T.C.
İNÖNÜ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

NESNELERİN İNTERNETİ UYGULAMALARINDA KAOS TEMELLİ GÖRÜNTÜ ŞİFRELEME

DOKTORA TEZİ

Cemile İNCE

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Davut HANBAY

25 Temmuz 2024

T.C
İNÖNÜ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

NESNELERİN İNTERNETİ UYGULAMALARINDA KAOS TEMELLİ GÖRÜNTÜ ŞİFRELEME

DOKTORA TEZİ

Cemile İNCE
(36193619012)

Tez Danışmanı: Prof. Dr. Davut HANBAY

25 Temmuz 2024

İNÖNÜ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

NESNELERİN İNTERNETİ UYGULAMALARINDA KAOS TEMELLİ GÖRÜNTÜ ŞİFRELEME

Tezi Hazırlayan: Cemle İNCE

Doktora Tezi

TEŞEKKÜR VE ÖNSÖZ

Bu tez çalışmasının her aşamasında yardım, öneri, bilgi, tecrübe ve desteklerini esirgemeden beni her konuda destekleyen ve yönlendiren danışman hocam Sayın Prof. Dr. Davut HANBAY'a,

Tüm hayatım boyunca olduğu gibi lisansüstü süresince de bana inanan ve güvenen annem, babam ve kardeşlerime,

Doktora süresince desteğini ve yardımını esirgemeyen canım eşim Kenan İNCE'ye; hayat motivasyon kaynaklarım, minnaklarım Enes'ime ve Emir'ime

teşekkür ederim.

ONUR SÖZÜ

Doktora tezi olarak sunduğum “Nesnelerin İnterneti Uygulamalarında Kaos Temelli Görüntü Şifreleme” başlıklı bu çalışmanın bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın tarafımdan yazıldığına ve yararlandığım bütün kaynakların hem metin içinde hem de kaynakçada yöntemine uygun biçimde gösterilenlerden oluştuğunu belirtir, bunu onurumla doğrularım.

Cemile İNCE

İÇİNDEKİLER

ÇİZELGELER DİZİNİ

ŞEKİLLER DİZİNİ

SEMBOLLER VE KISALTMALAR

PRN **:** Pseudo Random Number (Sözde Rasgele Sayı)

PRNG **:** Pseudo Random Number Generator (Sözde Rasgele Sayı Üreteçleri)

NIST **:** National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)

NPCR **:** Number of Pixel Change Rate (Piksel Değişim Oranı Sayısı)

SHA **:** Secure Hash Algorithm (Güvenli Hash Algoritması)

A **:** Adenin (Adenin)

T **:** Timin (Timin)

G **:** Guanin (Guanin)

C **:** Sitozin (Sitozin)

NSA **:** National Security Agency (Ulusal Güvenlik Ajansı)

GA **:** Genetik Algoritma

RFID **:** Radio Freuency Identifiction (Radyo Frekansı Tanımlama)

IoT **:** Internet of Things (Nesnelerin İnterneti)

QR **:** Quick Response (Hızlı Yanıt)

NFC **:** Near Field Communication (Yakın LAN iletişimi)

DES **:** Data Encryption Standard (Veri Şifreleme Standardı)

AES **:** Advanced Encrypted Standard (Gelişmiş Şifreleme Standardı)

RSA **:** Rivest-Shamir-Adleman

ECC **:** Ecliptic curve encryption (Ekliptik eğri şifrelemesi)

ISO **:** International Standart of Organization

UEC **:** İnternational Electronics Commission

RC4 **:** Rivest Cipher 4

BBD : Binary bit plane decomposition (İkili bit düzlemi ayrıştırması)

GCBD : Gray Code Bitplane Decompisition (Gri kod ikili bit düzlemi ayrıştırması)

TFPBD : Truncated Fibonacci p-code Bitplane Decompisition

RGB : Red Green Blue

ML : Machine Learning

MSE : Mean Square Error (Ortalama Karesel Hata)

MAE : Mean Absolute Error (Ortalama Mutlak Hata)

PSNR : Peak Signal to Noise Ratio (Tepe Sinyal Gürültü Oranı)

NPCR : Number of Pixels Change Rate (Piksel Sayısı Değişim Oranı)

UACI : Unified Average Changing Intensity (Birleşik Ortalama Değişen Yoğunluk)

KGA : Köşe Geçiş Algoritması

DOPÇ : Doğrusal Olmayan Permütasyon Çatısı

NPF : Nonlinear Permutation Framework (Doğrusal Olmayan Permutasyon Çerçevesi)

ÖZET

Doktora Tezi

NESNELERİN İNTERNETİ UYGULAMALARINDA KAOS TEMELLİ GÖRÜNTÜ ŞİFRELEME

Cemile İNCE

İnönü Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

97+XVIII sayfa
2024
Danışman: Prof. Dr. Davut HANBAY

Bilişim sistemlerinin gelişmesi ve Nesnelerin İnterneti (IoT) cihazlarının yaygınlaşmasıyla, veri güvenliği kritik bir önem kazanmıştır. Karmaşık algoritmaların kullanılabildiği standart bilgisayar sistemlerinin aksine, IoT cihazlarının sınırlı donanım kapasiteleri, hafif ve özelleştirilmiş şifreleme çözümlerini zorunlu kılmaktadır. Bu vizyon ile bu çalışmada, IoT ortamları için kaos temelli görüntü şifreleme algoritmaları kategorisinde iki farklı hafif ve verimli görüntü şifreleme yöntemi önerilmiştir. Birinci yöntem, Köşe Geçiş Algoritması (KGA) piksel karıştırma yöntemiyle görütü şifreleme kategorisinde yer almaktadır. Kaos tabanlı yayılma yöntemleriyle entegre olan KGA, kapsamlı bir şifreleme şeması oluşturmakta ve sıkı istatistiksel ve diferansiyel özellikler göstermektedir.

KGA algoritmasında piksel karıştırma algoritmalarıyla yapılan çalışmalar kıyaslanmış ve önerdiğimiz algoritmanın avantajları gözler önüne serilmeye çalışılmıştır. KGA ile benzer üç algoritmanın işlem süreleri karşılaştırılmıştır. Sonuç olarak yapılan tüm testlerde önerilen algoritma alternatiflerine göre daha iyi sonuçlar vermiştir. Ayrıca ilgili çalışmalar arasında

UACI, NPCR, PSNR ve entropi değerleri üzerinden karşılaştırmalar değerlendirilmiştir. Sonuç olarak UACI ve NPCR için en iyi sonuçlar önerilen algoritmadan elde edilmiştir. Diğer değerlendirme ölçütleri olan PSNR ve entropi de kabul edilen aralıktadır.

İkinci yöntem ise çok katmanlı Doğrusal Olmayan Permütasyon Çatısı (DOPÇ) 2B matris dönüşüm temelli bir şifreleme yaklaşımı sunmaktadır. Standart 2B matris haritalama yöntemlerinin aksine, DOPÇ'nin permütasyon matris üzerindeki adım sayısı değişkendir ve algoritmanın gerçekleştirilme aşamalarında 3 farklı 1B kaotik harita (zaslavsky, chebyshev ve lojistik harita) kullanarak şifreleme karmaşıklığı artırılmaktadır. Her iki yöntemin de detaylı performans değerlendirmeleri sunulmuş ve benzer yöntemlerle karşılaştırılmıştır. Test sonuçları, önerilen algoritmaların alternatiflerine kıyasla yüksek şifreleme karmaşıklığına ve düşük işlem zamanında ulaştığını göstermektedir. KGA yöntemi, NPCR ve UACI değerlendirme kriterlerinde 99,6093 ve 33,4648 değerleri ile beklenen değerden çok az sapma göstererek, IoT sistemlerinin sıkı güvenlik gereksinimlerini karşılamaktadır. DOPÇ yöntemi, şifreleme adımlarını görüntüyü tek bir gezintide tamamlayarak yüksek verimlilik sunmaktadır. 14 SIPI veri kümesi görüntüsü üzerinde yapılan testlerde DOPÇ ortalama NPCR 99,6122, UACI 33,4690 ve bilgi entropisi 7,9993 değerleri elde edilmiştir. Her iki yöntemin yüksek anahtar alanı sayesinde kaba kuvvet saldırılarına dayanıklı olduğu gösterilmiştir.

Anahtar Kelimeler: Hafif siklet görüntü şifreleme, Nesnelerin İnterneti, Kaos, Kaotik Haritalar, Köşe Geçiş Algoritması, Çok Katmanlı Doğrusal Olmayan Permütasyon Algoritması, Piksel Karıştırma

ABSTRACT

CHAOS-BASED IMAGE ENCRYPTION IN INTERNET OF THINGS APPLICATIONS

Cemile İNCE

Inonu University
Graduate School of Nature and Applied Sciences
Department of Computer Engineering

97+XVIII page
2024

Supervisor: Prof. Dr. Davut HANBAY

With the development of information systems and the proliferation of Internet of Things (IoT) devices, data security has gained critical importance. Unlike standard computer systems where complex algorithms can be used, the limited hardware capacities of IoT devices necessitate lightweight and customized encryption solutions. With this vision, in this study, two different lightweight and efficient image encryption methods are proposed in the category of chaos-based image encryption algorithms for IoT environments. The first method, Corner Transition Algorithm (CGA), is in the category of image encryption by pixel mixing method. Integrated with chaos-based propagation methods, KGA creates a comprehensive encryption scheme and exhibits stringent statistical and differential properties.

In the KGA algorithm, studies with pixel mixing algorithms were compared and the advantages of our proposed algorithm were tried to be revealed. The processing times of KGA and three similar algorithms were compared. As a result, in all tests performed, the proposed algorithm gave better results than its alternatives. In addition, comparisons between relevant studies were evaluated based on UACI, NPCR, PSNR and entropy values. As a result, the best results for UACI and NPCR were obtained from the proposed algorithm. Other evaluation metrics, PSNR and entropy, are also within the accepted range. The second

method offers a multi-layer Nonlinear Permutation Framework (DOPF) 2D matrix transformation based encryption approach.

