KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

KAOTİK HARİTALAR KULLANARAK GÖRÜNTÜ ŞİFRELEME

YÜKSEK LİSANS TEZİ

Bilgisayar Müh. Cihat KELEŞ

HAZİRAN 2012
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

KAOTİK HARİTALAR KULLANARAK GÖRÜNTÜ ŞİFRELEME

Bilgisayar Müh. Cihat KELEŞ

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"BİLGİSAYAR YÜKSEK MÜHENDİSİ"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 25.05.2012
Tezin Savunma Tarihi : 18.06.2012

Tez Danışmanı : Yrd. Doç. Dr. Mustafa ULUTAŞ

Trabzon 2012

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalında

Cihat KELEŞ tarafından hazırlanan

KAOTİK HARİTALAR KULLANARAK GÖRÜNTÜ ŞİFRELEME

başlıklı bu çalışma, Enstitü Yönetim Kurulunun 29 / 05 / 2012 gün ve 1458 sayılı kararıyla oluşturulan jüri tarafından yapılan sınavda

YÜKSEK LİSANS TEZİ

olarak kabul edilmiştir.

Jüri Üyeleri

Başkan : Prof. Dr. İ. Hakkı ALTAŞ …...……

Üye : Yrd. Doç. Dr. Mustafa ULUTAŞ …...……

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

Prof. Dr. Sadettin KORKMAZ

Enstitü Müdürü

ÖNSÖZ

Kaos teorisi ile kriptografi arasında birçok ortak nokta vardır. Kaotik sistemler, karıştırma ve yayılma gibi temel kriptografik gereksinimlerini doğal olarak bulundurdukları için şifreleme sistemlerinde kullanılabilirlikleri üzerine araştırmacılar tarafından çalışmalar yapılmaktadır.

Bu çalışmada, piksel tabanlı karıştırma ve bit tabanlı piksel karıştırma aşamalarının yayılma aşamasına olan etkileri yeni bir yayılma yaklaşımı üzerindeki incelenmiş, kaotik resim şifrelemenin geleneksel yöntemlerle resim şifrelemeye göre avantajları ve dezavantajları ortaya konulmuştur.

Çalışmamda danışmanlığımı üstlenen değerli hocam Yrd. Doç. Dr. Mustafa ULUTAŞ'a çalışmam boyunca manevi desteklerini eksik etmeyen sevgili arkadaşlarım Mengü DEMİR'e, Arş. Gör. Mustafa YAZICI ve Esra ODABAŞ YILDIRIM başta olmak üzere, tüm çalışma arkadaşlarıma teşekkür ederim.

Cihat KELEŞ

Trabzon 2012

TEZ BEYANNAMESİ

Yüksek Lisans Tezi olarak sunduğum "KAOTİK HARİTALAR KULLANARAK GÖRÜNTÜ ŞİFRELEME" başlıklı bu çalışmayı baştan sona kadar danışmanım Yrd. Doç. Dr. Mustafa ULUTAŞ'ın sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuarlarda yaptığımı/yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim. 26/06/2012

Cihat KELEŞ

İÇİNDEKİLER

Sayfa No

Yüksek Lisans Tezi

ÖZET

KAOTİK HARİTALAR KULLANARAK GÖRÜNTÜ ŞİFRELEME

Cihat KELEŞ

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Danışman: Yrd. Doç. Dr. Mustafa ULUTAŞ
2012, 62 Sayfa

Ağ teknolojisi son on yılda önemli ölçüde gelişmiştir. Askeri, ticari ve tıbbi veri tabanları gibi gizli olması gereken veri kaynakları bulut teknolojisiyle işlenmekte ve saklanmaktadır. Aynı şekilde video konferansı, kaynak paylaşımı ve istek uygulamalar üzerindeki video güvenilir, hızlı ve sağlam güvenlik sistemleri gerektirmektedir. Metin mesajlarını şifrelemek için tasarlanan standart şifreleme yöntemleri, görüntülerin komşu pikselleri arasındaki yüksek korelasyonu ve büyük veri miktarından dolayı görüntü şifreleme gereksinimlerini tam olarak yerine getirememektedir. Bu nedenle, resim ve video akışı gibi çoklu ortam içeriğini şifreleme yöntemleri bilim adamları için aktif bir araştırma alanıdır. Özellikle çoklu ortamların şifrelenmesinde kaos teorisi etkin araştırma konularından bir tanesidir.

Bu çalışmada ilk olarak kriptografinin temelleri ve çoklu ortam içeriğinin şifrelenme sorunlarından bahsedilmiştir. Sonra, kaos teorisi özetlenmiş ve kriptografi ile ortak özellikleri incelenmiştir. Karıştırma ve yayılma tabanlı bir görüntü şifreleme yöntemi kaotik haritalar kullanılarak tasarlanmış ve uygulanmıştır. Kaotik ve geleneksel yöntemlerle şifrelenmiş görüntülerin istatistiksel ve güvenlik testleri yapılarak elde edilen ölçüm değerleri karşılaştırılmıştır.

Anahtar Kelimeler: Kaos, Dinamik Sistemler, Resim Şifreleme, Rastgelelik, Yayılma, Karıştırma, Kriptanaliz.

Master Thesis

SUMMARY

IMAGE ENCRYPTION USING CHAOTIC MAPS

Cihat KELEŞ

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering
Supervisor: Assoc. Prof. Mustafa ULUTAŞ
2012, 62 Pages

Networking technology have improved considerably over the last decade. Data sources like military, commercial and medical image databases which needs to be confidential are stored and processed on the cloud. Likewise, video conferencing, resource sharing and video on demand applications require reliable, fast and robust security systems. Standard encryption methods designed to encrypt text messages can not fulfill image encryption requirements due to both high correlation among adjacent pixels and vast amount of data. Therefore, encryption methods to process multimedia content like image and video stream are an active research field for scientists. In particular, application of chaos theory in multimedia content encryption is one of the active research topics.

Fundamentals of cryptography and issues in multimedia content encryption are presented first. Then general theory of chaos is outlined and similarity to cryptography is investigated. An image encryption system with confusion and diffusion based on a chaotic map is designed and implemented. Statistical and security analysis measures of well known test images encrypted by both the chaotic and standard encryption methods are compared.

Keywords: Chaos, Dynamic Systems, Image Encryption, Randomness, Diffusion, Confusion, Cryptanalysis.

ŞEKİLLER DİZİNİ

Sayfa No

TABLOLAR DİZİNİ

SEMBOLLER DİZİNİ

C	Düz Metin
D	Şifre Çözme Fonksiyonu
E	Şifreleme Fonksiyonu
$f^n(x)$	Başlangıç Değeri x Olan fonksiyonun n. İterasyonu
K_e	Şifreleme Anahtarı
K_d	Şifre Çözme Anahtarı
L	Resmin Gri Seviye Değeri
m	Karıştırma Aşamasındaki Döngü Sayısı
MxN	Resim Boyutu
n	Şifrelemedeki Toplam Döngü Sayısı
p, q	Arnold Cat Haritasının Kontrol parametreleri
P	Şifreli Metin
P(x, y)	Resmin (x, y) Konumundaki Piksel Değeri
q(.)	Bit Ayrıştırma Fonksiyonu
r	Logistic Haritanın Kontrol Parametresi
R	Gerçek Sayılar Kümesi
$round_k$	K Duyarlılığında Yuvarlama Fonksiyonu
S_i	Sözde Rastgele Sayı Üretecinin i. İterasyonda Ürettiği Değer
x_n	Yörüngenin n. İterasyondaki Değeri
$\oplus$	Exclusive-or, XOR kapısı
Λ	Lyapunov Üsteli
δ	Dinamik Bir Sistemin İki Farklı Noktası Arasındaki Uzaklık

1. GENEL BİLGİLER

1.1. Giriş

Değerli bilgiyi koruma ihtiyacı tarihin çok eski dönemlerinden günümüze kadar var olmuştur. Roma zamanında Julius Sezar, mesaj şifrelemede kullanılmak için şifreleme araçlarına ihtiyaç duyulduğunu görmüştür. Bu ihtiyacın ortaya çıkmasından sonra insanlar önemli mesajları saklayabilmek için onları anlaşılmaz hale getirmeye çalışmışlardır. Çok eski devirlerden günümüze kadar geliştirilmekte olan şifreleme teknikleri, sayısal (digital) ortamların ortaya çıkmasıyla yeni bir yüz kazanmıştır. Ses, video veya yazılım gibi sayısal içeriklerin şifrelenmesinde ve bu içeriklere olan erişim kontrollerinde, bilgi gizlice verilerin içinde saklı hale getirilmiştir.

Şifre bilimi olan kriptolojinin bir alt çalışma alanı olan kriptografi, Yunanca *crypto* (gizli) *graph* (yazım) kelimelerinden gelmektedir. Tam olarak Türkçe karşılığı "şifre yazım"dır. Son yıllarda ses ve görsel bilgilerin güvenliği, internetin hızlı gelişimiyle beraber daha fazla önem kazanmıştır. Açık ağlarda, askeri ve medikal resimler gibi önemli bilgilere yetkisiz erişim ve benzeri potansiyel riskler mevcuttur. Bundan dolayı çoklu ortam güvenliğini sağlayabilmek için güçlü şifreleme şemaları geliştirme gereksinimi duyulmuştur. Metin bilgisinin şifrelenmesi için güvenliği iyi geliştirilmiş DES [1] (Data Encryption Standard), AES [2] (Advanced Encryption Standard) gibi şifreleme algoritmaları kullanılmaktadır. Ancak haberleşmede çoklu ortam bilgisinin geleneksel şifreleme algoritmalarıyla şifrelenmesi zordur. Bunun sebebi ses ve görsel verinin büyük veri kapasitesi, güçlü piksel korelasyonu ve düşük şifrelenme performansı gibi özelliklere sahip olmasıdır.

Modern çoklu ortam gereksinimleri için geleneksel şifreleme algoritmaları çok fazla uygun değildir. Bundan dolayı birçok araştırmacı resim ve video şifreleme için daha iyi çözümler üretmeye çalışmaktadır. Son yıllarda, özellikle kaotik sistemler çoklu ortam şifrelemesi için önemli bir araştırma alanı olmuş ve kaotik şifreleme alanında dikkate değer çalışmalar yapılmıştır. Kaotik sistemlerin bu derece ilgi çekmesinin sebebi, basit bir forma sahip olmaları ve dinamiklerindeki karmaşıklıktır. Kaos tabanlı güvenlik uygulamaları, sürekli dinamik sistemler ile güvenli haberleşmeyi amaçlayan analog kaotik güvenli haberleşme [3, 4] ve ayrık dinamik sistemler ile güvenliği amaçlayan sayısal kaotik

şifreleme sistemleri [5, 6, 7] olarak ikiye ayrılmaktadır. Güvenliğin, günümüz bilgisayar teknolojilerinde sağlanmasında, kaosun sonlu duyarlıklı makinelerde sayısal olarak gerçekleştirilmesi daha uygundur.

Fridrich'in 1998 yılında yayınladığı kaotik resim şifreleme şemasından [8] sonra kaotik resim şifreleme alanında birçok araştırma yapılmıştır. Bu şifreleme sistemlerin çalışma ilkesi, genellikle piksel karıştırması (confusion) ve bu karıştırmadan sonra her bir pikselin sırayla şifrelenmesi üzerinedir. Resim şifrelemede iki veya daha yüksek boyutlu kaotik haritalar, doğallıklarının bir sonucu olarak resmi 2 boyutlu bir dizi olarak ele aldıklarından şifrelemenin piksel karıştırma aşamasında kullanılmışlardır [9]. Guan 2 boyutlu kaotik cat haritasını [10], Lian ise 2 boyutlu kaotik standart haritayı [11] resim şifrelemede kullanmıştır.

Bu çalışmadaki amaç, ayrık kaotik haritaları kullanarak güvenli resim şifreleme yapmaktır. Yeni bir piksel yayılma önerisi getirilmiş, piksel tabanlı karıştırma ve bit tabanlı piksel karıştırma aşamalarının yayılma aşamasına olan etkileri ayrı ayrı incelenmiştir. Her iki karıştırma yaklaşımının karşılaştırılmaları yapılarak, geleneksel şifreleme algoritmalarına karşı avantajları ve dezavantajları ortaya konulmuştur. Sonuç olarak geliştirilen uygulamanın sonuçları incelenmiş ve güvenlik analizleri yapılmıştır.

1.2. Kriptografinin Temelleri

Kriptografi, veri bütünlüğü (Data Integrity), gizlilik (Confidentiality), kimlik doğrulama (Authentication) ve reddedilemezlik (Non-repudiation) gibi hedefleri gerçekleştirmeyi ilke edinen bir çalışma alanıdır [12, 13, 14]. Kriptanaliz var olan şifreleme sistemlerini kırmayla ilgilenen bir çalışma alanıdır. Birbirlerine bağlı olan kriptografi ve kriptanaliz, kriptoloji biliminin birer alt dallarıdır. Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür.

Yetkisiz bir uç sistem haberleşme ağına bağlanarak, gizli olması gereken bilgiye erişebilir. Bu durumda bilginin gizliliği korunmalıdır. Gizlilik, bilginin şifrelenmesi ile sağlanır. Bununla birlikte, gizlilik güvenli iletimin kısıtlanmış tek tanımı değildir. Gönderici ve alıcı sistemler birbirlerinin kimlik denetimini yapsalar bile, iletilen içeriğin kötü niyetli kişilerce veya kazara değiştirilmemiş olduğundan emin olmak isterler. Veri

bütünlüğünün sağlanması için, yetkisiz bir şekilde bilgi değiştirildiğinde haberleşen taraflar bu durumu tespit ederler.

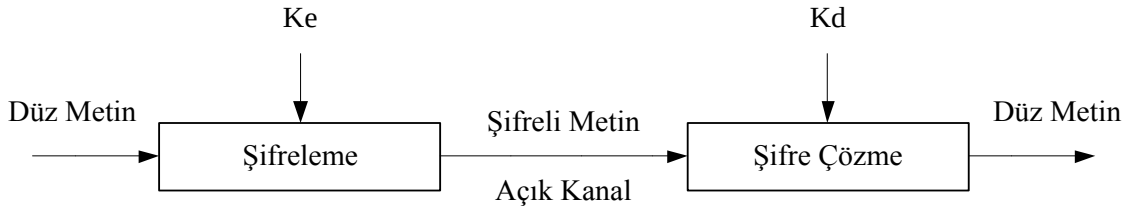
Gönderici ve alıcı tarafların her ikisinin de iletişime katılan diğer tarafın kimliğini doğrulayabilmesi gerekir. Diğer tarafı doğrulamak demek, aslında iddia ettikleri taraf olup olmadıklarını anlamak demektir. Doğrulama metotları ile haberleşen taraflar, karşılıklı olarak birbirlerinin kimliklerini belirleyebildiği gibi mesajın gerçek kaynağından gelip gelmediği de tespit edilebilir. Reddedilemezlik ise mesajı alan uç sistemin herkese, gönderenin bu mesajı gerçekten gönderdiğini ispatlayabilmesidir.

Şifrelemedeki temel amaç, mesajı sadece yetkili tarafın orijinal haline geri döndürebileceği şekilde anlaşılmaz hale getirmektir. Bir şifreleme sistemi düz metin (P), şifreli metin (C), anahtarlar (K_e, K_d), şifreleme (E) ve şifre çözme (D) dönüşümleriyle (1)'deki gibi ifade edilebilir. Düz metin şifreleme anahtarı kullanarak şifrelenir.

$$C = E_{K_e}(P) \tag{1}$$

Burada E şifreleme fonksiyonunu, K_e şifreleme anahtarını temsil etmektedir. Elde edilen C şifreli metni, D şifre çözme fonksiyonu ile şifre çözme anahtarı kullanarak orijinal P düz metnine (2)'deki gibi geri dönüştürülür. Burada, bir metin sadece şifre çözme anahtarı ile orijinal haline dönüştürülebilmektedir. Genel bir şifreleme yapısı Şekil 1.1'de gösterilmektedir.

$$P = D_{K_d}(C) \tag{2}$$



Şekil 1.1. Genel bir şifreleme sisteminin yapısı. Şifreleme ve Şifre çözme

1.2.1. Kerckhoffs İlkesi

Kerckhoffs ilkesi [15] Claude Shannon tarafından "düşman sistemi biliyor." biçiminde yeniden ifade edilmiştir. Güvenilir şifreleme sistemleri Kerckhoffs ilkesine uymalıdır. Bu prensibe göre, kriptanalist şifreleme anahtarı dışında sistem hakkındaki tüm detayları bilse dahi şifreleme sistemi güvenli olmalıdır. Özet olarak sistem, şifreleme, şifre çözme ve anahtar üretme algoritmaları bilinse dahi güvenli olmalıdır.

1.2.2. Şifreleme Algoritmalarının Sınıflandırılması

Modern şifreleme algoritmaları, şifrelemeyi ne şekilde yaptıklarına ve anahtarların gizli veya açık olma durumlarına göre farklı şekilde sınıflandırılabilirler [16, 17].

1.2.2.1. Şifreleme Yapısına Göre Sınıflandırma

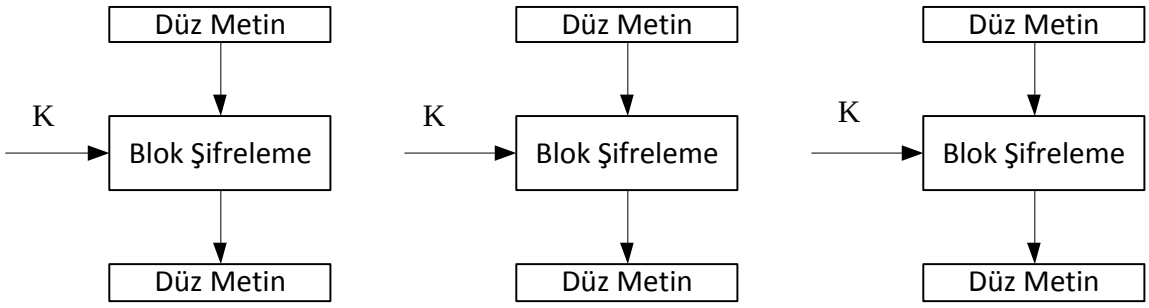
Şifreleme algoritmaları yapılarına göre, blok şifreleme ve akım şifreleme olarak sınıflandırılırlar. Blok şifrelemede sabit boyutlu bir düz metin bloğu aynı boyuttaki şifreli metin bloğuna dönüştürülür. Blok boyutları algoritmalarda farklılık göstermektedir. Büyük bloklu şifreleme algoritmalarında güvenlik daha fazladır, ancak daha karmaşık bir şifrelemeye sahip olduklarından dolayı performansları blok boyu ile ters orantılıdır. Modern blok şifreleme algoritmaları aşağıdaki özellikleri bulundurmalıdırlar [18].

1. Değişken anahtar boyu
2. Non-lineerliği sağlayan karıştırma işlemleri
3. Değişken düz metin ve şifreli metin blokları
4. Değişken döngü sayıları

Blok şifrelemelerde, bloklar algoritmanın yapısına göre birbirlerinden ayrı veya birbirlerine bağlı olarak şifrelenir. Blok şifreleme algoritmalarında anahtarın uzunluğu ya da anahtarın bit sayısı en temel saldırı olan kaba kuvvet ataklarına karşı yeterli uzunlukta olmalıdır. Örneğin DES algoritması 56-bit şifreleme anahtarına sahipken, AES algoritması DES'in bu zayıflığını örter niteliktedir ve 128, 192, 256 bit anahtar seçenekleri mevcuttur.

Blok şifrelemede birkaç farklı şifreleme modu vardır. Elektronik kod kitabı (ECB - Electronic Code Book) modunda aynı değerlere sahip bloklar, aynı şifreli metin bloklarına

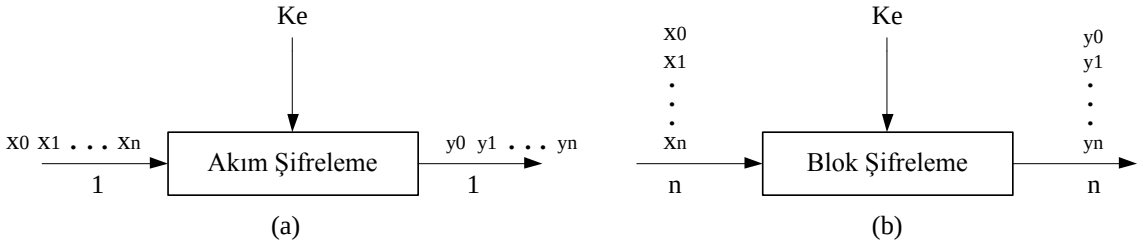
dönüştürülür. Bu durum, içeriğinde benzer bloklar bulunduran düz metinlerin bu modda şifrelenmesinin güvenli olmadığını gösterir. Bu düşük güvenliğin ortadan kaldırılabilmesi için şifre blok zinciri (CBC – Cipher Block Chaining), şifre geri besleme (CFB - Cipher FeedBack) ve çıktı geri besleme (OFB - Output FeedBack) gibi farklı blok şifreleme modları kullanılır. Şifre blok zinciri modunda her bir düz metin bloğuna bir önceki şifreli metin bloğu ile XOR işlemi uygulanır. Bu durum, elektronik kod kitabı modundaki aynı düz metin bloklarının aynı şifreli metin bloklarını üretmesi gibi güvenlik eksikliğini ortadan kaldırır. Aynı etki, şifre geri besleme modu ile de gerçekleştirilebilir. Elektronik kod kitabı modu, hesaplama karmaşıklığının diğer modlara göre daha düşük ve paralelleştirmeye uygun yapıya sahip olduğundan dolayı, diğer blok şifreleme modlarına göre daha performanslı çalışır. Şifrelemenin kullanım amacına göre tüm modların avantajları ve dezavantajları mevcuttur. Şekil 1.2'de Elektronik kod kitabı modunun çalışma prensibi gösterilmiştir.



