T.C.

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ÇOK-BOYUTLU KAOTİK SİSTEMLERE DAYALI RENKLI GÖRÜNTÜ ŞİFRELEME YÖNTEMİ

YÜKSEL LİSANS TEZİ

MİR MOHAMMAD REZA ALAVİ MİLANİ

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ SALİM CEYHAN

BİLECİK, 2022

10497759

T.C.

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ÇOK-BOYUTLU KAOTİK SİSTEMLERE DAYALI RENKLI GÖRÜNTÜ ŞİFRELEME YÖNTEMİ

YÜKSEL LİSANS TEZİ

MİR MOHAMMAD REZA ALAVİ MİLANİ

TEZ DANIŞMANI

Dr. ÖĞR. ÜYESİ SALİM CEYHAN

BİLECİK, 2022

10497759

BEYAN

"*Çok-Boyutlu Kaotik Sistemlere Dayalı Renkli Görüntü Şifreleme Yöntemi*" adlı yüksek lisans tezinin hazırlık ve yazımı sırasında bilimsel araştırma ve etik kurallarına uyduğumu, başkalarının eserlerinden yararlandığım bölümlerde bilimsel kurallara uygun olarak atıfta bulunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, tezin herhangi bir kısmının Bilecik Şeyh Edebali Üniversitesi veya başka bir üniversitede başka bir tez çalışması olarak sunulmadığını, aksinin tespit edileceği muhtemel durumlarda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

<table>
<tr><td colspan="4">Bu çalışmanın,
Bilimsel Araştırma Projeleri (BAP), TÜBİTAK veya benzeri kuruluşlarca desteklenmesi durumunda; projenin ve destekleyen kurumun adı proje numarası ile birlikte, ETİK KURUL onayı alınması durumunda ise ETİK KURUL tarih karar ve sayı bilgilerinin beyan edilmesi gerekmektedir.</td></tr>
<tr><td>DESTEK ALINMIŞTIR</td><td></td><td>DESTEK ALINMAMIŞTIR</td><td>X</td></tr>
<tr><td colspan="4">Destek alındı ise;</td></tr>
<tr><td colspan="4">Destekleyen kurum;</td></tr>
<tr><td colspan="3">Desteğin Türü</td><td>Proje Numarası</td></tr>
<tr><td colspan="3">1- BAP (Bilimsel Araştırma Projesi)</td><td rowspan="3"></td></tr>
<tr><td colspan="3">2- TÜBİTAK</td></tr>
<tr><td colspan="3">Diğer; ……</td></tr>
<tr><td colspan="4">ETİK KURUL onayı var ise;</td></tr>
<tr><td colspan="3">ETİK KURUL karar tarih/sayı:</td><td>……/……</td></tr>
</table>

Mir Mohammad Reza Alavi Milani

.. /.. /2022

İmza

…….....

ÖNSÖZ

Tezimi hazırlarken bilgisi ve tavsiyeleriyle beni yönlendiren sayın Dr. Öğr. Üyesi Salim CEYHAN' a ve destekleriyle yanımda olan aileme teşekkürü bir borç bilirim.

Tüm bu çalışmalar süresince bana varlıkları ile destek ve moral veren, yoğun çalışmalarım boyunca sabır gösteren ve motivasyon desteği olan eşime her daim yanımda oldukları için teşekkürlerimi sunarım.

Mir Mohammad Reza Alavi Milani

2022

ÖZET

ÇOK-BOYUTLU KAOTİK SİSTEMLERE DAYALI RENKLI GÖRÜNTÜ ŞİFRELEME YÖNTEMİ

Bilişim teknolojilerinin gelişmesi ve internette yayınlanan verilere yetkisiz erişim olasılığının artmasıyla birlikte verilerin korunması ihtiyacı önemli bir konu haline gelmiştir. Veri güvenliğinde faydalı olabilecek yöntemlerden biri şifrelemedir. Veri şifreleme kullanılarak, veriler farklı ortamlarda güvenli bir şekilde kolayca dağıtılabilir. Bu tez, dijital görüntüler için kaos teorisine dayalı bir şifreleme yöntemini sunmakta ve incelemektedir. Şifrelenmiş görüntüler üzerinde yapılan testler ve analizler, sunulan yöntemin gerekli verimliliğe sahip olduğunu göstermektedir. Şifreleme, bilgileri yalnızca yetkili kişilerin anlayabileceği şekilde düzenleme yöntemidir. Teknik olarak bu, düz metni şifreli metne dönüştürme işlemidir. Daha basit bir ifadeyle, şifreleme, okunabilir verileri alır ve anlaşılmaz ve rastgele görünecek şekilde değiştirir. Şifreleme, bu işlemi gerçekleştirmek için bir şifreleme anahtarının kullanılmasını gerektirir. Bu anahtar, şifreli mesajın hem göndericisinin hem de alıcısının bildiği bir dizi matematiksel değerdir. Şifrelenmiş veriler rastgele gibi görünse de şifreleme mantıksal ve öngörülebilir bir şekilde yapılır, öyle ki şifrelenmiş verilere sahip olan ve verileri şifrelemek için kullanılan anahtara sahip olan taraf, verilerin şifresini çözebilir ve düz metne dönüştürebilir. Ancak güvenli bir şifreleme, üçüncü bir tarafın tahmin edemeyeceği veya şifrelenmiş metni çeşitli araçlar kullanarak düz metne dönüştüremeyeceği kadar karmaşık olmalıdır. Bu tezde, görüntü şifreleme için etkin bir yöntem önerilmiştir. Uygulamadan sonra önerilen yöntem, veri güvenliği analizi için var olan çeşitli araçlarla değerlendirilmiştir. Sonuçlar, önerilen yöntemin görüntü şifreleme için kabul edilebilir olduğunu göstermektedir.

Anahtar Kelimeler: Görüntü Şifreleme, Kaotik harita, Rastgele sayı, Baker haritası.

ABSTRACT

COLOR IMAGE ENCRIPTION METHOD BASED ON MULTI-DIMENTIONAL CHAOTIC SYSTEMS

With the development of information technologies and the increase in the possibility of unauthorized access to data published on the Internet, the need for data protection has become an important issue. One of the methods that can be useful in data security is encryption. By encryption, data can be easily distributed securely in different environments. This article presents and examines a chaos theory-based encryption method for digital images. Tests and analysis on encrypted images show that the presented method has the necessary efficiency. Encryption is a method of organizing information in such a way that only authorized persons can understand it. Technically, this is the process of converting plain text to ciphertext. In simpler terms, encryption takes readable data and changes it to appear incomprehensible and random. Encryption requires the use of an encryption key to perform this operation. This key is a set of mathematical values known to both the sender and receiver of the encrypted message. Although encrypted data may seem random, encryption is done logically and predictable so that the party that owns the encrypted data and owns the key used to encrypt the data can decrypt the data and convert it to plain text. However, secure encryption must be so complex that a third party cannot guess or convert the ciphertext to plain text using various tools. In this thesis, an efficient method for image encryption is proposed. After the application, the proposed method was evaluated with various tools available for data security analysis. The results show that the proposed method is acceptable for image encryption.

Keywords*:* Image Encryption, Chaotic map, Random number, Baker map.

İÇİNDEKİLER

Sayfa No

ŞEKİLLER LİSTESİ

Sayfa No

TABLOLAR LİSTESİ

Sayfa No

LİST DİZİNİ

Sayfa No

SİMGELER VE KISALTMALAR LİSTESİ

Simgeler

r : Lojistik harita sistem katsayısı

X_n : Lojistik harita sistem değişkeni

n : Lojistik harita yineleme sayısı

α : Baker harita kontrol parametresi

b : İyileştirilmiş Baker harita lineer katsayısı

$k_{i,j}$: i. karaktere ve j. bitine karşılık gelen ikili bit

x_0 : Başlangıç ilk değer

y_0 : Başlangıç ikinci değer

M : Görüntünün uzunluğu

N : Görüntünün genişliğini

P(i, j) : Görüntünün bir piksel değeri

Kısaltmalar

RNG : Rastgele Sayı Üreticisi

FIPS : Federal Bilgi İşleme Standardı

AES : Gelişmiş Şifreleme Standardı

DES : Veri Şifreleme Standardı

IDEA : Uluslararası Veri Şifreleme Algoritması

PGP : Oldukça İyi Gizlilik

RSA : Rivest–Shamir–Adleman

SSL : Güvenli Yuva Katmanı

WIFI : Kablosuz Sadakat

WEP : Kablolu Eşdeğer Gizlilik

DNA : Deoksiribo nükleik asit

ASCII : Bilgi Değişimi için Amerikan Standart Kodu

RGB : Kırmızı – Yeşil – Mavi

NPCR : Değişen piksel hızı sayısı

UACI : Birleşik ortalama değiştirilmiş yoğunluk

1. GİRİŞ

İnsanların verileri çeşitli iletişim kanallarında paylaştığı birçok bağlam vardır. Genellikle kamuya açık olan farklı ortamlarda veri yayınlamak güvenli olmayabilir ve güvenlik riskleri getirebilir (Chen vd., 2019: 97549) (Dou vd., 2020:8). Bu amaçla veri iletimini güvenli hale getirmek için çeşitli yöntemler geliştirilmiştir. Veri iletimini güvenli hale getirmenin yollarından biri veri şifrelemedir. Veri şifreleme kullanılarak farklı ortamlarda daha kolay yayınlanabilirler. Elbette veri şifreleme, verileri yetkisiz erişimden korumak için steganografi ve filigranlama gibi farklı şekillerde yapılabilir (Morkel vd., 2005:3) (Subramanian vd., 2021: 23410) (Wadhera vd., 2022:127) (Mahto vd., 2021:2). Veri şifreleme farklı yol ve yöntemlerle araştırılmıştır. Bazı şifreleme yöntemleri geleneksel yöntemlere dayalıdır (Arab vd., 2019:6666) ve bazıları modern yöntemler (Anandkumar vd., 2020:25) kullanmıştır. Metinsel veriler (Singh vd., 2015:75) (Sangwan vd., 2012:29), bazıları görüntü verileri (Liu vd., 2014:328) (Hua vd., 2019:411) ve bazıları ses verileri (Lima vd., 2016:8405) için bazı şifreleme yöntemleri önerilmiştir.

Bu arada görüntülerin şifrelenmesi, multimedya programlarında görüntülerin güvenliği için önemli bir rol oynayan ve multimedya verilerinin güvenli iletimi için iletişim alanında var olan endişeleri çözebilecek en önemli konulardan biridir (Hasimoto-Beltrán, 2008:3). Görüntü şifrelemeyi diğer şifrelemelerden ayıran özellikler, veriler, yüksek uyumluluk ve yüksek görüntü verisi fazlalığı arasında güçlü bir bağıntıdır. Ayrıca görüntüler, metinsel verilere göre daha yüksek veri hacmine sahiptir (Darwish vd., 2018:294). Sayısal görüntülerin özelliklerine göre, AES veya DES gibi geleneksel yöntemlerin kullanılması, bu yöntemler düşük hız ve küçük anahtar alanı içerdiğinden verimli olamamaktadır (Wang vd., 2010: 615). Bu nedenle görüntü şifreleme için çeşitli ve daha modern yöntemler önerilmiştir (Abd-El-Atty vd., 2021:2) (Yan vd., 2021: 10952).

Görüntü şifreleme için etkili yöntemler arasında kaotik sistemlerin kullanılması yer almaktadır. Kaotik sistemler, sözde rasgele sayılar üretmede çok verimli olabilen ve görüntü şifrelemede kullanılabilen özelliklere sahiptir. Kaotik haritalamaların etkili özellikleri, başlangıç değerlerine karşı yüksek hassasiyetleri ve yüksek periyodik olmalarıdır. Kaos haritalarının özellikleri, rastgele özelliklere ve yüksek hıza sahip sözde rasgele sayılar üretmeyi mümkün kılar. Birçok çalışma, kaotik fonksiyonların görüntü şifreleme için çok etkili olabileceğini göstermiştir (Suneja vd., 2019:698) (Kumar vd., 2020:3) (Gu vd., 2006:493).

Bununla birlikte, tek boyutlu ve çok boyutlu olmak üzere iki kaotik sistem kategorisi önerilmiştir. Tek boyutlu kaotik fonksiyonlar daha basit bir yapıya sahiptir ve daha kolay ve çok daha yüksek hızda yürütülür (Talhaoui vd., 2021:13). Bununla birlikte, Tek boyutlu kaotik fonksiyonlar, yaygın olarak tartışıldığı ve üzerlerinde birçok çalışma yapıldığı için güvenlik açısından biraz daha az güvenilirdir (Norouzi vd., 2015:782). Elbette çok boyutlu kaos fonksiyonları da aynı bakış açısıyla güvenilirliğini yitirmiştir. Son zamanlarda kaos fonksiyonlarının güvenlik gücünü artırmaya yönelik çalışmalar yapılmaktadır (Liu vd., 2021:1101). Bu yazıda, daha yüksek bir güven derecesine sahip olduğu kanıtlanmış olan Baker haritası adı verilen bir kaos işlevinden geliştirilmiş özel bir işlev türü kullanacağız (Liu vd., 2017:7). Genellikle görüntü şifreleme sistemleri iki aşamada analiz edilir: anahtar oluşturma ve piksel şifreleme. Anahtar oluşturma aşamasında, bir dizi sözde rastgele veri oluşturulur ve bu aşamada kaotik eşlemeler kullanılır. Şifreleme aşamasında üretilen sözde rastgele veriler, görüntülerin piksel verileriyle karıştırılarak şifreleme işlemi ve şifreli görüntülerin üretilmesi gerçekleştirilir.

Bu tezde, rastgele sayılar dizisi oluşturmak için Baker haritası kaotik fonksiyonunu kullandık. Kriptografik işlemde üretilen rastgele veriler, tezin 3. bölümünde sunulan algoritmaya göre kullanılır. İkinci kısım kaos sistemlerini ve özellikle Baker harita fonksiyonunu tanıtmaktadır ve üçüncü kısımda önerilen algoritma tartışılacaktır. Dördüncü bölümde önerilen yöntem değerlendirilecektir.

2. KRİPTOLOJİ

2.1 Kriptografinin Tarihi

Şifreleme tekniklerini ilk kullananları incelerken, Sezar (Roma imparatoru) ve Müslüman bir bilim adamı olan Al-Kandi'yi buluyoruz. Elbette bunlar çok temel şifreleme yöntemlerini icat etmişler. Örneğin, tüm metinde alfabenin belirli bir miktarda harflerini hareket ettirerek, şifreleme yapılır ve yalnızca taşınan harflerin sayısını bilen biri orijinal metni çıkarabilirdi.

Başka bir ilke şifreleme yöntemi, belirli bir çapa sahip bir silindir üzerine bir kâğıt şeridi sarmak ve ardından mesajı sarılı kâğıda yazmaktı. Açıkçası, silindirin çapını bilmeden mesajı okumak çok zor olacak ve sadece silindirin aynı kopyalarına sahip olanlar mesajı okuyabilecek. 20. yüzyılda aynı yöntem, yüksek hızlı şifreleme için elektrik motorlarıyla birlikte kullanılıyordu. Bunun örnekleri Lorentz şifreleme makinesinde ve Almanya tarafından II. Dünya Savaşı'nda askeri mesajları şifrelemek için kullanılan Enigma şifreleme makinesinde görülebilir.