Unlike standard 2D matrix mapping methods, the number of steps on the permutation matrix of DOPÇ is variable and the encryption complexity is increased by using 3 different 1D chaotic maps (Zaslavsky, Chebyshev and logistic maps) in the implementation stages of the algorithm. Detailed performance evaluations of both methods are presented and compared with similar methods. Test results show that the proposed algorithms achieve high encryption complexity and low processing time compared to alternatives. The KGA method meets the stringent security requirements of IoT systems, showing little deviation from the expected value with values of 99.6093 and 33.4648 in the NPCR and UACI evaluation criteria. The DOPÇ method offers high efficiency by completing the encryption steps in a single image navigation. In the tests performed on 14 SIPI dataset images, DOPÇ average NPCR values of 99.6122, UACI of 33.4690 and information entropy of 7.9993 were obtained. Both methods have been shown to be resistant to brute force attacks thanks to their high key space.

Keywords: Lightweight image encryption, Internet of Things, Chaotic Maps, Corner Traverse Algorithm, A Multilayer Nonlinear Permutation Framework for Lightweight Image Encryption, Pixel Scrambling

1. GİRİŞ

1.1. Kriptolojinin Tarihçesi

Yazının icadından beri insanlar verinin korunması ve gizliliğinin sağlanması amacıyla birçok yöntem geliştirmiş ve kriptoloji bilim dalının temellerini oluşturmuşlardır. Adını yunanca gizlenmiş manasında kryptos ve yazı manasındaki grafein kelimelerinin birleşiminden alan kriptografi, bir verinin ya da bilginin erişilmesinin istenmediği kişilerce anlamlandırılamayacak seviyede karıştırılması, anlamsız hale getirilmesi olarak tanımlanabilir (Mardon et al., 2021). Bu dönüşüm matematiksel fonksiyon ve denklemlerle sağlanır. Şifrelenmiş veriye yetkili kişilerin erişilebilmesi için, anlamsız haldeki verinin tekrar eski haline dönüştürülebilmesi gerekmektedir. Çünkü kriptografi çift yönlü bir işlemdir. Kriptografik sürecin sonucu olan şifrelenmiş veriden ham veriyi elde etme çalışmasına da kriptanaliz denilmektedir. Bu iki çalışma alanı birlikte kriptoloji bilimini oluşturmaktadır.

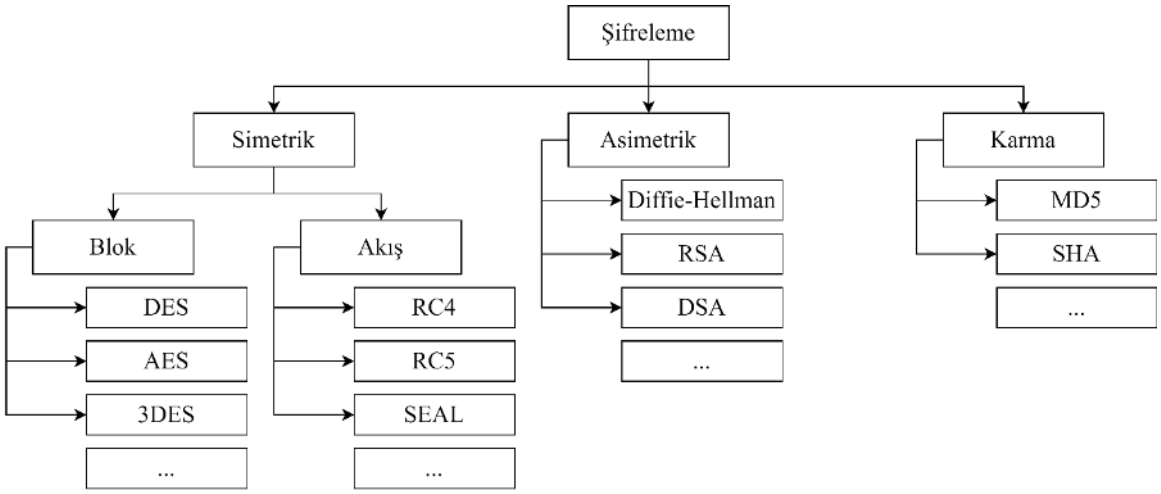
Bilgi gizliliğinin öneminin anlaşılması milattan önceki dönemlere kadar dayandırılmaktadır. MÖ 60-50 yıllarında Roma İmparatoru Julius Cesar devlet haberleşmelerinde Sezar şifreleme yöntemini kullanmıştır. O zaman kullanılan Sezar algoritması veriyi oluşturan her kelimenin harfleri kendinden sonra gelen üç harf sonra ile değiştirilerek şifrelenirdi. Sezar şifreleme harflerin yerlerinin değiştirilmesine dayanan belki de en ilkel şifrelerdendir (Carter & Magoc, 2007).

1586 yılında Blaise de Vigenere, Sezar şifrelemesine benzer ancak ondan farklı olarak anahtar alan kavramıyla birlikte yeni bir şifreleme tekniği geliştirmiştir (Society & Society, 2010). Örneğin anahtar olarak BHFC gibi bir şifre ile metindeki her bir harfin bu anahtara göre öteleneceği bir şifreleme tekniği önermiştir. Buna göre birinci harf 2 adım (B), ikinci harf 8 adım (H), üçüncü harf 6 adım (F), dördüncü harf 3 adım (C) ötelenecek ve beşinci harfe geçildiğinde şifre baştan uygulanacaktır. Kırılmasının imkânsız olduğu düşünülen Vigenere algoritması 1863 yılında kırılmıştır. Daha sonraki yıllarda bütün dünyada daha gelişmiş şifreleme algoritmaları denenmiş, 2. Dünya Savaşı'nda Alman ordularının kendi aralarında iletişiminin gizliliğini sağlayan Enigma cihazı geliştirilmiştir (Rejewski, 1982).

Enigma kullanılarak mors kodlarıyla radyo frekansları üzerinden iletilen veriler uzun süre güvenli bir şekilde kullanılabilmiştir. Enigma kendinden önceki bir dizi şifreleme adımını bir arada toplayan bir cihazdır. İlk aşamada şifreleme sisteminin bilinmesi, ikinci olarak şifrelenmenin nasıl gerçekleştiği ve son olarak da örnek bir mesajın deşifrelemesi aşamalarından oluşmaktadır. Temel olarak yer değiştirme ve farklı sayıdaki ardışık rotorlardan oluşan Enigma, İngiliz matematikçi Alan Turing ve ekibinin geliştirdiği Bombe isimli elektromekanik cihaz kullanılarak şifrelenmiş mesajları kırabilmiş ve ikinci dünya savaşının seyrini değiştiren kriptosistem olarak tarihe geçmiştir (Tang et al.).

1950'lere kadar sadece uluslararası devletlerin güvenliği için kullanılan kriptografik yöntemler, kişisel bilgisayarların icadı ve internetin yaygınlaşmasıyla kapsam değiştirmiştir. Günümüzde hayatımızın her aşamasında kullanmakta olduğumuz internet, yaptığımız her işlemin yetkisiz kişilerin erişimine açık olabileceği ve bu sebeple güvenlik tedbirlerinin zorunlu olduğu bir platform haline gelmiştir. Bilgi güvenliğinin önemini anlayan dünya devletleri, kırılamaz diye önerilen ve kullanılan tüm yöntem ve şifrelemelerin bile bir gün ele geçirilip kırılacağının anlaşılması üzerine yeni ve daha güçlü ifeleme yöntem ve algoritmaların geliştirilmesine önem vermişlerdir (Sethi & Sarangi, 2017).

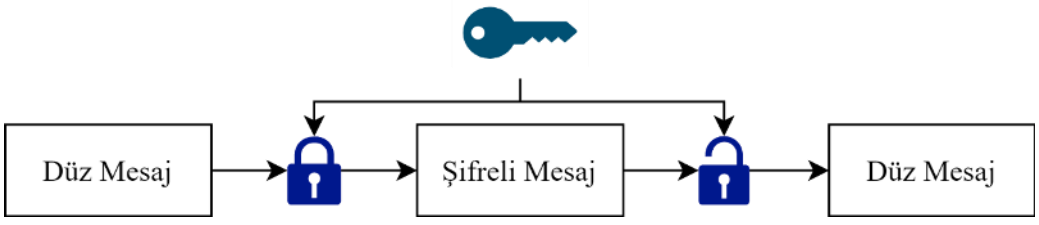
1976 yılına kadar geliştirilmiş olan kriptografik algoritmaların tamamı şifreleme ve şifre çözme adımları için aynı anahtarı kullanmaktaydı, yani simetrikti. Ancak 1976 yılında Whitfield Diffie ve Martin Hellman'ın birlikte geliştirdikleri Diffie-Hellman anahtar değişim algoritması ile birlikte şifreleme ve deşifreleme adımlarında değişik anahtarlar kullanan asimetrik algoritmalar geliştirilmeye başlanmıştır. DES (Data Encryption Standard – Veri Şifreleme Standartı) şifreleme yapısı simetrik şifreleme algoritmalarının standart haline getirilmiş ilk uygulamasıdır (Yingbing & Yongzhen, 2014). Asimetrik şifreleme daha yüksek güvenlik sunmakla birlikte işlem karmaşıklığı simetrik sistemlere göre daha yüksektir. Asimetrik şifreleme yöntemine örnek olarak RSA(Rivest-Shamir-Adleman) verilebilir (Kansal&Mittal, 2014). Şifreleme yöntemlerinin ve yaygın kullanılan algoritmaların genel kategorizasyon şeması Şekil 1.1'de verilmiştir.



Şekil 1.1: Sık kullanılan şifreleme algoritmalarının kategorizasyonu

1.2. Simetrik Şifreleme Yöntemleri

Simetrik şifreleme, gizli anahtarlı şifreleme, A gönderici ve B alıcı arasındaki tek anahtarla hem şifreleme hem deşifrelemenin yapıldığı şifreleme yöntemidir. Bu yöntemde güvenlik tek anahtarın gizliliğine bağlıdır. Simetrik yöntemlerin asimetrik yöntemlere göre en büyük avantajı işlem süresidir. Buna karşılık tek şifrenin güvenliğine dayanır olması, asimetrik şifrelemeye göre dezavantajıdır. DES, AES gibi şifreleme yöntemleri en sık kullanılan simetrik şifreleme algoritmalarındandır (Jamgekar & Joshi, 2013). Simetrik şifreleme yöntemleri blok şifreleme ve akış şifreleme olmak üzere iki alt kategoriye ayrılmaktadır. Blok şifrelemede anahtar boyutu blok boyutuna göre ayarlanırken, akış şifrelemede anahtar boyutu akış uzunluğu kadar değil, tekrar eden kısa bir anahtar şeklinde kullanılır. Simetrik şifreleme çalışma mantığı Şekil 1.2'de verilmiştir.

