0 & 0 & 0 & 5 & 2 & 6 & 3 \\ 0 & 0 & 0 & 1 & 3 & 2 & 1 \\ \hline 1 & 5 & 2 & 3 & 6 & 7 & 2 \\ 2 & 3 & 1 & 4 & 5 & 3 & 1 \\ 6 & 5 & 2 & 1 & 3 & 1 & 5 \\ 3 & 2 & 1 & 4 & 1 & 2 & 3 \end{array}\right]^{-1} \times \begin{bmatrix} 169 \\ 57 \\ 17 \\ 175 \\ 125 \\ 123 \\ 72 \end{bmatrix} = \begin{bmatrix} 8 \\ 29 \\ 242 \\ 96 \\ 170 \\ 137 \\ 141 \end{bmatrix} \tag{2.13}$$

2.1.3. Hiyerarşik Gizli Görüntü Paylaşım Şeması

Bu bölümde tez çalışmasında önerilen birleştirici hiyerarşik sır paylaşım şemasına, birleştirici hiyerarşik gizli görüntü paylaşım şeması önerilmiştir. Önerilen hiyerarşik gizli görüntü paylaşım şemasında, Blakley'nin yöntemi esas olarak kullanılmıştır. (t,n) hiyerarşik sır paylaşım şeması için önerilen gizli görüntü paylaşım şeması iki alt bölümden oluşur.

- Paylaştırma Algoritması: gizli görüntü *n* paya bölünür ve *n* katılımcıya bir pay değeri verilir.
- Yeniden Yapılandırma Algoritması: herhangi *t* katılımcı kendi paylarını bir araya koyarak, gizli görüntü yeniden elde edilir.

Birleştirici hiyerarşik gizli görüntü paylaşım şeması için iki farklı şema önerilmiştir. Birinci şemanın gizli görüntüde ki deneyimleri göz önüne alınarak, ikinci şemanın önerilmesine gerek duyulmuştur. Bu şemalarda gizli veri $N \times M$ boyutlarındaki

dijital bir resimdir. İlerleyen bölümlerde iki şemanın yapılandırması ve farkları detaylıca verilmiştir.

Şema1:$N \times M$ boyutlu gizli görüntü t adet örtüşmeyen pikselden oluşan gruplara parçalanır. Her grup t boyutlu uzaydaki bir noktayı ifade etmektedir. Her seviye için t adet pikselden oluşan noktayı kesen farklı hiper düzlem denklemi kullanarak, n tane pay görüntüsü üretilir. t adet piksel düzlem denkleminin katsayıları olarak belirlenir. Gizli görüntünün parlaklık değerleri gri seviyede olmasından dolayı, tanımlanan hiper düzlem denklem değerinin 251 modül osu alınır. 251 değeri, gri seviyesinde olan görüntünün piksellerin parlaklık aralığındaki [0-255] en büyük asal sayı değeridir. Böylece yeniden yapılandırma aşamasında lineer denklik sisteminin tek çözümü olacaktır. Bu yöntemde pay görüntü boyutları $1/t$ dir. Böylece iletim zamanı ve depolanma gereksinimleri açısından avantaj sağlamaktadır. Ancak bu yöntemde gizli görüntüyü yeniden yapılandırmasında, üst seviyelerden olan katılımcıların pay görüntüleri katılmadığı durumunda, gizli görüntü ile ilgili bazı bilgiler açığa çıkarılır. Böylece önerilen şemanın güvenliği saplanmamış anlama geliyor ve bu durum hassas görüntüler için uygun olmamaktadır. Paylaştırma algoritması aşağıda verilen adımlar halinde verilmiştir.

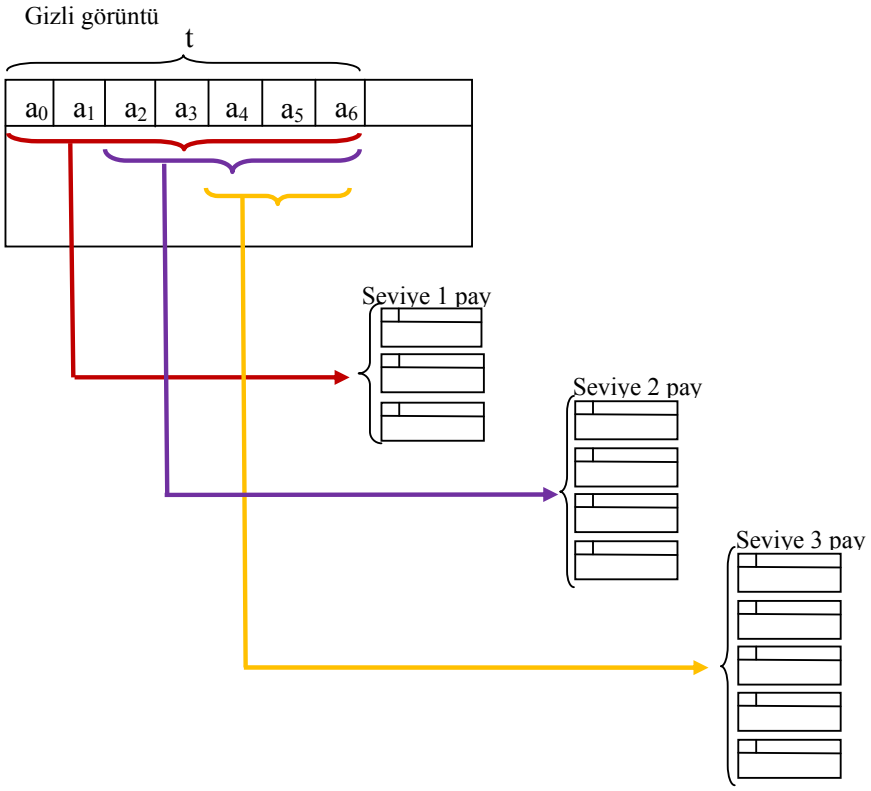
1- Gizli görüntü bir permutasiyon fonksiyonuyla karıştırılır.
2- Her seviye için (2.14)'deki denklem üretilir:

$$P_i(x) = (\sum_{j=t_{i-1}}^{t-1} a_j \, . x)\%251 \;\; , 0 \leq i \leq m \qquad (2.14)$$

m seviyeler sayısıdır.

3- Gizli görüntün t adet örtüşmeyen gruplara parçalanır ve hiperdüzlemin katsayıları olarak $(a_0, a_1, a_2, \dots, a_t)$'ile tanımlanır.
4- Her katılımcı için $x = (x_0, \dots, x_{t_i-1})$ değeri rasgele seçilir ve $s_i = P_i(x_0, \dots, x_{t_i-1})$ pay değerleri hesaplanır.
5- Üzerinde işlem yapılmamış olan pikseller, ardışık alınır ve pay değerleri hesaplanır.

Önerilen birleştirici hiyerarşik gizli görüntü paylaşım şeması şekil 2.2'de gösterilmiştir.



Şekil 2.2. Birleştirici hiyerarşik görüntü paylaşım şeması (şema1)

Şema 2: $N \times M$ boyutlu gizli görüntünün bir piksel değeri alınır ve Shamir'in yöntemini kullanarak t parçaya bölünür. Üretilen t parça t boyutlu uzaydaki bir noktayı ifade etmektedir. Her seviye için üretilen t parçadan oluşan noktayı kesen farklı hiper düzlem denklemi kullanarak, n tane pay görüntüsü üretilir. t adet üretilen parça, düzlem denkleminin katsayıları olarak belirlenir. Bu yöntemde pay görüntü boyutları gizli görüntünün boyutunun aynısıdır. Böylece iletim zamanı ve depolanma miktarı şema 1'e karşılık daha düşüktür. Ancak şema 2'de önerilen yöntem, şema 1'de olan problemin üstesinden gelmiştir. Bu yöntemde gizli görüntüyü yeniden yapılandırmasında, üst seviyelerden olan katılımcıların pay görüntüleri katılmadığı durumunda, gizli görüntü ile ilgili hiçbir bilgi açığa çıkarılmaz ve bu durum hassas görüntüler için uygun olmaktadır. Paylaştırma algoritması aşağıdaki verilen adımlar halinde tanımlanmıştır.

1- Gizli görüntü bir permutasiyon fonksiyonuyla karıştırılır.

2- Her seviye için (2.15)'deki verilen denklem üretilir:

$$P_i(x) = (\sum_{j=t_{i-1}}^{t-1} a_j \, . x)\%251 \;\; , 0 \leq i \leq m \qquad (2.15)$$

m seviyeler sayısıdır.

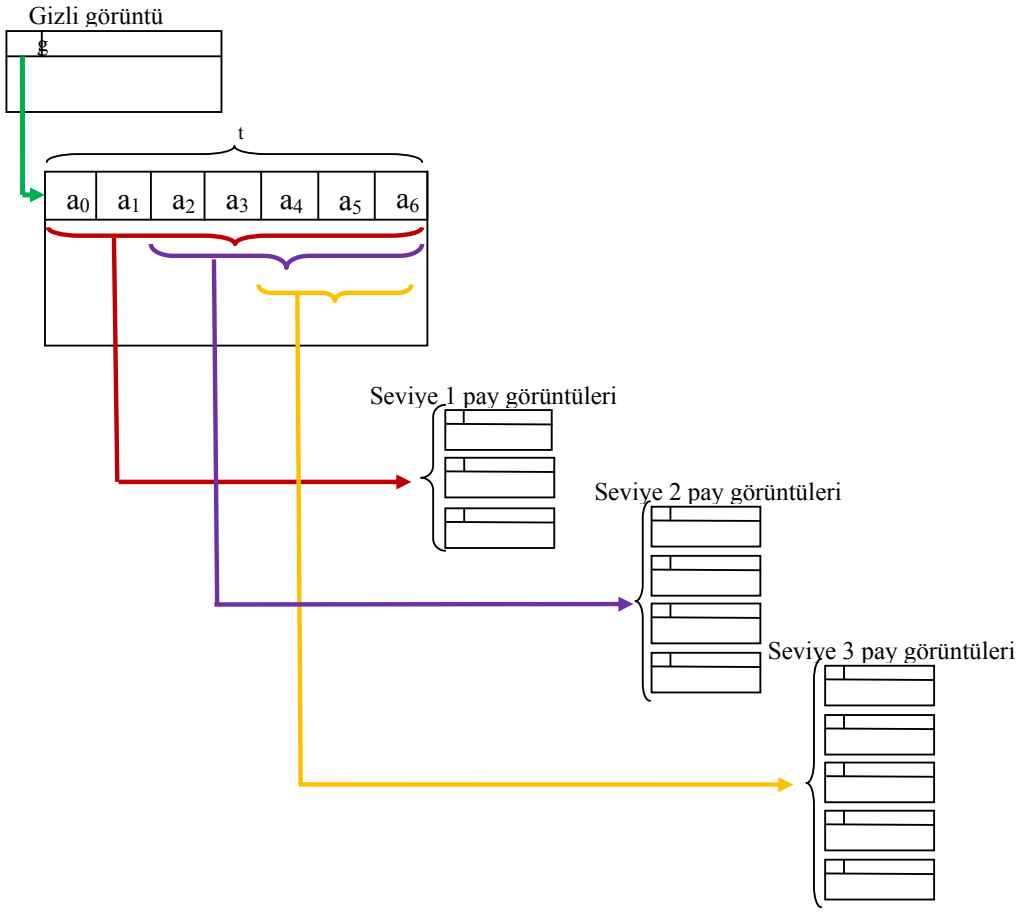
3- Gizli görüntünün her pikseli için aşağıdaki adımlar tekrarlanır.