2.2 Kirkhofun Altı İlkesi

1883'te August Kirkhoff, "Askeri Kriptografi" başlıklı iki makale yayınladı. Bu iki makalede, şifreleme kurallarından biri olarak, ikinci ilkesi bilim adamları tarafından gelişmiş kriptografide hala kullanılan altı temel ilke vardı:

- Şifreleme sistemi teoride olmasa da pratikte kırılmaz.
- Şifreleme sistemi herhangi bir gizli veya gizli bilgi içermemelidir. Aksine, gizli olan tek şey şifre anahtarıdır.
- Şifre anahtarı, öncelikle kolayca değiştirilebilir ve ikinci olarak hatırlanabilir ve şifre anahtarının ezberlenmesine gerek kalmayacak şekilde seçilebilir olmalıdır.
- Şifreli metinler telgraf hatları üzerinden iletilebilir olmalıdır.
- Şifreleme cihazı veya şifrelenmiş belgeler bir kişi tarafından taşınabilir olmalıdır.
- Şifreleme sisteminin kurulumu kolay olmalıdır.

Bilgisayarların ortaya çıkması ve bilgi işlem güçlerinin artması ile kriptografi bilgisi bilgisayar bilimi alanına girmiş ve bu olgu kriptografi konularında üç önemli değişikliğe neden olmuştur:

1. Yüksek bilgi işlem gücünün varlığı, daha karmaşık ve etkili şifreleme yöntemleri oluşturmayı mümkün kıldı.
2. Esas olarak mesajları şifrelemek için kullanılan kriptografik yöntemler, yeni ve çok sayıda kullanım alanı buldu.
3. Zamana kadar, şifreleme esas olarak metin sel bilgiler üzerinde alfabeler kullanılarak yapılıyordu; ancak bilgisayarın gelişi, her türlü bilgi üzerinde ve bit bazında şifreleme yapılmasına neden oldu.

İnternetin benzeri görülmemiş genişlemesi ve büyümesi, insanların, kuruluşların ve kurumların yaşam ve çalışma faaliyetlerinde kapsamlı değişikliklere neden oldu. Bilgi güvenliği, tüzel ve gerçek kişilerin ortak sorunlarından biridir. Yetkisiz kişilerin hassas bilgilere erişiminin olmamasının sağlanması, bilgilerin İnternet'te dağıtılmasıyla ilgili en önemli güvenlik sorunlarından biridir. Başkaları tarafından görülmesini istemediğimiz hassas bilgiler pek çok şeyi içerir. Bu tür bilgilerden bazıları şunlardır:

- Kredi kartı bilgisi
- Forumlarda üyelik numaraları
- Özel bilgi
- Kişisel bilgi ayrıntıları
- Bir kuruluştaki hassas bilgiler
- Banka hesapları hakkında bilgi

2.3 Şifreleme Hizmeti

Genel olarak şifreleme hizmeti, şifreleme tekniklerine dayalı olarak elde edilen yetenek ve olasılığı ifade eder. Bilgisayarlar kriptografi alanına girmeden önce, kriptografinin kullanımı neredeyse mesajı şifrelemek ve içindeki verileri gizlemekle sınırlıydı. Ancak gelişmiş şifrelemede, aşağıdakiler de dahil olmak üzere çeşitli hizmetler sağlanır:

- **İçerik Gizliliği**: İletinin içeriğini gizlemenin ana ve birincil hizmeti olan, içeriği yalnızca yetkili kişilerin bilebileceği şekilde bilgi gönderilmesi veya saklanması.
- **İçerik Bütünlüğü**: Bilgilerin doğruluğunun sağlanması ve gönderim sırasında orijinal içeriğinin değiştirilmemesi anlamına gelir. Bilgilerin ilk içeriğinin değiştirilmesi kazara (gönderme yolundaki sorunlardan dolayı) veya kasıtlı olabilir.

- **İçerik Doğrulaması**: Bilgiyi gönderenin kimliğinin tanınması ve güvence altına alınması ve kişilerin kimliğinin tahrif edilmesinin imkansızlığı anlamına gelir.
- **İnkar edilemezlik**: Bilgiyi gönderen kişinin gelecekte onu göndermeyi veya içeriğini inkar edemeyeceği anlamına gelir.

2.4 Kriptografinin Temelleri

Bilindiği üzere bilgi güvenliğini artırmak için çeşitli şifreleme sistemleri oluşturulmuştur. Bütün bu sistemlerde iki temel ilke vardır ve bunlar çok önemlidir.

- **Artıklık (Redundancy)**

İlk ilke, tüm şifrelenmiş mesajların bir miktar fazlalık (yedek veri) içermesi gerektiğidir, diğer bir deyişle, gerçek bilgilerin şifrelenip olduğu gibi gönderilmesine gerek yoktur. Şifrelenmiş bir dize, kod çözüldükten sonra orijinal mesaja eşdeğer olmamalıdır; Bunun yerine, gereksiz ve hesaplanmış veriler içine gömülmelidir.

Daha iyi anlamak için, 55.000 ürüne sahip bir şirketin yeni siparişlerini e-posta sistemi aracılığıyla aldığını varsayalım. Firma programcıları, etkili ve verimli programlar yazdıklarını düşünerek, ürün sipariş mesajlarının 19 bayt olması gerektiğine karar verirler; 16 bayt müşteri adı ve ardından 3 bayt veri alanı (bir bayt ürün sayısı ve 2 bayt ürün numarası). Ayrıca son 3 baytın çok uzun bir anahtarla şifrelendiğini ve bu anahtarın sadece müşteri ve şirkette olduğunu düşünürler. İlk bakışta, bu plan güvenli görünebilir, çünkü pasif bir davetsiz birisi, bilgilerin şifresini hiçbir şekilde çözemez. Ama ne yazık ki bu mantıkta, pratikte onu kullanılmaz bir plana dönüştüren temel bir hata var.

Diyelim ki kin nedeniyle şirketten kovulan bir çalışan şirketten intikam almak isteyen biri ortaya çıktı. Bu amaçla şirketten ayrılmadan önce şirketin müşterilerinin bir listesini yanına alır. (Müşteri listesi gizli değildir ve şifrelenemez.) Müşterilerin gerçek isimlerini kullanarak sahte siparişler göndermek için bir program yazar. Şifre anahtarlarının listesine sahip olmadığı için son 3 bayta rastgele değerler koyarak firmaya yüzlerce sahte sipariş gönderebilir. Bu mesajlar alındığında, şirketin bilgisayar sistemi önce her müşterinin mesaj gövdesinin şifresini çözmesi için anahtarı bulur. Bu 3 baytın tüm değerleri geçerli olduğundan (yani içindeki rastgele değerler deşifre edildikten sonra rastgele ancak geçerli bir değer haline gelir), bu nedenle bilgisayar satın alma siparişlerini ve faturaları yazdırmaya başlar. Bu sayede kişi bilgisayarın kendisi için ürettiği mesajların ne anlama geldiğini kendisi anlayamasa da aktif bir bozucu (kovulan çalışan), şirket için büyük sorunlara neden olabilir! Bu sorun, tüm mesajlara

biraz fazlalık ekleyerek çözülebilir. Dolaysıyla şifrelemenin ilk ilkesi, mesajlar bir miktar fazlalık içermelidir söylenebilir.

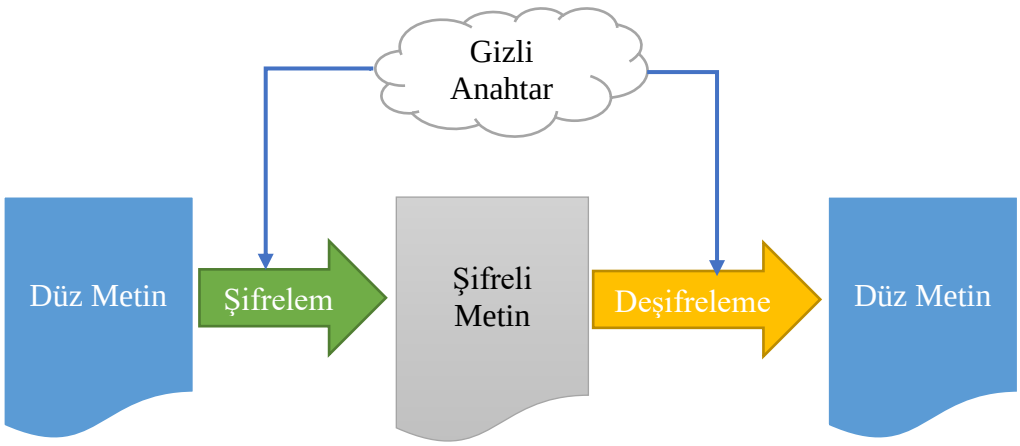
- **Mesajların Tazeliği (Freshness)**

Kriptografideki ikinci temel ilke, alınan her mesajın taze ve yeni olduğundan veya başka bir deyişle yeni gönderildiğinden emin olmak için hesaplamalar yapmanız gerektiğidir. Bu, Aktif Davetsiz Misafirin eski mesajları yeniden göndermesini önlemek için gereklidir. Bu yapılmazsa, işten çıkarılan çalışan, içeriğinin ne olduğunu bilmese bile, telefon hattından ayrılarak önceki geçerli mesajları tekrarlayabilir; bu nedenle, kriptografinin ikinci ilkesi: tekrar eden cümleleri (mesaj tekrarı) etkisiz hale getirmek için önlemler alınmalıdır.

Mesajların güncelliğini sağlamanın bir yolu, mesajların sınırlı bir süre, örneğin birkaç saniye için geçerli olması için onlara bir zaman damgası koymaktır. Artık alıcı, alınan mesajları aynı birkaç saniye boyunca tutabilir ve bunları yeni mesajlarla karşılaştırabilir; bu yöntemle mükerrer mesajlar kolayca silinebilir, çünkü yeniden gönderilen mesajlar da dahil olmak üzere, kullanım süresi amaçlanan süreden daha uzun olan mesajlar artık geçerli değildir.

2.4.1 Simetrik ve Asimetrik Kripto Sistemler

Simetrik şifreleme, veri şifreleme ve şifre çözme için tek bir anahtar kullanan bir şifreleme yöntemidir. Bu en eski ve en iyi bilinen şifreleme tekniğidir. Gizli anahtar, güvenli bir rasgele sayı üreteci (RNG) tarafından oluşturulan bir sözcük, sayı veya bir dizi karakter veya sayı olabilir. Mesaj, anahtardaki şifreleme algoritmasının kurallarına göre değiştirilir. Simetrik şifreleme yoluyla iletişim kuran kişiler, bilgileri şifrelemek ve şifresini çözmek için anahtarları değiş tokuş etmek zorundadır. Simetrik şifreleme genel yapısı Şekil 2.1 de gösterilmiştir.



Şekil 2.1. Simetrik Şifreleme

Simetrik şifreleme algoritmaları kullanılarak veriler, şifresini çözecek gizli anahtarı olmayan birinin anlayamayacağı bir forma dönüştürülür. Hedeflenen alıcı mesajın gizli anahtarına sahip olduğunda, mesajın şifresini orijinal ve anlaşılır biçimine geri döndürmek için ters şifreleme işlemi gerçekleştirilir. Banka düzeyinde şifreleme için, FIPS 140-2 gibi endüstri standartlarına göre doğrulanmış bir RNG kullanılarak simetrik anahtarlar oluşturulmalıdır. Simetrik bir şifreleme sisteminde aşağıdakiler de dahil olmak üzere beş ana bileşen vardır:

- **Düz Metin (Plain Text)**

Düz metin terimi, kodlanması gereken anlaşılabilir ana mesajı ifade eder. Düz metin genellikle yetkisiz kişiler tarafından görülmemesi gereken hassas veriler içerir.

- **Anahtar (Key)**

Anahtar, şifre çözme yöntemi olarak tanımlanır. Anahtar olmadan şifrelenmiş metnin şifresi çözülemez ve okunamaz. Anahtar, düz metin olarak yapılan tüm anahtarlar ve değişiklikler hakkında bilgi sağlar. Bir şifreleme türü olan simetrik şifrelemede anahtarın taraflar arasında paylaşılması gerekir ve şifre çözme yöntemi evrensel değildir. Gönderici ve alıcı nihai olarak anahtarı paylaştığından, şifre çözme olasılığı anahtara bağlıdır.

- **Şifreli Metin (Cipher Text)**

Şifreli metin, şifrelenmiş ve gönderilmeye hazır metindir. Bu metin rastgele miktarda veri içerebilir ve okunamaz.

- **Kriptografik Algoritmalar (Encryption)**

Bir şifreleme algoritması aslında verileri (düz metin) şifreli metne dönüştürmek için kullanılan matematiksel bir formüldür. Bazı şifrelemelerde, bir algoritma verileri tahmin edilebilir bir şekilde değiştirmek için bir anahtar kullanır, böylece şifrelenmiş veriler rastgele görünse bile, anahtarın yeniden uygulanmasıyla düz metne geri dönüştürülebilir.

- **Şifre Çözme Algoritması (Decryption)**

Şifre çözme algoritmasında, şifreli metne gizli anahtar uygulanarak düz metne dönüştürülür. Şifre çözme genellikle şifrelemeyi tersine çevirir.

Simetrik şifreleme, günümüz teknolojisinde birçok uygulamaya sahiptir. Bazı güvenlik uzmanları, çoğu durumda bu algoritmanın uygulamaları asimetrik algoritmalardan farklıysa, yalnızca asimetrik algoritmalar önerir. En yaygın kullanılan ve popüler simetrik şifreleme algoritmalarından bazılarından AES, DES, IDEA, Blowfish, RC4, RC5 and RC6 söylenilebilir.

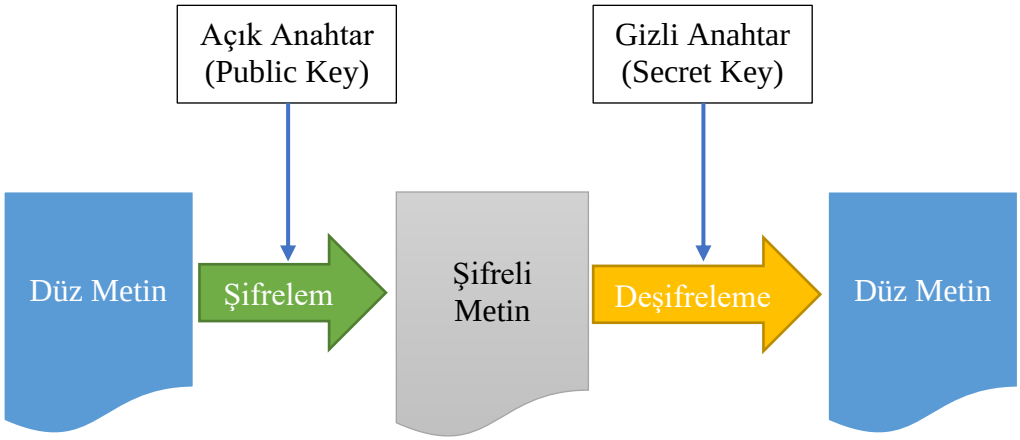
Simetrik şifreleme eski bir şifreleme yöntemi olmasına rağmen, asimetrik şifrelemeden çok daha hızlı ve verimlidir. Asimetrik şifreleme, performans sorunları, veri boyutu ve yoğun işlemci kullanımı nedeniyle ağlara zarar verir. Simetrik şifrelemenin (asimetrik ile karşılaştırıldığında) daha iyi performansı ve daha hızlı hızı nedeniyle, toplu şifrelemede (büyük miktarda veri şifreleme) simetrik şifreleme yaygın olarak kullanılır.