Şekil 1.2. Blok şifrelemede elektronik şifre kitabı modu

Akım şifrelemede, birim zamanda büyük bloklar yerine bitler veya daha küçük düz metnin birimleri şifrelenir. Bundan dolayı blok şifrelerden daha hızlıdırlar. Genel olarak akım şifrelemede anahtar, kriptografik sözde rastgele sayı üreteçleri (CPRNG) ile bit dizisi olarak üretildikten sonra düz metin ile mantıksal olarak birleştirilir. Bu işlem genellikle XOR, XNOR, add, mod gibi operatörlerle gerçekleştirilir [19, 20, 21]. Günümüzde standartlaştırılmış bir akım şifreleme algoritması mevcut değildir. Şekil 1.3'de blok ve akım şifreleme arasındaki yapısal fark gösterilmektedir. Akım şifreleme algoritmaları aşağıdaki özelliklere sahiptir [22].

1. Çok yüksek güvenliğe sahip değillerdir
2. Güvenlik kriptografik sözde rastgele sayı üreteçlerine bağlıdır
3. CPRNG tahmin edilemez diziler oluşturmalıdır
4. Çok hızlıdırlar

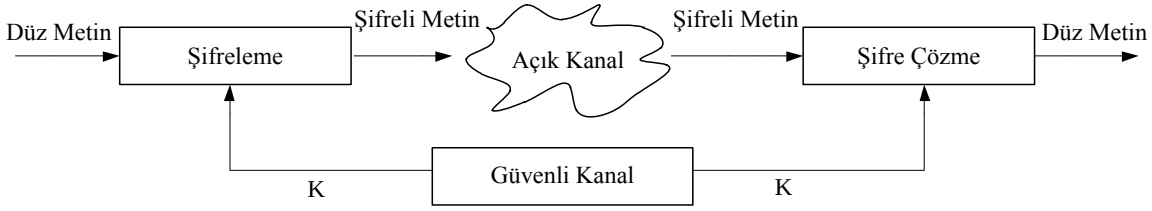


Şekil 1.3. Akım (a) ve Blok (b) şifreleme ile n adet bitin şifrelenmesi

1.2.2.2. Anahtara Göre Sınıflandırma

Şifreleme ve şifre çözme için iki anahtar K_e ve K_d sırasıyla kullanılmaktadır. Bu anahtarların birbirinin aynısı olduğu durumlarda algoritma, gizli anahtarlı şifreleme veya simetrik şifreleme olarak tanımlanmaktadır. Simetrik şifrelemede anahtar, haberleşen uç sistemler arasında göndericiden alıcıya güvenli bir kanaldan gönderilmelidir. Şifreleme ve şifre çözme anahtarlarının farklı olduğu durumlarda ise sistem açık anahtarlı veya asimetrik şifreleme olarak tanımlanmaktadır. Asimetrik şifrelemede şifreleme anahtarı K_e herkes tarafında bilinmekte, K_d şifre çözme anahtarı ise gizli olarak kalmaktadır.

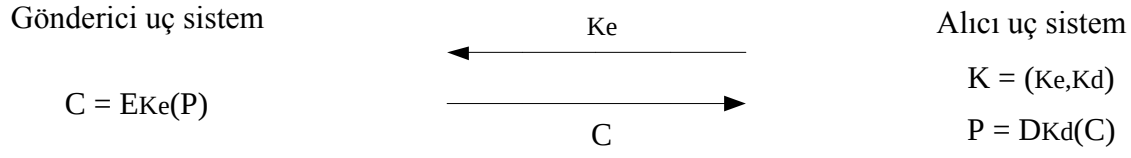
Simetrik şifrelemede Şekil 1.4'deki gibi gönderici taraf, düz metni şifreleme anahtarı ile şifreleyerek alıcıya gönderir. Alıcı aynı anahtar ile şifreyi çözüp, düz metni yeniden elde etmektedir.



Şekil 1.4. Simetrik şifrelemenin genel yapısı

Simetrik şifreleme sadece şifrelemeyle değil, kimlik denetimiyle de ilgilenir. Kimlik denetiminde kullanılan yöntemlerden biri Mesaj doğrulama kodu (MAC - Message Authentication Codes)´dur. Mesaj doğrulama kodları, sayısal imza ile benzer amaçlarla kullanılır. Ancak Mesaj doğrulama kodları ile kimlik denetimi için çift anahtarlı kriptografi yerine tek anahtarlı kriptografi, yani sadece üzerinde anlaşılan ortak anahtar kullanılır. Yani bu şekilde kimlik denetimini sadece istenilen kullanıcı yapabilir. Sayısal imzada olduğu gibi gönderenin açık anahtarına sahip herhangi birinin imzayı doğrulayabilmesi gibi bir durum söz konusu değildir. Gizli anahtarlı kriptografide temel problem, göndericinin ve alıcının üçüncü bir kişinin eline geçmesini engelleyerek ortak bir anahtar üzerinde anlaşmalarıdır. Bu durum, iki tarafın dinlenme korkusu duymadan iletişim kurmasını sağlayacak bir yöntem gerektirir. Gizli Anahtarlı şifrelemede kullanılan iki kullanıcının da anlaştığı anahtarın istenmeyen kişilerin eline geçmesi engellenmelidir. Anahtarların üretilmesi, iletilmesi ve saklanması anahtar yönetimi olarak bilinir.

Asimetrik şifrelemede, şifreleme ve şifre çözme anahtarları farklıdır. Açık anahtarlı kriptografi geleneksel kriptografinin anahtar dağıtım problemini çözmektedir [23, 24]. Açık anahtarlı kriptografi tek anahtar kullanan simetrik şifreleme algoritmalarının yerine, iki ayrı anahtarın asimetrik kullanımını öngörür. Bu sistemde alıcı taraf iki ayrı anahtara sahiptir. Bu anahtarlardan biri açık anahtar (public key) diğeri ise, özel anahtar (private key) olarak adlandırılır. Açık anahtar, bir tarafın şifreli iletişim kuracağı diğer taraflara iletilir, yani herkesin erişimine açıktır. Gizli anahtar ise sadece sahibinin erişebileceği şekilde gizli tutulmaktadır. Bu anahtarlar birbirlerine matematiksel bir ilişkiyle bağlanmıştır. Ancak anahtarlardan birini kullanarak diğerini bulmak çok zordur. Asimetrik şifreleme Şekil 1.5'de gösterilmektedir.



Şekil 1.5. Asimetrik şifrelemenin genel yapısı

Açık anahtarlı kriptografinin öncelikli avantajı, gizli anahtarın herhangi bir şekilde taşınması gibi bir durum söz konusu olmadığı için daha fazla güvenlik sağlamasıdır. Yani

gizli anahtar güvenliği konusuna çözüm getirmiştir. Bunun aksine gizli anahtarlı yapılarda, şifrelemede ve şifre çözmede kullanılan anahtar aynı olduğu için, gizli anahtarın el ile ya da iletişim kanalları üzerinden iletilmesi söz konusudur. Bu da gizli anahtarın istenmeyen kişiler tarafından elde edilmesi olasılığını ortaya çıkarır.

Açık anahtarlı yapıların diğer bir önemli avantajı reddedilemez sayısal imzalar oluşturabilmesidir. Gizli anahtarlı kriptografi kullanılarak yapılan kimlik denetiminde gizli bir bilginin açık bir ağ üzerinden veya üçüncü bir taraf aracılığıyla paylaşılması gerekmektedir. Bu durumda taraflardan biri, anahtarın diğerlerince kötü niyetle kullanıldığını iddia edebilir. Ancak açık anahtarlı yapılarda herkes kendi sayısal imzasından sorumlu olduğu için böyle bir durum söz konusu değildir. Bu özelliğe reddedilemezlik denir.

Açık anahtarlı yapıları kullanmanın bir dezavantajı şifreleme hızıdır. Çoğu gizli anahtarlı yapı açık anahtarlı yapılara göre daha hızlıdır. En güvenli ve hızlı yöntem iki yapıyı birlikte kullanmaktır. Açık anahtarlı yapılar, gizli anahtarlı yapıların yerine geçmeye aday değil, daha çok onları daha güvenli hale getirecek tamamlayıcı bir unsurdur. Örneğin, gizli anahtarları açık ağlar üzerinden taşımak için açık anahtarlı kriptografi kullanılır. Tablo 1'de simetrik ve asimetrik şifreleme yöntemlerinin karşılaştırılması yapılmıştır.

Tablo 1. Simetrik ve asimetrik şifreleme yapılarının karşılaştırılması

Simetrik Şifreleme	**Asimetrik Şifreleme**
Şifreleme ve şifre çözme için aynı anahtar kullanılır.	Şifreleme ve şifre çözme için farklı anahtarlar kullanılır.
Gönderici ve alıcı arasında anahtar paylaşımı gerekmektedir.	Gönderici ve alıcı birbirlerini tamamlayan iki anahtardan birine sahip olmalıdır.
Algoritma ve bir miktar düz metin bilgisi gizli anahtarı belirlemek için yeterli olmamalıdır.	Algoritma ve şifreleme anahtarı bilgisi şifre çözme anahtarını belirlemek için yeterli olmalıdır.
Gizli anahtar güvenli bir şekilde saklanmamalıdır.	Şifre çözme anahtarı güvenli bir şekilde saklanmalıdır.

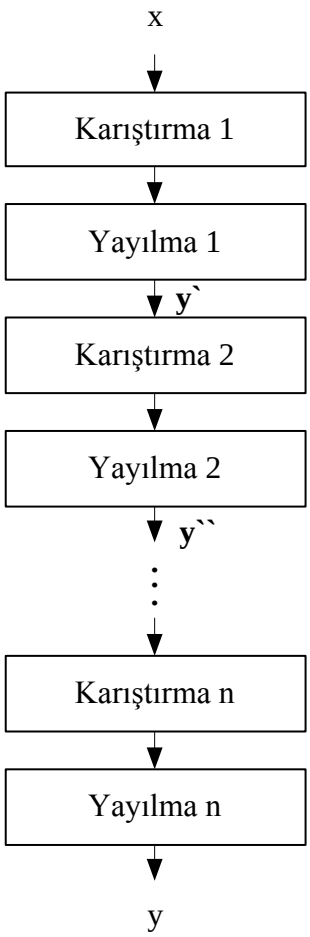
1.3. Karıştırma ve Yayılma

Cloude Shannon “Gizli sistemlerin haberleşmesi” [25] adlı makalesinde güçlü şifreleme algoritmalarının, karıştırma (confusion) ve yayılma (diffusion) tekniklerini temel alması gerektiğini vurgulamıştır.

Karıştırma, anahtar ve düz metin arasındaki ilişkin belirsizleştirilme işlemidir. Genel olarak karıştırmayı gerçekleyebilmek için yerine koyma (substitution) teknikleri kullanılmaktadır. Karıştırmadaki amaç düz metin blokları ile şifreli metindeki bloklar arasındaki istatistiksel bağlantının ortadan kaldırılmasıdır.

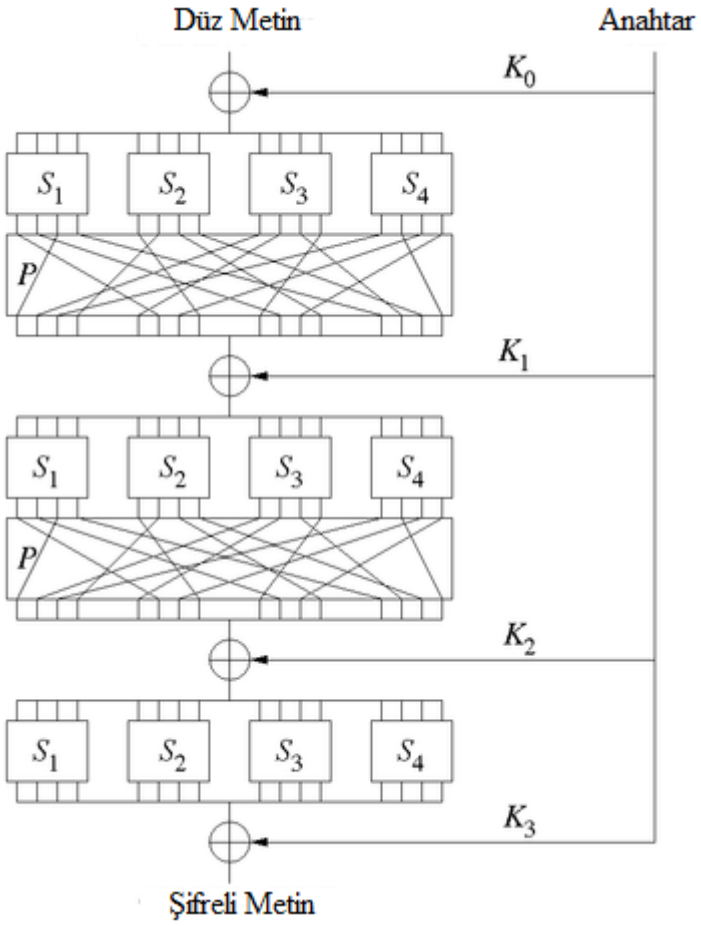
Yayılma, düz metnin tek bir sembolünün şifreli metin üzerindeki birçok sembol üzerinde etkili olmasıdır. Buradaki amaç düz metnin istatistiksel özelliklerini saklamaktır. Böylece kriptanalist benzer düz metin ve şifreli metin çiftleri üzerinde analiz yapsa da, şifreli metne denk gelen düz metin hakkında tahmin yapamaz.

Günümüzde tüm blok şifreleme sistemleri sırasıyla her iki işlemi de Şekil 1.6’daki gibi veriye uygulamaktadır. Sadece karıştırma ve sadece yayılma işlemini gerçekleştiren sistemler güvenli değildir. Her iki işlemi gerçekleştirerek çok güvenli şifreleme sistemleri kurulabilir.



Şekil 1.6. Genel bir şifreleme yapısında sırasıyla karıştırma ve yayılma

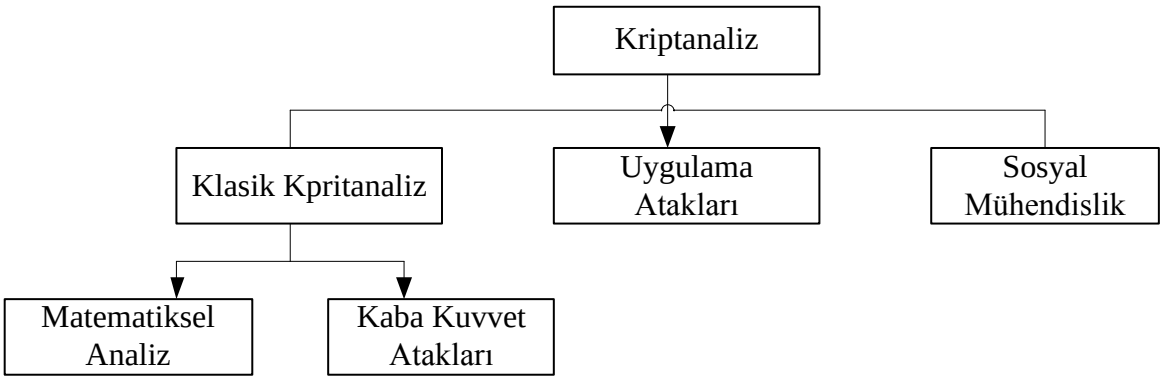
Karıştırma ve yayılmanın her ikisini de gerçekleştirebilmek için basit bir yol yerine koyma karıştırma ağıdır (SPN – Substitution - Permutation Network). Yerine koyma yer değiştirme ağları, AES gibi bazı şifreleme algoritmalarının yapısında bulunur. Yerine koyma ve yer değiştirme ağ yapısında anahtar ve bir düz metin bloğu girdi olarak alınarak birden fazla döngü içinde, bu girdilere yerine koyma kutuları (Substitution-Box) ve yer değiştirme kutuları (Permutation-Box) uygulanır. Bu şekilde karıştırma ve yayılma aşamaları sağlanmış olur. Şekil 1.7'de iki döngülü bir yerine koyma yer değiştirme ağı gösterilmektedir.



Şekil 1.7. İki döngülü bir yerine koyma yer değiştirme ağı

1.4. Kriptanaliz

Kriptanaliz, kriptografik sistemleri kırma bilimidir. Kriptanaliz modern kripto sistemler için büyük önem taşımaktadır. Şifreleme metotlarının analizlerinin yapılmadığı bir durumda, algoritmaların güvenli olup olmadıkları hakkında bilgi sahibi olamayız. Kriptografik sistemlerin güvenli olduklarından emin olmanın tek yolu güvenlik analizlerinin yapılmasıdır. Şifreleme sistemlerini kırmak için birçok yöntem vardır. Bu yöntemlerin genel sınıflandırılması Şekil 1.8'de gösterilmiştir.



Şekil 1.8. Kriptanalizin sınıflandırılması

Klasik kriptanaliz, şifreli metinden düz metni elde etmeye veya şifreli metinden anahtarı elde etmeye çalışır. Matematiksel analiz ile eldeki veriler değerlendirilip şifreleme metodunun yerel yapısının incelenmesi suretiyle bilgi elde edilmeye çalışılır.

Yalnız şifreli metin saldırısı, (ciphertext only) sadece şifreli metin bilgisine dayanılarak yapılır. Düz metin ve anahtar bilgisine sahip olmayan kriptanalist, biraz şifreli metin hakkında bilgiye sahiptir. Bu durumda tahmin edilen düz metinler elde edilmeye çalışılır.

Bilinen düz metin saldırısı, (known plaintext) bilinen bir miktar düz metin şifreli metin çiftlerine dayanarak yapılır. Bu durumda uygun düz metin farklı anahtarlar ile şifrelenerek eldeki şifreli metin elde edilmeye çalışılır. Böylece anahtar tahmin edilebilir.

Seçilmiş düz metin saldırısı, (chosen plaintext) bilinmeyen anahtarı elde etmeyi amaçlar. Kriptanalist düz metinleri herhangi bir anahtarla şifreleyip, elde ettiği şifreli metinleri düz metinlerle karşılaştırarak anahtarı elde etmeye çalışır. Bu atağın en çok bilinen örneği, blok şifrelere ve hash fonksiyonlarına karşı uygulanabilen diferansiyel kriptanalizdir [48].

Kaba Kuvvet ataklarında ise anahtar uzayındaki mümkün olan tüm anahtarlar denenerek şifre kırılmaya çalışılır. Günümüzde çok hızlı bilgisayarların ortaya çıkmasıyla kaba kuvvet ataklarına karşı koyabilmek için anahtar boyları daha büyük sistemler geliştirilmektedir.

Uygulama ataklarında, algoritmanın koşulduğu donanımdan faydalanılarak gizli anahtar elde edilmeye çalışılır. Örneğin gizli anahtar üzerinde işlem yaparken merkezi işlem biriminin çektiği akım ölçülerek gizli anahtar elde edilebilir.

Sosyal Mühendislikte gizli anahtar insanlar tarafından şantaj, kandırma gibi yöntemlerle elde edilebilir.

1.5. Kaotik Sistemler

Kaotik sistemler, bir önceki periyottan elde edilen çıktının bir sonraki periyot için girdi olarak kullanıldığı geri beslemeli dinamik sistemlerdir. Değişkenler arasındaki ilişki doğrusal olmadığından dolayı, girdi ve çıktı arasındaki ilişki orantılı değildir. Birçok farklı girdinin sürekli değişerek fiziksel değişimler ve farklı düzenler yaratması ve bu düzenlerin yine kendisini etkilemesi, insan zekasının ve günümüzdeki gözlem ve bilimsel tahmin yeteneklerinin çok üstünde olmasından dolayı kaos olarak nitelendirilmektedir. Kaotik sistemler tüm girdileri değerlendirip, ona göre nihai bir davranış ortaya koyarlar.

Bir kaotik sistemde değişkenler arasındaki ilişki, önemsiz görünen değişkenler ve sistemin başlangıç koşulları, sistemin davranışı açısından büyük önem taşımaktadır. Kaos teorisi başlangıç koşullarındaki küçük değişikliklerin sistemin yörüngesindeki zamana bağlı değişimlerini inceler. Değişkenlerin çok sayıda olması, ortamı kaotik yapan temel etkendir. Kaotik terimi, insanın hesaplamaya muktedir olmadığı, son derece karmaşık, ama kendi iç düzenine sahip bir süreç olarak tanımlanabilir. Kaotik hareketin, rastgele her durumu alamadığı, yalnız belli bir olasılıklar kümesi içerisinde cereyan ettiği ortaya konmuştur. Yani kaos, oldukça karmaşık olmasına rağmen, aslında kendi içinde bir düzene sahiptir. Bu durum deterministik kaos olarak bilinir. Aynı zamanda nedeni ve seyri bilinemeyen, hesaplanamaz olan rastlantısal kaos kavramı da mevcuttur. Ancak kriptografinin ilgilendiği deterministik kaostur.

1.5.1. Ayrık Dinamik Sistemler

Dinamik sistemler, sistemin durumunu belirten bir noktanın geometrik uzayda zamana olan bağımlılığı ile devamlı gelişen sistemlerdir. Herhangi bir zamanda, dinamik

bir sistem gerçek sayılardan oluşan bir duruma sahiptir. Bulunduğu durum uzayında o andaki durumu bir noktayla gösterebilir. Dinamik sistemlerin mevcut durumdan nasıl başka bir duruma geçeceklerini açıklayan gelişim kuralları vardır. Bu gelişim kuralları deterministikdir.

Ayrık zamanlı dinamik bir sistem iteratif bir haritalamadır. Tamsayı kümesinin elemanı olan iterasyon sayısı t, sonraki iterasyonlara da atanabilir bir değerdir. Bir X metrik uzayının (X, f) çiftin de f: X→X fonksiyonu, dinamik sistemin ayrık *t* zamanında durumunu belirlemeyi işaret eder. Burada t doğal bir sayıdır ve ayrık-zamanlı dinamik bir sistemin zamanını gösterir. Dinamik bir sistemin başlangıç koşulundan itibaren durum uzayında izlediği noktalar, o dinamik sistemin yörüngesidir. Bir dinamik sistemde her $x \in X$; n, m = 0,1,2, … için $f^0(x) = x$ birim fonksiyondur. $f^n = f \circ f \circ ... \circ f$, f fonksiyonunun n haritalamasının bileşkesidir. $\{ f^n(x)\}$ dizisi n = 0,1,2,… için x noktasının, bulunduğu dinamik sistemdeki yörüngesini gösterir.