4- Gizli görüntünün bir piksel değeri S, alınır.

- Shamir'in yöntemini kullanarak, t parçaya $(a_0, a_1, a_2, \dots, a_t)$ bölünür ve (2.14)'deki denklemin katsayıları olarak belirlenir.
- Her katılımcı için $x = (x_0, \dots, x_{t_i-1})$ değeri rasgele seçilir ve (2.14)'deki denklemi kullanarak, $s_i = P_i(x_0, \dots, x_{t_i-1})$ pay değerlerini hesaplanır.

5- Üzerinde işlem yapılmamış olan pikseller, ardışık alınır ve 4deki adımlar uygulanarak pay değerleri hesaplanır.

Şema 2'de önerilen birleştirici hiyerarşik gizli görüntü paylaşım şeması şekil 2.3'de gösterilmiştir.



Şekil 2.3. Birleştirici hiyerarşik görüntü paylaşım şeması (şema 2)

Şema3:Şema 1'de önerilen yöntemde gizli görüntüyü yeniden yapılandırmasında, üst seviyelerden olan katılımcıların katılmadığı durumunda bile, gizli görüntü ile ilgili bazı bilgiler açığa çıkarılır, böylece gizlilik sağlanmamıştır. Bu problemin üstesinden gelmek için bu yöntemde değişiklilik vererek gizlilik özelliği sağlanmıştır. Önerilen şemada her grupta olan piksel değerleri, birinci pikselle XORlanmaktadır. Burada pay boyutu $M \times N/t_m$ kadardır. Paylaştırma algoritması aşağıda verilen adımlar halinde verilmiştir.

1. Gizli görüntü bir permutasiyon fonksiyonuyla karıştırılır.
2. Her seviye için (2.16)'deki denklem üretilir:

$$P_i(x) = (\sum_{j=t_{i-1}}^{t-1} a_j \,.\, x)\%251 \;\; , 0 \le i \le m \qquad (2.16)$$

m seviyeler sayısıdır.

3. Gizli görüntün t adet örtüşmeyen gruplara$(k_0, k_1, k_2, \dots, k_t)$ parçalanır. $a_0 = k_0,\; a_j = k_j \oplus k_0 \;\; , \; 1 \le j \le t-1$, hiper düzlemin katsayıları olarak $(a_0, a_1, a_2, \dots, a_t)$'ile tanımlanır.
4. Her katılımcı için $x = (x_0, \dots, x_{t_i-1})$ değeri rasgele seçilir ve $s_i = P_i(x_0, \dots, x_{t_i-1})$ pay değerleri hesaplanır.
5. Üzerinde işlem yapılmamış olan pikseller, ardışık alınır ve pay değerleri hesaplanır.

Yeniden yapılandırma

Yeniden yapılandırma algoritmasında, t veya daha fazla katılımcının pay değerlerini bir araya gelmesi soncu, gizli görüntü yeniden elde edilir.

Şema 1'de önerilen birleştirici hiyerarşik sır paylaşım şeması, yeniden yapılandırma algoritması adımlar halinde aşağıdaki şekilde verilmiştir.

1- t tane katılımcının pay görüntülerinin ilk piksel değeri $(s_0, s_1, \dots, s_{t-1})$, alınır.

2- Alınan piksel değerleri $(s_0, s_1, \dots, s_{t-1})$, denklem (2.17)'de yerleştirilir ve gizli görüntün ilk grubunun piksel değerleri, $(a_0, a_1, a_2, \dots, a_t)$, hesaplanır. $x = (x_0, \dots, x_{t_i-1})$değerleri dağıtıcı tarafından belirlenmiştir.

$$s_i = P_i\big(x_0, \dots, x_{t_i-1}\big) = (\sum_{j=t_{i-1}}^{t-1} a_j \,.\, x)\%251 \;\; , 0 \le i \le m \qquad (2.17)$$

3- İşlem yapılmamış olan,t katılımcının pay görüntülerinin piksel değerleri ardı ardına alınır ve $(a_0, a_1, a_2, \dots, a_t)$ katsayıları hesaplanır.

4- Permutasiyon fonksiyonunun tersi kullanılarak gizli görüntü elde edilir.

Şema 2'de önerilen hiyerarşik sır paylaşım yöntem için, yeniden yapılandırma algoritması adımlar halinde aşağıdaki şekilde verilmiştir.

1- t tane katılımcının pay görüntülerinin ilk piksel değeri $(s_0, s_1, \dots, s_{t-1})$, alınır.

2- Alınan piksel değerleri $(s_0, s_1, \dots, s_{t-1})$, denklem (2.18)'de yerleştirilir ve gizli görüntün ilk kısmi piksel değerleri, $(a_0, a_1, a_2, \dots, a_t)$, hesaplanır. $x = (x_0, \dots, x_{t_i-1})$değerleri dağıtıcı tarafından belirlenmiştir.

$$s_i = P_i(x_0, \dots, x_{t_i-1}) = (\sum_{j=t_{i-1}}^{t-1} a_j \,.\, x)\%251 \;\; , 0 \le i \le m \qquad (2.18)$$

3- Lagrange interpolasyonu kullanarak gizli görüntünün ilk piksel değerleri, a_0 hesaplanır.

4- İşlem yapılmamış olan, t katılımcının pay görüntülerinin piksel değerleri ardı ardına alınır ve gizli görüntü piksel değerleri hesaplanır.

5- Permutasiyon fonksiyonunun tersi kullanılarak gizli görüntü elde edilir.

Şema 3'de önerilen birleştirici hiyerarşik sır paylaşım şeması, yeniden yapılandırma algoritması adımlar halinde aşağıdaki şekilde verilmiştir.

1- *t* tane katılımcının pay görüntülerinin ilk piksel değeri $(s_0, s_1, \dots, s_{t-1})$, alınır.

2- Alınan piksel değerleri $(s_0, s_1, \dots, s_{t-1})$, denklem (2.19)'da yerleştirilir ve gizli görüntün ilk grubunun piksel değerleri, $(a_0, a_1, a_2, \dots, a_t)$, hesaplanır. $x = (x_0, \dots, x_{t_i-1})$değerleri dağıtıcı tarafından belirlenmiştir.

$$s_i = P_i(x_0, \dots, x_{t_i-1}) = (\sum_{j=t_{i-1}}^{t-1} a_j \,.\, x)\%251 \;\; , 0 \le i \le m \qquad (2.19)$$

3- İşlem yapılmamış olan,t katılımcının pay görüntülerinin piksel değerleri ardı ardına alınır ve $(a_0, a_1, a_2, \dots, a_t)$ katsayıları hesaplanır.

4- $k_0 = a_0,\; k_j = a_j \oplus a_0$, $1 \le j \le t-1$ hesaplayarak, $(k_0, k_1, k_2, \dots, k_t)$ piksel değerleri elde edilir.

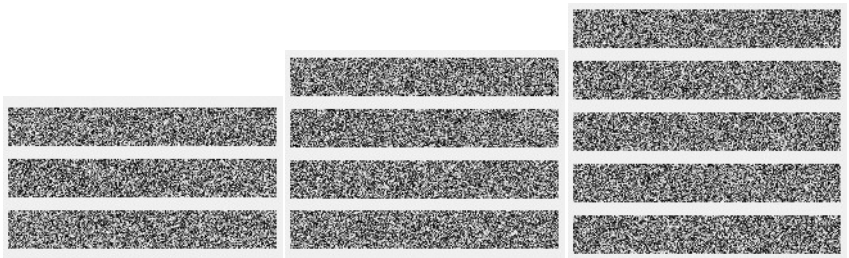
5- Permutasiyon fonksiyonunun tersi kullanılarak gizli görüntü elde edilir.

Önerilen şemalar için yapılan testler ve elde edilen deneysel sonuçlar aşağıda verilmektedir. Deneysel gizli görüntü olarak, 210×210 büyüklüğündeki gri seviye gizli görüntü şekil 2.4'de verilmektedir.

Şekil 2.4. 210×210 büyüklüğündeki gri seviye gizli görüntü

İlk deney olarak örnek 2.1'de tanımlanan hiyerarşik erişim yapısını kullanarak ve şema 1de önerilen paylaştırma algoritmasını uygulayarak belirlenen gizli görüntüyü üç farklı seviyede olan 12 katılımcı arasında paylaştırılmıştır.

Şekil 2.5'de önerilen yöntemin uygulanması sonucu seviyeler için elde edilen pay görüntüleri verilmektedir. Şekil 2.5(a)da birinci seviyenin, şekil 2.5(b)de ikinci seviyenin ve şekil 2.5(c)de üçüncü seviyenin pay görüntüleri gösterilmiştir. Üretilen pay görüntüleri gizli görüntünün $1/7$ kadardır.

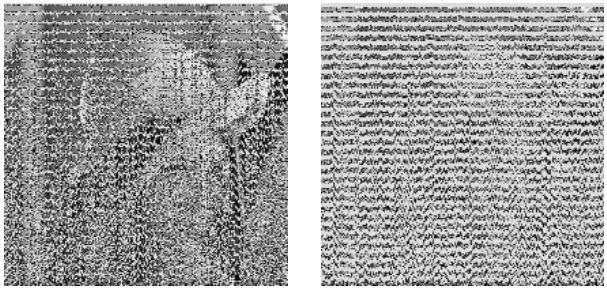


(a) (b) (c)

Şekil 2.5. Üretilen 210×30 pay görüntüleri (a) birinci seviyenin pay görüntüleri (b) ikinci seviyenin pay görüntüleri (c) üçüncü seviyenin pay görüntüleri

Yeniden yapılandırma aşamasında örnek 2.1'de tanımlanan hiyerarşik erişim yapısını sağlayacak şekilde 7 katılımcının pay görüntüleri bir araya gelmesi durumunda gizli görüntü elde edilmektedir. Bu yöntem için elde edilen PSNR değeri sonsuzdur.

Ancak eğer yeniden yapılandırma aşamasında birinci seviyeden hiçbir katılımcı katılmazsa, gizli görüntü kısmi olarak elde edilir. Bu durum Şekil 2.6'de gösterilmiştir. Şekil 2.6(a)'da birinci ve şekil 2.6(b)'da birinci ve ikinci seviyeden katılımcı olamadığı durumu gösterilmektedir.

