KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KELEBEK OPTİMİZASYON ALGORİTMASI İLE KAOTİK TABANLI GÖRÜNTÜ ŞİFRELEME

YÜKSEK LİSANS

AHU KARABULUT

Mühendislik Bilimleri Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Dr. Öğr.Üyesi Uğur ERKAN

TEMMUZ 2021

KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KELEBEK OPTİMİZASYON ALGORİTMASI İLE KAOTİK TABANLI GÖRÜNTÜ ŞİFRELEME

YÜKSEK LİSANS TEZİ

AHU KARABULUT

180825225

Mühendislik Bilimleri Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Dr. Öğr.Üyesi Uğur ERKAN

İkinci Danışman: Doç. Dr. Abdurrahim TOKTAŞ

TEMMUZ 2021

TEZ ONAYI

Ahu KARABULUT tarafından hazırlanan KELEBEK OPTİMİZASYON ALGORİTMASI İLE KAOTİK TABANLI GÖRÜNTÜ ŞİFRELEME adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Karamanoğlu Mehmetbey Üniversitesi Fen Bilimleri Enstitüsü Mühendislik Bilimleri Ana Bilim Dalı'nda Bilgisayar Mühendisliği **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman:	İkinci Danışman:
Dr.Öğr.Üyesi Uğur ERKAN	*Doç.Dr.Abdürrahim TOKTAŞ*

Jüri Üyeleri İmza:

Doç.Dr. Metin TOZ

Doç.Dr. Kemal ADEM

Dr.Öğr.Üyesi Uğur ERKAN

Tez Savunma Tarihi: 08/07/2021

Yukarıdaki sonucu onaylarım

Ünvanı, Ad SOYAD

Enstitü Müdürü

Doç.Dr. Ahmet KAYABAŞI

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Ahu KARABULUT

Rahmetli babama ve canım anneme

ÖNSÖZ

KELEBEK OPTİMİZASYON ALGORİTMASI İLE KAOTİK TABANLI GÖRÜNTÜ ŞİFRELEME adlı çalışmada, yeni bir kaotik harita ve kelebek optimizasyon algoritması kullanılarak görüntü şifreleme işlemi gerçekleştirilmiştir.

Bu çalışmanın gerçekleştirilmesinde çok emeği olan destek ve katkılarından dolayı danışmanım Dr. Öğr.Üyesi Uğur ERKAN'a sonsuz teşekkürlerimi sunarım.

Çalışmalarımı gerçekleştirirken destek ve katkıları olan ikinci danışmanım Doç. Dr. Abdurrahim TOKTAŞ'a teşekkür ederim.

Tez çalışmam süresince yanımda olan aileme özelliklede hayatımın dönüm noktalarında yönlendirmeleriyle abime, sabrı ve pozitif düşünmeyi öğreten sevgili anneme ve beni bu günlere kadar getiren okumam için desteğini esirgemeyen azim ve çalışma duygusunu aşılayan rahmetli babama sonsuz teşekkür ederim.

Temmuz 2021 Ahu KARABULUT

İÇİNDEKİLER

Sayfa

KISALTMALAR

AES **:** Advanced encryption Standard

DES **:** Data encryption Standard

IDEA **:** International Data encryption Algorithm

NPCR **:** Number of Pixels Change Rate

UACI : Unified Average Changing Intensity

FPGA : Field Programmable Gate Arrays

BOA : Butterfly Optimizaton Algorithm-Kelebek Optimizasyon Algoritması

GA : Genetic Algorithm -Genetik Algoritma

PSO : Particle Swarm Optimization-Parçacık Sürü Algoritması

ACO **:** Ant Colony Algorithm-Karınca Kolonisi Algoritması

3DES **:** Üçlü Veri şifreleme Standardı

RSA **:** Rivest–Shamir–Adleman

SE **:** Sample Entropi

PE **:** Permütasyon Entropi

LE **:** Lyspunov Entropi

1D **:** 1 Boyutlu (One Dimension)

IEEE **:** Institute of Electrical and Electronics Engineers

1DSP-IE **:** One-dimensional sinusoidal image encryption- Bir boyutlu sinüslü çalışan görüntü şifreleme

1CS-IE **:** One-cosine sinusoidal image encryption-1 Boyutlu kosinüs ve sinus ile görüntü şifreleme

SEMBOLLER

P(n) **:** Bilgi entropi

H(m) **:** Bilgi Rastgeleliği

$\bar{H}_{kT_B}(m)$ **:** Yerel Shannon entropisi

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

ÖZET

Yüksek Lisans

KELEBEK OPTİMİZASYON ALGORİTMASI İLE KAOTİK TABANLI GÖRÜNTÜ ŞİFRELEME

Ahu KARABULUT

Karamanoğlu Mehmetbey Üniversitesi

Fen Bilimleri Enstitüsü

Mühendislik Bililmleri Ana Bilim Dalı

Danışman: Dr. Öğr.Üyesi Uğur ERKAN

2. Danışman: Doç. Dr. Abdurrahim TOKTAŞ

07, 2021, 81 sayfa

Teknolojinin gelişmesi ile birlikte, artan multimedya ve iletişim araçları veri transferini hızlandırmıştır. Veri transferinde en çok kullanılan veri tiplerinden birisi digital görüntülerdir. Digital görüntüler gizli ve mahrem bilgiler içerebilir. Bu nedenle, görüntüler herkese açık ağ üzerinde gönderildiğinde karşı tarafa şifreli olarak iletilmelidir.

Görüntü şifreleme işlemlerinde en çok kullanılan yöntem kaosa dayalı yöntemlerdir. Kaosa dayalı yöntemler de kaotik haritalar kullanılmaktadır. Bu tez çalışmasında bir boyutlu yeni bir kaotik harita önerilmiştir. Önerilen bu kaotik harita en yaygın performans testlerinde başarılı sonuçlar vermiştir. Bir çok görüntü şifreleme uygulamasında optimizasyon teknikleri görüntünün tamamı uygulandığı için gerçek zamanlı kullanmak mümkün olmamaktadır. Bu çalışmada ise, Kelebek Optimizasyon Algoritması (Butterfly Optimization Algorithm-BOA)'nı kullanarak görüntü entropi değerini maksimum ve bitişik pikseller arası korelasyonu minumum yapacak anahtarı bulmaya dayalı bir şifreleme yöntemi önerilmiştir. Optimizasyon algoritmasını gerçek zamanlı uygulamalarda kullanılabilmek için görüntü üzerinde 80 x 80'lik bir kesitte optimum anahtar aranmaktadır. Daha sonra, optimum anahtar ile görüntünün tamamı şifrelenmektedir.

Yeni önerilen görüntü şifreleme sisteminin performansını ölçmek için, 10 adet en yaygın kullanılan görüntüler üzerinde histogram analizi, korelasyon analizi, local entropi, global entropi, anahtar duyarlılık analizi, korelasyon analizi, diferansiyel atak analizi, gürültü ve veri kaybı analizi, seçilen açık metin saldırısına ve bilinen açık metin saldırısı analizi ve hız analizi gibi bazı güvenlik testleri uygulandı. Elde edilen bulgular, tasarlanan sistemin görüntü şifrelemek için yüksek güvenlik seviyesine sahip olduğunu doğrulamaktatır.

AnahtarKelimeler: Görüntü şifreleme, kelebek optimizasyon algoritması, Lojistik harita

ABSTRACT

MsThesis

CHAOS-BASED IMAGE ENCRYPTION USING BUTTERFLY OPTIMIZATION ALGORITHM

Ahu KARABULUT

Karamanoğlu Mehmetbey University

Graduate School of Natural andAppliedSciences

Department of Engineering Sciences

Supervisor: Dr. Öğr.Üyesi Uğur ERKAN

2. Supervisor: Asst. Prof. Abdürrahim TOKTAŞ

07, 2021, 81 pages

Increasing multimedia and communication tools have accelerated data transfer with the development of technology. One of the most used data types in data transfer is digital images. Digital images may contain confidential information. Therefore, when images are sent over the public network, they must be transmitted encrypted to the other party.

Chaos-based methods are the most widely used method in image encryption processes. Chaotic maps are also used in methods based on chaos. In this thesis, a new one-dimensional chaotic map is proposed. This proposed chaotic map has yielded successful results in the most common performance tests. In many image encryption applications, it is not possible to use real-time optimization techniques because the entire image is applied. In this study, an encryption method based on finding the key that will maximize the image entropy value and minimize the adjacent pixels correlation using the Butterfly Optimization Algorithm (BOA) is proposed. In order to use the optimization algorithm in real-time applications, the optimum key is sought in an 80 x 80 section on the image. Then, the whole image is encrypted with the optimum key.

To measure the performance of the system, histogram analysis, correlation analysis, local entropy, global entropy, key sensitivity analysis, correlation analysis, differential attack analysis, noise and data loss analysis, occlusion-attack analysis, known plaintext attack, chosen plaintext attack analysis and speed analysis were applied. The findings confirm that the designed system has a high security level for image encryption.

Keywords: Image encryption, Butterfly optimization algorithm, Logistic map

1. GİRİŞ

Teknolojinin hızla gelişmesi ve hayatlarımıza dâhil olması nedeniyle internet erişiminin olduğu cihazlara ulaşım kolaylaşmakta ve bu sayede internet kullanımı gittikçe artmaktadır. İnternet üzerinden (herkese açık ağlar) dijital görüntülerin iletilmesi nedeniyle, güvenli olmayan internet ortamında yer alan bilgi iletimi gün geçtikçe artmaktadır (Nadhom ve Loskot, 2018). Bu nedenle herkese açık ağlar üzerinden iletilen bilgileri korumak çok önemli hale geldi. Özellikle, kritik öneme sahip askeri görüntü verileri, gizli video konferans, medikal görüntüleme sistemi, kablolu TV gibi birçok uygulama dijital görüntüleri depolamak ve iletmek için hızlı ve sağlam bir güvenlik sistemine ihtiyaç duyar. Dijital görüntülerin veri fazlalığı ve bitişik pikseller arasında güçlü korelasyon gibi özelliklerinden dolayı metin şifrelemede kullanılan yöntemlerin görüntü şifrelemede kullanılması uygun değildir. Metin şifrelemede kullanılan IDEA (International Data Encryption Algorithm), DES (Data Encryption Satandart), 3DES (3 Data Encryption Satandart), AES (Advanced Encryption Satandart), RSA (Rivest-Shamir-Adleman) and Blowfish vb. gibi geleneksel metin şifreleme algoritmaları, büyük bir hesaplama süresi ve hesaplama gücü gerektirdiği için gerçek zamanlı görüntü şifrelemeye uygun değildir (Belazi, Abd El-Latif ve Belghith, 2016; Jia Chen, Xue ve Lai, 2008; Patil, Narayankar, Narayan ve Meena, 2016). Gerçek zamanlı görüntü şifreleme için daha az zaman ve bununla birlikte güvenlikten ödün vermeyen yöntemler tercih edilmelidir (Belazi ve diğerleri, 2016).

Görüntülerin herkese açık ağlar üzerinden paylaşımı, güvenlik ihtiyaçlarını karşılamak için, güçlü güvenlik özelliklerine sahip şifreleme tekniklerinin geliştirilmesine sebep olmuştur. Son 5 yılda, literatürde farklı tekniklerle geliştirilen çok sayıda şifreleme algoritması önerilmiştir (Pak ve Huang, 2017; Chai, ve diğerleri, 2019; Hua ve diğerleri, 2019; Suri ve Vijay, 2019; Mansouri ve Wang, 2020). Pak ve Huang (2017), 1D kaotik haritanın kombinasyonunu kullanan yeni bir renkli görüntü şifrelemesi sunmuşlardır. Chai ve diğerleri (2019), DNA dizi işlemlerine ve kaotik sistemlere dayalı yeni bir görüntü şifreleme algoritması

önermişlerdir. Hua ve diğerleri (2019) görüntü şifreleme için kosinüs dönüşümüne dayalı kaotik sistem geliştirmişlerdir. Bunun tersi olarak, Mansouri ve Wang (2020), yeni bir tek boyutlu sinüs destekli kaotik harita kullanarak görüntü şifreleme algoritmasındaki uygulaması üzerine çalışmışlardır. Bunlardan farklı olarak ise Suri ve Vijay (2019), renkli görüntü şifreleme için senkronize iç içe geçmiş bir lojistik harita-DNA yaklaşımı sunan bir şifreleme sistemi geliştirmişlerdir.

Görüntü şifreleme kaotik ve kaotik tabanlı olmayan olarak ikiye ayrılmaktadır. Görüntü şifrelemede, kaos bilimi ve kriptografi arasındaki benzerliklerden dolayı kaotik haritaya dayalı teknikler yaygın olarak kullanılmaktadır. Ayrıca, kaotik şifreleme haritaları tek boyutlu ve çok boyutlu olmak üzere ikiye ayrılır. Tek boyutlu kaotik haritalar, basit yapılıdır ve kolay uygulanabilirler. Çok boyutlu haritalar ise karmaşık yapılıdır ve geniş kaotik aralıkları ile yüksek güvenlik sunmaktadır. Bu da uygulanmasını güç hale getirmektedir. Kaotik haritaların geliştirelerek görüntü şifreleme işleminde kullanımı gün geçtikçe artmaktadır. Güçlü bir güvenlik için genişletilmiş kaotik değer aralığına sahip kaotik bir harita tasarlamak gerekir. Literatürde kaotik haritalar uygulanarak görüntü şifreleme gerçekleştirilen birçok çalışma mevcuttur. (Pak ve Huang, 2017; M. Li, Nkandeu ve diğerleri 2019; Wang, Liu ve Fan, 2019; Ghazvini ve diğerleri, 2020; Mansouri ve Wang, 2020; Mboupda Pone ve Tiedeu, 2020; X. Wang ve diğerleri, 2020; Midoun ve diğerleri 2021; Wang ve Talhaoui, 2021). Bu çalışmaların birçoğu parametrelere karşı yüksek hassasiyet, sözde rastgele davranış, periyodik olmama, donanım ve yazılımda uygulama basitliği ve karıştırma özelliği ile ayrışmaktadır.

Görüntü şifreleme iki ana işlem barındırmaktadır. İlk aşama piksellerin yerlerini değiştirme aşaması olan permutasyon ve ikinci aşama ise piksel değerlerinin değiştirilmesi olan difüzyon bölümüdür (Çavuşoğlu ve diğerleri, 2017). Permutasyon aşamasında mevcut piksellerin konumları koatik harita yardımı ile farklı konumlara taşınarak karıştırılmaktadır (Junxin Chen ve diğerleri, 2018). Difüzyon aşamasında orjinal görüntüye ait herhangibir istatistiki bilgi kalmaması için mevcut pikselin sahip olduğu ışıklık değeri değiştirilmektedir.

Görüntü şifrelemede, optimizasyon algoritmaları en sık uygulanan yöntemlerdendir. Bir problemin çözüm uzayındaki en iyi sonucu veren çözüm optimizasyon ile bulunur. Bir başka değişle istenilen şartlara göre en iyi sonucu veren çözümün bulunmasıdır. Günümüzde birçok problemin çözümünde farklı optimizasyon

algoritmaları kullanılmaktadır. Genetik algoritma (Genetic Algortihm-GA), karınca kolonisi algoritması (Ant Colony Algorithm-ACO) ve parçacık sürüsü optimizasyonu (Particle Swarm Optimization-PSO) algoritması görüntü şifrelemede kullanılan meta-sezgisel yaklaşımlardır. Enayatifar ve diğerleri (2014), genetik algoritmada DNA dizisinin bir kombinasyonu yoluyla görüntüleri şifrelemek için hibritleştirilmiş bir model ortaya koymuşlardır. Şifreleme için anahtarlar üreten Karınca Kolonisi Optimizasyonu sürü zekasına dayalı bir algoritmadır. Sreelaja ve Vijayalakshmi Pai (2012), binary görüntüleri şifrelemek için ACO algoritmasıyla anahtar üreten bir yaklaşım önermişlerdir. Bu yaklaşımda binary görütüleri şifrelemek için orijinal görüntüdeki karakterleri dağıtarak ACO'ya kullanarak bir anahtar akışı oluşturmuşlardır. X. Wang ve Li (2021), parçacık sürüsü optimizasyonu ve kaotik haritaya dayalı bir şifreleme algoritması önermişlerdir. PSO algoritması ile bilgi entropisine ve korelasyon katsayısına dayanan ve en iyi anahtar değerini döndüren şifreleme yöntemi sunmuşlardır.

Önerilen optimizasyona dayalı görüntü şifreleme algoritmaları, şifrelenecek görüntünün tamamında işlem yaptıkları için iterasyonlar uzun sürmekte ve üretilen anahtarı optimize etmek zorlaşmaktadır. Bu nedenle gerçek zamanlı uygulamalarda kullanılması mümkün görülmemektedir. Kelebek optimizasyon algoritmasının (Butterfly optimization algorithm (BOA)) 3 aşama vardır. İlk olarak, başlangıç popülasyonunun üretilmesitir. İkinci aşama, iterasyonların gerçekleştirilmesidir. Son aşama ise, en iyi çözümün bulunduğu algoritmanın sonlandırılması aşamasıdır. BOA'da, parametre sayısı değişmeden kaldığından, bilgileri saklamak için sabit boyutlu bellek tahsis edilmesi ve local optimumdan kolaylıkla global optimum noktasına yakınsaması ve yüksek doğruluk oranı ile diğer optimizasyon algoritmalarından öne çıkmaktadır (Arora ve Singh, 2019). Bu çalışmada BOA rastgele üretilen şifrelenmiş anahtarı optimize eder ve her iterasyon da yeni rastgele üretilen anahtar kullanılır.

Bu tez araştırmasının katkıları aşağıdaki şekilde özetlenmiştir;

- İlk olarak bütün görüntü yerine, görüntünün sol üst köşesi (0,0) olacak şekilde rastgele olarak belirlenen x ve y koordinatları başlangıç olarak 80x80' lik bir parça alınıp şifreleme işlemi gerçekleştirilerek optimum anahtar elde edilmektedir. Daha sonra optimum anahtar ile görüntünün tamamı şifrelenmektedir.

- Bu çalışmada bir boyutlu yüksek hassasiyete sahip yeni bir kaotik harita önerilmiştir. Önerilen bu kaotik harita performans değerlendirme kriterlerinin hepsinde diğer karşılaştırılan kaotik haritalardan daha başarılı çıkmıştır.

2. LİTERATÜR ARAŞTIRMASI

2.1 Kaos Kuramı

Kaos Teorisi, öngörülemeyen sistemlerin davranışını tahmin etme bilimidir. Kaos teorisi, göktaşlarının hareketi, elektronik sistemler, meteorolojiden iklim tahminleri, insan kalbinin atışı, borsa ve ekonomi gibi çok çeşitli sistemlerin karmaşık işleyişine açılan bir pencere olan bir kaos denizinden güzelce düzenlenmiş yapıları çıkarmamızı sağlayan matematiksel bir araç takımıdır. Kaos Teorisinin merkezinde, kaos ve düzenin her zaman taban tabana zıt olmadığına dair fikir vardır. Kaos teorisindeki ilk deney, bir meteorolog olan Edward Lorenz tarafından gerçekleştirildi. Lorenz, hava durumu tahmini için bir denklem sistemi ile çalıştı. 1961'de Lorenz, rüzgar hızı, sıcaklık gibi 12 değişkene dayalı bilgisayar modeli kullanarak geçmiş hava durumu dizinini yeniden oluşturmak istedi (Lorenz, 1973). Bu değişken ve değerler, zaman içinde grafiğe döküldü. Lorenz değişken değerleri altı yerine üç ondalık basamağa yuvarladı. Yapılan değişiklik iki aylık simüle edilmiş hava koşullarının tamamını büyük oranda değiştirdi. Böylece Lorenz, önemsiz görünen faktörlerin sonuç üzerinde çok büyük bir etkiye sahip olabileceğini kanıtladı. Sonuç olarak kaos teorisi, ilgisiz görünen olayların sonuçlarını dramatik bir şekilde etkileyebilecek küçük olayların etkilerini araştırır.

2.2 Kaotik Sistemler

Kaotik sistemler kaos ve düzenin karışımıdır. Dışarıdan tahmin edilemeyen kaotik davranışlar sergilerler fakat iç işleyişleri ortaya çıktığında saat gibi işleyen mükemmel deterministik bir denklem seti keşfedilir. Rastgelelik ile kaosa gizlenmiş bilgiler bir çok kaotik sistemin içerdiği üç ortak özellikte bulunabilir.

Tahmin edilemezlik: Karmaşık bir sistemin bütün başlangıç koşullarını mükemmel ayrıntıda asla bilemeyeceğimiz için, karmaşık bir sistemin nihai sonuçlarını tahmin etmeyi düşünmeyiz. Bir sistemin işleyişinin ve sonuçlarının ölçülmesindeki en ufak hatalar bile dramatik şekilde büyütülecek ve herhangi bir tahmini boş hale getirecektir. Dünyadaki bütün kelebeklerin etkilerini ölçmek imkansız olduğundan,

doğru uzun menzilli hava tahmini her daim imkansız olacaktır. Kaos basit bir düzensizlik değildir. Kaos, şaşırtıcı şekillerde ortaya çıkan düzen ve düzensizlik arasındaki geçişleri araştırır.

Kaotik sistemin, bazı belirleyici özellikleri vardır. Bu özellikler temel olarak:

- Başlangıç parametrelerine yüksek duyarlılık,
- Sistemin analitik bir çözümünün olmaması,
- Rastgele değil deterministik olması,
- Gürültü benzeri güç spektrumlarına sahip olması,
- Herhangi başlangıç koşulunun belirlenememesidir (belirsizlik ilkesi).

