T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
ELEKTRİK – ELEKTRONİK ANABİLİM DALI

IKEDA VE HENON KAOTİK HARİTALARI KULLANARAK GÖRÜNTÜ ŞİFRELEME

YÜKSEK LİSANS TEZİ

HAZIRLAYAN: Yeter ŞEKERTEKİN
DANIŞMAN: Yrd. Doç. Dr. Özkan ATAN

VAN-2017

T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
ELEKTRİK – ELEKTRONİK ANABİLİM DALI

IKEDA VE HENON KAOTİK HARİTALARI KULLANARAK GÖRÜNTÜ ŞİFRELEME

YÜKSEK LİSANS TEZİ

HAZIRLAYAN: Yeter ŞEKERTEKİN

VAN-2017

KABUL VE ONAY SAYFASI

Elektronik Anabilim Dalı'nda Yrd. Doç. Dr. Özkan Atan danışmanlığında, Yeter Şekertekin tarafından sunulan **"Ikeda ve Henon Kaotik Haritaları Kullanarak Görüntü Şifreleme"** isimli bu çalışma Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili hükümleri gereğince 28/07/2017 tarihinde aşağıdaki jüri tarafından oy birliği ile başarılı bulunmuş ve yüksek lisans tezi olarak kabul edilmiştir.

Başkan: Doç. Dr. Mustafa TÜRK İmza:

Üye: Doç. Dr. Rıdvan SARAÇOĞLU İmza:

Üye: Yrd. Doç. Dr. Özkan ATAN İmza:

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun …./..../….. tarih ve ..... sayılı kararı ile onaylanmıştır.

İmza

……..……..

Enstitü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Yeter ŞEKERTEKİN

ÖZET

IKEDA VE HENON KAOTİK HARİTALARI KULLANARAK GÖRÜNTÜ ŞİFRELEME

ŞEKERTEKİN, Yeter
Yüksek Lisans Tezi, Elektrik - Elektronik Anabilim Dalı
Tez Danışmanı: Yrd. Doç. Dr. Özkan ATAN
Temmuz 2017, 94 sayfa

Bu tez çalışmasında haritalar olarak da bilinen kaotik ayrık sistemlerden ikisi kullanılarak bir görüntü şifreleme ve şifre çözme algoritması geliştirilmiş, bu algoritma Matlab benzetim ortamında denenmiştir. Görüntü denilen yapıların kendine has özelliklerinden dolayı, düz metin şifrelemede güvenilir sonuçlar veren klasik şifreleme metotları, görüntü şifrelemede güvenlik açısından yetersiz kalmaktadır. Bu yüzden, kriptolojinin (şifreleme bilimi) gereksinimlerinin önemli ölçüde karşılık bulduğu kaotik sistemler kullanılarak güvenilir bir görüntü şifreleme algoritması geliştirilmesi amaçlanmıştır. Bu kapsamda, yer değiştirme ve yerine koyma işlemleri için kullanılan haritaların kaotik açıdan özellikleri incelenmiş ve bu haritalar, şifrelemede en çok kullanılan diğer kaotik haritalarla karşılaştırılmıştır. Geliştirilen algoritmada ilk önce Ikeda kaotik harita ile piksellerin konumu değiştirilmiştir. Ardından Henon kaotik harita ile piksellerin gri renk seviyesi değiştirilmiş, sonrasında ise Ikeda harita ile piksellerin konumu ikinci kez değiştirilmiştir. Böylelikle, istatiksel açıdan yeterince güçlü bir algoritma elde edilmeye çalışılmıştır.

Çalışmada geliştirilen algoritma, görüntünün karakteristik özellikleri göz önünde bulundurularak çeşitli güvenlik ve performans testlerinden geçirilmiştir. Böylece şifreleme ve kriptanaliz açısından incelenen algoritmanın, bazı görüntü şifreleme algoritmalarına göre daha güvenilir sonuçlar verdiği doğrulanmıştır.

Anahtar kelimeler: Henon, Ikeda, Görüntü Şifreleme, Kaos

ABSTRACT

IMAGE ENCRYPTION USING IKEDA AND HENON CHAOTIC MAPS

ŞEKERTEKİN, Yeter
M. Sc. Thesis, Electrical-Electronics Engineering
Supervisor: Assist. Prof. Dr. Özkan ATAN
July 2017, 94 Pages

In this study, an image encryption and decryption algorithm have been developed using two of the chaotic discrete systems known as maps and it is simulated on Matlab environment. Owing to the fact that images have peculiar features, traditional encryption methods which have reliable results for plain text encryption don't satisfied in terms of image encryption. Therefore, it is intended that developing a secure image encryption algorithm using chaotic systems which are matched with requirements of cryptology. In this context, it is examined features of Ikeda and Henon chaotic maps which are used for permutation and substitution, and they are compared to other chaotic maps most used in image encryption. In the developed algorithm, it is permuted positions of pixels using Ikeda chaotic map firstly, and then changed gray levels of pixels using Henon chaotic map. After that, the positions of pixels are changed using Ikeda map again. In this way, it is tried to be obtained an algorithm that is strong enough statistically.

Some security and performance tests are applied to developed algorithm by considering the characteristic features of the images. The results of cryptanalysis of the algorithm, and other tests show that it is obtained more secure algorithm when it is compared to some algorithms.

Keywords: Chaos, Henon, Ikeda, Image Encryption

ÖNSÖZ

Hayatımın her aşamasında olduğu gibi, bu tezin hazırlanma aşamasında da maddi ve manevi desteklerini benden hiçbir zaman esirgemeyen sevgili aileme çok teşekkür ediyorum. Görüşleri ve desteğiyle her zaman yanımda olan kıymetli danışmanım Yrd. Doç. Dr. Özkan Atan'a da teşekkürü borç bilirim.

2017

Yeter ŞEKERTEKİN

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELER LİSTESİ

Çizelge **Sayfa**

ŞEKİLLER LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
E_k	Şifreleme fonksiyonu
C	Şifrelenmiş bilgi
D_k	Şifre çözme fonksiyonu
K	Anahtar
BV	Başlangıç vektörü
m	Mesaj

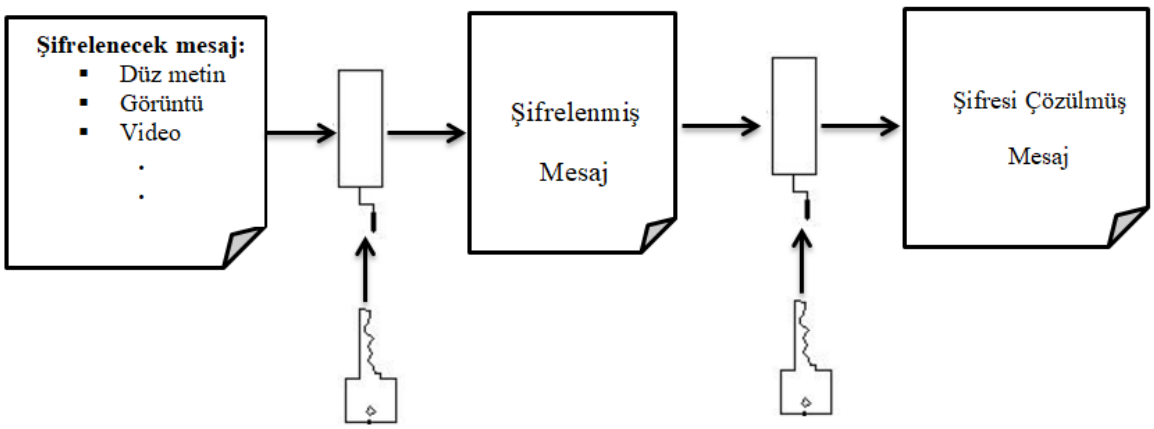
Kısaltmalar	**Açıklama**
AES	Gelişmiş Şifreleme Standardı
CBC	Zincirleme Şifre Blok
CFB	Şifre Geribildirim Modu
CTR	Sayaç Modu
DES	Veri Şifreleme Standardı
ECB	Elektronik Kod Kitabı
IDEA	Uluslararası Veri Şifreleme Algoritması
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü
NPCR	Piksel Değişim Oranı Sayısı
OFB	Çıkış Geribildirim Modu

FPGA	Alanda Programlanabilir Kapı Dizileri
RC4	Rivest Şifre 4
RC5	Rivest Şifre 5
RC6	Rivest Şifre 6
RSA	Rivest, Shamir, Adleman
SPN	Yerine Koyma-Yer Değiştirme Ağı
UACI	Birleşik Ortalama Değişim Yoğunluğu

1. GİRİŞ

Teknolojinin her geçen gün gelişmesi ve hayatlarımıza dâhil olmasının bir sonucu olarak internet erişiminin olduğu cihazlara erişim kolaylaşmakta ve bu sayede internet kullanımı gittikçe artmaktadır. İstatistiklere göre 2016 yılı itibarıyla dünya genelinde aktif internet kullanıcı sayısı 3.5 milyar iken, bu oran cep telefonu kullanıcıları için 5 milyarı bulmaktadır (www.statista.com, Mayıs 2017). Bu oranla birlikte güvenli olmayan internet ortamında yer alan bilgi miktarı da artmaktadır. Bu bilgilerin içinde önemli bir miktarı dijital görüntüler oluşturmaktadır. Bu görüntüler kişisel ve özel olabileceği gibi, kritik öneme sahip askeri ya da medikal görüntüler de olabilmektedir.

Bilginin güvenli olmayan ağ üzerinden paylaşımı, onun korunması için çeşitli yollar aranması sonucunu doğurmuştur. Bilgiyi korumak amacıyla geliştirilen şifreleme bilimi kriptoloji, gönderilecek mesajın bir anahtarla şifrelenmesi ve alıcı tarafta sadece doğru anahtara sahip kişi tarafından çözülmesi ilkesine dayanır. Şekil 1.1 şifreleme biliminin temel çalışma mantığını anlatmaktadır.



Şekil 1.1. Şifrelemenin temsili gösterimi.

Görüntü şifreleme, görüntünün kendine has özellikleri sebebiyle metin mesajlarının şifrelendiği metotlardan farklı metotlarla gerçekleştirilmektedir. Çünkü metin mesajları için kullanılan yöntemler, görüntü için yeterince güvenilir sonuçlar vermemektedir (Chen ve ark., 2004; Li ve ark., 2007). Görüntü şifrelemede en çok uygulanan yöntemler; yer

değiştirme, yerine koyma ya da bu iki yöntemin birlikte kullanıldığı yöntemlerdir. Kaos bilimi ve kriptografi arasındaki benzerliklerden ötürü, bu aşamalar gerçekleştirilirken kaotik fonksiyonlar kullanılabilmektedir (Kocarev, 2001; Masuda ve ark., 2006).

Ayrık kaotik fonksiyonlar olarak bilinen kaotik haritalar, bir ya da birden fazla boyutta olabilir. Şifrelemede doğrudan haritalar kullanıldığı için, birden fazla ve çok boyutlu haritaların kullanılması şifreleme algoritmasını daha güvenilir kılacaktır. Literatürde kaotik haritalar kullanılarak görüntü şifrelemenin gerçekleştirildiği birçok çalışma mevcuttur. Bu çalışmaların çoğunluğunda kullanılan haritanın kaotik özelliklerine de bağlı olarak başarılı sonuçlar elde edilmiştir (Patidar ve ark., 2010; Cao, 2013; Belazi ve ark., 2016).

Tez çalışmasında yer değiştirme ve yerine koyma işlemleri birlikte gerçekleştirilerek bir görüntü şifreleme algoritması önerilmiştir. Bu işlemler için sırasıyla Ikeda ve Henon kaotik haritaları kullanılmıştır. Her iki harita da sahip oldukları kuvvetli kaotik özellikler sebebiyle tercih edilmiştir. Önerilen şifreleme algoritmasında haritalar kullanılarak bir anahtar belirlenmiş ve şifreleme – şifre çözme işlemleri bu anahtar aracılığıyla gerçekleştirilmiştir. Algoritma, gri ve renkli resimlere uygulanarak literatürde bilinen güvenlik analizlerine tabi tutulmuştur. Sonuç olarak görüntüler için güvenilir ve hızlı bir şifreleme algoritması geliştirilmiştir.

2. KAYNAK BİLDİRİŞLERİ

Kaos bilimi ve kriptografi arasındaki benzerliklerin fark edilmesi ve kaosun kriptografide kullanılmaya başlanması, 1991 senesine kadar uzanmaktadır (Habutsu ve ark., 1991). EuroCrypt konferansında kaotik Tent haritası kullanılarak kaotik bir şifreleme metodu önerilmiştir. Fakat aynı konferansta bu metodun kırılması üzerine kaotik şifreleme üzerinde çok durulmamıştır. Bu çalışmanın kriptanalizi, Biham tarafından yapılmıştır (Biham, 1991).

Takip eden senelerde çeşitli kaotik haritaların geliştirilmesi ve bunların farklı boyutlarda kullanımı sağlanarak daha farklı şifreleme yöntemleri geliştirilmiştir. Bu yöntemler arasında sadece yer değiştirme ya da sadece yerine koyma işlemlerinin gerçekleştirildiği algoritmaların yanında, her ikisinin piksel ya da bit bazında gerçekleştirildiği algoritmalar da mevcuttur.

İki boyutlu kaotik haritalar kullanılarak şifrelemenin gerçekleştirilebileceği fikri ilk olarak Pichler ve Scharinger tarafından ortaya atılmıştır (Pichler ve Scharinger, 1994). Jiri Fridrich ise bu çalışma üzerinden giderek iki boyutlu Baker kaotik haritasını üç boyuta çıkarmış ve bir görüntü şifreleme algoritması oluşturmuştur. Algoritmada yer değiştirme için üç boyutlu Baker haritasını kullanan Fridrich, yerine koyma işlemleri için ise lineer olmayan geri beslemeli kaydedici kullanmıştır. Algoritmanın avantajları arasında değişebilir anahtar ve blok boyutu, şifreleme ve şifre çözme zamanlarının aynı olması ve algoritmanın hızlı olması sayılabilir. Dezavantajı ise, anahtar büyüklüğünün blok büyüklüğüne bağlı olması söylenebilir (Fridrich, 1998).

Kocarev ve Jakimoski (2001) üstel ve lojistik haritalarla Feistel yapısını birlikte kullanarak bir şifreleme algoritması geliştirmiştir. Bu çalışmada açık metin 64 bitlik bloklara ayrılmış ve her blok 8 bitlik anahtar grupları tarafından işleme tabi tutulmuştur. Feistel yapıların en önemli parçası olan S – box (yerine koyma tablosu) fonksiyonları kaotik haritalardan elde edilmiştir. Çalışmanın ikinci bölümünde lineer ve diferansiyel kriptanaliz yapılmış ve yeterli güvenlik seviyelerine ulaşıldığı gözlenmiştir.

Bir diğer çalışma ise Chen ve ark., tarafından yapılmıştır (Chen ve ark., 2004). Geliştirilen algoritmada, iki boyutlu Cat haritası üç boyuta genişletilmiş ve piksellerin yerlerinin değiştirilmesi için kullanılmıştır. Yer değiştirmeden sonra ise, mod (modulo) ve xor (özel-veya) işlemleri aracılığıyla yayma işlemi gerçekleştirilmiştir. Anahtar hassasiyeti ve bazı istatiksel testlerin uygulandığı algoritmanın güvenilir sonuçlar vermesinin yanında, şifreleme ve şifre çözme sürelerinin nispeten uzun olduğu söylenebilir.

Lian ve ark. (2005) , Cat ve Baker haritalarına göre daha fazla parametre sayısına sahip olduğu için Standart harita kullanarak bir şifreleme algoritması geliştirmiştir. Bu algoritmada karıştırma (confusion) ve yayılma (diffusion) işlemleri kaotik haritalar aracılığıyla gerçekleştirilmiştir. Karıştırma işleminde Standart harita kullanılırken; yayılma işleminde ise Lojistik haritanın dâhil olduğu bir fonksiyon kullanılmıştır. Her bir işlemde kullanılan alt anahtar grupları ise Skew Tent harita kullanılarak üretilmiştir. Geliştirilen algoritmada, Cat ve Baker kaotik haritalarının şifreleme işlemlerinde bir eksiklik olarak görülen (0,0) pozisyonundaki pikselin değerinin değişmemesi sorunu da çözülmüştür. Anahtar uzayı, anahtar hassasiyeti, istatiksel saldırılar açısından değerlendirilen algoritma tatmin edici sonuçlar vermiştir. Hesaplama ve karmaşıklık açısından geleneksel şifreleme yöntemlerinden biri olan DES ile karşılaştırılan algoritma, daha iyi performans sergilemiştir.

Kriptoloji çevrelerince çeşitli yönlerden eksik görülen ve bu yüzden profesyonel bir şekilde kullanılmayan kaotik sistemlerin, kriptolojide daha etkin bir şekilde kullanımını sağlaması ve beklentileri karşılaması açısından Alvarez ve Li bir derleme yapmıştır (Alverez ve Li, 2006). Sadece yol gösterici olması amacıyla yapılan bu çalışmada değinilen temel konular arasında; kaotik sistemlerin özelliklerini koruduğu aralığın kullanılması, ayrık hale getirilip kullanılacak kaotik sistemlerde ayrıklaştırılma işleminden sonra oluşabilecek negatif etkilerin iyi bir şekilde değerlendirilmesi gibi konuların yanında, anahtar seçimi ve tanımıyla ilgili uyulması beklenen sıkı kurallara da değinilmiştir. Bu bağlamda önerilen kurallar arasında, anahtarın tamamının ve üretilme sürecinin eksiksiz bir şekilde tanımlanması, anahtarın bir bölümünün açık metin ya da anahtarın bilinmeyen kısmı için ipucu vermemesi ve anahtar uzayının güvenlik açısından 2^{100} ' den büyük olması gibi hususlar yer almaktadır. Ayrıca şifrelemenin istatiksel açıdan incelenmesi

gerektiğine de değinilmiştir. Bu konuda tavsiye edilen kurallardan biri, farklı anahtarlarla şifrelenen mesajın tüm anahtarlar için istatiksel olarak aynı olması gerektiğidir. Sistemin çeşitli istatiksel saldırılarla denenmesi de önerilmektedir. Kriptosistemin uygulama ayağında ise makul ölçülerde maliyet ve hızda sistemin kolay uygulanabilir olması gerektiği vurgulanmıştır.

Gerçekleştirilen bir diğer kaotik şifreleme algoritması ise Pareek ve ark. (2006)'nın yılında Lojistik harita kullanarak ortaya koydukları algoritmadır. Bu çalışmada iki tane Lojistik harita ve 80 bitlik bir anahtar kullanılmış, güvenlik seviyesini artırmak için anahtar değeri her 16 piksellik blok şifrelenmesi sonrasında değiştirilmiştir. Kullanılan iki haritanın başlangıç değerleri ise anahtarlar kullanılarak hesaplanmıştır. Şifreleme işlemi, ikinci haritanın aldığı değerlerin belli aralıklara bölünmesi sonucu, o aralığa karşı gelen işlemle gerçekleştirilmiştir. Behnia ve ark.'nın yaptığı çalışmada ise şifreleme için Jacobian eliptik haritaları kullanılmıştır (Behnia ve ark., 2013). Her iki çalışmada da önerilen algoritmalar çeşitli istatistik testlere tabi tutulmuş ve güvenilir sonuçlar elde edildiği belirtilmiştir.

Kaotik görüntü şifrelemede güvenliği artırmak ve algoritmayı çeşitli açılardan iyileştirmek için çeşitli haritaların birlikte kullanıldığı çalışmalar da yapılmaya başlanmıştır. Bunlardan biri de Wei-bin ve Xin'in Henon ve Arnold kaotik haritaları birlikte kullandığı şifreleme çalışmasıdır (Wei-bin ve Xin, 2009). Bu çalışmada yer değiştirme işlemi Arnold kaotik haritasıyla; yayılma işlemi ise Henon kaotik haritasıyla gerçekleştirilmiştir. Güvenlik değerlendirmesinde ise, histogram analizine, anahtar uzayına ve anahtar hassasiyetine yer verilmiştir. Anahtar hassasiyetinde tatmin edici sonuç veren algoritma için, anahtar uzayı tam olarak belirtilmemiş olup, şifreli görüntünün histogramı ise tam olarak olması beklenen şekilde eşit dağılımlı sonuç vermemiştir.

Farklı iki kaotik harita kullanılarak yapılan bir diğer çalışma ise Patidar ve ark. (2010)'nın Standart ve Lojistik haritaları kullanarak yaptığı çalışmadır. Bu çalışmada, iki kere yer değiştirme ve iki kere yayılma işlemi gerçekleştirilmiştir. Yer değiştirme işleminin ilki, başlangıç koşullarından ve iki tamsayıdan oluşan gizli anahtardan türetilen ikincil bir anahtar kullanılarak gerçekleştirilmiştir. İkinci yer değiştirme işleminde ise kaotik haritalar kullanılarak oluşturulan dizilim kullanılmıştır. Yayılma işlemi, yatay ve dikey olarak her iki yönde gerçekleştirilmiştir. Güvenlik değerlendirmesinde histogram analizi, anahtar

hassasiyeti, korelasyon katsayıları ve korelasyon dağılımı, anahtar uzayı ve hız performansı gibi konular ele alınmıştır. Sonuçlar algoritmanın etkili bir şifreleme gerçekleştirdiğini ortaya koymaktadır.