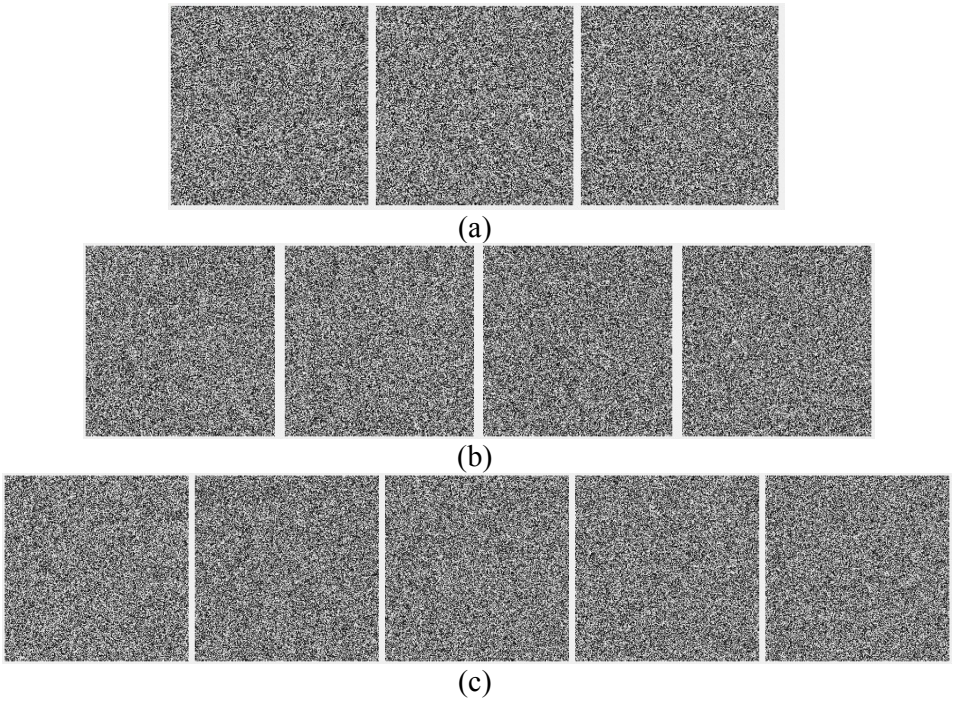


(a) (b)

Şekil 2.6. Yeniden yapılandırılan gizli görüntü (a) birinci seviyeden (b) birinci ve ikinci pay görüntüsü olmadığı durum

Bir başka deney olarak örnek 2.1'de tanımlanan hiyerarşik erişim yapısını kullanarak ve şema 2'de önerilen paylaştırma algoritmasını uygulayarak belirlenen gizli görüntüyü üç farklı seviyede olan 12 katılımcı arasında paylaştırılmıştır.

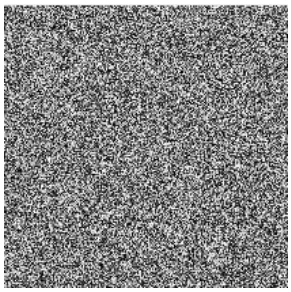
Şekil 2.7'da önerilen yöntemin uygulanması sonucu seviyeler için elde edilen pay görüntüleri verilmektedir. Şekil 2.7(a)'da birinci seviyenin, şekil 2.7(b)'de ikinci seviyenin ve şekil 2.7(c)'de üçüncü seviyenin pay görüntüleri gösterilmiştir. Üretilen pay görüntüleri gizli görüntüyle aynı büyüklüktedir.



Şekil 2.7. Üretilen 210×210 pay görüntüleri (a) birinci seviyenin (b) ikinci seviyenin (c) üçüncü seviyenin pay görüntüleri

Yeniden yapılandırma aşamasında örnek 2.1'de tanımlanan hiyerarşik erişim yapısını sağlayacak şekilde 7 katılımcının pay görüntüleri bir araya gelmesi durumunda gizli görüntü kayıpsız olarak elde edilmektedir.

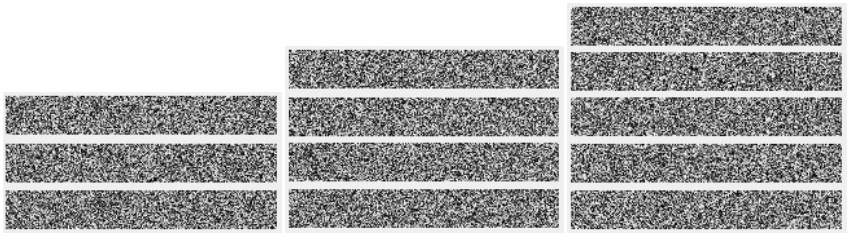
Bu şemada eğer yeniden yapılandırma aşamasında birinci seviyeden hiçbir katılımcı katılmazsa, gizli görüntü yeniden elde edilmemektedir. Bu durum Şekil 2.8'de gösterilmiştir.



Şekil 2.8. Birinci seviyeden pay görüntüsü olmadığı durumunda yeniden yapılandırılan gizli görüntü

Şema 3'de önerilen yöntem incelenmiştir. Örnek 2.1'de tanımlanan hiyerarşik erişim yapısını kullanarak ve şema 3'de önerilen paylaştırma algoritmasını uygulayarak belirlenen gizli görüntüyü üç farklı seviyede olan 12 katılımcı arasında paylaştırılmıştır.

Şekil 2.9'de önerilen yöntemin uygulanması sonucu seviyeler için elde edilen pay görüntüleri verilmektedir. Şekil 2.9(a)da birinci seviyenin, şekil 2.9(b)de ikinci seviyenin ve şekil 2.9(c)de üçüncü seviyenin pay görüntüleri gösterilmiştir. Üretilen pay görüntüleri gizli görüntünün $1/7$ kadardır olması, şema 1'de verilen yöntemin aynı boyutunda olduğu gözlemlenmiştir.



(a) (b) (c)

Şekil 2.9. Üretilen210×30 pay görüntüleri (a) birinci seviyenin (b) ikinci seviyenin (c) üçüncü seviyenin pay görüntüleri

Yeniden yapılandırma aşamasında örnek 2.1'de tanımlanan hiyerarşik erişim yapısını sağlayacak şekilde 7 katılımcının pay görüntüleri bir araya gelmesi durumunda gizli görüntü kayıpsız olarak elde edilmektedir. Bu şemada eğer yeniden yapılandırma aşamasında birinci seviyeden hiçbir katılımcı katılmazsa, gizli görüntü yeniden elde edilmemektedir ve şemanın güvenliği sağlanmıştır.

Tablo 2.1'de önerilen şemaların ve diğer yöntemlerin kıyaslanması gösterilmiştir. Tablodan da gözlenebileceği gibi, tez çalışmasındaki önerilen yöntemlerde hiyerarşik düzeni sağlanmıştır. Önerilen şema 1de pay boyutunun $1/t$ kadar küçük olduğu zaman, hiyerarşik eşik koşulu sağlanmadı durumda görüntü ile ilgili bilgi açığa çıkarılmaktadır ancak şema 2de pay görüntülerin gizli görüntüyle aynı boyutta olduğu durumda, bu problem giderilmiştir. Şema 3'de bir başka yöntem kullanarak hem pay boyutun küçültülmüştür ve hem gizlilik sağlanmıştır.

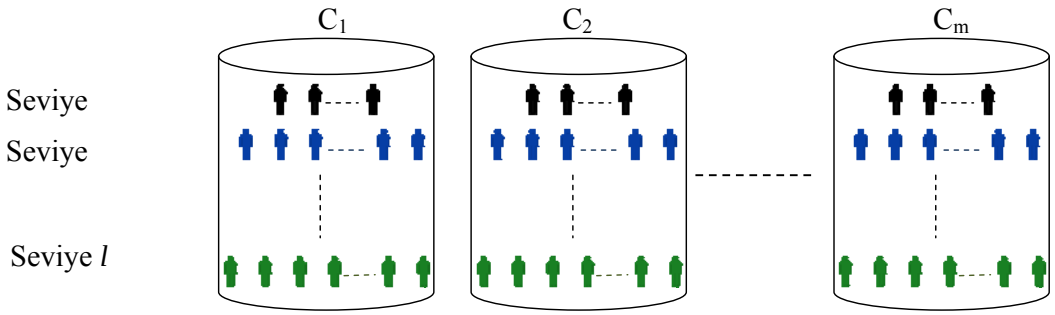
Tablo 2.1. Önerilenyöntem ve diğer yöntemlerin karşılaştırılması

	Tso[38]	Chen[37]	Ulutaş[39]	Guo[40]	Guo (katsayıları değiştirerek)	Önerilen yöntem (şema1)	Önerilen yöntem (şema2)	Önerilen yöntem (şema3)
Hiyerarşik Yapı	Hayır	Hayır	Hayır	Evet	Evet	Evet	Evet	Evet
Kayıpsız Gizli Görüntü	Hayır	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Gizlilik Özelliğinin Sağlanması	Evet	Evet	Evet	Hayır	Evet	Hayır	Evet	Evet
Pay Boyutu	$\frac{M \times N}{t}$	$M \times N$	$\frac{M \times N}{t}$	$\frac{M \times N}{t_m}$	$\frac{M \times N}{t_0}$	$\frac{M \times N}{t_m}$	$M \times N$	$\frac{M \times N}{t_m}$

2.2. İç İçe Bölütlenmiş Erişim Yapısı

Çok parçalı erişim yapılardan birisi bölütlenmiş erişim yapısıdır. Bu yapıda katılımcılar ayrık bölümlere ayrılır ve her bir bölümde olan katılımcılar aynı rolü vardır ve her bölüm için bir eşik miktarı tanımlanmıştır. Tanımlanan genel eşik miktarı bölümlerden katılan katılımcının toplam sayısını gösterir. Her bir bölümden katılan katılımcı sayısı, bölümün sabit eşik miktarından büyük olsa ve katılımcıların toplam sayısı genel eşik miktarından büyük olursa, gizli veri yeniden elde edilebilmektedir.

Ancak gerçek hayatta bazı durumlarda her bölümde olan katılımcılar, aynı seviyede olmayabilirler. Örnek olarak, bir nükleer bombanın ateşlenmesi için üç kurumun bir araya gelmesi gerekir, her kurumun katılımcıları kendi kurumunda aynı seviyeden olmaya bilirler. Böylece ateşleme onayı vermek için her kurumdan katılan katılımcı sayısı hiyerarşik erişim yapısına uygun olması gerekmektedir ve üç kurumun bir araya gelmesi gerekir. Tanımlanmış olduğumuz iç içe bölütlenmiş erişim yapısında, her bölümde olan katılımcılar hiyerarşik seviyelere ayrılmıştır. İçerikli bölütlenmiş erişim yapısı, tanım 2.10'da verilmektedir. Şekil 2.10'da önerilen iç içe bölütlenmiş erişim yapısı gösterilmiştir.



Şekil 2.10. İç içe bölütlenmiş erişim yapısı

Tanımlama 2.1: $C = \{C_1, C_2, \dots, C_m\}$, n katılımcının bölümleridir. Bölümlerin eşik miktarı sırasıyla $T = \{t_1, t_2, \dots, t_m\}, 1 \le t_i \le |C_i|, 1 \le i \le m$, $C_i \cap C_j = \emptyset$, $1 \le i < j \le m$ ve genel eşik miktarı $\sum_{i=1}^{m} t_i \le t \le n$ olsun. Her C_i bölümünde olan katılımcılar kümesi, l seviyeden oluşsun, yani $C_i = \cup_{j=0}^{l} U_{i,j}$ ve $U_{i,j} \cap U_{i,j+1} = \emptyset$, $0 \le j \le l$, $1 \le i \le m$. $\mathrm{k} = \{k_{i,j}\}_{j=0}^{l}$ her bölümde ki olan seviyeler için, monoton yükselen eşik değerler sırası olsun, $0 < k_0 < \cdots < k_l$ ve $t_i = k_{i,l}$ dir. İçerikli bölütlenmiş erişim yapısı aşağıda verilen ifadeyle tanımlanır.

$$\Gamma = \left\{ \mathrm{A} \subseteq \mathcal{C} \mid \left\{ \left| A \cap (\cup_{z=1}^{j} U_{i,z}) \right| \ge k_{i,j}, \forall j \in \{1, \dots, l\} \right\} \forall\, i \in \{1, \dots, m\} \right\} \quad ve\ |A| \ge t \qquad (2.20)$$

2.2.1. İç İçe Bölütlenmiş Sır Paylaşım Şeması

Tanım 2.1'de verilen erişim yapısı için ideal sır paylaşım şeması adımlar halinde aşağıdaki şekilde önerilmiştir:

1. $m - 1$ tane rastgele $c_1, \dots, c_{m-1} \in GF(q)$ değeri seçilir ve

$$g(x) = G + c_1 x + \cdots + c_{m-1} x^{m-1} \qquad (2.21)$$

polinomunu tanımlanır. $G = g(0)$ sır değeri ve $g_i = g(x_i), i = 1, \dots, m$ her bölüm için üretilen kısmi sır miktarıdır.