1.5.2. Kaotik Sistemlerin Özellikleri

Kaos teorisi başlangıç koşullarına büyük ölçüde duyarlı olan dinamik sistemlerin davranışlarını inceleyen bir çalışma alanıdır. Kaotik sistemlerin zamana bağlı değişimleri uzun vadede tahmin edilememektedir. Ancak bu değişim deterministiktir ve başlangıç koşullarıyla belirlenir. Kaotik sistemlerin bu belirlenebilir doğal yapıları, bu sistemleri tahmin edilebilir yapmamaktadır [26]. Ayrık kaotik bir sistem (3)'deki gibi iteratif bir f fonksiyonuyla (kaotik harita) ve I durum uzayıyla tanımlanır.

$$x_{n+1} = f(x_n) \tag{3}$$

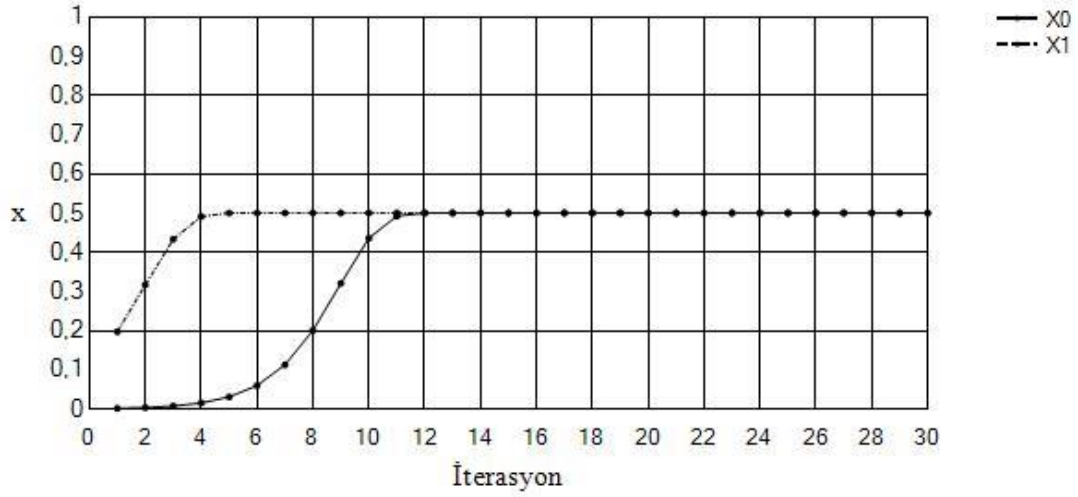
Burada $x_n \in I$ ayrık bir zamanda sistem durumunu gösterir. Kaotik bir harita kendi durum uzayını yine kendi durum uzayına haritalar. Kaotik sistemler kontrol parametreleri ile kontrol edilirler. Gerçek dünyada bu parametreler yörünge boyunca sabit kalmayabilir. Kaotik üretecin çıkışı, kaotik bir dizi ortaya çıkararak kaotik sistemin zamanla değişen durumunu gösterir.

Dinamik bir sistemin kaotik olarak tanımlanabilmesi için başlangıç koşullarına duyarlılık, topolojik geçişkenlik ve periyodik noktaların yoğunluğu şartlarının tümünü sağlaması gerekmektedir [27] .

1.5.2.1. Başlangıç Koşullarına Duyarlılık

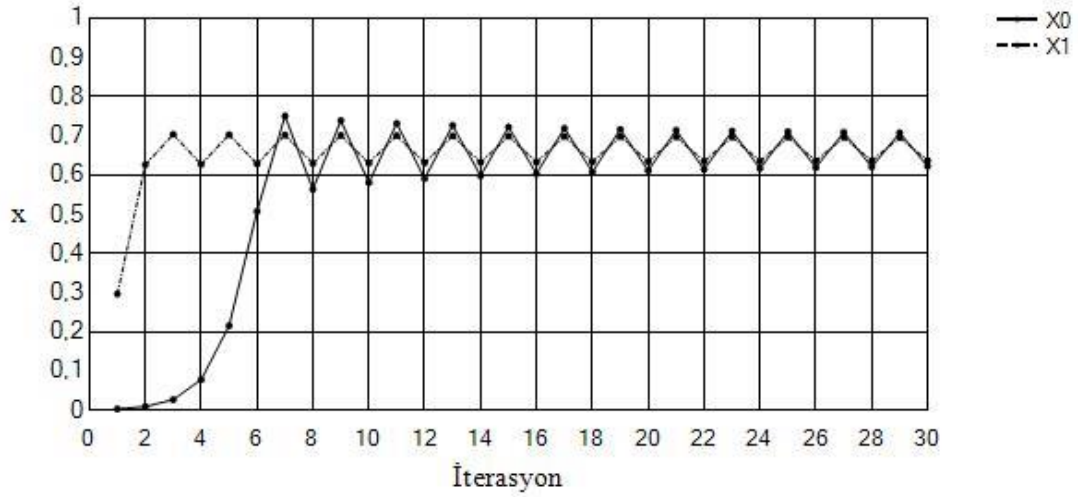
Başlangıç koşullarına duyarlılık, mevcut sistemdeki her bir noktanın yörüngesinin diğer noktaların yörüngelerinden farklı olmasıdır. Mevcut sistemin başlangıç koşullarındaki en ufak bir değişim, sistemlerin farklı yörüngeler izlemesine neden olur. Bu değişim, sistemlerin zaman serileri incelenerek gözlemlenebilir.

Dinamik bir sistemin kaotik davranışlar sergilediği durumlarda, bu sistemin izlediği yörünge tahmin edilemez. Sistemin kaotik davranış göstermediği durumlarda sistem ya bir noktaya doğru çekilir ya da *n* periyotluk bir yörünge üzerine oturur. Başlangıç koşulları ne olursa olsun kontrol parametreleri sistemin kaosa girmesi için uygun değilse, sistem bir süre sonra tüm başlangıç koşulları için aynı davranışları sergilemeye başlar. Şekil 1.9'da (5)'deki logistic haritanın yörüngesi kontrol parametresi r = 2 durumunda, herhangi iki farklı başlangıç değeri için tek bir noktaya doğru çekilmektedir [28]. Bu durumda sistem tek bir noktada kararlıdır.



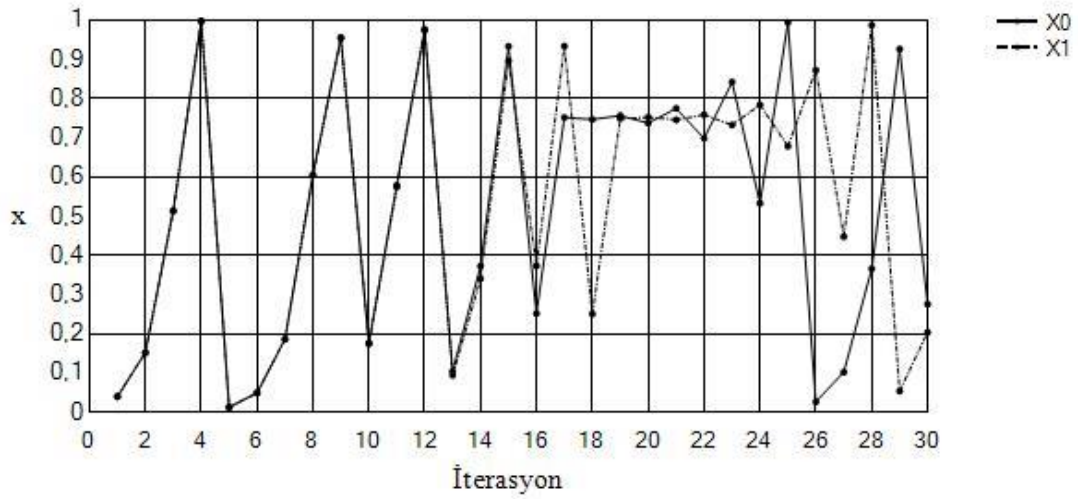
Şekil 1.9. Logistic haritanın r = 2 kontrol parametresi için zamanla davranışı

Şekil 1.10'da logistic haritanın yörüngesi r = 3 kontrol parametresi ile iki periyotlu bir yörüngeye doğru çekilmektedir. Bu durumda sistem iki periyotlu bir yörüngede kararlıdır.



Şekil 1.10. Logistic haritanın r = 3 kontrol parametresi için zamanla davranışı

Bir noktada veya belirli bir periyodda kararlı olan dinamik sistemler kaotik davranış göstermezler. Bu sistemler tahmin edilebilir sistemlerdir. Çünkü tüm başlangıç koşulları için bir süre sonra benzer davranışları gösterirler. Kaotik ortamda ise sistemler tamamen kararsızdır. Herhangi bir nokta veya periyot üzerinde kararlı olmadıklarından dolayı, birbirine çok yakın başlangıç koşullarında dahi yörüngeler birbirinden farklı ve tahmin edilemezdir. Bu durum kriptografi için olmazsa olmaz bir özelliktir. Şekil 1.11'de logistic harita, r = 3,99 kontrol parametresi ile birbirine çok yakın iki başlangıç değeri için bir süre sonra farklı davranışlar göstermeye başlar. Sistemin bu durumdaki davranışı tüm başlangıç değerleri için farklı ve düzensizdir. Bundan dolayı kararsız olan kaotik sistemlerin davranışları tahmin edilemez.

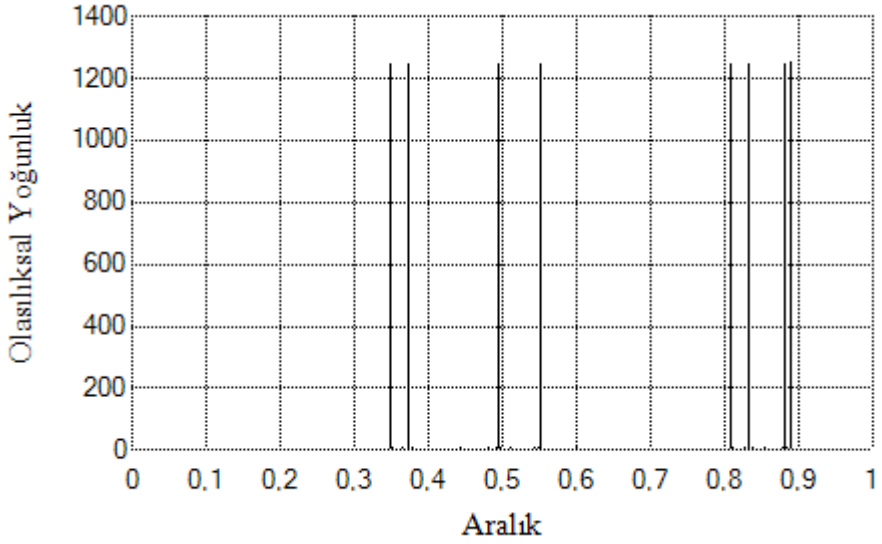


Şekil 1.11. Logistic haritanın r = 3,99 kontrol parametresi için zamanla davranışı

1.5.2.2. Topolojik Geçişkenlik

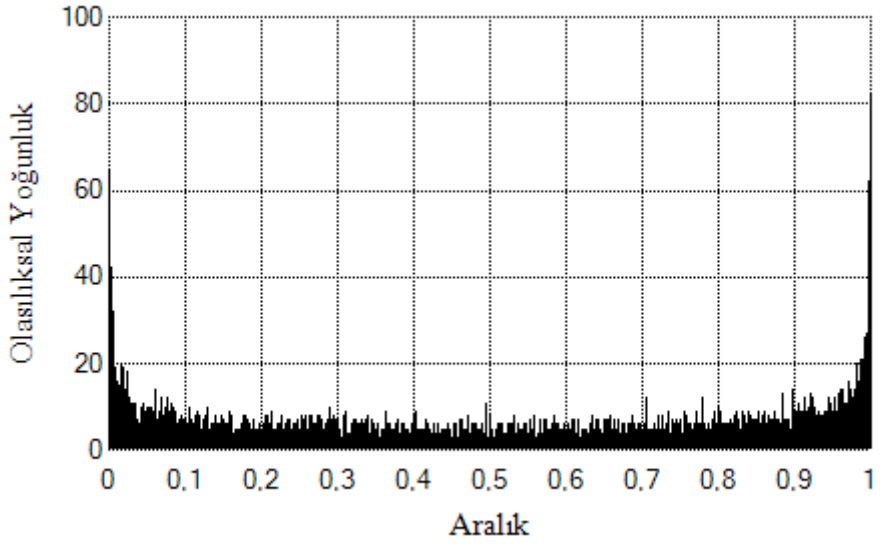
Topolojik geçişkenlik, zamanla gelişen kaotik bir sistemin tanımlı olduğu aralıkta tüm alt bölgeleri ziyaret etmesi olarak ifade edilir. Tüm alt bölgeleri ziyaret eden sistem yörüngesinin bu davranışı, düzensiz ve tahmin edilemez olduğu gibi deterministiktir. R gerçek sayılar kümesinde tanımlı f: R→R fonksiyonu ve R kümesinde I ve J gibi iki açık küme için k > 0 ve $f^k(I) \cap J \neq 0$ ise sistem topolojik geçişkendir denir.

Kaotik sistemlerin tanımlı oldukları alanda, tüm başlangıç değerlerinin yoğun bir yörüngesi vardır. Bu yörünge sistemin tüm alt alanlarını ziyaret eder. Şekil 1.12'de logistic haritanın r = 3,56 kontrol parametresi için yörüngesinin olasılıksal dağılımı gösterilmektedir. Sistem yörüngesi sistemin tanımlı olduğu bölgede sadece belli alt alanlarda yoğun olduğu için, sistem bu parametre ile kaotik özellik göstermemektedir.



Şekil 1.12. Logistic haritanın r = 3,56 parametresi için yörüngenin olasılıksal dağılımı

Şekil 1.13'de logistic haritanın r = 3,999 kontrol parametresi için sistem yörüngesinin olasılıksal dağılımı gösterilmektedir. Sistem kaosa girdiğinde yörünge düzensiz davranışlar ile tüm komşu alt bölgeleri ziyaret eder. Bu durum sistemin tanımlı olduğu alanın tüm alt alanlarında, sistem yörüngesinin yoğun olduğunu göstermektedir. Bu olasılıksal dağılım sistem kaosa girdiğinde tüm başlangıç koşulları için benzerdir.



Şekil 1.13. Logistic haritanın r = 3,999 parametresi için yörüngenin olasılıksal dağılımı

1.5.2.3. Periyodik Noktaların Yoğunluğu

Dinamik sistemlerde yörünge, sistemin gelişim fonksiyonuna bağlı noktalar kümesidir. Periyodik noktaların yoğunluğu, sistem uzayındaki her bir noktanın zamanla periyodik bir yörüngeye yaklaşmasıdır. Sistemin tanımlı olduğu uzayda seçilen iki nokta arasındaki mesafe ne kadar küçük olursa olsun, bu mesafe içinden en az bir periyodik yörünge geçmektedir. R gerçek sayılar kümesinde tanımlı f: R→R fonksiyonu için $f^n(x_0) = x_0$, n > 0 ise x_0 noktası periyodik bir noktadır ve sistem n periyotluk bir yörüngeye sahiptir. Başlangıç koşullarına duyarlı bir sistem topolojik geçişkenliğe sahip değilse ve periyodik yörüngeleri yoğun olmayan bir sistemse kaotik davranış göstermemektedir.

1.5.3. Bir Boyutlu Kaotik Sistemler

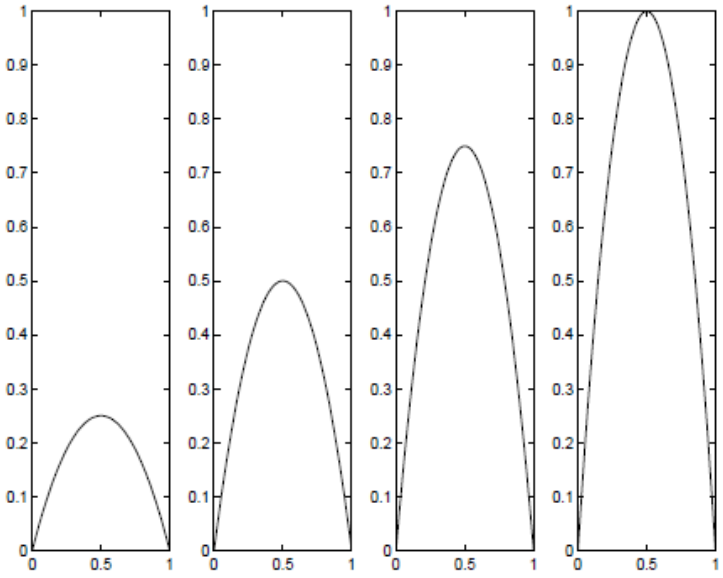
Bir boyutlu ayrık kaotik sistemler karmaşık özellik gösterebilen basit sistemler olduklarından kaosu anlayabilmek için üzerlerinde oldukça fazla çalışılma yapılmıştır. Kaotik sistemlerin basit bir sınıfı olan 1 boyutlu kaotik haritalar bir fark denklemi şeklinde (4)'deki gibi ifade edilebilir.

$$x_{n+1} = f(x_n, r), n = 0,1,2,3 \ldots \quad (4)$$

Burada x durum değişkeni ve r sistemin kontrol parametresidir. Sistemin x_{n+1} değeri sadece x_n değişkeni tarafından belirlenmektedir. Logistic harita (5) belirli şartlarda kaotik özellik gösteren 1 boyutlu polinomsal bir haritadır. Logistic harita kaotik davranışı gözlemleyebilmek için özellikle bu çalışmada seçilmiş ve resim şifrelemenin yayılma aşamasında kullanılmıştır.

$$x_{n+1} = r\, x_n\, (1 - x_n) \quad (5)$$

Burada r kaotik davranışı kontrol eden kontrol parametresi, n ise ayrık zaman durumunu göstermektedir. Sistem durumu olan x_n değerinin [0,1] aralığında olması için, r [0,4] aralığında olmalıdır. Şekil 1.14'de kontrol parametresi r'nin farklı değerleri için logistic haritanın polinomsal grafikleri gösterilmektedir.



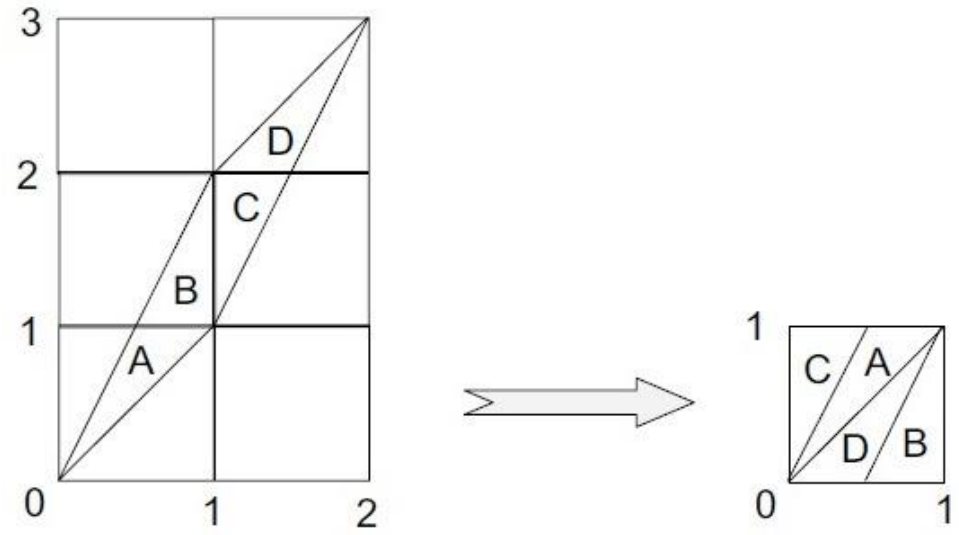
Şekil 1.14. Logistic haritanın sırasıyla r = 1, 2, 3, ve 4 değerleri için grafikleri

1.5.4. İki Boyutlu Kaotik Sistemler

Çok boyutlu kaotik haritaların basit yapıları olan 2 boyutlu haritalar, kaotik özellik gösteren ve üzerlerinde birçok çalışma yapılmış haritalardır. 2 boyutlu haritalar doğal yapılarından dolayı kaotik resim şifrelemeye çok uygundurlar. En çok bilinen 2 boyutlu kaotik haritalardan biri Arnold cat haritası (6)'daki gibi ifade edilir [29].

$$\begin{bmatrix} x_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_n \\ Y_n \end{bmatrix} \bmod 1 \tag{6}$$

Tersi (7)'deki gibi alınabilen 2 boyutlu Cat haritası tanımlı olduğu bölgeyi korur. Karakteristik özelliklerinden biri uzatma (stretch) ve katlama (fold) mekanizması olan kaotik cat haritasının geometrik gösterimi Şekil 1.15'deki gibidir.



Şekil 1.15. Arnold cat haritasının uzatma ve katlama yapısı

$$\begin{bmatrix} x_n \\ Y_n \end{bmatrix} = \begin{bmatrix} 1+ab & -a \\ -b & 1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ Y_{n+1} \end{bmatrix} \bmod 1 \tag{7}$$

R gerçek sayılar kümesi olmak üzere eğer $R^n \rightarrow R^n$'de tanımlı bir f haritası $m\left(f^{-1}(A)\right) = m(A)$ şartını sağlıyorsa, bu harita alan korumalı bir haritadır. Burada A R^n'de bir alt bölgedir, m(A) A'nın n boyutu ölçüsüdür. Bir doğrusal dönüşüm eğer determinantı 1 ise, alan korumalıdır. Yani haritalama 2 boyutlu bir uzayda her zaman kendi içine olmaktadır.