Awad ve Saadane, 2010 yılında piksellerin direkt fiziksel konumlarını ve değerlerini değiştirmek yerine bit seviyesinde değişiklik yaparak şifreleme gerçekleştirmeyi amaçlamıştır (Awad ve Saadane, 2010). Bu yöntemle yapılan ilk çalışmalar Grp&Cross permütasyonu olarak bilinir. Shi ve Lee bu çalışmada rastgele n – biti değiştirerek şifrelemeyi herhangi bir programlanabilen mikroişlemcide gerçekleştirmiştir (Shi ve Lee, 2000). Bu çalışmanın devamı olarak bit seviyesinde şifreleme için farklı yöntemler ve farklı mikroişlemcilerde yapılan çalışmalar karşılaştırılmıştır (Lee ve ark., 2001; Hilewitz ve ark., 2004). Socek tarafından önerilen çalışmada ise piksellerin konumları, bit değerleri Parçalı Lineer Kaotik Harita kullanılarak yeniden konumlandırılmıştır (Socek ve ark., 2005). Awad ve Saadane (2010)'nin çalışmasında Grp, Cross ve Socek algoritmaları Parçalı Lineer Kaotik Harita ve değiştirilmiş Parçalı Lineer Kaotik Harita kullanarak gerçekleştirilmiş ve karşılaştırmalı bir çalışma elde edilmiştir. Çalışmanın deneysel sonuçları, korelasyon ve entropi değerlerinin önerilen Parçalı Lineer Kaotik Harita kullanıldığında daha iyi sonuçlar verdiğini ve güvenilir bir şifreleme metodu olarak kullanılabileceğini göstermiştir.

Abir Awad ve Dounia Awad, geliştirdikleri algoritma ile şifrelenmiş bir görüntüyü haberleşme kanalı üzerinden bozulmamış bir şekilde gönderebilmek ve deşifrelenmiş görüntüyü tekrar elde edebilmeyi amaçlamıştır (Awad ve Awad, 2010). Önerilen yöntem ile içinde Socek (Socek ve ark., 2005), Xiang (Xiang ve ark., 2006),Yang (Yang ve ark., 2009), Lian (Lian ve ark., 2005) ve Wong (Wong ve Kwok, 2010)' un çalışmalarının olduğu algoritmalardaki eksiklikler de giderilmiştir. Awad ve Awad (2010) tarafından geliştirilen yöntemde, yer değiştirme ve yayılma işlemleri için iki tane değiştirilmiş Parçalı Lineer Kaotik Harita kullanılmıştır. Yer değiştirme için Xiang ve Socek metotları kullanılmıştır. Şifrelenen ve şifre çözme sonucu elde edilen görüntülerin histogram analizi yapılmış, anahtar hassasiyeti incelenmiştir. Bazı istatiksel testlerin de uygulandığı algoritma güvenilir sonuçlar vermiştir. Ayrıca, iletilme sırasında meydana gelebilecek hatalar incelenirken, bozularak iletilen piksellerdeki hataların başka piksellere yansımadan kaldığı görülmüştür. Ayrıca, NIST (Ulusal Standartlar ve Teknoloji Enstitüsü)

standartlarına göre de değerlendirilen algoritma Socek algoritmasıyla karşılaştırılmış ve daha iyi sonuçlar elde edilmiştir.

El Latif ve ark. (2013), şifreleme için renkli resimlerin renk uzaylarında değişiklik yaparak ve kuantum kaotik haritasını kullanarak şifreleme işlemini gerçekleştirmiştir. Renkli görüntünün parlaklık elemanına Wavelet transformu uygulandıktan sonra, kuantum kaotik haritası yardımıyla resme yatay ve dikey yönlerde yayma işlemi uygulanmıştır. Histogram analizi, anahtar hassasiyeti, korelasyon dağılımı, entropi analizi gibi yapılan güvenlik testlerinin hepsinden beklentilere uygun sonuçlar vermiştir.

Yang ve ark. (2010) ise kaotik şifrelemenin yanında kimlik doğrulama işlemini de gerçekleştirmişlerdir. Şifreleme ve şifre çözme işlemleri için kullanılacak anahtar kaotik harita ve açık resim bilgisinin özeti kullanılarak oluşturulmuştur. Yer değiştirme ve yayma işlemleri için iki farklı kaotik haritanın kullanıldığı çalışmada kimlik doğrulama işlemleri için de kaotik haritaların başlangıç değerleriyle oluşturulan özet anahtarlar kullanılmıştır. Çalışma, çeşitli testler uygulanarak güvenlik analizinden geçirilmiş ve algoritmanın sadece bir tur uygulanması sonucu etkili ve güvenli bir görüntü şifreleme yöntemi oluşturulduğu üzerinde durulmuştur. Buna ek olarak şifreleme ve şifre çözme hızlarının iyileştirilebileceğine değinilmiştir.

François ve ark. (2012) ise yaptıkları çalışmada kaotik bir fonksiyon oluşturularak şifreleme işlemi gerçekleştirilmiştir. Çalışmada özellikle anahtar uzayını genişletmeye büyük önem verilmiştir. Gri ve renkli resim için sonuçları verilen çalışmada en önemli istatiksel testler uygulanarak algoritmanın güvenilirliği test edilmiştir. Bazı çalışmalarda ise şifreleme için birden fazla kaotik harita kullanılarak yeni bir harita oluşturulmuş ve şifreleme algoritması bu harita kullanılarak gerçekleştirilmiştir. Bu çalışmalara örnek olarak; Norouzi ve Mirzakuchaki (2014), Zhou ve ark. (2014), Cao (2013), Tong (2013), Sathiskumar ve ark. (2011) ‘nın yaptığı çalışmalar örnek verilebilir. Her bir çalışmaya histogram, entropi ve anahtar hassasiyeti analizinin yanında, korelasyon analizi gibi istatiksel testler uygulanmış ve güvenilir sonuçlar elde edilmiştir.

Yeni şifreleme metotlarının geliştirilmesinin yanında, var olan yöntemlerin iyileştirilmesi de önemli bir konudur. Liu ve Li (2013), çalışmalarında AES algoritması için anahtar üretimini kaotik haritalar kullanarak gerçekleştirmiş ve böylece renkli resim

şifrelenmesinde AES algoritmasını daha güvenli bir metot haline getirmişlerdir. Bir diğer çalışmada ise yer değiştirme ve yayma işlemleri için sadece kaotik haritalar kullanılmamış; şifrelenecek resimden elde edilen parametrik değerler de kullanılmıştır (Murillo - Escobar ve ark., 2015). Sadece renkli resim için sonuçların verildiği çalışma, DNA kodlama ve Logistic kaotik harita ile şifrelemenin gerçekleştirildiği Liu ve ark. (2012)'nın çalışması ile karşılaştırılmış ve Liu (2014)'nun ortaya koyduğu çeşitli performans analizlerinin ve istatiksel testlerin yer aldığı analiz ile kıyaslanmıştır. Bunun sonucunda geliştirilen yöntemin daha güvenli ve gerçek zamanlı uygulamalar için daha uygun olduğu belirtilmiştir.

Tong ve ark. (2015)'nın gerçekleştirdiği çalışmada ise rasgele sayı üreteci ile anahtar üretimi için dört boyutlu sürekli kaotik sistem kullanılmış; yer değiştirme ve yayma işlemleri için de Cat kaotik haritası kullanılmıştır.

Başka bir çalışma ise, iki boyutlu Cat haritasının yeniden düzenlenerek, yayma ve yer değiştirme işlemlerinin bitler üzerinde gerçekleştirildiği çalışmadır (El Assad ve Farajallah, 2016). Ayrıca şifrelemede kullanılacak rasgele sayı üreteci için de El Assad ve Noura (2011) tarafından geliştirilen kaotik sayı üreteci kullanılmıştır. Önerilen algoritmanın tüm istatiksel testleri geçtiği ve bilinen tüm saldırılara karşı dayanıklı olduğu, ayrıca çalışmanın donanımsal uygulamalar için de uygun olduğu vurgulanmıştır.

Xu ve ark. (2016), bit bazında gerçekleştirilen bir çalışma ortaya koymuştur. Bu çalışmada şifrelenecek resmin bitlerle ifade edilmesi için Zhou ve ark. (2014) tarafından geliştirilen yöntemlerden biri kullanılmıştır. Resim ikili bit düzleminde ayrıştırıldıktan sonra, resme belirlenen aşamalara göre sırasıyla yer değiştirme ve yayma işlemleri uygulamıştır. Bu işlemlerde ise kaotik haritalar kullanılmıştır. Birçok benzetim ve performans analizinin yer verildiği çalışmada tek bir round sonucunda güvenilir ve etkili bir şifreleme yöntemi elde edildiği özellikle belirtilmiştir.

Wang ve ark. tarafından yapılan çalışmada görüntü şifrelemede temel olarak kullanılan yer değiştirme ve yayma işlemlerinin ayrı ayrı ve birlikte kullanımı ele alınarak bir performans değerlendirmesi yapılmıştır (Wang ve ark., 2016). Elde edilen sonuçlara göre ilk önce yer değiştirme ve ardından yayma işleminin gerçekleştirildiği uygulama en verimli sonuçların alındığı uygulama olmuştur.

Stoyanov ve Kordov (2014) tarafından yapılan çalışmada ise yer değiştirme işlemleri için Chebyshev polinomu; yayma işlemleri için de Duffing haritası kullanılmıştır. Benzer bir çalışma da Hanchinamani ve Kulakarni (2014) tarafından yapılmıştır. Bu çalışmada yer değiştirme işlemleri için iki boyutlu Zaslavskii kaotik haritası kullanılmış; yayma işlemleri için de Hadmard dönüşümü kullanılmıştır. Hussain ve ark. (2013)'nın önerdiği şifreleme algoritması ise yer değiştirme işlemlerinin Skew Tent haritasına göre; yayma işlemlerinin ise benzeşim dönüşümüne göre gerçekleştirildiği bir çalışmadır.

Var olan haritaların kuantum formlarının geliştirilmesiyle şifrelemede kuantum haritalar da kullanılmaya başlanmıştır. Akhshani ve ark. (2012)'nın önerdiği algoritmada şifrelemede Kuantum Logistic harita kullanılmış ve en az klasik kaotik haritaların kullanımının sunduğu kadar güvenilir bir şifreleme metodu elde edilmiştir.

Zhou ve ark. (2013)'nın yaptığı çalışmada bir boyutlu kaotik haritaların güvenlik yönünden eksikliklerini giderebilmek için bir boyutlu Logistic, Tent ve Sinüs kaotik haritalarının birlikte kullanıldığı anahtarlamalı bir algoritma önerilmiştir. Bu algoritmada kullanılacak harita anahtarlamanın sonucuna göre belirlenmiş ve belirlenen dönüşüm işlemi gerçekleştirilmiştir.

Bu zamana kadar bahsedilen bazı çalışmalarda da görüldüğü gibi kaotik haritalarda kimi değişiklikler ve iyileştirmeler yapılması ya da birden fazla kaotik haritanın kullanılarak yeni bir harita oluşturulması şifrelemede daha etkili sonuçlar alınmasını sağlayabilmektedir. Bu amaçla yapılan bir çalışmada bir boyutlu Logistic ve Sinüs kaotik haritaları kullanılarak iki boyutlu yeni bir harita oluşturulmuştur. Çalışmada bu haritanın ayrı ayrı Sinüs ve Logistic haritalardan daha iyi kaotik özelliklere sahip olduğu gösterilmiştir. Geliştirilen harita ile bir kaotik matris oluşturulmuştur. Kaotik matris ise belirli aşamalardan oluşan kaotik dönüşüm ile yer değiştirme ve yayılma işlemlerinde kullanılmıştır. Önerilen dönüşüm ile satır ve sütunda yapılacak yer değiştirme işlemleri teker teker değil aynı anda gerçekleştirilmiştir. Çalışmada yüksek güvenlik seviyesi ve hız vurgulanmıştır (Hua ve ark., 2015).

Belazi ve ark. (2016) ise yer değiştirme ve yayma işlemlerini ikişer defa gerçekleştirmiştir. Yayma işlemlerinin birinde Hussain ve ark. (2013)' nın önerdiği S-box yapısı kullanılmıştır. Yer değiştirme işlemlerinde ise önerilen yeni bir kaotik harita ile

Logistic harita kullanılmıştır. Kullanılan haritanın kaotiklik özelliklerini artırmak ve dolayısıyla daha güvenilir şifreleme algoritmaları oluşturabilmek için Liu ve ark. (2015), Li ve ark. (2006)'nın geliştirdiği kaotik haritadaki temel fonksiyonu değiştirerek daha geniş anahtar uzayına sahip olmayı ve durum uzayının yapısını saklamayı amaçlamıştır. Şifrelemede kullanılacak anahtar bu haritadan elde edilmiştir. Üretilen anahtarlar yer değiştirme ve yayma işlemlerine dâhil edilmiştir ve tüm istatiksel testler geçilmiştir.

Zhang ve Zhang (2014) tarafından yapılan çalışmada resim bloklara ayrılıp sadece yer değiştirme işlemi yapıldığı için algoritma istatiksel saldırılara açıktır. Bunun için önerilen yeni çalışmada Logistic haritada değişiklik yapılarak iki farklı dizilim üretilmiş ve bu dizilimler bit ve piksel kaydırma ile piksel değerlerini rasgele yaymak için kullanılmıştır. Çalışmanın hızlı ve güvenli olmasından dolayı gerçek zamanlı uygulamalarda kullanılabileceği belirtilmiştir (Ponnain ve Chandranbabu, 2016).

Hem piksel, hem bit bazında değişiklik yaparak şifreleme gerçekleştiren bir çalışma da Khanzadi ve ark. (2014) tarafından yapılmıştır. Bu çalışmada piksellerin konumu kaotik haritaların dizilimleri kullanılarak değiştirildikten sonra görüntünün bit düzlemi sekiz bölüme ayrılarak yer değiştirme ve yayılma işlemleri her bölüme ayrı ayrı uygulanmıştır. Bu işlemlerde ise rasgele sayı üretecinden elde edilen dizilim ve matrisler kullanılmıştır. Ve sadece gri renk seviyesindeki görüntüler şifrelenmiştir.

3. MATERYAL ve YÖNTEM

3.1. Materyal

Tez çalışması kapsamında geliştirilen programların denenmesi ve sonuçlar için, Intel Core i7- Q740 işlemciye sahip Windows 10 işletim sistemi kurulu olan 64 bitlik ve 16 GB RAM hafızalı dizüstü bilgisayarda Matlab 2013 ortamı kullanılmıştır.

3.2. Kriptolojiye Giriş

Günümüzde olduğu gibi tarih boyunca da bilgi her zaman gücün kaynağı olmuş ve bu yüzden de kıymetini korumuştur. Şifreleme bilimi olarak da bilinen kriptoloji tam da bu noktada, bilgiyi koruma amacıyla ortaya çıkmıştır. Fakat geçmişte olduğu gibi artık amaç sadece bilgiyi düşmandan gizlemek değil; baş döndürücü bir hızla gelişen ve değişen teknoloji ile birlikte sahip olduğumuz bilgiyi de koruyabilmektir.

Modern kriptoloji, bilginin bir anahtarla şifrelenmesi ve bu şifreyi sadece anahtara sahip olan kişinin çözebilmesi ilkesine dayanır.

3.3. Kriptolojinin Tarihsel Gelişimi

3.3.1. Kaydırmalı şifreleme sistemi

Kriptografi Yunanca'da crypto(gizli) ve graph(yazım) kelimelerinden türemiştir. Kriptografinin bilgiyi gizlemek amaçlı kullanılması milattan önce 1900lü yıllara kadar dayanmaktadır. Kriptografinin ilk örnekleri kaydırmalı şifreleme (shift cipher) mantığına göre yapılmıştır. Bu yöntemlerden en bilineni Milattan önce geliştirilen Sezar şifrelemedir. En basit şifreleme yöntemi olan Sezar şifreleme, metindeki her harfin kendisinden üç harf ötelenerek yeniden yazılmasıyla oluşturulmuştur. Örneğin; şifrelenmek istenen kelime 'kriptoloji' olsun. Öncelikle, her bir harfin alfabede kaçıncı sırada olduğu belirlenir.

K R İ P T O L O J İ

14 – 21 – 12 – 20 – 24 – 18 – 15 – 18 – 13 – 12

Sezar şifreleme yönteminde her harfin yerine kendisinden üç harf sonraki harf gelir. Buna göre yukarıdaki örnekte her harf üç harf kadar ötelenirse, şifrelenmiş kelimenin yeni hali aşağıdaki gibi olacaktır.

KRİPTOLOJİ → NTLŞVRORML

Matematiksel olarak ifade edilecek olursa;

$C = E_{k_1}(m) \quad , \; m = D_{k_2}(C)$ (1)

Eş. 1' de C(cipher text) şifrelenmiş mesaj, E(encryption) şifreleme fonksiyonu, m(message) şifrelenecek mesaj, k(key) anahtar ve D(decryption) olmak üzere ifadeler sırasıyla şifreleme ve şifre çözme işlemlerini ifade etmektedir.

P = $\sum = \{A, B, C \ldots Z\}$, $\forall \, x, y \, \epsilon \, P$ olmak üzere;

Sezar şifrelemede, x şifrelenecek harfin alfabedeki sayısal karşılığı ise şifreleme ve şifre çözme işlemleri aşağıdaki gibi ifade edilebilir.

$E_k(x) = x + k(mod29) \qquad D_k(y) = y - k(mod29)$ (2)

Fakat kaydırmalı şifreleme tek alfabeli bir şifrelemedir ve bu mantığa göre her harfin yerine sadece bir harf gelebilir. Anahtar olarak 29 elemanlı alfabe kullanıldığı için anahtar büyüklüğünün de 29 olduğu söylenebilir. Harflerin kullanım frekansı ve diğer istatiksel yöntemler kullanılarak bu sistem kolaylıkla kırılabilir.

3.3.2. Yer değiştirme şifreleme sistemi

Kaydırmalı şifreleme sisteminde anahtar olarak tek bir alfabenin kullanılması yeterli güvenlik sağlamadığı için çoklu alfabe kullanımına dayalı yöntemler geliştirilmiştir. Bunlardan biri Viegenere şifreleme sistemidir. Viegenere şifreleme yönteminde, açık metin olarak adlandırılan bilgi, anahtar olarak belirlenen bir kelime ile şifrelenir. Açık metin anahtarın uzunluğu kadar bloklara ayrılır ve açık metindeki her bir harf bu şekilde anahtarla şifrelenir. Aşağıdaki bir diğer örnekte 'kriptoloji' kelimesi anahtar olarak seçilen 'şifre' kelimesiyle şifrelenmiştir.

KRİPTOLOJİ → 14 21 12 20 24 18 15 18 13 12

ŞİFRE → 23 12 7 21 6

Öncelikle açık metin anahtar uzunluğu 5 olduğu için 5'li bloklara ayrılır. Yukarıdaki örnekte açık metin böylece 2 bloktan oluşmuş oldu.

14 21 12 20 24 | 18 15 18 13 12 (Açık metin)

23 12 7 21 6 | 23 12 7 21 6 (Anahtar)

8 4 19 12 1 | 12 27 25 5 18 (Şifrelenmiş metin)

Şifrelenmiş yazıdaki sayıların harf karşılıkları yazılırsa, GÇÖİAİVUDO gizli metni elde edilir. Şifreleme işlemi burada da 29 harfli alfabe temel alınarak gerçekleştirilmiştir.

Viegenere şifreleme sisteminde ise anahtarın uzunluğu bilindiği takdirde, şifrenin çözülmesi kaydırmalı şifreleme sistemleri kadar kolay olabilmektedir.

3.3.3. Permütasyon şifreleme sistemi

Temel anlamıyla permütasyon, elemanları yeniden sıralama işlemidir. Permütasyon şifreleme sisteminde, şifrelenecek mesaj belirli uzunlukta bloklara ayrılarak gerçekleştirilen permütasyon işlemine göre yeniden yazılarak şifrelenir.

Örneğin; şifrelenecek ifade 'görüntü şifreleme' ve seçilen blok uzunluğu ise n= 4 olsun.

Permütasyon işlemi $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ şeklinde belirlenip, mesaj n uzunluğunda bloklara ayrılırsa;

GÖRÜ NTÜŞ İFRE LEME

ÖÜRG TŞÜN FERİ EEML ifadesi elde edilir. n değerini saklı tutmak için aradaki boşluklar kaldırılır. Böylece şifreli mesaj ÖÜRGTŞÜNFERİEEML halini alır.

3.4. Anahtar Türlerine Göre Şifreleme Sistemleri

3.4.1. Asimetrik şifreleme (Açık anahtarlı şifreleme)

Eş. 1' de verilen ifadede şifreleme ve şifre çözme işlemlerinin aynı k anahtarı kullanılarak gerçekleştirildiği görülür. Asimetrik şifreleme sistemlerinde şifreleme ve deşifreleme için kullanılan anahtarlar farklıdır. Şifreleme için kullanılacak anahtar herkes

tarafından bilinirken (public key), şifre çözme için kullanılacak anahtar gizli tutulur(private key).

Asimetrik şifrelemede kullanılacak fonksiyonun sadece ek bir bilgi kullanarak çözülebilen tek yönlü bir fonksiyon olması gerekir.

Tek yönlü bir fonksiyon şöyle tanımlanır (Smart, 2003).

$f: X \to Y$ olmak üzere;

1. $\forall x \in X$ için $f(x)$ fonksiyonunu hesaplamak kolay olmalı,
2. $y = f(x)$ ifadesinde y verildiğinde x'in elde edilmesi zor olmalı

Verilen tek yönlü fonksiyonda x, ancak $\phi(y)$ ek bilgisi ile elde edilebilir.