2. Her bölüme karşılıklı düşen, $t_i - 1$ tane $a_{i,1}, \dots, a_{i,t_i-1}$ miktarları rastgele seçilir ve m tane $f_i(x) = g_i + \sum_{j=1}^{t_i-1} a_{i,j}x^j$, $i = 1, \dots, m$, polinomu oluşturulur.

3. $\sum_{i=1}^{m} t_i \leq t$ den dolayı, $R = t - \sum_{i=1}^{m} t_i$. Böylece R tane $b_0, \dots, b_{R-1}$ rastgele değerler seçilir ve $f(y) = \sum_{i=t_i}^{t_i+R-1} b_{i-t_i}y^i$polinomunu tanımlanır.

4. Her bölüm için $f_{i,j}(x, y) = (f_i(x))^{k_{j-1}} + f(y)$, $i = 1, \dots, m$ ve $j = 0, \dots, l$ polinomu üretilir ($k_{-1} = 0$). ($f(x) = k_i + \sum_{j=1}^{t_i-1} a_{i,j}x^j$ polinomial'ın türevi, $f'(x) = \sum_{j=1}^{t_i-1} j a_{i,j}x^{j-1}$ olarak belirlenir).

5. her bir katılımcıya $u_{i,j,z} \in U_{i,j} \in C_i$, $1 \leq z \leq n_i$ (n_i her bölüm için katılımcı sayısıdır) için bir $(x_{i,j_z}, y_{i,j_z}) \neq 0$ değeri verilir. iki farklı katılımcı aynı (x_{i,j_z},y_{i,j_z}) miktarını alamaz. Her katılımcının pay değeri, $f_{i,j}(x_{i,j_z}, y_{i,j_z})$ ye eşittir.

Teorem 2.1: tanım 2.1'de ki bölütlenmiş erişim yapısı için önerilen sır paylaşım şeması mükemmel ve idealdir. Sadece $A \in \Gamma$gizli veriyi yeniden elde edebilir.

İspat: Eğer $A \in \Gamma$ olsa, o zaman *A*'daki olan katılımcılar *S* sırını yeniden elde edebilirler. Belirlemeliyiz ki *S* sırını yeniden elde etmek için, her bölüm kendine bağlı s_i kısmi sırrı, yeniden elde etmesi gerekir. Her bölümden en az t_i katılımcının katılması gerekmektedir. katılan olan katılımcıların sayısı $n_1, \dots, n_m$ olsun ve$n_i \geq t_i$ ve $\sum_{i=1}^{m} n_i \geq t$. Her bölümden katılan olan n_i sayıda katılımcının, $n_i \cap (\bigcup_{z=1}^{j} U_{i,z}) \geq k_j$ koşulunu sağlaması gerekmektedir. Yani $A = \bigcup_{i=1}^{m} C_i$ katılımcıların yetkili altkümesidir, eğer $|A| = t$, $|A \cap C_i| \geq t_i$, $i \in \{1, \dots, m\}$ ve $C_i \cap (\bigcup_{z=1}^{j} U_{i,z}) \geq k_j$, $j = 0, \dots, l$. *A* da olan tüm katılımcıların payları bir araya gelerek sırrı yeniden elde etmekleri için, bir lineer sistemin çözülmesi gerekir. Kurulan lineer denklemler sisteminde, denklemlerin sayısı en az bilinmeyenlerin sayısı kadardır yani her bölümle ilgili t_i sayıda bilinmeyen g_i , $a_{i,j}$ katsayılar vardır ve R sayıda da bilinmeyen b_i vardır ki tüm denklemlerde ortaktır. Bu denklemler lineer bağımsızlar(yani her katılımcıya verilen katsayı değerleri bir matrisin satırlarını oluşturur ve aynı olamadıklarından dolayı hiçbir satır diğer satırla veya sütünler birleştirmesi olarak olmamaktadırlar) böylece yeniden yapılandırma matrisinin determinantı sıfır olamaz. Böylece Sistemin tek bir çözümü vardır çünkü en az *t* denklem ve *t* bilinmeyen vardır. k_ikısmi sırrı elde ettikten sonra, K sırrı elde edilmektedir. Böylece sırra ulaşabilme sağlanmıştır.

Eğer katılımcılar kümesi *A*, yetkisiz ise $A \notin \Gamma$, *A* nın katılımcıları, lineer sisteminin bilinmeyen katsayılarını çözme esnasında, bazı sayıda denklem kaybıyla

karşılaşır. Farz edelim $A \notin \Gamma$ değil. O halde iki olasılık vardır. İlk olasılık, bir i bölümü vardır ki $\alpha_i < t_i$ dır . Bu durumda k_i kısmi sır bulunamaz. İkinci olasılık, tüm $\alpha_i \geq t_i$ ama $\sum_{i1}^{l} \alpha_i < t$ dir. Boylece $b_1, \ldots, b_R$ için tek çözüm vardır. Böylece yetkisiz altküme, gizli bilgiyle alakalı hiçi bir bilgiye erişemez. Böylece gizlilik sağlanmıştır.

Sırra ulaşabilme ve sırrın gizliliği sağlandığından dolayı önerilen sır paylaşım şeması mükemmeldir. Katılımcılara verilen pay değeri, sır değerinin alanına eşit olduğundan dolayı, bilgi oranı bire eşittir. Mükemmellik özelliğin sağlanması ve bilgi oranın bire eşit olmasından dolayı önerilen sır paylaşım şeması idealdir.

Örnek 2.8: İki kurumun var olduğu farz edilir ve eşik değerleri her kurum için sırasıyla $t_1 = 4, t_2 = 5,\ t = 10$ olsun. Birinci kurum iki seviyeden oluşur ve her seviyeler için eşik değerler sırasıyla $k = \left(k_{1,1}, k_{1,2}\right) = (1,4)$ ve ikinci kurum ise üç seviyeden oluşmaktadır ve eşik değerleri sırasıyla $k = \left(k_{2,1}, k_{2,2}, k_{2,3}\right) = (1,3,5)$ olsun. Bu durumda, A yetkili küme olmak için en az 10 katılımcının katılması gerekir ayrıca bu 10 katılımcının en az dört katılımcısı birinci kurumdan ve beş katılımcısı ikinci kurumdan olması gerekir. Ancak her kurumun katılımcıları hiyerarşik olduğundan dolayı, birinci kurumdan katılın dört katılımcının en az 1'i en üst seviyeden yani $U_{1,1}$'den ve en az dört katılımcıda $U_{1,1} \cup U_{1,2}$'den olması gerekmektedir. İkinci kurumdan ise beş katılımcının, en az 1 katılımcı $U_{1,1}$'den, 3 katılımcı $U_{1,1} \cup U_{1,2}$ ve 5 katılımcı da $U_{1,1} \cup U_{1,2} \cup U_{1,3}$'den olması gerekmektedir. $R = t - \sum_{i=1}^{m} t_i = 10 - 9 = 1$olduğundan dolayı en az bir katılımcıda herhangi bir kurumdan olabilir.

Örnek 2.9: Önerilen sır paylaşım yöntemi, örnek 2.8'de verilen erişim yapısı için uygulanması yapılandırmaktadır. 15 katılımcı olduğu farz edilir, 6 katılımcı birinci kuruma ve 9 katılımcı ise ikinci kuruma ait olsun. Gizli veri $G = 23$, GF(29) alanında bir değer olsun. İlk adımda her kurum için kısmi sır değerlerini üretilir bunun için denklem 2.2.2'yi kullanarak $g = g(x), i = 1, \ldots, m$ oluşturulur, iki kurum $m = 2$ olduğu için :

$g(x) = G + c_1 x$, ve $c_1 = 13, x_1 = 2$ ve$x_2 = 5$ olsun.

$g_1 = g(x_1) = (23 + 13 \times 2) mod\ 29 = 20$

$g_2 = g(x_2) = (23 + 13 \times 5) mod\ 29 = 1$

Birinci kurum için $t_1 - 1 = 4 - 1 = 3$ tane, $a_{1,1} = 11, a_{1,2} = 21, a_{1,3} = 18$ rasgele değer seçilir ve üç dereceden olan polinom üretilir:

$$f_1(x) = g + \sum_{j=1}^{t_1-1} a_{1,j}x^j = g_1 + \sum_{j=1}^{3} a_{1,j}x^j = 20 + a_{1,1}x + a_{1,2}x^2 + a_{1,3}x^3$$
$$= 20 + 11x + 21x^2 + 18x^3$$

İkinci kurum için $t_2 - 1 = 5 - 1 = 4$ tane$a_{2,1} = 9, a_{2,2} = 6, a_{2,3} = 25, a_{2,3} = 14$ rastgele değer seçilir ve dorumcu dereceden olan polinom seçilir:

$$f_2(x) = s_2 + \sum_{j=1}^{t_2-1} a_{2,j}x^j = s_2 + \sum_{j=1}^{4} a_{2,j}x^j$$
$$= 1 + a_{2,1}x + a_{2,2}x^2 + a_{2,3}x^3 + a_{2,4}x^4$$
$$= 1 + 9x + 6x^2 + 25x^3 + 14x^4$$

$\sum_{i=1}^{2} t_i \leq t, 9 \leq 10$den dolayı $R = t - \sum_{i=1}^{2} t_i = 10 - 9 = 1$ dir, boylece 1 tane $b_0 = 17$ rasgele değer seçilir ve her bölüm için aşağıda verilen polinomlar üretilir:

$$f_1(y) = \sum_{i=t_1}^{t_1+R-1} b_{i-t_1}y^i = \sum_{t=4}^{4+1-1} b_{4-4}y^4 = b_0y^4 = 17y^4$$
$$f_2(y) = \sum_{i=t_2}^{t_2+R-1} b_{i-t_2}y^i = \sum_{t=5}^{5+1-1} b_{5-5}y^5 = b_0y^5 = 17y^5$$

Her bölümün seviyeleri için üretilen polinomu aşağıda verilmiştir:

$$f_{i,j}(x, y) = (f_i(x))^{k_{j-1}} + f_i(y), j = 0, \dots, l$$

Birinci bölümün seviyelerine verilen polinom, aşağıda verilen ifadelerle tanımlanmıştır:

Birinci bölümün en üst seviyesi $j = 0$ için:

$$f_{1,0}(x, y) = (f_1(x))^{k_{0-1}} + f_1(y) = f_1(x) + f_1(y) = 20 + 11x + 21x^2 + 18x^3 + 17y^4$$

Birinci bölümün ikinci seviyesi $j = 1$ için:

$$f_{1,1}(x,y) = (f_1(x))^{k_{1-1}} + f_1(y) = \left(f_1(x)\right)^{k_0} + f_1(y) = \left(f_1(x)\right)' + f_1(y)$$
$$= 11 + 42x + 54x^2 + 17y^4$$

İkinci bölümün en üst seviyesi $j = 0$ için

$$f_{2,0}(x,y) = (f_2(x))^{k_{0-1}} + f_2(y) = f_2(x) + f_2(y)$$
$$= 1 + 9x + 6x^2 + 25x^3 + 14x^4 + 17y^5$$

İkinci bölümün ikinci seviyesi $j = 1$ için

$$f_{2,1}(x,y) = (f_2(x))^{k_{1-1}} + f_2(y) = \left(f_2(x)\right)^{k_0=1} + 2(y) = \left(f_2(x)\right)' + f_2(y)$$
$$= 9 + 12x + 75x^2 + 56x^3 + 17y^5$$

İkinci bölümün üçüncü seviyesi $j = 2$ için

$$f_{2,2}(x,y) = (f_2(x))^{k_{2-1}} + f_2(y) = \left(f_2(x)\right)^{k_1=3} + f_2(y) = \left(f_2(x)\right)''' + f_2(y)$$
$$= 150 + 336x + 17y^5$$

Her bir bölümün katılımcılarına, (x_{i,j_z}, y_{i,j_z}) değeri verilir ve $s_{i,j_z} = f_{i,j}\left(x_{i,j_z}, y_{i,j_z}\right),\ z = 1, \dots, n_i (n_i$katılımcı sayısıdır) ve $i = 1, \dots, m$, $j = 0, \dots, l$, pay miktarı üretilir ($n_1 = 6$ ve $n_2 = 9$).