Asimetrik Kriptografi, asimetrik kriptografiden daha gelişmiş bir kriptografi versiyonudur. Bu yöntem, ortak anahtar şifrelemesi olarak da bilinir, çünkü uygulamalarından biri, istenen kilit için bir ortak anahtar tanımlandığındadır. Bu yöntem de blockchain teknolojisinde popüler yöntemlerden biridir ve sistemin güvenliğini arttırır.

En ünlü asimetrik şifreleme algoritmalarından biri RSA algoritmasıdır. Dijital imzalarda ve PGP ve SSL bölümlerinde kullanılan algoritma. Asimetrik şifrelemenin simetrik şifrelemeye göre özel bir noktası vardır, yani bu yöntemde şifreleme ve şifre çözme için bir çift anahtar vardır. Bu anahtarlar özel ve açık anahtarlardır ve bu iki anahtar arasında onları ilişkili bir çift olarak tanımlayan matematiksel bir ilişki vardır.

Asimetrik şifreleme yöntemindeki özel şifreleme ve şifre çözme mekanizması, bu yöntemin işlenmesi için daha fazla enerji ve zaman gerektirmesini sağlar. Blockchain teknolojisinde genellikle çokça karşılaştığımız özellik bu.

Bu özellik, ağ ve şifreleme uzmanlarının bu yöntemi tüm bilgileri şifrelemek için değil, bazı özel adımları şifrelemek için kullanmasını sağlar. Bu adımlar arasında kimlik doğrulamadan bahsedilebilir. Asimetrik şifreleme yönteminin uygulama durumları arasında, kullanıcılara açık anahtar verdiğimizde ve onlara özel anahtarın bulunmadığı ve yalnızca cihaz veya sunucuya açık olduğu durumlardan bahsedebiliriz. Asimetrik şifreleme Şekil 2.2 de gösterilmektedir.



Şekil 2.2. Asimetrik Şifreleme

Bu yöntemin bir başka kullanımı da siteleri güvenli ve özel bir şekilde görüntülemektir. Bu amaçla asimetrik şifreleme yönteminin ortak ve özel anahtar çifti kullanılır. Bu durumda, PC'nizin genel anahtarı ve sunucunun özel anahtarı vardır. Asimetrik algoritma, dağıtımla ilgili sorunları ortadan kaldırır, çünkü bu algoritmada anahtar değişimine gerek yoktur; Özel bir anahtar kalır ve cihaza veya kullanıcılara bir genel anahtar sağlanır. Asimetrik algoritma ayrıca ağ veya süreç güvenliği sağlar; çünkü bu yöntemde özel anahtarın yayınlanmasına gerek yoktur. Ayrıca, bu algoritma mesajı reddetme veya reddetme olasılığını ortadan kaldırır.

2.4.2 Akış ve Blok Şifreleyiciler

Simetrik şifreleme algoritmasında, simetrik şifrelemenin genel yapısını koruyarak verileri şifreleyen iki tür şifreleme vardır.

- Şifre Bloğu Simetrik Şifreleme Algoritmaları (Block Cipher)

Bu yöntemde bilgiler daha küçük metin bloklarına dönüştürülür ve özel bir gizli anahtar kullanılarak şifrelenir. Bu şifreleme yönteminde parçalar için kullanılan geleneksel boyut 64, 128 veya 256 bittir. AES, DES, IDEA, Blowfish, RC5 ve RC6 bu tür şifrelemedir.

- Akış Şifreleme Algoritmaları (Stream Cipher)

Bu yöntemde blok yapmak yerine her karakterin bilgisi tek başına şifrelenir. Bu türün en popüler algoritmalarından biri, kablosuz ağlarda (WIFI) 802.11 standardında WEP şifrelemesinde kullanılan RC4'tür.

2.5 Rasgele Sayı Üretimi

Rastgele sayılar üretmenin bilgisayar oyunlarından bahislere kadar çeşitli kullanımları vardır. Bu sayılar son zamanlarda kriptografi alanında çok önemli hale gelirken. Bu sayıların

üretilmesi için, bazıları gerçek rasgele sayılar üretmek için, bazıları ise sözde rasgele sayılar üretmek için kullanılan çeşitli yöntemler vardır. Bu arada kriptografide yaygın kullanım açısından sözde rasgele sayıların üretimi daha fazla ilgi görmüştür.

Rastgele sayıların üretilmesi, çeşitli bilimlerdeki araştırmacıların çok dikkatini çeken bir konudur. Genel olarak, yapısına göre rastgele sayılar iki ana kategoriye ayrılabilir: gerçekten rastgele sayılar ve sözde rastgele sayılar. Gerçekten rasgele sayılar üretmek için öngörülemeyen bir rasgele değişken kullanılır. Ancak sözde rasgele sayılar, başlangıç koşullarında ve sabit ortamda belirli sayıları içerir. Yazılım tarafından üretilen rastgele sayılar genellikle sözde rastgeledir. Bu sayılar gerçekten rastgele değildir ve tohuma bağlı algoritmalara dayalı olarak üretilir. Tohumu biliyorsanız, rastgele sayılar tahmin edilebilir. Bu sayıların üretimi, Python ve diğer programlama dilleri gibi günlük araçlarda, hatta Excel'de bile kolaylıkla oluşturulabilecekleri ölçüde düşünülmüştür. Bu araçların çoğu, rastgele sayılar üretmek için Mersenne Twister algoritmasını kullanır.

Rastgele sayılar üretme konusu uzun zamandan beri fizik bilimleri gibi bilimlerde büyük ilgi görmektedir ve son zamanlarda bilgisayar alanında yapılan ilerlemelerle bilgisayar bilimi alanında özellikle kriptografi alanında birçok uygulamaya sahip olmuştur. Ayrıca, sözde rasgele sayıların, güvenli iletişim ve gürültü üretiminde sözde rasgele sayıların kullanımı da dahil olmak üzere çeşitli bilgisayar alanlarında birçok uygulaması vardır.

Sözde rasgele sayıların kullanımına bir örnek, bir anahtardan oluşturulan rasgele listelerin oluşturulmasıdır. Bu rastgele liste kriptografide kullanılabilir. Şifrelemede, şifrelenen kaynağın orijinal haline döndürülmesi gerektiği düşünüldüğünde, rastgele sayıların yeniden üretilmesine ihtiyaç vardır. Bu nedenle, kriptografide sözde rasgele sayıların kullanımı yaygın olarak kullanılmıştır. Rastgele sayıların kullanımı hem blok şifrelemede hem de akış şifrelemede kullanılmıştır.

Üretim hızı ve yüksek dağılım, sözde rasgele sayıların üretiminde bilim adamlarının en sevdiği özellikler arasındadır. Bu konu, kaos olgusunun ve onu yöneten denklemlerin keşfedilmesiyle yeni bir aşamaya girmiştir. Aslında, sözde rasgele üreteçlerde kaos denklemlerinin tanıtılması, üreteçlerin başlangıç değerlerine karşı çok yüksek bir duyarlılığına neden olmuştur. Sözde rasgele sayılar üretmenin klasik yöntemlerinden biri, aynı zamanda yüksek hızda ve uygun dağılımla rastgele veriler üreten çapraz çarpma yöntemidir. Ancak bu benzersiz özelliklere rağmen, bu algoritmanın daha geniş uygulamasını zorlaştıran bazı zayıf yönleri vardır. Bu tezde, bir dizi sözde rasgele oluşturucunun tanıtılmasından sonra, çapraz

çarpım algoritması araştırılmış ve ardından lojistik kaotik haritalama, özel özellikleri ile birlikte tanıtılmış ve onun yardımıyla, çapraz çarpım algoritmasının zayıflığı ortaya konmuştur. Erken yakınsamada çarpma algoritması ve sınırlı sayıda sözde rasgele sayıların üretilmesi çözüldü. Son olarak önerilen yöntemin ara yönteme göre üstünlüğü Monte Carlo test simülatörü yapılarak kanıtlanmıştır.

Simülasyonun güçlü yönleri ve yetenekleri arasında, çalışılan sistemi özel ve kritik koşullar altında ve sistemin karşılaşacağı olasılıklar altında incelemesi ve analiz etmesi vardır. Bu benzersiz simülasyon yeteneği, büyük ölçüde rastgele sayılara bağlıdır. Başka bir deyişle, simülasyon yeteneğinin temel temeli rasgele sayılara dayanmaktadır. Bazı simülasyon bilim adamlarının görüşüne göre, rastgele sayılar simülasyonun somunları ve cıvataları olarak kabul edilir. Öte yandan, rasgele sayı üretimi rasgelelik kriterleriyle ne kadar tutarlı olursa, modelleme ve simülasyon sonuçlarının analizinin etkinliği üzerinde elbette büyük bir etkisi olacaktır. Bu tezde, ilk olarak, farklı rasgele sayı dizileri veya daha doğrusu sözde rasgele sayılar incelenmekte ve analiz edilmektedir. Ardından, rastgele sayı üretmenin bazı yaygın ve basit yöntemleri incelenir. Elde edilen sonuçlar, bu yöntemlerin basit olmasına rağmen, rasgele sayıların üretilmesinin problemli ve sözde parçalanma olduğunu açıkça göstermektedir. Daha sonra, elde edilen analizlerin sonuçları kullanılarak rasgele sayılar üretmek için mevcut yöntemlerin bir kombinasyonuna dayanan birleştirilmiş bir yöntem sunulmaya çalışılmıştır.

Sözde rasgele sayıların üretimi uzun zamandan beri ilgi çeken alanlardan biridir ve günümüzde kriptografinin artan önemi ve bu tip sayıların kriptografide kullanılması ile araştırmacıların ilgi odağı haline gelmiştir. Eskisinden daha fazla dikkat. Bu tezde, kaos haritasına dayalı rasgele sayılar listesi oluşturmak için etkili bir yöntem sunulmaktadır. Oluşturulan rastgele liste, görüntü şifrelemede önemli bir veri olarak kullanılır.

2.5.1 Kaotik Sistemler

Kaos teorisi, dinamik sistemlerde ele alınan teorilerden biridir. Dinamik sistemler zamanla değişir ve fizik ve davranış bilimleri dahil olmak üzere birçok bilimde özel bir yere sahiptir (Bak vd., 1988:364) (Beek , 1989:56). Kaos tartışması daha önce tartışılmış olsa da bu teorinin çalışmalarının başlangıcı, 1965 yılında meteorolojik konuları araştıran Edward Lorenz adlı bir kişi tarafından görülebilir (Lorenz, 1965:2). Kaotik sistemleri inceleyerek, meteorolojik tahminlerin başlangıç koşullarındaki küçük bir değişikliğin sistemin tepkisinde büyük dalgalanmalara neden olduğu sonucuna vardı.

Kaos teorisi, başlangıç koşullarına çok duyarlı dinamik sistemler alanında öne sürülen matematikteki en önemli teorilerden biridir. Kaos kelimesi kelimenin tam anlamıyla "tam bir düzensizlik"; "tam bir organizasyon veya düzen eksikliği" anlamına gelir. Bu teori aslında ilginç bir paradokstur, "doğal olarak öngörülemeyen" sistemlerin davranışlarını tahmin etmek için bir bilimdir. Aslında kaos teorisi, kaostan güzel yapılar elde etmemizi sağlayan matematiksel bir araçtır.

Kaos teorisinin temeli, düzen ve kaosun her zaman zıt olmadığı fikridir. Kaotik sistemler, düzen ve kaosun büyüleyici bir birleşimidir. Onlara dışarıdan baktığımızda öngörülemez davranırlar ve düzensizlik gösterirler, ancak bu sistemlerin içinde düzen ile çalışan bir dizi deterministtik denklem görüyoruz.

Kaos, genellikle doğrusal olmayan bir dinamiğe uygulanan bir addır. Bu ifade, sözde basit, doğrusal ve iyi huylu sistemlerin karmaşık davranışını açıklamak için kullanılır. Kaotik davranış, rastgele dış gürültüden güçlü bir şekilde etkilenen bir sistemin davranışına benzer şekilde düzensiz ve genellikle rastgele görünür. Kaosun matematiksel tanımı, deterministtik bir dinamik sistemin başlangıç koşullarına (genelde kelebek etkisi olarak bilinir) duyarlılığı nedeniyle öngörülemeyen uzun vadeli davranışıdır. Kaos teorisi, deterministtik doğrusal olmayan dinamik sistemlerde kararsız periyodik davranışın nitel çalışması olarak tanımlanır.

Kaos kelimesi, düzensizliği ve herhangi bir yapı veya düzen eksikliğini gevşek bir şekilde tanımlar. Ancak, kaotik sistemlerin davranışının rastgele göründüğü söylenmelidir. Ancak kaotik davranışın oluşmasında bir tesadüf unsurunun varlığına gerek yoktur ve bazı dinamik sistemler (deterministtik) de kaotik davranış gösterebilir. Bugün, kaos teorisi çeşitli alanlarda ve eğilimlerde çok fazla etki kazanmıştır. Hal böyle olunca kaostan eser olmayan bir bilim ya da organizasyon bulmak zor. Çeşitli fonksiyonlar belirli koşullar altında kaotik davranır. Bu tez, iki boyutlu bir haritalama olan Baker harita işlevini kullanmıştır. Bu bölümün geri kalanında, önce Baker haritasının standart formunu tanıtacağız ve ardından genişletilmiş versiyonunu inceleyeceğiz.

2.5.2 Kaotik Sistemlerin Özellikleri

Kaos, genellikle gürültüsüz olan çok basit sistemlerde meydana gelir. Aslında, bu sistemler esasen "deterministtir"; Yani sistemin başlangıç koşulları hakkında doğru bilgi ile gelecekteki davranışı tahmin edilebilir. Sonuç olarak kaos, sınırlı, periyodik olmayan (periyodik olmayan) ve gürültülü salınım olarak tanımlanabilir. Başka bir deyişle, deterministtik bir sistem, rastgele girdileri olmasa bile rastgele davranır. Kararsız doğrusal

olmayan sistemlerde, alt harmonikler, yarı periyodik salınımlar ve kaotik davranış dahil olmak üzere çeşitli garip etkiler vardır.

Deterministtik ve kaotik davranışa sahip bazı sistemler şunlardır: atmosferik sistemler, güneş sistemi, jeolojik levhalar, türbülans akışı, nüfus artışı, güç elektroniği devreleri vb. Ancak biyoloji, bilgisayar bilimi, ekonomi, mühendislik, finans, matematik, meteoroloji, felsefe, fizik, politika, psikoloji, borsa ve robotik gibi birçok başka alanda kaos var.

Kaotik dinamik sistemler aşağıdaki özelliklere sahiptir:

- Başlangıç koşullarına duyarlıdırlar.
- Değişken rotasyonları yoğundur.
- Topolojik olarak birleştirilirler.

Başlangıç koşullarına duyarlılık, mevcut yoldaki küçük bir bozulmanın gelecekte çok farklı davranışlara yol açabileceği anlamına gelir. Topolojik bileşim ayrıca zaman içinde sistemin herhangi bir bölge veya faz uzayının açık kümesinin sonunda herhangi bir diğer belirli bölge ile örtüşeceği şekilde geliştiği anlamına gelir.