Asimetrik şifreleme sistemlerinden en bilinenler; RSA, Merkle – Hellman, El – Gamal, Rabin, Pallier algoritmalarıdır.

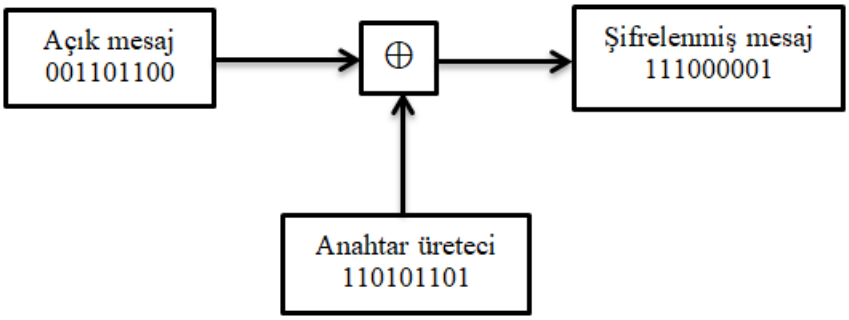
3.4.2. Simetrik şifreleme (Kapalı anahtarlı şifreleme)

Simetrik şifrelemede, açık anahtarlı sistemlerin aksine şifreleme ve şifre çözme aşamalarında aynı k anahtarı kullanılır. Farklı anahtarların kullanıldığı simetrik şifreleme sistemleri olsa da anahtarların birbirlerinden elde edilmesi mümkündür. Fakat açık anahtarlı sistemlerde böyle bir şey mümkün değildir.

Simetrik şifreleme işlemlerin mesajın bitler üzerinden ya da bloklara ayrılması şeklinde yapılması açısından ikiye ayrılır: Akım şifreleme ve blok şifreleme sistemleri.

3.4.2.1. Akım şifreleme sistemleri

Akım şifreleme Şekil 3.1'deki diyagramda olduğu gibi ifade edilebilir. Modern akım şifreleme algoritmalarına örnek olarak RC4, Lineer Geri Beslemeli Kaydırmalı Kaydediciler (Linear Feedback Shift Registers) örnek verilebilir.



Şekil 3.1. Akım şifreleme sisteminin gerçekleştirilmesi.

Yukarıdaki diyagramda

m_1, m_2 ... açık mesaj bitleri;

k_1, k_2 ... anahtar bitleri;

c_1, c_2 ... şifrelenmiş mesaj bitleri olmak üzere;

$$c_i = m_i \oplus k_i \qquad m_i = c_i \oplus k_i \tag{3}$$

Eş. 3 sırasıyla şifreleme ve şifre çözme fonksiyonlarını ifade eder.

Akım şifreleme ve blok şifreleme arasındaki temel fark, akım şifreleme sisteminin hafızalı olmasıdır. Böylece bit akışında şifrelenecek sıra belirlenir.

3.4.2.2. Blok şifreleme sistemleri

Blok şifreleme sistemlerinde mesaj bloklara ayrılarak şifreleme yapılır. En bilinen blok şifreleme sistemleri arasında DES, AES, RC5, RC6 sayılabilir. Bunların içinde 1970lerde geliştirilen DES (Data Encryption Standard) 56 bitlik anahtar uzunluğuna sahip olduğu için bütün uygulamalarda yeterli güvenlik sağlayamıyordu. DES algoritması aslında Feistel algoritması üzerinde yapılan bir değişiklikle geliştirilmiştir.

Feistel algoritması kullanarak yapılacak şifreleme işlemi Eş. 4'teki denklemlerle ifade edilebilir. Şifrelenecek yapının iki eşit bloğa ayrılması sonucu L_0 ve R_0 elde edilir.

$L_i = R_{i-1}$

$$R_i = L_{i-1} \oplus F(K_i, R_{i-1}) \quad (4)$$

Deşifreleme işlemi ise Eş. 5'te yazılan denklemlerle gerçekleştirilir.

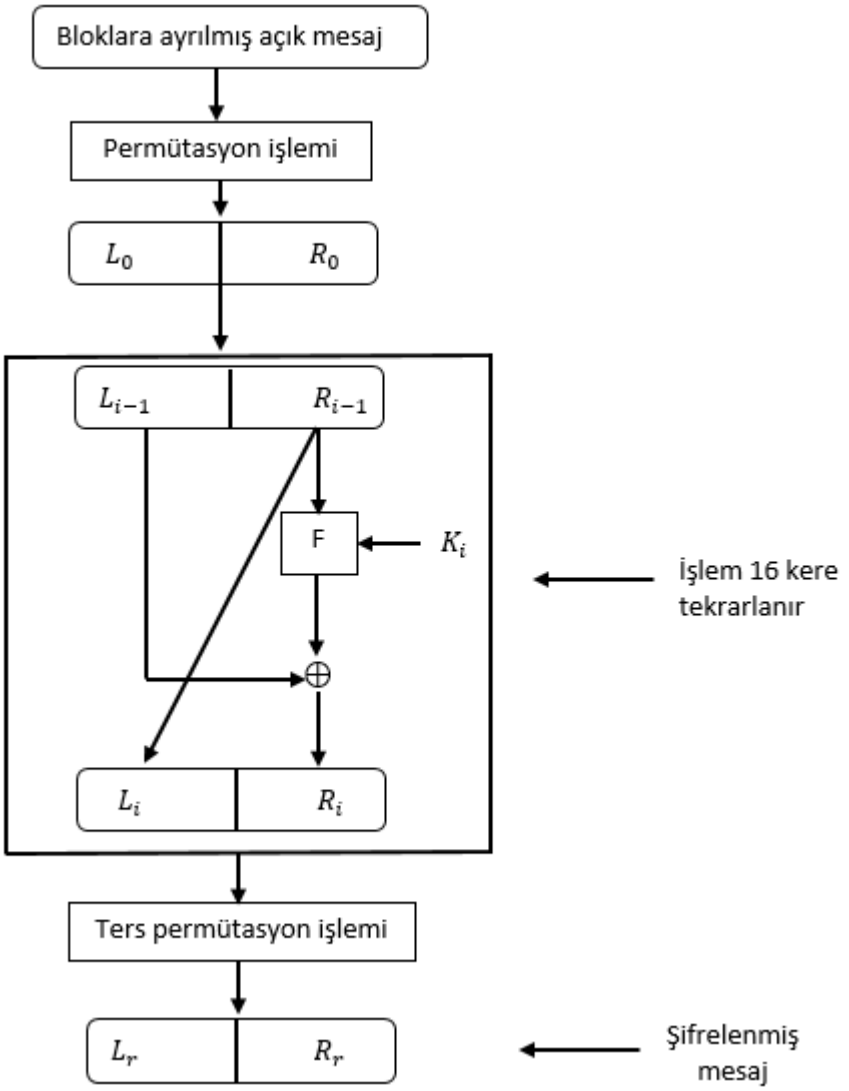
$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus F(K_i, L_i) \quad (5)$$

DES algoritması elde edilirken Feistel algoritmasında yapılan değişiklikler şöyle sıralanabilir:

- Round sayısı $r = 16$ olarak alınmıştır.
- Blok büyüklükleri 64 bittir.
- Anahtar uzunluğu 56 bittir.
- Her bir aşamada kullanılan K_i anahtarının uzunluğu 48 bittir.

Şekil 3.2'de şemada DES algoritmasının işleyiş şeması verilmiştir (Smart, 2003).



Şekil 3.2. DES algoritmasının işleyişi.

Yukarıdaki akış diyagramında en başta gerçekleştirilen permütasyon işlemi Şekil 3.3'teki tabloya göre gerçekleştirilir.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Şekil 3.3. İlk permütasyon işlemini gerçekleştiren matris.

Şemadaki F fonksiyonu içerisinde gerçekleşen işlemler ise şöyle sıralanabilir:

i. Genişletme Permütasyonu: Bu işlemde mesajın sağ yarısı 32 bitten 48 bite çıkarılır ve Şekil 3.4'teki permütasyon tablosuna göre bitlerin yeri değiştirilir.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Şekil 3.4. Genişletme Permütasyonu işlemini gerçekleştiren matris.

ii. K_i Anahtarının Katılımı: Genişletme ve permütasyon işlemlerinden sonra elde edilen 48 bitlik çıktı, K_i anahtarı ile exor işlemine tabi tutulur.

iii. Ayırma: Xor işlemi sonrasında elde edilen 48 bitlik bilgi 6 bitlik 8 gruba ayrılır.

iv. Yerine Koyma Tablosu (S-Box): Şekil 3.5'teki tablolardan görüleceği üzere her S-Box 4 satır ve 16 sütundan oluşur. S-Box' ların girişindeki 6 bit hangi satır ve sütunun

kullanılacağını belirler. Bunlardan 1. ve 6. kullanılacak satırı belirlerken, kalan bitler sütunu belirler.

S-Box 1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-Box 2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S-Box 3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S-Box 4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S-Box 5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S-Box 6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S-Box 7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S-Box 8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Şekil 3.5. Kullanılan S-Box matrisleri.

v. Yer Değiştirme Tablosu (P-Box): Her S-Box çıkışından elde edilen bitler bir araya getirilir ve bu 32 bitlik yapıya Şekil 3.6'da verilen tabloya göre permütasyon işlemi uygulanır.

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

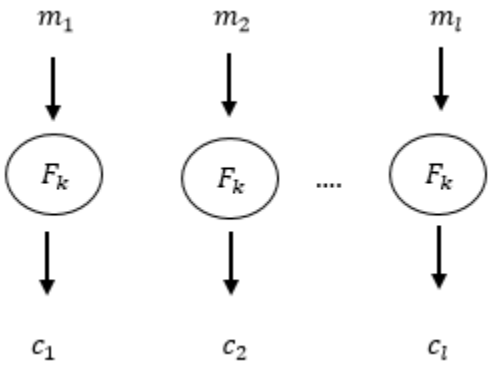
Şekil 3.6. S-Box çıkışından sonra permütasyonda kullanılan matris.

3.5. Çalışma Şekilleri

DES ya da Rijndael gibi şifreleme algoritmaları farklı yöntemlerle şifreleme işlemlerini gerçekleştirebilir. Bu yöntemlerden bazıları ECB(Electronic Code Book – Elektronik Kod Kitabı), CBC(Cipher Block Chaining – Zincirleme Şifre Blok), OFB(Output Feedback Mode – Çıkış Geribildirim Modu), CFB(Cipher Feedback Mode - Şifre Geribildirim Modu), CTR(Counter Mode – Sayaç Mod) şeklinde verilebilir (Katz ve Yindell, 2015).

3.5.1. ECB

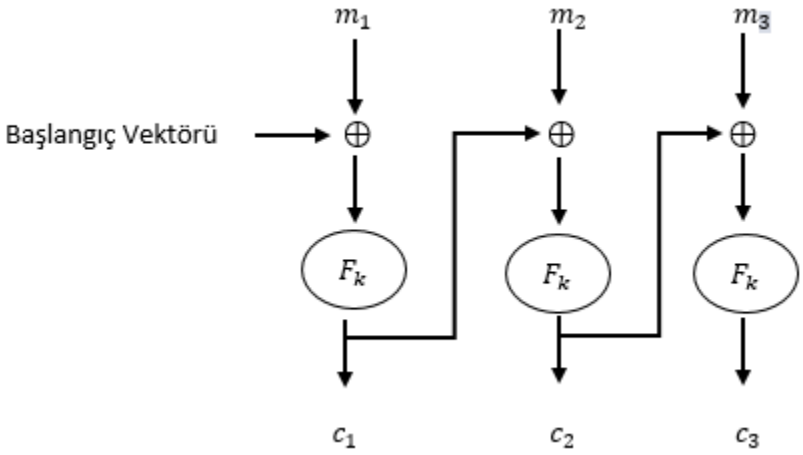
Şifrelenecek mesaj bloklara ayrılır ve her blok birbirinden bağımsız şifrelenir. Kullanımı kolay olmasına karşın, silme ve araya girme saldırılarına dayanıksız olduğu söylenebilir. Aşağıdaki diyagram ECB modunun çalışma prensibini anlatmaktadır.



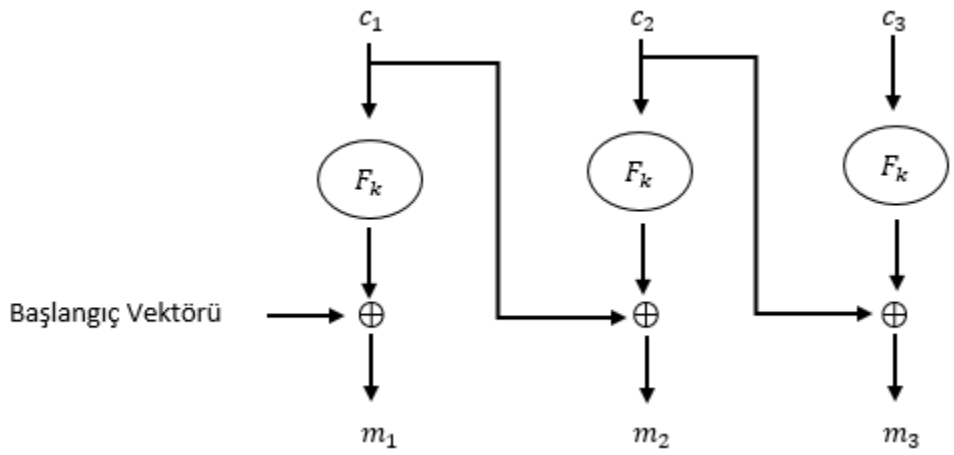
Şekil 3.7. ECB yönteminin çalışma prensibi.

3.5.2. CBC

CBC modu blok şifreleme için en iyi seçeneklerden biridir. Ayrıca silme ve araya girme saldırılarına karşı da daha iyi sonuçlar vermektedir. Şekil 3.8 ve 3.9'da sırasıyla bu yöntemin şifreleme ve deşifreleme aşamaları gösterilmiştir.



Şekil 3.8. CBC yöntemiyle şifreleme işlemi.



Şekil 3.9. CBC yöntemiyle deşifreleme işlemi.

Matematiksel olarak ifade edilecek olursa;

$c_1 = F_k(m_1 \oplus BV)$ $\quad BV$: $Başlangıç\ vektörü$

$$c_i = F_k(m_i \oplus c_{i-1}) \tag{6}$$

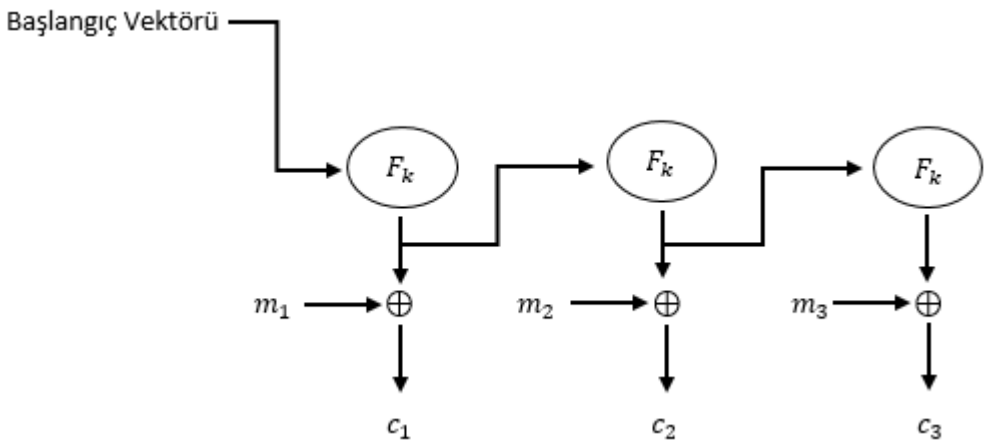
$$m_1 = F_k(c_1) \oplus BV$$

$$m_i = F_k(c_i) \oplus c_{i-1} \tag{7}$$

Eş. 6 şifreleme işlemini; Eş. 7 deşifreleme fonksiyonlarını göstermektedir.

3.5.3. OFB

OFB metodu aynı zamanda asenkron akım şifreleme metodu olarak da bilinir. Şekil 3.10 OFB yönteminin şifreleme işlemini nasıl gerçekleştirdiğini göstermektedir. Eş. 8 ve Eş. 9 sırasıyla şifreleme ve deşifreleme fonksiyonlarını ifade etmektedir.



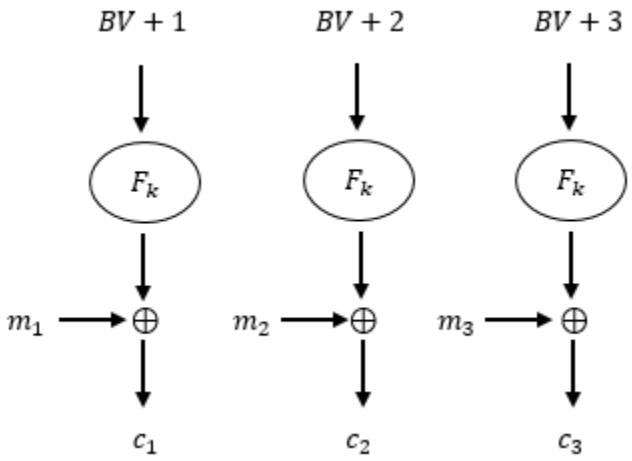
Şekil 3.10. OFB yöntemiyle şifreleme işlemi.

$y_0 = BV$ $BV: Başlangıç\ vektörü$ ve $y_i = F_k(y_{i-1})$ olmak üzere;

$$c_i = y_i \oplus m_i \tag{8}$$

3.5.4. CTR

Sahip olduğu avantajlardan dolayı günümüzde kullanılan modern yöntemlerden biridir. Önceden bahsedilen yöntemlerde birinci bloğun şifrelenmesi işlemi bitmeden ikinci bloğa geçilemezken, CTR metodu paralel işlem yapmaya imkân vererek aynı anda birden fazla bloğun şifrelenmesini mümkün kılmaktadır. Şifreleme işlemi Eş. 9'da ifade edilmektedir.



Şekil 3.11. CTR yöntemiyle şifreleme işlemi.

$$c_i = m_i \oplus F_k(BV + i) \tag{9}$$

3.6. Kriptanaliz

Geliştirilen bir algoritmanın gerekli güvenlik unsurlarını taşıyıp taşımadığını belirlemek için yapılan çalışmalar kriptanaliz başlığı altında toplanabilir. İyi bir şifreleme yöntemi, gerçekleştirilebilecek tüm saldırılara karşı koyabilecek ve mesajı açığa çıkarmayacak şekilde tasarlanmalıdır.

Bir algoritmayı kırmak amaçlı gerçekleştirilebilecek saldırılar aşağıdaki başlıklar altında toplanabilir (Alvarez ve Li, 2006):

- Gizli Metin Saldırısı(Cipher text – Only Attack): Saldırıyı yapan kişi, haberleşme kanalını dinleyerek gizli metinden elde ettiği bölümleri kullanarak şifreleme anahtarını ve açık metni elde etmeye çalışır.
- Açık Metin Saldırısı (Plaintext – Only Attack): Gizli metinin bir kısmını elde eden kişi, açık metinden de bir bölüm elde ederek şifreleme anahtarını bulmaya çalışır.

- Seçilmiş Açık Metin Saldırısı (Chosen – Plaintext Attack): Bu yöntemde saldırgan sadece açık ve gizli metine ulaşmakla kalmayıp, açık metinden istediği bölüme de erişebilir. Böylece istediği bölümleri seçerek karşılaştırma yapma imkânına sahip olur.
- Seçilmiş Gizli Metin Saldırısı (Chosen – Cipher text Attack): Saldırgan gizli metnin bir kısmını seçerek ona karşılık gelen açık metni kullanır.
- Kapsamlı Anahtar Araştırması (Exhaustive Key Search): Bu yöntemde saldırgan açık metni tamamen çözmek için şifreleme anahtarını elde etmeye çalışır. Bunun için anahtar uzayındaki olası tüm seçenekleri dener. Anahtar uzayı küçükse günümüz imkânları dâhilinde saldırı başarılı sonuç verebilir.

3.7. Görüntü Şifreleme

Her geçen gün hayatımıza daha fazla dâhil olan ve gittikçe gelişen teknoloji, bilgisayar ve internet kullanımının mümkün olduğu cihazlara erişimin kolaylaşmasını sağlayarak, sadece düz metin değil; bir o kadar da görüntü, video ve ses dosyasının da internet dünyasında yerini almasını sağladı. Böylece, kişisel bilgilerin korunması meselesi hiç olmadığı kadar önemli bir konuma geldi. Gelişen teknolojiyle birlikte, kriptografi biliminde de güvenliği olabildiğince iyi sağlamak adına çeşitli denemeler yapılmakta, farklı veri türleri için farklı metotlar uygulanmaktadır.

Bir görüntünün sahip olduğu bazı karakteristik özellikler dolayısıyla klasik şifreleme metotları güvenlik ve hız açısından yeterli olmamaktadır. AES, RC5, ya da IDEA gibi şifreleme algoritmaları metin mesajları için kayda değer güvenlik sağlarken, görüntü şifrelemede aynı verimlilik sağlanamamaktadır (Korrochano, 2005).