Örneğin Birinci kurumun birinci seviyesinin birinci katılımcısına verilen pay değeri:

$$s_{1,0_1} = f_{1,0}\left(x_{1,0_1}, y_{1,0_1}\right) = f_{1,0}\left(x_{1,0_1}, y_{1,0_1}\right)$$

Önerilen yapıya göre aşağıda verilen lineer sistem üretilir ve Katılımcılara (x_{i,j_z}, y_{i,j_z}) değerleri genel olarak verilir. Her bir katılımcıya tanımlanan (x_{i,j_z}, y_{i,j_z}) değerini lineer sitemde yerleştirerek, pay miktarları hesaplanır ve sonra katılımcılar arasında dağıtılır:

$$\left(x_{1,0_1}, y_{1,0_1}\right) = (1,1), \left(x_{1,0_2}, y_{1,0_2}\right) = (2,2), (x_{1,1_3}, y_{1,1_3}) = (3,3), \left(x_{1,1_4}, y_{1,1_4}\right) = (4,4),$$
$$\left(x_{1,1_5}, y_{1,1_5}\right) = (5,5), (x_{1,1_6}, y_{1,1_6}) = (6,6)$$

İkinci kurumun katılımcıları için:

$$\left(x_{2,0_1}, y_{2,0_1}\right) = (3,3), (x_{2,0_2}, y_{2,0_2}) = (1,1), (x_{2,0_3}, y_{2,0_3}) = (5,5),$$
$$\left(x_{2,1_4}, y_{2,1_4}\right) = (2,2), (x_{2,1_5}, y_{2,1_5}) = (4,4), (x_{2,1_6}, y_{2,1_6}) = (3,3),$$
$$\left(x_{2,2_7}, y_{2,2_7}\right) = (1,1), \left(x_{2,2_8}, y_{2,2_8}\right) = (2,2), (x_{2,2_9}, y_{2,2_9}) = (3,3)$$

$$\begin{bmatrix}
1 & x_{1,0_1} & x_{1,0_1}^2 & x_{1,0_1}^3 & 0 & 0 & 0 & 0 & 0 & y_{1,0_1}^4 \\
1 & x_{1,0_2} & x_{1,0_2}^2 & x_{1,0_2}^3 & 0 & 0 & 0 & 0 & 0 & y_{1,0_2}^4 \\
\hline
0 & 1 & x_{1,1_3} & x_{1,1_3}^2 & 0 & 0 & 0 & 0 & 0 & y_{1,1_3}^4 \\
0 & 1 & x_{1,1_4} & x_{1,1_4}^2 & 0 & 0 & 0 & 0 & 0 & y_{1,1_4}^4 \\
0 & 1 & x_{1,1_5} & x_{1,1_5}^2 & 0 & 0 & 0 & 0 & 0 & y_{1,1_5}^4 \\
0 & 1 & x_{1,1_6} & x_{1,1_6}^2 & 0 & 0 & 0 & 0 & 0 & y_{1,1_6}^4 \\
\hline
0 & 0 & 0 & 0 & 1 & x_{2,0_1} & x_{2,0_1}^2 & x_{2,0_1}^3 & x_{2,0_1}^4 & y_{2,0_1}^5 \\
0 & 0 & 0 & 0 & 1 & x_{2,0_2} & x_{2,0_2}^2 & x_{2,0_2}^3 & x_{2,0_2}^4 & y_{2,0_2}^5 \\
0 & 0 & 0 & 0 & 1 & x_{2,0_3} & x_{2,0_3}^2 & x_{2,0_3}^3 & x_{2,0_3}^4 & y_{2,0_3}^5 \\
\hline
0 & 0 & 0 & 0 & 0 & 1 & x_{2,1_4} & x_{2,1_4}^2 & x_{2,1_4}^3 & y_{2,1_4}^5 \\
0 & 0 & 0 & 0 & 0 & 1 & x_{2,1_5} & x_{2,1_5}^2 & x_{2,1_5}^3 & y_{2,1_5}^5 \\
0 & 0 & 0 & 0 & 0 & 1 & x_{2,1_6} & x_{2,1_6}^2 & x_{2,1_6}^3 & y_{2,1_6}^5 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_{2,2_7} & y_{2,2_7} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_{2,2_8} & y_{2,2_8} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_{2,2_9} & y_{2,2_9}
\end{bmatrix} \times \begin{bmatrix} g_1 \\ a_{1,1} \\ a_{1,2} \\ a_{1,3} \\ g_2 \\ a_{2,1} \\ a_{2,2} \\ a_{2,3} \\ a_{2,4} \\ b_0 \end{bmatrix} = \begin{bmatrix} s_{1,0_1} \\ s_{1,0_2} \\ s_{1,1_3} \\ s_{1,1_4} \\ s_{1,1_5} \\ s_{1,1_6} \\ s_{2,0_1} \\ s_{2,0_2} \\ s_{2,0_3} \\ s_{2,1_4} \\ s_{2,1_5} \\ s_{2,1_6} \\ s_{2,2_7} \\ s_{2,2_8} \\ s_{2,2_9} \end{bmatrix}$$

Her katılımcıya verilen (x_{i,j_z}, y_{i,j_z}) değeri yukardaki matrise yerleştirirlir ve pay miktarları uretilir:

$$\left[\begin{array}{cccccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 2 & 4 & 8 & 0 & 0 & 0 & 0 & 0 & 16 \\
\hline
0 & 1 & 3 & 9 & 0 & 0 & 0 & 0 & 0 & 81 \\
0 & 1 & 4 & 16 & 0 & 0 & 0 & 0 & 0 & 256 \\
0 & 1 & 5 & 25 & 0 & 0 & 0 & 0 & 0 & 625 \\
0 & 1 & 6 & 36 & 0 & 0 & 0 & 0 & 0 & 1296 \\
\hline
0 & 0 & 0 & 0 & 1 & 3 & 9 & 27 & 81 & 243 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 5 & 25 & 125 & 625 & 3125 \\
\hline
0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 8 & 32 \\
0 & 0 & 0 & 0 & 0 & 1 & 4 & 16 & 64 & 1024 \\
0 & 0 & 0 & 0 & 0 & 1 & 3 & 9 & 27 & 243 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 32 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 243
\end{array}\right] \times \left[\begin{array}{c} 20 \\ 11 \\ 21 \\ 18 \\ 1 \\ 9 \\ 6 \\ 25 \\ 14 \\ 17 \end{array}\right] = \left[\begin{array}{c} 0 \\ 20 \\ 18 \\ 8 \\ 26 \\ 23 \\ 19 \\ 14 \\ 4 \\ 23 \\ 3 \\ 5 \\ 27 \\ 17 \\ 22 \end{array}\right]$$

Yeniden yapılandırma aşamasında en az 10 katılımcının pay miktarları bir araya gelmesi gerekmektedir. Fakat bu 10 katılımcının örnek 2.1'de verilen erişim yapısını sağlaması gerekir. $R = 1$olduğuna göre bir katılımcı birinci bölümün birinci seviyesinden olduğu farz edilir. Yeniden yapılandırma matrisi, M_A ,üretilir:

$$\left[\begin{array}{cccccccccc}
1 & x_{1,0_2} & {x_{1,0_2}}^2 & {x_{1,0_2}}^3 & 0 & 0 & 0 & 0 & 0 & {y_{1,0_2}}^4 \\
\hline
0 & 1 & x_{1,1_3} & {x_{1,1_3}}^2 & 0 & 0 & 0 & 0 & 0 & {y_{1,1_3}}^4 \\
0 & 1 & x_{1,1_5} & {x_{1,1_5}}^2 & 0 & 0 & 0 & 0 & 0 & {y_{1,1_5}}^4 \\
0 & 1 & x_{1,1_6} & {x_{1,1_6}}^2 & 0 & 0 & 0 & 0 & 0 & {y_{1,1_6}}^4 \\
\hline
0 & 0 & 0 & 0 & 1 & x_{2,0_2} & {x_{2,0_2}}^2 & {x_{2,0_2}}^3 & {x_{2,0_2}}^4 & {y_{2,0_2}}^5 \\
0 & 0 & 0 & 0 & 1 & x_{2,0_3} & {x_{2,0_3}}^2 & {x_{2,0_3}}^3 & {x_{2,0_3}}^4 & {y_{2,0_3}}^5 \\
\hline
0 & 0 & 0 & 0 & 0 & 1 & x_{2,1_5} & {x_{2,1_5}}^2 & {x_{2,1_5}}^3 & {y_{2,1_5}}^5 \\
0 & 0 & 0 & 0 & 0 & 1 & x_{2,1_6} & {x_{2,1_6}}^2 & {x_{2,1_6}}^3 & {y_{2,1_6}}^5 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_{2,2_7} & y_{2,2_7} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x_{2,2_9} & y_{2,2_9}
\end{array}\right]$$

Katılan katılımcıların pay miktarlarını ele alınır. Aşağıda verilen lineer denklem çözülür. Kısmi gizli veriler elde ettikten sonra denklem 2.2.2'yi kullanarak gizli veri elde edilir.

$$\left[\begin{array}{cccccccccc} 1 & 2 & 4 & 8 & 0 & 0 & 0 & 0 & 0 & 16 \\ \hline 0 & 1 & 3 & 9 & 0 & 0 & 0 & 0 & 0 & 81 \\ 0 & 1 & 5 & 25 & 0 & 0 & 0 & 0 & 0 & 625 \\ 0 & 1 & 6 & 36 & 0 & 0 & 0 & 0 & 0 & 1296 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 5 & 25 & 125 & 625 & 3125 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 4 & 16 & 64 & 1024 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 & 9 & 27 & 243 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 243 \end{array}\right]^{-1} \times \left[\begin{array}{c} 20 \\ 18 \\ 26 \\ 23 \\ 14 \\ 4 \\ 3 \\ 5 \\ 27 \\ 22 \end{array}\right] = \left[\begin{array}{c} 20 \\ 11 \\ 21 \\ 18 \\ 1 \\ 9 \\ 6 \\ 25 \\ 14 \\ 17 \end{array}\right]$$

Elde edilen kısmi sır miktarlarını, $g_1 = 20$ ve$g_2 = 1$, kullanarak, aşağıda verilen lineer denklem çözülür ve sır miktarı elde edilir.

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix}^{-1} \times \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 23 \\ 13 \end{bmatrix}$$

2.2.2. İç İçe Bölütlenmiş Gizli Görüntü Paylaşım Şeması

Sır paylaşım şeması birçok uygulamalarda yapılmıştır, bunların birisi gizli görüntünün gizliliğini sağlamaktır. Önermiş olduğumuz iç içe bölütlenmiş sır paylaşım şeması, gizli görüntü paylaşımı üzerinden örneklendirilir.