Kaos, dinamik sistemlerin karmaşık davranışını tanımlamak için kullanılan bir terimdir. Kaos aslında bu sistemlerin davranış türlerinden biridir. Alt tutarlılık ve sözde periyodiklik, bu sistemlerdeki diğer davranış türleridir. Bu bilim dalına daha genel olarak, doğrusal olmayan bir sistemin dinamik davranışının (yani zaman davranışı) araştırıldığı "doğrusal olmayan dinamikler" (Doğrusal Olmayan Dinamikler) denir. Doğrusal olmayan bir sistem, zaman denklemleri (diferansiyel denklemler) doğrusal olmayan, yani değişken denklemde doğrusal olmayan bir biçimde görünen bir sistemdir. Doğrusal olmayan sistemler, doğal olayların incelenmesinde her zaman önemli bir rol oynar ve son yıllarda bunlar üzerinde kapsamlı araştırmalar yapılmıştır.

Bu araştırma büyümesinin ana nedeni, güçlü ve düşük maliyetli hesaplamalar olasılığıdır. Kapalı form çözümleri olan lineer sistemlerden farklı olarak, lineer olmayan sistemlerin az sayıda kapalı form çözümleri vardır ve bu nedenle sayısal yöntemler lineer olmayan fenomenleri bulma ve analiz etme sürecinde önemli bir rol oynar. Düşük maliyetli bilgisayarların ortaya çıkmasından önce, yalnızca bazı araştırmacılar doğrusal olmayan simülasyonlar gerçekleştirebildi. Bugün, kişisel bilgisayarı olan herkes doğrusal olmayan bir sistemi simüle edebilir.

Buraya kadar belirttiğimiz ön bilgilere göre, kaotik sistemlerin lineer olmayan sistemlere göre bazı özelliklerini inceliyoruz.

- **Doğrusal olmama**

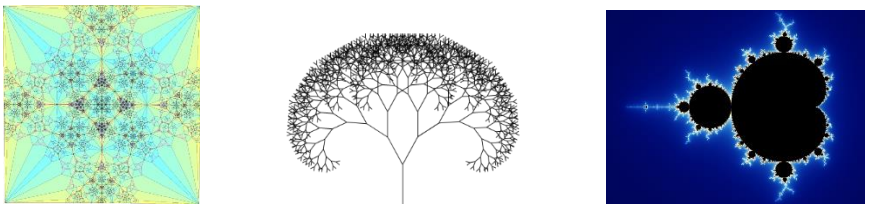
Bu, çıktının girdiyle doğru orantılı olmadığı anlamına gelir, başka bir deyişle, bir değişkendeki değişiklikler, ilgili değişkenlerde orantılı bir değişikliğe veya reaksiyona neden olmaz. Açıkçası, işler teoreminin toplamı doğrusal olmayan sistemler için geçerli değildir.

- **Başlangıç koşullarına aşırı hassasiyet**

Kelebek etkisi ve kaos teorisinin arka planı bölümlerinde ve kaosu tanımlamanın ve anlamanın ilk adımında, Lorentz sistemi için kaotik sistemin başlangıç koşullarına tepki duyarlılığını gözlemledik. Kaotik sistemler, başlangıç koşullarına çok duyarlı olan doğrusal olmayan dinamik sistemlerdir ve bu tür sistemlerin başlangıç koşullarındaki küçük bir değişiklik, bu sistemlerin gelecekteki davranışlarında büyük değişikliklere neden olacaktır. Bu fenomen, kaos teorisinde kelebek etkisi olarak bilinir.

- **Bencillik**

Kaos teorisinde; Parçalar ve bütün arasında bir tür benzerlik fark edilebilir. Bu şekilde, kalıbın her parçası bütünle aynıdır. Kaotik denklemlerde, çizim desenleri parçalar ve bütün arasında bir tür benzerlik gösterir, öyle ki desenin her bir parçası aynı ve bütüne benzer. Geometride fraktal olarak da bilinir. Bu özellik sınıfta bahsedilen bir ağaç yaprağı, bir kar tanesi, "von Koch" eğrisi veya holografik ekran yeteneği gibi örneklerle açıklanabilir. Şekil 2.3 Wikipedia sitesinde bulunan bazı fraktal örneklerini göstermektedir.



Şekil 2.3. WikiPedia Sitesinden Fraktal Örnekleri

Kaynak: (Wikipedia, 2022)

- **İnanılmaz emiciler**

Dinamik bir sistemin davranışı, denge noktasına asimptotik olarak yakınsak, değişken, yarı dönüşümlü veya kaotik olabilir. Bir sistemdeki aralıklı davranış, frekans oranının önemli bir sayı olmaması için çoklu frekanslar ve harmonikler ile durum değişkenlerinin salınımını içerir. Kaotik sistemde baskın bir periyodiklik yoktur veya başka bir deyişle bu sistem sonsuz periyodikliğe sahiptir. Kararlı sistemin denge noktasına doğru asimptotik hareketinde denge noktasına soğurucu deriz. Ayrıca, alternatif veya yarı-periyodik harekette, durumun tüm

yollarının doğru gittiği uzayın parçası diyoruz. Şekil 2.4, bu emicilerden bazılarını göstermektedir. Başlangıç koşullarına oldukça duyarlı olan başka emici türleri de vardır. Kaotik sistemlerin özelliklerinden ve özelliklerinden biri, faz yollarının kümesi olan bu yutucuların varlığıdır. Bu emiciler, bir dizi boncuktan oluştuğu için şaşırtıcı emiciler olarak adlandırılır. Noktalar, sıfır hacimli ve sonsuz yüzeyli noktalar topluluğudur (Crilly vd., 2012:59).

Kaotik davranışa izin veren üç veya daha fazla boyutlu durum uzayının tanımlayıcı özelliği, durum yörüngelerinin uzayın bazı bölgelerinde birbirini keserek ve keserek sınırlı kalabilmesidir. Bu yollarla ilişkili geometrinin daha garip hale geldiği açıktır ve bunlar, içerideki durum yollarının gerildiği ve katlandığı aynı garip çekicilerdir. Bu özellik, bazı yolların diğerlerinden uzaklaşırken yakınsamasına neden olur.

- **Uyumluluk**

Görünüşte düzensiz sistemler, çevreleriyle ilgili olarak canlı organizmalar gibi hareket eder ve kendileri ile çevreleri arasında bir tür dinamik uyumluluk yaratır.

2.5.3 Kelebek Etkisi ve Kaos Teorisinin Arka Planı

Pratikte, kaos teorisi, 1960 yılında bir bilgisayarda hava durumu modellerini simüle eden MIT meteorolog Edward Lorentz'in çalışmasından kısmen uyarlanmıştır.

İki yıl boyunca, meteoroloji bilimciler, nispeten değişmeyen ve tamamen ılımlı hava koşullarına sahip belirli bir bölgenin hava durumunu inceliyor ve tüm değişiklikleri kaydediyorlardı. Her gün sabah altıda atmosferik değişiklikleri kaydetmek için bir cihazı açtılar ve değişiklikleri öğleden sonra altıya kadar kaydettiler. İkinci yılın sonbaharında, aniden, kaydedilen değişikliklerin grafiği garip bir şekilde değişti ve şiddetli atmosferik değişikliklerin meydana geldiğini gösteren rahatsız edici bir grafik kaydedildi. Bu, görünür bir değişiklik olmadığındaydı. Düşüşten sonra her şey normale döndü. Bu garip konu bilim adamlarının bu alanda çalışmalar yapmasına neden oldu. Ertesi yılın sonbaharında her şeyi izlediler ve gözlemlerinin sonucunu buldular. O yerin yakınında sonbaharda bir grup göçmen kuşun gittiği bir göl vardı ve görünüşe göre bu kuşlar haritalarda ciddi bir değişikliğe neden oldu.

Bu kuşların kitlesel uçuşu, kanatlarının hareketinin atmosfere baskı yapmasına neden oldu ve bu basınç yandaki hava moleküllerine aktarıldı ve sonunda cihazın harita kayıt sensörüne ulaştı. Bu konuyu gözlemleyen bilim adamlarından birine, bu kuşlar olmasaydı ne olurdu diye düşündürdü? Bir bilgisayar programı kullanarak, bölgenin konumunu simüle etti ve programı bir kez kuşların varlığında ve bir kez de yokluğunda çalıştırdı. Kuşlar oradayken bilgisayar, koşulları tam olarak rutine göre ve gerçeğe dayalı olarak gösterdi; ancak kuşların

varlığı olmadan, bölgede neredeyse 12 hektarlık bir alanı yok edecek büyük bir fırtına oluşacaktı. Görünüşe göre o kuşların tüyleri bu fırtınanın oluşmasını engellemiş. Daha ciddi ve derinlemesine incelemeler yaptıktan ve dünya atmosferini simüle ettikten sonra, kaos teorisinin en önemli sloganı haline gelen bir sonuca vardılar: "Afrika'da bir kelebek çırpınır ve Güney Amerika'da bir hortum oluşur". O kelebeğin kanat çırpışının atmosfere getirdiği basınç çok küçük olabilir ama yoğunlaşma süreci bu küçücük basıncın zamanla ve belli bir mesafe kat ettikten sonra büyük bir fırtınaya dönüşmesine neden olur. Bu nedenle, "kelebek etkisi" terimi, Edward Lorentz'in bir makalesinden sonra tanıtıldı. 1972'de "Brezilya'da kanat çırpan bir kelebek Teksas'ta kasırgaya neden olabilir mi?" başlıklı bir makale sundu. Dünyanın ikliminden çözülemez bir diferansiyel denkleme ulaşan çok basit bir matematiksel model araştırıyordu ve denildiği gibi bu denklemi çözmek için bilgisayar aracılığıyla sayısal yöntemlere başvurdu. Bunu ardışık günlerde yapabilmek için bir günün son çıktısının sonucunu ertesi günün başlangıç koşulları olarak girecektir. Lorentz sonunda, aynı başlangıç koşullarına sahip farklı simülasyonların sonuçlarının tamamen farklı olduğunu gözlemledi. Bilgisayarın çıktısı incelendiğinde Lorentz'in kullandığı bilgisayarın çıktıyı 4 ondalık basamağa kadar yuvarladığı ve bu bilgisayarın içindeki hesaplamalar 6 ondalık basamakla yapıldığından son basamağın kaybının böyle bir etkisi oldu. Yuvarlama hareketindeki değişikliklerin miktarı, bir kelebeğin çırpma etkisine yakındır. Bu gerçek, uzun vadede hava durumunu tahmin etmenin imkansızlığını gösterdi. Lorentz'in gözlemleri kaos teorisi konusunu daha gündeme getirdi. "Kelebek etkisi" argo ifadesi, kaos teorisinin özel dilinde "başlangıç koşullarına hassas bağımlılık" olarak çevrilir. Gerçek dünyadaki çoğu sistem, belirli bir işlemi tekrarlayarak çalışır. Lorentz iklimi örneğinde, güneş tarafından dünya yüzeyinin ısıtılması ve atmosferin radyasyon yoluyla dış uzaya soğutulması işlemi sürekli tekrarlanan bir işlemdir. Böyle bir sistemde bir dizi başlangıç değerinin kaotik davranışa neden olduğu gösterilebilir. Hava durumu dışında, diğer dinamik sistemlerde başlangıç koşullarına duyarlılık görülebilir. Basit bir örnek, bir dağın tepesine yerleştirilmiş bir toptur. Bu top, çarpma yönüne bağlı olarak, çok küçük bir darbe ile çevredeki vadilerden herhangi birine düşebilir.

Bu nedenle kelebek etkisi birçok bilimsel olgu ve terim gibi günlük konuşmalara girmiş ve apaçık bir gerçek olarak kabul edilmiştir. Genel olarak bakıldığında kelebek etkisinin bir sistemde görülebilmesi için iki özelliğin olması gerekir:

- Sistemin doğrusal olmayan davranışı vardır.
- Sistemin her anının durumu, bir önceki anın durumunun bir fonksiyonudur.

2.5.4 Kaos Tabanlı Görüntü Şifreleme

Günümüzde, dijital dünyada, mesaj alışverişinde ve ticari alışverişte bilgi koruması temel ve önemli bir rol oynamaktadır. İşlemin güvenlik ihtiyaçlarını sağlamak için şifreleme kullanılmaktadır. Bu konunun önemine ve geleneksel aşamadan dijital aşamaya geçişe göre, görüntünün en önemli bileşeni olarak kabul edilebilecek şifreleme yöntemlerinin kullanılması gerekli görünmektedir. Son yıllarda, görüntü şifreleme için çeşitli şifreleme algoritmaları ve yöntemleri tanıtılmış, bunların çoğu veri şifreleme için kaos işlevlerini ve genetik şifrelemeyi kullanmıştır. Bu görev için birçok yöntem önerilmiştir, kaos teorisine dayalı yöntemler, onları şifreleme sistemlerinin yapılandırılmasının önemli bir parçası haline getiren benzersiz özelliklere sahiptir.

Görüntüleri iletmek için klasik şifreleme yöntemlerinin kullanılması, zayıf iletim hızı ve zayıf iletim güvenliği gibi dezavantajlara sahiptir. Son yıllarda bu eksiklikleri gidermek için çeşitli yöntemler önerilmiştir, bu yöntemlerden biri de kaos sistemlerine dayalı kriptografik algoritmalar oluşturmaktır ancak normalde bu algoritmalarda kullanılan klasik kaos fonksiyonlarının zayıf yönleri vardır. Örnek olarak, lojistik ve günah kaos fonksiyonları mekânsal alanda düzgün olmayan bir dağılıma sahiptir, ayrıca bu fonksiyonlar belirli bir mekânsal alanda kaotik bir yapıya sahiptir.

Görüntü şifreleme için bazıları kaos işlevleriyle entegre edilmiş çeşitli yöntemler önerilmiştir. En yeni ve en başarılı görüntü kodlama yöntemlerinden biri DNA tabanlı görüntü kodlamadır. Kaos sistemlerinin başlangıç değerine duyarlılık ve rasgelelik gibi doğal özelliklerinden dolayı, kaos sistemine dayalı görüntü şifreleme yöntemi, yüksek güvenlikli şifreleme için uygun görünmektedir. Bu tür şifreleme tipik olarak iki adım gerektirir: permütasyon ve yayılma. Permütasyon adımında, pikselin gri seviyesi değiştirilmeden bir kaos haritası yardımıyla görüntü pikseli atanır. Daha sonra, yayılma adımında, her pikselin değeri, bir permütasyon dizisi kullanılarak değiştirilir.

2.5.5 Standart Lojistik Harita

İlk kez, Hayes ve diğerleri, 1993 yılında bilgi iletiminde kaotik sinyallerin kullanımını önerdi (Hayes vd., 1993:3031). Genellikle, bu sinyaller, başlangıç değerlerine çok duyarlı olan bir dizi sözde rasgele sayı üretebilir ve bu özellik kriptografide (Pisarchik vd., 2006: 033118-1) çok önemli olabilir.