Bir görüntüde klasik şifreleme yöntemlerinin yetersiz kalmasına sebep olan ve farklı yöntemlerin kullanılmasını gerektiren başlıca özellikler şöyle sıralanabilir:

- Yüksek miktarda fazlalık (high redundancy) ve verinin büyüklüğü
- Birbirine yakın pikseller arasındaki yüksek korelasyon(benzerlik)

Bunlara ek olarak görüntünün şifrelemede avantaj sayılabilecek bazı özellikleri de vardır. İnsan görüşünün esnek olması ve görüntüdeki bilginin bir metindeki bilgi kadar hassas olmaması bu avantajlardan sayılabilir.

Görüntü şifreleme için kullanılan metotları kaosa dayalı olan ve kaosa dayalı olmayan yöntemler şeklinde ikiye ayırmak mümkündür. Başka bir sınıflandırma biçimi ise tam şifreleme ve kısmi şifreleme şeklinde yapılabilir.

Görüntü şifrelemede çoğunlukla kullanılan bazı yöntemler vardır. Bunlar; yer değiştirme, yerine koyma ya da her ikisinin bir arada kullanıldığı yöntemlerdir(substitution– permutation network). Bu yöntemler piksel ya da bit tabanlı gerçekleştirilmesine göre de farklılık gösterir.

Yer Değiştirme (Permutation): Bir blok içerisindeki değerlerin belirli bir permütasyona göre yerlerinin değiştirilmesi işlemidir.

Yerine Koyma (Substitution): Bir blok içerisindeki değerlerin bir fonksiyona ya da bir tabloya göre değerlerinin değiştirilmesi işlemidir.

Shannon' un en önemli eserinde bahsettiği gibi güvenli bir şifreleme işlemi ancak yer değiştirme ve yerine koyma işlemlerinin tekrarlanması ile mümkündür (Shannon, 1949). Bundan yola çıkılarak substitution – permutation network (SPN – Yerine koyma-yer değiştirme ağı) sistemleri oluşturulmuştur.

3.8. Kaotik Sistemler

Kaos evrende neredeyse her şeyde var olan bir sistemdir. Kaosa dair ilk çalışmalar meteorolog Edward N. Lorenz tarafından 1963' te yapılmıştır (Lorenz, 1963). Lineer olmayan kaos, başlangıç koşullarına hassas bağlılığıyla ve rasgele gibi davranışlarıyla pek çok alanda ilgi odağı olmaya devam etmektedir. Lorenz' in, "Brezilya' da kanat çırpan bir kelebek Texas'ta bir fırtınanın başlamasına sebep olabilir mi?" ifadesinden yola çıkılarak, başlangıç koşullarına olan hassas bağlılık, 'kelebek etkisi' şeklinde ifade edilmiştir.

Kaotik sistemlere ait bazı özellikler aşağıdaki gibi sıralanabilir:

- Kaos, lineer olmayan kararlı bir süreç sonucu oluşur.

- Dağınık ve düzensiz görünmesinin yanında istatiksel rasgelelik testlerini geçer.
- Başlangıç koşullarına ve parametrelerine aşırı derecede hassasiyet gösterir.
- Parametrelerinin belli bir aralıkta olma zorunluluğu vardır. Parametreleri uygun bir aralıkta seçildikten sonra herhangi bir başlangıç değeriyle kaotik bir sistem oluşturulabilir.

3.8.1. Kaotik davranışın ölçülmesi

Kaotik bir davranışın ölçülmesi için dikkat edilen bazı noktalar vardır. Bunlar arasında Lyapunov üstelleri, entropi ve sistemin kaç boyutlu olduğu önemli yer tutmaktadır.

Lyapunov üstelleri çekicilerin ortalama yakınsama ve ıraksama oranını vermekle beraber, sistemin başlangıç koşullarına ne kadar hassasiyetle bağlı olduğu konusunda da bilgi verir.

Kolmogorov entropi denen yöntem ile de çekicinin bir yörünge boyunca ne kadar kaybı olduğu belirlenebilir.

Kaotik sistemin kaç boyutlu olduğu ise, sistemin geometrik yapısı hakkında bilgi verir (Jiu ve Chi, 2008).

3.8.2. Ayrık kaotik sistemler

Ayrık kaotik fonksiyonların, diğer bir deyişle haritaların, matematiksel ifadesi için pek çok tanım olmasına rağmen basitçe ele alınırsa bir boyutlu bir harita şöyle ifade edilir:

f Fonksiyonu $\Delta = [0,1]$ aralığında sürekli bir fonksiyon ise;

$f: \Delta \rightarrow \Delta$, $x_{k+1} = f(x_k)$ ve $x_0 \in \Delta$ olmak üzere f fonksiyonunun aşağıda verilen maddelerin sağlanması durumunda kaotik olduğu söylenebilir.

1. *Başlangıç koşullarına hassas bağlılık*

$\exists\delta > 0\,, \forall x_0\ \in \Delta\,, \varepsilon > 0\,, \exists n \in N\,, y_0 \in \Delta$:

$$|\mathrm{x}_0 - \mathrm{y}_0| < \varepsilon \Longrightarrow\ |f^n(x_0) - f^n(y_0)| > \delta \tag{10}$$

Eş. 10 sağlandığı sürece fonksiyonun başlangıç koşullarına hassas bir şekilde bağlı olduğu söylenebilir.

2. *Topolojik Geçişlilik*

$\forall\ \Delta_1, \Delta_2 \subset \Delta\,, \exists x_0 \in \Delta_1\,, n \in N:$

$$f^n(x_0) \in\ \Delta_2 \tag{11}$$

Eş. 11deki şartın sağlandığı durumda fonksiyonun topolojik geçişliliğe sahip olduğu söylenebilir.

3. *Δ üzerindeki periyodik noktaların yoğunluğu*

$P = \{p \in \Delta \mid \exists\ n \in N : f^n(p) = p\}$ kümesi f'in periyodik noktalarının kümesi olsun.

$$\bar{P} = \Delta \tag{12}$$

3.8.2.1. Lyapunov üstelleri

Kaotik bir çekicinin yayılma yönündeki iki yakın yörüngesi birbirinden uzaklaşırken, daralma yönünde ise bu iki yörünge birbirine yakınsar. Bu yakınsama ve ıraksama üstel fonksiyonlarla ifade edilirse bu üstellere Lyapunov üstelleri denir. Lyapunov üstellerinin sayısı, sistemin kaç boyutlu olduğu hakkında bilgi verir ve en az bir pozitif

Lyapunov üsteli, sistemin kaotik olduğunu gösterir. Pozitif Lyapunov üsteli ne kadar büyükse, sistemin öngörülebilir zaman ölçeği de o kadar kısadır (Jiu ve Chi, 2008).

Ayrık bir kaotik sistemin Lyapunov üsteli şöyle elde edilir:

x_0 herhangi bir başlangıç koşulu, $\{x_k\}_{k=0}^{\infty}$ p- boyutlu bir haritanın yörüngeleri ve $m_1(k), m_2(k), m_3(k) \dots m_p(k)$ sistemin öz değerleri olmak üzere, i. Lyapunov üsteli aşağıdaki gibi elde edilir:

$$\lambda_i = \lim_{k\to\infty} \frac{1}{k} \ln|m_i(k)| \tag{13}$$

3.8.2.2. Kolmogorov entropi

Metrik Entropi ya da Kolmogorov – Sinai entropi olarak da bilinir. Çekicide bir yörünge boyunca kaybolan bilgi hakkında bir ölçü sunar. Başka bir deyişle, Kolmogorov entropi, çekici boyunca var olan noktaların tahmin edilebilirliğinin bir ölçüsüdür.

Entropinin belirlenmesi için dinamik bir çekici ε^L büyüklüğünde L bölgeye ayrılsın. $P_{i_0,i_1,\dots i_n}$ değerleri i_0'ın $t = 0$'da; i_1'in $t = T$'de, i_2'in $t = 2T$ anında bulunduğu yörüngenin olasılığı olmak üzere;

$$K_n = -\sum_{i_0,i_1,\dots i_n} P_{i_0,i_1,\dots,i_n} \ln\left(P_{i_0,i_1,\dots,i_n}\right) \tag{14}$$

$K_{n+1} - K_n$ yörüngedeki bilgi kaybını ifade etmek üzere, Kolmogorov entropi Eş. 15 ile hesaplanabilir.

$$K = \lim_{T\to 0} \lim_{\varepsilon\to 0^+} \lim_{N\to\infty} \frac{1}{NT} \sum_{n=0}^{N-1} (K_{n+1} - K_n) \tag{15}$$

3.8.2.3. Çekicinin boyutu

Kaotik bir sistemin dinamikleri değişse bile, bir çekiciyle sınırlanan kaotik hareketin geometrik yapısı ve boyutu değişmez. Esasında, kaotik çekicinin boyutu, çekicideki bir

yeri, belli bir doğruluk payıyla belirlemek için gereken bilgiyi sağlamalıdır. Bu durum, bilginin boyutu, aşağıdaki formülle ifade edilebilir:

$$d_I = \lim_{\varepsilon \to 0} \frac{\rho[B_x(\varepsilon)]}{\ln \varepsilon} \qquad (d_I\text{: information dimension}) \tag{16}$$

$\rho[B_x(\varepsilon)]$ ifadesi x noktası merkez olmak üzere, ε yarıçaplı bir küredeki noktaların toplamını verir. Daha ayrıntılı ifade edilecek olursa, U birim basamak fonksiyonu ve M faz uzayındaki noktaların sayısı olmak üzere;

$$\rho[B_x(\varepsilon)] \approx \frac{1}{M} \sum_{i=1}^{M} U(\varepsilon - \|x_i - x\|) \tag{17}$$

Eşitliği yazılabilir.

Buradan görüldüğü gibi, eşitlik sadece belli bir x noktasına bağlı olduğu için, Grassberger ve Procaccia Eş. 18'i kullanarak bu bağlılığı elimine etmeyi amaçlamıştır.

$$C(\varepsilon) = \frac{1}{M^2} \sum_{i,j=1, i \neq j}^{M} U(\varepsilon - \|x_i - x_j\|) \tag{18}$$

Bu eşitlik kullanılarak korelasyon boyutu hesaplanacak olursa;

$$d_C = \lim_{\varepsilon \to 0} \frac{\ln C(\varepsilon)}{\ln \varepsilon} \tag{19}$$

Bunlara ek olarak Lyapunov üstelleri ve Lyapunov boyutu arasında da sıkı bir bağ vardır.

Lyapunov boyutu Eş.20 ile ifade edilir.

$$d_L = k + \frac{\lambda_1 + \lambda_2 + \cdots + \lambda_k}{|\lambda_{k+1}|} \qquad k = max\{i: \lambda_1 + \cdots + \lambda_i > 0\} \tag{20}$$

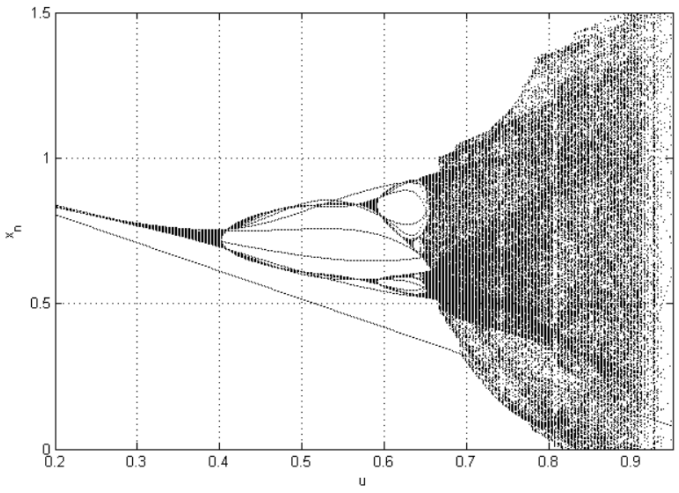
Kolmogorov entropi ve Lyapunov üstelleri arasındaki bir ilişkiden bahsetmek de mümkündür. Bir boyutlu haritalarda Kolmogorov entropi, Lyapunov üsteline eşitken; daha fazla boyuta sahip haritalarda bir noktanın diğer noktalar üzerindeki etkisinden dolayı durum biraz daha değişmektedir.

K , sistem hakkında kaybedilen bilginin oranını göstermek üzere aşağıdaki gibi Lyapunov üstelleri cinsinden ifade edilebilir.

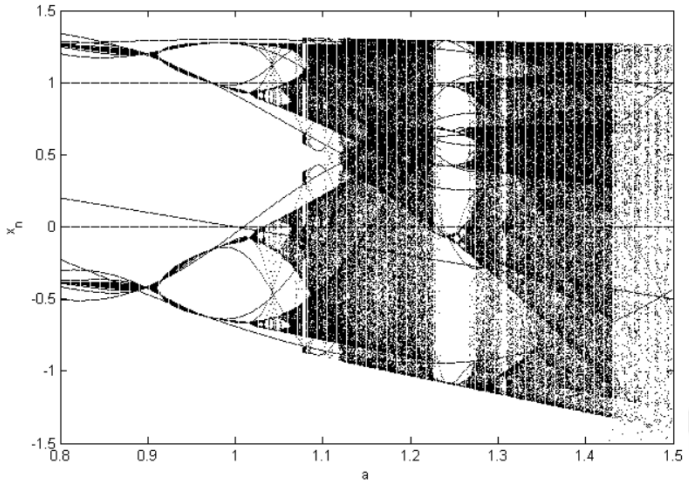
$$K = \sum_i \lambda_i \tag{21}$$

3.8.2.4. Çatallaşma diyagramı

Çatallaşma diyagramı kaotik haritanın içerdiği parametreye göre nasıl değiştiğini gösterir. Diğer bir deyişle parametrenin kaotik harita üzerindeki etkisini anlamanın bir yoludur. Şekil 3.12 ve Şekil 3.13'te sırasıyla Ikeda ve Henon kaotik haritalarının çatallaşma diyagramları verilmiştir. Şekillerden de görüleceği gibi haritada kullanılan parametrelerin etkili olduğu aralıklar çatallaşmanın arttığı ve sistemin kaotiklik özelliği gösterdiği aralıklardır.



Şekil 3.12. Ikeda kaotik haritasının çatallaşma diyagramı.



Şekil 3.13. Henon kaotik haritasının çatallaşma diyagramı.

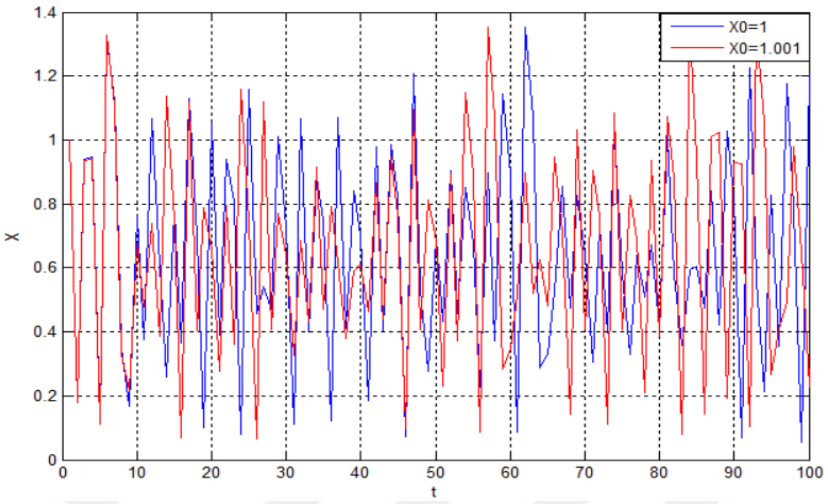
3.8.3. Ikeda kaotik harita

Ikeda kaotik harita Eş.22'te ifade edilen bir ayrık kaotik sistemdir (Ikeda, 1979).

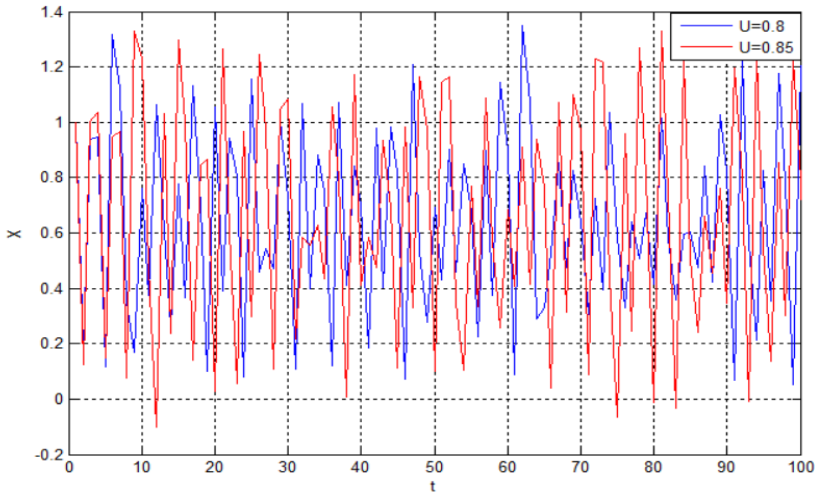
$$x_{n+1} = 1 + u(x_n \cos t_n - y_n \sin t_n)$$
$$y_{n+1} = u(x_n \sin t_n + y_n \cos t_n)$$
$$t_n = c - \frac{6}{1+x_n^2+y_n^2} \qquad c = 0{,}4 \tag{22}$$

Denklemlerde yer alan u sistem parametresidir ve kaotik bir sistem elde edebilmek için bu değerin şu aralıkta olması gerekir: u = [0.5, 0.95]

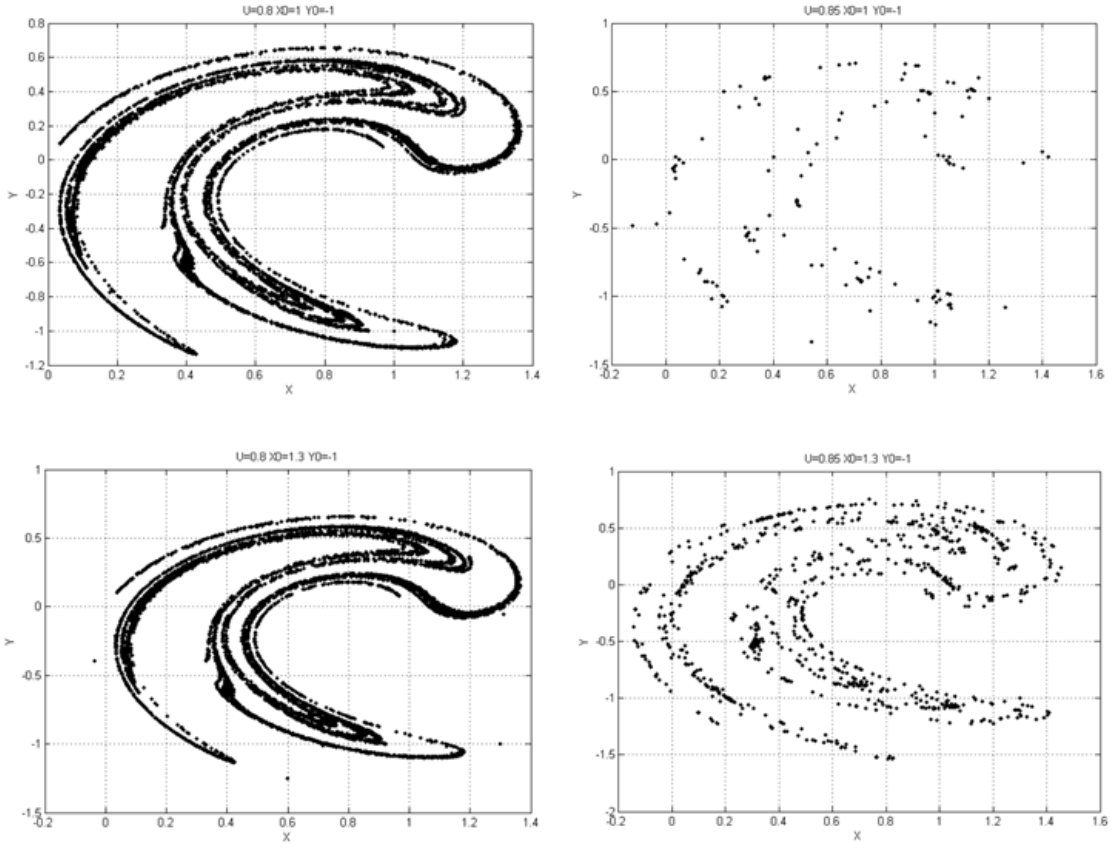
Şekil 3.14'te Ikeda haritasının başlangıç değerlerine hassas bir şekilde bağlı olduğu görülmektedir. Aralarında 10^{-3} kadar fark olan iki başlangıç noktası için, aynı parametre değeri için x_n fonksiyonu çizdirildiğinde fark açıkça görülmektedir. Şekil 3.15'te ise parametre hassasiyeti gösterilmiştir. Aynı başlangıç koşulları ile olması gereken aralık korunması koşuluyla parametre değeri değiştirilmiştir. Şekil 3.16'da Ikeda kaotik haritasının farklı başlangıç değerleri ve farklı u parametre değerleri için faz diyagramı verilmiştir.



Şekil 3.14. Ikeda kaotik haritasının başlangıç koşullarına olan hassas bağımlılığı.



Şekil 3.15. Ikeda kaotik haritasının ‘u’ parametresine hassas bağımlılığı.



Şekil 3.16. Farklı parametre ve başlangıç değerleri için Ikeda haritasının faz diyagramı.

3.8.4. Henon kaotik haritası

1978'de keşfedilen Henon kaotik sistemi aşağıdaki denklemlerle ifade edilir (Petrisor, 2003).