1.5.5. Sabit Noktalar ve Periyodik Yörüngeler

Sabit bir nokta olan x, $x_{n+1} = f(x_n)$ fonksiyonunda $x = f(x)$ şeklinde gösterilir. Eğer $n > 0$ olacak şekilde $f^n(x) = x$ ve $0 \leq k \leq n$ olacak şekilde $f^k(x) \neq x$ ise, x noktasının n periyotluk çekici bir nokta olduğunu söyleyebiliriz.

İtici ve çekici olmak üzere iki çeşit sabit nokta vardır. Örneğin $f(x) = x^2$ fonksiyonunda 0 ve 1 sabit noktalardır. Bu sabit noktalara yakın bölgelerde, fonksiyon yörüngesinin ne şekilde olduğu incelendiğinde itici ve çekici noktalarının tespiti mümkündür. Eğer bu fonksiyonda $x_0 = 0.1$ olacak şekilde x_0 noktasını seçersek, yörünge 0.1, 0.01, 0.0001, 0.00000001, … olacak şekilde sıfır noktasına çekilir. Gerçekte $0 \leq x_0 < 1$ olacak şekilde seçilen herhangi bir x_0 noktası 1 noktasından uzaklaşarak 0

noktasına doğru çekilir. Burada 0 çekici, 1 ise itici noktalardır. Bir boyutlu logistic haritanın sabit noktaları (8)'deki gibi hesaplanabilir.

$$x_{1/2} = \frac{-(1-r) \pm (1-r)}{2r} \tag{8}$$

Sabit noktalarda olduğu gibi periyodik noktalarda çekici, itici ve nötr olarak sınıflandırılabilir. Örneğin $f(x) = x^2 - 1$ fonksiyonu 0,-1,0,-1,… yörüngesinde 2 periyotluk bir döngüye sahiptir. Tablo 2'de farklı kontrol parametreleri için logistic haritanın ürettiği değerler gösterilmektedir. Bu değerler incelenerek sistemin hangi noktalarda veya periyotlarda kararlı olduğunu veya sistemin kararlı olup olmadığını olduğunu gözlemleyebiliriz.

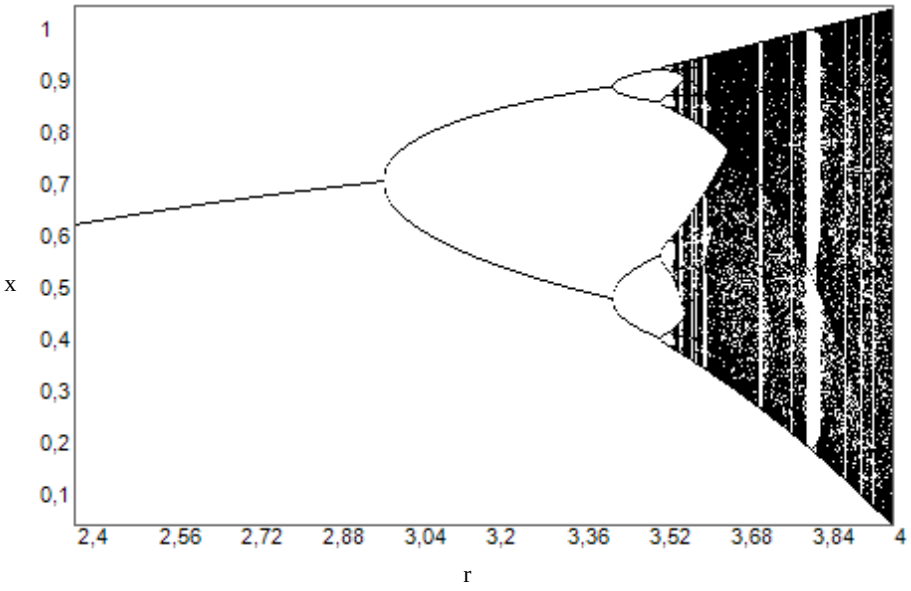
Tablo 2. Farklı r kontrol parametre değerleriyle logistic haritanın yörüngeleri

n	r = 0.5	r = 2.0	r = 2.7	r = 3.2	r = 3.5	r = 3.8
1	0.1000	0.1000	0.1000	0.1000	0.1000	0.1000
2	0.0450	0.1800	0.2430	0.2880	0.3150	0.3420
3	0.0215	0.2952	0.4967	0.6562	0.7552	0.8551
4	0.0105	0.4161	0.6750	0.7219	0.6470	0.4707
5	0.0052	0.4859	0.5923	0.6424	0.7993	0.9467
6	0.0026	0.4996	0.6520	0.7351	0.5614	0.1916
7	0.0013	0.5000	0.6126	0.6231	0.8618	0.5886
8	0.0006	0.5000	0.6407	0.7515	0.4168	0.9202
9	0.0003	0.5000	0.6215	0.5975	0.8508	0.2790
10	0.0002	0.5000	0.6351	0.7696	0.4443	0.7645
11	0.0001	0.5000	0.6257	0.5675	0.8641	0.6842
12	0.0000	0.5000	0.6323	0.7854	0.4109	0.8211
13	0.0000	0.5000	0.6277	0.5393	0.8472	0.5583
14	0.0000	0.5000	0.6310	0.7951	0.4531	0.9371
15	0.0000	0.5000	0.6287	0.5214	0.8673	0.2240
16	0.0000	0.5000	0.6303	0.7985	0.4029	0.6606
17	0.0000	0.5000	0.6292	0.5148	0.8420	0.8519
18	0.0000	0.5000	0.6300	0.7993	0.4657	0.4793
19	0.0000	0.5000	0.6294	0.5133	0.8709	0.9484
20	0.0000	0.5000	0.6298	0.7994	0.3936	0.1861
21	0.0000	0.5000	0.6295	0.5131	0.8353	0.5755
22	0.0000	0.5000	0.6297	0.7995	0.4814	0.9284
23	0.0000	0.5000	0.6296	0.5131	0.8738	0.2527
24	0.0000	0.5000	0.6297	0.7995	0.3860	0.7177
25	0.0000	0.5000	0.6296	0.5130	0.8295	0.7699
26	0.0000	0.5000	0.6296	0.7995	0.4950	0.6731
27	0.0000	0.5000	0.6296	0.5130	0.8749	0.8362
28	0.0000	0.5000	0.6296	0.7995	0.3830	0.5206
29	0.0000	0.5000	0.6296	0.5130	0.8271	0.9484
30	0.0000	0.5000	0.6296	0.7995	0.5005	0.1860

1.5.6. Dallanma Diyagramı

Dinamik sistemlerde dallanma, sistem parametreleri değiştikçe sistem davranışının niteliksel bir değişimidir. Bazı parametreler kümesinde sistem sabit bir noktada veya periyodik bir yörüngede kararlıdır. Ancak bazı parametre kümelerinde sistem kararsızdır. Dallanma, sistem kararlı durumdayken kontrol parametrelerinin değişmesiyle yeni sabit noktaların ve periyodik yörüngelerin ortaya çıkması olarak tanımlanır.

Ayrık dinamik sistemlerde periyot çiftlemesi, mevcut sistemin o andaki yörüngesinin periyot sayısını ikiye katlaması ile yeni bir davranış göstermesidir. Logistic haritanın dallanma diyagramı Şekil 1.16'da gösterilen grafikteki gibidir.

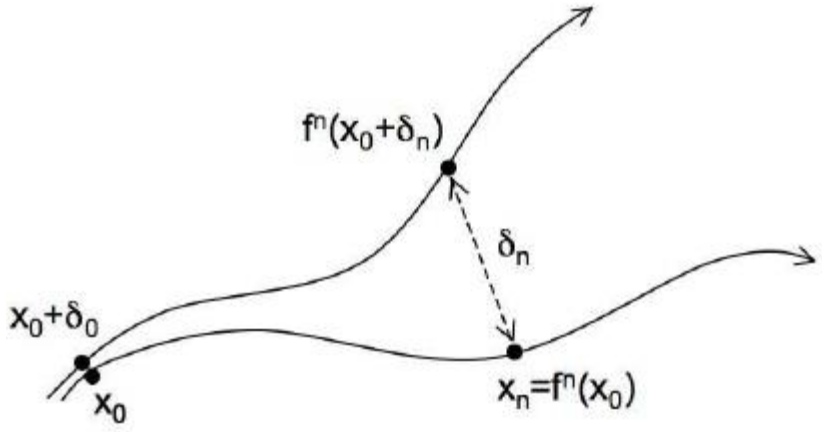


Şekil 1.16. Logistic haritanın dallanma grafiği

Logistic haritanın dallanma grafiği incelendiğinde herhangi bir $x_0 \in [0,1]$ ve $r > 0$ için $f^n(x)$, $n \to \infty$ durumunda sistemin davranışı gözlemlenebilmektedir.
Kontrol parametresi $0 < r < 1$ için sistemin bir tek $x = 0$ sabit noktası vardır. $1 < r < 3$ durumunda, $f(x) = x$ çözüldüğünde sistemin $x = 0$ ve $x = 1 - 1/r$ noktalarında iki adet sabit noktası olduğu görülmektedir. Kontrol parametresi $r > 3$ durumundan sonra sistem periyodu devamlı 2^n şeklinde çiftlenerek artmaktadır.

1.5.7. Lyapunov Üstelleri

Kaotik dinamik sistemler başlangıç koşullarına duyarlı sistemlerdir. Dinamik sistemlerin başlangıç koşullarına olan duyarlılıklarının ölçümü lyapunov üstelleri ile ifade edilebilir. Lyapunov üstelleri dinamik sistemlerde, komşu yörüngelerin birbirlerine yaklaşma veya uzaklaşma durumlarını inceleyerek, başlangıç koşullarından uzaklaşma oranlarını Şekil 1.17'deki gibi verir. Eğer sistem n boyutlu ise n adet lyapunov üsteli vardır.



Şekil 1.17. Kaotik bir sistemin yakın noktalarına ait yörüngelerin zamanla uzaklaşması

R gerçek sayılar kümesinde tanımlı $f : R \to R$ dinamik sisteminde $x_0$ve y_0 farklı birer nokta ve aralarındaki uzaklık $\delta = |y_0 - x_0|$ olsun. Bir iterasyondan sonra yeni uzaklık $\delta_1 = |y_1 - x_1|$ ve $y_1 = f(y_0)$, $x_1 = f(x_0)$ olarak hesaplanır. Eğer Λ'yi $\delta_1 = e^{\Lambda}\delta$ olarak tanımlarsak, Λ bir iterasyon sonucunda δ uzaklığından δ_1 uzaklığına olan büyümenin üstel oranını ölçer ve n iterasyon sonunda δ_n uzaklığı (9)'daki gibi hesaplanır.

$$\delta_n = |f^n(x_0) - f^n(y_0)| = \delta e^{n\Lambda} \tag{9}$$

Bu denklem (10)'daki gibi ifade edilebilir.

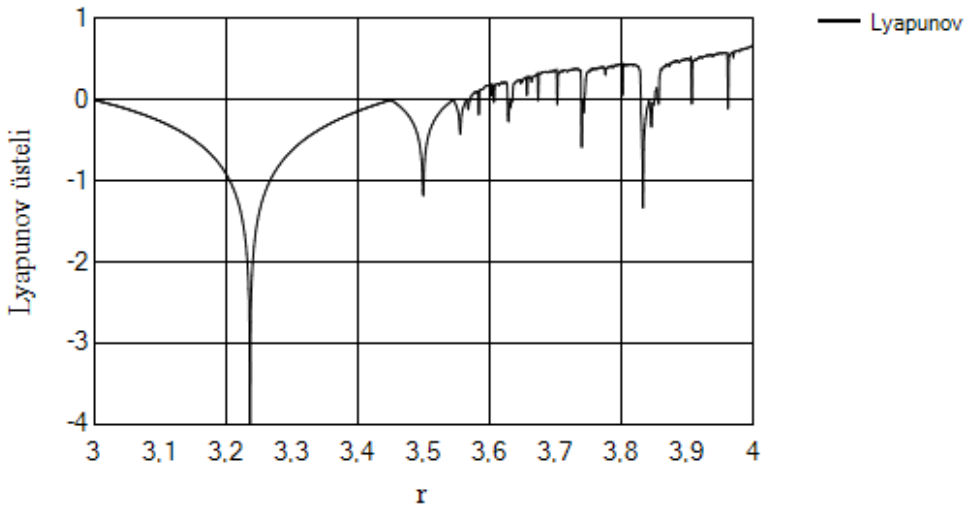
$$\Lambda = \left(\frac{1}{n}\right) \ln |f^n(x_0) - f^n(y_0)|\delta \tag{10}$$

Ölçülemeyecek kadar yakın başlangıç koşullarının uzaklığı δ olarak dikkate alındığında, kaotik ayrık dinamik sistemlerin lyapunov üsteli (11)'deki gibi hesaplanabilir [30].

$$\Lambda(x_0) = \lim_{n\to\infty} \lim_{\delta\to 0} \left(\frac{1}{n}\right) \ln\{|[f^n(x_0 + \delta) - f^n(x_0)]/\delta|\} \tag{11}$$

Kaotik ortamda lyapunov üsteli pozitif değere sahiptir. Lyapunov üstelinin değerindeki pozitif artış başlangıç koşullarına olan duyarlılığın daha fazla olduğunu göstermektedir. Lyapunov üstelinin negatif olduğu durumlarda, sistem sabit bir noktaya veya periyodik bir yörüngeye çekilir. Lyapunov üstelinin sıfıra eşit olduğu durumlar ise sistemin kararlı olduğunun göstergesidir.

Tüm çok boyutlu kaotik sistemlerin en az bir pozitif lyapunov üsteli ve çekiciyi sınırlandırmak içinde en az bir negatif lyapunov üsteli olmalıdır. Çok boyutlu kaotik sistemlerin lyapunov üstellerinin toplamı negatiftir. Şekil 1.18'de 1 boyutlu logistic haritanın, farklı r kontrol parametre değerlerine göre lyapunov üstellerinin grafiği gösterilmektedir. Bu grafikten logistic haritanın kaotik davranış gösterdiği parametre değerleri gözlemlenebilir. Lyapunov üstelinin pozitif değeri arttıkça kaotik özellikte artmaktadır. Yani sistemin en yüksek lyapunov üsteli değerine sahip olduğu durum, en fazla kaotik özellik gösterdiği durumdur.



Şekil 1.18. Logistic haritanın lyapunov üstellerinin r =[3,4] durumundaki grafiği

1.5.8. Tahmin Edilememezlik ve Rastgelelik

Rastgelelik denilince ilk akla gelen, birbirinden bağımsız rastgele üretilmiş ve aralarında herhangi bir fonksiyonel ilişkinin olmadığı sayılar dizisidir. Tahmin edilemezlik ise kriptografide, herhangi bir sayı dizisinde herhangi bir n konumundaki değerden önceki ve sonraki değerlerin tahmin edilememesidir. Birbiriyle büyük ölçüde ilişkili olan rastgelelik ve tahmin edilemezlik arasında farklar bulunmaktadır. Tamamen rastgele olan bir süreç aynı zamanda tahmin edilemezdir. Ancak bunun tersi doğru değildir. Tahmin edilemeyen süreçler gerçek manada rastgele olmayabilir [31].

1.5.8.1. Gerçek Rastgele Sayı Üreteçleri

Gerçek rastgele sayı üreteçleri, çıktılarının pratikte bir daha üretilemeyeceği sistemlerdir. Örneğin bozuk bir parayı bir yüzünü 0 diğer yüzünü 1 olarak kabul ederek 100 defa fırlatıp çıkan sonucu 100 bit şeklinde kaydettiğimizde aynı bit dizisini aynı yolla tekrar elde etmemiz hemen hemen imkânsızdır. Aynı diziyi üretmek $\frac{1}{2^{100}}$ gibi çok düşük bir olasılıkla mümkündür. Çünkü üretilen dizi elemanları fonksiyonel olarak birbirinden bağımsızdır.

Gerçek rastgele sayı üreteçleri fiziksel bir işlem gerektirmektedir. Yazı tura, yarı iletken gürültü, sayısal devrelerde zaman bilgisini sağlayan darbelerin zaman içinde rasgele olarak ileri geri kaymaları (clock jitter) ve radyoaktif bozulma bunlara birer örnektir. Kriptografik uygulamalar için son derece yavaş olan gerçek rastgele üretme metotları günümüzde hala kullanılmaktadır [32]. Kriptografide gerçek rastgele sayı üreteçleri uç sistemler arasında dağıtılmak üzere oturum anahtarları (*session keys*) üretiminde kullanılmaktadır.

1.5.8.2. Sözde Rastgele Sayı Üreteçleri

Sözde rastgele sayı üreteçleri bir başlangıç değeri kullanarak rastgele özellikte olasılıksal dağılıma sahip diziler üretirler. Genellikle s_0 başlangıç değeri olarak alınıp rekürsif olarak (12)'deki gibi üretilir.

$$s_{i+1} = f(s_i), i = 0,1 \ldots \quad (12)$$

Bu üreteçlerin en çok bilinen örneklerinden biri (13)'deki Linear congruential generator'dür [33].

$$s_{i+1} = as_i + b \bmod m, i = 0,1 \ldots \quad (13)$$

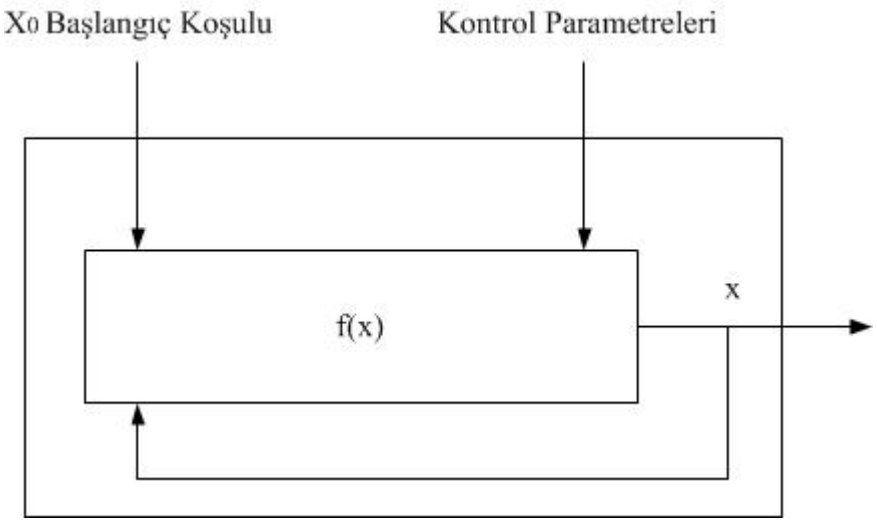
Sözde rastgele sayı üreteçleri gerçek manada rastgele değillerdir. Çünkü tamamen deterministik olduklarından yeniden hesaplanabilirler. Bu üreteçlerin çıktılarının en önemli ve genel özelliği istatistiksel olarak gerçek rastgele sayı dizisine yaklaşımıdır. Kriptografi dışında sözde rastgele sayıların kullanıldığı birçok alan vardır. Rastgele veri girişine ihtiyaç duyan simülasyon, yazılım testleri ve daha birçok alanda kullanılırlar. ANCI C bildirimlerinde rand() fonksiyonunun bulunma sebeplerinden biride sözde rastgele sayıların yaygın bir alanda kullanılmalarıdır.

1.5.8.3. Kaotik Sözde Rastgele Sayı Üreteçleri

Kriptografik olarak güvenli sözde rastgele sayı üreteçleri, sözde rastgele sayı üreteçlerinin özel bir türüdür. Bu özel türdeki üreteçler tahmin edilemez çıktılar üretirler. Bunun manası çıkış dizisinin n sembolü verilince, bu alt dizinin bir sonraki veya bir önceki sembol dizilerinin hesaplanamamasıdır. Kriptografik güvenli rastgele sayı üreteçleri kriptografide anahtar üretimi ve sayısal imza gibi uygulamalarda kullanılmaktadır.

Kriptografide ihtiyaç duyulan rastgelelik, kaotik sistemlerin doğal yapısında mevcuttur. Başlangıç koşullarına olan duyarlılıkları ve topolojik geçişkenlikleri, kriptografik olarak güvenli rastgele sayı üreteçleri olarak kullanılmalarını sağlar. Bu özelliklerinden dolayı kriptografide rastgele sayı üretmede yaygın bir şekilde kullanılmışlardır [34, 35, 36]. Kaotik sistemlerin, çok iyi rastgele sayı üreteçlerinin sahip olması gereken uzun döngü, güçlü rastgelelik, entropi, hız ve yeniden üretilebilirlik gibi önemli özellikleri vardır. Ancak kaotik sistemler genellikle sürekli sistemlerdir ve gerçek sayılar veya karmaşık sayılar kümesinde tanımlıdırlar. Gerçek sayılardan tam sayılara

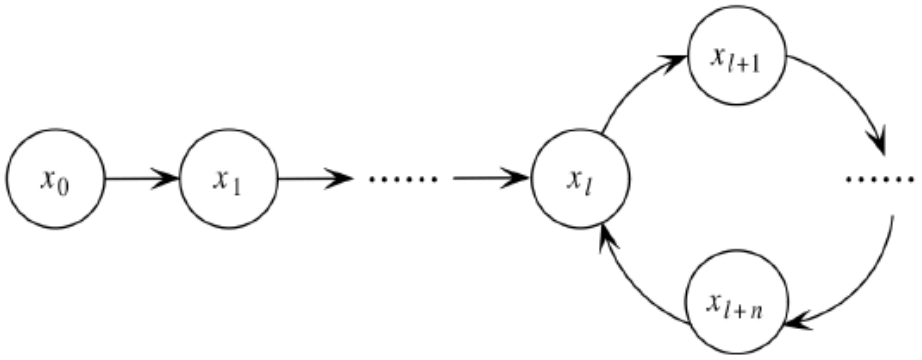
dönüşümde kaotik davranışta azalmalar olmaktadır. Şekil 1.19'da kaotik bir sözde rastgele sayı üretecin nasıl çalıştığı gösterilmektedir.