Önerilen gizli görüntü paylaşım şeması iki alt bölümden oluşur:

- Paylaştırma algoritması: Gizli görüntü *n* paya bölünür ve her bir katılımcıya bir pay değeri verilir.
- Yeniden yapılandırma algoritması: Tanımlanan erişim yapısına uygun katılımcılar paylarını bir araya koyarak, gizli görüntü yeniden elde edilir.

Tanımlanan iç içe bölütlenmiş erişim yapısı göz önüne alınmaktadır. Gizli görüntü paylaştırma algoritması adımlar halinde aşağıda verilen biçimdedir:

G gizli görüntü ve *n* katılımcı sayısı olsun. Paylaştırma algoritmasını kullanarak *n* tane pay görüntüsü elde edilmektedir.

Adım1. Gizli görüntünün ilk piksel değeri, *G*, alınır. Her bir piksel için 1-1 den 1-3 deki adımlar yapılır:

1-1 $m + R - 1$ sayıda $c_1, \dots c_{m+R-1}$değer seçilir ve aşağıda verile denklemi kullanarak her bölüm için, kısmi sır miktarlarını üretilir:

$$g(x) = G + c_1 x + \cdots + c_{m+R-1} x^{m+R-1}$$

m bölümler sayısı ve $R = t - \sum_{i=1}^{m} t_i$dır.

1-2 Her bölüm için x_i miktarı verilir. Üretilen kısmi sır miktarı, $g_i(x_i) = g(x_i)$ ye eşittir.

Adım 2. Her bölüme karşılıklı olan, $t_i - 1$ tane $a_{i,1}, \dots, a_{i,t_i-1}$ değerleri rasgele seçilir. Aşağıda verilen polinomlar tanımlanır:

$f_i(x) = g_i + \sum_{j=1}^{t_i-1} a_{i,j} x^j$, $g_1, \dots, g_m$ gizli görüntünün üretilen kısmi piksel değerlerini gösterir.

$f(y) = \sum_{i=t_i}^{t_i+R-1} b_{i-t_i} y^i$ polinomunu tanımlanır. $b_{i-t_i} = g_{m+1}, \dots, b_{i-t_i+R-1} = g_{m+R}$gizli görüntünün üretilen kısmi piksel değerlerini gösterir.

Adım3. Her bölümün seviyeleri için aşağıdaki denklem üretilir

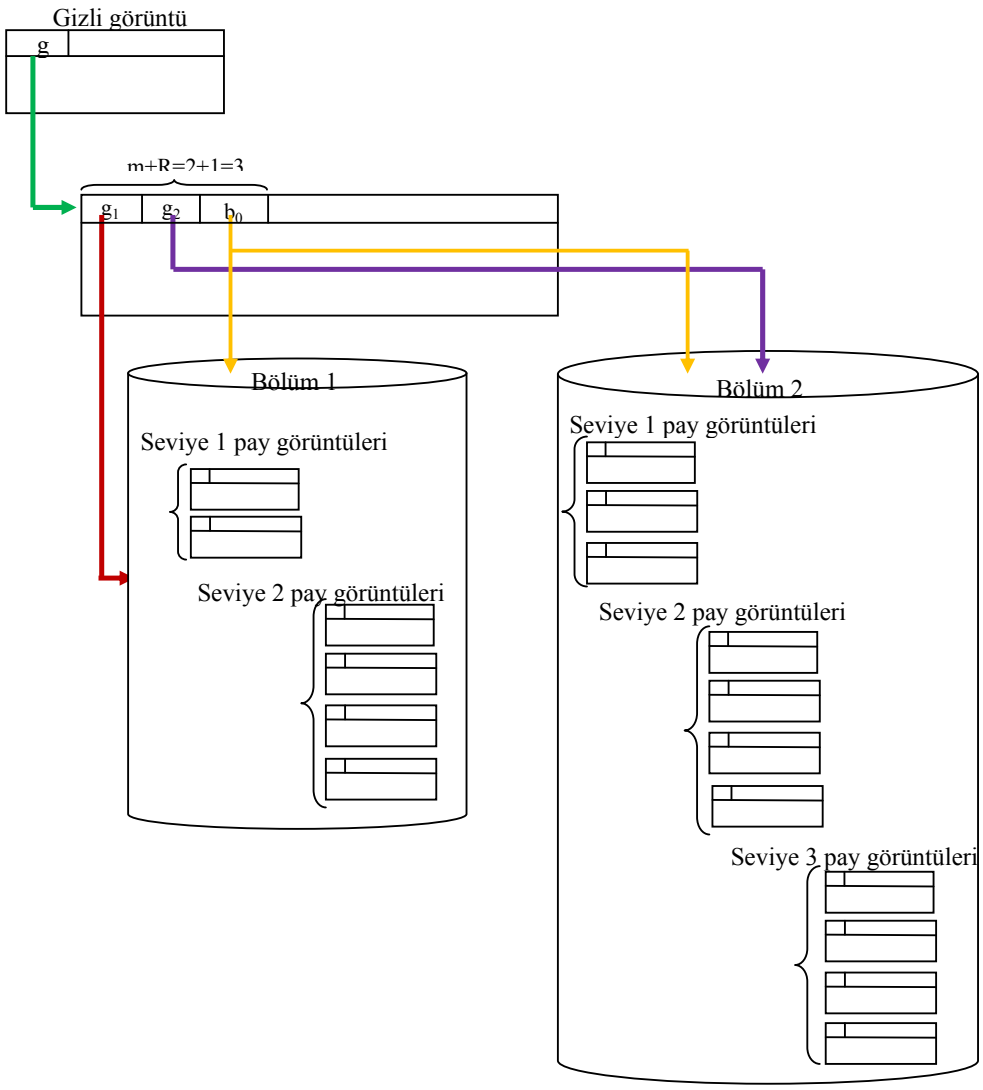
$$f_{i,j}(x, y) = (f_i(x))^{k_{j-1}} + f(y), i = 1, \dots, m \text{ ve } j = 0, \dots, l$$

m bölümler sayısını ve l her bölümün seviye sayısını gösterir. $k_j$her seviyenin eşik değeridir.

Adım 4.*i*'yiminci bölümden ve *j*'yimci seviyeden olan z'iyimci katılımcıya x_{i,j_z} değeri rasgele seçilir ve $s_{i,j}(x_{i,j_z}, y_{i,j_z}) = (f_i(x_{i,j_z}))^{k_{j-1}} + f(y_{i,j_z})$ pay görüntü değeri üretilir.

Adım 5. Üzerinde işlem yapılmamış olan gizli görüntünün piksel değerleri ardı ardına alınır ve pay görüntüler üretilir.

İç içe bölütlenmiş erişim yapısı için tanımlanan gizli görüntü paylaşım şeması şekil 2.11'da gösterilmiştir.



Şekil 2.11.İç içe bölütlenmiş gizli görüntü paylaşım şeması

Gizli görüntüyü yeniden yapılandırması için katılan katılımcı sayısı, en az genel eşik değerine eşit olması gerekir ve her bölümden katılan katılımcı sayısı en az o bölümün eşik değeri kadar olması gerekir. Her bölüm içinde katılımcılar hiyerarşik düzenlenmiş olduğundan dolayı, her bölümden katılan katılımcılar aynı anda en az her seviyeye karşılıklı olan eşik değeri kadar olması gerekmektedir. Bir başka değişle, gizli görüntüyü yeniden yapılandırması için katılan katılımcılar, iç içe bölütlenmiş erişim yapısını sağlaması gerekmektedir. Her bölüm, gizli görüntünün kısmi piksel değerlerini belirlemektedir. Kısmi piksel değerleri ele alındıktan sonra, gizli görüntünün piksel değeri elde edilir. Yeniden yapılandırma algoritması aşağıdaki verilen adımlar halinde tanımlanmıştır.

Adım 1. Her bölüm için t_i katılımcının pay görüntülerinin,$s_{i,j}\left(x_{i,j_z}, y_{i,j_z}\right)$, ilk piksel değeri alınır.

Adım 2. (2.21)'deki gibi t_i adet lineer bağımsız denklem elde edilir:

$$s_{i,j}\left(x_{i,j_z}, y_{i,j_z}\right) = \left(f_i\left(x_{i,j_z}\right)\right)^{k_{j-1}} + f\left(y_{i,j_z}\right) \quad (2.21)$$

$f_i\left(x_{i,j_z}\right) = g_i + \sum_{j=1}^{t_i-1} a_{i,j} {x_{i,j_z}}^j$ ve $f\left(x_{i,j_z}\right) = \sum_{i=t_i}^{t_i+R-1} b_{i-t_i} {x_{i,j_z}}^i$ dir.

Adım 3. (2.21)'de kurulan lineer denklik sistemini, matris tersleme yöntemini kullanarak hesaplanır.

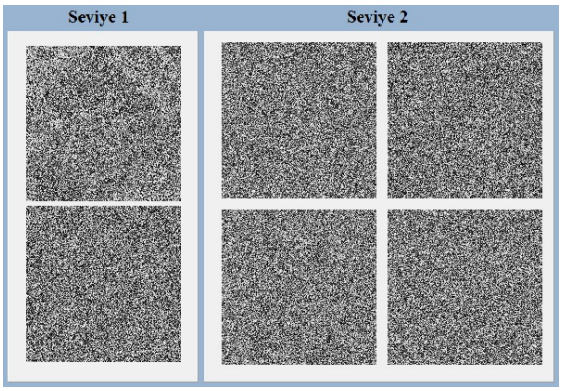
Adım 4. Her bölümden üretilen kısmi gizli görüntünün piksel değerleri ele alını ve bir lineer denklem sistemi kullanarak, gizli görüntünün piksel değeri elde edilir.

Önerilen şema için yapılan testler ve elde edilen deneysel sonuçlar aşağıda verilmektedir. Deneysel gizli görüntü olarak, 210×210 büyüklüğündeki gri seviye gizli görüntü şekil 2.12'de verilmektedir.

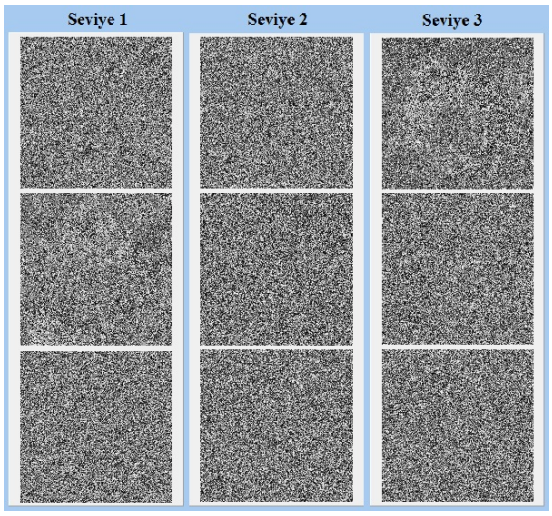
Şekil 2.12. 210×210 büyüklüğünde gri seviye gizli görüntü

Örnek2.8'de tanımlanan bölütlenmiş erişim yapısını kullanarak ve bölütlenmiş gizli görüntü paylaşım algoritmasını kullanarak belirlenen gizli görüntü iki bölümde olan 15 katılımcı arasında paylaştırılmıştır.