Bazı koşullarda kaotik özelliklere sahip olabilen en basit doğrusal olmayan sistemlerden biri lojistik haritalamadır. Bu haritalama ilk olarak 1838'de Pierre Francois Verholst tarafından

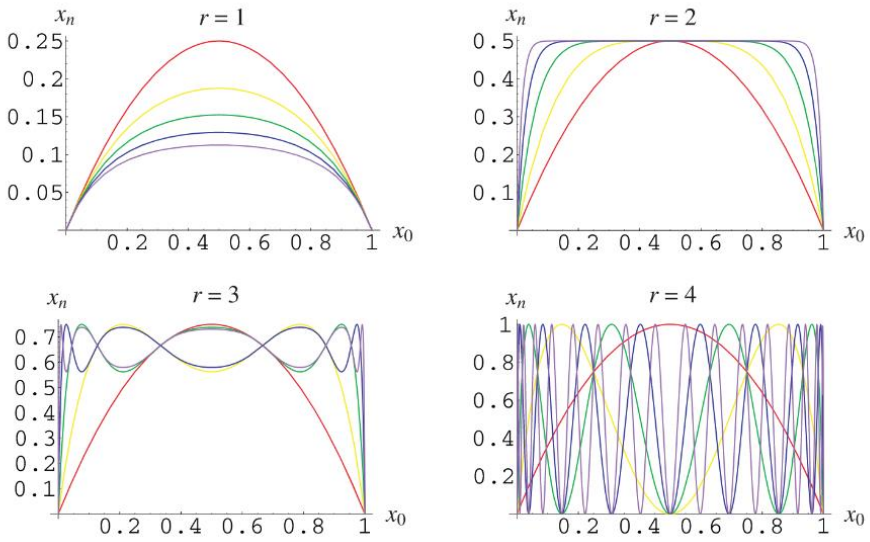
bir demografik model tasarlamak için tanıtıldı ve daha sonra sözde rasgele sayı üreteci olarak incelendi. Başlangıç koşullarına çok duyarlı olan bu eşleme, uzun bir sözde rasgele sayı dizisi oluşturmak için kullanılabilir. Bu uzun rastgele dizi, görüntü verileri gibi büyük verileri şifrelemek için kullanılabilir.

Lojistik haritası genel olarak aşağıdaki şekilde sunulur:

$$X_{n+1} = rX_n(1 - X_n) \tag{2.1}$$

Burada r sistem katsayısı, $X_n \in (0,1]$ sistem değişkeni ve n yineleme sayısıdır. Sistemin etkin şekilde çalışa bilmesi için başlangıç değeri olarak x_0 değerine ihtiyaç var. Bu değer genelde probleme uygun seçilmektedir. Bu çalışmada x_0 değeri şifrelemede kullanılacak anahtardan elde edilmektedir.

Aslında Lojistik haritası her durumda kaotik davranışlarına sahip değil. Örneğin şekil 2.4 da göründüğü gibi bu harita r değerine bağlı farklı durumlarda bulunabilir. Burada önemli olan uzun peryodik rasgele sayıların üretebilmesi.



Şekil 2.4. Lojistik Harita Farklı *r* Değerlerde (Weisstein, 2001)

Kaynak: (Wikipedia, 2022)

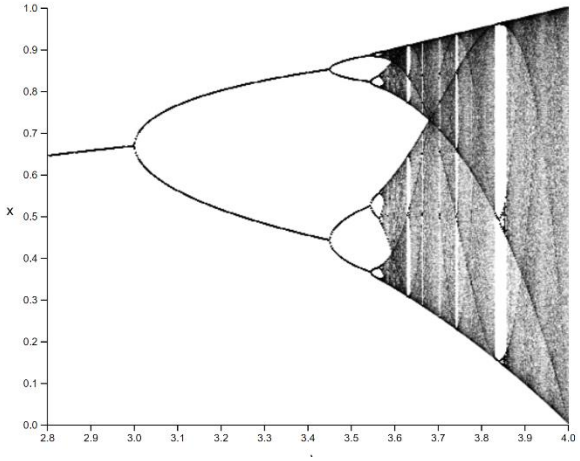
Şekil 2.4'e göre lojistik fonksiyonu *r* değerine oldukça bağlıdır. Burada *r* =1, 2 ve 3 de kaotik özellikler görünmemektedir, ancak *r*=4 de kaotik özellikleri görünür. *r* değerini daha dikkatli incelemek için çatallanma (Bifurcation) diyagramı incelenebilir. Bu diyagram aslında, bir durumun karmaşıklığını göstermenin bir yoludur. Bu diyagramda, sistemlerin çekicilikleri

r parametresinin bir fonksiyonu olarak çizilmiştir. Çatallanma diyagramı olarak bilinen bu diyagram, dinamik sistemlerin incelenmesinde çok önemli bir araçtır.

Tartışılan diyagram aşağıdaki gibi hazırlanır:

- İlk olarak, *r* belirlenir ve bir başlangıç koşulu seçilir.
- Ardından işlev, dinamiklerin geçici kısmı için 10.000 kez gibi belirli bir sayıda tekrarlanır.
- Daha sonra fonksiyon 1000 kez daha tekrarlanır ve elde edilen değerler *r* sütununa çizilir.
- Daha sonra *r* değeri arttırılır ve işlem tekrarlanır.

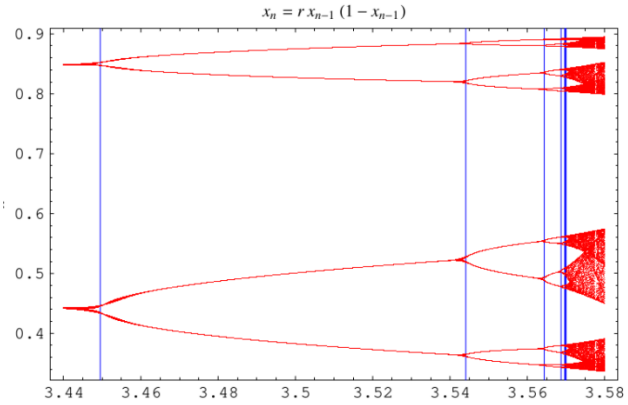
Şekil 2.5, bu işlemle ilgili diyagramı göstermektedir. Bu diyagramda *x* ekseni *r* ile ilgili değerler ve *y* ekseni fonksiyonun değişken değeri olarak göstermektedir.



Şekil 2.5. Lojistik Harita İçin Çatallanma

Kaynak: (Weisstein, 2001)

Şekil 2.5'da görüldüğü gibi, *r* arttıkça periyot olayları açıkça ikiye katlanır. Bir noktada tüm noktaların geniş bir spektruma yayıldığı ve süreklilik gibi bir şey oluşturduğu da görülebilir. Ayrıca, çatallanma diyagramında benzer garip yapıların yanı sıra kaos görünümünde periyodik davranış rejimlerinin olduğunu görüyoruz. Bu özellik Şekil 2.6'de gösterilmektedir.



Şekil 2.6. Lojistik Haritada *r* Değerine Göre İkiye Katlama

Kaynak: (Weisstein, 2001)

Tüm bu özellikler göz önüne alınarak, lojistik haritanın *r* değeri 3.5 ile 4 arasında olduğunda kaotik davranışlara sahip olduğu açıkça anlaşılmaktadır.

2.5.6 Baker Harita

Baker haritası, birim kareden içe doğru elde edilen kaotik bir haritadır. Bu fonksiyon topolojik olarak eşlenik at haritasına benzer. Çoğu kaotik harita gibi, Baker işlevi de operatörün oluşturduğu özel koşullarda kaotik özelliklere sahiptir. Baker haritasına ilişkin genelleştirilmiş fonksiyon denklem 2.2 de verilmiştir.

$$(x_n, y_n) = \begin{cases} (\frac{x_{n-1}}{\alpha}, \alpha y_{n-1}) & 0 < x_{n-1} \leq \alpha \\ (\frac{x_{n-1}-\alpha}{1-\alpha}, (1-\alpha)y_{n-1} + \alpha) & \alpha < x_{n-1} \leq 1 \end{cases} \quad (2.2)$$

α bir kontrol parametresi ve (0, 1) aralığında ise kaotik karakterli sonuçlar üretebilir.

Kaos işlevleri, bilgisayar gibi sınırlı bir hassas bilgi işlem aygıtında üretiliyorsa, durum alanı sınırlıdır. Böyle durumlarda bu kaos fonksiyonlarıyla oluşturulan diziler doğal olarak periyodik hale gelir. Böyle bir durumda istenen kaotik fonksiyon, kaotik beklentisini karşılamamaktadır. Böyle bir duruma dinamik yıkım denir (Li vd., 2004:1). Kaos haritaları, dinamik yıkıma rağmen şifreleme için yeterince güvenli kabul edilemez. Bu nedenle, bu tezde, dinamik bozulma problemini çözen kaos fonksiyonunun geliştirilmiş versiyonunu kullandık.

2.5.7 İYİLEŞTİRİLMİŞ BAKER HARİTA SİSTEMİ

(Liu vd., 2017:7)'de önerilen yönteme göre, gecikme başlatma yöntemine dayalı dinamik yok etme problemini ortadan kaldırmak için *a* parametresini değiştirmek için aşağıdaki doğrusal fonksiyon kullanılabilir.

$$g(x_i) = bx_i + by_i + 1 - 2b \tag{2.3}$$

Burada 0 <b <1 lineer katsayıdır. Denklem 2.3'e uygulayarak ve genel bağıntı 1'i kullanarak fırıncı fonksiyonunun Gecikme-giriş haritasını denklem 2.4 olarak düşünebiliriz.

$$(x_n, y_n) = \begin{cases} \left(\frac{x_{n-1}}{g(x_{n-1})},\ g(x_{n-1})y_{n-1}\right), & 0 < x_{n-1} \leq \alpha \\ \left(\frac{x_{n-1}-g(x_{n-1})}{1-g(x_{n-1})}, (1-g(x_{n-1}))y_{n-1} + g(x_{n-1})\right), & \alpha < x_{n-1} \leq 1 \end{cases} \tag{2.4}$$

Bu tezde, fırıncının geliştirilmiş işlevi, sözde rasgele sayılar üretmek için kullanılmıştır.

3. SUNULAN KAOS TABANLI GÖRÜNTÜ ŞİFRELEME

3.1 Giriş

Dijital görüntüler yapısal olarak piksel adı verilen birkaç noktadan oluşmakta ve her piksel 0 ile 255 arasında olan üç sayı şeklindedir. Bu sayılar pikselde olan kırmızı, yeşil ve mavi değerlerini temsil etmektedir. Genelde pikseller arasında bağlantılar olabilir, örneğin komşu piksel değerleri arasındaki farklar çok fazla olmamaktadır. Bu özellik kriptanalizler tarafından istatistik incelemeler için çok önemli ip ucu sayılır. Etkili şifreleme yöntemi bu tarz bağlantıları ortadan kaldırmalıdır. Genelde bu işlem piksel değerlerini değiştirerek veya piksellerin birbiri ile yer değişimi yaparak gerçekleştirilir. Bu tezde önerilen yöntem ise piksel değerlerini değiştirerek şifreleme işlemini yapmaktadır. Değiştirilen değerler daha sonra deşifreleme esnasında tekrardan orijinal değerlere geri dönüştürülmelidir. Dolaysıyla şifreme anahtarından elde edilen rasgele sayılar şifreleme işleminde kullanılmaktadır. Aynı rasgele sayılar karşı tarafta deşifreme işlemi yaparken elde edilirse, orijinal görüntü üretilebilir. Aynı rasgele sayıları elde edilebilmesi için şifrelemede kullanılan anahtarın aynısı deşifrelemede de kullanılmalı. Burada önemli olan şifreleme/deşifreleme işlemleri anahtar kelimeye oldukça bağlı olmasıdır. Öyle ki anahtar kelimesinin şifreleme ve deşifreleme işlemlerinde en az farklılığı, deşifrelemeden elde edilen görüntü orijinal görüntüden çok farklı olmalıdır. Önerilen yöntem buna benzer birkaç durumlara dayanaklı olmalı. Bu tezin analiz bölümünde yöntemin performansı çeşitli durumlar için incelenmiştir.

Önerilen yöntemde piksellerin değerlerinin değiştirmesi için pikselin görüntüde bulundu konumu yanı sıra rasgele 256 elemanlı dizi kullanılmıştır. 256 elemanı rasgele dizide 0 ile 255 arasında sayılar rasgele konumlarda yer almalıdır. Sayıların dizideki konumları anahtar kelimesine bağlı rasgele şekilde belirlenmeli. Bu dizinin oluşumunda kaos haritalardan faydalanmıştır. Kaos haritadaki başlangıç değer şifrelemede kullanılan anahtar kelimeden elde edilmiştir. Kaotik sistemlerin başlangıç değerlere ne kadar hassas olduğunu göz önüne alarak, üretilen rasgele dizi ne kadar anahtar kelimesine bağlı olduğu anlaşılabilir. Önerilen algoritma görüntünün her bir pikselini seçer. Pikselin sayısal değerine, konumuna ve rastgele listeye dayalı olarak şifrelenmiş görüntüdeki karşılık gelen piksel için yeni bir değer üretir.

3.2 Rastgele Liste Oluşturma

Önerilen yöntemde, denklem 2.3'e göre geliştirici Baker'in eşlemesi kullanılmıştır. Bu eşleme için iki başlangıç değeri ve b adlı bir katsayı gereklidir. Gerekli başlangıç değerleri şifreleme anahtarından elde edilir. Ayrıca, kaotik koşullar yaratmak için b'nin değeri 0 ile 1

arasında değer seçilmelidir. Bu tezde ve önerilen yöntemde *b* katsayısının değeri 0.2 olarak kabul edilmiştir.

Diğer miktarlar, yani x_0 ve y_0, kullanıcının girdiği anahtar kelimeden hesaplanır. Bilindiği üzere anahtar kelimeler birkaç karakterden oluşmaktadır. Karakter sayısında herhangi sınırlama olmamakla birlikte en az sekiz karakter oluşması önerilmektedir. Bu aşamada her karakterin ASCII kod değerinden faydalanarak istenirler değerler hesaplanır. Karakterlerin değerleri ikili sayıya dönüştürülür ve yan yana geldiğinde ikili sayı dizisi elde edilir. Daha sonra ikili sayı dizisini normal sayı ile dönüştürüp, dizinin boyutundaki en büyük sayıya bölerek 0 ile 1 arasında bir sayı elde edilir. Elde edilen sayı x_0 olarak kabul edilebilir. Öte yandan ikili sayının tersini üzerinde aynı işlemleri yaparak y_0 değeri de hesaplayabiliriz. Bu işlemler denklem 3.1 de uygun bir biçimde gösterilmektedir.

$$\begin{cases} x_0 = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{7} k_{i,j}*2^{i*8+j}}{2^{n*8}} \\ y_0 = \frac{\sum_{i=n-1}^{0}\sum_{j=0}^{7} k_{i,j}*2^{i*8+j}}{2^{n*8}} \end{cases} \tag{3.1}$$

Burada $k_{i,j}$, i. karaktere ve onun j. bitine karşılık gelen ikili değerdir. Denklemde göründüğü gibi x_0 değerinin hesaplamasında ikili dizi soldan sağa taranır ve her bit kendi değerine göre diğerleri ile toplanmaktadır. Öte yandan y_0 değerini hesaplamada ayni işlem ikili dizinin sağdan sola dikkate alınarak yapılmaktadır. Bu işlem daha farklı yöntemler ile yapılabilir, örneğin tek ve çift sıralara ayırarak x_0 ve y_0 değerler hesaplanabilir. Biz bu çalışmada başlangıç değerleri elde etmek için denklem 3.1'i kullanmaktayız.