Meteorolojist olan Edward Lorenz, meteorolojik değişimlerin başlangıç koşullarına olan hassas bağlılığını buldu. Lorenz havadaki ısı değişimlerini gösterebilmek için, aşağıdaki denklem 2.1-2.2-2.3 zaman değişkeni değiştikçe üç boyutlu uzayda çizdiği yörüngenin değiştiğini ve ortaya çıkan grafiğin iki nokta etrafında yoğunlaştığını fark etti. Bu noktalara Lorenz Çekerleri ya da Garip Çekerler denir (Janeiro, 1999).

$$\frac{dx}{dy} = -ax + ay \tag{2.1}$$

$$\frac{dy}{dt} = -bx - y - zx \tag{2.2}$$

$$\frac{dz}{dt} = -cx + xy \tag{2.3}$$

2.3 Güvenli İletişim

Teknolojinin kullanımının artmasıyla, bilginin bütünlüğü, erişilebilirliği, korunması ve bilgi transferi gibi önemli konular ön plana çıkmaktadır. Dünya genelinde dijital görüntülerin herkese açık ağlar üzerinden aktarımı nedeniyle, güvenli olmayan internet ortamında yer alan bilgi miktarı da artmaktadır (Nadhom ve Loskot, 2018). Bu nedenle iletilmek istenen bilgileri korumak çok önemli hale geldi. Özellikle kritik öneme sahip dijital görüntüleri depolamak ve iletmek için hızlı ve sağlam bir güvenlik sistemi gerektirir. Güvenli iletişim, iki kuruluşun veya şahsın iletişim kurduğu ve üçüncü bir şahsın dinlemesini istemediği durumdur. Kuruluşların kulak misafiri olmaya veya müdahale etmesine karşı konulacak ve sezilmeyecek bir şekilde

iletişim kurması gerekir. Güvenli iletişim, üçüncü şahısların veya kurumların söylenenleri engelleyemeyeceği veya değiştiremeyeceği kesin bilgi paylaşabileceği araçları içerir. Dinleme ve şifreleme gibi yöntemlere rağmen, hiçbir iletişim tam anlamıyla güvenliği garanti edememektedir. Kriptoloji, literatürde bilgi güvenliğini sağlamak adına kullanılan yaygın bir şifreleme sanatıdır. Kriptolojinin özelliği gereğince, gönderici tarafından bilginin başkaları tarafından anlaşılabilirliği yok edilir ve sadece alıcı tarafında bu bilginin anlaması sağlanır.

Güvenli olmayan kanallardan önemli bilgiler gönderilirken bilgiyi korumak için şifreleme kullanılır. Bilgi güvenli bir ortamda şifrelenerek, güvenli olmayan kanal boyunca şifreli olarak aktarılması ve alıcının sağlıklı bir şekilde çözülebilmesi kriptolojinin ana amacıdır. Digital görüntünlerin şifreli olarak iletilmesi en yaygın kullanılan tekniklerden birisidir. Bu yüzden literatürde, görüntünün güvenliğinin ve gizliliği sağlanması için birçok şifreleme algoritma önerilmiştir.

2.4 Görüntü Şifreleme

İnternet üzerinden (herkese açık ağlar) dijital görüntülerin iletilmesi nedeniyle, güvenli olmayan internet ortamında yer alan bilgi iletimi gün geçtikçe artmaktadır (Nadhom ve Loskot, 2018). Bu nedenle herkese açık ağlar üzerinden iletilen bilgileri korumak çok önemli hale geldi. Görüntü şifreleme yöntemi ile transferi yapılacak şifreli görüntü, sadece gönderilen kişi tarafında çözülebilecek, benzersiz bir yapıya dönüştürülür. Görüntü şifreleme için daha kısa zaman da şifreleme yapan ve güvenlikten ödün vermeyen şifreleme algoritmaları tercih edilir. Şifreleme alanında son zamanlarda yaygın olarak kullanılan kaos tabanlı görüntü şifreleme yöntemi diğer şifreleme sistemlerine göre daha iyi sonuçlar vermektedir. Bu da, kaosun bu alandaki kullanımını giderek arttırmaktadır. Kaotik sistemler üzerine kurulan bu şifreleme algoritmaları, kimi zaman iyi sonuçlar verirken beraberinde bazı dezavantajları da getirmektedir (Bu ve Wang, 2004; Afarin ve Mozaffari, 2013). Özellikle renkli görüntüdeki veri boyutu fazla olduğundan kaos tabanlı şifreleme sistemleri performans açısından düşük olabilir. Kaotik tabanlı görüntü şifreleme algoritmalarında, şifreli görüntünün düz görüntüye ait herhangi bir istatistiki bilgi barındırmaması için düz görüntüye permütasyon ve difüzyon işlemleri uygulanır. Bu sayede, şifrelenmiş görüntünün güvenliği artırılmış olur.

Kaotik haritanın boyutuna göre kaos tabanlı görüntü şifreleme algoritmaları üç çeşittir. Birincisi bir boyutlu kaotik tabanlı görüntü şifreleme algoritmalarıdır (Pareek ve diğerleri, 2006). İkincisi, iki veya daha çok boyutlu kaotik tabanlı görüntü şifreleme algoritmalarıdır (Peng ve diğerleri, 2009). Üçüncüsü ise hem diğer şifreleme algoritmalarını hem de kaotik sistemleri aynı şifreleme algoritmasında kullanarak hibrit bir yöntemle şifreleme işlemini gerçekleştirmektir (G. Chen ve diğerleri 2004).

Bir boyutlu kaotik haritalar basit yapıları, uygulanmasının kolay olması ve daha düşük hesaplama maliyetine sahip olmaları gibi avantajlara sahiptir. Bir boyutlu kaotik haritaların uygulanması kolay olduğundan gerçek zamanlı uygulamalar için gayet uygundur. Bir boyutlu kaotik harita kullanılarak yapılan görüntü şifrelemelerde, eğer kaotik harita peryodik bölgeler üretiyorsa kaotik yörüngeleri tahmin edilebildiğinden orjinal görüntüye ait bilgiler elde edilebilmektedir.

Yüksek boyutlu kaotik harita kullanılarak yapılan görüntü şifreleme işlemlerinde, sonlu kaotik yörüngeler periyodik duruma gelmemektedir. Yüksek boyutlu kaotik sistemlerde yörüngülerin tahmin edilmesi zor olduğu için gerçek zamanlı uygulamalarda orjinal görüntüye ait bilgilerin çıkarılması zordur. Değişken uzayının genişliği yardımıyla güvenlik de genişletilmiş olur.

Hem farklı şifreleme algoritmalarından hem de kaotik bir sistemden yararlanılarak yapılan bir şifreleme sisteminde permütasyon ve difüzyon işlemleri ayrı ayrı uygulamak yerine tek bir şifreleme sistemiyle uygulanabilir. Bu şekilde yapılan bir şifreleme algoritmasının güvenilirliği arttırabilir ama hız ve maliyet açısından şifrelemeyi olumsuz olarak etkileyebilir.

2.5 Optimizasyon

Gerçel fonksiyonun en düşük (minumum) ya da en yüksek değerleri (maksimum) bulmak amacı ile tanımlı bir aralıkta rastge sayı değerlerinide içeren bir fonksiyon aracılığıyla sistematik olarak bir problemi incelemek ya da çözme işlemine optimizasyon denir. Pek çok klasik yöntemlerle çözülemeyen problemler optimizasyon ile çözülebilir. Optimizasyon algoritmaları, karar verme süresini hızlandırmak ve karar kalitesini arttırmakta kullanılarak gerçek hayatta karşılaşılan problemlerin etkin, doğru ve gerçek zamanlı çözümünde kullanılmaktadır. Fonksiyon, hangisinin "en iyi" olabileceğini belirlemek için farklı seçeneklerin

karşılaştırılmasına sebep olur. Optimizasyon tekniklerinin planlı şekilde uygulanması başarı ve gelişmeyi beraberinde getirir. Optimizasyon teknikleri şunlardır: Minimum maliyet, maksimum kar, optimum tasarım, optimum yönetim, minimum hata, varyasyon ilkeleri. Optimizasyon yöntemleri ise şu şekilde sıralanabilir:

Sezgisel Algoritmalar: Sonucun doğruluğunun veya kanıtlanabilir olup olmadığını önemsememektedir ama iyiye yakın çözüm yolları elde eder. Sezgisel algoritmalar, arama süresinde daha verimli hale gelebilmek için en iyi çözümü aramayı bırakarak çözüm zamanını daraltırlar (Nazari-Heris ve diğerleri 2018).

Metasezgisel Algoritmalar: Belirli bir probleme özgü olmayan arama işlemlerine yön veren metottur. Amacı arama uzayını etkili şekilde keşfederek ve yerel en iyi konumlara takılıp kalmayı engelleyecek yapıları bularak en iyi veya en iyiye çok yakın sonuçları elde etmektir. Yerel arama tekniklerinden, karmaşık öğrenme işlemlerine kadar değişim gösteren yapıdadır (P. Wang ve diğerleri, 2020).

Benzetim (simülasyon) ile Senaryo Analizleri: Benzetim, bir sitemin veya sürecin çalışmasını taklit etmektedir. Sistem için yapay geçmiş üretilmesine ve gerçek sistemin tipik özelliklerine dair çıkarımlar yapmak üzere üretilen geçmişin gözlemlenmesine olanak verir. Zaman içinde sistemin işleyişinin taklididir. Bazı koşullar altında sistemin hareketlerinin gözlemlenebilmesi için, bu sistemin modellenmesi olarak da tanımlanabilir. Zamanla değişen bir sistemin hareketleri, geliştirilen bir benzetim modeli ile sistemin çalışması ile ilgili kabuller setinden oluşan sistemin ilgilenilen varlıkları arasındaki matematiksel, mantıksal ve sembolik ilişkiler ile ifade edilir.

Matematiksel Programlama: Optimizasyon modelleri sistemin mekanizmasını ve özelliklerini yansıtan, içindeki ve çevresindeki diğer sistemlerle olan etkileşimleri içeren matematiksel ifadelerden oluşmaktadır. Bu matematiksel ifadeler sistemin ölçülebilen özelliklerini tespit eden parametrelerden, en iyi sonuçları verecek sonuç değerlerini tanımlayan değişkenlerden, en iyi performans ölçütünden ve sistemin özelliklerini ve sınırlarını belirten kısıtlardan oluşmaktadır.

2.6 Optimizasyon ile Görüntü Şifreleme

Optimizasyon şifreleme yöntemlerinde 2 şekilde kullanılmaktadır. İlk olarak kaotik haritaların başlangıç değerlerini üreten anahtarı optimize etmekte kullanılmaktadır.

Bu yolla şifreli görüntünün yüksek bir entopi değerine sahip olması ve bitişik pikseller arasındaki korelasyonun minimum olması amaçlanmaktadır. Optimizasyon algoritmalarının görüntü şifrelemede ikinci kullanım alanı, kaotik haritanın parametrelerinin optimize edilmesidir. Kaotik haritaların performanslarını değerlendirmek için çeşitli testler bulunmaktadır. Bu testleri maliyet fonksiyonunda kullarak kaotik haritanın performansı optimizasyon algoritmaları tarafından artırılmaktadır. Dolayısıyla şifreleme algoritmasının performansı artmaktadır.

Optimizasyon algoritmalarının iyi seçilen maliyet fonksiyonlarıyla şifreleme yöntemlerine uygulanması daha yüksek performanslı görüntü şifrelemeyide beraberinde getirmektedir. Optimizasyon algoritmalarının görüntü şifrelemeye uygunlandığı ve başarılı sonuçlar verdiği çok fazla sayıda çalışma vardır (Afarin ve Mozaffari, 2013; Aslam ve Santhi, 2019; H. Li ve diğerleri, 2021).

2.7 Kelebek Optimizasyon Algoritması

Kelebek optimizasyon algoritması (Butterfly optimization algorithm (BOA)) kelebeklerin yiyecek arama ve çiftleşme davranışını taklit eden popülasyon tabanlı metasezgisel algoritmadır. BOA'daki esas motivasyon, kelebeklerin yiyecek arama ve çiftleşme davranışlarını taklit etmektir (Arora ve Singh, 2019). BOA'da bütün kelebekler, arama uzayında optimizasyon işlemini gerçekleştirmek için arama ajanı olarak kabul edilir. Kelebeklerin yiyecek bulmak ve çiftleşecek eşini bulmak için kullandıkları en önemli duyu kokudur. BOA'nın diğer meta-sezgisel algoritmalardan temel farklarından birisi her kelebeğin kendine özgü kokuya sahip olmasıdır. Kelebekler, farklı koku yoğunluklarını çok hassas algılayabilen ve sınıflandırabilen canlılardır. Her bir kelebek, gıda kalitesinin uygunluğu veya çifleşme hakkında bilgi vermek için diğer kelebeklere belirli yoğunlukta koku yaymaktadır. Yiyecekler, çözüme karşılık gelen arama uzayındaki bir konumla da ilgilidir. Her kelebek, koku yayarak gıda kalitesinin uygunluğunu paylaşabilir ve gıdanın bulunduğu konumu etki alanındaki diğer kelebekler tarafından herhangibir yerden algılanabilir. Böylelikle sosyal bir ağ kurulmuş olmaktadır.

BOA'da üç parametreye bağlı temel bir algılama kavramı vardır: duyusal modalite (c), uyaran yoğunluğu (I) ve güç üssü (a). Duyusal modalitesi, uyaran tarafından enerji gücünü ölçer. BOA'da modalite kokudur. Uyaran yoğunluğu (I), uyaranın büyüklüğünü gösterir ve arama uzayındaki çözümlerin amaç değeri ile doğrudan

bağlantılıdır. Amaç değeri daha yüksek (koku) olan bir kelebek varsa, çevresindeki diğer kelebeklerin bunu hissedebileceği ve ona çekileceği anlamına gelir. Kuvvet üssü, uyarıcıyı ayarlamasını sağlamaktadır. Kelebek optimizasyon algoritmasında I, bir çözümün nesnel değerini ifade etmektedir. f, kelebekler tarafından algılanan göreceli bir değerdir. Koku denklem 2.4'deki gibi formülize edilir:

$$f = cI^a \tag{2.4}$$

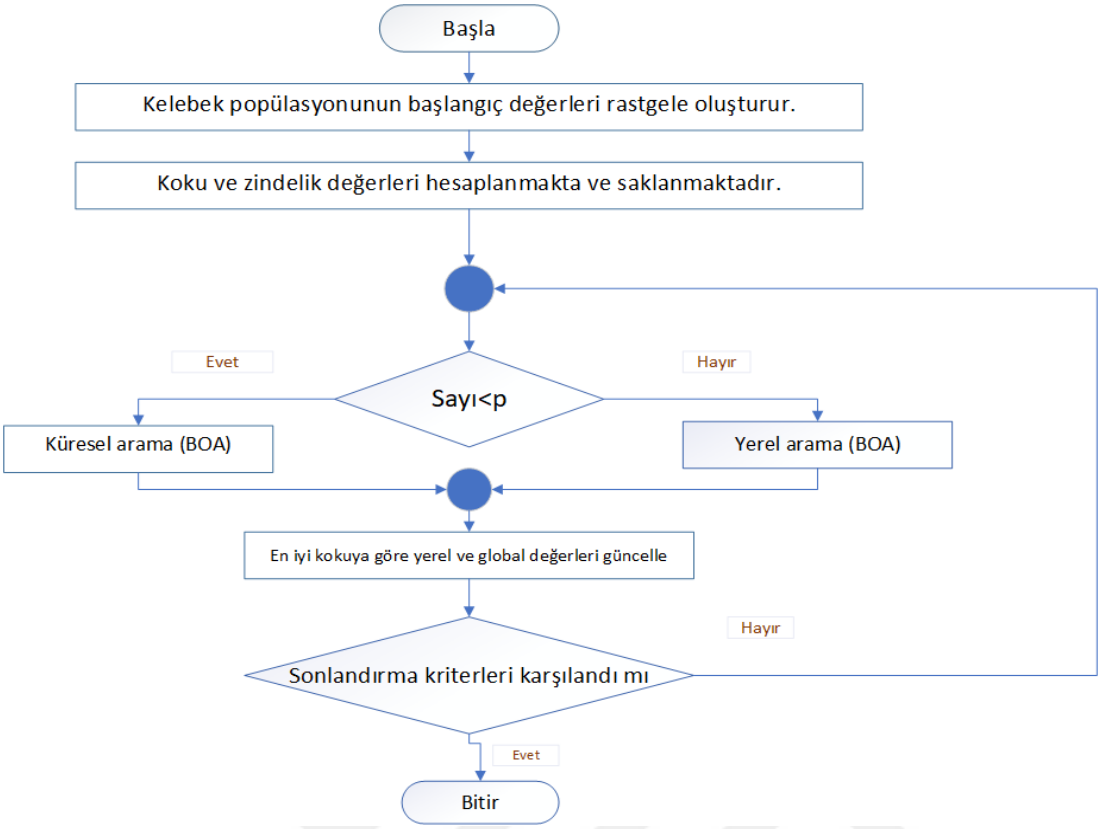
burada, f kokunun diğer kelebekler tarafından ne kadar güçlü algılandığı, c duyusal modalite, I uyaran yoğunluğu ve a modaliteye bağlı güç üssüdür ve değişen emilim derecesini açıklar. Bu çalışmada a ve c 'yi [0,1] aralığında seçtik. Standart BOA'yı tanımlayan sözde kod Algoritma 2'de ve akış şeması Şekil 2.1'de verilmiştir (Arora ve Singh, 2019). BOA'nın global arama ve yerel arama olarak iki önemli aşaması vardır. Global aramada, g^* tüm çözümler arasında bulunan mevcut en iyi çözümü temsil eder ve global arama deklem 2.5 gibi tanımlanır:

$$x_i^{i+1} = x_i^t + (r^2 \times g^* - x_i^t) \times f_i \tag{2.5}$$

burada x^t i, t'inci yineleme sayısında çözüm vektörünü belirtmektedir. i'inci kelebek kokusu f_i ile gösterilir ve r, [0, 1] aralığında rastgele bir sayıdır. Buna ek olarak, yerel arama aşaması aşağıdaki denklem 2.6'daki gibi ifade edilebilir:

$$x_i^{i+1} = x_i^t + \left(r^2 \times x_j^t - x_k^t\right) \times f_i \tag{2.6}$$

burada, x_j^t ve x_k^t, arama uzayında j'inci ve k'inci rastgele çözümlerdir. Kelebekler yiyecek ve çiftleşme ortağı aranması, hem local hem de global aramada gerçekleşebilir. Eş durumu ve yağmur, rüzgar gibi çeşitli koku almayı zorlaştıran diğer durumlar göz önüne alındığında, arama faaliyetlerinde önemli bir p payı olabilir. Bu nedenle, BOA'da global arama ile yerel arama arasında geçiş yapmak için bir geçiş olasılığı p kullanılır.



Şekil 2.1: Kelebek optimizasyon algoritması akış şeması.

2.8 Görüntü Şifreleme İçin Güvenlik Testleri

Literatürde, görüntü şifreleme sistemlerinin kalitesini, güvenilirliğini ve gelen saldırıların sistemi zayıflatıp zayıflatmadığını ölçmek için standart güvenlik testleri bulunmaktadır. Bu sunulan testlerden bazıları aşağıda açıklanmaktadır.

2.8.1 Anahtar uzayı analizi

İyi bir şifreleme sistemi kaba kuvvet saldırılarına karşı koyacak kadar yeterli anahtar uzunluğuna sahip olmalıdır. Teorik olarak kaba kuvvet saldırıları ile çözülmeyen şifreleme sistemi yoktur. Günümüzde şifreleme sistemlerinin kaba kuvvet saldırılarına dayanabilmesi için en az anahtar uzunluğu 2^{100} uzunluğuna sahip olmalıdır (Alvarez ve Li, 2006; Liu, Wang ve Kadir, 2014). Eğer önerilen şifreleme sisteminin anahtar uzunluğu 2^{100}'den büyükse, şifreleme sistemi kaba kuvvet saldırılarına karşı dirençlidir.

2.8.2 Anahtar hassasiyeti analizi

Şifreli görüntü saldırısında, kriptanalist bir grup açık görüntü ve bunlara karşılık şifreli görüntüler bulundurur. Bu bilgiler kullanılarak gizli anahtara ulaşılması

amaçlanır (Deepan ve diğerleri 2014). Şifreleme algortiması, açık ve gizli anahtarların değiştirilmesine duyarlı olmalıdır. Duyarlı bir şifreleme sistemi kaba kuvvet ataklarına karşı koyacak anahtar uzunluğuna sahip olmalıdır. Şifreleme algoritmasında kullanılacak farklı anahtarların tamamı şifreleme sisteminin anahtar alanını oluşturur. Şifreleme ve şifre çözme işlemlerinde kullanılan anahtardaki küçük bir değişiklik çıktı sonucunu değiştirmelidir. Açık anahtar üzerinde uygulanan hassasiyet analizinde, açık anahtar ile şifrelenen görüntülerde farklı şifreli görüntüler üretilir. Gizli anahtar üzerinde yapılan hassasiyet testinde şifre çözme işlemini bir bit değişiklikle elde edilen şifresi çözülmüş farklı görüntüler elde edilir.

2.8.3 Bilgi entropisi analizi

Bilgi entropisi, görüntünün belirsizliğini yansıtan temel yöntemdir. Bir görüntünün entropi değeri ne kadar yüksek olursa sistemin kaos derecesi o kadar yüksektir. Eğer entropi değeri düşükse görüntünün tahmin edilebilirliği o kadar yüksektir. Gri ölçekli görüntülerde teorik olarak entropi değeri maksimum 8 olmaktadır. Şifreli bir görüntünün entropi değeri 8'e ne kadar yakın olursa şifreleme performansı o kadar yüksektir.