Şekil 1.19. Kaotik bir sözde rastgele sayı üretecinin yapısı

1.5.8.4. Kaosun Ayrıklaştırılması

Kaosun sayısal kriptografide kullanımı, kaotik haritaların belli bir aralıkta kullanılmasını temel alır. Şifreleme amacıyla kaotik haritaların simülasyonları bilgisayarlarda gerçekleştirilmektedir. Ancak kaosun özelliklerinden dolayı birçok sayısal sistem, daha fazla güvenlik beklentisinin aksine başarısız sonuçlar vermiştir. Örneğin tanımlı olduğu aralıkta gerçekten kaotik olan harita, bilgisayar ortamında olması gereken itici ve çekici periyodik noktaları tanımlı olduğu aralıkta göremez. Dinamik bir sistemi bilgisayar üzerinde iterasyona soktuğumuzda bilgisayarın sonlu bir duyarlılığa sahip olduğunu görürüz. Bundan dolayı topolojik geçişkenlik bilgisayar üzerinde tam olarak sağlanamaz. Çünkü dinamik sistemler bilgisayar üzerinde gerçek sayılardan oluşan bir aralığa yerleştirilemez. Bunun sebebi sayısal bilgisayarların gerçek sayıları tam olarak temsil edememesidir. Bundan dolayı dinamik sistemleri, ayrık ve sonlu bir durumda bilgisayar üzerinde gerçeklenebilecek şekilde adapte etmek gerekir. Şekil 1.20'de tipik bir sayısal kaotik sistemin yörüngesi gösterilmektedir.



Şekil 1.20. Tipik bir sayısal kaotik sistemin yörüngesi

Sürekli kaosu sayısal kriptografiye uygulayabilmek için sonlu durum yaklaşması veya kaotik sistemin benzeri kullanılabilir. Orijinal kaotik sistemin özelliklerini göz önüne alırsak, ayrıklaştırma (14)'deki asimptotik yaklaşımı sağlamalıdır.

$$\lim_{k\to\infty} \max_{x\in X} |f(x) - F(x)| = 0 \tag{14}$$

$$F(x) = \text{round}_k(\, f(x)\,) \tag{15}$$

Burada $f(x)$ sürekli kaotik fonksiyon ve $F(x)$ ayrıklaştırılmış benzeridir. Kayan noktalı aritmetiğinde $F(x)$ (15)'deki gibi ifade edilir. Burada $\text{round}_k(\, f(x)\,)$, z argümanını k duyarlılığına yuvarlayan bir fonksiyondur. $F(x)$ fonksiyonu 32 bitlik bitlik duyarlılıkta kaotik bozulmayı asgari düzeye indirmektedir [37]. Kaosun ayrıklaştırılması için birçok yaklaşım mevcuttur. Ayrık durum kaotik sistemler için temel iki yaklaşım sırasıyla, sürekli kaosa kayan noktalı yaklaşımı ve ayrık kaostur. Kaotik sistemlerin sayısal uygulamaları için genel yaklaşım sonlu duyarlılıkta kayan noktalı aritmetiğidir. Sistem durumu kayan noktalı sayılar vektörüdür ve f kaotik haritası kayan noktalı CPU tarafından değerlendirilir. Kayan noktalı aritmetiği birçok şifreleme algoritmalarında kullanılmıştır [38, 39, 40, 41].

Diğer bir yaklaşım kaotik özellikler gösteren ayrık-durum ayrık-zaman sistemlerin tasarlanmasıdır [42]. İkili aritmetiği temel olan bu yöntem sayısal cihazlar için kayan-noktalı yaklaşımından çok daha doğaldır. Bu yaklaşıma örnek olan doğrusal olmayan yerine koyma kutuları (S-Box – Substitution Boxes) gibi ikili haritalar, geleneksel

kriptografide DES ve AES şifreleme algoritmaları gibi birçok şifreleme algoritmasının yapısında yaygın bir şekilde kullanılmaktadır.

1.6. Kaos Tabanlı Kriptografi

Kaos deterministik bir süreçtir. Ancak kaosun doğası, kaotik sistemlerin başlangıç koşullarına ve kontrol parametrelerine duyarlılığıyla rastgele bir görünümde olmasını sağlar. Kaosun bu özelliği şifreleme algoritmaları için aranan bir özelliktir. Kaosun deterministik olması şifrelemede kullanılmasını, rastgeleliği ise şifreleme sistemleri için analitik ataklara karşı koymasını sağlar.

Kriptografi bilgi güvenliğinde bir çalışma alanıdır. Genel olarak verinin iletilmesinde gizliliği ve veri bütünlüğünü temel alır. Geleneksel kriptografi sayılar teorisini ve cebirsel işlemi kullanır. Kaos kendine has özellikleri olan bir mekanizmaya sahiptir ve tanımlı olduğu uzay gerçek sayılar veya karmaşık sayılardır. Bundan dolayı kriptografideki kullanımı kaotik kriptografi olarak adlandırılarak yeni bir çalışma alanı ortaya konulmuştur. Kaosun doğal yapısından dolayı, kaotik kriptografinin geleneksel kriptografiden farkları vardır.

Verimli ve güçlü kaotik şifreleme sistemlerinin tasarlanmasında dikkat edilmesi gereken noktalar vardır. Şifreleme algoritmasında kullanılan şifreleme anahtarı yeterli uzunluğu sağlayabilecek bir kaotik uzaydan seçilmelidir. Anahtar uzayı 2^{100}'den daha küçük olmamalıdır. Gerçek sayılar üzerine tasarlanan şifreleme sistemi bilgisayarlar üzerinde gerçek manada kaotik olmayan davranışlar sergileyebilir. Bu kaotik bozulmayı ortadan kaldırabilmek veya asgariye indirebilmek için, kullanılan kaotik haritaların çıktılarının tamsayı olacak şekilde formüle edilmesi gerekir. Tüm anahtarlar için şifreli metin dağılımı rastgele olmalıdır.

1.6.1. Kaotik Sistemler ve Kriptografi Arasındaki İlişki

Araştırmacılar 1990'lardan bu yana kaos ile kriptografi arasında güçlü bir ilişki olduğunu vurgulamaktadırlar. Kaotik sistemlerin doğal birçok özelliği geleneksel kriptografide ihtiyaç duyulan özelliklerle örtüşmektedir. Tablo 3'de bu özelliklerden bazıları gösterilmektedir.

Tablo 3. Kaotik sistemler ve kriptografi arasındaki benzerlikler

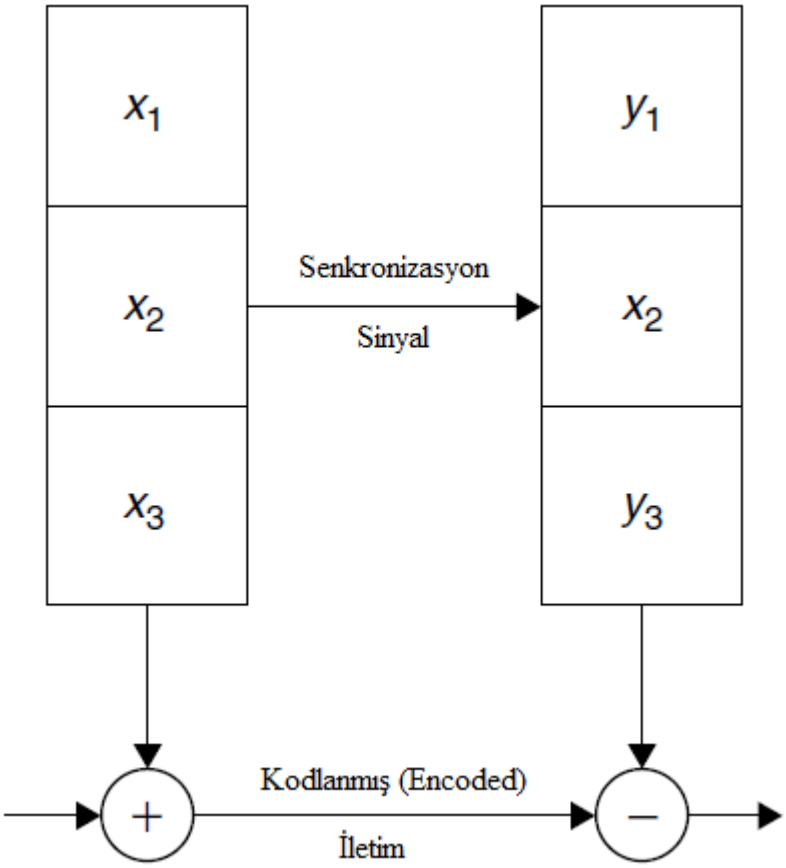
Kaotik özellik	**Kriptografik özellik**	**Açıklama**
Ergodiklik	Karıştırma	Tüm girişler için aynı çıktı dağılımı
Başlangıç koşullarına duyarlılık	Düz metin ve anahtardaki küçük bir değişimin bir şifreli metine etkisi	Girişteki ufak bir değişiklik çıktıda büyük bir değişime yol açar.
Karışma özelliği	Bir bloktaki değişim tüm düz metni etkiler.	Yerel bölgedeki değişim tüm bölgeyi etkiler.
Deterministik dinamikler	Deterministik sözde rastgelelik	Deterministik bir süreç rastgele benzeri davranışlar gösterir.

Kaotik kriptografi bazı yönleriyle geleneksel kriptanalize daha dayanıklıdır. Diğer taraftan bu özelliğinden dolayı çok fazla kriptanaliz karmaşıklığına sahiptir. Bu da şifreleme güvenliğinin çok açık tanımlanamadığı anlamına gelmektedir.

Karıştırma ve yayılma özellikleri dinamik sistemlerin doğal olarak sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşullarına ve kontrol parametrelerine bağımlılığı, bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer, başlangıç koşulları veya kontrol parametrelerine bağımlıdır. Başlangıç koşulları ve kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından, bu bağımlılık çok güçlüdür. Sonuç olarak kaotik sistemler, başlangıç koşullarına ve kontrol parametrelerine bağımlılıkları sayesinde yayılma özelliğine sahiptir.

Kaotik sistemlerin ergodiklik özelliği, kaotik yörüngenin uzun vadeli davranışının başlangıç koşullarına ve kontrol parametrelerine bağımlılığını ortaya koymaktadır. Buradan, bir kaotik sistemden üretilen yörüngelerin bir kümesinden istatistikî olarak başlangıç koşulları ve kontrol parametrelerinin tam değerlerinin çıkarılmasının mümkün olmadığı görülebilir. Sonuç olarak kaotik sistemler karıştırma özelliğini göstermektedir.

Dachselt ve Schwarz'a göre [43] geleneksel kriptografi ayrık zamanda ayrık değerlerde çalışırken, kaotik kriptografi sürekli veya ayrık zamanlarda, sürekli değerlerle çalışır. Kaotik kripto sistemler analog ve sayısal olarak ayrılmaktadır. Çoğu analog kaotik şifreleme sistemi kaos senkronizasyonu üzerine tasarlanmıştır. Kaos senkronizasyonu 1990'larda geliştirilmiş bir tekniktir [44]. Genel olarak iki kaotik sistem, alıcıdan vericiye iletilen bir veya daha fazla sinyali kontrol ederek iletimi sağlamaktadır. Şekil 1.21'de kaos senkronizasyonunu temel alan genel bir kaotik haberleşme tekniği gösterilmektedir.



Şekil 1.21. Kaos senkronizasyonuna dayalı analog haberleşme yapısı

Sayısal kaotik şifreleme sistemleri sayısal bilgisayar için tasarlanmıştır. Kaotik haritalar sonlu hesaplama duyarlılığında şifreleme için kullanılmaktadır. Sayısal kaotik şifreleme kaos senkronizasyonuna bağlı değildir. Sayısal kaotik şifreleme sistemleri ayrık kaotik sistemlere dayalıdır.

Geleneksel kriptografide genel olarak blok ve akım almak üzere iki tip şifreleme vardır. Blok şifrelemede düz metin blokları şifreli metin bloklarına haritalanır. Akım

şifrelemede düz metnin veri dizisi ilişkili şifreli metin dizisine dönüştürülür. Her iki yaklaşımda kaotik şifreleme sistemleri tasarımında kullanılabilir. Kaotik blok şifrelemede, düz metin kaotik haritalar için başlangıç koşulu olarak ele alınabilir. Kontrol parametreleri veya haritalamadaki iterasyon sayısı ile şifreli metin üretilmektedir [45]. Kaotik akım şifrelemelerde güvenlik kaotik sözde rastgele sayı üreteçlerine bağlıdır.

1.6.2. Kaotik Kriptografinin Avantajları ve Dezavantajları

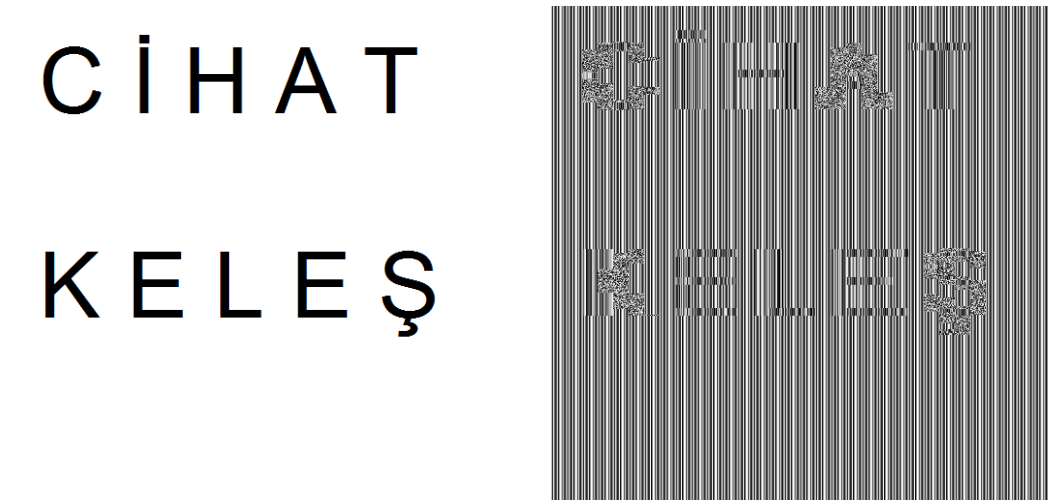
Tüm kaotik şifreleme algoritmaları, gerçek sayılar kümesinde tanımlı dinamik sistemleri kullanır. Bundan dolayı sayısal bilgisayarlarda gerçeklenmeleri zordur. Gerçek sayıların sayısal bilgisayarlar ile tam olarak temsil edilememesi kaosun bu bilgisayarlar üzerinde gerçeklenebilmesi için büyük bir sorundur. Sonlu birer makine olan bilgisayarlar üzerinde gerçeklenen kaotik sistemlerin kaotik özelliklerinde bozulmalar olmaktadır.

Kaotik haritaların doğası gereği, geleneksel güvenlik analiz metotları, bu tür şifrelemelerde yetersiz kalmaktadır. Çünkü bu analizler geleneksel şifreleme sistemleri için geliştirilmiştir. Kaotik kripto sistemlerin güvenliği, şifrelemede kullanılan kaotik haritaların gücüne bağlıdır. Kriptografide bu haritaları analiz edebilecek yeteri kadar güvenlik analizi metotları geliştirilememiştir. Bundan dolayı kaotik şifreleme metotlarının güvenlik analizleri hali hazırda bulunan geleneksel güvenlik analiz metotları, istatistiksel analiz, kaba kuvvet teknikleri gibi teknikler kullanılarak yapılmaktadır. Bu tür teknikler, kaotik şifrelemenin tam olarak ne kadar güvenli olduğunu açıkça ortaya koyamamaktadır. Çünkü, kaos kendine özgü rastgele benzeri davranışından dolayı geleneksel istatistiksel analizlere karşı dirençlidir. Ancak bu durum kaotik şifreleme için geleneksel güvenlik analizlerine karşı büyük bir avantaj gibi görünse de, güvenlik analizlerinin zor olması nedeniyle, sistemin güvenliği kolaylıkla garanti edilememekte ve güvenliğinin seviyesi tam olarak tanımlanamamaktadır. Bundan dolayı günümüzde kaotik şifreleme sistemlerine örnek gösterilebilecek herhangi standart bulunmamaktadır.

1.6.3. Kaotik Sayısal Resim Şifreleme Algoritmaları

Resimlerin, metin mesajlardan farklı olarak kendine has özellikleri vardır. Genellikle büyük boyutlarından dolayı geleneksel şifreleme yöntemleri resim şifrelemede yavaş kalmaktadır. Temel olarak resim ve metin şifreleme arasında bazı farklar vardır [46, 47]. Metin verisinin şifreli durumu kayıpsız bir şekilde orijinal haline dönüştürülmektedir. Ancak resim şifrelemede, şifreli resim orijinal durumuna dönüşümünde biraz kayıplar olabilmektedir. Metin verisi kelime dizilerinden oluşur. Direk olarak blok veya akım şifreleme sistemleriyle şifrelenebilir. Ancak sayısal resimler genellikle 2 boyutlu dizilerde temsil edilirler.

Sayısal bir resim, depolama biriminde büyük yer kapladığı için direk olarak şifrelemede çok verimli değildir. AES ve DES gibi şifreleme algoritmalarında özel düzenlemeler yapılmadığı sürece resim şifrelemede zafiyetler ortaya çıkar. Şekil 1.22'de AES şifreleme algoritmasının, 256 bit uzunluğundaki anahtar ile elektronik şifre kitabı modunda resim şifreleme sonucu gösterilmektedir. Düz resmin yerel bölgelerindeki benzer piksel değerleri AES ile bloklar halinde şifrelenerek, şifreli resimde aynı bölgeye haritalanmaktadır. Elektronik şifre kitabı modunda, tüm blok şifrelemelerde aynı düz metin blokları aynı şifreli metin bloklarına dönüştürülür. Bundan dolayı tüm piksel değerleri aynı olan arka plana sahip resimler, aynı veri bloklarıyla aynı şifreli blokları üretirler. Bu durum şifreli resmin kolayca anlaşılabilmesine neden olmaktadır. Sadece bilgiyi şifreleme ve şifre çözme için kullanılan en iyi yöntemlerden biri depolama boyutunu azaltmak ve iletim zamanını kısaltmak için yapılan resim sıkıştırmadır.

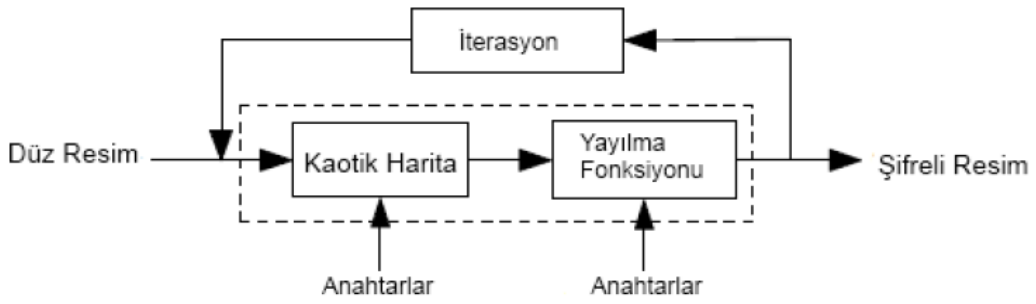


(a) (b)

Şekil 1.22. Elektronik şifre modunda 256 bitlik anahtarlı AES ile resim şifreleme

1.6.3.1. Kaotik Resim Şifreleme Sistemlerinin Genel Yapısı

Resim şifrelemenin metin şifrelemeden daha farklı gereksinimleri vardır. Alternatif olarak kaos teorisi ve basit ayrık kaotik haritalar, kaos tabanlı şifreleme gerçekleştirmek için son derece uygundurlar. Bu basit eşitliklerle resim şifrelemenin gereksinimleri olan piksel karıştırma ve yayılma işlemleri kolayca gerçekleştirilebilir. Fridrich, kaos tabanlı resim şifrelemelerinin sırasıyla karıştırma ve yayılma gibi 2 aşamadan oluşması gerektiğini belirtmiştir [8]. İlk aşama olan karıştırma aşamasında pikseller, değerleri değiştirilmeden karıştırılırlar. Komşu pikseller arasındaki korelasyonu bozmak için $m \geq 1$ olacak şekilde ilk aşama olan karıştırma aşamasında m döngü mevcuttur. Genel bir kaotik resim şifreleme yapısı şekil 1.23'de gösterilmiştir.



Şekil 1.23. Genel bir karıştırma yayılma tipinde kaotik resim şifreleme

Anlamlı bir resimde pikseller birbirlerine yaklaştıkça, aralarındaki korelasyonda güçlü bir şekilde artmaktadır. Düz resimde bulunan komşu pikseller arasındaki korelasyon çok güçlüdür. Bu korelasyonu ortadan kaldırmak için komşu piksellerin farklı noktalara taşınması gerekir. Bu taşıma resim şifreleme sistemlerinin karıştırma aşamasında, deterministik bir şekilde yapılmaktadır. Böylece piksellerin değerleri deterministik olarak değiştiği için, pikseller şifre çözme aşamasında gerçek konumlarına geri getirilebilmektedir. Aynı zamanda bu karıştırma rastgeleliğe çok yakın ve tahmin edilemezdir. Kaotik haritalar bu ihtiyacı, karıştırma ve ergodik özellikleri ile doğal olarak karşılamaktadır. Bunu tersi alınabilen basit eşitliklerle sağlamaktadırlar. Bu eşitliklerin başlangıç koşullarına ve kontrol parametrelerine çok fazla duyarlı olan çıktıları akım şifrelemelerde anahtar olarak da kullanılabilmektedir.

İkinci aşama olan yayılma aşaması, istatistiksel ilişkiyi ortadan kaldırmak için gereklidir. Bu aşamada piksel değerleri birbirlerine bağımlı bir şekilde değiştirilirler. Bundan dolayı tek bir piksel tüm pikseller üzerinde güçlü bir etkiye sahip olmaktadır. Kriptografide bir giriş sembolü değiştiğinde çıkış sembollerinin büyük ölçüde değişmesine çığ etkisi (avalanche effect) denir. Karıştırma ve yayılma aşamaları n ≥ 1 olacak şekilde n defa tekrarlanır.