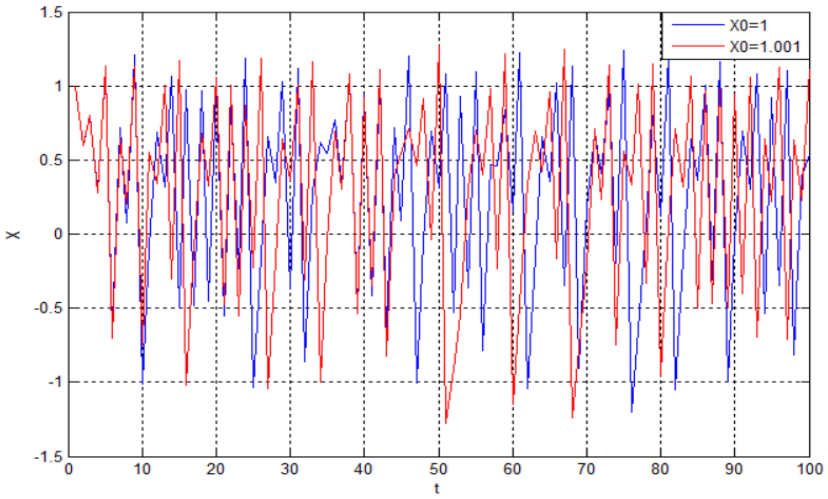
$$x_{n+1} = 1 - ax_n^2 + y_n$$

$$y_{n+1} = bx_n \tag{23}$$

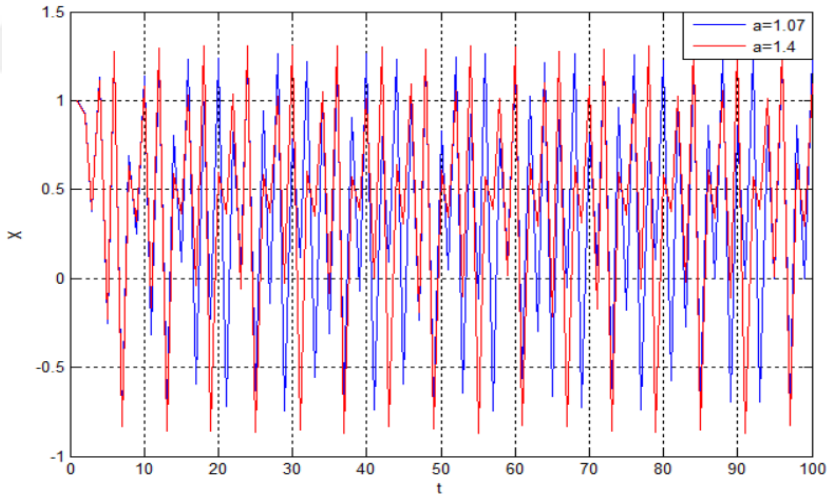
Eş. 23' te $a = 0.3$ ve $b \in [1.07\,,1.4\,]$ şeklinde seçilecek olursa kaotik bir sistem elde edilir.

Şekil 3.17 ve Şekil 3.18'de Henon kaotik haritasının farklı başlangıç değerleri ve farklı a parametre değerleri için faz diyagramı verilmiştir. Kaotik sistemlerin en belirgin

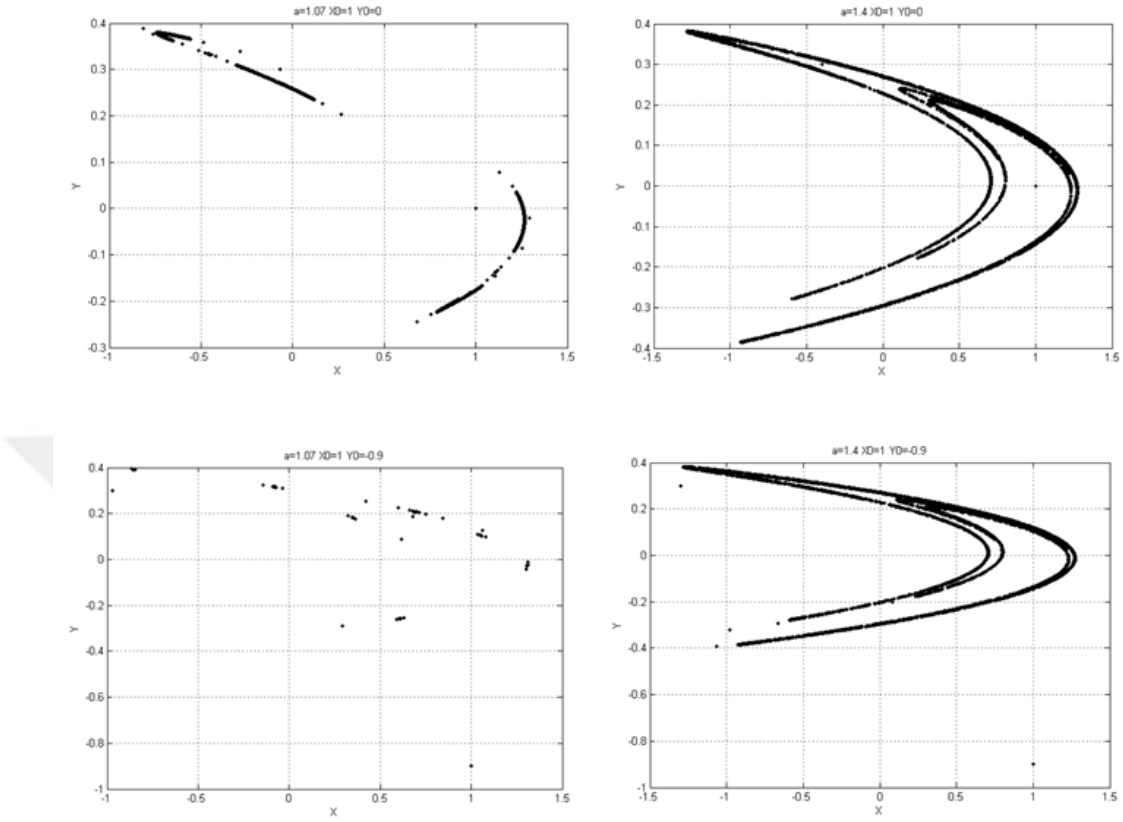
özelliklerinden olan başlangıç koşullarına ve parametrelere aşırı hassasiyet şekillerde açık bir şekilde görülmektedir.



Şekil 3.17. Henon kaotik haritasının başlangıç koşullarına olan hassas bağımlılığı.



Şekil 3.18. Henon kaotik haritasının ‘a’ parametresine hassas bağımlılığı.



Şekil 3.19. Farklı parametre ve başlangıç değerleri için Henon haritasının faz diyagramı.

3.8.5. Kaos ve kriptografi arasındaki ilişki

Kaos ve kriptografi arasındaki benzerlikler pek çok çalışmanın konusu olmuştur (Dachselt ve Schwarz, 2001; Kocarev, 2001; Masuda ve ark., 2006). Shannon, kaos araştırmalarından önce kriptografik algoritmalarda kaotik bir sistemin özelliklerinden olan başlangıç koşulları ve parametrelere olan hassas bağlılıkla, karışma özelliğinin kullanılması gerektiğinden bahsetmiştir (Shannon, 1949). Kaos biliminin en temel özelliklerinden olan başlangıç koşullarına hassas bağlılık, kriptolojide anahtara olan hassas bağlılığa karşılık geldiği gibi, kriptolojide algoritmanın güvenliğini artırmak için gerçekleştirilen tekrarlar, kaotik sistemlerde ise iterasyonlara karşılık gelmektedir. Bir kaotik harita topolojik geçişliliğe sahip olduğu için ergodiklik özelliğine de sahiptir. Yani, durum uzayı sonlu sayıda parçaya ayrıldığında, haritanın herhangi bir yörüngesi bütün bölgelerden geçer. Bu

özellik ise kripto sistemlerin yayılma özelliğine karşılık gelir. Bunun gibi benzerlikler, kaosun kriptografide kullanımını kaçınılmaz kılmıştır. İki bilim arasındaki temel fark ise, kriptolojinin tamsayılardan oluşan sınırlı bir alanda; kaosun ise gerçek sayılardan oluşan sonsuz bir alanda çalışmasıdır. Bundan dolayı kaos kriptolojide kullanılırken haritalar denilen ayrık fonksiyonlar şeklinde ifade edilerek kullanılır. Bahsedilen özellikler Çizelge 3.1'de özetlenmiştir.

Çizelge 3.1. Kaotik sistemler ve kriptografi arasındaki benzerlikler.

Kaotik Sistemler	**Kriptografik Algoritmalar**
Başlangıç koşullarına ve parametrelere hassas bağlılık	Anahtara hassas bağlılık
Haritalarda iterasyonlar yapılması	Algoritmaların tekrarlanması(round)
Ergodiklik	Yayılma

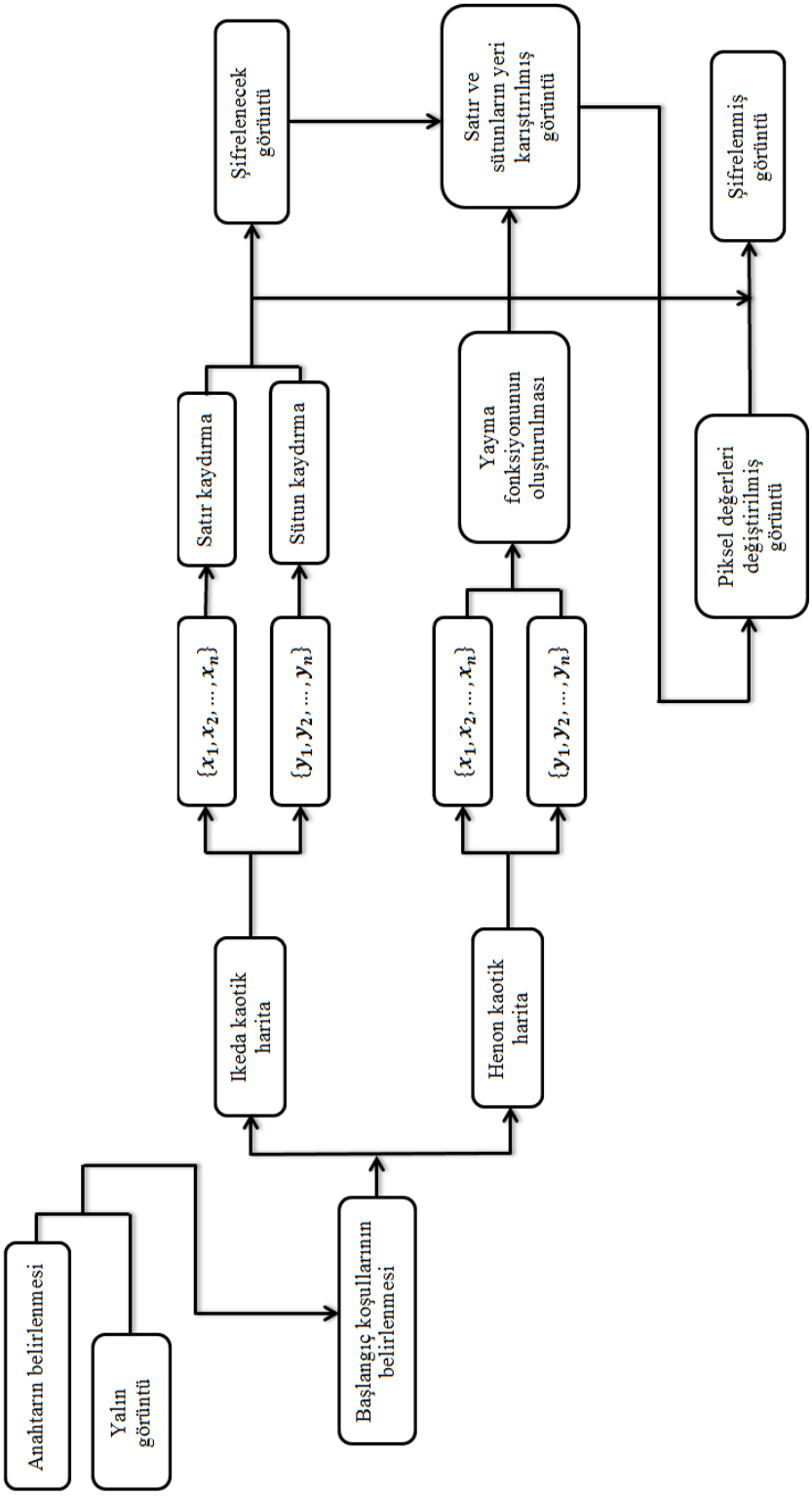
4. BULGULAR VE TARTIŞMA

Tez çalışmasında gri renk seviyesine sahip görüntülerle renkli görüntülerin şifreleme ve şifre çözme işlemleri gerçekleştirilmiştir. Şifreleme aşamasında Ikeda kaotik haritası yer değiştirme işlemlerinde; Henon kaotik haritası ise yayılma işleminde kullanılmıştır. Her iki haritanın başlangıç değerleri ve birer parametresi ise şifreleme – şifre çözme anahtarını oluşturmak için kullanılmıştır. Şifreleme ve şifre çözme işlemleri gerçekleştirildikten sonra algoritmanın güvenliği çeşitli analizlere tabi tutulmuştur. Histogram analizi, anahtar hassasiyeti analizi, korelasyon analizi ve hız değerlendirmesi bu analizlerden bazılarıdır.

4.1. Gri Seviyeli Görüntülerin Şifrelenmesi

İki boyutlu bir matris olarak düşünülebilen gri seviyeli bir görüntü $I = f(x, y)$ şeklinde ifade edilebilir. Bu ifadede x ,görüntünün satırına denk gelirken; y ise sütununu belirtmektedir. I ise x ve y ile belirtilen pikselin değerini belirtmektedir.

Verilen örneklerde sırasıyla görüntünün satır ve sütun konumları karıştırılmış; ardından pikselin değeri değiştirilmiştir. Aşağıda bu işlemler sırasıyla gösterilmiştir.



Şekil 4.1. Şifreleme algoritmasının akış diyagramı.

Akış diyagramı daha ayrıntılı incelenecek olursa yapılan işlemler aşağıdaki gibi anlatılabilir:

1. Öncelikle şifreleme ve deşifreleme işlemlerinde kullanılacak olan anahtar, kullanılan kaotik haritaların başlangıç değerlerini oluşturmada kullanılacak elemanlardan ve bu kaotik haritaların parametrelerinden oluşacak şekilde belirlenir. Yapılan çalışmalarda anahtar aşağıdaki gibi belirlenmiştir.

u ve b haritaların parametreleri olmak üzere, anahtar aşağıdaki gibi belirtilir.

$$Anahtar = \left[X_0^{ikeda}, Y_0^{ikeda}, u, b, X_0^{henon}, Y_0^{henon}\right]$$

$$Anahtar = [0.957559999 \quad 0.957969999 \quad 0.876549999 \quad 1.388999999 \quad 1.000019999 \quad 0.000019999]$$

2. Görüntünün boyutu *MxM* ise Ikeda kaotik haritası M iterasyona uğratılarak X ve Y dizilimleri elde edilir. Ikeda kaotik haritasının başlangıç değerleri Eş. 24 ifadesiyle elde edilir.

$$x_0^{ikeda} = anahtar(1) * mod(sum(Input), 256)$$
$$y_0^{ikeda} = anahtar(2) * mod(sum(Input), 256) \qquad (24)$$

3. Elde edilen X ve Y dizilimleri ayrı birer matris olarak kaydedilir. X diziliminin P matrisinde; Y diziliminin Q matrisinde kaydedildiği kabul edilsin.

4. X ve Y dizilimleri kendi içlerinde küçükten büyüğe doğru sıralanarak elde edilen dizilimler ise P' ve Q' şeklinde kaydedilir.

5. P' ve Q' matrislerinde kaydedilen her bir X ve Y değerinin P ve Q matrislerindeki konumları bulunarak satır ve sütunların konumlarını karıştırmada kullanılacak matrisler oluşturulur.

6. Bu matrislerden X diziliminin konumunu tutan matris satırların yerlerinin değiştirilmesinde; Y diziliminin konumunu tutan matris ise sütunların yerlerinin değiştirilmesinde kullanılır.

7. Piksellerin konumları değiştirildikten sonra ise Henon kaotik harita $M * M$ iterasyona uğratılır ve bir diğer X ve Y dizilimi elde edilir. Henon kaotik haritasının başlangıç değerleri Eş. 25 ifadesiyle elde edilir.

$$x_0^{Henon} = anahtar(5) * mod(sum(Input), 256)$$

$$y_0^{Henon} = anahtar(6) * mod(sum(Input), 256) \quad (25)$$

8. Henon kaotik haritasıyla elde edilen x_Henon ve y_Henon dizilimleri Eş. 26'da belirtilen denklemlerle tam sayıya dönüştürülür.

$$X = \text{floor}(\text{mod}(\text{x\_Henon} * 10^{14}, 256))$$

$$Y = \text{floor}(\text{mod}(\text{y\_Henon} * 10^{14}, 256)) \quad (26)$$

9. Tam sayıya dönüştürülen dizilimler, yayma işleminin gerçekleştirilmesi için Eş. 27'de ifade edilen denklemde kullanılır.

$$I_{yeni} = ((((I(i) \oplus X(i)) \oplus Y(i)) \oplus mod((X(i) + Y(i)), 2^8)) \oplus X(i)) \oplus mod((X(i) + Y(i)), 2^8) \quad (27)$$

Verilen işlem aşağıdaki döngüde yer aldığı gibi her bir piksele uygulanarak pikselin değeri değiştirilir.

$for\ i = 1{:}\, n * n$

$I_{yeni} = ((((I(i) \oplus X(i)) \oplus Y(i)) \oplus mod((X(i) + Y(i)), 2^8)) \oplus X(i)) \oplus mod((X(i) + Y(i)), 2^8)$

end

10. Yayma işleminden sonra algoritmayı istatiksel açıdan daha güvenilir hale getirmek için satır ve sütunların konumunu değiştirme işlemi bir kez daha gerçekleştirilir.

11. Şifre çözme işleminde ise yukarıda bahsedilen adımların hepsi sondan başlanarak gerçekleştirilir.

Renkli resimlerde bahsedilen şifreleme aşamaları kırmızı, yeşil ve mavi renk kanallarının hepsine ayrı ayrı uygulanır. İşlemlerin sonunda üç kanaldan elde edilen sonuçlar bir araya getirilerek şifrelenmiş görüntü elde edilir.