2.8.4 Histogram analizi

Histogram, bir görüntünün piksel değerlerinin dağılımını göstermek için kullanılmaktadır. Düz görüntülerin piksel değerlerinin dağılımı genellikle eşit değildir. Şifrelemeden sonra şifreli görüntünün piksel değerlerinin dağılımı ne kadar düzgün olursa, şifreleme performansı o kadar yüksek ve saldırılara karşı o kadar dirençli olmaktadır. Şifreli bir görüntüyü çözülebilme için kriptanalist, histogram kullanarak piksel değerlerinin tekrar sayılarına bakmaktadır. Bu yolla şifreli görüntü üzerinde istastiki bilgiler bularak düz görüntüye ait bilgiler elde etmek istemektedir. Bu tarzda saldırılar istatistiksel saldırı olarak adlandırılmaktadır. Bu tarz saldırıların önüne geçebilmek için şifreli görüntünün histogramının tek düze olması beklenmektedir.

2.8.5 Korelasyon analizi

İstatistiksel korelasyon iki rastsal değişken arasındaki doğrusal ilişkinin yönünü ve gücünü belirten bir ölçüdür. Şifrelenmiş bir görüntüde, bitişik iki pikselin korelasyonu minimum seviyede olmalıdır. n elemanlı bir dizide x ve y rastgele iki değişken olmak üzere korelasyon katsayısı, bağımsız değişkenler arasındaki ilişkinin

yönü ve büyüklüğünü belirten katsayıdır. Korelasyon katsayı, (-1) ile (+1) arasında bir değer alır. Düz bir görüntüde korelasyon katsayısı oldukça yüksektir. Şifrelenmiş bir görüntüde korelasyon katsayısının 0'a yakın olması beklenmektedir.

2.8.6 Ki-kare testi ve varyans analizi

Histogram bir görüntünün piksel dağılımını görsel olarak göstermektedir. Ki-kare testi ve varyans, bir görüntünün tekdüze dağılımdan ne ölçüde saptığını görsel olarak değil nicel olarak değerlendirmek için kullanılmaktadır. Ki-kare ve varyans değeri ne kadar düşükse, görüntünün dağılımı o kadar tek düze olmaktadır. Ki-kare testi ve varyans analizi şifreli görüntülerin şifreleme etkisini doğrulamak için kullanılmaktadır.

2.8.7 Differansiyel atak analizi

Şifreli metinlere ait diferansiyel atak analizi ilk olarak Biham ve Shamir (Biham ve Shamir, 1993) tarafından ortaya atılmıştır. Diferansiyel atakta amaç, gizli anahtarı şifreli metin veya görüntüleri inceleyerek tahmin etmeye dayanmaktadır. Kriptanalist, şifrelenmemiş düz görüntüleri sürekli değiştirerek bu görüntülere karşılık gelen şifreli görüntüleri analiz ederek gizli anahtara ulaşmaya çalışır. Diferansiyel atak, görüntü üzerindeki küçük değişikliklerin şifreli görüntü üzerinde nasıl değişiklikler gerçekleştirdiğini inceler. Eğer şifreli görüntüler arasında benzerlik veya bir ilişki elde edilebilirse, bu durum gizli anahtarın belirlenmesine neden olabilir. Eğer düz görüntü üzerinde yapılan değişiklik şifreli görüntüde önemli bir değişime sebep oluyorsa diferansiyel ataklar o kadar etkisiz kalmaktadır.

2.8.8 Veri kaybı saldırı analizi

Ağ üzerinde şifreli görüntülerin iletimi sırasında görüntünün bir parçasını kaybedebilir veya gürültüden etkilenebilirler. Ağ iletimi sırasında veya kötü niyetli imha saldırıları nedeniyle şifreli görüntüde bazı veriler kaybolabilir. Bu nedenle, güçlü bir şifreleme sisteminin görüntüyü kırpma saldırılarına karşı direnip direnemeyeceği belirlenmelidir (Zheng ve Jin, 2015). Ayrıca, ağ üzerinde iletim sırasında görüntü gürültü nedeniyle bozulabilir. İletim esnasında veri kaybına neden olacak bilinen üç gürültü türü vardır; Tuz ve Biber gürültüsü (SPN - Salt & Pepper noise), Gauss gürültüsü (GN - Gaussian noise) ve Benek gürültüsü (SN - Speckle noise). Hasarlı şifreleme görüntü başarılı bir şekilde kurtarılabilirse, şifreleme algoritması veri kaybı ve tıkanıklık saldırılarına karşı savunma yeteneği vardır.

2.8.9 Gürültü analizi

Ağ üzerinde görüntüler iletilirken görüntü çok çeşitli gürültülere maruz kalması olasıdır. Bu gürültü nedeniyle orijinal görüntü net bir şekilde elde edilemez. Şifreli görüntünün tekrar düz görüntüye dönüştürülmesi sırasında bir takım sorunlara neden olabilir. Şifreleme sisteminin iyi bir güvenilirlik seviyesine sahip olabilmesi için, tasarlanan algoritmanın gürültünün etkilerine karşı çok dirençli olması gerekmektedir. İyi bir şifreleme algoritmasının, farklı yoğunluklarda gürültüye maruz kalmuş şifreli görüntüyü orijinal haline benzer şekilde geri döndürmesi beklenmektedir.

2.8.10 Bilinen açık metin ve seçilmiş açık metin analizi

Bir şifreleme sisteminin güvenlik kalitesini değerlendirirken, gizli anahtar dışındaki tüm parametreler bilindiğinde bir şifreleme sisteminin güvenliğine bakılmasıdır. Bunu değerlendirmek için 2 saldırı çeşidi vardır.

Bilinen açık metin saldırısı: düz görüntüyle şifreli görüntü elde edilebilir, ama şifreleme sisteminin diğer ayrıntılarının bilinmediği saldırı tipidir.

Seçilmiş açık metin saldırısı: şifreleme sisteminin tüm detayları bilinen saldırı tipidir. Bu yolla, şifre çözme sisteminden şifreli görüntü yoluyla karşılık gelen düz görüntü elde edilebilir.

Bilinen açık metin ve seçilmiş açık metin saldırısı şifreleme sistemlerinin güvenlik zaaflarını ortaya çıkarmak için etkili bir saldırı tipidir. Görüntü şifreleme sistemi bu iki saldırıya karşı koyarsa, diğer saldırılara da direnebilir.

2.8.11 Hız analizi

Sistemde şifreleme ve şifre çözme işlemlerinin hızı sistemin gerçek zamanlı uygulanabilirliğini göstermektedir. Bunu gerçekleştirmek için bir takım işlemler uygulanır. İlki algoritmada, bit düzeyinde yapılan ayrıcalık veya mümkün olduğunca az zaman tüketen işlemlerin kullanılmasıdır. Öte yandan tek seferlik üretim için kaotik sistemden elde edilen veriler permütasyon ve difüzyon işlemi için kullanılmıştır. Görüntünün yalnızca önemli bir kısmına tek sefer uygulanması yine permütasyon ve difüzyon işlemleri birleştirilerek ve permütasyon ve difüzyon işleminin görüntünün tamamına tek sefer uygulanmasıyla zamanda yarıya yarıya

tasarruf edilir. Alınan tüm bu önlemler, şifreleme hızının arttırılmasını destekleyebilir.

3. MATERYAL METOD

Bu bölümde ilk önce yeni önerilen kaotik harita tanıtımıştır. Daha sonra, yeni önerilen kaotik haritanın karşılaştırmalı performans testleri gerçekleştirilmiştir. İkinci olarak, yeni önerilen şifreleme yönteminin aşamaları verilmiştir.

3.1 Yeni Kaotik Harita

Bu bölümde, yeni bir 1B kaotik harita önerilmektedir. Matematiksel olarak kaotik harita denklem 3.1'deki şekilde tanımlanır:

$$x_{n+1} = mod(r * x_n(1 - x_n) * e^8 + e^1 * x_n, 1); \quad (3.1)$$

burada $0 < x_n < 1$, r kaotik kontrol parametresidir. Yeni önerilen kaotik harita $0 < r \leq 10$ değerleri arasında davranış sergiler ve kaotik özellikler gösterir. Bu nedenle, klasik lojistik haritaya kıyasla, kaotik kontrol parametresi uzayının (r) genişlemesi nedeniyle daha geniş bir aralıkta kaotik davranış gösterir.

3.2 Yeni Kaotik Harita Güvenlik Testleri

3.2.1 Performans analizi

Yeni önerilen kaotik haritanın performansı en çok bilinen değerlendirme ölçütleriyle ölçülmüştür. Bu bölümde, duyarlılığını ve kaotik davranış aralığını değerlendirmek için kaotik haritamız üzerinde performans testleri yapılmıştır. Uygulanan analizler aşağıda verilmiştir.

1. Çatallanma Analizi (Bifurcation)
2. Yürünge Analizi (Trajectory)
3. Lyapunov üssü Analizi (Lyapunov Exponent (LE))
4. Örnek Entropi Analizi (Sample Entropy (SE))
5. Permütasyon Entropi Analizi (Permutation Entropy (PE)
6. 0-1 Analizi (Zero Test)

Bu analiz sonuçlarına bakıldığında önerilen kaotik haritanın yüksek karmaşıklıkta diziler üretilebildiği gözlenmektedir. Yeni önerdiğimiz kaotik haritayı, literatürde en

bilinen kaotik haritalarla karşılaştırıyoruz. Karşılaştırılan kaotik haritalar Çizelge 3.1'de verilmiştir.

Çizelge 3.1 : Karşılaştırma çizelgesi.

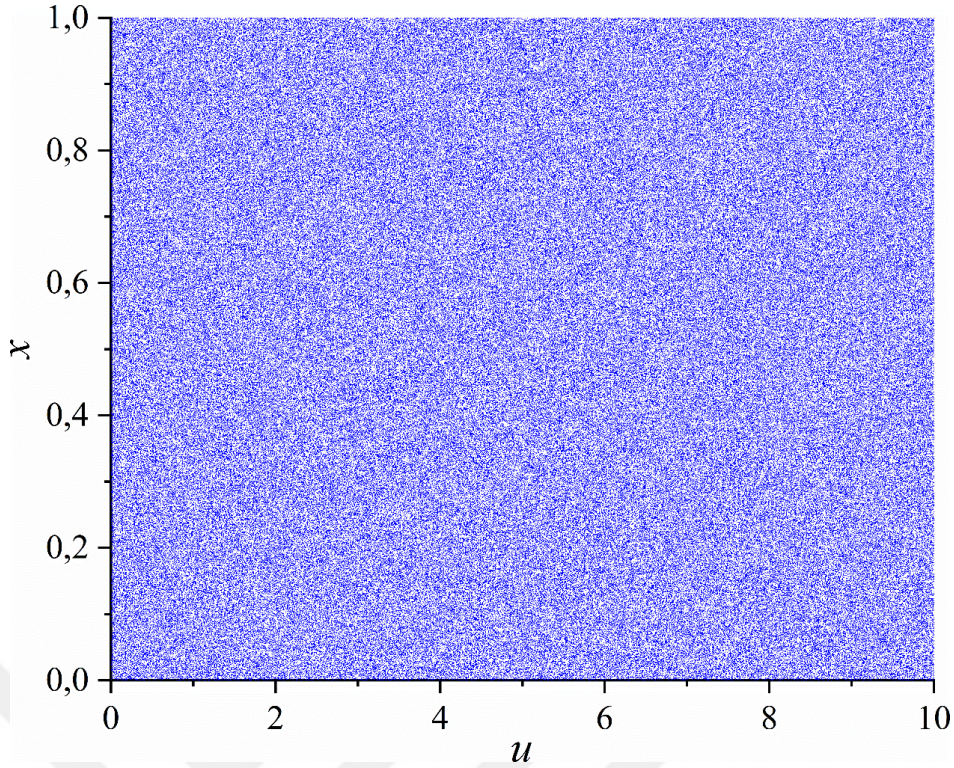
Sıra Numarası	Makale ismi	Atıf
1	A modified method for image encryption based on chaotic map and genetic algorithm	(Ghazvini ve diğerleri, 2020)
2	A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme	(Mansouri ve Wang, 2020)
3	Image Encryption Algorithm Based on Synchronized Parallel Diffusion and New Combinations of 1D Discrete Maps	(Nkandeu ve diğerleri, 2020)
4	A sensitive dynamic mutual encryption system based on a new 1D chaotic map	(Midoun ve diğerleri, 2021)
5	A new color image encryption using combination of the 1D chaotic map	(Pak ve Huang, 2017)
6	A novel 1D chaotic system for image encryption, authentication and compression in cloud	(H. Li ve diğerleri, 2021)
7	Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map	(M. Li ve diğerleri, 2019)
8	A new one-dimensional chaotic system with applications in image encryption	(X. Wang ve diğerleri, 2020)
9	Digital image scrambling based on a new one-dimensionalcoupled Sine map	(Yosefnezhad Irani ve diğerleri, 2019)

3.2.2 Çatallanma testi

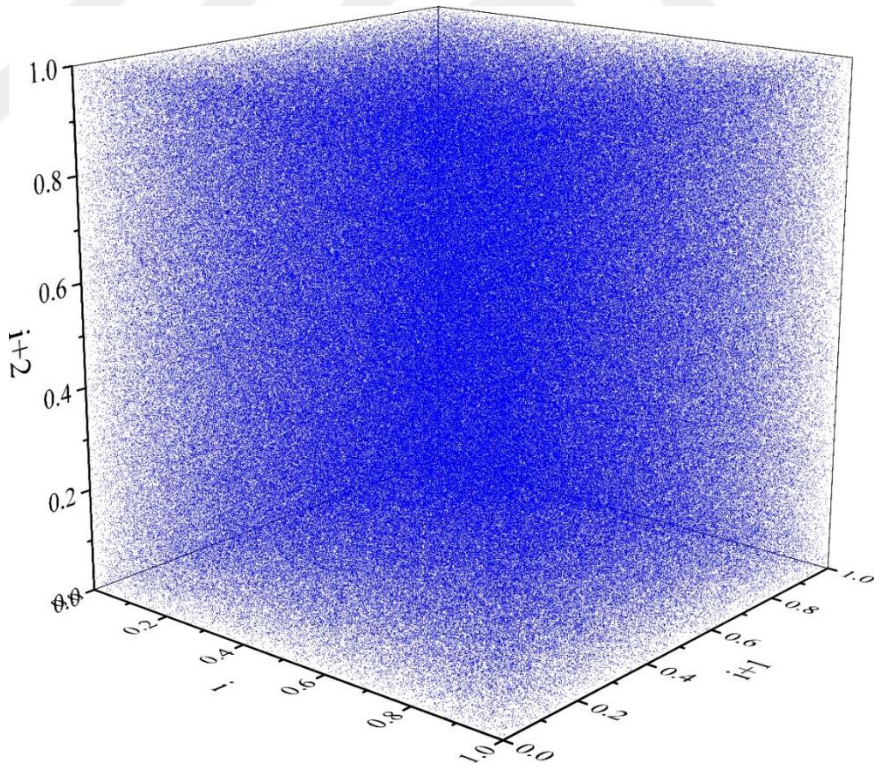
Dinamik bir sistemin kaotik davranışı, kaotik harita tarafından üretilen dizilerin çatallanma diyagramı kullanılarak görsel olarak değerlendirilir. Yeni önerilen kaotik haritanın çatallanma diyagramı Şekil 3.1'de gösterilmiştir. Yeni önerilen kaotik haritanın yörüngelerinin 0'dan 1'e tüm alana eşit olarak dağıldığını görülmektedir. Bu nedenle, yeni önerilen kaotik harita şifreleme algoritmalarında kullanılmaya uygun kaotik diziler üretmektedir.

3.2.3 Yörünge testi

Dinamik sistemin kaotik davranışı, üretilen zaman serilerinin yörüngesi kullanılarak belirlenebilmektedir. Teorik olarak sistemin rastgeleliği, yörüngesinin kaplayabileceği alan miktarı ile temsil edilir. 3B yörünge grafiğini kullanılarak, başlangıç değerlerine ve kontrol parametrelerine göre dinamik sistemin yörünge davranışları gözlemlenmektedir. Şekil 3.2'de yeni kaotik haritanın 3B yörüngesi gösterilmektedir. Şekil 3.2'de görüldüğü gibi yeni önerilen kaotik haritanın yörüngesi çok geniş bir alanı alanı kapsamaktadır.



Şekil 3.1: Önerilen 1B kaotik haritanın çatallanma diyagramı.



Şekil 3.2: Önerilen 1B kaotik haritanın 3B kaotik yörüngesi.

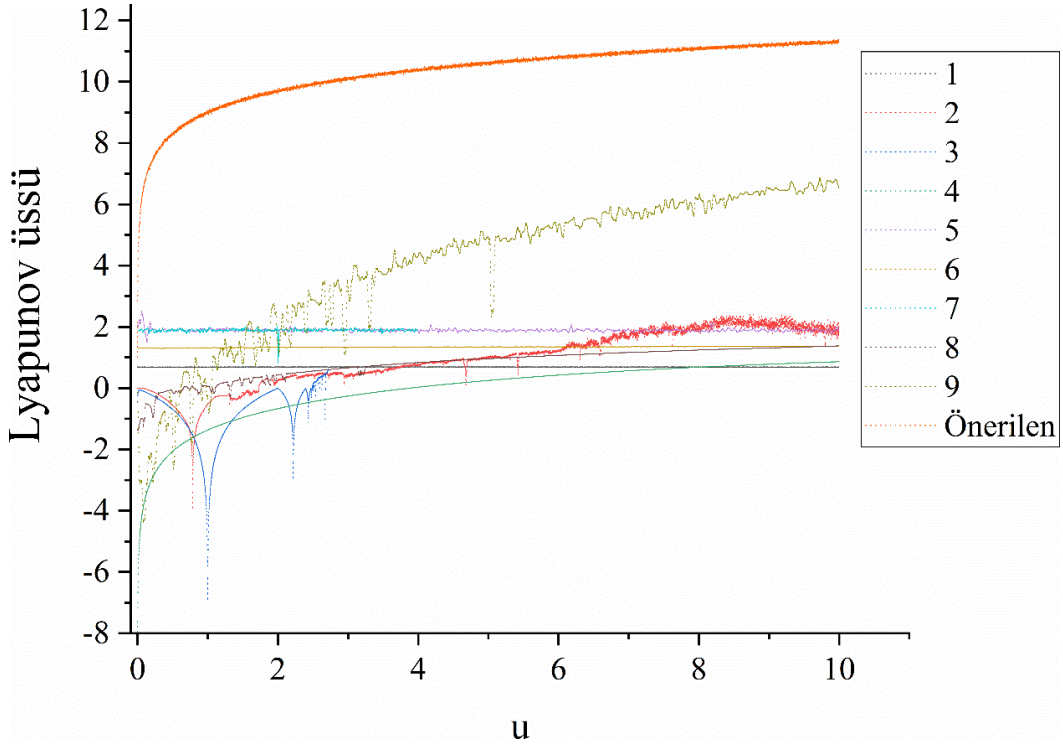
3.2.4 Lyapunov üssü testi

Lyapunov üssü, dinamik bir sistemin kaotik özelliklerini araştırmak için kullanılan önemli bir parametredir. Bir haritanın hassasiyeti ve kalitesi Lyapunov tabanı

kullanılarak incelenmektedir. $X_n + 1 = f(X_n, r)$, denklemine sahip bir 1B harita için Lyapunov üssü denklem 3.3'deki gibi tanımlananır:

$$\mathrm{L} = \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{k=0}^{n-1}\ln|f'X_n|\right\} \tag{3.3}$$

Literatürdeki ve yeni önerilen kaotik haritanın Lyapunov üs değerleri Şekil 3.3'de gösterilmektedir. Şekil 3.3'de, yeni önerilen kaotik haritanın literatürde karşılaştırılan kaotik haritalara göre daha büyük Lyapunov üssü değerine sahip olduğu görülmektedir.

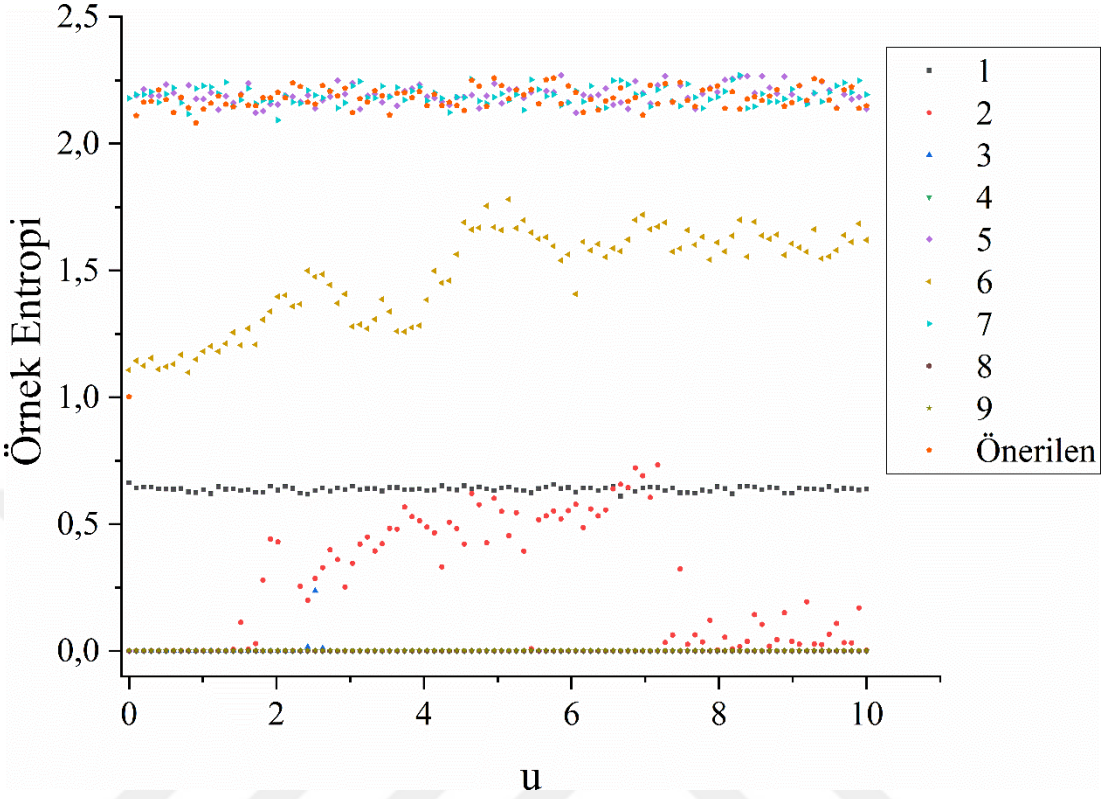


Şekil 3.3: Yeni önerilen 1B kaotik haritanın literatürle karşılaştırılması sonucu elde edilen Lyapunov Üssü grafiği.