Kaotik resim şifreleme sistemlerinin genel olarak temel aldığı Fridrich'in yayılma aşamasında [8] seçilen bir c_{-1} başlangıç değeri ile düz resmin tüm p_i piksel değerleri sırasıyla birbirlerine etki ederek (16)'daki gibi yeniden düzenlenir.

$$c_i = p_i + G(c_{i-1}) \bmod L \quad i = 0, 1, 2 \ldots \tag{16}$$

Burada L mümkün olan piksel değerlerini, c_i şifreli resmin piksel değerlerini ve G bir önceki iterasyonda elde edilen şifreli resmin c_{i-1} piksel değerlerini girdi olarak alıp, rastgele değerler üreten bir fonksiyonu temsil etmektedir. G rastgele değerlerle oluşturulmuş bir kontrol tablosu veya yerine koyma kutuları olarak da seçilebilir.

Şifre çözme işleminde ise, yayılma aşamasının etkisi orijinal p_i piksel değerlerinin (17)'deki gibi, bilinen c_{-1} değeri kullanılmak suretiyle geri elde edilmesiyle ortadan kaldırılır.

$$p_i = c_i - G(c_{i-1}) \bmod L \quad i = 0, 1, 2 \ldots \tag{17}$$

2. YAPILAN ÇALIŞMALAR BULGULAR VE TARTIŞMA

2.1. Giriş

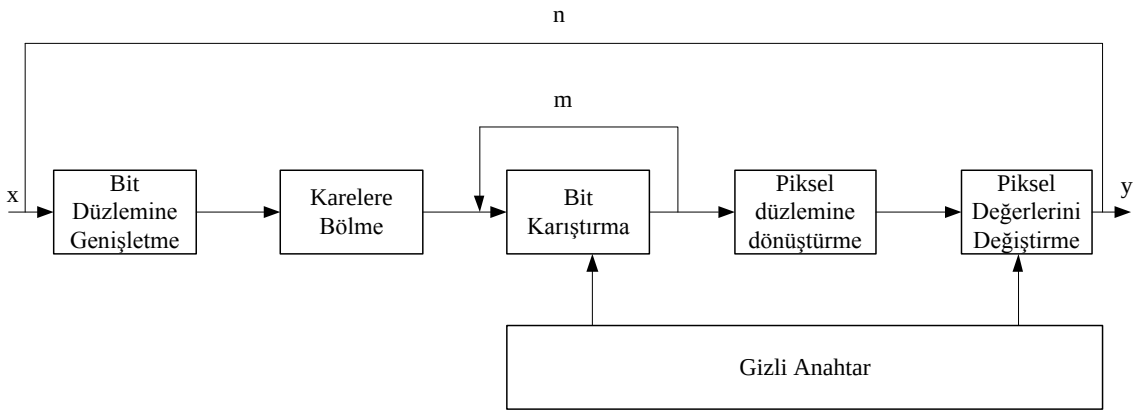
Bu bölümde bit tabanlı piksel karıştırma aşamasına sahip güvenli kaotik resim şifreleme gerçekleştirilmiştir. Piksel tabanlı resim karıştırma kullanılarak yapılan şifreleme ile AES şifreleme standardı bazı analizlerde karşılaştırılmış ve gerekli güvenlik analizleri yapılmıştır. İki aşamalı şifreleme yönteminde bit tabanlı piksel karıştırma için 2 boyutlu kaotik Arnold cat haritası kullanılmıştır. Yayılma aşamasında ise logistic harita kullanılmış, düz resim pikseline birbirlerinden bağımsız bir şekilde etki eden, birden fazla parametre kullanarak güvenli resim şifreleme gerçekleştirilmiştir. Şifrelemenin karıştırma aşaması hem piksel tabanlı hem de bit tabanlı karıştırma ile ayrı ayrı gerçekleştirilerek, bu iki yaklaşımın güvenilirlikleri de ayrı ayrı test edilmiştir.

2.2. Şifreleme

Bu çalışmadaki kaotik resim şifreleme yöntemi sırasıyla iki iteratif, karıştırma ve yayılma aşamalarından oluşmaktadır. İlk olarak düz resim bit düzlemine genişletildikten sonra, eşit oranlarda sekiz ayrı kare parçaya ayrılmaktadır. İlk aşama olan karıştırma aşamasında bu ikili sekiz resmin pikselleri iki boyutlu kaotik cat harita kullanılarak birbirinden bağımsız olarak karıştırılmaktadır. Pikselleri karıştırılmış olan karesel ikili sekiz resim tekrar birleştirildikten sonra, bir boyutlu logistic haritanın ürettiği rastgele değerler ve şifreli resim için bir önceki iterasyonda üretilen piksel değeri ile XOR işlemine tabi tutulmaktadır. Komşu pikseller arasındaki korelasyonun bozulması ve düz resim ile şifreli resim arasındaki ilişkinin anlaşılamaması için birinci aşama olan karıştırma aşaması, tüm ikili resimler için $m \geq 1$ olacak şekilde m döngü olarak gerçekleştirilir. Tüm şifreleme adımı $n \geq 1$ olacak şekilde n döngüden oluşmaktadır. Kaotik haritaların başlangıç koşulları, kontrol parametreleri ve şifrelemenin döngü sayısı n, şifreleme anahtarları olarak belirlenmiştir.

Karıştırma aşamasında bit tabanlı piksel karıştırma ile yayılma aşamasına geçmeden düz metnin bazı istatistiksel özelliklerinin belirlenemez hale gelmesi ile geleneksel kaotik

resim şifreleme yöntemlerinin zayıflıkları ortadan kaldırılmıştır. Bit tabanlı kaotik resim şifreleme yönteminin genel yapısı Şekil 2.1'de gösterilmiştir.



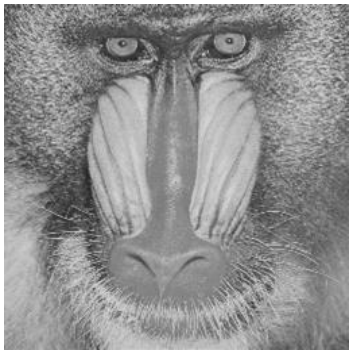
Şekil 2.1. Bu çalışmadaki kaotik resim şifreleme metodunun genel yapısı

2.2.1. Bit Tabanlı Piksel Karıştırma

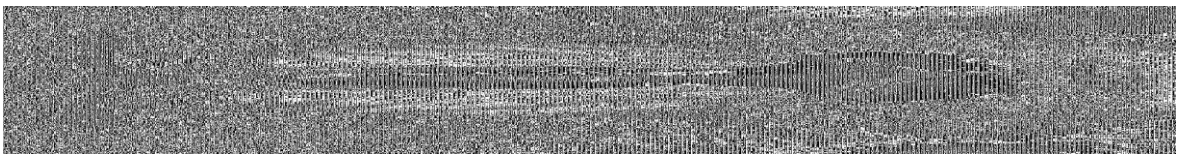
İlk aşama olan bit tabanlı piksel karıştırmada, düz resim öncelikle bit düzlemine genişletilir. Gri seviye bir resim için parlaklık bir grup numara ile siyahtan beyaza nicelenmiştir. Parlaklığın bölümlenmesi sayısallaştırmadaki duyarlılığa bağlıdır ve gri seviye bir resim için genel olarak 256 olarak kullanılmaktadır. Sayısal bilgisayarlarda gri seviye 8 bitlik format ile (18)'deki gibi temsil edilmektedir.

$$G(x,y) = b(7)b(6)\dots b(0) \tag{18}$$

Burada G(x, y), resmin (x, y) koordinatındaki piksel değerini, parantez içindeki sayılar ise pikselin en yüksek seviye bitinden en düşük seviye bitine kadar olan indis sayılarını göstermektedir. 256 gri seviyeye sahip MxN boyutlu bir resim, bit tabanlı Mx(Nx8) boyutlu ve pikselleri sadece iki mümkün değere (0 ve 1) sahip olabilen ikili bir resme genişletilir. Düz resmin bir pikseline ait her bir bit, genişletilmiş ikili resmin bir pikselin değeri olarak kabul edilir. Örnek olarak Şekil 2.2'de ve Şekil 2.3'de sırayla gri seviye mandrill resmi ve bu resmin bit düzlemine genişletilmiş ikili resmi gösterilmektedir.



Şekil 2.2. Düz mandrill resmi



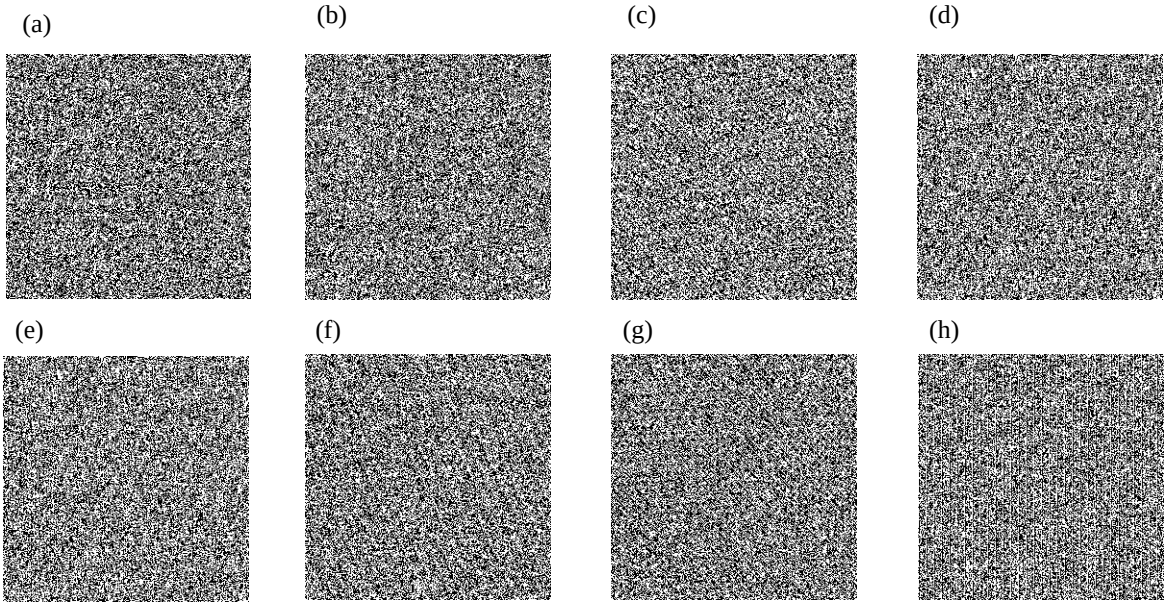
Şekil 2.3. Mandrill resminin bit düzlemine genişletilmiş hali

İlk aşama olan karıştırma aşamasında, ilk önce bit tabanına genişletilmiş olan resim soldan sağa doğru sekiz ayrı karesel MxN boyutlu parçaya ayrılır. Her bir kare resim birbirlerinden bağımsız kontrol parametreleri ile kaotik cat haritası kullanılarak karıştırılır.

Arnold Cat haritasının sonlu bir kümede resim şifrelemede kullanılabilmesi için, kaotik özellikleri korunarak ayrıklaştırılması gerekmektedir. Ayrık Cat haritası IxI birim kareden NxN kafes alanına, (x, y) boyutları değiştirilerek (19)'daki gibi ifade edilir.

$$\begin{bmatrix} x_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_n \\ Y_n \end{bmatrix} \bmod N \tag{19}$$

Burada N kare resmin genişliği veya yüksekliğidir. Birer tamsayı olan kontrol parametreleri p ve q ile birlikte m döngü sayısı gizli anahtarların bir parçasıdır. Orijinal resimdeki (x_n, y_n) piksel konumları, (x_{n+1}, y_{n+1}) ise piksel karıştırma sonucunda oluşan resimdeki yeni piksel konumlarıdır. Pikselleri karıştırılmış sekiz karesel resim Şekil 2.4'de gösterilmektedir.



Şekil 2.4. (a) – (h) sırasıyla pikselleri karıştırılmış sekiz karesel resim

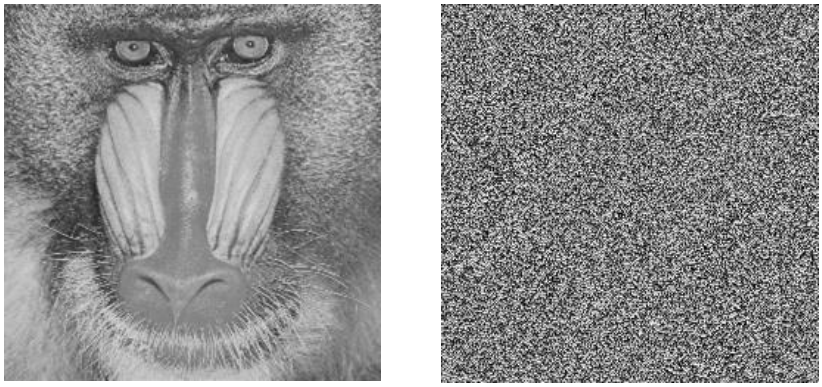
Kaotik cat haritası ayrıklaştırıldıktan sonra kaotik özelliklerini kısmen kaybeder. Sonlu bir alanda tanımlanmış ve kaotik özellikleri tam manasıyla barındırmayan ayrık cat haritası periyodiktir. Bundan dolayı şifreleme aşamasında iterasyon sayıları periyodik olmayacak şekilde seçilmelidir. Tablo 4'de farklı boyutlara sahip bazı resimlerin tekrar orijinal haline dönüşmesi için gerekli olan iterasyon sayıları gösterilmiştir. Bu iterasyon sayıları aynı zamanda NxN birim alanında ayrık kaotik cat haritasının periyot sayılarını vermektedir.

Tablo 4. Ayrık kaotik cat haritası ile karıştırılan n boyutlu resmin orijinal haline dönmesi için gereken döngü sayısı

nxn matris döngüsü (piksel değerleri)	**Orijinal resme dönmek için iterasyon sayısı**
300x300	300
183x183	60
124x124	15
150x150	300
157x157	157
100x100	150
147x147	56

2.2.2. Yayılma

İlk aşama olan karıştırma aşamasında, bit düzlemine genişletilen ve sekiz ayrı resme ayrılarak pikselleri karıştırılan ikili resimler birleştirilerek tekrar piksel tabanlı MxN boyutlu resim elde edilir. Sekiz karesel resmin birleştirilmesiyle elde edilen bit tabanlı Mx(Nx8) boyutlu ikili resmin, birbirini takip eden ve piksel değerleri 1 veya 0 olan sıralı sekiz pikselinin değerleri difüzyon aşamasına girecek olan MxN boyutlu resmin 8 bitlik piksel değerini oluşturur. Şekil 2.5'de Mandril resminin karıştırma aşamasından sonra elde edilen sekiz karesel ikili resmin piksel düzlemine getirilmiş durumu gösterilmektedir.



(a) (b)

Şekil 2.5. (a) düz mandrill resmi, (b) karıştırma aşaması sonrası mandrill resmi

Yayılma aşamasında piksel değerleri, bu değerlere sırayla (5) logistic harita kullanılarak üretilen rastgele 8 bitlik rastgele değerler ve şifreli resim için bir önceki iterasyonda üretilen piksel değeri ile XOR işlemi uygulanarak değiştirilir. Logistic harita ile üretilen rastgele 8 bitlik değerler sıralı olarak, her bir iterasyon tarafından kaotik ortamda üretilir. Bundan dolayı bu değerler birbirlerine bağımlıdır ve en ufak bir değişiklik tüm piksel değerlerine etki eder. Difüzyon aşaması (20)'deki gibi gerçekleştirilir.

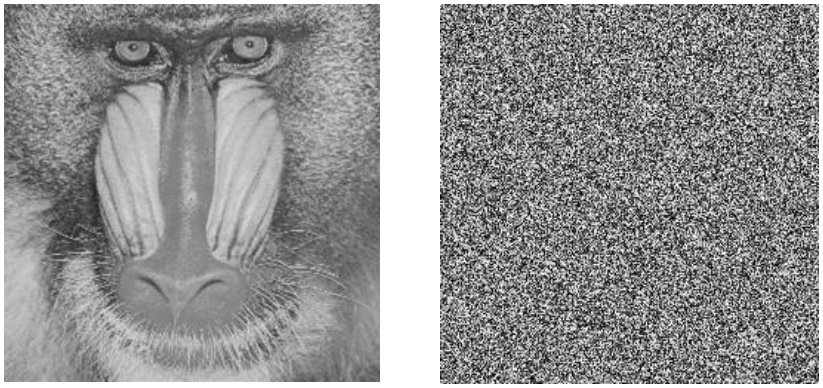
$$C_i = p_i \oplus C_{i-1} \oplus q(f(x_0)), L) \tag{20}$$

Burada f(.) fonksiyonu logistic haritadır. Fonksiyonun ilk aldığı başlangıç değeri x_0 gizli anahtarın bir parçasıdır ve C_{-1} değeri x_0 olarak alınır. XOR işlemi için gereken bitler q(.) fonksiyonu ile elde edilerek orijinal resmin p_i piksel değeri ile işleme tabi tutulur. Bu işlem sonucunda pikselin yeni değeri elde edilir. XOR işlemi için gereken ve logistic haritanın ürettiği rastgele değerleri uygun hale getirmek için gereken q(.) fonksiyonu (21)'deki şekilde ifade edilir.

$$q(x, L) = 2^L . x \tag{21}$$

Burada değeri 0 veya 1 olan $x = 0.b_1b_2b_3 \ldots b_M$ değeri f(.) fonksiyonu ile elde edilen $x \in (0, 1)$ değerinin virgülden sonraki ilk M bitidir. M değeri 256 gri seviye ile gösterilen resimler için 8 olarak alınır. Yayılma aşamasında bir pikselin değeri kendisinden sonra gelen piksel değeri üzerinde etkilidir. Şifreli pikselin üzerinde aynı zamanda logistic harita ile elde edilen rastgele değerler de etkili olduğundan dolayı, şifreli pikselin değeri

birbirinden bağımsız değerler tarafından üretilmiş olur. Böylece sistemin kriptanalist tarafından değerlendirilmesi zorlaştırılmış olur. Yayılma aşamasından sonra nihai şifreli resim elde edilir. Şekil 2.6'de düz resim ve şifreli resim çifti gösterilmektedir.



(a) (b)

Şekil 2.6. (a) düz mandrill resmi, (b) şifreli mandrill resmi

2.3. Şifre Çözme

2 boyutlu Cat haritası ve XOR işlemi geri dönüşümü olan işlemlerdir. Şifre çözme işlemi aynı anahtarlarla, yayılma ve karıştırma işlemleri uygulanarak gerçekleştirilir. Yani sondan başlayarak geriye doğru şifreleme aşamaları uygulanarak şifre çözme işlemi gerçekleştirilir. Yayılma aşaması sonucunda oluşan şifreli resmi, yayılmadan önceki durumuna döndürmek için ters difüzyon işlemi (22)'deki gibi uygulanır.

$$p_i = C_i \oplus C_{i-1} \oplus q(f(x_0)), L) \tag{22}$$

Ters yayılma işleminden sonra elde edilen MxN boyutlu resim, bit düzlemine genişletilerek Mx(Nx8) boyutlu, 0 veya 1 değerlerine sahip ikili resim elde edilir. Bu ikili resim MxN boyutlarında olan sekiz parçaya ayrılır. Sekiz karesel resim Arnold cat haritasının tersi ile (23)'deki gibi aynı parametrelerle ve aynı sayıda döngü ile karıştırılır.

$$\begin{bmatrix} x_n \\ Y_n \end{bmatrix} = \begin{bmatrix} 1+ab & -a \\ -b & 1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ Y_{n+1} \end{bmatrix} \bmod N \tag{23}$$

Ters ayrık cat haritası ile karıştırılan karesel resimler bit düzleminden piksel düzlemine birleştirilerek düz resim elde edilir.

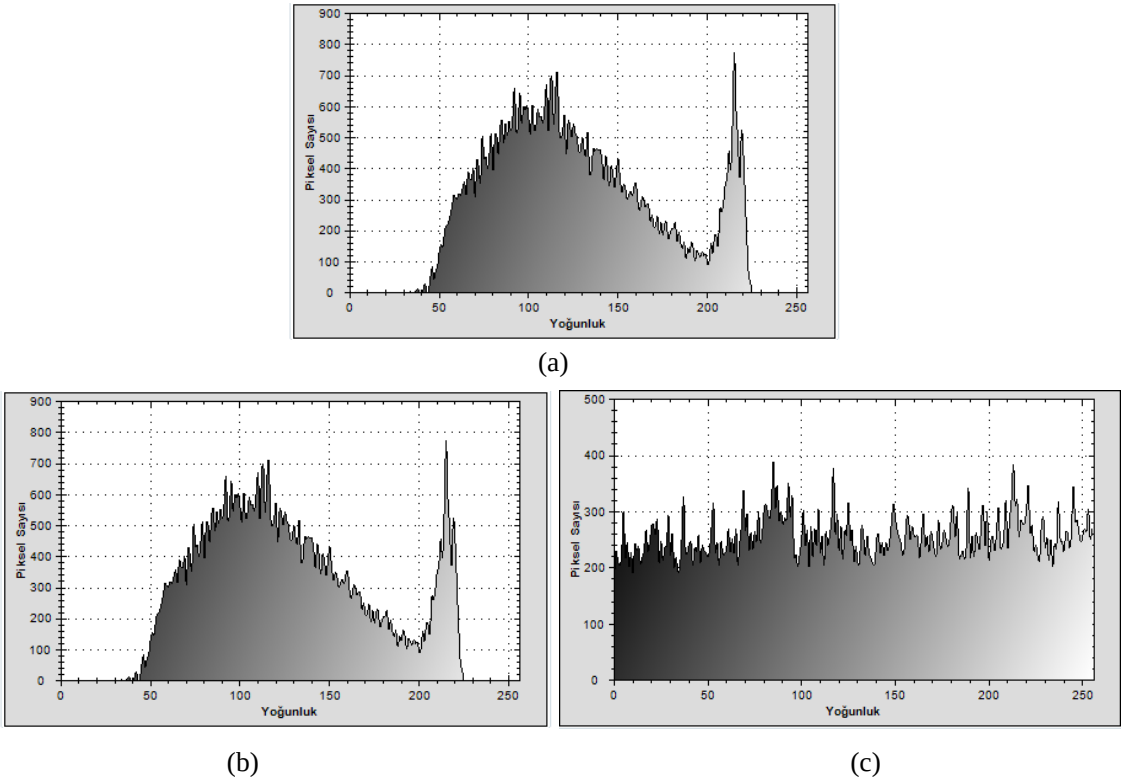
2.4. Deneysel Sonuçlar ve Güvenlik Analizi

Bir şifreleme sisteminin kalitesi, uygun performansla şifreleme ve şifre çözme işlemini gerçekleştirmesi ve yetkisiz uç sistemin düz metin hakkında bilgi elde edememesi ile doğru orantılıdır. İyi bir şifreleme sistemi bilinen tüm ataklara karşı güvenli olmalıdır.