Renkli görüntülerde farklı olarak gerçekleştirilen bir diğer durum ise yayma fonksiyonunun üç kanal için de farklı olmasıdır. Renkli görüntülerde aşağıdaki yayma fonksiyonları kullanılmıştır:

Kırmızı renk kanalında;

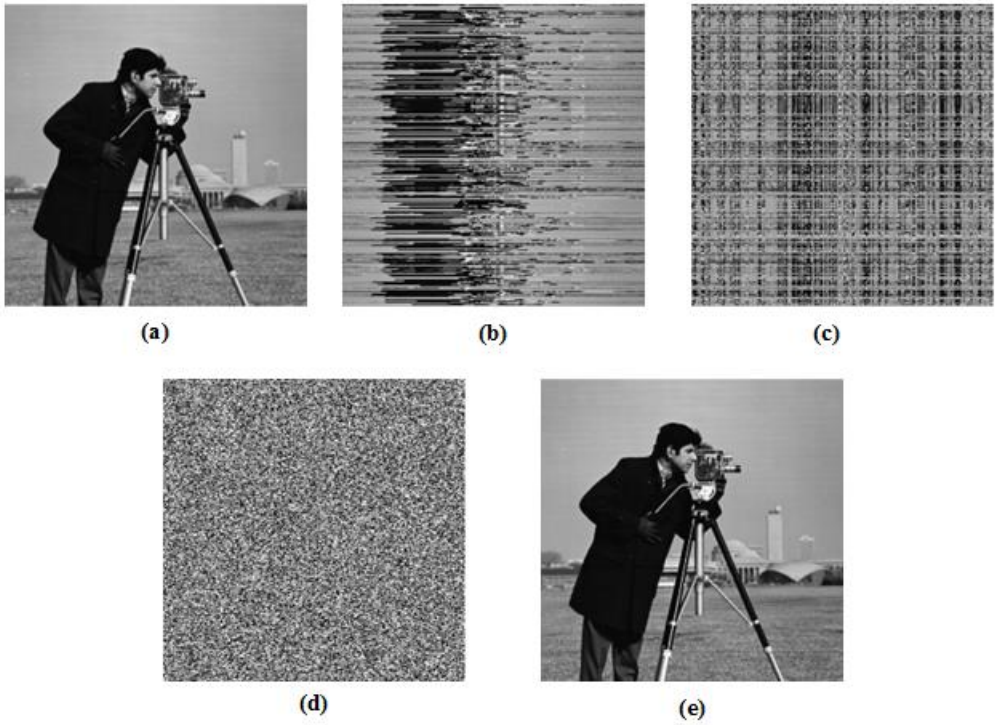
$$K_{yeni}(i) = ((((K(i) \oplus X(i)) \oplus Y(i)) \oplus mod((X(i) + Y(i)), 2^8)) \oplus X(i)) \oplus Y(i) \quad (28)$$

Yeşil renk kanalında;

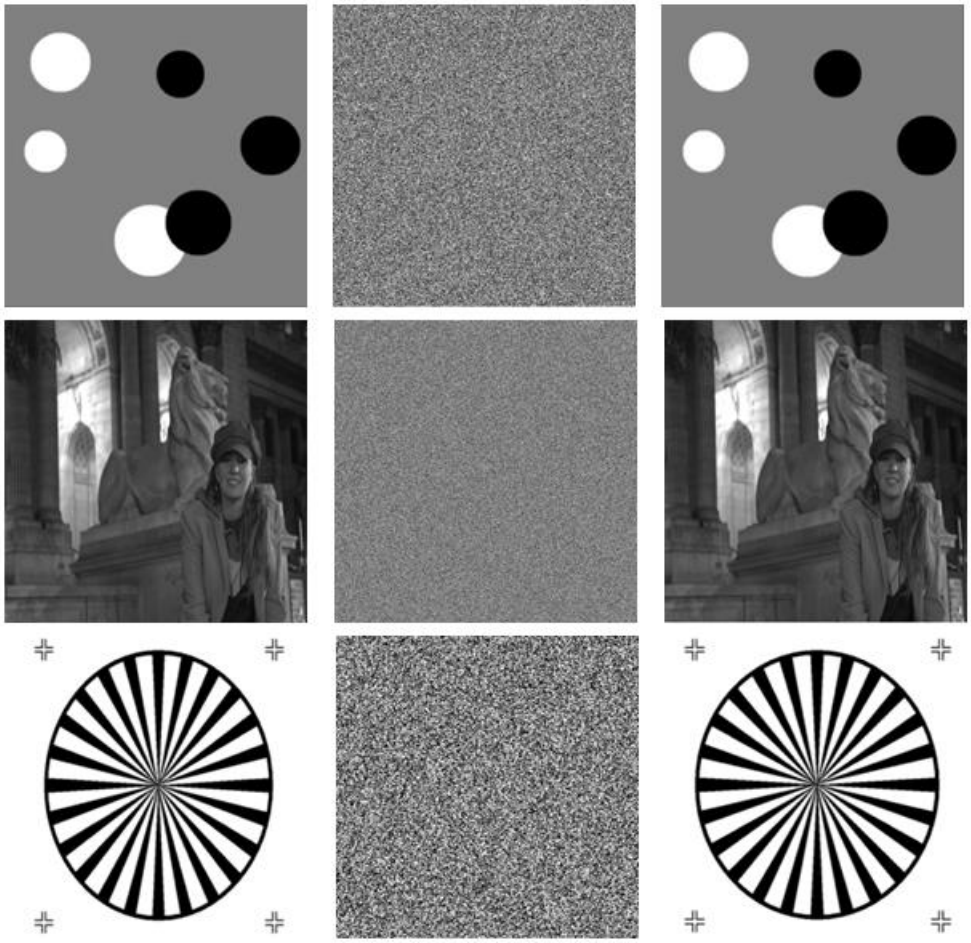
$$Y_{yeni}(i) = ((((Yesil(i) \oplus X(i)) \oplus Y(i)) \oplus mod((X(i) + Y(i)), 2^8)) \oplus X(i)) \oplus mod((X(i) + Y(i)), 2^8) \quad (29)$$

Mavi renk kanalında;

$$M_{yeni}(i) = ((((M(i) \oplus X(i)) \oplus Y(i)) \oplus mod((X(i) + Y(i)), 2^8)) \oplus mod((X(i) + Y(i)), 2^8)) \oplus Y(i) \quad (30)$$



Şekil 4.2. a) Cameraman.tif görüntüsü b) Görüntünün satırlarının kaydırılması sonucu elde edilen görüntü c) Görüntünün sütunlarının kaydırılması sonucu elde edilen görüntü d) Piksel değerleri değiştirilen görüntü e) Şifre çözme sonucu elde edilen görüntü.



Şekil 4.3. a) Şifrelenecek görüntüler b) Şifrelenmiş görüntüler c) Şifre çözme sonucu elde edilen görüntüler.

4.2. Renkli Görüntülerin Şifrelenmesi

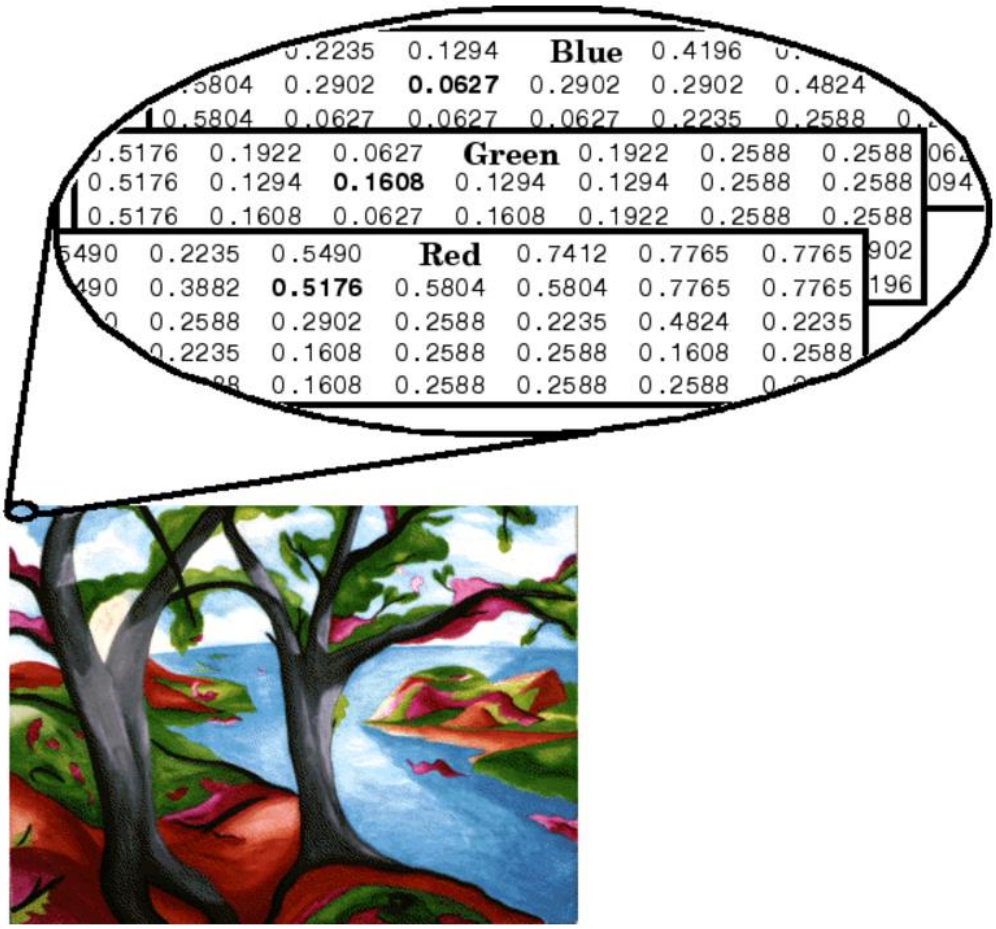
Renkli görüntüler genel olarak $I = f(x, y, z)$, $z \in \{1, 2, 3\}$ şeklinde ifade edilir. Ana renkler;

$$Red(kırmızı) = f(x, y, 1)$$

$$Green(yeşil) = f(x, y, 2)$$

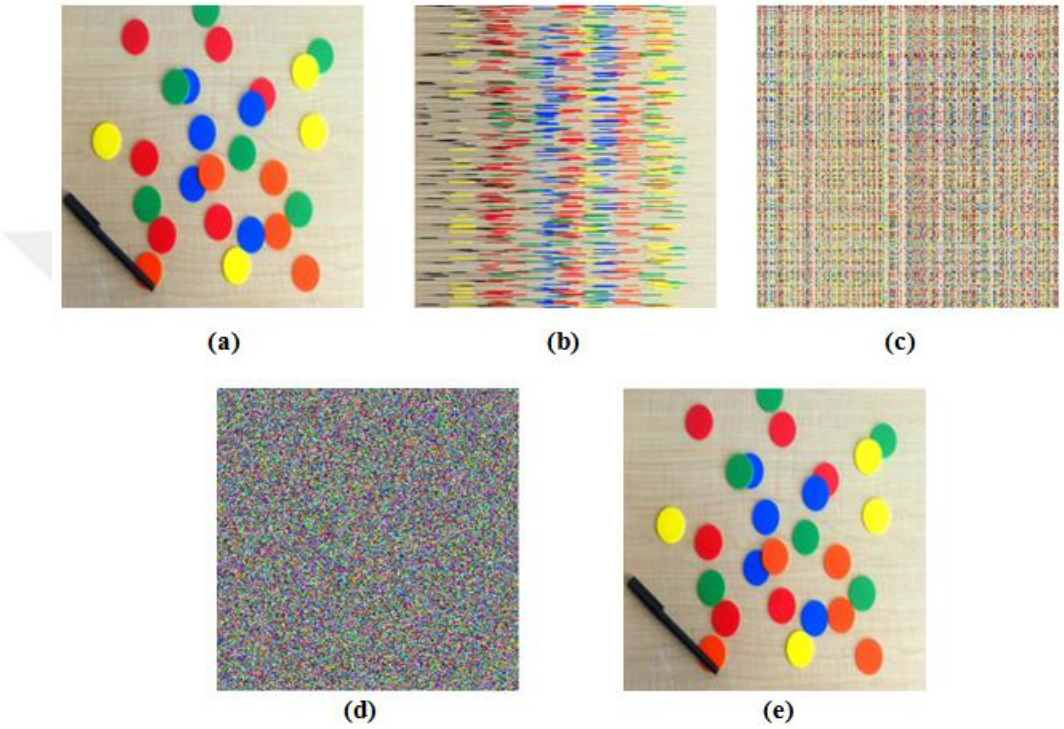
$$Blue(mavi) = f(x, y, 3)$$

ifadelerine denk gelir. Pikselin değeri her üç renk matrisinin değerleriyle belirlenir.



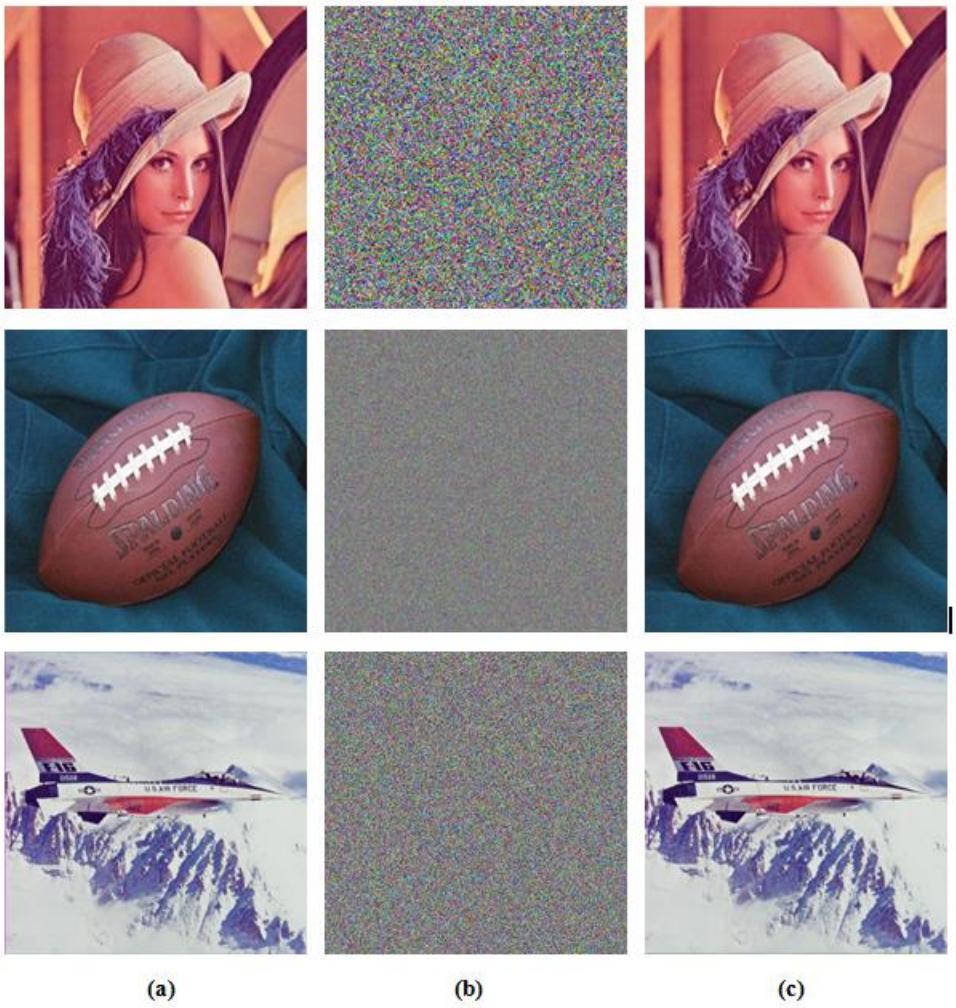
Şekil 4.4.Renkli resmin R–G–B bileşenleri
(https://www.mathworks.com/help/matlab/creating_plots/image-types.html,Mayıs 2017).

Renkli bir görüntü şifrelenirken algoritmadaki aşamalar kırmızı, yeşil ve mavi renk kanallarına ayrı ayrı uygulanır (Bkz. Bölüm 4.1). Şekil 4.5'te verilen örneklerde bu aşamalar belirtilmiştir.



Şekil 4.5. a) ColoredChips.png görüntüsü b) Görüntünün satırlarının kaydırılması sonucu elde edilen görüntü c) Görüntünün sütunlarının kaydırılması sonucu elde edilen görüntü d) Piksel değerleri değiştirilen görüntü e) Şifre çözme sonucu elde edilen görüntü.

Şekil 4.6'da ise çeşitli renkli görüntüler için şifreleme ve deşifreleme sonuçları verilmiştir. Görüntülerden de açıkça anlaşıldığı gibi şifrelenmiş görüntü baştaki görüntüye ait herhangi bir ipucu taşımamaktadır.



Şekil 4.6. a) Şifrelenecek renkli görüntüler b) Şifrelenmiş görüntüler c) Şifre çözme sonucu elde edilen görüntüler.

4.3. Çalışmanın Güvenlik Analizi

Bir şifreleme algoritması geliştirildiğinde en önemli adımlardan biri de kriptanalizdir. Kriptanaliz bölümünde algoritma belirli güvenlik testlerinden geçirilir ve çeşitli saldırılara maruz bırakılır. Elde edilen sonuçlar geliştirilen yöntemin ne kadar güvenli olduğu konusunda bilgi verir. Bu çalışma için yapılacak güvenlik testleri; histogram analizi, anahtar hassasiyeti testi, diferansiyel analiz, Shannon entropi testi ile korelasyon katsayısı ve dağılımı analizidir.

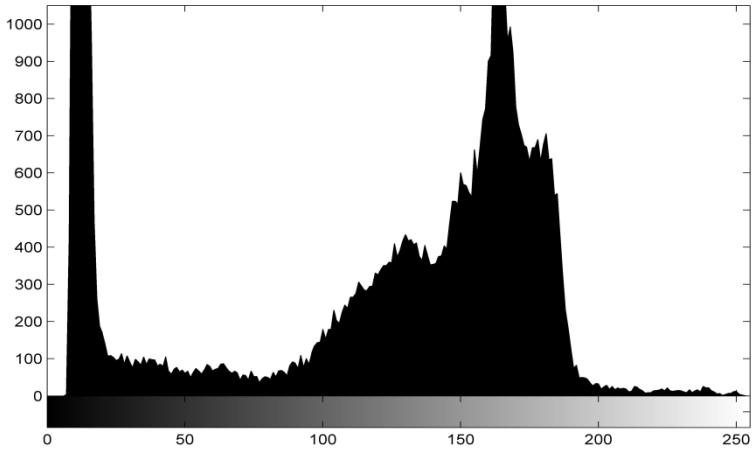
4.3.1. Histogram analizi

Histogram, dijital bir görüntüdeki her bir renk değerinde kaçar tane piksel olduğunu gösteren grafiktir. Başka bir ifadeyle, histogram [0,G] aralığında L toplam olası yoğunluk seviyesinin Eş. 31'de belirtildiği bir ayrık fonksiyondur.

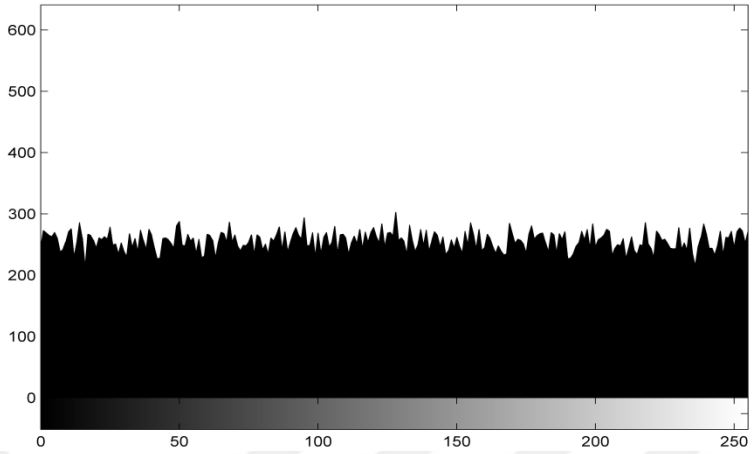
$$h(r_k) = n_k \tag{31}$$

Eş. 31' de r_k $[0, G]$ aralığındaki k. seviyedeki yoğunluk olmak üzere, r_k yoğunluk seviyesindeki toplam piksel sayısı ise n_k ile ifade edilmektedir (Gonzales ve ark., 2009).

Şifrelemeden sonra beklenen, histogramın tek düze bir yapıya sahip olmasıdır. Böylece histogramdaki istatiksel bilginin kullanılarak görüntüye ulaşılması zorlaştırılır.



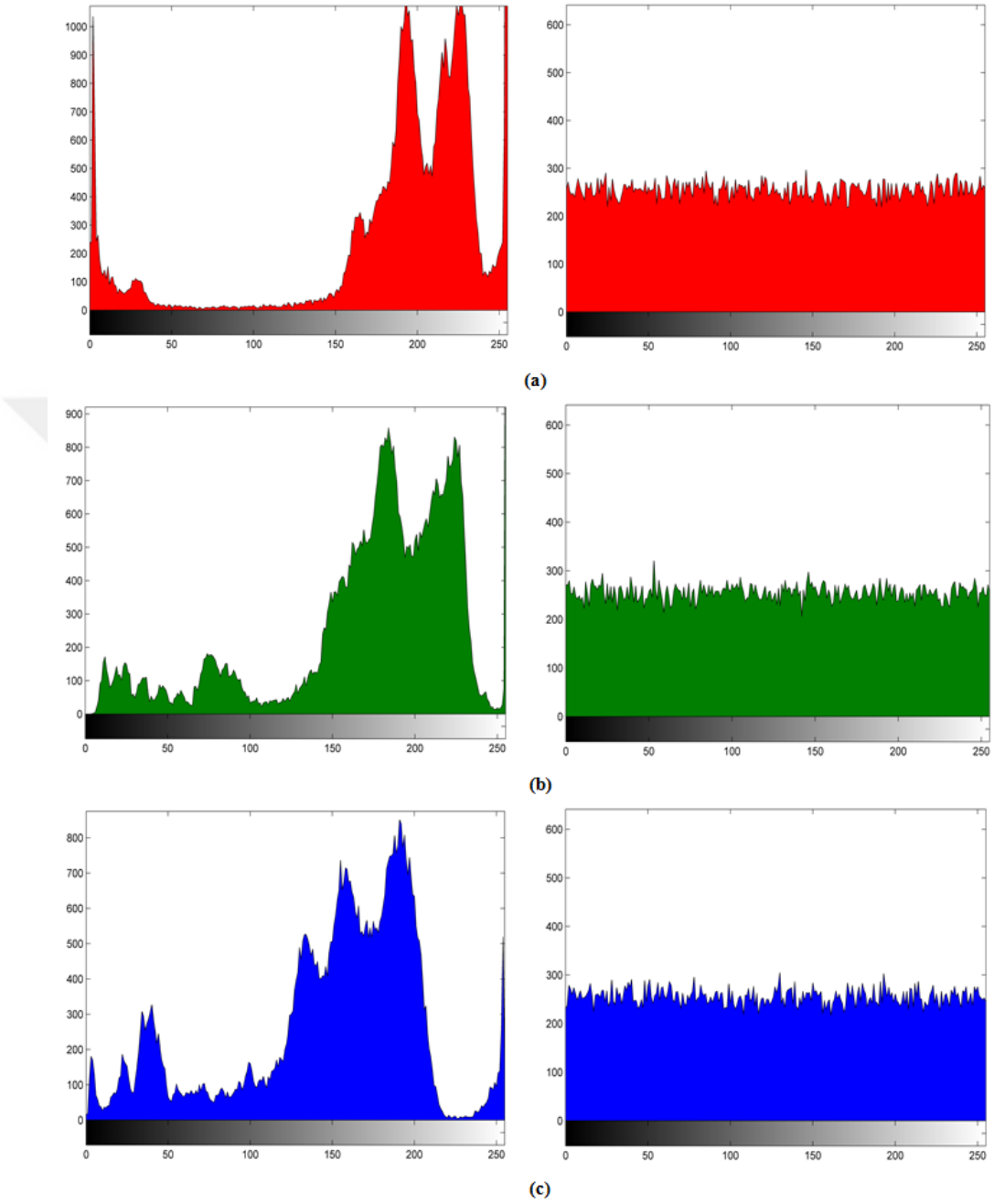
Şekil 4.7. Cameraman.tif görüntüsünün histogramı.