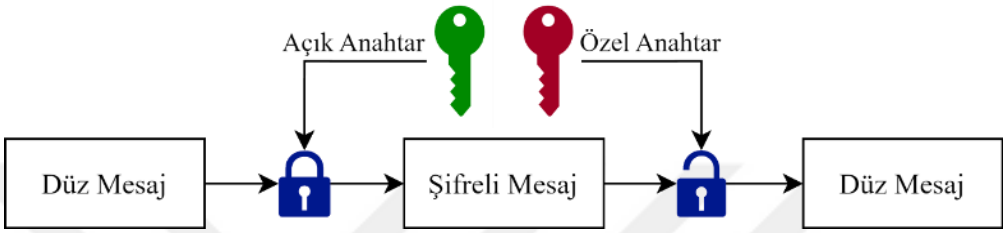


Şekil 1.2: Simetrik şifreleme yöntemi anahtar alan yapısı

1.3. Asimetrik Şifreleme Yöntemleri

Şifreleme ve deşifreleme işlemleri için birbirinden farklı anahtarların kullanıldığı bir şifreleme sistemidir. Açık anahtar ile şifrelenen veri gizli anahtar ile çözülebilmektedir. Bu

sayede asimetrik şifrelemede simetrik şifrelemenin tek anahtar dezavantajı ortadan kaldırılmaktadır. Fakat bu durum işlem süresini arttırmaktadır. Bu yöntemlerin temelinde çarpma gibi işlem yapması kolay ancak geri döndürülmesi zor yaklaşımlar kullanılır. Örneğin iki sayıyı çarpmak kolay iken bir sayısının hangi iki sayının çarpımı olduğunu bulmak zordur. RSA(Rivest-Shamir-Adleman), DSA (Dijital Subtraksiyon Anjiyografi), Diffie Helmann algoritmaları en çok bilinen asimetrik şifreleme algoritmalarıdır (Yassein et al., 2017). Asimetrik şifreleme yöntemlerinin genel çalışma mantığı Şekil 1.3'te sunulmuştur.



Şekil 1.3: Asimetrik şifreleme yöntemi anahtar alan yapısı

1.4. Karma Şifreleme Yöntemleri

Karma (hash) fonksiyonları modern kriptografinin yapı taşlarıdır. Karma işlevi, giriş veri boyutu ne olursa olsun çıkış verisini küçük ve sabit verilere dönüştürmek için kullanılan bir şifreleme algoritmasıdır. Hash algoritmasının veri çıkışına hash değeri veya özet adı verilir. Hash fonksiyonlarının temel işleyişi herhangi bir tetikleyiciye ihtiyaç duymaz ve tek yönlü çalışır. Tek yönlü işlem, girdiyi belirli bir çıktıdan hesaplamanın imkânsız olduğu anlamına gelir. Karma fonksiyonlarının temel kullanım alanları şunlardır:

1. Dijital imzaların oluşturulması ve doğrulanması
2. Sağlama toplamı/Mesaj bütünlüğü kontrolleri
3. MAC aracılığıyla kaynak bütünlüğü hizmetleri
4. Anahtar oluşturma protokolleri ve algoritmalarında alt anahtarların türetilmesi
5. Sahte rastgele sayıların üretilmesi

Simetrik, asimetrik ve karma şifreleme yöntemlerinin karekterisitk özellikleri çizelge 1.1 de verilmiştir.

Çizege 1.1: Simetrik, asimetrik, karma şifreleme yöntemlerinin özellikleri

Özellik	Simetrik	Asimetrik	Karma
Anahtar Sayısı	1	2	0
NIST'in tavsiye ettiği anahtar uzunluğu	128 bit	2048 bit	256 bit
Genel olarak kullanılan anahtar uzunluğu	Kompleks	Basit & Güvenli	Yok
Anahtarla eşleşme hızı etkisi	Hızlı	Nispeten yavaş	Hızlı
Karmaşıklık	Orta	Yüksek	Orta
Örnek Algoritmalar	AES, Blowfish, Serpent, 3DES, RC4	RSA, DSA, ECC, Diffie Hellman	SHA-224, SHA 256, SHA 512, SHA 384

1.5. Görüntü Şifrelemenin Temelleri

Şifrelemenin iki temel amacı bulunmaktadır. Bunlar verileri güvenli şekilde depolamak ve/veya iletmek. Bilişim sistemlerindeki donanımsal gelişmeler paralelinde işlem gücü artmakta, sonuç olarak işlem karmaşıklığı daha yüksek, öngörülemez algoritmalar zorunlu hale gelmektedir. Kriptanaliz yöntem ve algoritmaları geliştikçe verilerin korunması için kriptografik yöntemler yetersiz hale gelebilmektedir (H. Kaur & Kakkar, 2017). Şifrelenecek veriler nümerik, metin, bir boyutlu doğrusal diziler veya daha yüksek boyutlu görüntü ve video verisi olabilirler. Veri türleri arasındaki farklılıklar şifreleme işleminde de farklı yaklaşımları gerektirebilmektedir. Dijital görüntü, piksel koleksiyonundan oluşan bütüncül veri olarak tanımlanabilir (Bukhari et al., 2017). Başka bir deyişle piksel kavramı, görüntü verisinde sayısal verinin elde edilmesini sağlayan en küçük birimdir (Smith, 1995). Bir görüntüdeki anlamlı parçacıklar birçok pikselden oluşmaktadır. Bu durum pikseller arası korelasyonun yüksek olması anlamına gelmektedir. Bu sebeple görüntü verisinin şifrelenmesi standart şifreleme yöntemlerinden farklı yaklaşımlar kullanılarak daha güvenli hale getirilebilir.

Klasik simetrik ve asimetrik şifreleme yöntemleri metin verileri üzerinde çok güçlü şifreleme yöntemleri olarak kabul edilir (Yingbing & Yongzhen, 2014; Simmons, 1979). Ancak bu yöntemler görüntü verilerinin şifrelenmesinde zayıf kalmaktadır. Bunun temel olarak iki sebebi vardır. Öncelikle görüntü verileri metin verilerine göre daha yüksek boyutludur. Bu sebeple görüntü şifreleme işleminde klasik yöntemler (özellikle asimetrik şifreleme) uzun işlem sürelerine sahiptir. İkinci farklılık ise görüntü verilerinde pikseller

arası korelasyon, metinlerdeki harfler arası korelasyona göre çok yüksek olmasıdır. Bu sebeple metin verilerinden farklı olarak korelasyonun bozulabilmesi amacıyla görüntü korelasyon bozucu işlemler gerekmektedir.

Görüntü verilerinin güvenliğinin sağlanması için farklı yöntemler bulunmakla birlikte (F. Cao et al., 2003; Venkatraman et al., 2004; Shini et al., 2012) Nesnelerin İnterneti (IoT-internet of things) gibi düşük donanım seviyesindeki cihazlarda bütün yöntemler uygulanabilir değildir. IoT insan müdahalesi olmadan internet üzerinden veri toplayan ve paylaşan, fiziksel cihazlar, nesneler ve sensörlerden oluşan birbirine bağlı bir ağdır (Atzori et al., 2010). Bu teknoloji, otomasyon verimliliği ve karar alma süreçlerini geliştirme potansiyeli nedeniyle çeşitli endüstrilerde önemli bir ilgi görmüştür. Ancak genel olarak IoT cihazları tek başına yüksek kapasiteli cihazlar değildir. Daha ziyade farklı katmanlarda farklı işlemler gerçekleştiren cihazların belirli bir amaç için bir araya getirilmesiyle anlam kazanırlar (Čolaković & Hadžialić, 2018). IoT sistemlerinin ilk bakışta zayıflık gibi görünen bu özelliği, bu sistemlere esneklik kazandırmaktadır. Bu sayede tıp, çevre, tarım, ulaştırma, sanayi gibi birçok alanda yaygın olarak kullanılmaktadır (Rahmani et al., 2022; Gubbi et al., 2013; Anuradha et al., 2021). Bu yaygınlığı ile beraber IoT cihazlarının düşük bellek boyutu, düşük bant genişliği ve kısa pil ömrü gibi birçok sınırlaması vardır. Bu nedenle DES, AES, RSA, IDEA gibi klasik şifreleme yöntemleri yüksek kaynak tüketimi gerektirdiğinden IoT cihazlarda kullanıma uygun değildir (Callebaut et al., 2021; Samie et al.; 2016; Capra et al., 2019; Bembe et al., 2019; Zeadally et al., 2020). Kısıtlı bir takım uç işlem birimlerinde çalıştırılabilir olsa dahi verimli bir yaklaşım olmayacaktır (Ouedraogo et al., 2021; Benazer et al., 2021; Petrellis et al., 2019). Bu sebeple kısıtlı donanım seviyesine sahip cihazların dijital güvenliği hafif şifreleme algoritmaları sayesinde sağlanmaktadır (Dhanda et al., 2020; Alassaf et al., 2019). Hafif sıklet görüntü şifreleme algoritmaları aynı sebepler ile geliştirilen ancak görüntü verisine odaklanan yöntemlerdir.

Bütün şifreleme algoritmaları veriyi anlamsız hale getirmek için iki temel operatör kullanır: konfüzyon (karıştırma) ve difüzyon (yayma). Ancak bu aşamalar bir sıralama veya hiyerarşi bildirmez. Her iki aşamanın sıralaması veya iç mekanizmaları değişiklik gösterebilmektedir. Görüntü şifreleme algoritmaları da bu iki temel adım ile tanımlanabilmektedir. Piksel kaydırma, kaotik denklemler, permütasyon, matris dönüşümleri ve kuantum teorisine dayalı algoritmalar çoğunlukla piksel karıştırma ve yayma aşamalarında kullanılan yaklaşımlardandır (Abbas, 2016; Jie Wang & Liu, 2022; Y. Cao, 2013; Hariyanto & Rahim, 2013).