Bu bölümde bilinen bazı güvenlik analizleri yapılmıştır. Karıştırma aşamasında piksel tabanlı ve bit tabanlı karıştırma yöntemleri ayrı ayrı gerçeklenerek yayılma aşamasına olan etkileri analiz edilmiştir. Ayrıca bu çalışmadaki şifreleme yönteminin bazı güvenlik testleri AES şifreleme standardı ile karşılaştırılarak yapılmıştır. Tüm testler ve analizler Intel Core i7 2.00 GHz işlemci, 8 GB bellek, 500 GB hard disk ve 64 bit Windows 7 Professional işletim sistemine sahip kişisel bir bilgisayarda yapılmıştır. Uygulama .NET 4 platformunda C# dili kullanılarak geliştirilmiş ve grafikler bu platformda elde edilmiştir.

2.4.1. Histogram Analizi

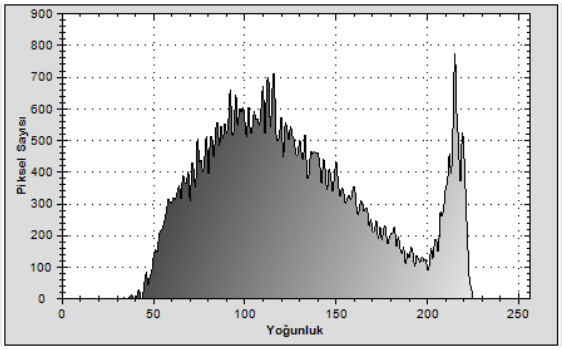
Histogram, sayısal bir resim içindeki renk değerlerinin kaçar adet bulunduğunu gösteren grafiksel bir gösterimdir. Bu grafiğe bakılarak resim hakkında parlaklık ya da ton bilgisi elde etmek mümkündür. Şekil 2.7'de 256x256 boyutlu Mandril resminin, yayılma aşaması kullanılmadan bit tabanlı ve piksel tabanlı karıştırma ile elde edilen şifreli resimlerin histogram grafikleri karşılaştırılmıştır.



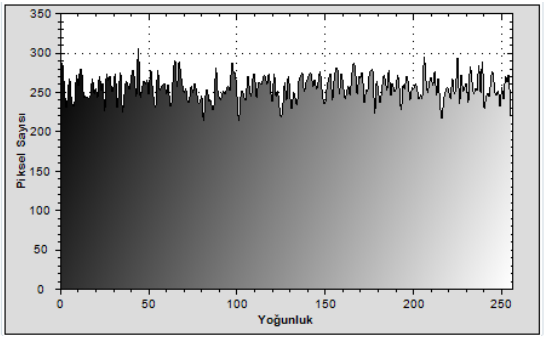
Şekil 2.7. Histogram karşılaştırılması (a) Düz mandrill resminin histogram grafiği (b) piksel tabanlı sadece karıştırma ile şifrelenen resmin histogram grafiği (c) bit tabanlı tek döngü sadece karıştırma ile şifrelenen resmin histogram grafiği

Histogram grafiklerinden de anlaşıldığı gibi, piksel tabanlı karıştırmada düz resmin histogram bilgisinde herhangi bir değişiklik olmamasına rağmen, bit tabanlı karıştırma ile elde edilen şifreli resmin histogram grafiği doğrusal karakterliye ve düzenliliğe yakındır. Karıştırma aşamasında sadece piksellerin karıştırılması orijinal resmin bazı istatistiksel özelliklerini ortadan kaldırmamaktadır. Bit tabanlı karıştırmada ise piksel değerleri değiştiği için, yayılma aşamasında daha düşük döngülerle güvenli şifreleme yapılabilmektedir. Bit tabanlı karıştırma ile bu çalışmadaki resim şifreleme yönteminin yayılma aşamasında daha etkili olduğu anlaşılmaktadır.

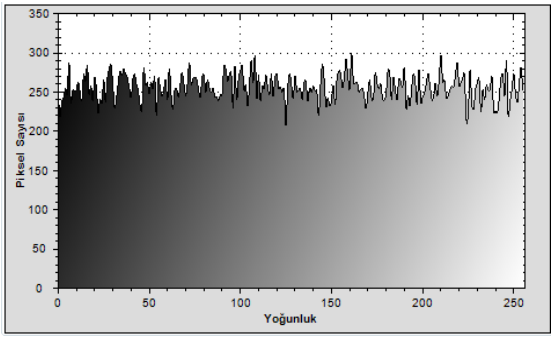
Düz resmin istatistiksel özelliklerini tam olarak kaldırmak için şifreleme sistemleri resim pikselleri üzerinde sırasıyla yayılma işlemini uygularlar. Şekil 2.8'de 256x256 boyutlu mandrill resminin bu tez çalışması ile şifrelenmiş şifreli resmi ve AES şifreleme algoritması ile şifrelenmiş şifreli resmin histogram değerleri karşılaştırılmıştır. Karşılaştırılan yöntemlerin orijinal resmin histogram bilgilerini sakladığı grafiklerden anlaşılmaktadır.



(a)



(b)



(c)

Şekil 2.8. Histogram karşılaştırılması (a) Düz mandrill resminin histogram grafiği (b) bu çalışmadaki yöntem ile şifrelenmiş şifreli resmin histogram grafiği (c) AES şifreleme standardı ile şifrelenmiş resmin histogram grafiği

2.4.2. Korelasyon Katsayıları

Korelasyon, olasılık kuramında ve istatistikte iki rastsal değişken arasındaki doğrusal ilişkinin yönünü ve gücünü belirtir. Genel istatistiksel kullanımda korelasyon, bağımsızlık durumundan ne kadar uzaklaşıldığını gösterir. Korelasyon katsayısı, bağımsız değişkenler arasındaki ilişkinin yönü ve büyüklüğünü belirten katsayıdır. Bu katsayı, (-1) ile (+1) arasında bir değer alır. Pozitif değerler direk yönlü doğrusal ilişkiyi; negatif değerler ise ters yönlü bir doğrusal ilişkiyi belirtir. Korelasyon katsayısı 0 ise söz konusu değişkenler arasında doğrusal bir ilişki yoktur. Farklı durumlar için farklı korelasyon katsayıları geliştirilmiştir. Bunlardan en iyi bilineni Pearson çarpım-moment korelasyon katsayısıdır. İki değişkenin kovaryansının, yine bu değişkenlerin standart sapmalarının çarpımına bölünmesiyle elde edilir. Bu çalışmada iki resim arasındaki bağımlılığı ölçmek için Pearson korelasyon katsayıları kullanılmıştır.

Anlamlı bir resimdeki yatay, düşey ve diyagonal iki komşu piksel arasındaki korelasyon genellikle yüksektir. Çünkü anlamlı bir resimde piksel değerleri birbirine

oldukça yakındır. Bitişik iki piksel arasındaki bağıntıyı test etmek için korelasyon analizi yapılır. İlk önce şifreli resimden rastgele p adet yatay, düşey ve diyagonal komşu piksel çifti seçilir. Her çiftin korelasyon katsayıları r_{uv} (27)'deki gibi hesaplanır.

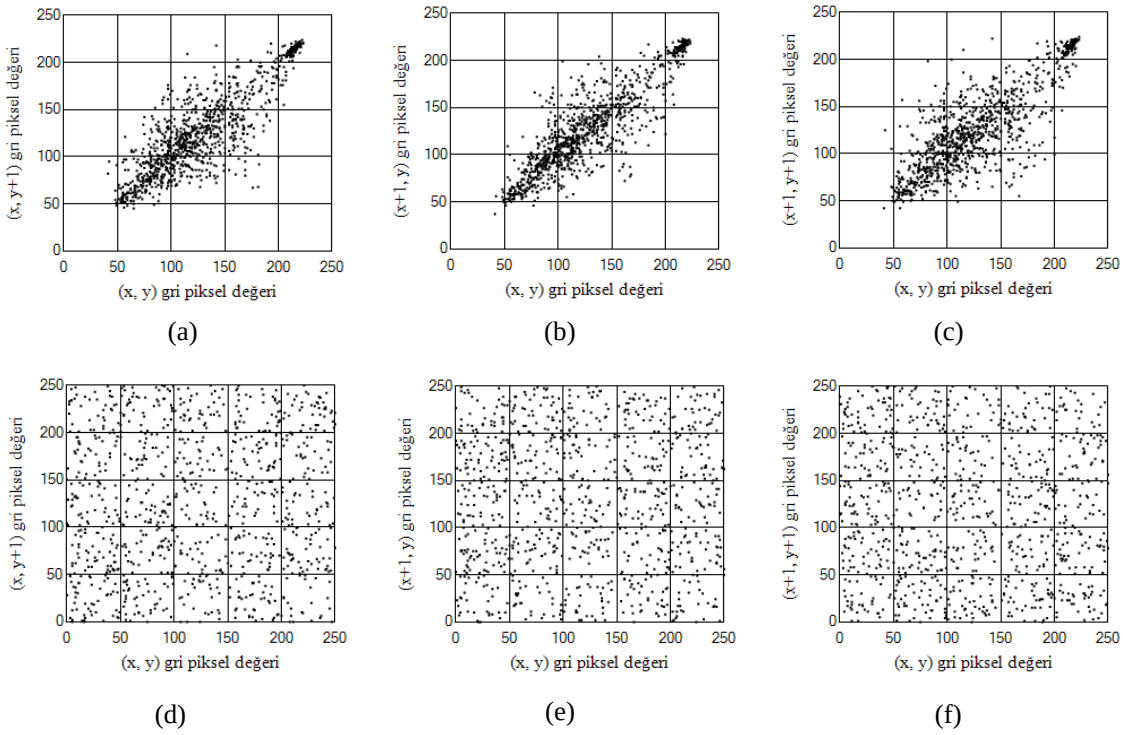
$$E(u) = \frac{1}{p}\sum_{i=1}^{p} u_i \tag{24}$$

$$D(u) = \frac{1}{p}\sum_{i=1}^{p} (u_i - E(u))^2 \tag{25}$$

$$cov(u, v) = E\{(u - E(u))(v - E(v))\} \tag{26}$$

$$r_{uv} = \frac{cov(u, v)}{\sqrt{D(u)D(v)}} \tag{27}$$

Burada u ve v resimdeki bitişik iki pikselin değerleri ve p seçilen piksel çiftinin sayısını göstermektedir. Aynı hesaplama dikey ve köşegenler yönünde de hesaplanır. Düz görüntünün komşu pikselleri arasındaki korelasyon katsayıları genellikle fazladır ve 1'e yaklaşır. Şifrelenmiş görüntülerde ise genellikle küçüktür ve 0'a yaklaşır. İyi bir kripto sistem düz resimdeki bitişik piksellerin ilişkilerini şifreli resimde mümkün olduğu kadar ortadan kaldırmalıdır. 1000 çift komşu piksel ile yapılan korelasyon katsayısı analizinin grafiksel gösterimi Şekil 2.9'da gösterilmiştir. Düz resimdeki doğrusal piksel ilişkisinin şifreli resimde olmadığını Şekil 2.9'a bakarak kolayca anlayabiliriz. Tablo 5'de bu çalışmadaki şifreleme yönteminde piksel tabanlı karıştırmanın ve bit tabanlı karıştırmanın ayrı ayrı kullanılmasıyla şifrelenen resimlerin korelasyon katsayılarının karşılaştırmaları gösterilmiştir. Aynı zamanda AES şifreleme standardının farklı boylardaki anahtarlarıyla şifrelenen resmin yatay, dikey ve diyagonal komşuluklara göre hesaplanmış korelasyon katsayılarının karşılaştırmaları da bu tabloda gösterilmiştir.



Şekil 2.9. Korelasyon grafikleri (a), (b), (c) sırasıyla yatay, dikey ve diyagonal komşu piksellerin düz mandrill resmindeki ilişkileri (d), (e), (f) sırasıyla yatay, dikey ve diyagonal komşu piksellerin şifreli mandrill resmindeki ilişkileri

Tablo 5. Farklı yöntemlerle şifrelenen resimlere ait komşu piksellerin korelasyon katsayıları

	Düz Mandril Resmi	Bu çalışmadaki şifreleme yöntemi (m =2, n =3)	Piksel karıştırma kullanılarak yapılan şifreleme (m =2, n =3)	AES 128 bit anahtar	AES 256 bit anahtar
Yatay	0.96280	-0.03699	-0.02343	0.02857	0.01058
Dikey	0.93412	0.00095	-0.04028	0.01736	-0.03881
Diyagonal	0.91884	0.00053	0.02044	0.00722	-0.01624

2.4.3. Diferansiyel Atak Analizi

Diferansiyel kriptanaliz ilk defa Biham ve Shamir [48] tarafından ortaya atılmıştır. Seçilmiş düz metin atağı olan diferansiyel atakta amaç, gizli anahtarı bulmaktır. Diferansiyel atak, düz metin üzerindeki küçük değişikliklerin şifreli resim üzerinde ne gibi değişiklikler meydana getirdiğini inceler. Bu değişiklikler mümkün olan anahtarları belirlemede kullanılabilir.

Resim şifrelemede diferansiyel atak için genel strateji, rastgele seçilmiş orijinal resim ve rastgele bir pikseli değiştirilmiş halinin aynı anahtarla şifrelenmesi ile elde edilen şifreli resimlerinin karşılaştırılmasıdır. Eğer bu tarz analizlerde düz resim ve şifreli resim arasında anlamsal bir ilişki elde edilirse, bu durum anahtarın tespit edilmesinde kullanılabilir. Eğer düz resimdeki küçük bir değişiklik şifreli resimde tahmin edilemez önemli bir değişime yol açıyorsa, bu tarz diferansiyel ataklar etkisiz kalmaktadır. Bu çalışmadaki şifreleme yönteminin, diferansiyel ataklara karşı güvenilirliğini test etmek için en çok kullanılan iki ölçüm yöntemi olan piksel değişme oranının sayısı (NPCR - Number of Pixel Change Rate) ve birleşik ortalama değişen yoğunluk (UACI - Unified Average Changing Intensity) yöntemleri kullanılmıştır.

NPCR, tek bir pikselleri farklı iki düz resmin aynı anahtar ile şifrelenmesiyle elde edilen şifreli resimlerdeki piksel farklılıklarının oranıdır ve (29)'daki gibi hesaplanır. UACI, iki şifreli resim arasındaki ortalama yoğunluk farkıdır ve (30)'deki gibi hesaplanır. Burada c_1 ve c_2 sırasıyla, düz resmin ve tek bir pikseli değiştirilmiş halinin aynı anahtarla şifrelenmiş şifreli resimleridir.

$$D(i,j) = \begin{cases} 1, & c_{1(i,j)} \neq c_{2(i,j)} \\ 0, & \text{otherwise} \end{cases} \quad (28)$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \text{ x } N} \text{ x } 100\% \quad (29)$$

$$UACI = \frac{1}{MxN}\left[\sum_{i,j} \frac{|c_{1(i,j)} - c_{2(i,j)}|}{255}\right] \text{ x } 100\% \quad (30)$$

Bu çalışmada kullanılan şifreleme yönteminin farklı döngülerdeki NPCR ve UACI karşılaştırma sonuçları Tablo 6'da gösterilmektedir. Bu çalışmadaki NPCR ve UACI değerlerinin ideal değerlere zamanla çok çabuk yaklaşması, kaotik resim şifreleme yönteminin diferansiyel ataklara karşı güvenilir olduğunu göstermektedir.

Tablo 6. Çalışmadaki kaotik resim şifrelemenin NPCR ve UACI karşılaştırmaları

(m, n)	**NPCR**	**UACI**
	Bit tabanlı karıştırma ile	**Bit tabanlı karıştırma ile**
(1, 2)	57,96661	23,23257
(1, 3)	81,32934	20,40352
(1, 4)	83,13598	20,89685
(2, 2)	97,56011	29,91231
(2, 3)	99,52697	33,48819
(2, 4)	99,34311	33,18764
(3, 2)	99,66474	33,58573
(3, 3)	99,39046	33,39480
(3, 4)	99, 37811	33,13362

2.4.4. Performans Analizi

Özellikle gerçek zamanlı internet uygulamaları için şifreleme algoritmasının koşma hızı çok önemlidir. Bu çalışmadaki şifreleme yönteminin, AES ve kaotik bit tabanlı karıştırma metotlarının performans karşılaştırmaları Tablo 7'de gösterilmiştir.

Tablo 7. Farklı boyutlardaki resimlerin şifrelemelerdeki performans karşılaştırmaları

	Şifreleme süresi (ms)	
Algoritma	Resim boyutu 256x256	Resim boyutu 512x512
Çalışmadaki Yöntem (m =3, n =3)	0.252	0.873
Piksel tabanlı karıştırma ile çalışmadaki yöntem (m =3, n=3)	0.183	0.540
AES 128 bit	0.132	0.467
AES 256 bit	0.146	0.481

Çalışmamızda 256x256 boyutlarına sahip mandrill resmi için ortalama şifreleme hızı 0.252 ms'dir. Bu şifreleme hızı, algoritmanın paralel işlenmeye uygun bölümleri paralel işlenerek artırılabilir. Şifreleme yönteminin ilk aşaması olan bit karıştırma aşamasına tabi tutulan 8 ayrı resim arasında veri bağımlılığı yoktur. Bu durum, kolayca sistemin bahsedilen kısmının paralel işlenebilmesini sağlar.

2.4.5. Anahtar Duyarlılık Analizi

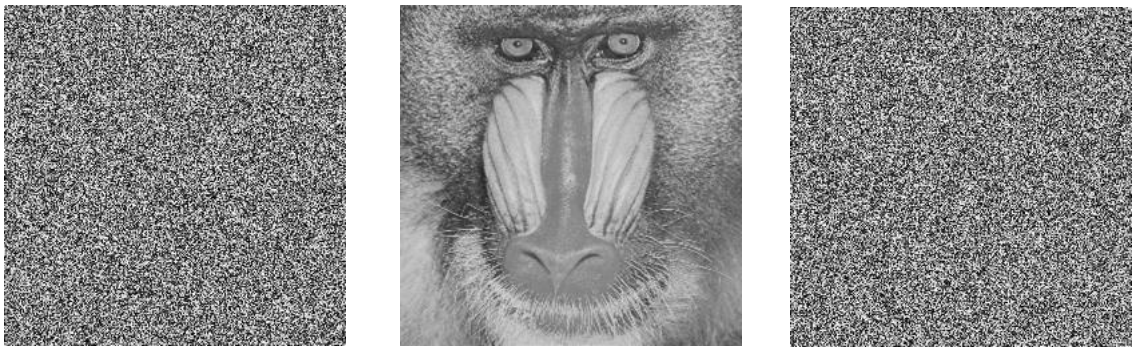
Güçlü bir şifreleme sistemi, şifreleme ve şifre çözme anahtarlarındaki çok küçük değişikliklere karşı duyarlı olmalıdır. Şifreleme aşamasında, şifreleme için kullanılan anahtardaki çok küçük bir değişiklik sonucu ortaya çıkan şifreli resim, gerçek şifreli resimden çok farklı olmalıdır. Yine benzer şekilde, şifre çözme aşamasında kullanılan anahtardaki çok küçük bir değişimle elde edilen yeni anahtar ile şifre çözme gerçekleştirildiğinde, elde edilen yeni düz resim ile gerçek düz resim arasında istatistiksel benzerlikler bulunmamalıdır.

Birbirine çok yakın anahtarlar ile yapılan şifreleme ve şifre çözme testleri, sistemin gizli anahtarlardaki en ufak bir değişime karşı duyarlı olduğunu göstermektedir. Aynı düz resmi, gerçek gizli anahtardaki küçük bir değişiklikle şifrelemeye soktuğumuzda üretilen şifreli resim ile gerçek şifreli resim arasındaki piksel farkları Tablo 8'de gösterilmektedir.

Şifreli resme, gerçek anahtar ve çok küçük bir değişikliğe uğramış anahtar ile şifre çözme işlemi uyguladığımızda elde edilen düz resimler Şekil 2.10'da gösterilmektedir. Tablo 8'den ve Şekil 2.10'dan anlaşıldığı gibi bu çalışmadaki şifreleme sistemi, şifreleme ve şifre çözme aşamalarında, anahtarlardaki çok küçük değişikliklere karşı duyarlıdır.