3.2.5 Örnek entropi testi

Örnek entropi (Sample Entropi (SE)) testi, zaman serilerinin karmaşıklığının nicel ölçümünü veren yaklaşık entropinin geliştirilmiş bir versiyonudur. SE, zaman serilerini değerlendirmekte karmaşıklığını ölçen istatistiksel bir araçtır. Kaotik harita tarafından üretilen dizinin kendine benzerliğini nicel olarak tanımlamak için kullanılır. SE değeri ne kadar yüksekse, kaotik dizinin karmaşıklığı o kadar yüksek ve o kadar karmaşıktır. Yeni önerilen ve literatürdeki diğer kaotik haritaların SE

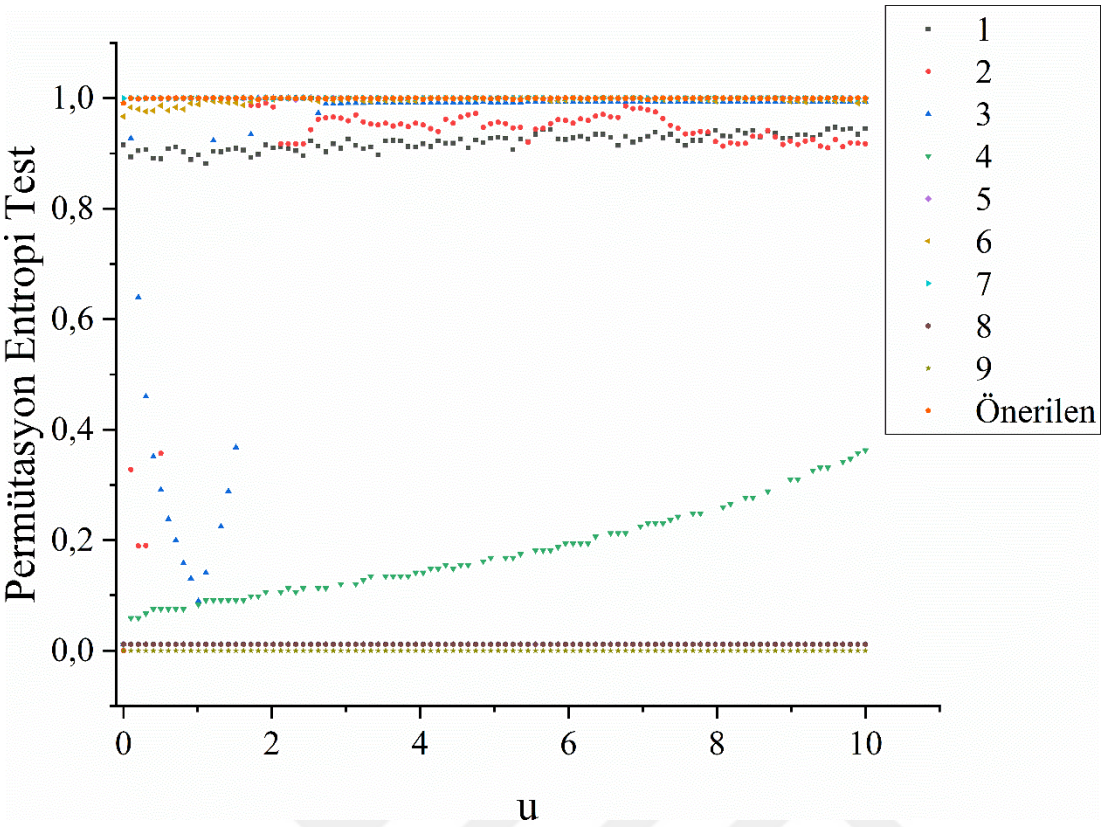
sonuçları Şekil 3.4'de gösterilmektedir. Yeni önerilen kaotik harita en yüksek SE değerine sahip haritalardan birisidir.



Şekil 3.4: Önerilen 1B kaotik haritanın literatürle karşılaştırılması sonucu elde edilen örnek entropi grafiği.

3.2.6 Permütasyon entropi testi

Permütasyon entropisi (PE), kaotik dizilerin karmaşıklığını ölçmek için kullanılan bir yöntemdir. PE değeri, 1'e ne kadar yakınsa kaotik dizi o kadar tahmin edilemez ve karmaşıktır. Şekil 3.5'de yeni önerilen haritaya ait PE değerleri gösterilmektedir. Yeni önerilen kaotik haritaya ait PE değerleri tüm diziler için neredeyse 1 değerini almaktadır. Bu da yeni önerilen kaotik haritanın yüksek bir karmaşıklığa sahip olduğunu ve üretilen kaotik dizinin tahmin edilemeyeceğini göstermektedir.



Şekil 3.5: Önerilen 1B kaotik haritanın literatürle karşılaştırılması sonucu elde edilen permüyasyon entropi grafiği.

3.2.7 0-1 testi

0-1 testi, kaotik bir sistemi tanımlamak için bir araç olarak uygulanmaktadır. LE'den farklı olarak, 0-1 testi dinamik sistemi yalnızca birkaç tur üretilen sekanslar için değerlendirir. Gerçek sabit r için, N dönüş sayısını ve $[Z\ (n)]\ (n\ =\ 1{,}2{,}3\ldots N)$, X veri serisini aşağıdaki denklem 3.4, 3.5, 3.6 ve 3.7'deki gibi hesaplanır:

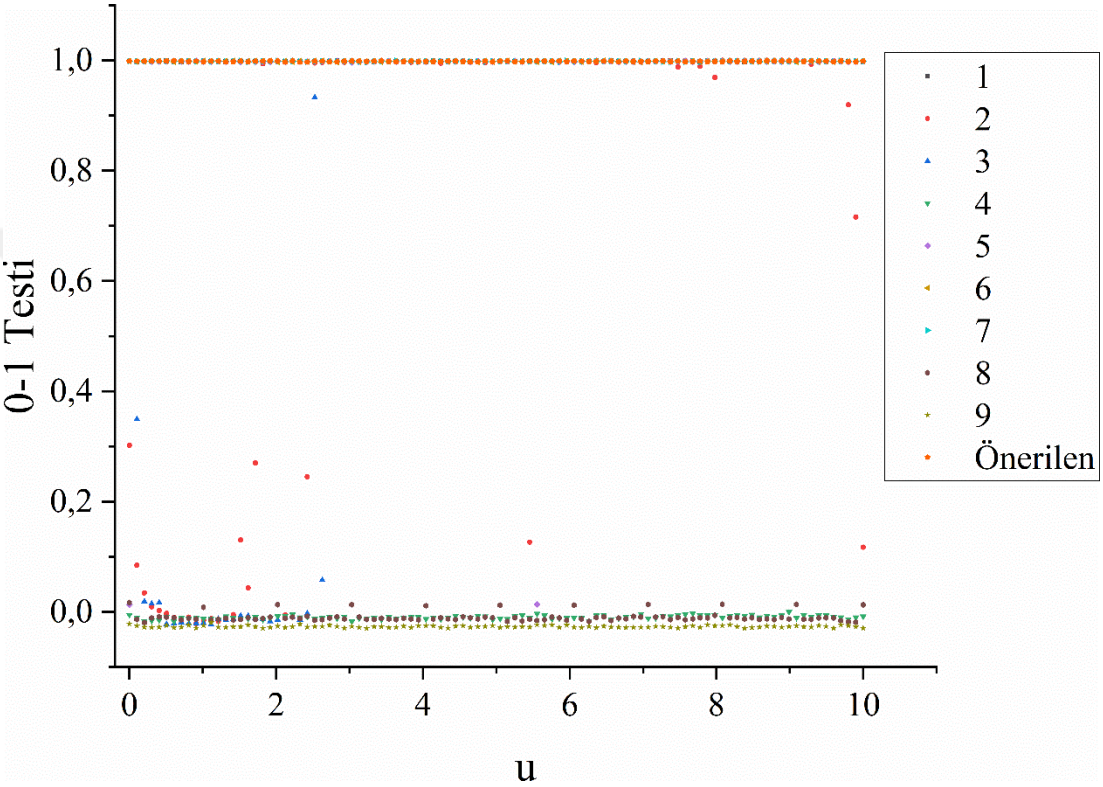
$$X = \frac{\log M(n)}{\log n} \tag{3.4}$$

$$\mathrm{M(n)} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{n} [p(i+n) - p(i)]^2 + [s(i+n) - s(i)]^2 \tag{3.5}$$

$$\mathrm{p(n)} = \sum_{i=1}^{n} D(i).\cos(ir) \tag{3.6}$$

$$s(n) = \sum_{i=1}^{n} D(i).\sin(ir) \tag{3.7}$$

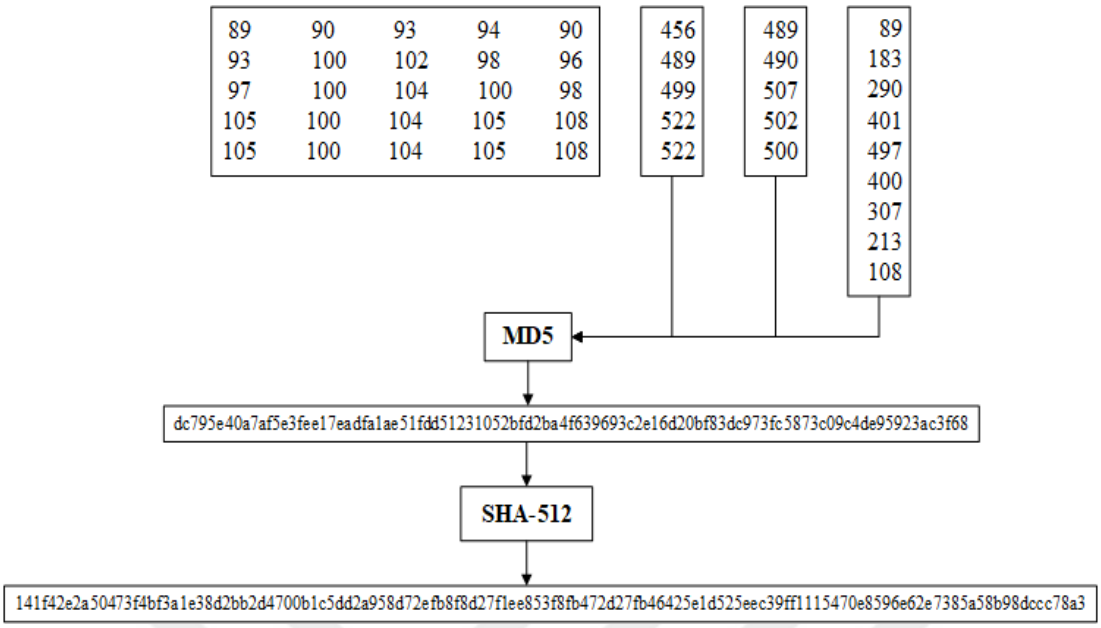
0-1 testinin sonucu 1 ise kaotik olduğunu ve 0 ise kaotik olmadığını göstermektedir. Şekil 3.6 yeni önerilen kaotik haritanın ve diğer kaotik haritaların 0-1 test sonuçları gösterilmektedir. Yeni önerilen 1-B kaotik haritayla üretilen kaotik diziler, başlangıç değerlerine yüksek hassasiyet göstermektedir.



Şekil 3.6: Önerilen 1B kaotik haritanın literatürle karşılaştırılması sonucu elde edilen 0-1 test analiz sonuçları grafiği.

3.3 Başlangıç Değerlerinin Üretilmesi

İlk olarak bu tez çalışmasında, herkese açık (publicKey) 512-bit uzunluğunda bir anahtar düz görüntüden üretilmektedir. Bu anahtar kriptografik özet algoritması (Message_Digest algortihm 5 (MD5)) yöntemi kullanılarak üretilmiştir. Anahtar üretmek için kullandığımız MD5 algoritması ile 3 satır matrisi oluşturulmaktadır. İlk satır matrisi, düz görüntünün satırlarının toplamından, 2. satır matrisi düz görüntünün sutünlarının toplamından ve 3. satır matrisi ise düz görüntünün köşegenlerinin toplamından oluşturulmaktadır. Lena görüntüsü üzerinde, sol üst köşesinin konumu (508,508) olan bir 5 x 5 bir matrisle herkese açık anahtar oluşumu Şekil 3.7'de verilmiştir.



Şekil 3.7: MD5 algoritması ile herkese açık anahtarın üretilmesi.

Şekil 3.7'de gösterildiği gibi, herkese açık üretilen anahtar ile yalnızca bizim erişimimize açık olan gizli anahtar XOR işleminden geçirilerek şifrelemede kullanılacak temel anahtar üretilmektedir.

Açık ve gizli anahtar onaltılık sayı tabanında ve 128 karakter uzunluğunda 2'li gruplar halinde, örneğin $(C8)_{16}=200_{10}$ şeklinde sırayla alınarak ondalık sayı sistemine dönüştürülmektedir. Böylelikle ondalık sayı tabanında,1x 64 uzunluğunda açık ve gizli anahtar elde edilmektedir. Elde edilen bu anahtarlar daha sonra XOR işlemine tabi tutularak temel anahtar (T) oluşturulmaktadır.

Başlangıç değerleriyle, permütasyon ve difüzyon işlemlerini gerçekleştirmek için kullanılan kaotik diziler oluşturulmaktadır. Şifrelemede kullanılacak iki kaotik diziyi üretmek için 2 adet kontrol parametresine ve 2 adet başlangıç değerine ihtiyaç vardır. Bu değerler, denklem 3.8, 3.9, 3.10 ve 3.11 ile hesaplanmaktadır.

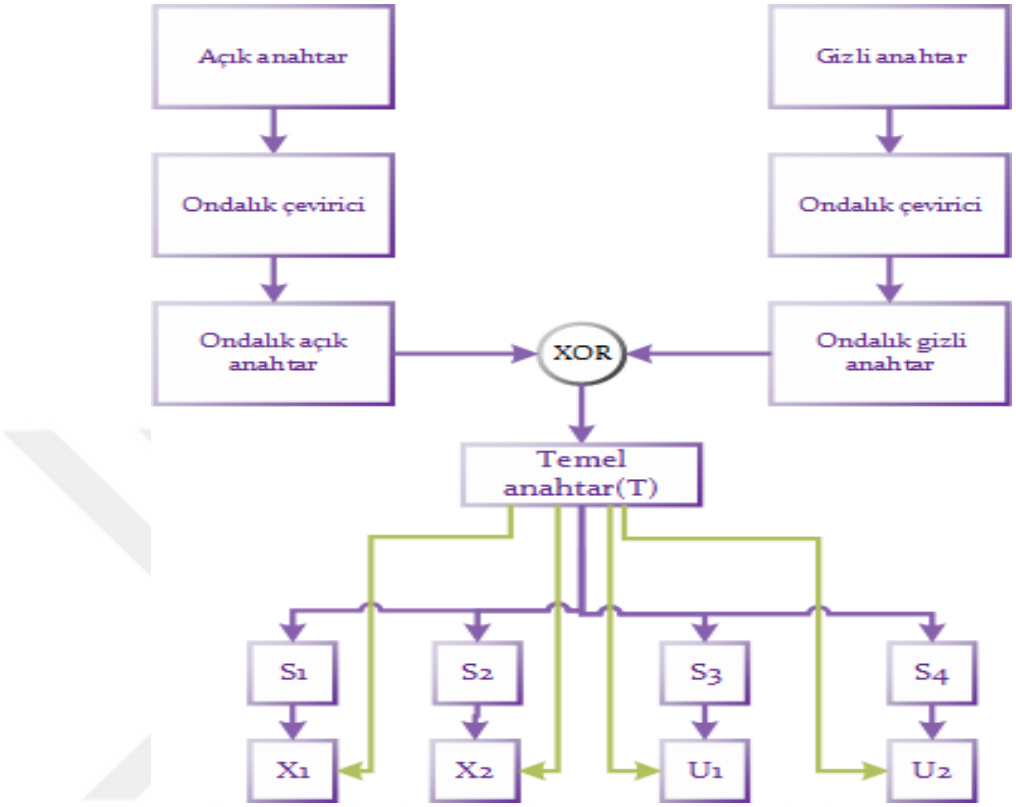
$$x_1 = (\sum_{i=1}^{16} T(i) + \text{mod}(\sum_{j=1}^{64} T(i), 255))/17 \times 255 \quad (3.8)$$

$$x_2 = (\sum_{i=17}^{32} T(i) + \text{mod}(\sum_{j=1}^{64} T(i), 255))/17 \times 255 \quad (3.9)$$

$$u_1 = \sum_{i=33}^{48} T(i) + mod(\sum_{j=1}^{64} T(i), 255)/17 \times 255 + mod(\sum_{i=33}^{48} T(i), 10) \quad (3.10)$$

$$u_2 = \sum_{i=49}^{64} T(i) + mod(\sum_{j=1}^{64} T(i), 255)/17 \times 255 + mod(\sum_{i=49}^{64} T(i), 10) \quad (3.11)$$

Burada; $x_1$ve x_2 başlangıç parametresi, $u_1$ve u_2 ise kontrol parametresini ifade etmektedir. T, 1x64 uzunluğunda temel anahtar matrisidir. Başlangıç değerleri olan x_1, x_2, u_1 ve u_2 üretimi Şekil 3.8'de gösterilmektedir.



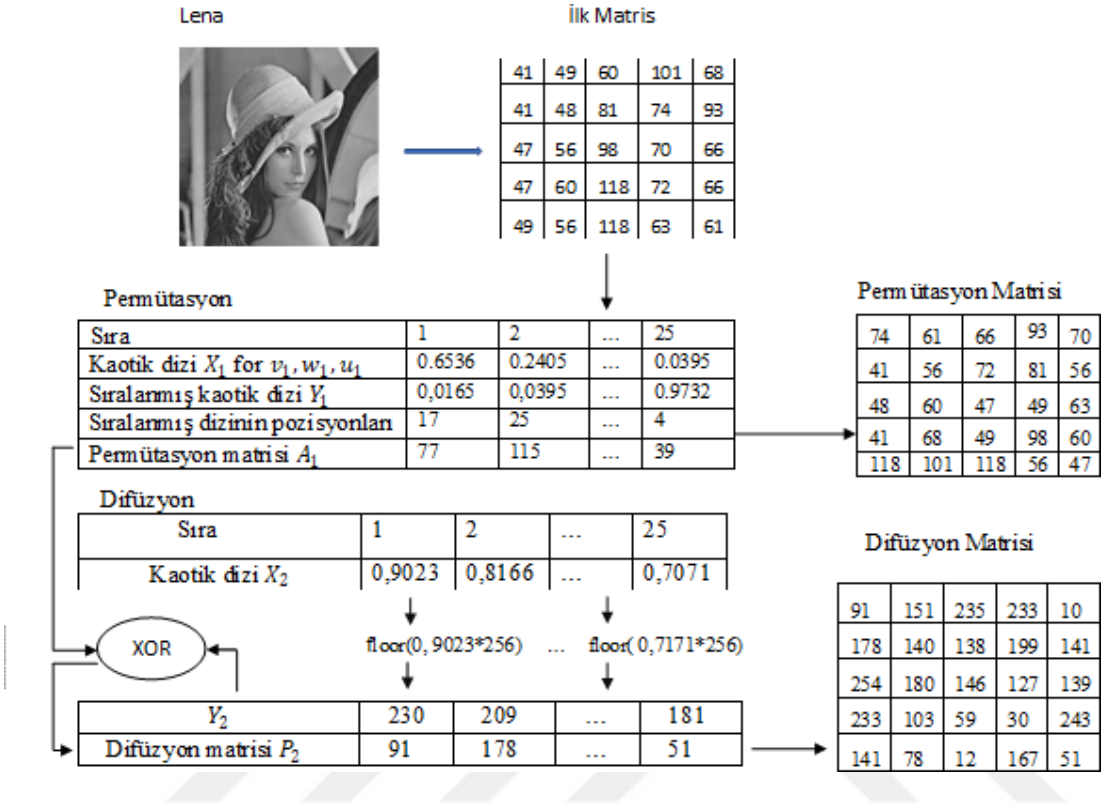
Şekil 3.8: Başlangıç değerlerinin üretilmesi.