Şekil 4.8. Şifrelenmiş Cameraman.tif görüntüsünün histogramı.

Şekil 4.7 ve Şekil 4.8'de gri renk seviyesine sahip bir görüntüye ait histogram bilgileri verilmiştir. Renkli bir görüntüde ise kırmızı, yeşil ve mavi renk kanallarının histogram bilgileri ayrı ayrı incelenmelidir. Üç renk kanalına ait histogramın da beklentileri karşılaması gerekmektedir. Yapılan çalışmalarda, renk kanallarında kullanılan yayılma fonksiyonunda yapılan bazı değişikliklerin kimi renk kanalına ait histogram için eşit dağılımlı sonuç verirken, kimi renk kanalında da beklentinin altında kalmasıyla sonuçlandığı görülmüştür.

Önerilen şifreleme algoritması kullanılarak renkli bir görüntünün şifrelenmesi sonucu renk kanallarına ait histogram bilgisi Şekil 4.9'da verilmiştir. Görüldüğü gibi şifrelemeden sonraki histogram, güvenilir bir algoritmadan beklenildiği gibi eşit dağılıma sahip olmuştur.



Şekil 4.9. ColoredChips.png görüntüsünün a) kırmızı kanalının ,b) yeşil kanalının , c) mavi kanalının şifrelenmeden önceki ve şifrelendikten sonraki histogramı.

4.3.2. Diferansiyel analiz

Diferansiyel saldırı, seçilmiş açık metin saldırısı olarak da bilinir. Saldırıyı yapan kişi şifreli mesajla, açık mesaj arasında bir ilişki bulmaya çalışır. Bu yüzden güvenli bir şifreleme algoritmasında, birbirinden sadece bir piksel bile farklı olan iki görüntü şifrelendiğinde, elde edilen şifreli görüntülerin birbirinden tamamen farklı olması beklenir.

Elde edilen şifreli görüntülerin karşılaştırılması için NPCR (Number of Pixel Change Rate – Piksel Değişim Oranı Sayısı) ve UACI (Unified Average Change Intensity – Birleşik Ortalama Değişim Yoğunluğu) testleri kullanılır (Wu ve ark., 2011).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} x100 \tag{32}$$

$$D(i,j) = \begin{cases} 1 \; if \; C_1(i,j) \neq C_2(i,j) \\ 0 \; if \; C_1(i,j) = C_2(i,j) \end{cases} \tag{33}$$

$$UACI = \frac{1}{N}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{2^k - 1}\right) x100 \tag{34}$$

Verilen denklemlerde C_1 ve C_2 birbirinden sadece bir piksel farklı olan görüntüleri ifade etmektedir. Gri renk seviyesindeki görüntülerde (150, 250) noktasındaki piksel değeri; renkli görüntülerde ise (1, 20, 1) noktasındaki piksel değeri değiştirilmiştir.

Gri renk seviyeli görüntüler için diferansiyel analiz sonuçları Çizelge 4.1'de; renkli resimler için diferansiyel analiz sonuçları ise Çizelge 4.2'te verilmiştir.

NPCR ve UACI için verilen formüllerden (Eş. 32 ve Eş. 34) kolaylıkla hesaplanabileceği gibi bu değerlerin teorik olarak %99.60 ve % 33.45'e mümkün olduğunca yakın olması gerekmektedir (El-Assad ve Farajallah, 2016). Sonuçlar buna ulaşıldığını göstermektedir.

Çizelge 4.1. Gri renk seviyeli görüntüler için diferansiyel analiz sonuçları.

Görüntü	NPCR (%)	UACI (%)
Airport	99.6140	33.3588
Barbara	99.6215	33.4584
Cameraman	99.6368	33.3805
Chemical Plant	99.6338	33.5866
Clock	99.6078	33.5208
Couple	99.5926	33.5540
Lena	99.5987	33.3496
Man	99.5865	33.1347
Moon Surface	99.6338	33.3617
Test-pattern	99.6292	33.3955
Ortalama	**99.6155**	**33.4101**

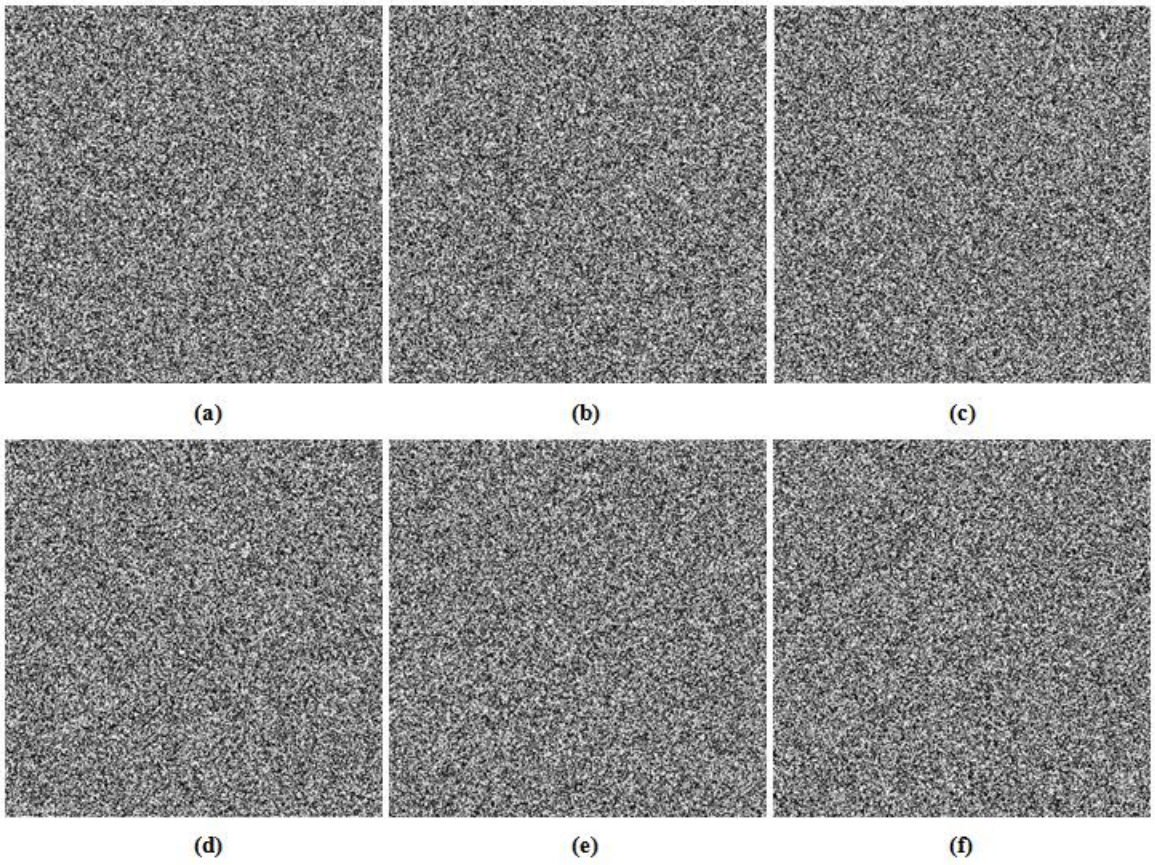
Çizelge 4.2. **‘**Lena’ renkli görüntüsü için diferansiyel analiz sonuçları.

	Önerilen Algoritma		**Murillo-Escobar ve ark. (2015)**	
	NPCR	**UACI**	**NPCR**	**UACI**
Kırmızı	99.594%	33.441%	99.63%	33.31%
Yeşil	99.60%	33.50%	99.60%	33.34%
Mavi	99.591%	33.50%	99.61%	33.43%
Ortalama	**99.60%**	**33.48%**	**99.61%**	**33.36%**

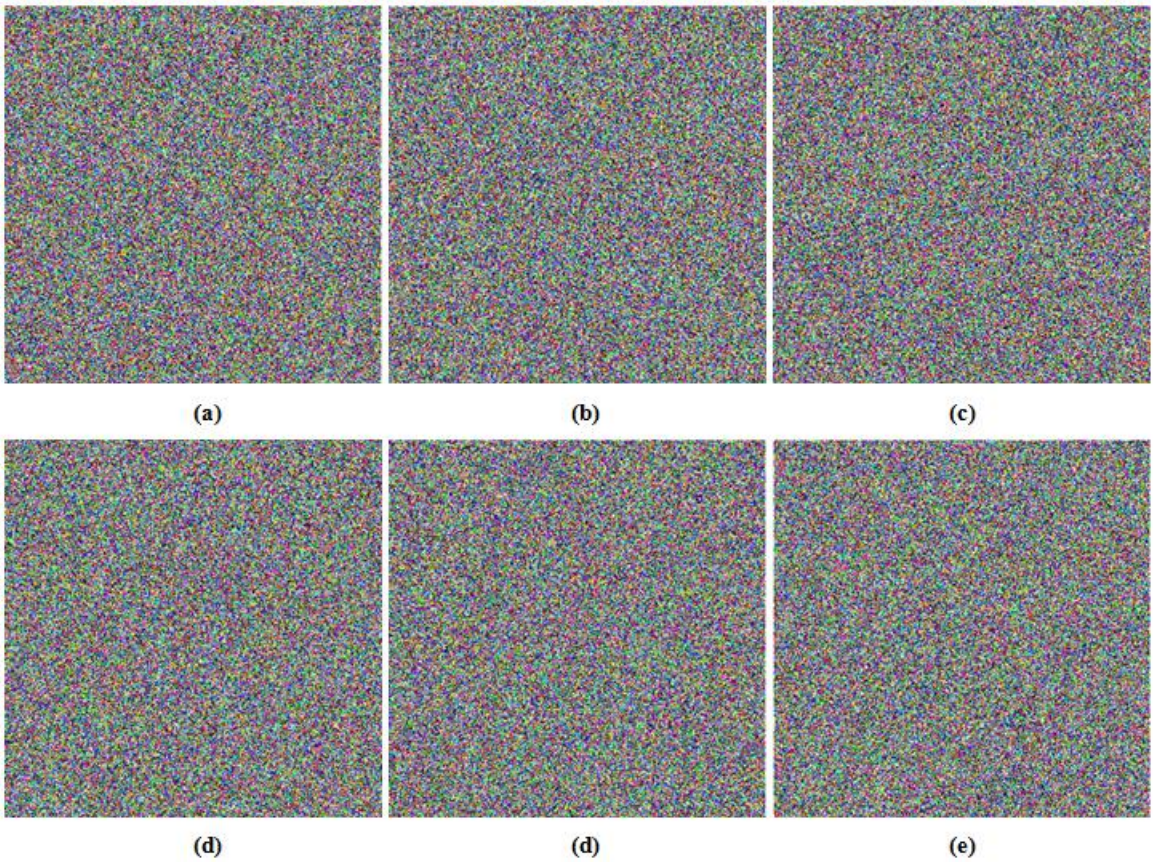
4.3.3. Anahtar hassasiyeti analizi

Geliştirilen algoritmanın yeterince güvenli olabilmesi için en önemli noktalardan biri de kullanılan anahtardaki en küçük bir değişikliğin bile deşifreleme aşamasında görüntüyü yeniden elde etmeye engel olmasıdır. Bunu test etmek için çalışmanın deşifreleme bölümünde anahtardaki her bir eleman sırasıyla 10^{-13} hassasiyetle

değiştirilmiş ve görüntü elde edilmeye çalışılmıştır. Hiçbir durumda görüntü elde edilememiştir.



Şekil 4.10. Cameraman.tif görüntüsü için; sırasıyla anahtarın a) birinci, b) ikinci, c) üçüncü, d) dördüncü, e) beşinci ve f) altıncı elemanının değiştirilmesi ile gerçekleştirilen şifre çözme işleminden elde edilen görüntüler.



Şekil 4.11. Lena görüntüsü için; sırasıyla anahtarın a) birinci, b) ikinci, c) üçüncü, d) dördüncü, e) beşinci ve f) altıncı elemanının değiştirilmesi ile gerçekleştirilen şifre çözme işleminden elde edilen görüntüler.

Anahtar hassasiyetine sayısal açıdan bakılacak olursa NPCR ve UACI testleri kullanılabilir. Çünkü bu testler iki görüntü arasındaki farklı olan piksel sayısı ve yoğunluğu hakkında bilgi vermektedir.

Çizelge 4.3 ve Çizelge 4.4 sırasıyla gri seviyeli ve renkli görüntüler için test sonuçlarını göstermektedir.

Çizelge 4.3. Lena.tif (512x512) görüntüsü için anahtar hassasiyeti analizi.

Anahtarın Değiştirilen Elemanı	NPCR	UACI
Anahtar(1) + 10^{-13}	99.60%	33.41%
Anahtar(2) + 10^{-13}	99.61%	33.49%
Anahtar(3) + 10^{-13}	99.59%	33.43%
Anahtar(4) + 10^{-13}	99.59%	33.50%
Anahtar(5) + 10^{-13}	99.60%	33.42%
Anahtar(6) + 10^{-13}	99.60%	33.46%
Ortalama	**99.60%**	**33.45%**

Çizelge 4.4. Lena.tiff (512x512x3) görüntüsü için anahtar hassasiyeti analizi.

Anahtarın Değiştirilen Elemanı	NPCR	UACI
Anahtar(1) + 10^{-13}	99.62%	33.47%
Anahtar(2) + 10^{-13}	99.60%	33.47%
Anahtar(3) + 10^{-13}	99.61%	33.50%
Anahtar(4) + 10^{-13}	99.62%	33.48%
Anahtar(5) + 10^{-13}	99.60%	33.42%
Anahtar(6) + 10^{-13}	99.61%	33.49%
Ortalama	**99.61%**	**33.47%**

4.3.4. Anahtar uzayı

Anahtar uzayı görüntüyü şifrelemek ve çözmek için kullanılabilecek olası anahtarlardan oluşan bir kümedir. Bu kümenin eleman sayısı ise, geliştirilen algoritmanın kaba kuvvet saldırılarına dayanıklılığı hakkında nicel bir değer sağlar. Kaba kuvvet saldırısı, mümkün olan tüm anahtarların denenerek doğru şifreleme anahtarının bulunmaya çalışıldığı bir saldırı türüdür. Günümüzde gelişmiş bilgisayar sistemleri ve teknolojinin geleceği düşünüldüğünde, kaba kuvvet saldırısının amacına ulaşması ihtimaline karşı anahtar uzayı mümkün olduğunca büyük olmalıdır. Alvarez'in ortaya koyduğu çalışmada algoritmanın güvenilirliği için anahtar uzayının en az 2^{100} olması gerektiği belirtilmektedir (Alvarez ve Li, 2006). Önerilen algoritmada anahtarı oluşturan elemanlar; Ikeda ve Henon

haritaların parametreleri ve haritaların başlangıç noktaları belirlenirken kullanılan değerlerdir.

$$key = [x_1 , y_1 , x_2, y_2, u, b] \quad u = [0.5 , 0.95] \;\; b = [1.07 , 1.4]$$

'Double' sınıfındaki elemanlar için hesaplama hassasiyeti 10^{16} alınırsa, anahtar uzayı aşağıdaki denklemle elde edilir (Xu ve ark., 2016).

'S' her bir elemanının alabileceği değerlerden oluşan kümeyi belirtirken, r algoritmanın uygulanma sayısını ve I ise haritaların tekrarlanma sayısını belirtir.

$$Anahtar\ uzayı = \quad rIS_{x_1}S_{x_2}S_{y_1}S_{y_2}S_uS_b = Ix(10^{16})^4x(0.95-0.5)x10^{16}x(1.4-1.07)x10^{16} \approx Ix1.485x10^{95} \approx Ix1.485x2^{315} \quad (35)$$

Çizelge 4.5. Önerilen algoritmanın anahtar uzayının bazı çalışmalarla karşılaştırılması.

Algoritmalar	Önerilen algoritma	Hua ve ark. (2015)	Murillo-Escobar ve ark. (2015)	Belazi ve ark. (2016)	Xu ve ark. (2016)
Anahtar uzayı	$> 2^{315}$	2^{256}	2^{128}	$> 2^{624}$	$> 2^{210}$

Eş. 35'te görüldüğü gibi anahtar uzayı 2^{315}'ten büyük bir değere sahiptir. Bu ise, algoritmanın kaba kuvvet saldırılarına dayanabileceğini ve sistemin güvenilir olduğunu gösterir. Çizelge 4.5'te yapılan karşılaştırmada ise anahtar uzayının Belazi ve ark. (2016)'nın çalışması hariç diğer çalışmalardan daha iyi bir değere sahip olduğu gösterilmiştir.

4.3.5. Korelasyon analizi

Bir görüntü için korelasyon, birbirine yakın iki piksel arasındaki benzerliği ifade etmektedir. r ile ifade edilen korelasyon katsayısı $[-1,1]$ aralığındadır. Yalın bir görüntüde korelasyon değeri oldukça yüksektir. Şifrelenmiş görüntüde ise beklenen, korelasyon

değerinin sıfıra yakın olmasıdır. Çünkü korelasyon katsayısının sıfıra yakın olması, iki piksel arasındaki benzerliğin çok az olduğunu; 1'e ya da -1'e yakın değerler ise benzerliğin arttığının bir ifadesidir.

Eş. 36'daki korelasyon elde edilirken Eş. 37 – 38 – 39 kullanılır.

$$E(x) = \frac{1}{R}\sum_{i=1}^{R} x_i \tag{36}$$

$$D(x) = \frac{1}{R}\sum_{i=1}^{R}((x_i - E(x))^2) \tag{37}$$

$$cov(x,y) = E\big[\big(x - E(x)\big)\big(y - E(y)\big)\big] = \frac{1}{R}\sum_{i=1}^{R}[\big(x_i - E(x)\big)(y_i - E(y))] \tag{38}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{39}$$

Denklemlerde x ve y ,sırasıyla satır ve sütun yönündeki pikselleri ifade etmektedir. Bu değerler kullanılarak çizilen ve yatay, dikey, köşegen yönlerde korelasyon dağılımını gösteren diyagramlar da yalın ve şifreli görüntülerin korelasyon dağılımı hakkında bilgi vermektedir.

Çizelge 4.6'da 256x256 boyutunda gri – renk seviyesindeki görüntüler için korelasyon katsayısı bilgileri verilmiştir.

Çizelge 4.7, Çizelge 4.8 ve Çizelge 4.9'da ise verilen 256x256 boyutundaki renkli görüntülerin sırasıyla kırmızı, yeşil ve mavi renk kanallarına ait korelasyon katsayısı bilgileri verilmiştir.

Çizelgelerden de görüldüğü gibi yalın görüntülerde korelasyon katsayıları 1'e oldukça yakınken, şifrelenmiş görüntülerde bu değer oldukça düşmekte ve sıfıra yaklaşmaktadır. Böylece, birbirinin komşuluğunda bulunan pikseller arasında bir ilişki kurma ihtimali de gittikçe azalmaktadır.

Çizelge 4.6. Gri – renk seviyesindeki görüntüler için korelasyon katsayısı bilgileri.

Görüntü Dosyası	Yalın Görüntü			Şifrelenmiş Görüntü		
	Yatay	**Dikey**	**Köşegen**	**Yatay**	**Dikey**	**Köşegen**
Airport	0.8745	0.8148	0.7407	0.0033	7.727e-04	0.0010
Barbara	0.9634	0.9457	0.9109	0.0079	0.0056	8.2582e-04
Cameraman	0.9593	0.9335	0.8947	-5.0917e-04	0.0117	-0.0052
Chemical Plant	0.8992	0.9468	0.8417	0.0025	0.0054	-0.0053
Clock	0.9741	0.9566	0.9074	-0.0035	0.0047	-0.0013
Couple	0.8890	0.9302	0.7993	0.0027	6.8798e-04	-0.0067
Lena	0.9728	0.9459	0.8939	0.0072	0.0033	0.0051
Man	0.9541	0.9405	0.8994	-7.5612e-04	0.0094	0.0041
Moon Surface	0.9392	0.9026	0.8252	0.0019	0.0070	-0.0037
Test-pattern	0.9134	0.8941	0.8193	0.0082	0.0070	-0.0052

Çizelge 4.7. Verilen renkli görüntülerin kırmızı renk kanalına ait çeşitli yönlerde korelasyon katsayısı bilgileri.

Görüntü Dosyası	Yalın Görüntü			Şifrelenmiş Görüntü		
	Yatay	**Dikey**	**Köşegen**	**Yatay**	**Dikey**	**Köşegen**
Airplane	0.9258	0.9390	0.8319	-0.0014	0.0046	0.0010
House	0.9355	0.9672	0.8553	0.0034	0.0035	0.0035
Lena	0.8927	0.8780	0.8135	0.0030	0.0076	0.0011
Mandrill	0.9220	0.9475	0.8947	4.2760e-04	-0.0020	-0.0012
Peppers	0.9358	0.9398	0.9210	-0.0021	0.0081	6.6007e-05

Çizelge 4.8. Verilen renkli görüntülerin yeşil renk kanalına ait çeşitli yönlerde korelasyon katsayısı bilgileri.

Görüntü Dosyası	**Yalın Görüntü**			**Şifrelenmiş Görüntü**		
	Yatay	**Dikey**	**Köşegen**	**Yatay**	**Dikey**	**Köşegen**
Airplane	0.9345	0.9324	0.8386	0.0057	-0.0013	0.0034
House	0.9476	0.9806	0.9149	0.0029	0.0038	-0.0051
Lena	0.8948	0.8737	0.8345	6.5775e-04	0.0045	-6.0958e-04
Mandrill	0.8401	0.8729	0.7804	0.0031	0.0030	0.0082
Peppers	0.9022	0.9080	0.8861	-0.0042	0.0060	0.0038

Çizelge 4.9. Verilen renkli görüntülerin mavi renk kanalına ait çeşitli yönlerde korelasyon katsayısı bilgileri.