Literatürde önerilmiş olan hafif sıklet görüntü şifreleme algoritmaları genel olarak üç ana adımdan oluşur:

1. Piksel karıştırma
2. Piksel Yayma
3. Anahtar XORlama

Bu adımların sıralaması bağımsız veya iç içe kullanılması, adımlarda kullanılan yaklaşımlar ve adımların tekrar sayıları değişmekle birlikte bu üç adım hafif sıklet görüntü şifreleme algoritmalarına anlaşılır bir bakış sunacaktır. Piksel karıştırma adımında sıklıkla kaotik permütasyon (B. Zhang & Liu, 2023) ve deterministik karıştırma algoritmaları (Javadikasgari et al., 2019; Xingyuan Wang & Sun, 2019) kullanılmaktadır. Bu adımın temel amacı piksel konumlarını değiştirerek aralarındaki yüksek korelasyonu kırmaktır. Bu sayede istatistiksel saldırılara karşı dayanıklılık sağlanır. Difüzyon adımında görüntünün piksel değerleri farklı teknikler kullanılarak görüntünün tamamına yayılır ve değiştirilir. Bu şekilde orijinal görüntüdeki tek bir pikseldeki değişiklik tüm şifreleme işlemine yayılır. Üçüncü adımda görüntü piksel değerleri şifreleme anahtarları kullanılarak değiştirilir (Dwivedi & Srivastava, 2023). Kaynak kısıtlı cihazlarda bahsedilen bütün işlem adımları için verimli, hafif siklet algoritmaların tercih edilmesi gerekmektedir. Böylece donanımsal olarak nispeten zayıf olan sistemler, daha güvenli çalışabilir hale gelecektir.

1.6. Tezin İçeriği

İkinci bölümde, tezin kapsadığı alanda yapılmış ilgili çalışmalar verilmiştir. Geçmişten günümüze şifreleme ve görüntü şifreleme algoritmalarından temel olarak bahsedilmiştir. Ayrıca görüntü şifreleme yöntemleri kategorize edilmiş ve açıklanmıştır.

Üçüncü bölümde, nesnelerin interneti kavramı açıklanmış, nesnelerin interneti katma yapısı belirtilmiştir. Ayrıca nesnelerin interneti ortamlarında kullanılan şifreleme algoritmaları açıklanmıştır.

Dördüncü bölümde, görüntü şifreleme temel kavramları verilmiş olup, görüntü şifrelemede kullanılan kaotik haritalar irdelenmiştir. Ayrıca görüntü şifreleme değerlendirme metrikleri de ayrıntılı olarak sunulmuş olup bölüm sonlandırılmıştır.

Beşinci bölümde, köşe geçiş algoritması ile doğrusal olmayan permütasyon çatısı algoritmalar tanıtılmış, bu algoritma ile pikseller üzerinde grçekleştirilen işlemler sıralı olarak anlatılmıştır. Daha sonra elde edilen şifreli görüntülerin metrik değerleri elde

edilmiştir. Daha sonra benzer mevcut çalışmalarla önerilen çalışma metrik değer sonuçları kıyaslanmıştır.

Altıncı bölümde elde edilen metrik değe sonuçları değerlendirilmiş, nesnelerin interneti uygulamalarında çalışma süreleri analiz edilmiştir.

2. İLGİLİ ÇALIŞMALAR

İletişim ağlarının yaşanan gelişmelerle birlikte, veri güvenliğinin sağlanması daha da önem kazanmıştır. Daha önce metin şifrelemede başarılı yöntemler olan RSA, DES, AES, IDEA gibi yöntemler görüntü şifrelemede yetersiz kalmıştır. Hacimli veri kapasitesi gibi bazı temel özelliklerin yalnızca görüntülerde mevcut olması nedeniyle metin şifreleme yöntemlerinden ayrılır (Ott, 2017). Ayrıca metin şifreleme yöntemleri, görüntü verilerinin dağıtılması ve karıştırılması işlemlerinde verimlilik bakımından yetersizdir (Hua et al., 2018). Veri iletiminde büyük boyutları sebebi ile iletilen veri içerisinde dijital görüntüler büyük bir orana sahiptir (Baeza et al., 2009). Bundan dolayı dijital görüntülerin iletiminde birçok farklı şifreleme yaklaşımının geliştirlmesi ve kullanılması zorunlu bir ihtiyaç haline gelmiştir.

Kaotik şifreleme yaklaşımlarından (Ur et al., 2020)'de Rehman ve arkadaşları, lojistik kaotik harita, burger haritası ve dinamik ikame kutularına dayalı yeni bir yaklaşım önermiştir. Önerilen yöntemin gri görüntülerin güvenli olmayan iletişim kanallarında iletilmesi için yüksek güvenlik sağladığı bildirilmiştir. Benzer çalışmalarda Lorenz, Skew, Tent, Line ve Henon haritaları kullanılarak, karıştırma adımı geliştirilmiş şifreleme algoritmaları mevcuttur (Ahmad, 2015; G. Zhou et al., 2015; Umar et al., 2024), Gao ve ark. Gao et al., 2006) çalışmalarında, tek boyutlu kaotik şifrelemenin küçük boyutlu anahtar alan ihtiva etmesi gerekçesiyle yeterince güvenli olmadığını belirtmişler ve güç fonksiyonu kullanan NCA (Nonlinear Chaos Algorithm) algoritmasını önermişlerdir. Renkli görüntüler işlenirken gri bileşenlere dönüştürülerek işlem yapmanın daha fazla artıklık ve düşük verimlilikle sonuçlandığını bildiren (H. Zhang et al., 2024) çalışmasında, renkli görüntülerin RGB bileşenleri arasındaki doğal bağlantıyı tamamen dikkate alan, fraktal ve kaos teorisini kullanan yeni bir renkli görüntü şifreleme algoritması (CIEA) sunulmuştur. 2D sinüs-kosinüs-lojistik eşleşme (2D-SCLC) hiper kaotik haritasının yeni bir modelinin önerildiği (Q. Chen & Lv, 2024) çalışmada, önerilen yöntemin güvenli sonuçlar elde ettiği, güvenlik testi araçlarını kullanarak NPCR ve UACI değerlerinin %99,61 ve %33,44'e ulaştığını ve ideal değere yakın olduğu bildirilmiştir. Sistemin benzer çalışmalara göre daha iyi dinamik özelliklere sahip olduğu, uygulanan NIST(National Institute of Standards and Technology) testleri sonucunda PRN (Pseudo Random Number)'lerin yüksek rasgelelik gösterdiği verilen sonuçlar arasındadır.

Kaotik sistemlere ve DNA kodlamasına dayalı başka bir görüntü şifreleme çalışmasında (H. Zhang & Hu, 2024), kaotik sistemlerin basit kontrol parametrelerine sahip

olduğu kaotik yaklaşımların kolayca tahmin edilebilir olduğunu bildirmektedir. Bu sorunu gidermek amacıyla, uygulama verimliliğini ve güvenliğini tamamen dikkate alan yeni bir eşzamanlı karışıklık-difüzyon görüntü şifreleme algoritması (SCD-IEA) sunulmuştur. Bu yötemde öncelikle bileşik-bağlantılı kaotik sistem (CCCS) kullanılmıştır. Bunu takiben, basit lojistik ve sinüs haritalamalarına dayanan, DNA kodlaması ve CCCS kullanılarak yeni bir görüntü şifreleme yöntemi önerilmiştir. Ancak DNA hesaplama karmaşıklığı dezavantajı da çalışmada belirtilmiştir. Frekans alanı tabanlı dijital görüntü şifreleme çalışmalarından (H. Wen et al., 2024)'de, ilk olarak, dijital görüntüyü uzamsal alandan frekans alanına haritalamak için düz metin görüntüsü tamsayı Dalgacık Dönüşümü (IWT-Integer Wavelet Transform) tarafından farklı frekans alt bantlarına ayrıştırılmıştır. İkinci olarak, düz metin karma değeri dinamik anahtar olarak seçilmiş ve her bir modülün şifrelenmesi için sırasıyla kullanılan dinamik kaotik sözde rastgele diziler oluşturulmuştur. Bit permütasyonlu üç boyutlu S-kutusu difüzyonu şifrelemek için tasarlanmıştır. Sonuç olarak frekans alanı görüntü şifrelemesinin, dijital fotoğrafların mahremiyetini korumak için tercih edilen yüksek güvenlikli bir teknik olduğu bildirilen çalışmada, pratik uygulamalar için tercih edilebilir bir çözüm olduğu sonuçlarla gösterilmiştir. Görüntü şifrelemenin güvenliğini daha da artırmak için, düz görüntüyü hem frekans alanında hem de uzay alanında aynı anda şifrelemek için ayrık Fourier dönüşümü ve Joseph geçişine dayalı yeni bir kaos tabanlı görüntü şifreleme algoritması (IEA) önerilen (M. Wang et al., 2024) çalışmasında, uygun kaotik diziyi oluşturmak için lojistik harita kullanılmış ve görüntüyü farklı başlangıç konumlarında ve değişken adım boyutlarında karıştırmak için geliştirilmiş Joseph geçişi uygulanmıştır. Önerilen IEA ile ilgili temel bulgu, ayrık Fourier dönüşümü ve Joseph geçişi kombinasyonunun, yaygın saldırı türlerine direnme performansının ölçülmesiyle doğrulanan görüntü bilgilerinin güvenliğini arttırdığı bildirilmiştir.

Ayrıştırma, renk uzayı füzyonu, dalga boyu çoğullamasını kullanan çoklu tek kanallı şifreleme öneren (Abuturab, 2024) çalışmasında, potansiyel saldırıları önlemek için iki ayrı şifre çözme anahtarının hibrit bir optoelektronik sistem kullanılarak uygulanabilir olduğu söylenmiştir. Sayısal simülasyon sonuçları ile önerilen yöntemin etkinliği gösterilmiştir.

Güvenlik için anahtar alanı oluşturmada SHA-512 karma fonksiyonunu kullanan (N. Zhou et al., 2024) çalışmasında, ayrık dalgacık dönüşümü ile sıkıştırılan görüntü, kesirli parçalara sahip pikseller üzerinde bit düzeyinde karıştırma ve yayma işlemi yaptığı bildirilmektedir. Ayrıca şifreli görüntünün rassallığını arttırmak ve içeriği gizlemek için üç

tur karıştırma ve dağıtma işlemi yapıldığı, sonuçların istatistiki ve diferansiyel analizleri başarılı bir şekilde geçtiği bildirilmiştir.

DNA seviyesinde permütasyon ve difüzyona dayandırılan çalışmada (Fan et al., 2023), dört boyutlu hiperkaotik sistem, SHA-512 karma algoritmasıyla birleştirilmiştir. Karma fonksiyonu ile üretilen başlangıç değerleri tek boyutlu diziler ve üç boyutlu küpler üzerinde yürütülen sekiz bazlı DNA düzeyinde permütasyon ve difüzyonu birleştirir. Uygulama sonuçları önerilen yaklaşımın birçok saldırı türüne karşı dayanımını göstermektedir.