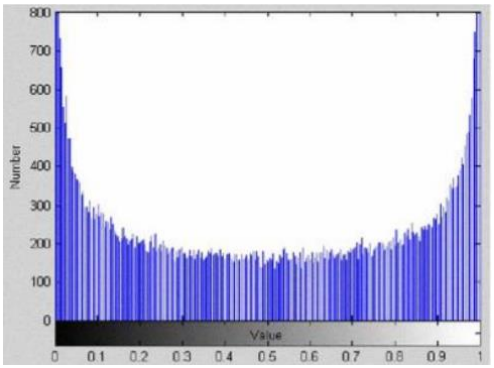
List 3.1. Başlangıç Değerlerin Hesaplanma Algoritması

```
ALGORITHM startPoints (KeyStr)
// Girilen anahtar kelimesinde Baker fonksiyon için başlangıç değerlerin hesaplanması.
//Giriş: Şifreleme anahtarı olarak KeyStr  //Çıktı: x ve y (başlangıç değerler)
k ← 8
sum1, sum2 ← 0
n ← KeyStr.Length
for i ←1 to n:
      sum1 ← sum1 +KeyStr[i]*pow(2,k)
      sum2 ← sum2 +KeyStr[n-i+1]*pow(2,k)
      k ← k +8
x ← sum1/pow(2,k)
y ← sum2/pow(2,k)
return x, y
```

Denklem 3.1 kullanarak x_0 ve y_0 değerler hesaplamak için List 3.1 de gösterildiği gibi algoritma kullanılabilir. Burada anahtar kelimesi *KeyStr* parametresi olarak algoritmaya gönderilir ve algoritmada anahtar kelime boyutuna göre denklem 3.1'e uygulamaktadır. Algoritma sonucunda rasgele listesinde kullanılacak başlangıç değerler hesaplanmaktadır.

Denklem 3.1'ten üretilen x_0 ve y_0 değerler, denklem 2.4'e yerleştirilir ve tekrarlayarak istenilen sayıda 0 ile 1 arasında rastgele sayı dizisi oluşturulur. Üretilen sayılar yöntem gereği 0 ile 255 arasında tam sayılara değişilmesi gerekiyor. Dolaysıyla sayıları 255'e çarparak, tam sayı kısmını kullanabiliriz.

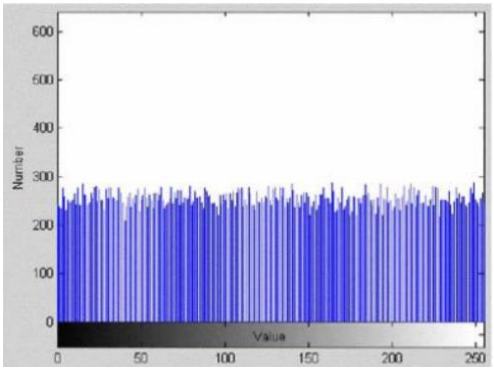
Kaotik sistemlerin özelliklerini araştırmak için sayılar dizisi üretilir ve üretilen sayıların histogram'i incelenir. Genelde uygun rasgele sayı üretim yöntemi eşit dağılımda sayı üretir. Şekil 3.1 normal kaotik sistemden üretilen rasgele sayıların histogram' ini göstermektedir.



Şekil 3.1. Normal Kaotik Sistemlerin Rasgele Sayı Dağıtımı

Şekilde gösterildiği gibi çoğu alanlarda eşit sayıda rasgele sayılar olmasına rağmen, 0 ile 1'e yakın bölgelerde daha fazla sayı üretilmektedir. Dolaysıyla bu bölgelerdeki değerler daha fazla üretilme ihtimale sahipler. Bu sıkıntıyı kaldırmak için üretilen sayılar bir kat sayıya çarpılır. Araştırmalara göre etkili kat sayı değeri 1000000 kabul edilmiştir. Elde edilen sayılar 0 ile 255 arasında olması için kat sayıya çarpılan değer 256 bölünür ve kalan kısmı kullanılır.

Şekil 3.2 da üretilen rasgele sayı, kat sayıya çarpıp ve 256'e kalanı hesaplandıktan sonra incelenmiştir.



Şekil 3.2. Kat Sayısı Kullandıktan Sonra Rasgele Sayı Dağıtımı

Şekilde göründüğü gibi elde edilen rasgele sayılar eşit dağılıma sahip ve her sayı eşit ihtimal ile üretilmektedir. Önerilen yöntem doğrultusunda üretilen rasgele sayılar 256 elemanlı dizide tutulmalıdır. Rasgele sayılar dizisinde tekrarlı sayı olmaması gerekiyor.

Rasgele sayılar dizisini oluşturmak için dizideki 256 elemanının her biri için rasgele bir sayı üretilmelidir. Üretilen sayılar daha önceki elemanlarda mevcut ise atılır ve tekrarsız sayılar üretilene kadar rasgele sayı üretimi tekrarlanır. Sonuçta 256 elemanın her birinde 0 ile 255 arasında tekrarsız sayı yerleştirilir. Eleman sayısı ile sayıların sayısı eşit olduğundan, 0 ile 255 arasında tüm sayılar dizide yerleştirilecektir. List 3.2'de rastgele dizi oluşturma ile ilgili bir algoritma verilmiştir.

List 3.2. Rastgele Liste Oluşturma Algoritması

```
ALGORITHM RandomList (KeyStr, b)
// 0'dan 255'e kadar tekrarlanmayan bir sayı listesi oluşturun.
//Giriş: Şifreleme anahtarı olarak KeyStr, Baker's Map'in kontrol parametreleri
olarak b
//Çıktı: RandList, rasgele sayı listesi
i ← 0
while i<256:
    R ← (xp*yp *1000000) mod 256  // denklem 2.3'ten verilen
    Chk ← 0
    for each L in RandList:
         if R == L then:
               Chk ← 1
     if Chk==0 then:
          RandList[i] ←R
          i++
return RandList
```

Algoritmada göründüğü gibi, her 256 eleman için bir rasgele sayı üretilmektedir. Üretilen rasgele sayı için denklem 2.3 kullanılmaktadır. Üretilen her rasgele sayı önce 1000000'e çarpılır ve daha sonra 256 bölünerek, kalan kısmı kullanılır. Ayrıca üretilen her rasgele sayı daha önceden yerleştirilen sayılar ile karşılaştırılır. Eğer daha önceden sayı başka bir elemanda yerleştirilmiş ise herhangi işlem yapmadan yeni rasgele sayı üretilir, eğer üretilen sayı başka elemanlarda yoksa, elemana yerleştirilir ve diğer elemana geçirilir.

3.3 Görüntü Şifreleme

Bu çalışmanın amacı etkin şekilde görüntüyü şifrelemektir. Daha önce bahsedildiği gibi bir görüntü piksellerden oluşmaktadır. Her pikselin değeri ve konumu var. Piksel değeri, kırmızı, yeşil ve mavi renklerinin miktarını ve konum ise pikselin görüntüde bulunduğu yeri belirlemektedir. Görüntüler matris yapısında olduğundan konumlar satir ve sütun olarak iki değişkende tutulmalı, ancak daha kolay şekilde işlemleri sürdürebilme amacıyla matris yapıda olan verileri bir boyutlu diziye aktarabiliriz.

Matris yapısından dizi yapısına dönüştürmek için önce matrisin ilk satırı, daha sonra ikinci satır ve aynı şekilde diğer satırlar sırasıyla diziye konumlanır. Böylece her pikselin konumu sadece bir değişken ile temsil edilebilir.

Önerilen yöntem iki aşamadan oluşmaktadır: şifreleme ve deşifreleme. Şifreleme / deşifreleme aşamasında daha önceden hazırlanan rasgele dizi kullanılacaktır. Dolaysıyla her pikselin değeri, konumu ve rasgele dizi verileri şifreleme / deşifreleme aşamasında kullanılacaktır. Elbette hem şifreleme hem de şifre çözme adımlarında aynı anahtarın kullanılması gerektiği unutulmamalıdır. Aksi takdirde, deşifreleme işlemi orijinal dosyayı kurtaramaz.

Şifreleme aşamasında görüntüdeki her piksel ayrı ayrı ele alınır ve şifreleme işlemi bunun üzerinde gerçekleştirilir. İlk olarak, matris biçimindeki görüntü dosyası tek boyutlu bir diziye dönüştürülür. Tek boyutlu diziye dönüştürme işlemi, önce bir satırın pikselleri diziye, ardından bir sonraki satırın pikselleri yazılacak şekilde yapılır. Bu işlem, görüntü matrisinin son satırına kadar gerçekleştirilir.

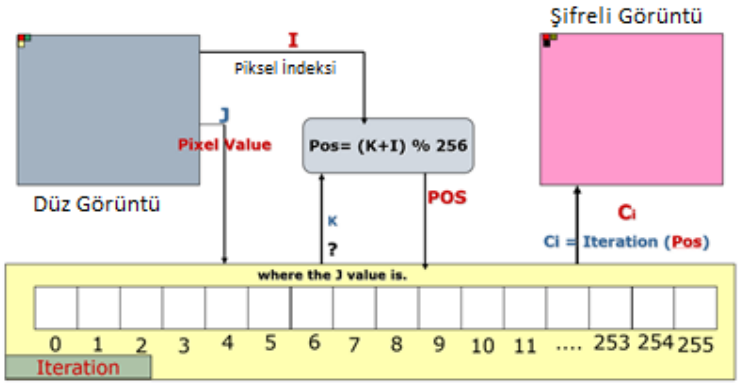
Piksellerden elde edilen dizideki her bir değer okunur ve rastgele oluşturulan listede aranır. Oluşturulan rastgele liste 0'dan 255'e kadar tüm değerlere sahip olduğu için istenen değer listede mevcut olacaktır. Aranan değer bulunduğunda, görüntü dizisinde okunan piksel indeksi ile rastgele listedeki karşılık gelen indeks eklenir ve yeni pozisyon hesaplanır. Elbette bu aşamada elde edilen toplamın kalanı 256 ile hesaplanır ve yeni bir pozisyon olarak kabul edilir.

Son olarak, rastgele listede hesaplanan indeksteki değer, şifrelenmiş bir piksel olarak kabul edilir ve şifreli görüntüdeki karşılık gelen piksele yerleştirilir. Şifreleme işlemi algoritma olarak List 3.3' de gösterilmiştir.

List 3.3. Şifreleme Algoritması

```
ALGORITHM Encryption (Image0,iteration)
// Görüntü şifrelemesi.
//Giriş: Şifrelenecek görüntü olarak Image0, rasgele dizi olarak iteration
//Çıktı: şifrelenmiş görüntü (Image1)
for n ← 0 to nWidth:
    for m ← 0 to mHeight:
       I ← (n*Image0->Width)+m
       R = GetRValue(Image0.Pixels[n][m])
       G = GetGValue(Image0.Pixels[n][m])
       B = GetBValue(Image0.Pixels[n][m])
       for s ← 0 to 255:
           if iteration[s]==R then:   k1 ← s
           if iteration[s]==G then:   k2 ← s
           if iteration[s]==B then:   k3 ← s
       ppR ← iteration [(i+k1) % 255]
       ppG ← iteration [(i+k2) % 255]
       ppB ← iteration [(i+k3) % 255]
       Image1.Pixels[n][m] = RGB(ppR,ppG,ppB);
return Image1
```

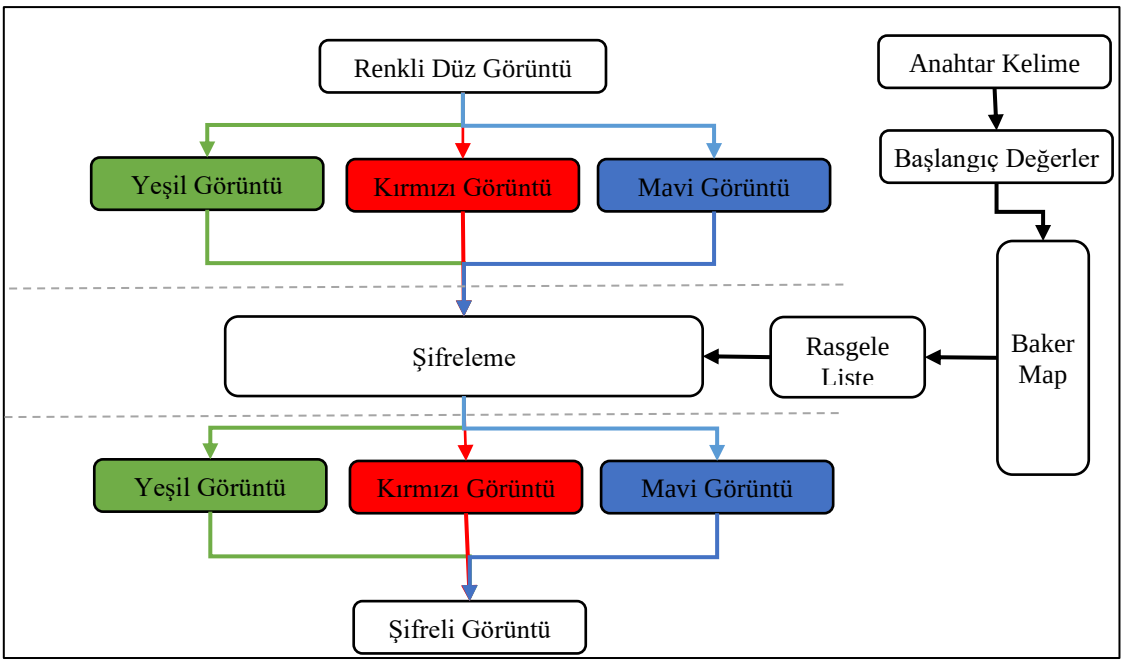
Algoritmada göründüğü gibi, görüntüden elde edilen her piksel için uç renk (RGB) ayrı ayrı şifrelenir. Algoritma sonunda şifrelenmiş katmanlar birleştirerek şifrelenmiş görüntü elde edilmektedir. Şifreleme aşaması ile ilgili işlem Şekil 3.3'de açıkça gösterilmiştir.



Şekil 3.3. Görüntü Şifreleme ile İlgili İşlemler

Şekil 3.3 de göründüğü gibi bir pikselin değerini değiştirmek için, bulunduğu konumu, kendi değeri ve rasgele sayılardan oluşan liste kullanılmaktadır. Burada Piksel değeri rasgele listede aranır, rasgele listede bulunduğu konum ile pikselin konumu toplanarak yeni konum hesaplanır. Konum 255'den fazla olmaması için 256 ile kalanı alınır. Rasgele listede yeni konumda bulunan değer şifrelenmiş görüntüye eklenir. Bu işlem tüm orijinal görüntü için yapılınca şifrelenmiş görüntü elde edilir.

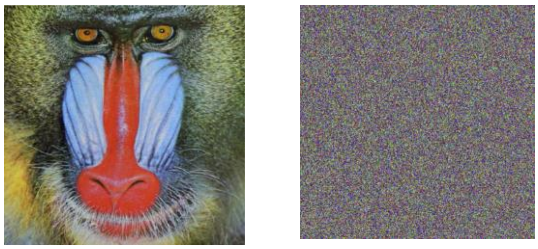
Şifreli görüntü verilerinin rastgele listeden sağlandığı göz önüne alındığında, değerler 0 ile 255 arasında olacak ve sayısal görüntü veri aralıkları ile ilgili herhangi bir sorun olmayacaktır. Şekil 3.4, genel olarak renkli görüntü için şifreleme işlemini göstermektedir.