Şekil 2.13 ve şekil 2.14'de önerilen yöntemin uygulanması sonucu her bölüm için üretilen pay görüntüleri verilmektedir. Üretilen pay görüntüleri gizli görüntünün aynı büyüklüktedir.



Şekil 2.13. 210×210 büyüklüğündeki birinci bölümünün pay görüntüleri



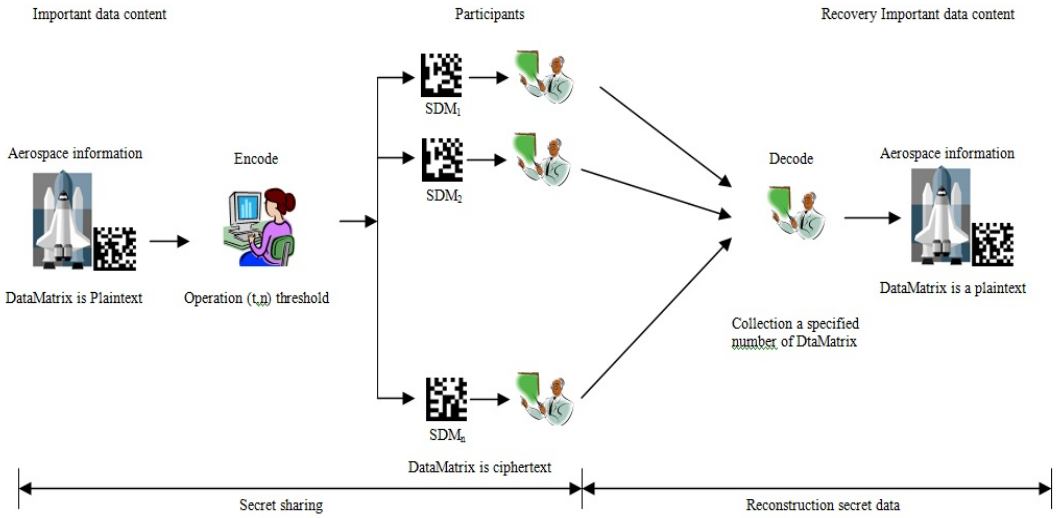
Şekil 2.14. 210×210 büyüklüğündeki ikinci bölümünün pay görüntüleri

Yeniden yapılandırma aşamasında örnek 2.1'de tanımlanan bölütlenmiş erişim yapısını sağlayacak şekilde 10 katılımcının pay görüntüleri bir araya gelmesi durumunda gizli görüntü elde edilmektedir. Bu yöntem için elde edilen PSNR değeri sonsuzdur.

2.3.Verimatrisi Paylaşım Şeması

VeriMatrisi barkodları üzerindeki bilgilerinin güvenliğinin sağlanması için sır paylaşım şeması önerilmektedir. Önerilen yöntemde Blakley'nin sır paylaşım şemasını kullanarak gizli metin paylara ayrılır. Ardından her bir pay VeriMatris içerisine gömülür.

Her bir VeriMatris payı gizli metin ile ilgili hiçbir bilgi açığa çıkarmamaktadır. Gizli metinin yeniden elde etmesi için VeriMatris payları önceden belirlenen eşik değerine eşit veya daha fazla olması gerekmektedir. Böylece VeriMatris üzerinde ki veriler anlamsız olmaktadır ve sadece bir kişi tarafından okunmamaktadır. Önerilen yöntem şekil 2.15'de gösterilmiştir.



Şekil 2.15. VeriMatris veri paylaşım şeması

Önerilen (t,n) VeriMatris veri paylaşım şeması aşağıda adımlar halinde verilmiştir.

Adım1: Gizli veri, t karakterli bölümlere $(a_1, \dots, a_t)$, ayrılır.

Adım2: t karakterin ASCII değerleri alınır

Adım3: Denklem (2.22) oluşturulur

$$p(x) = (a_1x_1 + \cdots + a_tx_t)\ mod\ 127 \qquad (2.22)$$

Adım4: Her bir katılımcı için rastgele çözüm seti $(x_{i,1}, \dots, x_{i,t}), i = 1, \dots, n$, seçilir ve $s_i = p_i(x_{i,1}, \dots, x_{i,t})$ da yerleştirerek pay değerleri üretilir.

Adım5: oluşturulan pay değerleri VeriMatris içerisine yerleştirilir. (VeriMatrisi üretiminde Ek1 de verilen yöntem kullanılmıştır.)

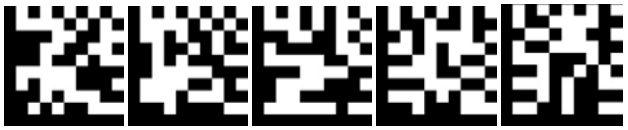
Yeniden yapılandırma aşamasında en az *t* sayıda VeriMatris payının bir araya gelmeleri gerekmektedir. Herhangi bir VeriMatris payı gizli veri ile ilgili hiçbir bilgi vermez. Yeniden yapılandırma algoritması aşağıda adımlar halinde verilmiştir.

Adım1: VeriMatris payının içerisindeki bilgiler elde edilir.

Adım2: elde edilen bilgiler $(s_1, \dots, s_t)$, denklem (2.23)'de yerleştirerek gizli veri elde edilir.

$$s = p(x) = ((a_1x_1 + \cdots + a_tx_t)\ mod\ 127)^{-1} \tag{2.23}$$

Örnek 2.10: "SECRETEST" kelimesini VeriMatrisle içerisine paylaştırılacaktır. Önce kelime *(t,n)*Blakley'in gizli paylaşım şemasını kullanarak *n* paya bölünüp, sonradan VeriMatrisler içerisine gömülecek. (3,5) eşik gizli paylaşımı kullanılarak gizli verinin ilk 3 karakteri alınır, "SEC" karakterleri paylaştırma algoritmasını kullanarak "-=h" karakterlerine karşı düşmektedir. VeriMatrisi kodlaması algoritmasınıkullanarak bir VeriMatrisinde yerleştirilir. Şekil 2.16'da üretilen VeriMatrisler gösterilmiştir.



Şekil 2.16. VeriMatris payları

3. SONUÇLAR VE ÖNERİLER

Tez çalışmasında çok parçalı sır paylaşım şemaları üzerinde yapılan araştırmalardan elde edilen sonuçlar aşağıda kısaca verilmiştir:

Çalışmada Simmons'un ve Tassa'nın tanımladıkları erişim yapıları göz önüne alınarak yeni bir ayrıcı ve birleştirici hiyerarşik sır paylaşım şeması önerilmiştir. Literatürdeki çalışmalara göre hiyerarşik sır paylaşım şemaları genellikle Shamir'in tanımladığı yönteme dayanmaktadır. Brickell, polinomial interpolasyon ve Simmons geometri tabanlı ayrıcı hiyerarşik sır paylaşım şeması önermişlerdir. Simmons'un yapısında yeniden yapılandırma matrisinin tanımlanmasından dolayı bu şema verimli değildir ve Tassa'nın tanımladığı birleştirici hiyerarşik erişim yapısına uygun olmamaktadır. Ghodosi ve arkadaşları, Shamir eşik şemasını kullanarak bir ideal hiyerarşik ve bölütlenmiş sır paylaşım şeması önermişlerdir. Ancak, bu şema sadece küçük sayıda olan katılımcılar için uygundur. Tassa tanımladığı birleştirici hiyerarşik erişim yapısı için, Brikhoff interpolasyonuna dayalı polinom türevlerini kullanarak ideal sır paylaşım şeması önermiştir. Bu tez çalışmasında diğer çalışmalardan farklı olarak Blakley'nin geometrik şeması hiyerarşik sır paylaşımında kullanılmıştır.

Ayrıcaçok parçalı erişim yapısı olan bölütlenmiş yapıya kısıtlamalar getirerek yeni bir iç içe bölütlenmiş sır paylaşım şeması önerilmiştir. Tez çalışmasında önerilen yaklaşımda bölütlenmiş erişim yapısı içerisinde hiyerarşik yapı bulunmaktadır. Tanımlanan iç içe bölütlenmiş erişim yapısı için yeni bir sır paylaşım şeması önerilmiş ve bu şemanın mükemmellik özelliği sağlanmıştır. Her katılımcının pay alanı, sırrın bilgi alanına eşit olduğundan, önerilen sır paylaşım şeması idealdir ve bilgi oranı bire eşittir.

Önerilen şemalar gizli görüntü paylaşım alanında kullanılmıştır. Literatürde gizli görüntü paylaşım şemaları daha çok eşik sır paylaşım şemaları için kullanılmıştır. Ancak gerçek uygulamalarda eşik şemaların çok da yararlı olmadığı belirlenmiştir. Bu yüzden benzeri durumlarda çok parçalı gizli görüntü paylaşım şemaları önerilmiştir. 2011 yılında Guo gizli görüntüler için, Tassa'nın önerdiği hiyerarşik sır paylaşım şemasını kullanmıştır. Bu tez çalışmasında önerilen hiyerarşik sır paylaşım şeması, gizli görüntü üzerinde uygulanmıştır. Guo'nun çalışmasında üst seviyeden katılımcı olmadığı durumda, gizli görüntü ile ilgili bilgiler erişilebilirken, tezde kullanılan yöntemde gizli görüntü ile ilgili hiç bir bilgi açığa çıkarılmamaktadır.

Bir başka kısımda ise önerilen iç içe bölütlenmiş sır paylaşım şeması, ilk olarak gizli görüntü üzerinde uygulanmıştır. Önerilen gizli görüntü paylaşım şemasında pay büyüklüğü, gizli görüntü büyüklüğündedir. Herhangi bir iç içe bölütlenmiş erişim yapısının koşulları sağlanmadığı durumda, örneğin bir bölümden katılımcı olmazsa, genel eşik miktarı sağlanmamışsa veya bölümlerin içerisinde olan hiyerarşik seviyelerden katılan katılımcılar en üst seviyeden olmazsa ve benzeri durumlarda, gizli görüntü ile ilgili hiçbir bilgi açığa çıkarılamamaktadır. Dolayısıyla, bu önerilen ideal şemanın mükemmellik özeliğinin sağladığını göstermektedir. Tüm önerilen gizli görüntü paylaşım şemalarında PSNR değeri sonsuzdur.

Tez kapsamında Blakley sır paylaşım şeması, VeriMatrisleri üzerinde uygulanmıştır. VeriMatrisi ürünle ilgili bazı bilgileri taşımaktadır, ancak tüm bu bilgiler mobil cihazlar kullanılarak herkes tarafından elde edilebilinir. Fakat bazı ürünlerin bilgisinin ortaya çıkmasını önlemek için VeriMatris paylaşım şeması kullanarak paylara bölünebilir ve dolayısıyla bilgilerin gizliliği tamamen sağlanmıştır.

Öneriler:

Önerilen iç içe bölütlenmiş erişim yapısı için geometrik tabanlı veya sayı teorisine dayalı yöntemler kullanılarak daha verimli ideal sır paylaşım şeması belirlenebilir.

Yeniden yapılandırma aşamasında gizli görüntünün yeniden oluşturulmasının hesapsal karmaşıklığının azaltılması ve depolanma gereksinimlerinin büyütülmesi açısından, gizlilik özelliği korunarak genişleme faktörünün iyileştirilmesi araştırmaları yapılabilir.

Ayrıca önerilen yaklaşımlar gizli görüntü paylaşımında steganografik tekniklerin kullanımıyla daha da güçlendirilebilir.

4. KAYNAKLAR

1. Shamir, A., How to Share a Secret. Communications of the Acm, 22(1979) 612-613.

2. Blakley, G.R., Safeguarding cryptographic keys. National Computer Conference, Haziran 1979, New York, Bildiriler Kitabı, 313-317.