Literatürde son yıllarda gerçekleştirilen çalışmalar incelendiğinde görüntü şifreleme için kullanılan yöntem ve algoritmaların çok çeşitli olduğu görülebilir. Bu yöntem ve algoritmalar iç içe geçmiş şekilde birbirleriyle kullanıldığı gibi tek başına kullanılarak da görüntü şifreleme işlemi yapılabilmektedir. Görüntü şifreleme teknikleri 10 farklı yaklaşım altında kategorize edilebilir. Bunlar:

1. Kaos temelli görüntü şifreleme
2. Permutasyon temelli görüntü şifreleme
3. Optiksel görüntü şifreleme
4. DNA temelli görüntü şifreleme
5. Frekans alanı tabanlı görüntü şifeleme
6. Karma temelli görüntü şifreleme
7. Evrimsel yöntemler kullanarak görüntü şifreleme
8. Bit düzlemi ayrıştırma kullanarak görüntü şifreleme
9. Çoklu görüntü şifreleme
10. Piksel karıştırma (scambling transform) kullanarak görüntü şifreleme

2.1. Kaos Temelli Görüntü Şifreleme

Kaotik sistemler, ergodiklik, aperiyodiklik, başlangıç koşullarına ve kontrol parametrelerine karşı yüksek hassasiyet ve yüksek sözde rastgelelik dahil olmak üzere çok sayıda mükemmel içsel özellikten yararlanır (Y. Li et al., 2017). Bu nedenle araştırmacılar kaotik sistemleri temel alan görüntü şifreleme algoritmaları da dahil birçok yaklaşım önermişlerdir. Bazı algoritmaların permütasyon işlemi yalnızca piksel konumunu değiştirir; ancak kaotik bir sistemin ürettiği kaotik dizi, düz metinden ve yayılma sürecinden bağımsızdır. Bu nedenle şifreli metin, seçilmiş düz metin ve seçilmiş şifreli metin saldırılarıyla kolayca çözülebilir. Yayılma işlemi, şifreli görüntünün histogramının oldukça tekdüze olduğu ve düz görüntünün histogramından önemli ölçüde farklı olduğu istatistiksel

ve diferansiyel saldırılara karşı direnci büyük ölçüde arttırmaktadır. İyi bir yayılma süreci için düz görüntüyle güçlü bir şekilde ilişkili olan bir anahtar akışı kullanılmalıdır. Farklı düz görüntüleri şifrelerken, şifreleme algoritmasından bağımsız farklı kaotik diziler elde edilebilir (Y. Li et al., 2017). Difüzyon aşamasında öncelikle kaotik sistemler kullanılarak anahtar akışı elde edilir. Daha sonra görüntü matrisi şifrelenir.

2.2. Permütasyon Temelli Görüntü Şifreleme

Permütasyon işlemi temel olarak veri parçalarının yer değiştirilmesi prensibine dayanmaktadır. Söz konusu görüntü verisi olduğunda piksel değerlerini değiştirmeden konumlarının değiştirilmesi şeklinde uygulanır. Fakat her adımda olduğu gibi permütasyon işleminde de kombine yaklaşımlar sergilenmektedir. Anahtar alana göre parçalara ayrılıp şifreleme algoritmasına göre piksel yerlerinin değiştirilmesi prensibine göre çalışır. Permütasyon temelli görüntü şifreleme yöntemi permütasyonun uygulanma şekline göre üç alt başlıkta incelenebilir. Bunlar;

1. Bit Seviyesi Permutasyonu
2. Piksel Seviyesi Permutasyonu
3. Blok Seviyesi Permutasyonu

2.3. Optiksel Görüntü Şifreleme

Optik şifreleme teknikleri, 2 boyutlu görüntü verilerinin yüksek hızda paralel işlenmesine, bilgilerin birçok farklı boyutta, yani birden fazla serbestlik derecesinde gizlenmesine olanak sağlayan bir yöntemdir (H. Hwang, 2012). Çift Rastgele Faz Kodlama (DRPE) olarak adlandırılan önemli bir optik şifreleme şeması, görüntünün hem giriş (uzay) hem de Fourier (uzaysal frekans) alanlarındaki rastgele faz difüzörleri (maskeler) ile çarpılmasını içerir (H. E. Hwang, 2012).

2.4. DNA Temelli Görüntü Şifreleme

Deoksiribonükleik asit, canlı organizmaların gelişimi ve işleyişi için bir depo, kalıtım ve genetik programın gerçekleşmesini sağlayan bir makro moleküldür. DNA molekülü, bir dizi nükleotidden oluşan genetik kod şeklinde biyolojik bilgi içeren bir yapıdır. Kimyasal açıdan bakıldığında DNA, tekrarlayan blok-nükleotitlerden oluşan uzun bir moleküldür (Maver, 2011), Her nükleotid azotlu bazlardan, şekerden (deoksiriboz) ve bir fosfat

grubundan oluşmaktadır. DNA'da dört tip baz (adenin (A), guanin (G), timin (T) ve sitozin (C)) vardır. Tamamlayıcılık ilkesine göre, zincirlerden birinin nitrojen bazları diğer zincirin nitrojen bazlarına hidrojen bağlarıyla bağlanır: adenin (A) yalnızca timine (T) ve guanin (G) yalnızca sitozine (C) bağlanır. Örneğin, bir polinükleotid zincirindeki sekans A-C-A-T-T-C-G-T ise, diğer zincirdeki nükleotidler T-G-T-A-A-G-C-A sekansı ile sıralanacaktır. DNA zincirinde 4 farklı sembol (A, C, G, T) bulunduğundan bunları dörtlü sayı sistemiyle (0, 1, 2, 3) değiştirebiliriz. İkili sistemde olduğu gibi 0 ve 1 hesaplamaları birbirini tamamlar, dolayısıyla dörtlü sistemde ikili tümleyen vardır. Burada 0 ile 3 ve 1 ile 2 birbirine tamamlayıcıdır. Adenin (A), timin (T) ve guanin (G) ile sitozin (C) birbirini karşılıklı olarak tamamladığından, bu durumda Watson-Crick modeline (DeMaria, 2003) göre DNA sembollerinin sekiz olası kodlaması vardır. Bu varyantlara aynı zamanda DNA sembollerinin kodlanması ve kodunun çözülmesine ilişkin kurallar da denir. Kural olarak, pratikte dördüncül sistemin sembolleri yerine ikili sistemin sembolleri kullanılır. DNA kodlanması ve kod çözümlemesi sayısallaştırması Çizelge 2.1'de sunulmuştur.

Çizelge 2.1: DNA kodlaması için kural tablosu

{0,1,2,3}	A	T	C	G
Kural 1	0	3	2	1
Kural 2	0	3	1	2
Kural 3	3	0	2	1
Kural 4	3	0	1	2
Kural 5	2	1	0	3
Kural 6	2	1	3	0
Kural 7	1	2	0	3
Kural 8	1	2	3	0

Çizelge 2.2: DNA kodlaması için ikili kodda kural tablosu

{00,01,10,11}	A	T	C	G
Kural 1	00	11	10	01
Kural 2	00	11	01	10
Kural 3	11	00	10	01
Kural 4	11	00	01	10
Kural 5	10	01	00	11
Kural 6	10	01	11	00
Kural 7	01	10	00	11
Kural 8	01	10	11	00

Görüntü şifrelemenin farklı adımlarında temel olarak DNA kodlama kullanılarak gerçekleştirilmiş görüntü şifreleme çalışmaları mevcuttur (Junxin Chen et al., 2020; Dua et al., 2020; Chai, Chen, et al., 2017; Akhavan et al., 2017; Y. Zhang, 2018). Çalışmalar DNA temelli görüntü şifreleme çalışmaları olsa da diğer görüntü şifreleme teknikleriyle birlikte kullanılması açısından ortaktır.

2.5. Frekans Alanı Tabanlı Görüntü Şifreleme

Filigranlama teknikleri uzaysal alan ve frekans alan açısından iki türe ayrılmıştır (X. Li et al., 2016). Filigran eklemek için görüntüdeki piksellerin değiştirilmesini dikkate alan en eski tekniklerdir. Spektrum ve en az anlamlı bit yaygın olarak kullanılan yaklaşımlardır. Ancak mekansal alan teknikleri bütün saldırı türlerine karşı dayanıklı değildir. Öte yandan, ayrık dalgacık dönüşümü (DWT) (Gangadhar et al., 2018; X. Wu et al., 2016) Ridgelet dönüşümü (H. Liu & Nan, 2013), ayrık kosinüs dönüşümü (DCT) (Z. Liu et al., 2011), ayrık Hadamard dönüşümü (DHT), (Tsui et al., 2008) ve ayrık Fourier dönüşümü (DFT) (Solachidis & Pitas, 2001) kullanılarak orijinal görüntüyü dönüştürerek filigranı eklemek için frekans alanı teknikleri kullanılır.

2.6. Karma Temelli Görüntü Şifreleme

Karma fonksiyonu temelde matematiksel yollarla sabit uzunlukta bilgi üretme işlemidir. Bu işlemi yaparken giriş verisinin uzunluğu ne olursa olsun çıkış verisinin uzunluğu karma fonksiyonuna göre sabittir. Karma fonksiyonu, geri dönüşü olmayan tek yönlü bir fonksiyondur. Yani çıkış bilgisinden giriş verisi elde edilemez. Karma fonksiyonları, verilerin bilgisayar üzerindeki bir temsilidir ve güvenli şekilde saklanmasını sağlar. Bu sayede verideki manipülasyonu belirlemede kullanılır. Veriler bir kez sindirildikten sonra, doğru karma algoritması ve karma anahtarı olmadan değiştirilemez. Bu fonksiyon; kimlik doğrulama, dijital imza, dosya şifreleme gibi birçok farklı şekilde kullanılabilir (Sani et al., 2024; Kumari et al., 2024; Madushanka et al., 2024). SHA-1'in güvenirliliğini kaybetmesi yani farklı verilere aynı karma sonucunu ürettiği tespit edilmesinin sonucunda NSA tarafından geliştirilen SHA-2, 2001 yılında NIST tarafından standartlaştırılmıştır. SHA-2, aslında farklı uzunluklardan oluşan bir karma algoritması ailesidir. SHA-224, SHA-256, SHA-384 ve SHA-512 gibi çeşitleri bulunur. En sık kullanılan türü SHA-256 algoritmasıdır. SHA algoritmalarının kıyaslama tablosu aşağıdaki çizelge 2.3'da verilmiştir. Karma algoritmaları görüntü şifreleme işlemlerinde yaygın kullanılan yöntemlerdendir (Q. Y. Zhang et al., 2024; G. Liu et al., 2024; Yang et al., 2024).