Şekil 3.4. Şifreleme Genel Yöntemi

Şekil 3.4 de göründüğü gibi renkli görüntülerin şifrelemesi için önce görüntü uç farklı katmanlara ayırarak, her katman üzerine şifreleme işlemi gerçekleştirilir. Daha sonra şifrelenmiş katmanlar birleştirilerek şifreli görüntü elde edilir.

Önerilen yöntemin nasıl çalıştığını göstermek için Matlab kullanarak şifreleme fonksiyonu geliştirilmiştir. Şekil 3.5, bir görüntü dosyası ve bunun geliştirilen fonksiyondan elde edilen şifrelenmiş görüntüsünün bir örneğini göstermektedir.



(a) (b)

Şekil 3.5. Bir görüntü ve Üç Rengi için Şifreleme Aşaması. (a) Düz Görüntü, (b) Şifreli Görüntü

3.4 Görüntü DeŞifreleme

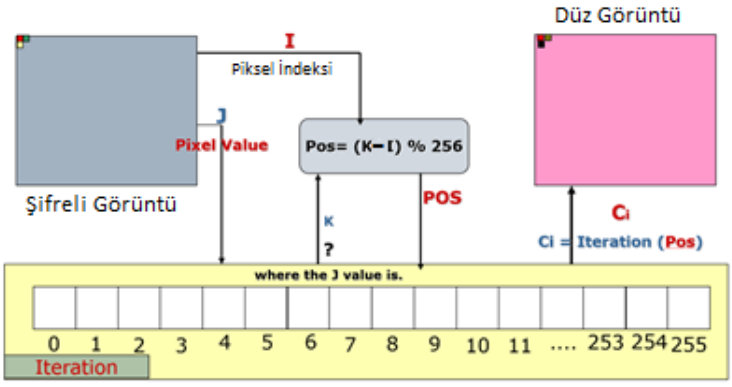
Kaos sistemlerine dayalı çoğu yöntemin sahip olduğu önemli özelliklerden biri mod gibi tersinir operatörlerin kullanılmasıdır. Bu özellik, şifre çözme aşamasını şifreleme aşamasına çok benzer hale getirir. Bu çalışmanın önerilen yönteminde de aynı şekildedir. Bu aşama ile Şifreleme aşaması arasındaki tek fark, yeni dizin hesaplanırken rastgele liste ve görüntü dizisinin endekslerinin çıkarılması ve kalanın 256 olmasıdır. Geri kalan durumlar şifreleme işlemine birebir benzer.

Aynen şifrelemede olduğu gibi, piksellerden elde edilen dizideki her bir değer okunur ve rastgele oluşturulan listede aranır. Oluşturulan rastgele liste 0'dan 255'e kadar tüm değerlere sahip olduğu için istenen değer listede mevcut olacaktır. Aranan değer bulunduğunda, görüntü dizisinde okunan piksel indeksi, rastgele listedeki karşılık gelen indeksinden çıkarılır ve yeni pozisyon hesaplanır. Elbette bu aşamada elde edilen toplamın kalanı 256 ile hesaplanır ve yeni bir pozisyon olarak kabul edilir. Son olarak, rastgele listede hesaplanan indeksteki değer, şifrelenmiş bir piksel olarak kabul edilir ve düz görüntüdeki karşılık gelen piksele yerleştirilir. Deşifreleme işlemi algoritma olarak List 3.4' te gösterilmiştir.

List 3.4. Deşifreleme Algoritması

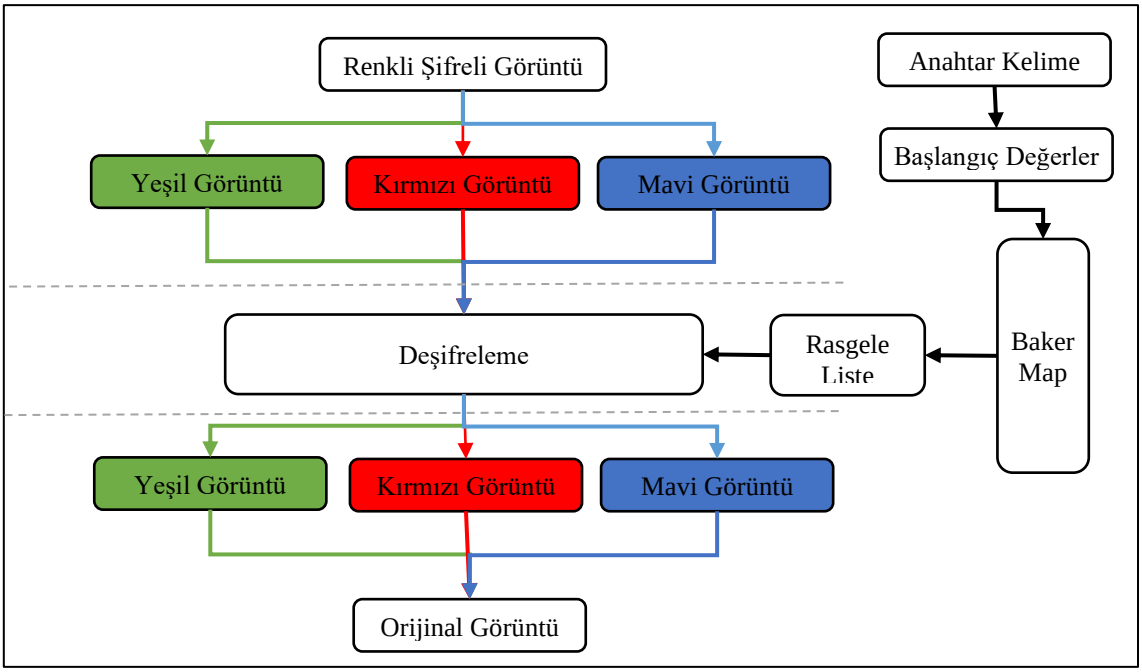
```
ALGORITHM Decryption (Image1,iteration)
// Görüntü deşifrelemesi.
//Giriş: Deşifrelenecek görüntü olarak Image1, rasgele dizi olarak iteration
//Çıktı: Düz görüntü (Image0)
for n ← 0 to nWidth:
    for m ← 0 to mHeight:
       I ← (n*Image0->Width)+m
       R = GetRValue(Image1.Pixels[n][m])
       G = GetGValue(Image1.Pixels[n][m])
       B = GetBValue(Image1.Pixels[n][m])
       for s ← 0 to 255:
           if iteration[s]==R then:   k1 ← s
           if iteration[s]==G then:   k2 ← s
           if iteration[s]==B then:   k3 ← s
       ppR ← iteration [(i-k1) % 255]
       ppG ← iteration [(i-k2) % 255]
       ppB ← iteration [(i-k3) % 255]
       Image0.Pixels[n][m] = RGB(ppR,ppG,ppB);
return Image0
```

Algoritmada göründüğü gibi, şifrelenmiş görüntüden elde edilen her piksel için uç renk (RGB) ayrı ayrı deşifrelenir. Algoritma sonunda deşifrelenmiş katmanlar birleştirerek düz görüntü elde edilmektedir. Deşifreleme aşaması ile ilgili işlem Şekil 3.6'de açıkça gösterilmiştir.



Şekil 3.6. Deşifreleme ile İlgili İşlemler

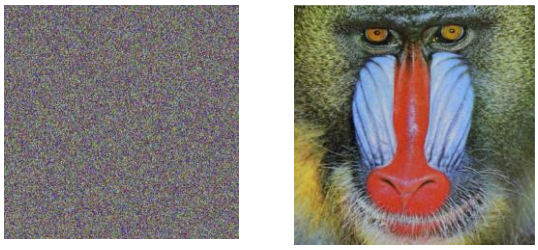
Şekil 3.7, genel olarak renkli görüntü için deşifreleme işlemini göstermektedir.



Şekil 3.7. Deşifreleme Genel Yöntemi

Şekil 3.7 de göründüğü gibi renkli görüntülerin deşifrelenmesi için önce görüntü uç farklı katmanlara ayırarak, her katman üzerine deşifreleme işlemi gerçekleştirilir. Daha sonra deşifrelenmiş katmanlar birleştirilerek orijinal görüntü elde edilir.

Şekil 3.8, bir şifrelenmiş görüntü ve elde edilen orijinal görüntüsünün bir örneğini göstermektedir.



(a) (b)

Şekil 3.8. Bir Görüntü ve Üç Rengi için Deşifreleme Aşaması. (a) Şifreli Görüntü, (b) Orijinal Görüntü

3.5 Önerilen Yöntemin Güvenlilik Analizleri

Önerilen herhangi şifreleme sisteminin iyi olup olmadığını incelenmesi gerekiyor. Bu incelemede işlemin kriptanalitik, kaba kuvvet ve istatistiksel ataklara karşı dayanaklık olması araştırılır. Bu amaçla sistemden elde edilen görüntüler, orijinal görüntüler ile karşılaştırılır. Karşılaştırma işlemlerin başarım ölçülendirmek için bazı güvenlik testler yapılabilir.

Önerilen sistemin etkinliğini görmek için şifreleme/deşifreleme algoritmasını Matlab ortamında uyguladık. Uygulanan algoritmada kullanıcı, görüntüyü şifrelemek için bir metin dizisi de olabilen şifreleme anahtarını girer. İstenen algoritma, alınan anahtara göre rastgele bir liste oluşturur ve orijinal görüntüyü şifreler. Görüntü şifrelemede, üç görüntü katmanının verileri ayrı ayrı ele alınır ve her katman ayrı ayrı şifrelenmiş katmanı oluşturur. Şifrelenmiş katmanların birleştirilmesiyle de şifrelenmiş görüntü elde edilir.

Şifreleme işleminin geri dönüşüm şeklinde de doğru çalışmalı. Şifrelenmiş görüntünün şifresini tekrar aynı önceki anahtarla çözersek orijinal görüntü elde edilmelidir. Şifrelenmiş görüntünün şifrelenmiş anahtardan farklı bir anahtarla şifresinin çözüldüğünü varsayalım. Bu durumda elde edilen görüntü, orijinal görüntü ile hiçbir benzerliği olmamalıdır. Şekil 3.9 bunu açıkça göstermektedir.

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

Şekil 3.9. (a) Düz Görüntü, (b) Anahtar$_1$ ile Şifrelenmiş Görüntü, (c) Anahtar$_1$ ile Şifresi Çözülmüş Görüntü, (d) Anahtar$_2$ ile Şifresi Çözülmüş Görüntü

3.5.1 Diferansiyel Analiz

Diferansiyel saldırılar, saldırganların şifrelenmiş görüntüler için kullandığı önemli özelliklerden biridir. Diferansiyel kriptografi, değişen girdi verilerinin çıktıları üzerindeki etkisinin incelenmesi olarak düşünülebilir. En iyi görüntü şifreleme algoritmaları, farklı saldırılara karşı daha dirençli olanlardır. Bu nedenle görüntü şifreleme algoritmaları, giriş bilgisinde veya kaynak görüntüde yüksek hassasiyete sahip olmalıdır. Piksel Sayısı Değişim Hızı (NPCR) ve Entegre Ortalama Değişim Yoğunluğu (UACI), düz metin ve anahtar kelimesine duyarlılığı ölçer. Bu, girdi orijinal görüntüde bir pikseli değiştirirsek çıktı bilgisinin (şifrelenmiş görüntü) etkisi anlamına gelir.

Diferansiyel saldırılarda genellikle görüntüdeki bir biti değiştirerek şifrelenmiş görüntüyü analiz edebilecek bağlantılar bulmaya çalışırlar. Şifreleme sistemi, bir bit değiştirilerek birçok farklı şifrelenmiş görüntünün üretilmesi koşulunu yaratırsa, diferansiyel saldırılara karşı dirençli olabilir. Genellikle sistemin diferansiyel saldırılara karşı etkinliğini

analiz etmek için iki önemli kriter incelenir. Bu ölçülerden biri piksel değişim oranlarının (NPCR) sayısı, diğeri ise birleşik ortalama değişim yoğunluğudur (UACI). Bu iki ölçüyü hesaplamak için denklem 3.2 ve3.37 ilişkileri kullanılabilir.

$$NPCR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} C(i,j)}{N*M} * 100\%, \quad (3.2)$$

$$UACI = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} |P_1(i,j) - P_2(i,j)|}{255*N*M} * 100\% \quad (3.3)$$

M ve N değerleri görüntünün uzunluğunu ve genişliğini gösterir. Ayrıca, P_1(i, j) bir görüntünün değişikliklerden önceki piksel değeri olarak kabul edilirse, P_2 (i, j) aynı pikselin değişikliklerden sonraki değeridir. Tablo 3.1, alfanın 0,001'e eşit olduğu durum için birkaç standart görüntü için bu iki ölçümle ilgili analizleri göstermektedir.

Tablo 3.1. (122.102)'de Bir Pikseli Değiştirerek NPCR ve UACI Analizi.

Image Name	NPCR	UACI	NPCR		UACI	
			Sınır	Durum	Sınır	Durum
Peppers (512*512)	99.6028	33.6092	99.5810	Geçti	33.1594 33.7677	Geçti
Mandrill (512*512)	99.6203	33.4541	99.5810	Geçti	33.1594 33.7677	Geçti
Lena (256*256)	99.5636	33.4512	99.5527	Geçti	33.1594 33.7677	Geçti

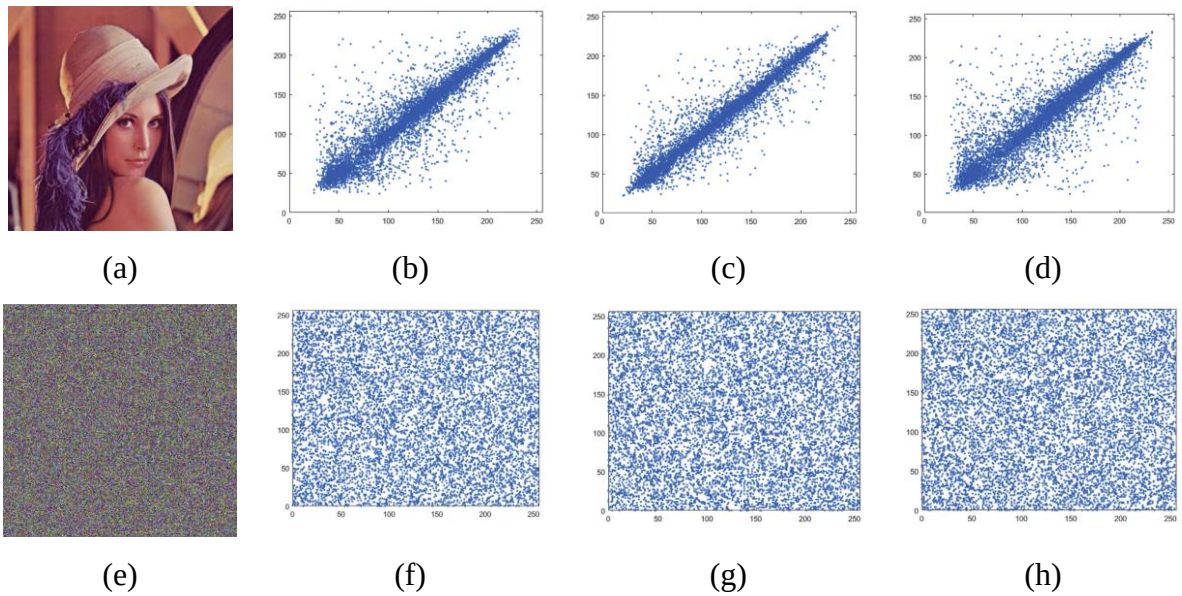
Tablo 3.1'de görülebileceği gibi, incelenen iki ölçüm kabul edilebilir değerlere sahiptir. Bu nedenle, bu yöntem diferansiyel saldırılara etkili bir şekilde direnebilir.