3. Mignotte, M., How to Share a Secret, Lecture Notes in Computer Science, 149(1983) 371-375.

4. Asmuth, C. ve Bloom, J., A modular approach to key safeguarding, IEEE Transactions on Information Theory, 29(1983) 208-210.

5. Ito, M., Saito, A., ve Nishizeki,T.,Multiple Assignment Scheme for Sharing Secret, Journal of Cryptology, 6, 6(1987) 15-20.

6. Benaloh, J.C. ve Leichter,J., Generalized secret sharing and monotone functions,Lecture Notes in Computer Science, 403(1990) 27-35.

7. Csirmaz, L., The Size of a Share Must Be Large. Journal of Cryptology, 10, 4(1997) 223-231.

8. Karnin, E. D., Greene,J. W.ve Hellman, M. E., On secret sharing systems,IEEE Transactions on Information Theory, 29, 1(1983) 35-41.

9. Beimel, A., Tassa,T. ve Weinreb,E., Characterizing ideal weighted threshold secret sharing, Journal on Discrete Mathematics, 22, 1(2008) 360-397.

10. Farras, O. ve Padro,C., Ideal Hierarchical Secret Sharing Schemes,Theory of Cryptography, 5978, (2010) 219-236.

11. Kasper, E., Nikov, V. ve Nikova, S., Strongly Multiplicative Hierarchical Threshold Secret Sharing,Information Theoretic Security, 4883,(2009)148-168.

12. Morillo, P., Padro, C., Saez, G. ve Villar, J. L., Weighted threshold secret sharing schemes. Information Processing Letters, 70, 5(1999) 211-216.

13. Nikov, V., Nikova,S. ve Preneel,B., Multi-party computation from any linear secret sharing scheme unconditionally secure against adaptive adversary: The zero-error case, Lecture Notes in Computer Science, 2846, (2003)1-15.

14. Tassa, T. ve Dyn,N., Multipartite secret sharing by bivariate interpolation, 33rd international conference on Automata, Languages and Programming , 2006, Venice, Italy , Bildiriler Kitabı II: 288-299.

15. Kothari, S., Generalized Linear Threshold Scheme, Proceedings of CRYPTO 84 on Advances in cryptology,(1985) 231-241.

16. Simmons, G.J., How to (Really) Share a Secret, Lecture Notes in Computer Science, 403(1989) 390-448.

17. Brickell, E.F., Some ideal secret sharing schemes, Journal of Combinatorial Mathematics and Combinatorial Computing, 6(1989) 105-113.

18. Tassa, T., Hierarchical threshold secret sharing, Journal of Cryptology, 20, 2(2007) 237-264.

19. Belenkiy, M., Disjunctive Multi-Level Secret Sharing,Cryptology ePrint Archive, 018(2008).

20. Kaşkaloğlu, K. veÖzbudak, F., Nested multipartite secret sharing, Computer Science and Automation Engineering (CSAE), 2011IEEE International Conference,Temmuz 2011, Shanghai, Bildiriler kitabı IV:66-73.

21. Pareek, N.K., Patidar,V. ve Sud,K.K., Image encryption using chaotic logistic map,Image and Vision Computing, 24, 9(2006) 926-934.

22. Thien, C. C. ve Lin, J. C., Secret image sharing,Computers and Graphics, 26, 5(2002) 765-770.

23. Alkharobi, T. M., Secret Sharing Using Artificial Neural Network, Doktora Tezi,Office of Graduate Studies ofTexas A&M University, 2004.

24. Knuth, D., The Art of Computer Programming, Third Edition,Addison-Wesley Professional,1969.

25. Ghodosi, H., Pieprzyk,J. ve Safavi-Naini,R., Secret Sharing in Multilevel and Compartmented Groups, Lecture Notes in Computer Science,1438(1998) 367-378.

26. Blundo, C., De Santis, A., Gargano, L. ve Vaccaro, U., Secret Sharing Schemes With Veto Capabilities, Lecture Notes in Computer Science,(1994)82-89.

27. Naor, M. ve Shamir,A., Visual cryptography, Lecture Notes in Computer Science, 950(1995)1-12.

28. Chi-Shiang, C. vePing-En, S., Secret Image Sharing with Steganography and Authentication Using Dynamic Programming Strategy,First International Conference on Pervasive Computing Signal Processing and Applications (PCSPA), 2010, China, Bildiriler Kitabı, 382-385.

29. Hsu, S.J.,Chuan-Feng, C., Sen-Ren, J. ve Chia-Tai, C., Distortion-free multiple images sharing scheme with universal share, Joint Conferences on Pervasive Computing (JCPC), 2009, Taipei, Taiwan, Bildiriler kitabı, 833-838.

30. 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.

31. Shi, R.H., Zhong, H.,Huang, L. ve Luo, Y., A (t, n) secret sharing scheme for image encryption. First International Congress on Image and Signal Processing, 2008, Bildiriler Kitabı III: 3-6.

32. Tso, H. K. ve Lou, D. C.Sharing Secret Image Based on Random Grids,2nd International Conference on Computer Science and its Applications,Aralık 2009, Korea,Bildiriler Kitabı, 1-5.

33. Wen-Pinn, F., Secret image sharing safety,14th Asia-Pacific Conference on Communications, 2008, Tokyo, Japan,Bildiriler Kitabı,1-4.

34. Bai, L., A Reliable (k, n) Image Secret Sharing Scheme,2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Eylül 2006, USA, Bildiriler Kitabı, 31-36.

35. Hao-Kuan, T., Der-Chyuan, L., Kai-Ping, W. ve Chiang-Lung, L.,A Lossless Secret Image Sharing Method,Eighth International Conference on Intelligent Systems Design and Applications, Kasım 2008, Taiwan,Bildiriler Kitabı III: 616-619.

36. Lukac, R. ve Plataniotis, K.N., Bit-level based secret sharing for image encryption,Pattern Recognition, 38, 5(2005) 767-772.

37. Chen, C.C. ve Fu, W. Y., A Geometry Based Secret Image Sharing Approach,Journal of Information Science and Engineering, 24(2008)1567-1577.

38. Tso, H. K.,Sharing Secret Images Using Blakley's Concept, Optical Engineering,47, 7 (2008) 1-3.

39. Ulutas, G., Ulutas, M. ve Nabiyev,V., Distortion free geometry based secret image sharing,Procedia Computer Science, 3, (2011) 721-726.

40. Guo, C., Chang,C.C. ve Qin, C., A hierarchical threshold secret image sharing,Pattern Recognition Letters, 33, 1(2012) 83-91.

41. Chaung, J.C., Hu, Y.C., Ko, H.J, A novel secret sharing technique using QR code,Computer Science Journals, 4,5(2010) 457-517.

42. Chen, T., The Application of Bar Code Forgery-Proof Technology in the Product Sales Management, 2008 International Symposium on Intelligent Information Technology Application Workshops, Aralık 2008, China, Bildiriler Kitabı, 936-939.

43. Chen, W.Y., Wang, J.W., Nested Image Steganography Scheme using QR-barcode technique,Optical Engineering, 48, 5(2009).

44. Chin-Ho, C., Wen-Yuan,C. ve Ching-Ming, T., Image Hidden Technique Using QR-Barcode,Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Eylül 2009, Japan,Bildiriler Kitabı, 522-525.

45. Clarke, C.K.P., Reed-Solomon error correction, BBC R&D White Paper, 2002.

5. EKLER

Ek-1. Matris Ters Çevirme

$A_{n\times n}$,verilen bir kare matrisi için, eğer bir matris $B_{n\times n}$ aşağıda verilen koşulları sağlarsa o zaman bu matrise A'nın tersi denilir ve $B = A^{-1}$ ile gösterilir:

$$AB = I_n \text{ ve } BA = I_n$$

Tüm kare matrisler her zaman tersi alınamaz. Tersi alınan matrise tekli olamayan denilir ve tersi alınamayan matrise tekli matris denilir

Ek-2. Lineer Bağımsızlık

$S = \{v_1, v_2, \dots, v_3\}$bir vektör kümesinin girdileri arasında bağımlılık ilişkisi olmazsa o zaman bu vektör lineer bağımsız küme söylenir. Oysa lineer bağımlı kümede en az bir vektör, diğer vektörlerin birleştirmesidir.

A kare matrisi için, eğer aşağıda verilen ifadelerin herhangi biri, A'nın nonsingular olması anlamına gelir:

- A'nın sütunları bir lineer bağımsız küme oluşturur.
- A'nın satırları bir lineer bağımsız küme oluşturur.

Ek-3. Galoise Alanı

Galoise alanın, Elemanların sayısı p^n formundadır ve p bir asal rakamdır ve n bir pozitif tamsayıdır. Her p asal sayı ve n pozitif tamsayı için, bir p^n elemanlı, sonlu alan vardır. P asal olmayan rakam olamaz, çunku alanlar üzerinde olan matematik işlemleri karşılamaz.

Galoise alanı elemanlar(rakamlar) kümesinden oluşur. Elemanlar bir ilk elamana dayanmaktadır ve genelde onu αyla gosterilmektedirve aşağıdaki verilen miktarları, bir 2^m elemanlı (ve $N = 2^m - 1$) kumeni biçimlendirmek için alır:

$0, \alpha^0, \alpha^1, \alpha^2, \ldots., \alpha^{N-1}$ (1)

α nın miktarı genelde 2 seşilir, buna rağmen başka miktarlarda kullanılabilir. α nı seştikten sonra, yuksek üsler(powers) , her adımda α yla çarparak sağlanabilir. Ancak galoise alanda ki çarpma kuralları farklıdır.

Ayrıca α formunda üsse için , her alanın elemanı aşağıdaki verilen polinominal ifadesiyle gösterilebilir:

$$a_{m-1}x^{m-1} + \cdots + a_1x + a_0$$

$a_{m-1}, \ldots, a_0$katsayıları, 0 ya 1 değeri alırlar. Boylece alan elemanı, $a_{m-1} \ldots a_0$ binary rakamlar ve 2^m alan elemanları(m bit rakamın, 2^m birleşimine karşılığıdır) kullanarak, tanımlayabiliriz.

Örnek olarak, 16 elemanı olan Galois alanında(GF(16) olarak tanımlanır ve $m = 4$ dur) polinominal temsilcisi:

$$a_3x^3 + a_2x^2 + a_1x^1 + a_0x^0$$

$a_3a_2a_1a_0$, 0000 den ta 1111'e eştir. Alternatif olarak bu alan elemanlarına 0 ta 15 ondalık eşdeğerinde gösterilebilir. Sonlu alanın matematiği, kullandığımız normal matematikken farklıdır.

ÖZGEÇMİŞ

Katira SOLEYMAN ZADEH; 1982 yılında Makoo, İRAN'da doğdu. İlköğretimini MakoonunRobab İlkokulunda bitirdikten sonra orta ve lise öğretimini Orumiye şehrinde Farhangiyan Ortaokulu ve Zahra Lisesi'nden mezun oldu. 2000 yılında Khoy AZAD Üniversitesi, Fen Bilimler Fakültesi, Bilgisayar Mühendisliği Bölümü'nü okumaya hak kazandı. Bu bölümden, 2005 yılında mezun oldu. 2006 yılından itibaren, Orumiye Tıp Fakültesinde Bilgisayar Laboratuarında ağ müdürü olarak görev yaptı. 2009 yılında, Karadeniz Teknik Üniversitesi, Fen Bilimler Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı'nda Yüksek Lisans Programına başladı.