Çizelge 2.3: Güvenli Hash Algoritmalarının uzunluk kıyaslamaları (Ince, 2023)

Algoritmalar	SHA-1	SHA-256	SHA-512
Mesaj Boyutu	2^{256}	2^{256}	2^{512}
Blok Boyutu	512	512	1024
Kelime Boyutu	32	32	64
Mesaj Özeti Boyutu	160	256	512
Güvenlik	80	128	256

2.7. Evrimsel Temelli Görüntü Şifreleme

Genetik algoritmalar (GA) evrimsel yöntemlerin temelidir ve ilk olarak John Holland tarafından önerilmiştir (Yadav & Prajapati, 2012). GA, iteratif çalışan ve rassal arama yapan bir algoritmadır. Çaprazlama, mutasyon, seçim gibi biyolojik süreçlerden esinlenerek geliştirilen GA, doğada güçlü olan bireyin hayatta kaldığı, zayıfların elendiği dogması üzerine kurulu bir algoritmadır (Holland J. H., 1975). GA'larda nüfus içindeki her bireyin amaç fonksiyonu değeri hesaplanır. GA'nın amacı en iyi amaç fonksiyon değerine sahip bireyleri bulabilmektir. Çaprazlama ve mutasyon işlemleriyle en iyi bireyleri bulmak için genlerin yerleri değiştirilerek işlem yapılır. GA'lar paralel çalışmaya uygun algoritmalardır. Böylece aynı anda birçok yerde arama yapılarak işlem hızı arttırılabilir. Evrimsel algoritma tabanlı yöntemler, adından da anlaşılacağı gibi yinelemeli bir yapıya sahiptir ve bu özel özellik, algoritmanın her yinelemede sonuçlarını iyileştirmesine yardımcı olur. Optimizasyon algoritmaları da yinelemelerin optimum sonucunu bulmaya yönelik çalıştığından bu algoritmalar da evrimsel yöntemlere örnektir (Kocak et al., 2024), (Jingya Wang et al., 2022). Bu yöntem diğer birçok yöntemle; karma algoritmaları, DNA kodlama, optimizasyon algoritmaları, karıştırma algoritmaları gibi birçok yöntemle birlikte kullanılarak görüntü şifreleme yöntemlerinde kullanılmıştır (M. Kaur et al., 2022; Bhowmik & Acharyya, 2023; Mali et al., 2015; Noshadian et al., 2018).

2.8. Bit Düzlemi Ayrıştırması Kullanarak Görüntü Şifreleme

İkili bit düzlemi ayrıştırması (Binary bitplane decomposition- BBD), gri bit düzlemi ayrıştırması (Gray Code Bitplane decomposition-GCBD) ve kesik fibonacci p-kodu bit düzlemi ayrıştırması (truncated Fibonacci p-code bitplane decomposition-TFPBD) olmak

üzere üç ana bit düzlemi ayrıştırması yöntemi vardır. BBD ve GCBD iki geleneksel ayrıştırma yöntemidir (Y. Zhou et al., 2014).

2.8.1. İkili bit düzlemi ayrıştırması

Negatif olmayan bir ondalık sayı N, aşağıdaki denkleme dayalı olarak ikili bir $\{b_{n-1}, \dots b_1, b_0\}$ edilir:

$$N = \sum_0^{n-1} b_i \, 2^i = b_0 \, 2^0 + b_1 \, 2^1 + \cdots + b_{n-1} \, 2^{n-1} \tag{2.1}$$

Piksel değerleri 0 ile 255 arasındaki ondalık sayılardan oluşur. Dolayısıyla her piksel 8 bitlik ikili dizilerle temsil edilir. İkili düzlemde bit ayrıştırması ile gri tonlamalı bir görüntüyü, 8 bit düzlemine ayrıştırmadır. Yani i. Bit düzlemi, gri tonlamalı görüntü içindeki her pikselin ikili temsilinin tüm i'inci bitlerinden oluşur. Bu bit düzlemleri arasında, daha yüksek bit düzlemleri orijinal görüntünün daha önemli görsel bilgilerini içerirken, daha düşük bit düzlemleri daha fazla ayrıntı gösterir.

2.8.2. Gri kod bit düzlemi ayrıştırması

Gri kod, birbirini takip eden iki kodun yalnızca bir bit konumunu değiştirdiği ikili yansımalı Gray kodu olarak bilinir.

$$g_i = \begin{cases} b_i \, , i = n-1 \\ b_i \oplus b_{i+1} \, , 0 \le i \le n-2 \end{cases} \tag{2.2}$$

Burada $\{b_{n-1}, .. b_1, b_0\}$ ve $g \, \{g_{n-1}, \dots . g_1, g_0\}$, N'in temsili ikili gray kodudur.

2.8.3. Kesilmiş fibonacci p-kodu bit düzlemlerinin ayrıştırılması

İkili gösterim kavramından hareketle, negatif olmayan bir ondalık sayı N, kesik Fibonacci p kodu $(t_{n-1}, \dots . t_2, t_1, t_0)$ kullanılarak temsil edilebilir.

$$N = \sum_{i=0}^{n-1} t_i \, T_p(i) = t_0 T_p(0) + \, t_1 T_p(1) + \cdots \dots \dots \dots \, t_{n-1} T_p(n-1) \tag{2.3}$$

Buradaki t_i ağırlık katsayısıdır ve $t_i \in [0,1]$ 'dir. Kesik fibonacci p-kodu dizisi;

$$T_p(i) = \begin{cases} 0 \, , & i < 0 \\ 1, & i = 0 \\ F_p(i+p), & i > 0 \end{cases} \tag{2.4}$$

Burada i indeks numarası, p mesafe parametresi ve $F_p(i+p)$ şu şekilde tanımlanan p-fibonacci dizisidir.

$$F_p(i) = \begin{cases} 0\,, & i < 0 \\ 1, & i = 0 \\ F_p(i-1) + F_p(i-p-1)\,, & i > 0 \end{cases} \quad (2.5)$$

2.9. Çoklu Görüntü Şifreleme

Bu algoritmalar, renkli görüntüleri şifrelemek için üç grup gri görüntüye (renkli görüntü, her bileşenin gri bir görüntü olarak kabul edildiği R, G ve B kanallarına ayrıştırılır) ihtiyaç duyar (Shao et al., 2014). Bu, renk bileşenleri arasındaki ilişkilerin kullanılmamasına ve üç kat daha büyük yineleme döngülerine ve faz fonksiyonlarına yol açar. Bu yaklaşımın bazı dezavantajları şunlardır:

Hesaplama Karmaşıklığı: Üç kat daha fazla yineleme döngüsü ve faz fonksiyonu kullanımı, algoritmanın daha karmaşık ve hesaplama açısından daha yoğun olmasına neden olur.

Veri Depolama: Üç gri görüntüye ihtiyaç duyulması, veri depolama gereksinimlerini üç kat artırır.

Renk Bilgisi Kaybı: Renk bileşenleri arasındaki ilişkiler kullanılmadığından, şifreleme işlemi sırasında renk bilgisi kaybolabilir. İnternetteki aşırı görüntü iletim yükünü azaltmak için son yıllarda çift (çoklu) görüntü şifreleme büyük ilgi görmüştür. Bu yöntem, tek bir görüntü yerine birden fazla görüntüyü kullanarak gizli bilgiyi gizleme ve korumayı amaçlar (Sui et al., 2015). Bu yaklaşımın tercih edilmesine sebep olan avantajları da bulunmaktadır. Bu avantajlar kısaca:

Daha Yüksek Güvenlik: Birden fazla görüntü kullanmak, brute force saldırılarına karşı daha yüksek direnç sağlar.

Daha Az Veri İletimi: Tek bir görüntü yerine birden fazla görüntü kullanmak, veri iletim yükünü azaltabilir.

Daha İyi Görüntü Kalitesi: Renk bileşenleri arasındaki ilişkiler kullanılarak, şifreleme işlemi sırasında görüntü kalitesi korunabilir (Jialun Chen et al., 2015).

2.10. Piksel Karıştırma Yöntemleri Kullanılarak Görüntü Şifreleme

Piksel karıştırma, görüntünün piksellerini rastgele veya belirli bir algoritmaya göre deterministik olarak yeniden düzenleyerek şifreleyen bir tekniktir. Piksel karıştırma, bir görüntü şifreleme veya yardımcı şifreleme tekniğidir. Ayrıca görüntü gizleme, paylaşma ve dijital filigranlamada önemli bir ön işlem ve/veya son işlem yöntemidir (Xiong et al., 2018). Bu yöntem, görüntünün görsel görünümünü bozarak yetkisiz erişimi engellemeyi amaçlar.

Piksel karıştırma diğer şifreleme yöntemlerine kıyasla daha basit ve anlaşılır yöntemlerdendir. Ayrıca diğer şifreleme yöntemlerine göre uygulaması daha az karmaşık olduğundan işlem süreleri daha kısadır. Arnold dönüşümü (Xiong et al., 2018), Jigsaw dönüşümü (Abou elazm et al., 2020), Fibonacci dönüşümü (Mishra, 2012), Knight turu (Singh et al., 2015), (Shashikiran et al., 2021), Lucas dönüşümü (Mishra, 2012), sihirli kare dönüşümü (Gaffar et al., 2020), hücresel otomata (Chai, Gan, et al., 2017) , Baker haritası (Mao et al., 2004) ve affine dönüşümü (Kengnou Telem et al., 2022), görüntü şifrelemede popüler görüntü karıştırma yöntemlerindendir.