3.5.2 İstatistiksel Analizler

3.5.2.1 Korelasyon katsayısı

İki değişken arasındaki ilişkinin derecesini, yoğunluğunu ve kuvvet seviyesini ve yönünü belirlemek için basit korelasyon analizi yapılır. Her iki değişken de sürekli değişken ise ve değişkenlere ilişkin veriler normal dağılım gösteriyorsa değişkenler arasındaki ilişki Pearson korelasyon katsayısı ile belirlenir. Korelasyon katsayısı ile belirlenen veya ölçülen istenen değişkenler arasındaki doğrusal bir ilişkidir. Değişkenler arasındaki ilişki doğrusal değilse, hesaplanan korelasyon katsayısı değişkenler arasındaki ilişkiyi ölçmek için uygun değildir.

Burada, görüntülerin komşu pikseller arasında doğrusal ilişkilere sahip olup olmadığını belirlemek için Şekil 3.10'de gösterilen analiz yapıldı.



Şekil 3.10. İki Bitişik Pikselin Korelasyonu (a) Lena'nın Düz Görüntüsü; (b) Düz Görüntünün Dikey Korelasyonu; (c) Düz Görüntünün Yatay Korelasyonu; (d) Düz Görüntünün Diyagonal Korelasyonu; (e) Lena'nın Şifreli Görüntüsü; (f) Şifreli Görüntünün Dikey Korelasyonu;

Pikseller arasındaki korelasyonu daha iyi kontrol etmek için şifrelenmiş görüntülerin korelasyon katsayısı da hesaplanabilir. Bu yazıda önerilen yöntemin korelasyon katsayısını diğer bazı yöntemlerle karşılaştırdık. Tablo 3.2, Lena görüntüsü için bu karşılaştırmayı göstermektedir.

Tablo 3.2. Önerilen Yöntem ve Bazı Farklı Yöntemler için Korelasyon Kıyaslaması

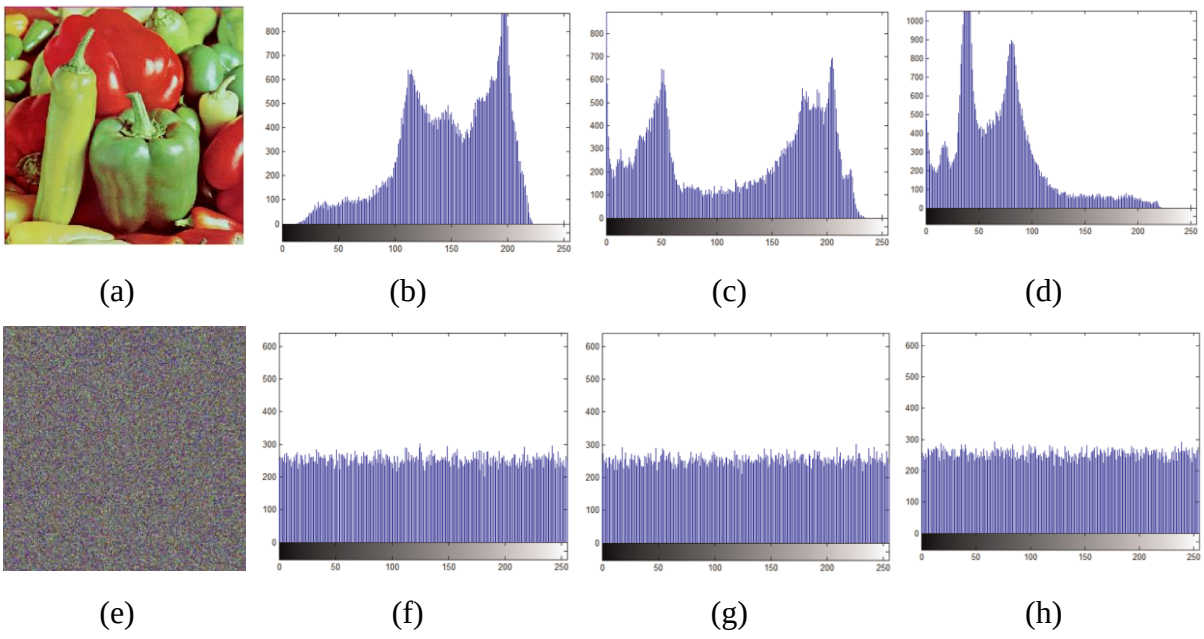
	Dikey	Yatay	Çapraz
Düz Lena Image	0.9883	0.9906	0.9823
(Wang vd., 2019:2816)	0.0003	0.0027	0.0012
(Chai, 2017:1170)	0.0014	0.0285	0.0013
(Zhang vd., 2018:6658)	0.0226	0.0245	0.0193
(Alawida vd., 2019:54)	-0.0017	-0.0084	-0.0019
Önerilen Metot	0.0049	0.0051	0.0011

Tablo 3.2'ye göre önerilen yöntemin diğer yöntemlere kıyasla net bir görüntüde güçlü bir etkileşimi önemli ölçüde azalttığı görülmektedir.

3.5.2.2 Histogram Analizi

Görüntüler için histogram, o görüntüdeki piksellerin dağılımını gösterir. Görüntülerin histogramları normalde eşit olmayan bir dağılıma sahipken, şifreli görüntüler tek tip histogram dağılımında olmalıdır. Bir görüntünün histogram dağılımı ne kadar düzgün olursa, istatistiksel saldırılara karşı o kadar dirençli olur. Çünkü bu tür görüntülerde kriptografik bir saldırıda kullanılacak görüntülerden herhangi bir istatistiksel bilgi çıkarılamaz.

Histogram analizi, bir görüntü şifreleme sisteminin etkinliğini gösterebilen analizler arasındadır. Dengeli histogramlara sahip görüntüler istatistiksel analize daha dirençlidir. Genellikle görüntüler dengeli histogramlardan oluşmaz; şifrelenmiş görüntü dengeli değilse, bilgisayar korsanlarına görüntü analizi için veri sağlayabilir. Bu nedenle, bir şifreleme sisteminin amaçlarından biri, dengeli bir histogram ile şifrelenmiş görüntüler oluşturmaktır. Şekil 3.11, bu tezde önerilen sistemin başarılı bir şekilde dengeli dağılımını göstermektedir.



Şekil 3.11. (a) Düz Görüntü, (b) Düz Görüntünün R Histogramı, (c) Düz Görüntünün G Histogramı, (d) B Düz Görüntünün Histogramı, (e) Şifreli Görüntü, (f) R Şifreli Görüntünün Histogramı, (g) G Cipher Görüntüsünün Histogramı, (h) B Cipher Görüntüsünün Histogramı,

3.5.3 Bilgi Entropisi

Bilgi teorisinde entropi, rastgele sayılar arasında sonsuz bir ilişki bulmak anlamına gelir. Bu ifade Shannon'ın entropisine dayanmaktadır ve denklem 3.4 ile özetlenebilir.

$$H(S) = \sum_{i=0}^{2N-1} P(s_i)\log\left(\frac{1}{P(s_i)}\right) \quad (3.4)$$

Bu ifadenin değeri küçük bir değere eşit ise istatistiksel analiz için daha uygundur. Bu nedenle uygun bir şifreleme yöntemi, şifrelenmiş görüntüdeki bu ifadenin değerini mümkün olduğunca yüksek yapmalıdır.

Tablo 3.3. Bazı Düz ve Şifreli Görüntülerin Entropi Sonuçları.

Görüntü	Düz Görüntü	Şifreli Görüntü
Lena	7.4472	7.9993
Peppers	7.6698	7.9975
House	7.0686	7.9963
Mandrill	7.7624	7.9991

Tablo 3.4. Entropi Sonuçlarını Karşılaştırma

Görüntü	Düz	Önerilen yöntem	(Wang vd., 2019:2813)	(Chai, 2017:1173)	(Zhang vd., 2018:6665)	(Alawida vd., 2019:54)
Lena	7.4472	7.9993	7.9993	7.9993	7.9885	7.9975

4. SONUÇ

Bu tezde, görüntü şifreleme için bir yöntem önerilmiştir. Önerilen yöntem, geliştirilmiş Baker haritasına dayalı olarak geliştirilmiştir. Geliştirilen haritanın temel özelliği kaotik haritalarda dinamik yıkım sorununu çözmüş olmasıdır. Ayrıca, kaotik işlevlerin yüksek duyarlılığı nedeniyle, bu tezde önerilen sistem, şifreleme anahtarına büyük ölçüde bağlıdır. Bu anlamda görüntü şifreleme için uygundur. Sonuçların analizleri, önerilen sistemin saldırılara ve şifreli görüntülerin yetkisiz kullanımına karşı yeterli güvenliğe sahip olduğunu göstermektedir. Ortak dijital ortamlarda yayınlanan verilerin her geçen gün artması nedeniyle yeni şifreleme sistemleri geliştirme ihtiyacı oldukça ciddidir. Önceki ve mevcut yöntemler, bilgisayar korsanları ve yetkisiz kullanıcılar tarafından incelenip analiz edildiğinden, geliştirilen yöntemler güvenilirliğini kaybedecektir. Bu nedenle saldırılara karşı yeni ve daha dirençli yöntemler geliştirmek, ortak ve ortak ortamları kullanma konusunda daha fazla güven getirebilir.

KAYNAKÇA

Abd-El-Atty, B., Iliyasu, A. M., Alanezi, A., & Abd El-latif, A. A. (2021). Optical image encryption based on quantum walks. *Optics and Lasers in Engineering*, 138, 106403.

Alawida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A new hybrid digital chaotic system with applications in image encryption. *Signal Processing*, 160, 45-58

Anandkumar, R., and Kalpana, R. (2020). A Review on Chaos-Based Image Encryption Using Fractal Function. In *Examining Fractal Image Processing and Analysis* (pp. 23-37). IGI Global.

Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. *The Journal of Supercomputing*, 75(10), 6663-6682.

Bak, P., Tang, C., & Wiesenfeld, K. (1988). Self-organized criticality. *Physical review A*, 38(1), 364.

Beek, P. J. (1989). Timing and phase locking in cascade juggling. *Ecological Psychology*, 1(1), 55-96.

Chai, X. (2017). An image encryption algorithm based on bit level Brownian motion and new chaotic systems. *Multimedia Tools and Applications*, *76*(1), 1159-1175.

Chen, L., Chen, J., Zhao, G., & Wang, S. (2019). Cryptanalysis and improvement of a chaos-based watermarking scheme. *IEEE Access*, 7, 97549-97565.

Crilly, A. J., Earnshaw, R., & Jones, H. (Eds.). (2012). Fractals and chaos. *Springer Science & Business Media*.

Darwish, S. M., and Noori, Z. H. (2018). Secure image compression approach based on fusion of 3D chaotic maps and arithmetic coding. *IET Signal Processing*, 13(3), 286-295.

Dou, Y., & Li, M. (2020). Cryptanalysis of a new color image encryption using combination of the 1d chaotic map. *Applied Sciences*, 10(6), 2187.

Gu, G., & Han, G. (2006, September). An enhanced chaos based image encryption algorithm. In First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06) (Vol. 1, pp. 492-495). IEEE.

Hasimoto-Beltrán, R. (2008). High-performance multimedia encryption system based on chaos. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 18(2), 023110.

Hayes, S., Grebogi, C., & Ott, E. (1993). Communicating with chaos. *Physical review letters*, 70(20), 3031.

Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. *Information Sciences*, 480, 403-419.

Kumar, M., Saxena, A., & Vuppala, S. S. (2020). A survey on chaos based image encryption techniques. In *Multimedia security using chaotic maps: principles and methodologies* (pp. 1-26). Springer, Cham.

Li, S.J., Chen, G.R., Mou, X.Q. (2004). On the dynamical degradation of digital piecewise linear chaotic maps. *Int. J. Bifurc. Chaos* 15, 3119–3151

Lima, J. B., & da Silva Neto, E. F. (2016). Audio encryption based on the cosine number transform. *Multimedia Tools and Applications*, 75(14), 8403-8418.

Liu, S., Guo, C., & Sheridan, J. T. (2014). A review of optical image encryption techniques. *Optics & Laser Technology*, 57, 327-342.

Liu, L., & Miao, S. (2017). Delay-introducing method to improve the dynamical degradation of a digital chaotic map. *Information Sciences*, 396, 1-13.

Liu, L., Xiang, H., & Li, X. (2021). A novel perturbation method to reduce the dynamical degradation of digital chaotic maps. *Nonlinear Dynamics*, 103(1), 1099-1115.

Lorenz, E. N. (1965). On the possible reasons for long-period fluctuations of the general circulation. In Proc. WMO-IUGG Symp. on Research and Development Aspects of Long-Range Forecasting.

Mahto, D. K., & Singh, A. K. (2021). A survey of color image watermarking: State-of-the-art and research directions. *Computers & Electrical Engineering*, 93, 107255.

Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In *ISSA* (Vol. 1, No. 2, pp. 1-11).

Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., and Mosavi, M. R. (2015). A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. *Multimedia Tools and Applications*, 74(3), 781-811.

Pisarchik, A. N., Flores-Carmona, N. J., & Carpio-Valadez, M. (2006). Encryption and decryption of images with chaotic map lattices. Chaos: An *Interdisciplinary Journal of Nonlinear Science*, 16(3), 033118.

Sangwan, N. (2012). Text encryption with huffman compression. *International Journal of Computer Applications*, 54(6).

Singh, L. D., & Singh, K. M. (2015). Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, 54, 73-82.

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. *IEEE access*, 9, 23409-23423.

Suneja, K., Dua, S., & Dua, M. (2019, March). A review of chaos based image encryption. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 693-698). IEEE.

Talhaoui, M. Z., and Wang, X. (2021). A new fractional one-dimensional chaotic map and its application in high-speed image encryption, *Information Sciences*, 550, 13-26.

Wadhera, S., Kamra, D., Rajpal, A., Jain, A., & Jain, V. (2022). A Comprehensive Review on Digital Image Watermarking. *arXiv preprint arXiv*:2207.06909.

Wang, X. Y., Yang, L., Liu, R., and Kadir, A. (2010). A chaotic image encryption algorithm based on perceptron model, *Nonlinear Dynamics*, 62(3), 615-621.

Wang, X., Feng, L., Li, R., & Zhang, F. (2019). A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. *Nonlinear Dynamics*, *95*(4), 2797-2824.

Weisstein, E. W. (2001). Logistic map. *https://mathworld. wolfram. com/*.

Yan, X., Wang, X., & Xian, Y. (2021). Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. *Multimedia Tools and Applications*, 80(7), 10949-10983.

Zhang, Y., & Tang, Y. (2018). A plaintext-related image encryption algorithm based on chaos. *Multimedia Tools and Applications*, *77*(6), 6647-6669.