3.3.1 Permütasyon

Düz görüntülerde, bitişik pikseller arasındaki korelasyon katsayısı oldukça yüksektir. Yatay-dikey ve çapraz bitişik pikseller arasındaki korelasyon katsayısı düz görüntülerde yüksektir. İyi bir şifreleme algoritmasının bitişik pikseller arasındaki korelasyon değerini düşürmesi önemlidir. Bitişik pikseller arasındaki korelasyonu düşürmek için şifreleme algoritmaları piksel konumlarını değiştirmektedir. Bu işleme şifreleme algoritmalarında permutasyon aşaması denilmektedir. Bu işlem yapılırken kaotik haritalar kullanılmaktadır. İlk olarak kaotik harita küçükten büyüğe sıralanmaktadır. Daha sonra düz görüntüdeki pikseller, sıralanan kaotik dizinin komum bilgilerine göre yer değiştirilmektedir. Böylelikle kontrollü bir yer değiştirme işlemi gerçekleştirilmektedir.

Bu çalışmada, permütasyon işlemi için, ilk olarak Bölüm 3.1'de önerilen kaotik harita ile X_1 kaotik dizisi oluşturulmaktadır. Daha sonra, X_1 kaotik dizisi küçükten büyüğe sıralanarak Y_1 dizisi ve P konum dizisi oluşturulur. X_1 dizisinde bulunan

elemanların P dizindeki sıra numaralarına göre oluşan yeni konumlarına göre, görüntünün piksel değerleri yer değiştirilerek A_1 permütasyon matrisi oluşturulmaktadır. Bu işlemler Şekil 3.9'de ve Algoritma 1'de gösterilmektedir.



Şekil 3.9: Permütasyon ve difüzyon aşamaları.

3.3.2 Difüzyon

İlk olarak uygulanan permütasyon işlemiyle, pikseller arasındaki korelasyon katsayısı azaltılmıştır. Fakat uygulanan bu permütasyon işlemi yalnızca piksellerin yerlerinin değiştirilmesi işlemini gerçekleştirdiği için piksel değerlerinde herhangi bir farklılık oluşmamıştır. Bu sebeple permütasyon uygulanarak oluşturulan yeni görüntü, orijinal görüntü hakkında bilgiler içermektedir. Bu durum, şifreleme algoritması üzerinde yalnızca permütasyon işlemi kullanmanın yeterince güvenli olmadığını ifade eder. Bunu ortadan kaldırmak için düz görüntüye ait herhangi bir bilgi şifreli görüntüde kalmaması için piksel değerlerinin değiştirilme aşaması olan difüzyon (manipülasyon) işlemi yapılmalıdır.

Permütasyon işleminden sonra yeni oluşturulan görüntüye ait piksellerin değerleri difüzyon aşamasında değiştirilmektedir. Böylelikle, difüzyon aşamasından ortaya çıkan görüntüde düz görüntüye ait hiçbir bilgi kalmamaktadır. Sonuç olarak,

şifrelenmiş görüntünün hem piksel değerleri hem de piksel konumları düz görüntüden tamamen farklıdır.

Permütasyon işlemi ile karıştırılmış görüntünün piksel değerlerini değiştirmek olan difuzyon aşaması Şekil 3.9'de ve Algoritma 1'de verilmiştir. İlk olarak, önerilen kaotik harita kullanılarak X_2 kaotik dizisi oluşturulur. X_2 dizisinin bütün elemanları 256 ile çarpılarak Y_2 matrisi elde edilir. Permütasyon işlemi sonrasında elde edilen A_1 matrisi ile Y_2 matrisi XOR işlemine tabi tutularak A_2 difüzyon matrisini oluşturulur. Yapılan bu işlemler, Şekil 3.9'de ve Algoritma 1'de verilmiştir.

3.3.3 Şifreleme algoritmasının sözde kodu

Şifreleme algoritması 3 aşamadan oluşmaktadır. İlk aşama başlangıç değerlerinin oluşturulmasıdır. İkinci aşama, piksel değerlerinin yerlerinin değiştirilmesi olan permutasyon kısmıdır. En son aşama ise, görüntünün piksel değerlerinin değiştirilmesi olan difüzyon bölümüdür. Bir kaotik dizi oluşturmak için başlangıç değerlerinin üretilmesi, Bölüm 3.2 anlatılmıştır. Diğer 2 aşama olan permütasyon ve difüzyon aşamalarının sözde kodu Algoritma 1'de verilmiştir.

Algoritma 1: Görüntü şifreleme algoritması.

1 Düz görüntüyü oku A

2 Bölüm 3.2.1'e göre başlangıç değerlerinin üret x_1, x_2, u_1 ve u_2

3 İki tane kaotik dizi üret $X_1 = [x_{1r}^1]_{1xmn}$, $X_2 = [x_{1r}^2]_{1xmn}$

4 $[Y_1\ P] = sort(X_1)$

5 **for** i=1 to mn

6 $\quad k = p_{1i}$

7 $\quad a_{1i}^1 = a_{1k}$

8 **End**

9 $Y_2 = floor(256X_2)$

10 $A_2 = A_1 \oplus Y_2$

11 A_2, mxn boyutuna getir

Algoritma 1'de ilk satırda, düz görüntü $1xmn$ boyutunda tek satırlık A matrisi oluşturulur. (Algoritma 1: satır 1). Sonrasında, başlağıç değerleri x_1, x_2, u_1, ve u_2, Bölüm 3.2'de anlatıldığı gibi üretilmektedir (Algoritma 1: satır 2). $1xmn$ uzunluğunda tek satırlık X_1 ve X_2 kaotik dizileri Bölüm 3.1'de önerilen yeni

kaotik harita kullanılarak üretilir (Algoritma 1: satır 3). Üretilen X_1 kaotik dizisi küçükten büyüğe sıralanır ve X_1 koatik haritada yer alan değerlerin indisleri P dizisine atanır (Algoritma 1: satır 4). 1xmn boyutundaki A matrisinde bulunan piksel değerleri P dizisindeki indis konumlarına göre yeni yerleri olan A_1 matrisine atanır (Algoritma 1: satır 5-8). Bu işlemden sonra düz görüntünün piksel değerleri karıştırılmış hali olan A_1 permutasyon matrisi elde edilir. Böylelikle şifrelemenin en önemli aşamalarından olan piksellerin karıştırma işlemi gerçekleştirilmiş olur. Şifreleme işlemini güçlendirmek için piksellerin değerlerini deşiştirerek görüntüye difüzyon işlemi uygulanır. Difüzyon işlemini uygulamak için ise, X_2 kaotik dizisi 256 sayısı ile çarpılıp aşağı yuvarlama işlemi yapılmıştır (Algoritma 1 satır 9). Aşağı yuvarlama işlemi (floor), sayının virgülden sonraki kısmının atılması işlemidir. Bu işlemler sonrasında $[1,2,3,\ldots,256]$ tam sayı değerlerinden oluşan 1xmn boyutunda Y_2 dizisi elde edilir. Bütün bu işlemler, A_1 matrisi ile XOR işlemi uygulayacağımız bir dizi elde etmek için gerçekleştirilmektedir. Y_2 permütasyon matrisi olan A_1 ile XOR işlemine tabii tutularak A_2 difüzyon matrisi elde edilmektedir (Algoritma 1 satır 10). Bu işlemle düz görüntüdeki piksel değerleri de değiştirilir. Son olarak, A_2 matrisi mxn boyutuna dönüştürülerek şifreli görüntü elde edilir.

3.3.4 BOA'nun uygulanması

3.4 Görüntüden Parça Alınması

Gerçek zamanlı görüntü şifreleme işlemi gerçekleştirmek için görüntüyü şifreleyecek optimum anahtarı elde etmek amacı ile görüntüden 80 x 80 boyutunda bir kesit alınmakta ve BOA optimizasyon işlemine tabii tutulmaktadır. Görüntünün tamamını işleme tabi tutarak optimum bir temel ahahtar aramak hem işlem uygulama yükü, hem zaman açısından maliyetlidir. Tüm görüntü üzerinde optimum temel anahtar arama işlemi gerçekleştirmek gerçek zamanlı uygulamalarda kullanmak için uygun bir yöntem değildir. Bu sebeple şifreleme işlemi gerçekleştirilmek için görüntüden rastgele seçilen 80 x 80 boyutunda bir kesit alınmaktadır. Bu kesite şifreleme işlemi uygulanmakta ve görüntünün tamamını şifreleyecek anahtar BOA ile optimize edilmektedir. Görüntüden alınan bu 80 x 80 'lik kesitin başlangıç koordinatları (x, y), rastgele iki koordinat üretilirek bulabilmektedir. Görüntü satır ve sütün boyutundan 80'lik parça çıkartılarak görüntü için belirlenen boyut aşılmamaktadır. Bu demek oluyor ki, 512 x 600 boyutundaki görüntüden optimize edilecek parçanın

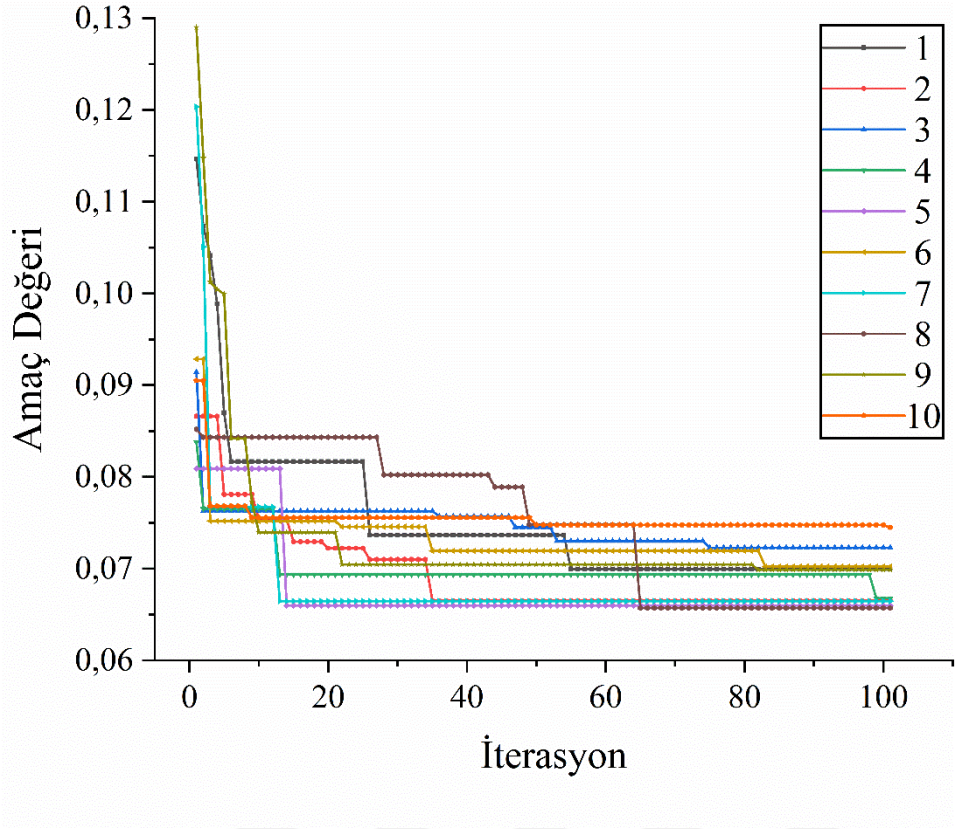
sağ alt köşe başlangıç noktaları (x, y) seçimi ([1 508] [1 512]) değerleri arasından rastgele olarak yapılmaktadır.

3.5 Başlangıç Popülasyonunun Oluşturulması ve Maliyet Fonksiyonu

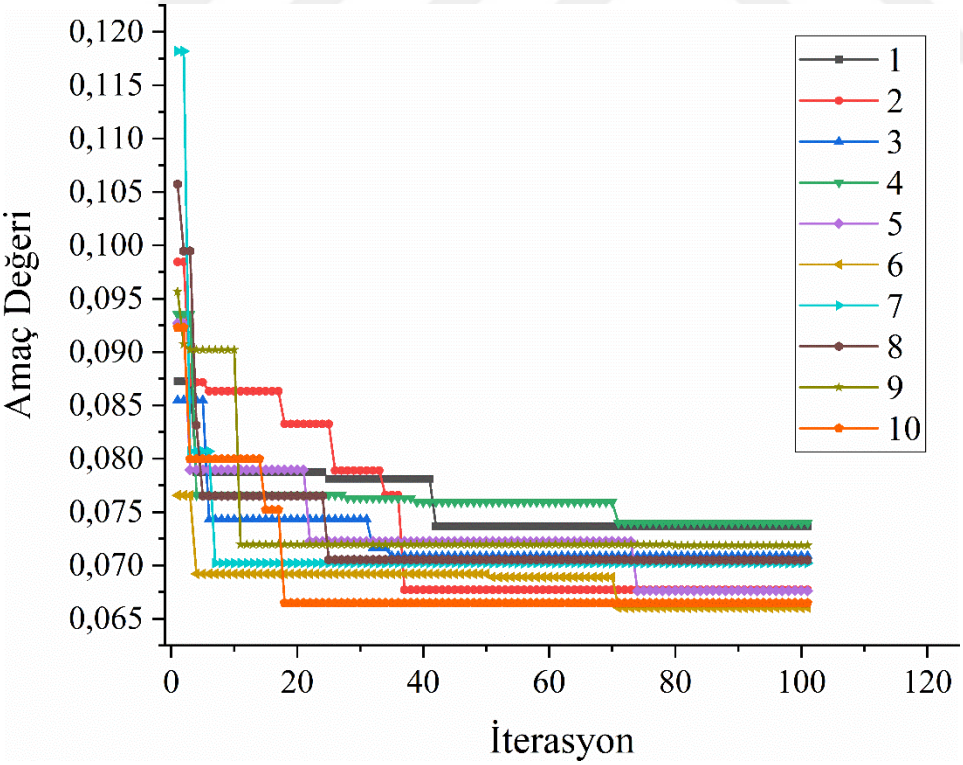
Görüntü şifreleme işleminin önceliği hızlı ve güçlü bir şifreleme yapısına sahip olmasıdır. Bu nedenle optimizasyon algoritması kullanılarak, görüntü şifreleme işleminde pikseller arası en düşük korelasyon katsayısını ve en yüksek entropi değerini veren anahtarı üretmek amaçlanmaktadır. Şifrelenmiş görüntüdeki pikseller arası korelasyon değerinin düşük olması şifreleme yönteminin gücünü göstermektedir. Ayrıca gri ölçekli 8-bit şifrelenmiş bir görüntüde entropi değerinin 8'e yakın olması istenmektedir. Korelasyon katsayısının ve entropi değerinin nasıl hesaplandığı detaylı bir şekilde Bölüm 2.7'de anlatılmıştır. Optimizasyon işlemini kolaylaştırmak için entropi değerini minumum amaç fonsiyonuna uydurmak için entropi değeri 8'den çıkarılır. Bilgi entropi ve korelasyon fonksiyonuna doğrusal ağırlıklandırma yapılmış ve iki farklı amaç için çalışan optimizasyonu tek bir amaç çözümüne ulaştırılmıştır. BOA'nun amaç fonksiyonu denklem 3.13'de verilmiştir.

$$F(\mathrm{c}) = w_1 C_o(c) + w_2(8 - H(c)) \tag{3.13}$$

Denklem de c şifreli görüntü, C_o korelasyon fonksiyonu, H bilgi entropi fonksiyonu ve w_1, w_2=0,5 ağırlık katsayıları olarak ifade edilmektedir. BOA optimizasyon algoritmasında kelebekler arasında bulunan amaç değerlerini hesaplamak için Bölüm 3.2.1 de bahsedilen temel anahtar ile XOR işlemi yapılmaktadır. Elde edilen sonuç ile düz görüntüden alınan 80x80'lik kesit ile denklem 3.13'e göre amaç değerleri hesaplanmaktadır. Hesaplanan amaç değerlerine göre kelebeklerin en iyi koku değeri ve sürüdeki en iyi kelebek koku değeri hesaplanır. Amaç değerlerinin iterasyon boyunca düşüşleri, Lena ve Cameraman görüntüleri için algoritmanın 10'ar kez çalıştırılmasının sonuçları aşağıda bulunan Şekil 3.10 ve Şekil 3.11'te verilmiştir.



Şekil 3.10: Lena için amaç değer grafiği.



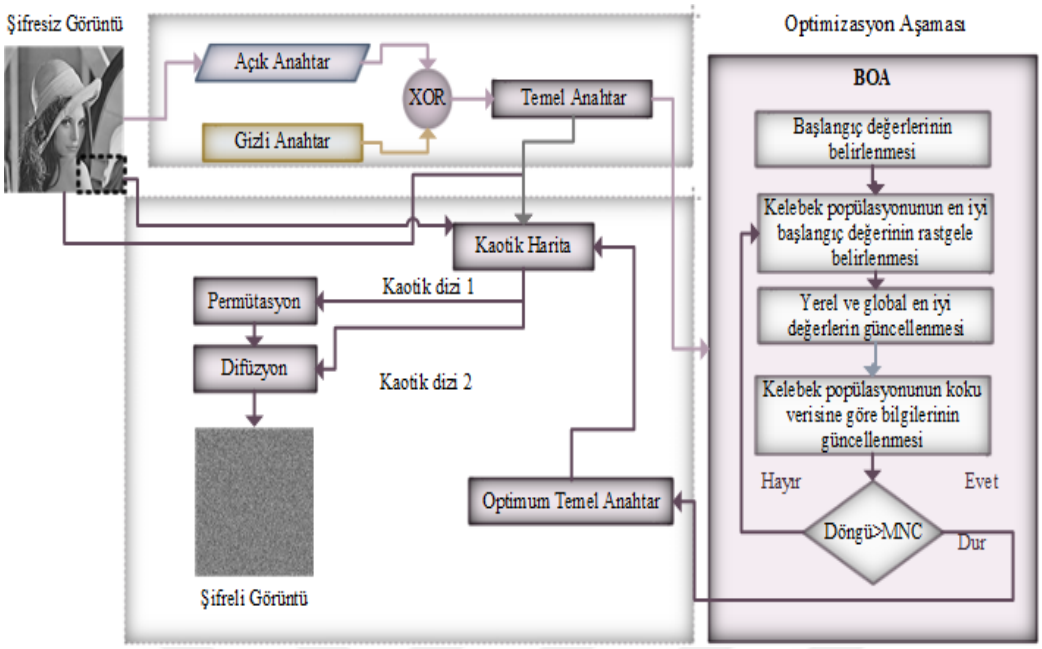
Şekil 3.11: Cameraman için amaç değer grafiği.

3.6 Görüntüyü Şifreleyecek Optimum Anahtarın Bulunması

Bir şifreleme sistemin en önemli unsurlarından birisi kullanılan anahtardır. Anahtar genelde şifreleme algoritmalarında kaotik dizilerin başlangıç değerlerini üretmekte kullanılmaktadır. Şifreleme işlemlerinde ise bu kaotik diziler kullanılmaktadır. Şifreleme algoritmasının performansı ise direk olarak bu kaotik dizilerin performansı ile değişmektedir. Bu çalışmada optimum anahtar elde etmek için kelebek optimizasyon algoritması kullanılmıştır. Kelebek optimizasyon algoritmasının sözde kodu Algoritma 2'de verilmiştir. İlk olarak, kelebek optimizasyon algoritmasında amaç fonksiyonu, başlangıç popülasyonu ve çözüm uzayı tanımlanmakta ve BOA'da kullanılan parametrelerin değerleri $x_i = (i = 1,2, \dots, n)$ atanmaktadır (Algoritma 2: satır 1-2). Kelebeklerin konumları, arama alanı içinde rastgele oluşturulduktan sonra, koku ve zindelik değerleri hesaplanmakta ve saklanmaktadır. (Algoritma 2: satır 3). Daha sonra, x_1, x_2, u_1 ve u_2 başlangıç değerleri Bölüm 3.2.1'e göre atandıktan sonra, her yinelemede, çözüm uzayındaki tüm kelebekler yeni konumlara taşınır (Algoritma 2: satır 4). Ardından amaç değerleri hesaplanır (Algoritma 2: satır 5-8). Amaç değerleri hesaplandıktan sonra global ve yerel aramalar gerçekleştirilir (Algoritma 2: satır 9-17). Durdurmak için uygun değerler sağlanana kadar bu işleme devam edilir. (Algoritma 2: satır 18-20). Önerilen şifreleme algoritmasının tamamına ait akış diyagramı Şekil 3.12'de gösterilmiştir.

Algoritma 2: Kelebek optimizasyon algoritması.

1	Amaç fonksiyonu $f(x)$, $x = (x_1, x_2, \dots, x_{dim})$, dim = 50 buyutlu
2	n Kelebeklerin başlangıç popülasyonunu oluştur. $x_i = (i = 1,2, \dots, n)$
3	Uyaran yoğunluğu l_i, $f(x_i)$,'deki x_i tarafından belirlenir.
4	Sensör modalitesi c, güç üssü a ve anahtarlama olasılığı p
5	**While** durdurma kriterleri karşılanmadı **do**
6	**For each** Popülasyondaki kelebek bf **do**
7	Eq1'i kullanarak bf için kokuyu hesaplayın
8	**End for**
9	en iyi bf bul
10	**For each** Popülasyondaki kelebek bf **do**
11	[0,1]'den rastgele bir sayı r üret
12	**İf** r<p
13	EQ2 kullanarak en iyi kelebeğe/çözüme doğru ilerleyin
14	**Else**
15	EQ3 kullanarak rastgele hareket edin
16	**End if**
17	**End for**
18	a değerini güncelle
19	**End while**
20	Blunan en iyi çözümü çıkar.



Şekil 3.12 : Görüntü şifreleme diyagramı.