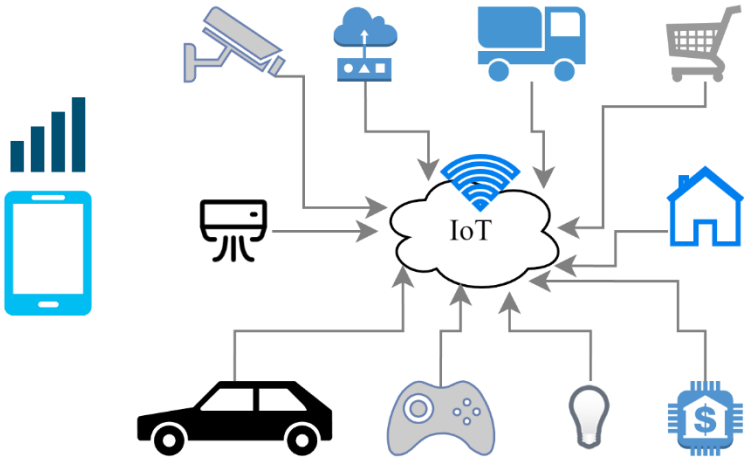
3. NESNELERİN İNTERNETİ

3.1. Nesnelerin İnterneti Kavramı

Nesnelerin İnterneti (IoT) kavramı, ilk kez 1999'da Kevin Ashton tarafından fiziksel dünyadaki nesnelerin algılayıcılar (sensör) yardımıyla ağa bağlanabildiği bir sistem olarak ifade edilmiştir (Bhatia et al., 2017). IoT, algılayıcılar ve RFID'ler gibi milyonlarca farklı nesneyi, cihazı akıllı bir şekilde birbirine bağlayan çok geniş kullanım alanına sahip teknolojilerdir. Bu sistemler birçok cihaz ve nesne içerdiğinden nesnelerin iletişimini yöneten mekanizmalara sahiptirler.

IoT sistemleri akıllı şehir sistemlerinde, akıllı park alanları, gelişmiş trafik sistemleri, şehirlerdeki trafik sıkışıklığını en aza indirmeye yardımcı olan ve aynı zamanda enerji tüketimini azaltmaya yardımcı olan ağ bağlantılı araçlar, akıllı ev teknolojileri gibi her alanda yaygın şekilde kullanılmaya başlanmıştır. IoT'nin temel amacı, çevreyi algılayan, bilgi toplayan ve işleyen, bu sayede işlerin verimli bir şekilde yapılmasını sağlayan akıllı ağlar oluşturmaktır. Böylece, zaman ve mekândan bağımsız tüm sistemlerin sürdürülebilirliğini sağlamaktadır. Cihazlar insan müdahalesi olmadan IP bağlantısını kullanarak kendi aralarında iletişim kurabilir ve çevrelerini analiz edebilirler.

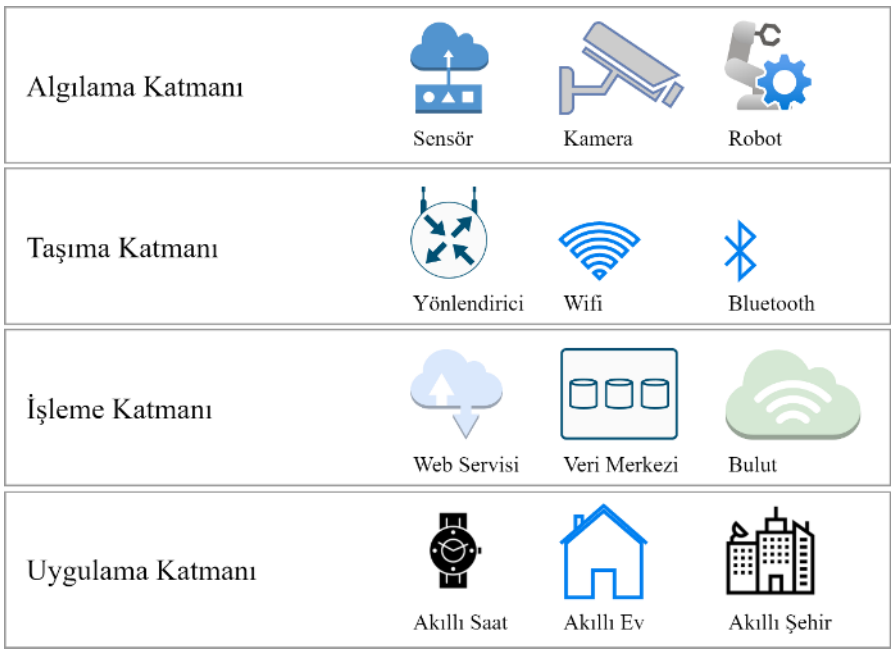
IoT ekosistemi, akıllı telefon ve tablet, bilgisayar, akıllı nesneler, algılayıcılar ve aktüatörlerden oluşur. Radyo frekansı tanımlama (RFID), Zigbee, Wifidirect, Hızlı Yanıt (QR) kodlarını kullanacak, Yakın alan iletişimi (NFC), kablosuz sensör ağı, yapay zekâ, cihazlar arasında iletişimin sağlanmasına yönelik sensör veya kablosuz teknolojiler içerir. Ancak özetle IoT'nin amacı hayatımızı daha verimli hale getirmektir. Üstelik IoT cihazları verimliliğin, işin otomasyonunun, operasyon hızının ve daha fazla birbirine bağlı dünyanın artmasına yardımcı olmaktır (Iera et al., 2010). IoT kullanım örnekleri Şekil 3.1'de gösterilmiştir.



Şekil 3.1: Nesnelerin interneti kullanım örnekleri

3.2. Nesnelerin İnterneti Katmanları

Sensörlerin giderek ucuzlaması ve elektronik cihazların boyutlarının küçülmesiyle beraber daha yaygın kullanım imkânı bulan IoT cihazları, insanın birçok nokta ile yüksek seviyede etkileşim içerisinde olmasını sağlamıştır. Nesnelerin interneti katmanları farklı çalışmalarda 3 ile 7 katman arasında kategorize edilse de temel olarak dört katmandan oluşmaktadır (Sethi & Sarangi, 2017). Bu katmanlar algılama katmanı, taşıma katmanı, işlem katmanı ve uygulama katmanlarıdır. Nesnelerin interneti katman yapısı şekil 3.2'de verilmiştir:



Şekil 3.2: Nesnelerin interneti katmanları ve örnek cihazları ve sensörleri

3.2.1. Algılama katmanı

Bu katmanda esas olarak nesneleri tanımlayan ve bilgi toplayan, adeta insan duyu organları gibi çalışılan katmandır. Barkod ve etiket okuyucular, RFID okuyucu-yazıcılar, kamera, GPS, sensörler gibi tüm algılayıcılar bu katmanda toplanmaktadır.

3.2.2. Taşıma katmanı

Algılama katmanı ekipmanlarının topladığı verilerin internet üzerinden taşındığı katmandır. Bu katmanın ana işlevi bilgiyi taşımaktır.

3.2.3. İşleme katmanı

Bu katmanda taşınan veriler işlenir. Bu katman, fiziksel ortamdan gelen verileri işleyip anlamlandırabilen bulut bilişim sistemlerinden oluşur. Sensörlerden toplanan ham veriler alınır ve bulut hizmetleri, büyük veri modülleri aracılığıyla işlenerek faydalı bilgilere dönüştürülür. İşleme katmanı aynı zamanda ara yazılım katmanı olarak da isimlendirilir (Susilo & Sari, 2020).

Bir IoT sistemi genellikle çok sayıda uç cihaz tarafından oluşturulan büyük hacimli verileri ağın kenarlarındaki birden fazla uç birimde işler. İşleme katmanının ara yazılımı, bu verileri uygulama katmanına hazırlamak için üç aşamalı bir yaklaşım kullanır. Bu aşamalar veri birikimi, veri soyutlama ve veri analizidir (Aziz & Haq, 2018). Bu aşamalarda yapılan işlemlerin özeti şu şekildedir:

Veri Birikimi: Farklı veri türlerini doğru şekilde tanımlar ve uygun depolama birimine atar. Ses ve video akışları ve görüntüler gibi yapılandırılmamış veriler genellikle daha fazla depolama alanı gerektirir. Cihaz okumaları, günlük değerleri ve ölçümlerden (telemetri verileri) oluşan yapılandırılmış veriler, alan açısından daha verimlidir ve veri ambarlarında depolanır (Kim et al., 2009).

Veri Soyutlama: Birden fazla kaynaktan veri toplamayı ve verilerin uygulama katmanı yazılımı tarafından okunabilecek bir formata dönüştürülmesini sağlar (Khan & Mian, 2020).

Veri Analizi: Büyük ve görünüşte rastgele veri kümeleri içindeki kalıpları tespit etmede uzmanlaşmış makine öğrenmesi (ML) veya derin öğrenme algoritmaları kullanılır (Susilo & Sari, 2020; Al-Garadi et al., 2020).

3.2.4. Uygulama katmanı

Çözümlenen verilerin uygulamalar tarafından kullanıldığı katmandır. İş gören uygulamaların nesnelerin interneti mimarisindeki yeri burasıdır. Uygulama katmanı, kullanıcıya ve uygulamaya özel hizmetlerin sunulmasından sorumludur. Akıllı evler, akıllı şehirler ve akıllı sağlık gibi Nesnelerin İnternetinin kullanılabileceği çeşitli uygulamalar bu katmanda tanımlanır (Sethi & Sarangi, 2017).

3.3. Nesnelerin İnterneti Uygulamalarında Kullanılan Şifreleme Algoritmaları

IoT, internetin önemli bir bileşeni ve birbirine bağlı milyonlarca nesne için hayati bir altyapı olarak kullanılmaktadır. Bu nedenle IoT'nin güvenliği son derece önemlidir. Gizlilik, güvenli depolama ve yönetim, yetkilendirme ve iletişimin yanı sıra erişim kontrolü gibi güvenlik faktörleri de IoT ortamındaki temel ve zorlu görevlerdendir (Rauscher & Bauer, 2018). IoT sistemlerde bir düğümde oluşan bir tehdit engellenemediği takdirde saldırı tüm sisteme etki eder. Bu nedenle IoT güvenliği, garantili iletişim ile sağlanmalı, verilere sadece yetkili kişilerin erişimine izin verilmeli, ayrıca sık güncelleme yapılarak akıllı uygulamalar saldırılara karşı korunmalıdır. IoT cihazların iletişim omurgası olan internet kurumsal ve bireysel siber saldırılara açık bir ortamdır. Güvenlik önlemleri yalnızca altyapı ve sistemle sınırlı olmayıp, donanım ve fiziksel güvenliği de gerektirebilir (Rajashree et al., 2018). Bu anlamda Kriptografi çalışma alanı IoT sistemleri için uygulama güvenliğini sağlamaya yönelik algoritmalar geliştirmektedir.