Tablo 8. Aralarında çok küçük fark bulunan anahtarlarla şifrelenen resmin piksel farkları

	NPCR	
Resim	**Resim boyutu 256x256**	**Resim boyutu 512x512**
Mandrill	99.60352	99.60645



(a) (b) (c)

Şekil 2.10. Şifre çözmede anahtar duyarlılığı (a) şifreli mandrill resmi (b) gerçek anahtarla şifresi çözülmüş düz mandrill resmi (c) anahtarda 10^{-15} kadar bir değişiklik yapılarak şifre çözülmesi sonucu oluşan anlamsız resim

2.4.6. Anahtar Uzayı Analizi

Etkili bir şifreleme sistemi kaba kuvvet ataklarına karşı koyacak kadar yeterli anahtar uzunluğuna sahip olmalıdır. Teorik olarak kaba kuvvet atakları ile kırılamayan şifreleme sistemi yoktur. Ancak mevcut teknoloji ile kaba kuvvet ataklarının başarılı olma süreleri, yeterli anahtar boylarıyla uzatılabilmektedir. Bundan dolayı AES gibi şifreleme sistemleri, birden fazla farklı anahtar boyları ile standartlaştırılmışlardır. AES şifreleme standardı 128, 192 ve 256 bit uzunluğundaki anahtarlar ile kullanılabilmektedir. Alvarez ve Li, günümüzde şifreleme sistemlerinin kaba kuvvet ataklarına karşı koyabilmesi için anahtar

boylarının en az 2^{100} uzunluğunda olması gerektiğini önermişlerdir [49]. Asimetrik ve simetrik şifreleme algoritmalarının anahtar uzunlukları birbirlerinden oldukça farklıdır.

Bit tabanlı kaotik şifreleme sisteminde gizli anahtar, karıştırma ve yayılma aşamalarındaki anahtarların birleşiminden oluşmaktadır. Karıştırma aşamasında ayrık kaotik cat haritası için p ve q kontrol parametreleri ve m döngü sayısı gizli anahtarlardır. Burada p, q ve m pozitif tamsayılardır. Difüzyon aşamasında $x_0 \in (0,1)$ ve kontrol parametresi $r \in (3.57,4)$ gizli anahtarlar olarak alınır. Burada r kontrol parametresinin (3.57, 4) aralığında sistemin kaotik olduğu bölgelerden seçilmesi gerekmektedir.

NxN boyutlu bir resmin şifrelenmesinde, ayrık kaotik cat haritasındaki p ve q değerleri pozitif olmak şartıyla sonsuz değerde alınabilir. Ancak, pratikte p ve q değerleri sadece N uzunluğunda sınırlıdırlar. Ayrık kaotik cat haritasında $[1, (p + k_1N), (q + k_2N), (p + k_1N)(q + k_2N) + 1]$ şeklindeki dört çift, pozitif k_1 ve k_2 değerleri için $[1, p, q, (pq + 1)]$ dört çifti ile aynı şifrelemeyi yapar. Bundan dolayı döngü sayısı m olan karıştırma aşamasındaki toplam anahtar sayısı N^{2m}'dir.

IEEE kayan-noktalı standardına [50] göre 64 bitlik çift duyarlılıklı sayıların hesaplama duyarlılıkları yaklaşık 10^{-15}'dir. Yayılma aşamasında x_0 için toplam anahtar sayısı 10^{15} ve r için yaklaşık anahtar sayısı toplamı $\frac{10^{15}}{2}$ 'dir. Bit tabanlı kaotik resim şifreleme için toplam anahtar uzayı H, birbirinden bağımsız iki şifreleme aşamasının anahtarlarının çarpımı ile belirlenir. $N \geq 256$, $m = 3$ olduğunda yaklaşık toplam anahtar uzayı $H(x_0, r, a, b, m) \geq 10^{15} \times \frac{10^{15}}{2} \times 256^6 \geq 2^{190}$'dır. Bu uzay kaba kuvvet ataklarına karşı koymak için yeterlidir.

2.4.7. Bilgi Entropisi Analizi

Entropi, 1948'de Shannon tarafından tanımlanan ve bilgi teorisinden gelen bir kavramdır [51]. Entropi sistemde var olan belirsizliğin derecesini ölçer. Bir dizi ne kadar tahmin edilebilir ise o kadar fazla bilgi içermektedir. Bu yüzden bilgiyi gizlemenin yolu, tahmin edilebilirliği ortadan kaldırmaktır. Bir mesajın entropisi H(m) (31)'deki gibi hesaplanabilir.

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log \frac{1}{p(m_i)} \quad (31)$$

Burada L toplam sembol sayısını belirtmektedir ve resim şifrelemede piksel değerlerinin toplam sayısıdır. Logaritma 2 tabanına göre alınmaktadır. Bir pikselin m_i değerinde olma olasılığı $p(m_i)$ ile gösterilir. Eğer şifrelenmiş resmin entropisi logaritma L'ye yeterince yaklaşırsa, resmin histogramı yeterince düzgündür denilebilir. Örneğin bir mesajın, 2^8 sembolü ($s = \{ s_1, s_2, \dots, s_{2^8} \}$) aynı olasılıkta bulundurduğunu varsayarsak, denklem (31) H(s) = 8 olacak şekilde gerçek rastgele değer üretir. Bu değer ideal olan değerdir. Fakat gerçekte, şifrelenen bir mesajın içeriği gerçek rasgele sembolleri çok nadir içerir. Bundan dolayı şifreli mesajın entropisi ideal değerinden düşüktür.

Şifrelenmiş resimdeki tüm gri seviye değerlerin bulunma olasılığı hesaplandıktan sonra, farklı döngülerle şifrelenmiş resmin H(m) entropi değerleri Tablo 9'da gösterilmiştir. Bu değerler ideal olan 8 değerine oldukça yakındır. Bundan dolayı şifreleme sisteminin entropi ataklarına karşı güvenli olduğu söylenebilir. Tablo 10'da kaotik bit tabanlı, kaotik piksel tabanlı ve AES şifreleme algoritması ile şifreleme sonucu elde edilen şifreli resimlere ait entropi değerlerinin karşılaştırılması gösterilmektedir.

Tablo 9. Farklı döngülerle şifrelenmiş mandril resminin entropi değerleri

	Entropi	
Döngü Sayıları (m, n)	**Resim boyutu 256x256**	**Resim boyutu 512x512**
(1, 2)	7,9969	7,9993
(1, 3)	7,9973	7,9992
(2, 2)	7,9970	7,9992
(2, 3)	7,9970	7,9993
(3, 2)	7,9973	7,9993
(3, 3)	7,9971	7,9993
(4, 2)	7,9971	7,9992
(4,3)	7,9970	7,9993

Tablo 10. Bit tabanlı, piksel tabanlı ve AES ile şifrelenmiş resmin entropi değerleri

	Entropi	
Algoritma	**Resim boyutu 256x256**	**Resim boyutu 512x512**
Piksel tabanlı karıştırma (m =3, n =2)	7,9968	7,9989
Bit tabanlı karıştırma (m =3, n=2)	7,9973	7,9993
AES 128 bit	7,9962	7,9992
AES 256 bit	7,9969	7,9993

2.4.8. Şifreleme Kalitesi Analizi

Resim şifreleme kalitesinin ölçümü, resim şifreleme tekniklerinin analizlerinde kullanılan bir değerlendirmedir. Bir resmin şifreleme işlemi ile değişen piksel değerleri, şifrelemeden önceki orijinal değerleri ile karşılaştırılarak şifreleme kalitesi ölçülür. Bir resmin şifreleme işlemi ile piksel değerleri büyük ölçüde değişir. Bu değişim düzensizdir. Piksel değerlerinde değişim ne kadar fazlaysa şifreleme tekniğinin etkisi ve kalitesi o kadar fazladır. Bir resim şifreleme algoritması için şifreleme kalitesi, düz resim ve şifreli resim arasındaki sapma (deviation) olarak ifade edilir [52].

P ve C sırasıyla, M x N boyutlarında ve L gri seviyede düz resim ve bu düz resmin şifreli resmini temsil etmektedir. P(x, y), C(x, y) ∈ { 0,1,2…L-1 } sırasıyla, P düz resim ve C şifreli resmin $0 < x < M - 1$ ve $0 < y < N - 1$ olacak şekilde (x,y) konumundaki gri seviye değerleridir. HL(P) her bir L gri seviye piksel değerinin şifreli resimde bulunma miktarı ve HL(C) her bir L gri seviye piksel değerinin düz resimde bulunma miktarı olarak tanımlanırsa, şifreleme kalitesi her bir L gri seviye miktarının ortalama değişimi olarak (32)'deki gibi hesaplanır

$$\text{Şifreleme Kalitesi} = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256} \tag{32}$$

Hazırlanan çalışmadaki bit tabanlı karıştırma kullanan resim şifreleme yöntemi için farklı döngülerde hesaplanan şifreleme kalitesi değerleri ve farklı şifreleme yaklaşımlarıyla karşılaştırılması Tablo 11'de gösterilmiştir. Tablo 11'e göre bit tabanlı karıştırma

kullanılarak yapılan kaotik şifrelemenin şifreleme kalitesi, piksel tabanlı karıştırma kullanılarak yapılan kaotik şifrelemeyle ve AES algoritmasıyla yapılan şifrelemeden daha iyidir.

Tablo 11. Farklı döngülerle çalışmadaki yöntem ve AES için şifreleme kaliteleri

	Şifreleme Kalitesi	
Döngü sayısı (m, n)	**Resim boyutu 256x256**	**Resim boyutu 512x512**
(1, 2)	193,50	797,29
(1, 3)	194,38	799,79
(2, 2)	194,06	799,22
(2, 3)	195,67	794,68
(3, 2)	192,35	797,32
(3,3)	195,86	795,66
AES 128 bit	190,27	793,76
AES 256 bit	190,45	794,37
Piksel Tabanlı Karıştırma (m= 3, n = 3)	189,40	789,67

3. SONUÇLAR

Bu tezde genel kaotik resim şifreleme yöntemlerinde yeni bir yaklaşım olan bit tabanlı kaotik piksel karıştırma yöntemi ile beraber, geliştirilmiş yayılma tekniği kullanılarak yeni bir resim şifreleme yaklaşımı önerilmiştir. Karıştırma aşamasında piksel tabanlı karıştırma ile bit tabanlı karıştırma ayrı ayrı kullanılarak, bu yaklaşımların güvenilirlikleri gözlemlenmiştir. Şifreleme yönteminde kullanılan kaotik haritaların özellikleri incelenerek sayısal sistemlerde kullanılabilirlikleri irdelenmiştir. Şifreleme yönteminin güvenilirliğini göstermek için, geleneksel şifrelemeler ile karşılaştırmalar da yapılarak gerekli güvenlik ve istatistiksel analizleri yapılmıştır.

Güvenlik ve istatistiksel analizler sonucunda, bit tabanlı kaotik karıştırmanın piksel tabanlı kaotik karıştırmaya nazaran, yayılma aşamasını çok daha fazla etkilediği yapılan testlerde gözlemlenmiştir. Bit tabanlı karıştırmada sekiz resim üzerinde işlem yapıldığı için hesaplama karmaşıklığı artmaktadır. Ancak şifrelemenin ilk aşaması olan karıştırma aşamasında, bit tabanlı karıştırma ile çok daha düşük döngülerde başarılı sonuçlar elde edilmiştir. Her iki yöntemin karşılaştırmalı olarak zayıf ve güçlü taraflarının değerlendirmeleri yapılmıştır.

Yayılma aşamasında her piksele etki eden parametre sayısı artırılarak sistem daha güvenli hale getirilmiştir. Böylece yayılma aşamasında analitik ataklara karşı daha düşük döngülerle daha fazla güvenilirlik elde edilmiştir.

4. ÖNERİLER

Bu çalışmada kaotik resim şifrelemelerde piksel yerine bit tabanlı karıştırma ile şifreleme önerilmektedir. Karıştırma aşamasında, bit tabanlı karıştırma istatistiksel özellikleri ortadan kaldırmada piksel tabanlı karıştırmadan daha başarılıdır.

Yayılma aşamasında piksel değerlerinin birden fazla parametreye bağlı olacak şekilde değişmesi güvenliği artırır. Analiz edilmesi gereken birden fazla parametre sistemi daha fazla güvenilir hale getirir.

Piksel tabanlı karıştırma ile yapılan şifrelemelerde istatistiksel özellikleri ortadan kaldırmak için gereken toplam döngü sayısı, bit tabanlı karıştırma ile yapılan şifrelemelere göre daha fazladır. Döngü sayısı hesaplama karmaşıklığı ile doğru orantılıdır. Bit tabanlı karıştırma ile daha düşük hesaplama karmaşıklığı elde edilebilir.

Diferansiyel ataklar düz metin üzerindeki değişikliklerin şifreli metin üzerindeki etkilerini inceler. Diferansiyel ataklara karşı koymak için gereken piksel değişim oranları, piksel tabanlı karıştırmaya nazaran bit tabanlı karıştırma ile daha düşük döngülerle elde edilebilir.

Hesaplama karmaşıklığı çok düşük olan tek boyutlu kaotik haritalar, resim şifrelemede düz resim ve şifreli resim arasındaki ilişkiyi ortadan kaldırmak için kullanılabilir. Piksel değerlerini değiştirmek için gereken rastgele değerleri düşük hesaplama karmaşıklığında tek boyutlu kaotik haritalar ile elde edebiliriz.

Kaotik şifreleme sistemlerinin analizi geleneksel şifreleme sistemlerinden biraz farklıdır. Çok fazla analiz karmaşıklığına sahip olan bu sistemlerin güvenlik analizlerinin çok iyi yapılması gerekmektedir.

5. KAYNAKLAR

1. FIPS 46, Data Encryption Standard, US Government Printing Office, Washington D. C, 1977.

2. FIPS 197, Advanced Encryption Standard, US Department of Commerce, Washington D. C, 2001.

3. Chen, J. Y., Wong, K. W. L., Cheng, M. ve Shuai, J. W., A Secure Communication Scheme Based on the Phase Synchronization of Chaotic Systems, Chaos, 13 (2003) 508-514.

4. Li, Z. ve Xu, D., A Secure Communication Scheme Using Projective Chaos Synchronization, Chaos, Solitons and Fractals, 22, 2 (2004) 477-481.

5. Habutsu, T., Nishio, Y., Sasase, I. ve Mori, S., A Secret Key Cryptosystem by Iterating a Chaotic Map, Proc. of Advances in Cryptology-CRYPTO '91, Ağustos 1991, California, Springer-Verlag, 127-140.

6. Baptista, M. S., Cryptography with Chaos, Physics Letters A, 240 (1998) 50-54.

7. Wong, K.W., A Fast Chaotic Cryptographic Scheme with Dynamic Look-up Table, Physics Letters A, 298, 4 (2002) 238-242.

8. Fridrich, J., Image Encryption Based on Chaotic Maps , In Proceedings IEEE Int. Conference on Sysytems, Man and Cybernetics (ICSMC 97), Ekim 1997, Orlando, 2, 1105-1110.

9. Mao, Y.B. ve Chen, G., Handbook of Computational Computing, Corrochano, E. B., 231-265, Springer-Verlag, Berlin, 2005.

10. Guan, Z.H., Huang, F.J. ve Guan, W.J., Chaos-based Image Encryption Algorithm, Physics Letters A, 346 (2005) 153-157.

11. Lian, S.G., Sun, J. ve Wang, Z., A Block Cipher Based on a Suitable Use of Chaotic Standard Map, Chaos, Solitons and Fractals, 26, 1 (2005) 117-129.

12. Schneier, B., Applied Cryptography , Second Edition, John Wiley and Sons, New York, 1996.

13. Kocarev, L., Chaos-Based Cryptography: A Brief Overview, IEEE Circuits and Systems Magazine, 1, 3 (2001) 6-21.

14. Stinson, D., Cryptography: Theory and Practice , Second Edition, Chapman & Hall / CRC, Boca Raton, 2002.

15. Kerckhoffs, A., La cryptographie militaire, Journal des sciences militaires, IX (1883) 161-191.

16. Mao, Y., Chen, G. ve Lian. S., A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps , International Journal of Bifurcation and Chaos, 14, 10 (2004) 3613-3624.

17. Li, S., Analyses and New Designs of Digital Chaotic Ciphers, Ph. D. Thesis, School of Electronics & Information Engineering, Xi an Jiaotong University, Xi an, 2003.

18. FIPS 81, Data Encryption Standard Modes of Operation, US Government Printing Office, Washington D. C, 1980.

19. Li, S., Chen, G. ve Zheng, X., Multimedia Security Handbook, CRC Press LLC, Boca Raton, 2004.

20. Mao, Y. ve Wu, M., A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption , IEEE Transactions on Image Processing, 15, 7 (2006) 2061-2075.

21. Mao, Y., Research on Chaos-Based Image Encryption and Watermarking Technology, Ph. D. Thesis, Department of Automatation, Nanjing University of Science & Technology, Nanjing, 2003.

22. Li, S., Mou, X. ve Cai, Y., Pseudo-Random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream Cipher Cryptography, Indocrypt, Aralık 2001, Berlin, Springer-Verlag LNCS, 316-329.

23. Kusters, R. ve Tuengerthal, M., Universally Composable Symmetric Encryption, 22nd IEEE Computer Security Foundations Symposium (CSF '09), Temmuz 2009, New York, Conference Publications, 293- 307.

24. Jin. H., Liao, Z., Zou, D. ve Li, C., Asymmetrical Encryption Based Automated Trust Negotiation Model , The 2nd IEEE International Conference on Digital Ecosystems and Technologies (DEST 2008), Şubat 2008, Phitsanulok, Conference Publications, 363- 368.

25. Shannon, C. E., Communication Theory of Secrecy Systems, Bell System Technical Journal, 28, 4 (1949) 656-715.

26. Werndl, C., What are the New Implications of Chaos for Unpredictability?, The British Journal for the Philosophy of Science, 60, 1 (2009) 195–220.

27. Hasselblatt, B. ve Katok, A., First Course in Dynamics: With a Panorama of Recent Developments. Cambridge University Press, Cambridge, 2003.

28. May, R. M., Simple mathematical model with very complicated dynamics. Nature, 261 (1976) 459-467.

29. http://en.wikipedia.org/wiki/Arnold's_cat_map Arnold's cat map. 10 Aralık 2011.

30. Elert, G., The Chaos Hypertextbook, http://hypertextbook.com/chaos Lyapunov Exponents. 20 Ocak 2012.

31. Gutmann, P., Naccache D., ve Palmer, C., Randomness in cryptography. IEEE security and privacy, 4, 2 (2006) 64-67.

32. Hu, Y., Liao, X., Wong, K. ve Zhou, Q., "A true random number generator based on Mouse movement and chaotic cryptography" Choas, solitons and Fractals, 40, 5 (2007) 2286-2293.

33. Lehmer, D.H., Mathematical methods in large-scale computing units, Ann. Computing Lab. Harvard Univ., 26 (1951) 141-146.

34. http://www.agner.org/random/theory/ Chaotic random number generators with random cycle lengths. 5 Şubat 2012.

35. Patidar, V., Pareek N. K. ve Sud, K. K., A pseudo random bit generator based on chaotic logistic map and its statistical testing, Journal of Informatical, 1, 1-3 (2009) 441-452.

36. Li, S. J., Mou, X. Q. ve Cai, Y. L., Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography, Indocrypt, Aralık 2001, Chennai, Lecture Notes in Computer Science, 316–329.

37. Chen, G., Mou. X. ve Li. S., On the Dynamical Degradation of Digital Piecewise Linear Choatic Maps, International Journal of Bifurcation and Chaos, 15, 10 (2005) 3119-3151.

38. Matthews, R., On the derivation of a chaotic encryption algorithm, Journal Cryptologia, 13, 1 (1989) 29-42.

39. Habutsu, T., Nishio, Y., Sasase, I. ve Mori, S., A secret key cryptosystem by iterating chaotic map, EUROCRYPT, Nisan 1991, Brighton, Lecture Notes in Computer Science, 127–140.

40. Bianco, M. E. ve Reed, D., An encryption system based on chaos theory, A.B.D. Patent No. 5048086, 1991.

41. Zhang, L., Liao, X. ve Wang, X., An image encryption approach based on chaotic maps, Chaos, Solitons and Fractals, 24 (2005) 759-765.

42. Waelbroeck, H. ve Zertuche, F., Discrete chaos, Journal of Physics A, 32, 1 (1999) 175-189.

43. Dachselt, F. ve Schwarz, W., Chaos and cryptography, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48, 12 (2001) 1498–1509.

44. Carroll, T. L. ve Pecora, L. M., Synchronizing Chaotic Circuits, IEEE Transactions on Circuits and Systems, 38, 4 (1991) 453-456.

45. Li, S., Analyses and newdesigns of digital chaotic ciphers. Ph.D.Thesis, Xi an Jiaotong Unversity, Xi an 2005.

46. Li, X., Knipe, J. ve Cheng, H., Image Compression and Encryption Using Tree Structures , Pattern Recognition Letters, 18, 8 (1997) 2439-2451.

47. Guo, J. I., Yen, J. C. ve Yeh, J. C., The Design and Realization of A New Hierarchical Chaotic Image Encryption Algorithm, In Proceedings Int. Symposium on Communications (ISCOM 99), Kasım 1999, Kaohsiung, Conference Publications 210-214.

48. Alvarez, G., Montoya, F., Romera, M. ve Pastor, G., Cryptanalysis of a chaotic secure communication system, Physics Letters A, 276 (2000) 191-196.

49. Alvarez, G. ve Li, S.J., Some basic cryptographic requirements for chaos-based cryptosystem, Int. J. Bifurcat. Chaos,16, 8 (2006) 2129–2151.

50. IEEE Computer Society, IEEE Standard for Binary Floating-Point Arithmetic, ANSI/IEEE, Los Alamitos, Ağustos 1985.

51. Shannon, C. E., A mathematical theory of communication, Bell System Technical Journal, 27, 4 (1948) 379–423.

52. Ahmed, H. H., Kalash, H. M. ve O. S. Farag Allah, Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images, Journal of Optical Engineering, 45, 10 (2006) 277-284.

ÖZGEÇMİŞ

1982 yılında Gümüşhane'de doğdu. İlköğrenimini Erzincan İnönü İlkokulu ve Erzincan Anadolu Lisesi'nde, orta öğrenimini Trabzon Tevfik Serdar Anadolu Lisesi'nde tamamladı. 2003 yılında Ahmet Yesevi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde lisans programına başladı ve 2008 yılında bu bölümden mezun oldu. 2009 yılında Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans programına başladı. 2011 yılından itibaren, PTT Genel Müdürlüğünde Bilgisayar Mühendisi olarak görev yapmaktadır. Yabancı dil olarak İngilizce ve Rusça bilmektedir.