Görüntü Dosyası	**Yalın Görüntü**			**Şifrelenmiş Görüntü**		
	Yatay	**Dikey**	**Köşegen**	**Yatay**	**Dikey**	**Köşegen**
Airplane	0.9126	0.9503	0.7977	0.0116	0.0053	-0.0055
House	0.9750	0.9821	0.9464	0.0126	-7.3188e-04	-0.0013
Lena	0.7898	0.7747	0.7229	0.0028	0.0096	0.0028
Mandrill	0.9146	0.9217	0.8718	-0.0020	0.0040	-0.0017
Peppers	0.8659	0.8755	0.8374	0.0053	0.0060	-0.0037

4.3.6. Entropi analizi

Entropi, belirsizliği ölçmenin bir yoludur. Entropinin yüksek olması, belirsizliğin de yüksek olduğu anlamına gelir. Şifreli bir görüntüde ise, entropinin yüksek olması piksellerin dağılımının yüksek oranda rasgele olduğunu gösterir. Bir görüntü için entropi aşağıdaki formülle hesaplanır.

$$H(m) = \sum_{i=0}^{K} p(x_i) \log_2 \left(\frac{1}{p(x_i)}\right) \tag{40}$$

Eş. 40'da K görüntüdeki toplam piksel sayısını, $p(x_i)$ ise i. konumda bulunan x_i pikselinin olasılığını göstermektedir.

Gri renk seviyesindeki bir görüntü için 2^8 muhtemel değer söz konusudur. Teorik hesaplamada entropinin maksimum değeri 8'dir. Bu ise, tüm piksellerin dağılımının eşit olduğunu, başka bir deyişle tüm piksellerin aynı olasılık değerine eşit olduğunu gösterir. Bu yüzden güvenilir bir şifreleme algoritmasından beklenen, entropinin mümkün olduğunca 8'e yakın olmasıdır.

Çizelge 4.10 ve Çizelge 4.11 256x256 boyutunda gri renk seviyeli ve renkli görüntüler için entropi değerlerini göstermektedir. Çizelgelerde görüldüğü gibi şifrelenmiş görüntülerin entropi değerleri 8'e oldukça yakındır. Entropinin 8'e yakın olması piksellerin dağılımının oldukça rasgele olduğunu göstermektedir.

Çizelge 4.10. Gri renk seviyeli yalın ve şifrelenmiş görüntüler için entropi değerleri.

Görüntü Dosyası	**Yalın Görüntü**	**Şifrelenmiş Görüntü**
Airport	6.6955	7.9965
Barbara	7.5839	7.9969
Cameraman	7.0097	7.9971
Chemical Plant	7.3424	7.9974
Clock	6.7057	7.9976
Couple	7.1720	7.9972
Man	7.5360	7.9975
Moon Surface	6.7093	7.9971
Lena	7.4311	7.9972
Test-pattern	5.6618	7.9973
Ortalama	**6.9847**	**7.9972**

Çizelge 4.11. Yalın ve şifrelenmiş renkli görüntüler için entropi değerleri.

Görüntü Dosyası	Yalın Görüntü			Şifrelenmiş Görüntü		
	Kırmızı	**Yeşil**	**Mavi**	**Kırmızı**	**Yeşil**	**Mavi**
Airplane	6.7259	6.8248	6.2062	7.9970	7.9975	7.9969
House	7.4021	7.2304	7.4274	7.9972	7.9972	7.9972
Lena	7.2418	7.5767	6.9171	7.9973	7.9968	7.9970
Mandrill	7.6051	7.3574	7.6662	7.9973	7.9973	7.9971
Peppers	7.1801	7.0145	6.8002	7.9967	7.9973	7.9968
Ortalama	**7.2310**	**7.2008**	**7.0034**	**7.9971**	**7.9972**	**7.9970**

4.3.7. Şifreleme süresi

Şifreleme süresi, esnek ve kullanışlı bir şifreleme sistemi için önemli bir etkendir. Önerilen şifreleme yöntemi gerçek zamanlı uygulamalarda kullanılabileceği için, güvenilir olmasının yanında sistemin aynı zamanda hızlı olması tercih edilen özellikler arasındadır.

Şifreleme ve şifre çözme süresi Matlab' deki 'tic' ve 'toc' komutlarıyla hesaplanmıştır. Materyal kısmında belirtildiği gibi, çalışmalar Intel i7 işlemciye sahip, Windows 10 işletim sistemi kurulu olan 64 bitlik dizüstü bilgisayarda Matlab 2013 ortamında gerçekleştirilmiştir. Şüphesiz ki, kullanılan donanımın ve yazılımın özellikleri hızı etkileyen en önemli faktörlerdendir.

Çizelge 4.12'de farklı boyutlarda çeşitli görüntüler için şifreleme süreleri verilmiştir.

Çizelge 4.12. Farklı boyutlardaki çeşitli gri renk seviyeli ve renkli görüntüler için şifreleme süresi.

Görüntü Dosyası	Görüntü Boyutu	Şifreleme Süresi(s)
Clock (5.1.12)	128x128	0.0527
	256x256	0.0723
	512x512	0.1332
	1024x1024	0.4004
Airplane (4.2.05)	128x128x3	0.5997
	256x256x3	0.5211
	512x512x3	0.6754
	1024x1024x3	1.3832

5. SONUÇLAR VE ÖNERİLER

Bu tezde yer değiştirme ve yerine koyma metotları kullanılarak bir görüntü şifreleme algoritması geliştirilmiştir. Yer değiştirme işlemleri için Ikeda kaotik haritası, yerine koyma işlemi için de Henon kaotik haritası kullanılmıştır. Algoritmadaki işlem sırası; yer değiştirme, yerine koyma ve tekrar yer değiştirme şeklindedir. Önemli noktalardan biri şifreleme işlemi sadece bir tur sonucunda gerçekleştirilmiştir. Ayrıca, yer değiştirme ve yerine koyma işlemlerinde kullanılan haritaların yeri değiştirildiğinde, geliştirilen algoritmadaki sonuçlara nazaran daha iyi sonuçlar elde edilmediği de gözlenmiştir. Algoritmanın güvenlik analizi için histogram ve entropi analizi, anahtar hassasiyeti testi ve korelasyon analizi yapılarak, şifreleme süresi ve anahtar uzayı büyüklüğü de belirlenmiştir. Şifreleme ve şifre çözme süresi Matlab komutlarının daha etkili kullanımıyla azaltılabilir. Verilen sonuçlar, Ikeda ve Henon kaotik haritalarının belirtildiği şekilde kullanımının görüntü şifreleme için güvenilir bir yol olduğunu ortaya koymaktadır.

Önerilen şifreleme yönteminin gerçek zamanlı uygulaması da büyük önem taşımaktadır. Bu yüzden şifrelenmiş görüntünün çeşitli modülasyon teknikleri kullanılarak gürültülü bir kanal üzerinden gönderilip alıcı tarafta tekrar elde edilmesi ve algoritmanın FPGA gibi bir mikroişlemci üzerinde denenmesi planlanmaktadır.

KAYNAKLAR

Akhshani, A., Akhavan, A., Lim, S.-C., Hassan, Z., 2012. An image encryption scheme based on quantum logistic map. ***Commun. Nonlinear Sci. Numer. Simul***., **17**(12): 4653–4661.

Alvarez, G., Li, S., 2006. Some basic cryptographic requirements for chaos-based cryptosystems , ***Int. J. Bifurc. Chaos***, **16**(8): 2129–2151.

Awad, A., Awad, D., 2010. Efficient image chaotic encryption algorithm with no propagation error. ***ETRI J.***, 32(5): 774–783.

Awad, A., Saadane, A., 2010. Efficient chaotic permutations for image encryption algorithms. ***Proc. World Congr. Eng.***, 30 Haziran – 2 Temmuz, Londra.

Behnia, S., Akhavan, A., Akhshani, A., Samsudin, A., 2013. Image encryption based on the Jacobian elliptic maps. ***J. Syst. Softw***., **86**(9): 2429–2438.

Belazi, A., El Latif, A. A. A., Belghith, S., 2016. A novel image encryption scheme based on substitution-permutation network and chaos. ***Signal Processing***, **128**: 155–170.

Biham, E., 1991. Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91**.** ***Proceedings Advances in Cryptology***, 532 – 534.

Cao, Y., 2013. A new hybrid chaotic map and its application on image encryption and hiding. ***Mathematical Problems in Engineering***, **2013**: 1 – 13.

Chen, G., Mao, Y., Chui, C. K., 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. ***Chaos, Solitons and Fractals***, **21**(3): 749–761.

Dachselt, F., Schwarz, W. 2001. Chaos and cryptography. ***IEEE Trans. Circuits Syst. I Fundam. Theory Appl***., **48**(12): 1498–1509.

El Assad, S., Farajallah, M., 2016. A new chaos-based image encryption system. ***Signal Process. Image Commun.***, **41**: 144–157.

El Assad, S., Noura, H. ***Generator of Chaotic Sequences and Corresponding Generating System***. wO Patent 2,011,121,218 Ekim 7, 2011.

El-Latif, a. A. A., Li, L., Wang, N. Han, Q., Niu, X., 2013. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. ***Signal Processing***, **93**(11): 2986–3000.

François, M. Grosges, T., Barchiesi, D., Erra, R., 2012. A new image encryption scheme based on a chaotic function. ***Signal Process. Image Communication***., **27**(3): 249–259.

Fridrich, J., 1998. Symmetric ciphers based on two-dimensional chaotic maps. ***Int. J. Bifurc. Chaos***, **8**(6) : 1259 – 1284.

Gonzalez, R. C., Woods, R. E., Eddins, S. L., 2009. ***Digital Image Processing Using Matlab***, Gatesmark Publishing, USA.94.

Habutsu, T., Nishio,Y., Sasase, I., Mori, S., 1991. A secret key cryptosystem by iterating a chaotic Map. ***Advances in Cryptology— EUROCRYPT '91*,547**:127-140.

Hanchinamani, G., Kulakarni, L., 2014. Image encryption based on 2-D Zaslavskii chaotic map and Pseudo Hadmard transform. ***International Journal of Hybrid Information Technology***, **7**(4): 185 – 200.

Hilewitz, Y., Shi, Z., Lee, R., 2004. Comparing fast implementations of bit permutation instructions. ***Signals, Syst.and Computers***. 7 – 10 Kasım, USA. 1856 – 1863.

Hua, Z., Zhou, Y., Pun, C. M., Chen, C. L. P., 2015. 2D Sine Logistic modulation map for image encryption. ***Information Sciences***, **297**: 80–94.

Hussain, I., Shah, T., Gondal, M. A., Mahmood, H., 2013. An efficient approach for the construction of LFT S-boxes using chaotic logistic map. ***Nonlinear Dyamics***, **71**: 133–140.

Ikeda, K., 1979. Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. ***Opt. Commun***., **30** (2): 257–261.

Jacimoski, G., Kocarev, L., 2001. Chaos and cryptography: Block encryption ciphers based on chaotic maps. ***IEEE Trans. Circuits Syst. I Fundam. Theory Appl***., **48**(2): 163 – 169.

Jiu, C., F., Chi, K., T., 2008. Chaos and Communications, Chap. 1, ***Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications***. World Scientific & Tsinghua University Press, Singapore.1.

Katz, J., Lindell, Y., 2015. Private Key Encryption, Chap. 3, ***Introduction to Modern Cryptography*** (Editor: Douglas R. Stinson). Chapman & Hall / CRC, USA. 43.

Khanzadi, H., Eshghi, M., Borujeni, S. E., 2014. Image encryption using random bit sequence based on chaotic maps. ***Arab. J. Sci. Eng.***, **39**(2): 1039–1047.

Kocarev, L., 2001. Cryptography : A brief overview. ***Circuits Syst. Mag. IEEE***, **1**(3): 6–21.

Korrochano, E., B., 2005. Chaos-Based Image Encryption, Chap. 8, ***Handbook of Geometric Computing***. Springer-Verlag Berlin Heidelberg, Germany. 231.

Lee, R. B., Shi, Z., Yang, X., 2001. Efficient permutation instructions for fast software cryptography. ***IEEE Micro***, **21**(6): 56–69.

Li, P., Li, Z., Halang, W. A., Chen, G., 2006. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. ***Phys. Lett. Sect. A Gen. At. Solid State Phys.***, **349**(6): 467–473.

Li, S., Chen, G., Cheung, A., Bhargava, B., Lo, K.-T., 2007. On the design of perceptual mpeg-video encryption algorithms. ***IEEE Transactions On Circuits And Systems for Video Technology***, **17**(2): 214 – 223.

Liu, H., Li, J., 2013. Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map. ***IET Information Security***., 7(4): 265–270.

Liu, L., Zhang, Q., Wei, X., 2012. A RGB image encryption algorithm based on DNA encoding and chaos map. ***Comput. Electr. Eng.***, **38**(5): 1240–1248.

Liu, Y., 2014. Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. ***Opt. Laser Technol***. **60**: 111 – 115.

Liu, Q., Li, P.-Y., Zhang, M.-C., Sui, Y.-X., Yang, H.-J., 2015. A novel image encryption algorithm based on chaos maps with Markov properties. ***Neurocomputing***, **169**(2): 150–157.

Lorenz, E., N., 1963. Deterministic non-periodic flow. ***Journal of Atmospheric Sciences***, **20**: 130 – 141.

Masuda, N., Jakimoski, G., Aihara, K., Kocarev, L., 2006. Chaotic block ciphers: From theory to practical algorithms. ***IEEE Trans. Circuits Syst. I Regul. Pap.***, **53**(6): 1341–1352.

Murillo-Escobar, M. A., Cruz-Hernandez, C. ,Abundiz-Perez, F., Lopez-Gutierrez, R. M., Acosta Del Campo, O. R., 2015. A RGB image encryption algorithm based on total plain image characteristics and chaos. ***Signal Processing***, **109**: 119–131.

Norouzi, B., Mirzakuchaki, S., 2014. A fast color image encryption algorithm based on hyper-chaotic systems. ***Nonlinear Dyamics***., **78**(2): 995–1015.

Pareek, N. K., Patidar, V., Sud, K. K., 2006. Image encryption using chaotic logistic map. ***Image Vis. Comput***., **24**(9): 926–934.

Patidar, V., Pareek, N. K. , Purohit, G., Sud, K. K., 2010. Modified substitution-diffusion image cipher using chaotic standard and logistic maps. ***Commun. Nonlinear Sci. Numer. Simul.,*** **15**(10): 2755–2765.

Petrisor, E. 2003. Entry and exit sets in the dynamics of area preserving Henon map. ***Chaos, Solitons and Fractals***, **17**(4): 651–658.

Pichler, F., Scharinger, J., 1994. Ciphering by Bernoulli shifts in finite Abelian groups. ***Contrib. to Gen. Algebr.***:465 – 476.

Ponnain, D., Chandranbabu, K., 2016. Crypt analysis of an image encryption algorithm and an enhanced scheme. ***Optik*** **127**(1): 192–199.

Sathishkumar, G. A., Bagan, D. K. B., Sriraam, D. N., 2011. Image encryption based on diffusion and multiple chaotic maps. ***International Journal of Network Security &Its Applications***, **3**(2): 181 – 194.

Shannon, C., E., 1949. Communication theory of secrecy systems. ***Bell System Technical Journal***, **28**(4): 656 – 715.

Shi, Z. S. Z. , Lee, R. B., 2000. Bit permutation instructions for accelerating software cryptography. ***Proc. IEEE Int. Conf. Appl. Syst. Archit. Process***. 138–148.

Smart, N., 2003. Block Ciphers, Chap. 8, ***Cryptography: An Introduction***. Mcgraw-Hill College, England.123.

Socek, D., Li, S., Magliveras, S. S., Furht, B., 2005. Enhanced 1-D chaotic key-based algorithm for image encryption. ***SECURECOMM '05 Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks.*** 5 – 9 Eylül, Washington. 406 – 408.

Stoyanov, B., Kordov, K., 2014. Novel image encryption scheme based on Chebyshev Polynomial and Duffing Map. ***The Scientific World Journal***, **2014**: 1 – 11.

Tong, X.-J., 2013. Design of an image encryption scheme based on a multiple chaotic map. ***Commun. Nonlinear Sci. Numer. Simul***., **18**(7): 1725–1733.

Tong, X. J., Zhang, M., Wang, Z., Liu, Y., Xu, H., Ma, J., 2015. A fast encryption algorithm of color image based on four-dimensional chaotic system. ***Journal of Visual Communication and Image Representation***, **33**: 219–234.

Wang, B., Xie, Y., Zhou, C., Zhou, S., Zheng, X., 2016. Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps. ***Optik***, **127**(7): 3541–3545.

Wei-bin, C. W. C., Xin, Z. X. Z., 2009. Image encryption algorithm based on Henon chaotic system, ***Int. Conf. Image Anal. Signal Process***., 2–5.

Wu, Y., Noonan, J. P., Agaian, S. 2011. NPCR and UACI randomness tests for image encryption, ***Journal of Selected Areas in Telecommunications (JSAT):***31 – 38.

Wong, K.-W., Kwok, B. S. H., 2010. A fast image encryption scheme based on a nonlinear chaotic map. ***ICSPS 2010 - Proc. 2010 2nd Int. Conf. Signal Process. Systems***. 5 – 7 Temmuz, Çin. 326 – 330.

Xiang, T., Liao, X., Tang, G., Chen, Y., Wong, K. W., 2006. A novel block cryptosystem based on iterating a chaotic map. ***Phys. Lett. Sect. A Gen. At. Solid State Phys.***, **349**(2006): 109–115.

Xu, L., Li, Z., Li, J., Hua, W., 2016. A novel bit-level image encryption algorithm based on chaotic maps. ***Opt. Lasers Eng.***, **78**: 17–25.

Yang, D., Liao, X., Wang, Y., Yang, H., Wei, P., 2009. A novel chaotic block cryptosystem based on iterating map with output-feedback. ***Chaos, Solitons and Fractals***, **41**(1): 505–510.

Yang, H., Wong, K.-W., Liao, X., Zhang, W., Wei, P., 2010. A fast image encryption and authentication scheme based on chaotic maps. ***Commun. Nonlinear Sci. Numer. Simul.***, **15**(11): 3507–3517.

Zhang, D., Zhang, F., 2014. Chaotic encryption and decryption of JPEG image. ***Optik***, **125**(2): 717–720.

Zhou, Y., Bao, L., Chen, C. L. P., 2013. Image encryption using a new parametric switching chaotic system. ***Signal Processing***, **93**(11): 3039–3052.

Zhou, Y., Bao, L., Chen, C. L. P., 2014. A new 1D chaotic system for image encryption. ***Signal Processing***, **97**: 172–182.

Zhou, Y., Cao, W., Chen, C. L. P., 2014. Image encryption using binary bitplane. ***Signal Processing***, **100**: 197–207.

ÖZGEÇMİŞ

1990 yılında Iğdır'da dünyaya geldi. Orta öğretimi Atatürk İÖO'nda ve liseyi Tuzluca Yüzüncü Yıl Lisesi'nde tamamladı. 2008 yılında başladığı Mersin Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'nü 2013 yılında birincilikle tamamladı. Aynı sene Ege Üniversitesi Fen Bilimleri Enstitüsü'nde yüksek lisansa başladı. 2014'te Yüzüncü Yıl Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'ne araştırma görevlisi olarak atanmasının ardından Dokuz Eylül Üniversitesi'ne altı aylık dil eğitimine gitti. Şu anda Yüzüncü Yıl Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'nde araştırma görevlisi olarak çalışmaktadır.

YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
LİSANSÜSTÜ TEZ ORİJİNALLİK RAPORU

Tarih: 02.08.2017

Tez Başlığı / Konusu:

Ikeda ve Henon Kaotik Haritaları Kullanarak Görüntü Şifreleme

Yukarıda başlığı/konusu belirlenen tez çalışmamın kapak sayfası, giriş, ana bölümler ve sonuç bölümlerinden oluşan toplam 92 sayfalık kısmına ilişkin, 02.08.2017 tarihinde şahsım tarafından 'iThenticate' intihal tespit programından aşağıda belirtilen filtreleme uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 5 (beş)'tir.

Uygulanan filtreler aşağıda verilmiştir:
- Kabul ve onay sayfası hariç,
- Teşekkür hariç,
- İçindekiler hariç,
- Simge ve kısaltmalar hariç,
- Gereç ve yöntemler hariç,
- Kaynakça hariç,
- Alıntılar hariç,
- Tezden çıkan yayınlar hariç,
- 7 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit inatch size to 7 words)

Yüzüncü Yıl Üniversitesi Lisansüstü Tez Orijinallik Raporu Alınması ve Kullanılmasına İlişkin Yönergeyi inceledim ve bu yönergede belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim. 02.08.2017

Yeter ŞEKERTEKİN

Adı Soyadı: Yeter ŞEKERTEKİN

Öğrenci No:159101020

Anabilim Dalı: Elektronik

Programı: Yüksek Lisans

Statüsü: ■ Y. Lisans Doktora □

DANIŞMAN ONAYI
UYGUNDUR

Yrd. Doç. Dr. Özkan ATAN

ENSTİTÜ ONAYI
UYGUNDUR