4. GÜVENLİK VE PERFORMANS ANALİZİ

Görüntü Şifreleme analizleri için 512x512 boyutunda, (Lena-Cameraman-Barbara-Baboon-Goldhill-Jetplane-Korsan-Livingroom-Lake) adlı 10 adet test görüntüsü kullanılmıştır. Görüntü şifreleme için kullanılan test analizleri aşağıdaki şekilde sıralanmaktadır.

- Gizli anahtar alanı analizi
- Anahtar duyarlılık analizi
- Bilgi entropi analizi
- Histogram analizi
- Korelasyon analizi
- Ki-kare analizi
- Diferansiyel atak analizi
- Veri kaybı analizi
- Gürültü analizi
- Seçilen açık metin saldırısına ve bilinen açık metin saldırısı analizi
- Hız zaman analizi

4.1 Gizli Anahtar Alanı Analizi

Bir görüntü şifreleme algoritmasının, Brute Force saldırılarına direnmek için yeterince büyük bir güvenlik anahtarı alanına sahip olması önemlidir. Önerilen şifreleme algoritmasında, permutasyon ve difusyon işlemlerinde kullanılmak için iki adet kaotik diziye ihtiyaç vardır. İki adet kaotik dizi üretmek için, dört adet değer lazımdır. Bunlar, kontrol parametresi u_1, u_2 ve başlangıç değeri x_1, x_2'dir. Dört değişken için şifreleme alanı genişliği $10^{16x4} = 10^{64}$ olacaktır. Kaba kuvvet saldırılarına dayanacak bir anahtarın, 2^{100}'den daha büyük bir anahtar değerine sahip olması gerekmektedir. Bu çalışmada anahtar hassasiyeti $10^{64} \cong 2^{213}$'dir. $2^{213} > 2^{100}$olduğundan, önerilen şifreleme algoritması kaba kuvvet saldırılarına karşı dirençlidir.

4.2 Anahtar Duyarlılık Analizi

Şifreleme algortiması, gizli anahtarların değiştirilmesine duyarlı olmalıdır. Gizli anahtardaki küçük bir değişiklik çıktı sonucununda büyük bir değişiklik ortaya çıkarmalıdır. Anahtar hassasiyetini analiz etmek için iki durum bulunmaktadır. Birincisi, gizli anahtarda yapılan 1-bit değişiklik yaparak şifreli görüntüler arasındaki farkın ölçülmesidir. İkincisi, gizli anahtarda 1-bit değişiklik yapılarak şifreli görüntüyü çözmektir. Çizelge 4.1'de, orijinal anahtar, anahtar 1, anahtar 2, anahtar 3 ve anahtar 4, yalnızca 1-bit farkıla dört gizli anahtar gösterilmektedir.

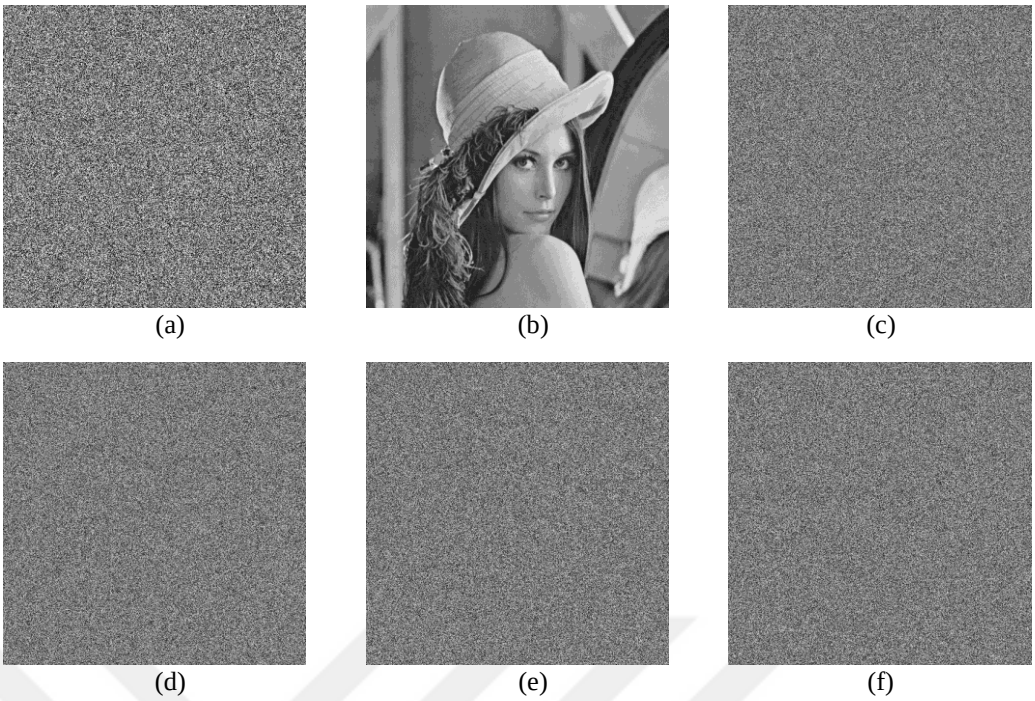
Çizelge 4.1 : Birden fazla anahtar kullanarak anahtar duyarlılık analizi.

Anahtar İsmi	**Anahtar**
Anahtar	5a219594e66546e4cb619bf60df1f7a43863ecbbc2d29b6d616c0af8b9276c175e0 d14d4dd4fd49fa49d50cc3038edde0638cb6e4f1d2bda964f8738ec1f8969
Anahtar 1	**6**a2c36e52365f3533520589f83ed80dcef3d1c2e6faa46b21a734416867294bc7c7 9c1e12d78daaf1eb579a55ba5e403aed40494542fbe4e50ada581407fe88b
Anahtar 2	**7**a2c36e52365f3533520589f83ed80dcef3d1c2e6faa46b21a734416867294bc7c7 9c1e12d78daaf1eb579a55ba5e403aed40494542fbe4e50ada581407fe88b
Anahtar 3	**8**a2c36e52365f3533520589f83ed80dcef3d1c2e6faa46b21a734416867294bc7c7 9c1e12d78daaf1eb579a55ba5e403aed40494542fbe4e50ada581407fe88b
Anahtar 4	**9**a2c36e52365f3533520589f83ed80dcef3d1c2e6faa46b21a734416867294bc7c7 9c1e12d78daaf1eb579a55ba5e403aed40494542fbe4e50ada581407fe88b

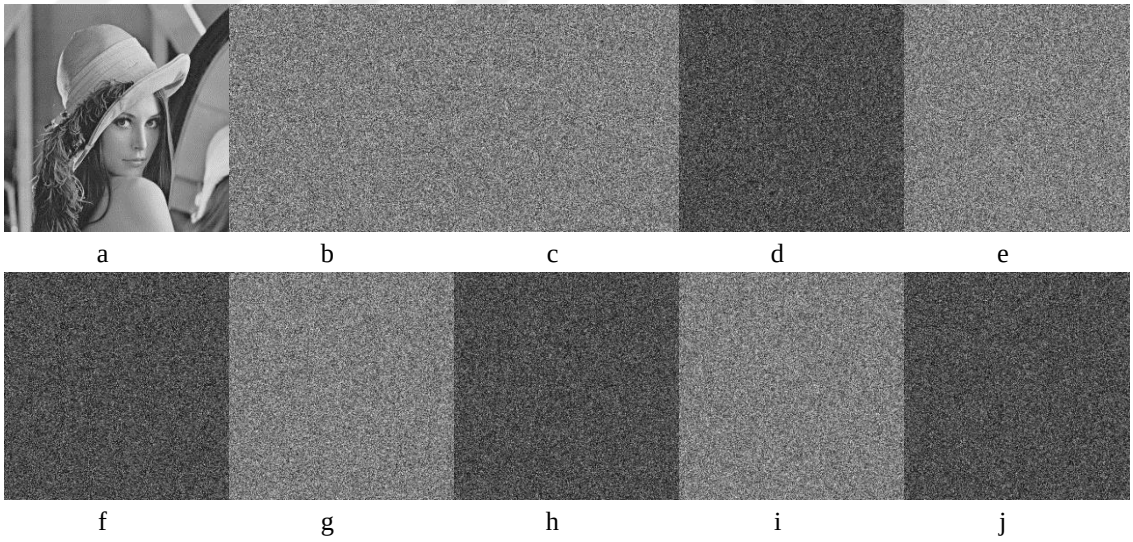
Çizelge 4.2 : Bir biti değiştirilmiş şifreli görüntüler arasında sayısal farklılıklar.

Şekiller	Şifreleme anahtarı	4.2(b)ile (%)'lik fark
4.2(c)	Anahtar 1	99.3858
4.2(e)	Anahtar 2	99.3843
4.2(g)	Anahtar 3	99.3877
4.1(i)	Anahtar 4	99.3927
Ortalama		99.3876

İlk durum için, Şekil 4.1'de gösterildiği gibi Lena görüntüsünü anahtar, anahtar 1, anahtar 2, anahtar 3 ve anahtar 4 ile şifresi çözülmüş görüntüler verilmiştir. 1-bit değiştirilmiş 4 gizli anahtar için, sırasıyla Şekil 4.1(c), (d), (e) ve (d) 'de gösterilen 4 şifresi çözülmüş görüntü gösterilmektedir. Algoritmamız gizli anahtarlara karşı çok hassas bir davranış sergilemektedir.



Şekil 4.1: Anahtar Duyarlılık Analizi1 (a) Anahtar ile şifreleme görüntüsü, (b) Orijinal Anahtar ile şifresi çözülmüş görüntü (c) Anahtar 1 ile şifrelesi çözülmüş görüntü, (d) Anahtar 2 ile şifresi çözülmüş görüntü, (e) Anahtar 3 ile şifresi çözülmüş görüntü, (f) Anahtar 4 ile şifresi çözülmüş görüntü.



Şekil 4.2: Anahtar duyarlılık analizi2: (a) düz görüntü; (b) Anahtar ile şifreli görüntü; (c) Anahtar1 ile şifreli görüntü; (d) b ve c görüntüleri arasındaki fark görüntüsü; (e) Anahtar2 ile şifreli görüntü; (f) b ve e görüntüleri arasındaki fark görüntüsü; (g) Anahtar3 ile şifreli görüntü; (h) b ve g görüntüleri arasındaki fark görüntüsü; (i) Anahtar4 ile şifreli görüntü; (j) b ve ı görüntüleri arasındaki fark görüntüsü.

Anahtar duyarlılığını ölçmek için ikinci olarak, anahtarda 1-bit değişiklik yapılarak şifreli görüntüler arasındaki farka bakılmaktadır. Bunu ölçmek için 1-biti değiştirilmiş anahtarla yapılan şifreli görüntüler ve bunlar arasındaki farklar Şekil 4.2'de verilmiştir. Şekil 4.2(a) orjinal Lena görüntüsü, 4.2(b) orijinal anahtar ile şifrelenmiş görüntü, Şekil 4.2(c) anahtar1 ile şifrelenmiş görüntü gösterilmektedir. Şekil 4.2(d)'de, Şekil 4.2(b)'den Şekil 4.2(c) görüntüsünün çıkarılmasıyla elde edilen fark görüntüsü gösterilmektedir. Şekil 4.2(e)'de, anahtar2 ile şifrelenmiş görüntü gösterilmektedir. Şekil 4.2(f) de, Şekil 4.2(b)'den Şekil 4.2(d) görüntüsünün çıkarılmasıyla elde edilen görüntü verilmektedir. Şekil 4.2(g)'de, anahtar 3 ile şifrelenmiş görüntü verilmektedir. Şekil 4.2(h)'da, Şekil 4.2(b) ile Şekil 4.2 (g) 'yi birbirinden çıkarılmasıyla elde edilen görüntü gösterilmektedir. Şekil 4.2 (i)'de, anahtar 4 ile şifrelenmiş görüntü gösterilmektedir. Son olarak, Şekil 4.2 (b) ile Şekil 4.2 (i)'ye ait fark görüntüleri Şekil 4.2(j)'de gösterilmektedir. Fark görüntüleri tamemen siyah (0) olsaydı veya fark görüntüleri üzerinde siyah alanlar olmuş olsaydı bu şifreli görüntüler arasında fark olmadığını gösterecekti. Şekil 4.2'deki fark görüntülerine bakıldığında hemen hemen hiç tamemen siyah piksele sahip görüntü bulunmamaktadır. Şifreli görüntüler arasındaki farkları sayısal değerle ifade etmek için, şifreli görüntüler arasındaki fark Çizelge 4.2'de gösterilmektedir. Çizelge 4.2(b) ile diğer şifreli görüntüler arasında ortalama fark %99.3876 bulunmaktadır. Bu sonuç, geliştirilen şifreleme yönteminin anahtar duyarlılığının çok yüksek olduğunu göstermektedir.

4.3 Bilgi Entropi Analizi

4.3.1 Global entropi

Bilgi entropisi değerlendirmesi, şifrelenmiş görüntülerin rastgeleliğini tahmin etmek için iyi bir yoldur. Bir sistemin düzensizlik derecesini açıklamak için entropi değeri kullanılmaktadır. Kayıpsız veri sıkıştırma, kriptografi ve makine öğrenimi dahil birçok alanda entropi kullanılmaktadır. Genel olarak, bilgi kaynağı ne kadar rastgele veya belirsizse olursa entropi değeri o kadar yüksek olmaktadır. Bu nedenle, bir şifreleme algoritmasının rasgeleliğini analiz etmek için bilgi entropisi kullanılır. Bilgi entropisi, denklem 4.1 ile hesaplanmaktadır.

$$\mathrm{H}(S) = -\sum_{i=0}^{2^m-1} p(S_i).log_2 p\left(\frac{1}{p(S_i)}\right) \tag{4.1}$$

Burada, P (·) piksel yüzdesini hesaplamak için ayrık olasılık yoğunluk fonksiyonudur. Bilgi entropisinin gri ölçekli görüntülerde maksimum değer olan 8'e yakın olması, şifrelenen görüntünün mükemmel rastgelelik özellikleri kazandığı anlamına gelir. Gri tonlamalı bir görüntü için S, [0,255] aralığında bir tam sayıdır. Gri tonlamalı görüntüdeki her piksel 8-bit ile temsil edilir. Çizelge 4.3'te 10 şifrelenmiş görüntünün entropi değeri verilmektedir. Görüntülerin entropi değeri 8'e yakındır ve bu da bilgi entropisinde iyi bir performansa sahip olduğu anlamına gelir. Şifrelenmiş görüntü piksel değerlerinin bir $[0, S]$ aralığında eşit olarak dağılması düz görüntüye ait herhangi bir istastiki bilgi kalmadığını göstermektedir.

4.3.2 Yerel entropi

Yerel entropi göründen rastgele seçilen blokların entropisinin ortalamasıdır. Bu değer, şifreli görüntünün yerel dağılımının analizini yapmaktadır. Bu değer ne kadar yüksek olursa, piksellerin şifreli görüntü içerisinde yerel olarak iyi dağıldığını gösterir. Bu entropiye Yerel Shannon entropisi de denilmektedir ve denklem 4.2'deki gibi hesaplanmaktadır.

$$\overline{H}_{k.T_B}(S) = -\sum_{i=0}^{k} \frac{H(S_i)}{k} \tag{4.2}$$

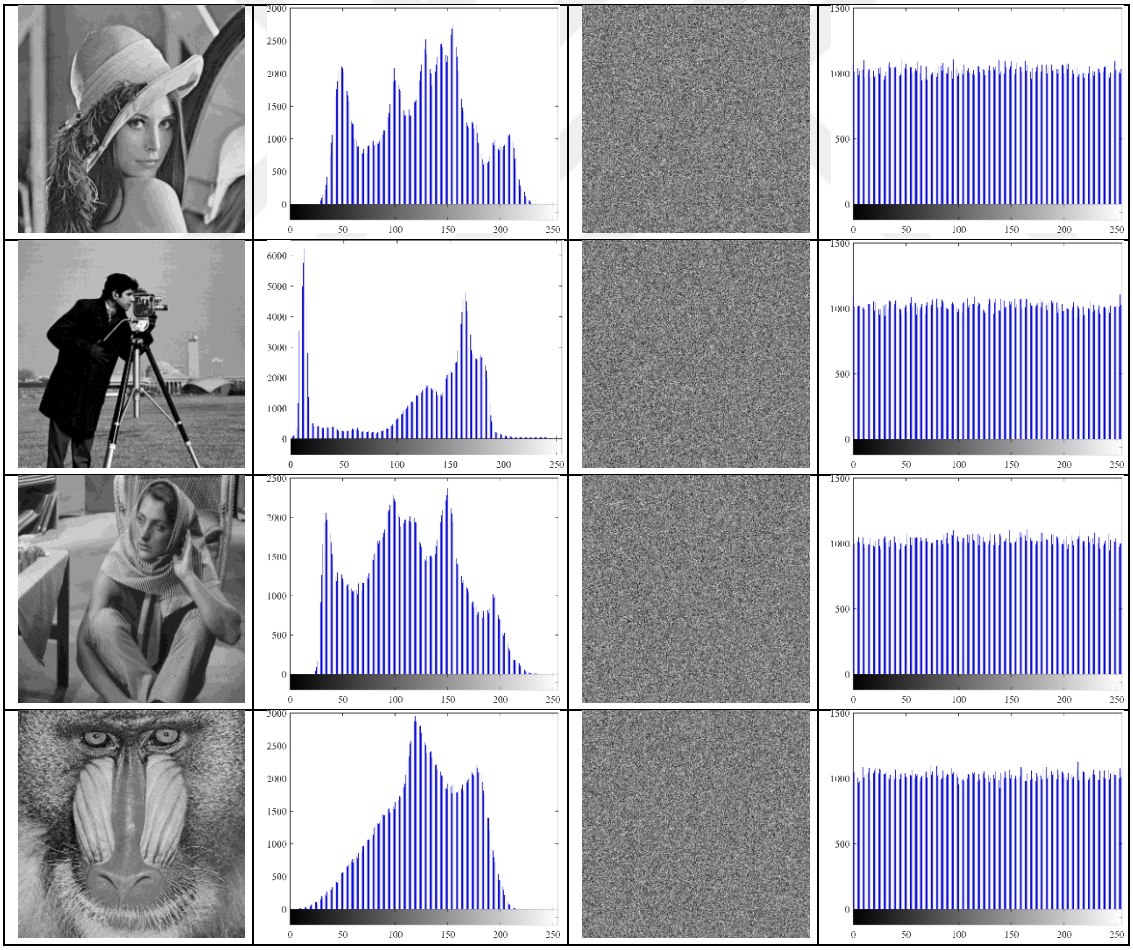
Burada S şifreli bir görüntü ve T_B rastgele seçilen piksel sayısıdır. k ise, seçilen blok sayısıdır. Bu tez çalışmasında $k = 50$ ve $T_B = 1936$ seçilmiştir. Test sonuçları Çizelge 4.3'te gösterilmektedir. Şifrelenmiş görüntüler, yerel entropi değerlerine göre iyi bir rastgelelik sağlamaktadır.

Çizelge 4.3 : Küresel entropi ve yerel entropi testleri.

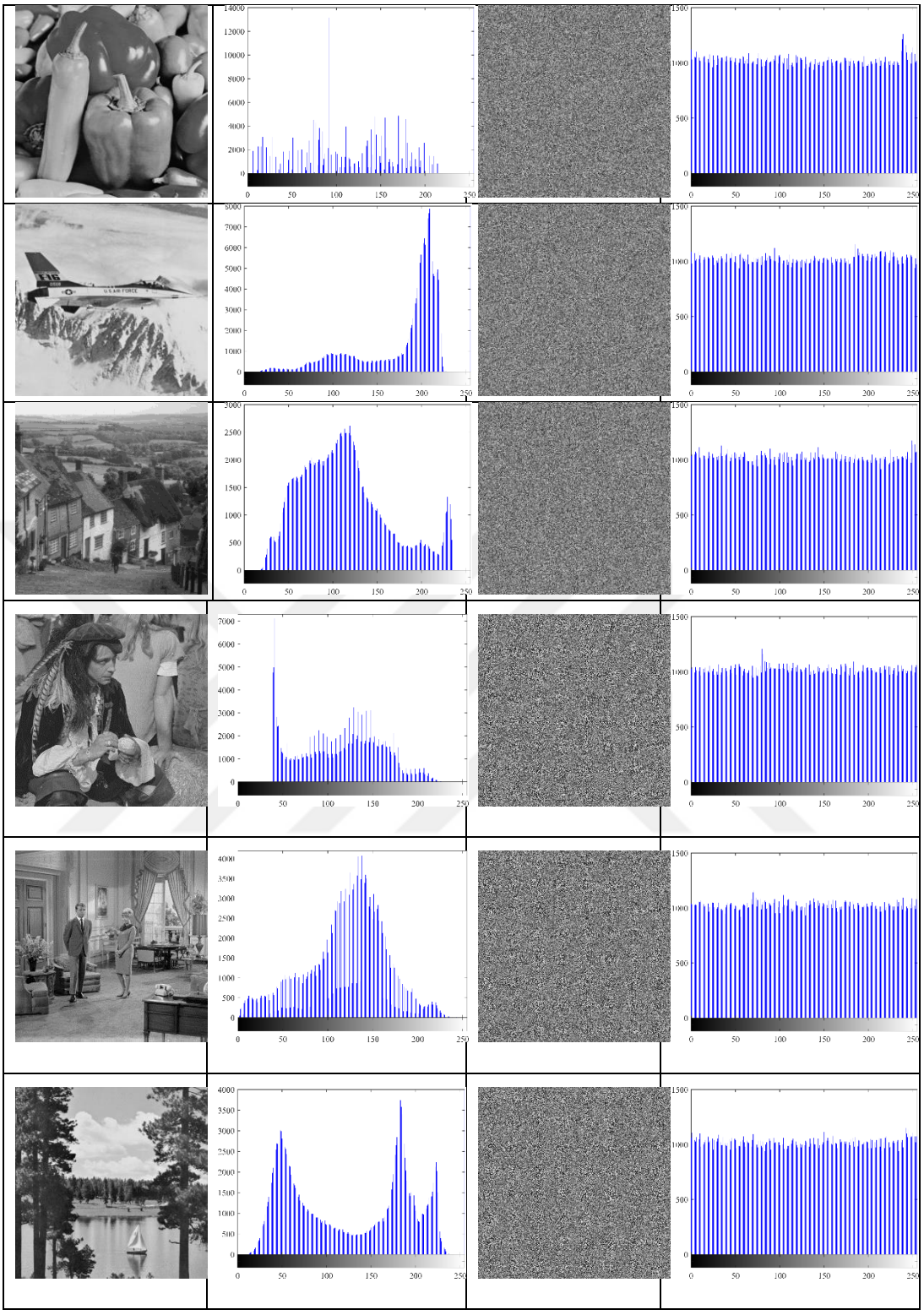
Test görüntüsü	Global Entropi	Yerel Entropi
Lena	7.9994	7.9129
Cameraman	7.9993	7.9121
Peppers	7.9993	7.9152
Baboon	7.9994	7.9133
Barbara	7.9994	7.9114
Goldhill	7.9993	7.9115
Jetplane	7.9993	7.9111
Korsan	7.9994	7.9090
Living room	7.9993	7.9101
Lake	7.9993	7.9171

4.4 Histogram Analizi

Bir görüntünün piksel değerlerinin dağılımını göstermek için histogram kullanılmaktadır. Düz görüntülerin piksel değerlerinin dağılımı eşit değildir ve bir bölgede yoğunlaşmaktadır. Şifreleme algoritmasıyle şifrelenen bir görüntüye ait histogram görüntüsünde piksel değerlerinin dağılımının düzgün olması beklenmektedir. Şifreli görüntünün histogramı ne kadar düzgün olursa şifreleme performansı o kadar iyidir ve saldırılara karşı dayanıklıdır. Ayrıca, şifrelenmiş görüntüde o kadar güvenlidir. Şekil 4.3'te, 10 adet düz ve şifrelenmiş görüntüye ait histogram grafikleri verilmiştir. Düz görüntünün piksel değerlerinin dağılımının bir bölgeye yerleştiği ve birbirinden farklı olduğu görülmektedir. Şifrelemeden sonra piksel değeri dağılımının eşit olarak dağıldığı görülmektedir. Böylelikle yeni önerilen şifreleme algoritmasının bilinen şifre saldırılarına karşı yeterli güvenliğe sahip olduğunu söylenebilir.



Şekil 4.3: 10 farklı orijinal görüntü ve karşılık gelen şifreli görüntülerin histogram analizi.



Şekil 4.3 (devam): 10 düz görüntü ve karşılık gelen şifreli görüntülerin histogram analizi.

4.5 Ki-kare Testi ve Varyans analizi

Şifreli bir görüntünün histogram tekdüzeliği Ki-kare (χ^2) testi ile ölçülür. χ^2 testi, şifreli bir görüntünün tekdüze dağılımdan ne kadar saptığını nicel olarak hesaplamak için kullanılmaktadır. χ^2 testi, denklem 4.3'e göre şu şekilde tanımlanır:

$$X^n = \sum_{k=1}^{n} \frac{\big(0(k) - E(k)\big)^2}{E(k)} \tag{4.3}$$

burada n, görüntü 8-bit olduğu için $2^8 - 1 = 255$ olmaktadır. Burada, $O(k)$ gözlenen değer ve $E\,(k)$ beklenen değerdir. $512 \text{ x } 512$ boyutlu bir görüntüde beklenen değer $(512 \text{ x } 512)/256 = 1024$'tür. χ^2 testinin başarılı olması için, $\alpha = 0.05$ önem seviyesi için χ^2 değerinin 293.2478'den küçük olması gerekmektedir. $512 \text{ x } 512$ gri tonlamalı 10 adet düz ve şifreli görüntü için χ^2 test sonuçları Çizelge 4.4'de verilmiştir. Yeni geliştirilen algoritmayla şifrelenen tüm görüntülerin χ^2 değerleri, olması gereken değerden daha düşüktür. Bu sonuçlar, önerilen şifreleme algoritmasının χ^2 testini geçtiğini göstermektedir. χ^2 testi sonuçlarına göre, önerilen şifreleme algoritması istastiki saldırılara karşı dayanıklıdır.

Şifreli görüntünün histogram piksel tekdüzeliği için histogramın varyans analizini yapılmaktadır. Küçük bir varyans değeri yüksek tek düzeliği gösterirken, yüksek bir varyans değeri düz olmayan bir histogramı göstermektedir. Çizelge 4.4'de χ^2 değerlerine ek olarak varyans ölçümleride verilmiştir. Önerilen şifreleme yöntemi, çok düşük değerler ürettiğinden tek düze bir dağılıma sahiptir. Varyans değeri, denklem 4.4'deki gibi hesaplanmaktadır.

$$Var(Z) = \frac{1}{n^2} \sum_{i=1}^{N} \sum_{j=1}^{N} \frac{1}{2} (z_i - z_j) \tag{4.4}$$

Burada, n gri ölçekli görüntüyü ifade eder ve $Z = \{z_1, z_2, \dots, z_{256}\}$ histogram değerlerinin vektörünü temsil etmektedir. z_i ve z_j sırasıyla i ve j'ye eşit olan piksel sayılarıdır.

Çizelge 4.4 : Ki-kare test görüntüsünün ki-kare değeri.

Test Görüntüleri	χ^2		Varyans	
	Düz Görüntü	Şifreli Görüntü	Düz Görüntü	Şifreli Görüntü
Lena	158344.71	247.35	633378.87	983.37
Cameraman	418530.14	261.25	1674120.58	994.41
Peppers	549151.27	255.84	2196605.10	989.66
Baboon	211365.83	262.46	845463.33	975.46
Barbara	144101.11	235.75	576404.47	996.40
Goldhill	161621.18	246.98	646484.72	985.27
Jetplane	100446.94	263.48	100446.94	986.12
Korsan	267545.48	234.99	1070181.92	997.21
Livingroom	110726.32	241.04	110726.32	969.31
Lake	181224.16	233.43	724896.67	998.52

4.6 Korelasyon Analizi

Düz görüntü çok fazla miktarda bilgi barındırmaktadır. Bu durum, bitişik piksellerin arasında güçlü bir korelasyon sağlar. İyi bir şifreleme algoritması bitişik pikseller arasındaki korelasyonu azaltmalıdır. Böylece şifreleme görüntünün daha iyi güvenlik performansına sahip olması sağlanır. Bu çalışmada sırasıyla yatay, dikey ve çapraz yönden korelasyonu hesaplamak için şifreli görüntüden rasgele 2500 çift bitişik piksel seçilmektedir. Korelasyon katsayısı, denklem 4.5, 4.6 ve 4.7 göre hesaplanır:

$$r_{x,y} = \frac{\mathrm{E}\Big(\big(\mathrm{x} - \mathrm{E}(\mathrm{x})\big)\big(\mathrm{y} - \mathrm{E}(\mathrm{y})\big)\Big)}{\sqrt{D(x)D(x)}} \tag{4.5}$$

$$E(\mathrm{x}) = \frac{1}{N}\sum_{i=0}^{N} x_i \tag{4.6}$$

$$\mathrm{D}(\mathrm{x}) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2 \tag{4.7}$$

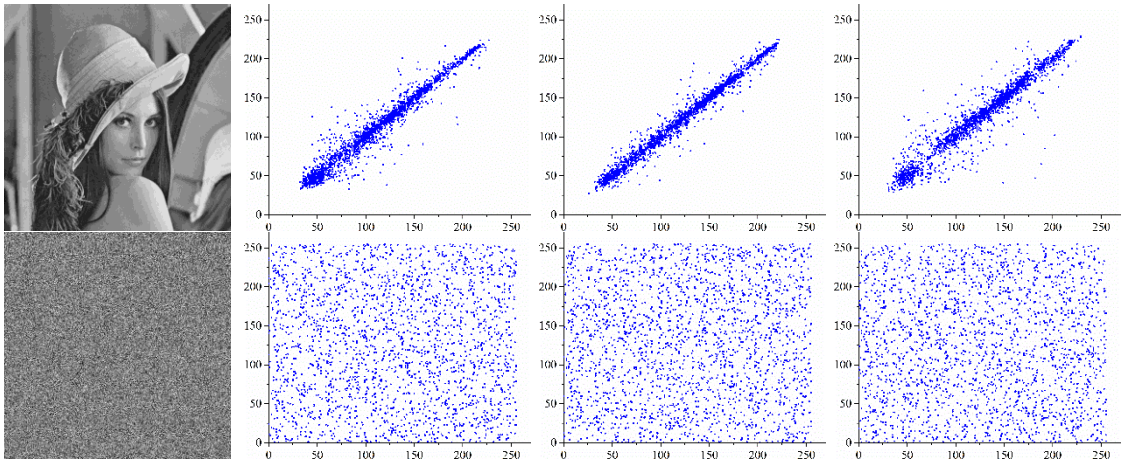
burada x ve y, iki bitişik pikselin gri seviye değerleridir. N, görüntüden seçilen toplam piksel sayısıdır. $E(x)$ ve $D(x)$ sırasıyla x değişkeninin beklentisi ve varyansıdır. On adet düz ve şifrelenmiş görüntülere ait bitişik piksellerin yatay-dikey-çapraz olarak korelasyon katsayıları Çizelge 4.4'te gösterilmektedir. Düz görüntülerin korelasyon katsayıları 1'e yakınken, şifreli görüntülerin korelasyon katsayıları 0'a yakındır. Önerilen şifreleme algoritması bitişik pikselller arasındaki

korelasyonu kaldırmıştır. Böylelikle düz görüntüye ait herhangibir istastiki bilgi şifreli görüntüde bulunmadığını göstermektedir.

Şekil 4.4'te düz ve şifreli Lena görüntüsü için yatay-dikey-çapraz yönde bitişik pikseller için görsel olarak korelasyon katsayıları gösterilmektedir. Düz görüntüde pikseller belli bir bölgede toplanmaktadır. Şifreli görüntüde ise, pikseller tüm bölgeye dağılmış olarak görülmektedir.

Çizelge 4.5 : Düz ve şifreli görüntülerde iki bitişik pikselin korelasyon katsayıları.

Görüntü	Orjinal görüntü			Şifreli görüntü		
	Yatay	Dikey	Çapraz	Yatay	Dikey	Çapraz
Lena	0.9716	0.9847	0.9585	$99x10^{-6}$ $51x10^{-6}$		$54x10^{-6}$
Cameraman	0.9823	0.9899	0.9724	$16x10^{-5}$	$24x10^{-5}$	$73x10^{-6}$
Peppers	0.8575	0.9587	0.8396	$20x10^{-6}$ $10x10^{-6}$		$68x10^{-6}$
Baboon	0.9337	0.9123	0.8671	$42x10^{-6}$ $84x10^{-6}$		$67x10^{-6}$
Barbara	0.9799	0.9799	0.9700	$16x10^{-5}$ $28x10^{-6}$		$33x10^{-6}$
Goldhill	0.9720	0.9696	0.9478	$31x10^{-6}$ $13x10^{-5}$		$56x10^{-6}$
Jetplane	0.9696	0.9726	0.9499	$13x10^{-5}$ $50x10^{-7}$		$96x10^{-6}$
Korsan	0.9600	0.9688	0.9415	$23x10^{-4}$ $79x10^{-5}$		$78x10^{-5}$
Cift	0.9447	0.9524	0.9097	$28x10^{-4}$ $36x10^{-5}$		$24x10^{-4}$
Manzara	0.9761	0.9764	0.9615	$85x10^{-5}$	$10x10^{-4}$	30.10^{-4}



Şekil 4.4: Lena görüntüsü için yatay-dikey-çapraz yönde bitişik piksel korelasyon görsel gösterimi. Üst satır düz görüntü ve alt satır şifreli görüntü.

4.7 Diferansiyel Atak Testi

Diferansiyel atak, düz görüntüde biraz değiştiğinde farklı düz görüntüler ve karşılık gelen şifreli görüntüler arasındaki ilişkiyi analiz ederek algoritmaya anlamaya çalışmaya dayanmaktadır. İyi bir şifreleme algoritmasında, düz görüntüde ufak bir değişiklik olduğunda şifreli görüntüde büyük bir farklılık ortaya çıkmalıdır. Eğer önerilen şifreleme yöntemi düz görüntüdeki herhangi bir değişikliğe karşı yüksek hassasiyete sahipse, farklı saldırılara karşı güvenli bir görüntü şemasıdır.

Bu testi yapmak için düz görüntü ve düz grüntünün 1-bit değiştirilmiş görüntü, şifreleme algoritmasıyla şifrenir ve iki şifreli görüntü elde edilmektedir. İki şifreli görüntü arasındaki farkı ölçmek, şifreleme yönteminin diferansiyel ataklara karşı gücünü gösterecektir. Bunu ölçmek için, piksel değişim oranı (Number of changing pixel rate (NPCR)) ve birleşik ortalama değişken yoğunluk (Unified averaged changed intensity (UACI)) kullanılan iki yöntemdir. NPCR iki şifreli görüntü arasındaki toplam farkı piksel-piksel ölçmektedir. Eğer iki şifreli görüntüdeki pikseller farklı ise 1 atamaktadır. UACI ise, iki şifreli görüntü arasında piksel-piksel yoğunluk farklarının toplamını ölçmektedir.

NPCR ve UACI denklem 4.8 ve 4.10'deki gibi tanımlanırlar:

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \mathrm{W(i,j)}}{\mathrm{MN}} \text{ x } 100 \tag{4.8}$$

$$W(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{4.9}$$

$$\mathrm{UACI} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[\frac{|C_1(i,j) - C_2(i,j)|}{(L-1)} \right] \text{ x } 100 \tag{4.10}$$

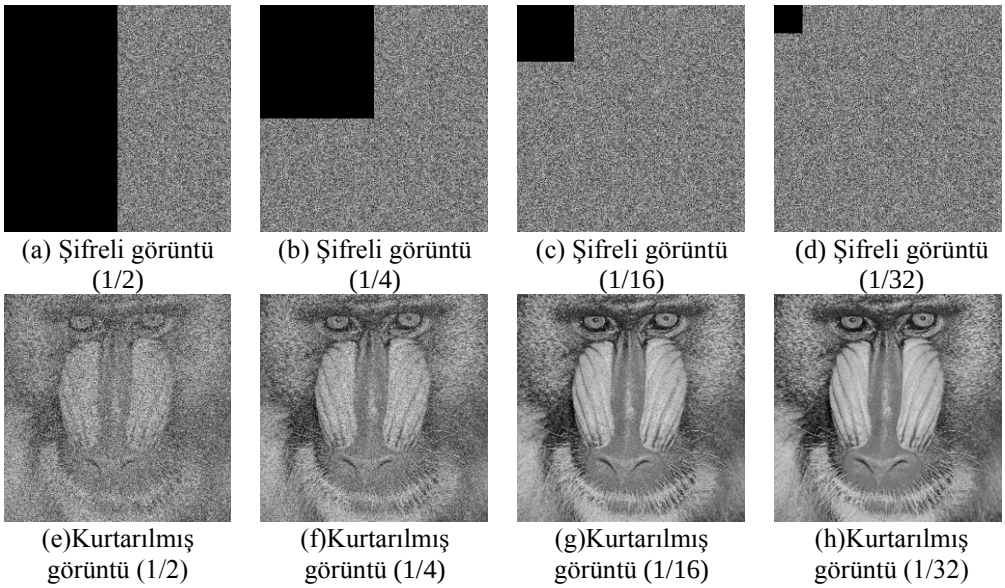
burada C_1 ve C_2, M x N boyutunda iki şifreli görüntüdür. L görüntünün gri tonlamalı seviyesidir ve 8 bitlik gri tonlamalı görüntü için L = 256. 8-bitlik gri tonlamalı bir görüntüde NPCR ve UACI için beklenen değerler %99.6094 ve %33.4635'tir. Çizelge 4.6, farklı şifreleme algoritması ile elde edilen NPCR ve UACI değerlerini gösterilmektedir. Şifreli görüntüdelerdeki NPCR ve UACI değerleri, istenen değerlere çok yakın değerlerdir.

Çizelge 4.6 : NPCR ve UACI değerleri.

Test Görüntüleri	NPCR (%)	UACI (%)
Lena	99.6014	33.4604
Cameraman	99.6128	33.4667
Peppers	99.6210	33.4730
Baboon	99.6150	33.4505
Barbara	99.5929	33.4654
Goldhill	99.5998	33.4775
Jetplane	99.6105	33.4546
Korsan	99.5975	33.4570
Livingroom	99.6082	33.4656
Lake	99.6075	33.4674

4.8 Veri Kaybı Saldırı Analizi

Ağ iletimi sırasında hata oluşabilir, yani şifrelenmiş görüntünün bir kısmı iletim sırasında kaybolabilir. Sistemin sağlamlığı, bilgilerin doğru şekilde geri yüklenip yüklenmediğine göre belirlenir. Bu tezde, şifrelenmiş görüntü, farklı boyutlarda veri kaybı saldırısına maruz bırakılmıştır. Şekil 4.5'da şifreli görüntü sırasıyla $1/2$, $1/4$, $1/16$ ve $1/32$ oranında veri kaybına maruz bırakılmıştır. Karşılık gelen kurtarılmış görüntüler Şekil 4.5'de alt satırda sırasıyla gösterilmektedir. Veri kaybı miktarı arttıkça yeniden yüklenen görüntülerde bulanıklığın arttığı görüldü. Ancak, görüntünün yarısı kaybolsa bile ana hatları hala geri getirilebilmektedir. Bu çalışmada önerilen algoritma, gerçek zamanlı aktarım kanalındaki görüntünün sağlamlığını garanti etmektedir.



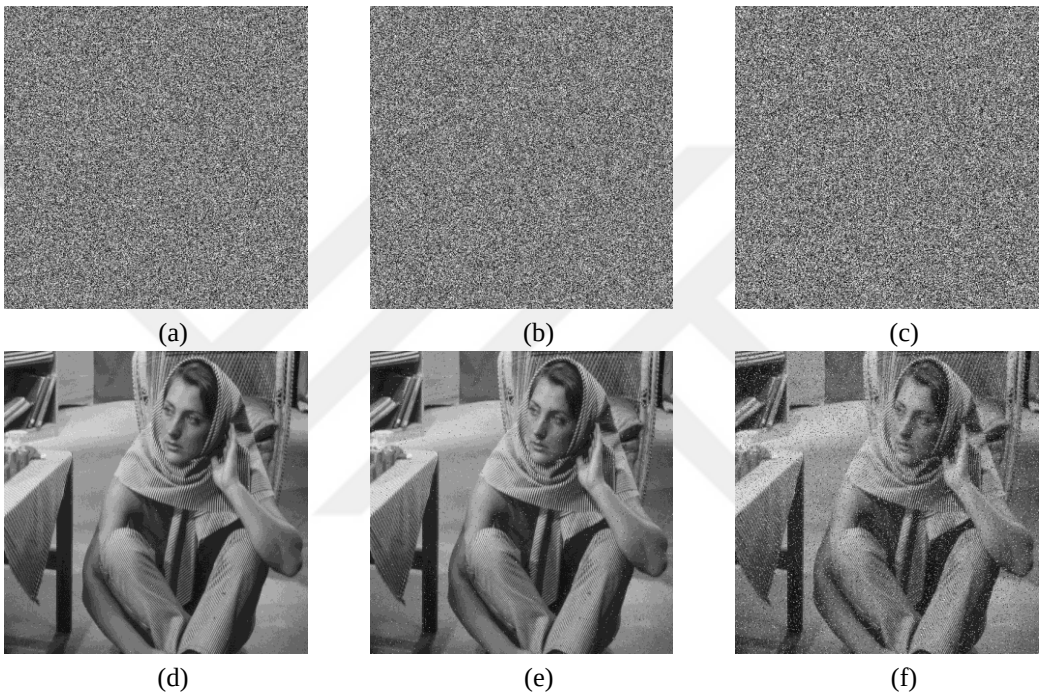
(a) Şifreli görüntü (1/2) (b) Şifreli görüntü (1/4) (c) Şifreli görüntü (1/16) (d) Şifreli görüntü (1/32)

(e)Kurtarılmış görüntü (1/2) (f)Kurtarılmış görüntü (1/4) (g)Kurtarılmış görüntü (1/16) (h)Kurtarılmış görüntü (1/32)

Şekil 4.5: Kırpma saldırısı simülasyon sonuçları.

4.9 Gürültü Analizi

Şifrelenmiş görüntü, aktarımı sırasında çeşitli tehditlere maruz kalır. Şifrelenmiş görüntüye yapılan saldırılar nedeniyle veriler kaybolabilir. Ek olarak, analog-dijital dönüştürme, dijital görüntü bilgilerinde kayıp veya hatalara neden olabilir. Bir görüntü şifreleme algoritması, gürültüden etkilenmiş şifreli görüntülere verilen zararı en aza indirebilmelidir. Şekil 4.6'da 0.001, 0.01 ve 0.1 oranında tuz biber gürültüsü eklenmiş şifreli ve onların şifresi çözülmüş görüntüleri verilmiştir. Önerilen şifreleme yönteminin gürültü etkilerine karşı iyi bir direnc sahip olduğunu gösterir.

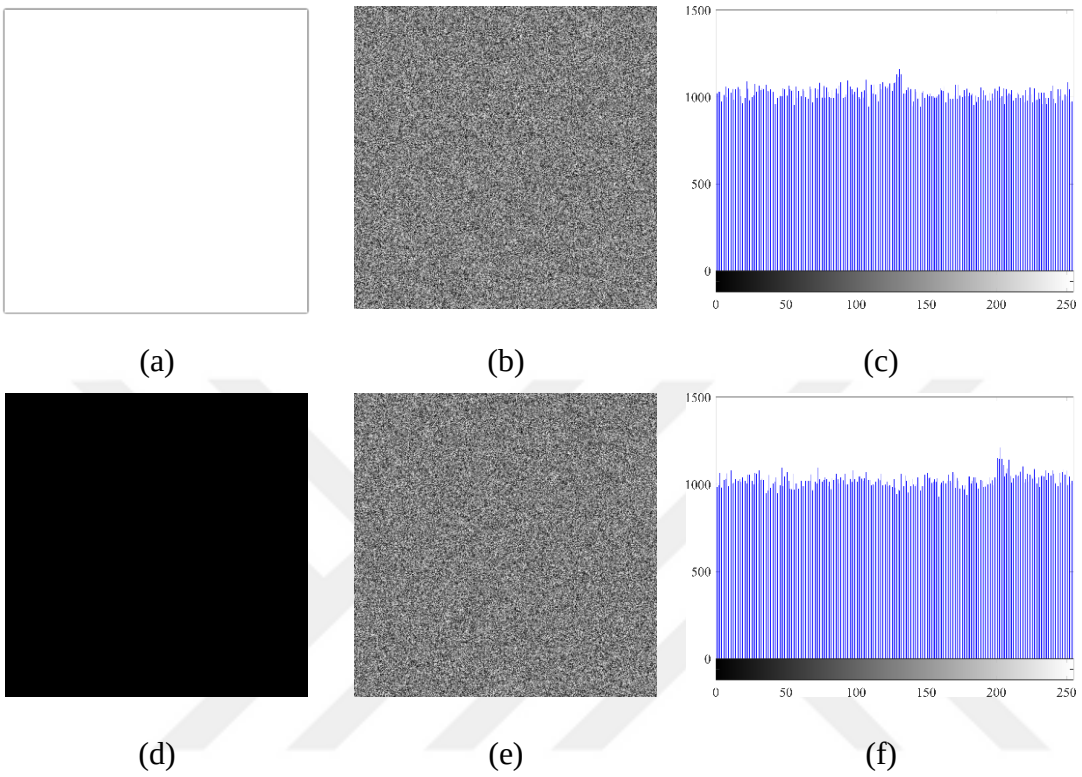


Şekil 4.6: Tuz biber gürültüsü eklenmiş ve geri döndürülmüş görüntüler a) 0.001 gürültü eklenmiş şifreli görüntü b) 0.01 gürültü eklenmiş şifreli görüntü b) 0.1 gürültü eklenmiş şifreli görüntü d) 0.001 gürültü eklenmiş şifreli görüntünün şifresi çözülmüş görüntüsü e) 0.01 gürültü eklenmiş şifreli görüntünün şifresi çözülmüş görüntüsü f) 0.1 gürültü eklenmiş şifreli görüntünün şifresi çözülmüş görüntüsü.

4.10 Seçilen Açık Metin Saldırısına Ve Bilinen Açık Metin Saldırısı Analizi

Görüntü şifreleme algoritmalarında en önemli aşamalarından birisi permutasyon aşamasıdır. Şifreleme yönteminin nasıl çalıştığını anlamak isteyen saldırganlar bu aşamayı devre dışı bırakmak için tamamen siyah veya beyaz görüntüler kullanarak şifreleme algoritmasını anlamaya çalışmaktadır. Kriptanalist seçilen açık metin saldırısında, düz görüntüyü belirleyebilir ve sonra şifreleyebilir. Bunun nedeni, şifreleme algoritmasıyla ilgili özellikleri öğrenmektir. Bilinen açık metin saldırısında kriptanalist, düz görüntüye ve şifreli bir örbeğine sahiptir. Bundaki amaç, gizli

anahtarı elde etmektir. Bu saldırılara karşı, şifreleme yöntemini test etmek için tamamen siyah veya beyaz görüntüler kullanılarak şifreleme algoritmasını anlamaya çalışırlar. Beyaz ve siyah görüntülere ait şifreli görüntülerin, diğer şifrelenen düz görüntülerin özelliklerinden farklı istastiki durumlar göstermemesi gerekmektedir.



Şekil 4.7: Beyaz ve siyah görüntülerin şifreleme sonuçları. a) Tamamen beyaz görüntü. b) Beyaz görüntünün şifreli görüntüsü. c) Şifreli görüntünün histogramı (b). d) Tamamen siyah görüntü. e) Siyah görüntünün şifreli görüntüsü. f) Şifreli görüntünün histogramı (e).

Beyaz ve siyah görüntülere ait şifreli görüntüler ve sayısal değerler Şekil 4.7 ve Çizelge 4.7'de gösterilmiştir. Siyah ve beyaz görüntüye ait şifreli görüntüler, diğer şifreli görüntülerden farksız görünmektedir. Histogram dağılımları tek tiptir, şifrelenmiş görüntülerin korelasyon katsayıları 0'a yakındır. Şifrelenmiş görüntülerin entropi değerleri 8'e yakındır ve tüm bu sonuçlar, önerilen algoritmanın tamamen beyaz ve tamamen siyahı etkili bir şekilde şifreleyebileceği anlamına gelir. Bu sonuçlara bakılarak, önerilen algoritmanın seçilen açık metin saldırısına ve bilinen açık metin saldırısına karşı dirençli olduğu söylenebilir.

Çizelge 4.7 : Beyaz ve siyah görüntüler için, seçilen açık metin saldırısı ve bilinen açık metin saldırısı test sonuçları.

İmages	Korelasyon Katsayısı			Ki kare UACI%	Küresel entropi	Yerel Entropi	NCPR%
	Horizontal	Vertical	Diagonal				
Beyaz	-0.0063	0.0059	0.0194	251.6836 33.4345	7.9993	7.9086	99.5979
Siyah	-0.0177	0.0212	0.0454	251.2695 33.4508	7.9993	7.9116	99.6246

4.11 Hız ve Zaman Karmaşıklığı Analizi

Görüntü şifrelemede en önemli ölçütlerden biriside önerilen şifreleme algoritmasının gerçek zamanlı olrak gerçekleştirilecek bir zamana sahip olmasıdır. Bu tez çalışmasındaönerilen yöntem 2.29 saniye toplam gerçekleşme zamanı ile gerçek zamanlı uygulamalar için uygundur. Bu zamanın içerisinde optimum anahtarı elde etme zamanıda bulunmaktadır. Bu tez çalışması, bu yönü ile diğer optimizasyon kullanan çalışmalardan ayrılmaktadır. Diğer optimizasyon kullanan şifreleme algoritmaları çok uzun çalışma süreleri gerektirdikleri için çoğu zaman gerçek zamanlı uygulamalar için uygun değildir.

4.12 Yapılan Analizlerin Literatürle Karşılaştırılması

Önerilen algoritmanın sonuçlarını karşılaştırmak için gerekli literatür çalışmaları Çizelge 4.8'de verilmiştir. Entropi, NPCR ve UACI ve korelasyon katsayılarının karşılaştırmaları sonuçlarında kullanılan literatürdeki çalışmalar sıra numarası sütünu ile ifade edilmiştir.

Çizelge 4.8 : Karşılaştırma çizelgesi.

Sıra Numarası	**Makale ismi**	Atıf
1	A modified method for image encryption based on chaotic map and genetic algorithm	(Ghazvini ve diğerleri, 2020)
2	An image encryption approach using particle swarm optimization and chaotic map	(Ahmad, Alam, Umayya, Khan ve Ahmad, 2018)
3	Evolutionary-based image encryption using biomolecules operators and non-coupled map lattice	(Abbasi, Mazinani ve Hosseini, 2021)

Lena, Cameraman, Barbara, Baboon ve Peppers görüntüleri için entrop, differential atak ve korelasyon sonuçları sırasıyla Çizelge 4.9, Çizelge 4.10 ve Çizelge 4.11'de verilmiştir.

Çizelge 4.9 : Bilgi entropi değerlerinin literatürle karşılaştırılması.

Görüntüler	Önerilen	1	2	3
Lena	7.9994	7.9720	7.9990	7.9995
Cameraman	7.9993	-	7.9991	7.9994
Barbara	7.9994	7.9852	7.9993	-
Baboon	7.9994	-	7.9986	7.9994
Peppers	7.9993	7.9797	7.9992	7.9994

Çizelge 4.10 : NPCR ve UACI sonuçlarının literatürle karşılaştırılması.

Görüntü	Test	Önerilen	1	2	3
Lena	NPCR	99.6014	99.228	99.5700	99.5998
	UACI	33.4604	30.147	33.3500	33.4715
Cameraman	NPCR	99.6128	-	99.5600	99.6071
	UACI	33.4667	-	33.4000	33.4647
Barbara	NPCR	99.5929	99.253	99.5800	-
	UACI	33.4654	30.972	33.6400	-
Baboon	NPCR	99.6150	-	99.5700	99.6101
	UACI	33.4505	-	33.1700	33.4238
Peppers	NPCR	99.6210	99.1670	99.5500	99.5983
	UACI	33.4730	30.6670	33.3500	33.4823

Çizelge 4.11 : Korelasyon katsayılarının literatürle karşılaştırılması.

Şifreli görüntü	Yön*	Önerilen	1	3
Lena	Y	99×10^{-6}	0.0033	0.0013
	D	54×10^{-6}	-0.0040	-0.0031
	Ç	51×10^{-6}	-0.0002	0.0038
Cameraman	Y	16×10^{-5}	0.0026	0.0177
	D	24×10^{-5}	0.0002	0.0078
	Ç	73×10^{-6}	-0.0015	-0.0115
Barbara	Y	16×10^{-5}	0.0017	-
	D	33×10^{-6}	0.0022	-
	Ç	28×10^{-6}	0.0011	-
Baboon	Y	42×10^{-6}	-0.0023	0.0112
	D	67×10^{-6}	-0.0002	0.0112
	Ç	84×10^{-6}	-0.0008	0.0112
Peppers	Y	20×10^{-6}	0.0068	-0.0168
	D	68×10^{-6}	-0.0022	-0.0182
	Ç	10×10^{-6}	0.0005	0.0041

*Y=yatay, D=Dikey, Ç=Çapraz

5. SONUÇLAR VE ÖNERİLER

Bu çalışmada, yeni bir kaotik harita kullanılarak BOA tabanlı bir görüntü şifreleme yöntemi tasarlanmıştır. İlk olarak, yeni bir boyutlu kaotik harita önerilmiştir. Önerilen haritada, literatürde yer alan lojistik haritaların eksiklikleri giderilmiştir. Yeni önerilen bir boyutlu kaotik harita, başlangıç değerlerinde ve kontrol parametresinin tüm değerlerinde kaotik davranış göstermektedir. Bunu göstermek için çatallama, yörünge, lyapunov üssü, örnek entropi, permütasyon entropi ve 0-1 testleri yapılmıştır. Yeni önerilen kaotik harita tüm testlerde karşılaştırılan diğer haritalardan daha iyi sonuç vermiştir. İkinci olarak; BOA ile optimum anahtar elde edilmiştir. BOA ile bitişik pikseller arası düşük korelasyon sağlayacak ve yüksek entropi değeri üretecek bir anahtar elde edilmiştir. Anahtar elde etmek için görüntünün tamamı üzerinde değil, 80×80'lik bir kesiti üserinde optimizasyon işlemi gerçekleştirilmiştir. Optimum anahtar elde edildikten sonra, bu anahtar ile görüntünün tamamı şifrelenmektedir. Daha sonra, önerilen şifreleme algoritmasının performansını değerlendirmek için 10 adet en bilinen düz görüntü için testler yapılmıştır. Şifreleme performansını ölçmek için anahtar alanı, anahtar duyarlılığı, entropi, histogram, Ki-kare, korelasyon, diferansiyel atak, veri kaybı saldırısı, gürültü ve seçilen ve bilinen açık metin saldırısına karşı analizleri yapılmıştır. Yapılan tüm testlerde, BOA'ya dayanan yeni şifreleme algoritması başarılı sonuçlar göstermiştir. Elde edilen sonuçlar literatürdeki diğer yöntemlerle karşılaştırıldığında, onlardan çoğunlukla daha başarılı olmuştur.

Gelecek çalışmalarda optimizasyon kullanılarak, yeni amaç fonksiyonları ekleyerek algoritmanın performasının artacağı düşünülmektedir. Bu çalışmada bitişik pikseller arasındaki korelasyon katsayısını düşürmek ve entropi değerini olabildiğince artırmak amaçlanmıştır. Gelecek çalışmalarda amaç fonksiyonlarına örnek ve permutasyon entropisi eklenip daha yüksek performanslı bir şifreleme yöntemi geliştirilebilir. Bunun yanında, kaotik harita üzerinde optimizasyon kullanarak yeni bir optimum kaotik harita üretilebilir.

KAYNAKLAR

Abbasi, A. A., Mazinani, M. ve Hosseini, R. (2021). Evolutionary-based image encryption using biomolecules and non-coupled map lattice. *Optics and Laser Technology*, *140*(June 2020), 106974. doi:10.1016/j.optlastec.2021.106974

Afarin, R. ve Mozaffari, S. (2013). Image encryption using genetic algorithm. *Iranian Conference on Machine Vision and Image Processing, MVIP*, *3*(1), 441–445. doi:10.1109/IranianMVIP.2013.6780026

Ahmad, M., Alam, M. Z., Umayya, Z., Khan, S. ve Ahmad, F. (2018). An image encryption approach using particle swarm optimization and chaotic map. *International Journal of Information Technology (Singapore)*, *10*(3), 247–255. doi:10.1007/s41870-018-0099-y

Alvarez, G. ve Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, *16*(8), 2129–2151. doi:10.1142/S0218127406015970

Arora, S. ve Singh, S. (2019). Butterfly optimization algorithm: a novel approach for global optimization. *Soft Computing*, *23*(3), 715–734. doi:10.1007/s00500-018-3102-4

Aslam, Y. ve Santhi, N. (2019). A Comprehensive Survey on Optimization Techniques in Image Processing. *Materials Today: Proceedings*, *24*, 1758–1765. doi:10.1016/j.matpr.2020.03.600

Belazi, A., Abd El-Latif, A. A. ve Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, *128*, 155–170. doi:10.1016/j.sigpro.2016.03.021

Biham, E. ve Shamir, A. (1993). Differential Cryptanalysis of the Data Encryption Standard. *Differential Cryptanalysis of the Data Encryption Standard*, (1993). doi:10.1007/978-1-4613-9314-6

Bu, S. ve Wang, B. H. (2004). Improving the security of chaotic encryption by using a simple modulating method. *Chaos, Solitons and Fractals*, *19*(4), 919–924. doi:10.1016/S0960-0779(03)00260-1

Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I. ve Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos, Solitons and Fractals*, *95*, 92–101. doi:10.1016/j.chaos.2016.12.018

Chai, X., Gan, Z., Yuan, K., Chen, Y. ve Liu, X. (2019). A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Computing and Applications*, *31*(1), 219–237. doi:10.1007/s00521-017-2993-9

Chen, G., Mao, Y. ve Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*, *21*(3), 749–761. doi:10.1016/j.chaos.2003.12.022

Chen, Jia, Xue, D. ve Lai, X. (2008). An analysis of international data encryption algorithm(IDEA) security against differential cryptanalysis. *Wuhan University Journal of Natural Sciences*, *13*(6), 697–701. doi:10.1007/s11859-008-0612-4

Chen, Junxin, Zhu, Z. liang, Zhang, L. bo, Zhang, Y. ve Yang, B. qiang. (2018).

Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. *Signal Processing*, *142*, 340–353. doi:10.1016/j.sigpro.2017.07.034

Deepan, B., Quan, C., Wang, Y. ve Tay, C. J. (2014). Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. *Applied Optics*, *53*(20), 4539. doi:10.1364/ao.53.004539

Enayatifar, R., Abdullah, A. H. ve Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering*, *56*, 83–93. doi:10.1016/j.optlaseng.2013.12.003

Ghazvini, M., Mirzadi, M. ve Parvar, N. (2020). A modified method for image encryption based on chaotic map and genetic algorithm. *Multimedia Tools and Applications*, *79*(37–38), 26927–26950. doi:10.1007/s11042-020-09058-3

Hua, Z., Zhou, Y. ve Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. *Information Sciences*, *480*, 403–419. doi:10.1016/j.ins.2018.12.048

Janeiro, D. (1999). Exists 751 06, 1197–1202.

Li, H., Yu, C. ve Wang, X. (2021). A novel 1D chaotic system for image encryption, authentication and compression in cloud. *Multimedia Tools and Applications*, *80*(6), 8721–8758. doi:10.1007/s11042-020-10117-y

Li, M., Wang, P., Liu, Y. ve Fan, H. (2019). Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map. *IEEE Access*, *7*, 145798–145806. doi:10.1109/ACCESS.2019.2945578

Liu, H., Wang, X. ve Kadir, A. (2014). Chaos-based color image encryption using one-time keys and choquet fuzzy integral. *International Journal of Nonlinear Sciences and Numerical Simulation*, *15*(1), 1–10. doi:10.1515/ijnsns-2011-0001

Lorenz, E. N. (1973). Predictability: Does the Flap of a Butterfly's Wings in Brazil Set off a Tornado in Texas? BT - AAAS Convention of the Global Atmospheric Research Program, *20*(4), 398–399.

Mansouri, A. ve Wang, X. (2020). A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. *Information Sciences*, *520*, 46–62. doi:10.1016/j.ins.2020.02.008

Midoun, M. A., Wang, X. ve Talhaoui, M. Z. (2021). A sensitive dynamic mutual encryption system based on a new 1D chaotic map. *Optics and Lasers in Engineering*, *139*(September 2020), 106485. doi:10.1016/j.optlaseng.2020.106485

Nadhom, M. ve Loskot, P. (2018). Survey of public data sources on the Internet usage and other Internet statistics. *Data in Brief*, *18*, 1914–1929. doi:10.1016/j.dib.2018.04.107

Nazari-Heris, M., Mohammadi-Ivatloo, B. ve Gharehpetian, G. B. (2018). A comprehensive review of heuristic optimization algorithms for optimal combined heat and power dispatch from economic and environmental perspectives. *Renewable and Sustainable Energy Reviews*, *81*(September 2016), 2128–2143. doi:10.1016/j.rser.2017.06.024

Nkandeu, Y. P. K., Mboupda Pone, J. R. ve Tiedeu, A. (2020). *Image Encryption*

Algorithm Based on Synchronized Parallel Diffusion and New Combinations of 1D Discrete Maps. *Sensing and Imaging* (C. 21). Springer US. doi:10.1007/s11220-020-00318-y

Pak, C. ve Huang, L. (2017). A new color image encryption using combination of the 1D chaotic map. *Signal Processing*, *138*, 129–137. doi:10.1016/j.sigpro.2017.03.011

Pareek, N. K., Patidar, V. ve Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, *24*(9), 926–934. doi:10.1016/j.imavis.2006.02.021

Patil, P., Narayankar, P., Narayan, D. G. ve Meena, S. M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*(December 2015), 617–624. doi:10.1016/j.procs.2016.02.108

Peng, J., Zhang, D. ve Liao, X. (2009). A digital image encryption algorithm based on hyper-chaotic cellular neural network. *Fundamenta Informaticae*, *90*(3), 269–282. doi:10.3233/FI-2009-0018

Ravichandran, D., Praveenkumar, P., Balaguru Rayappan, J. B. ve Amirtharajan, R. (2016). Chaos based crossover and mutation for securing DICOM image. *Computers in Biology and Medicine*, *72*, 170–184. doi:10.1016/j.compbiomed.2016.03.020

Sreelaja, N. K. ve Vijayalakshmi Pai, G. A. (2012). Stream cipher for binary image encryption using Ant Colony Optimization based key generation. *Applied Soft Computing Journal*, *12*(9), 2879–2895. doi:10.1016/j.asoc.2012.04.002

Suri, S. ve Vijay, R. (2019). A synchronous intertwining logistic map-DNA approach for color image encryption. *Journal of Ambient Intelligence and Humanized Computing*, *10*(6), 2277–2290. doi:10.1007/s12652-018-0825-0

Wang, P., Zhou, Y., Luo, Q., Han, C., Niu, Y. ve Lei, M. (2020). Complex-valued encoding metaheuristic optimization algorithm: A comprehensive survey. *Neurocomputing*, *407*, 313–342. doi:10.1016/j.neucom.2019.06.112

Wang, X. ve Li, Y. (2021). Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Optics and Lasers in Engineering*, *137*(January 2020). doi:10.1016/j.optlaseng.2020.106393

Wang, X., Li, Y. ve Jin, J. (2020). A new one-dimensional chaotic system with applications in image encryption. *Chaos, Solitons and Fractals*, *139*, 110102. doi:10.1016/j.chaos.2020.110102

Yosefnezhad Irani, B., Ayubi, P., Amani Jabalkandi, F., Yousefi Valandar, M. ve Jafari Barani, M. (2019). Digital image scrambling based on a new one-dimensional coupled Sine map. *Nonlinear Dynamics*, *97*(4), 2693–2721. doi:10.1007/s11071-019-05157-5

Zheng, Y. ve Jin, J. (2015). A novel image encryption scheme based on Hénon map and compound spatiotemporal chaos. *Multimedia Tools and Applications*, *74*(18), 7803–7820. doi:10.1007/s11042-014-2024-0