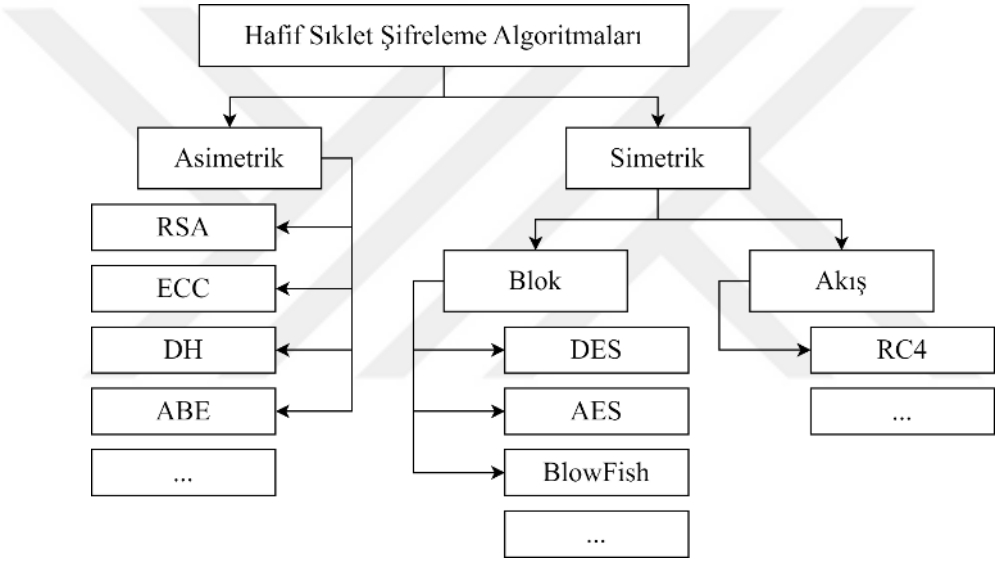
Siber güvenlik, bilişim sistemlerinde kullanılan verilerin yetkisiz erişime karşı korunmasına yönelik her türlü önlem olarak tanımlanabilir (Gündüz & Daş, 2022). Kişisel bilgilerin ifşa edilmesi, kredi kartı hırsızlıkları, gizli bilgilerin sızması, bilgisayar sistemlerine virüs saldırıları günlük olarak yapılan kötü niyetli saldırı örnekleridir. Entegre, gizli ve orijinal bilgilerin sağlanması IoT'nin en büyük güvenlik sorunudur (Chahal et al., 2020).

IoT'de sensörlerin, akıllı kartların ve diğer mikro cihazların bilgi işlem gücü sınırlıdır. Bu nedenle, fiziksel boyut, hesaplama gereksinimleri, enerji tüketimi ve sınırlı bellek ile ilgili kısıtlamalara sahip sistemlere hafif şifreleme modelleri uygundur. Hafif şifreleme, sınırlı kaynaklara sahip cihazlar için güvenli şifrelemenin uygulanmasına olanak tanıyan şifrelemedir. Uluslararası Standartlar Organizasyonu (ISO) ve Uluslararası Elektroteknik Komisyonu (UEC), bilgi ve iletişim teknolojisine ilişkin standartları belirleyen mercilerdir.

Bu standartlara göre "hafif kriptografi" olarak kabul edilecek algoritmalar aşağıdakilerle ilgili gereksinimleri karşılamalıdır:

1. Anahtar boyutu en az 80 bit en fazla 112 bit olmalıdır. Sınırlı pil ömrü olan IoT sistemlerde küçük anahtar alanı maksimum sürede güvenlik sağlamalıdır.
2. Yazılım için kod uzunluğu ve gerekli RAM miktarı, IoT platformu için mevcut standartlardan daha az kaynak gereksinimine sahip olmalıdır.
3. Donanım için kriptografik modelin kapladığı çip alanı ve enerji tüketimi, mevcut ISO standartlarına göre daha az olmalıdır.

IoT sistemlerde kullanılan hafif şifreleme yöntem ve algoritmaları da genel olarak simetrik ve asimetrik olarak iki ana kategoride toplanabilir. IoT için kullanılan hafif siklet algoritmaların kategorizasyonu şematik olarak Şekil 3.3.'de gösterilmiştir.



Şekil 3.3: IoT sistemlerinde kullanılan şifreleme algoritmaları (**RSA**: Rivest, Shamir ve Adleman, **ECC**: Elliptic Curve Cryptography, **DH**: Diffie-Helman, **DES**: Data Encryption Standart, **AES:** Advanced Encrypted Standard, **RC4:** Rivest Encryption 4).

4. GÖRÜNTÜ ŞİFRELEME

Görüntü şifreleme kriptografinin önemli bir çalışma alanıdır. Günümüz internet trafiğinin büyük bir bölümünü bireysel ve kurumsal görüntü verileri oluşturmaktadır. Bu durum görüntü şifrelemenin veri güvenliği ananındaki önemini göstermektedir. Bu bölümde görüntü şifreleme alanında kullanılan tanımlar, kavramlar, metodolojiler ve değerlendirme metrikleri gibi temel konular sunulacaktır.

4.1. Görüntü Şifrelemenin Tanımı

Dijital görüntüleri yetkisiz erişimden korumanın üç genel yolu şifreleme, steganografi ve filigranlamadır (Chelliah et al., 2013; Cox et al., 2011; Uhl & Pommer, 2005). Bu üç teknik arasında şifreleme, yüksek düzeyde güvenlik sağlamanın en önemli araçlarından biridir. İçerik gizliliği ve erişim kontrolü ile ilgilenirken, kimlik doğrulama ve telif hakkı koruması filigranlama teknikleriyle, gizlilik ise steganografi teknikleriyle ele alınmaktadır (Geetha et al., 2011). Dijital görüntüler, yüksek artıklık gibi benzersiz özellikler gösterir, pikseller arasında yüksek korelasyon gösterir ve boyutları nisbeten büyüktür. Görüntü tutarlılığının, veri iletimi, gerçek zamanlı işleme, görüntü sıkıştırma vb. gibi farklı görüntüleme uygulamalarının değişen ihtiyaçları vardır. Geleneksel metin şifreleme algoritmaları, görüntü şifreleme uygulamaları için uygun değildir. Bu faktörlerden dolayı araştırmacılar, bu makalenin odak noktasını oluşturan önemli miktarda görüntü şifreleme algoritması tasarlamış ve geliştirmiştir. Görüntü şifreleme, görüntüyü yetkisiz kişiler için anlamsız bir biçime dönüştürme işlemidir, böylece yalnızca yetkili bir alıcı görüntüyü yeniden oluşturabilir ve içindeki bilgiyi alabilir. Görüntüyü okunamayacak hale getirme yoluna şifreleme, ters işlemine ise şifre çözme (deşifreleme) adı verilir. Orijinal görüntüye düz görüntü, okunamayan görüntüye ise şifreli görüntü adı verilir.

4.2. Görüntü Şifreleme Temel Kavramları

Görüntü şifreleme işleminin tam olarak kavranabilmesi için aşağıdaki tanımların bilinmesi önemlidir.

Düz Görüntü (plain image/plain text image): Görüntü şifreleme algoritmasının girdisi olan şifrelenmek istenen orijinal görüntüdür. Görüntü şifreleme sisteminin girdilerinden biri düz görüntüdür ve iki boyutlu (2B) piksel değerleri matrisidir. Bir görüntü pikseli matematiksel olarak $P(x, y, v)$ şeklinde ifade edilebilir. Burada x ve y görüntü

matrisinin satır ve sütunu, v değeri ise piksel değeri ifade eder. Standart olarak bir görüntüde RGB (Red-Kırmızı, Green-Yeşil, Blue-Mavi) olmak üzere üç kanal bulunur.

Anahtar (key): Görüntü şifreleme ve şifre çözme işlemi için kullanılan gizli değerlerdir. Kriptografide Kerckhoffs prensibine göre güvenliği sağlayan ana öğe anahtardır. Bu sebeple yeterli karmaşıklığa sahip, kolay tahmin edilemez ve kolayca hesaplanamaz anahtar güvenli bir sistemin temelidir. Bir sistemin anahtarı simetrik ve asimetrik olmasına göre bir veya iki değerden oluşabilir. Simetrik sistemlerde, alıcı ve gönderici arasında güvenli bir kanal ile paylaşılması gereken tek bir anahtar vardır. Bu anahtar hem şifreleme adımında hem de deşifreleme adımında kullanılır. Asimetrik şifrelemede ise açıklanacak olan iki anahtar bulunur.

Açık Anahtar (public key): Asimetrik şifreleme sistemlerinde gönderici alıcının açık anahtarını kullanarak veriyi şifreler ve alıcıya gönderir. Alıcı ise, bir sonraki adımda açıklanacak olan, kendi özel anahtarını kullanarak veriyi tekrar okunaklı hale getirir. Bu sebeple asimetrik şifrelemede güvenli bir kanal üzerinden anahtar değişimine ihtiyaç yoktur.

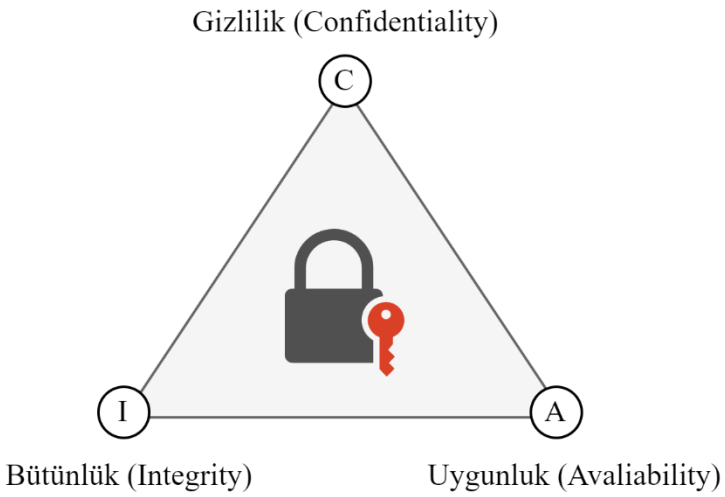
Özel Anahtar (Private key): Yalnızca alıcının bildiği ve şifreli görüntünün şifresini çözmek için kullanılan gizli değerdir. Özel anahtarın gizliliği alıcının sorumluluğundadır.

Şifreli Görüntü (cipher image): Şifreleme işleminin çıktısı ve şifre çözme işleminin girişidir.

Görüntü Şifreleme (image encryption): Girdi verisi olarak düz görüntü ve anahtar/açık anahtar kullanılarak şifreli görüntü oluşturma işlemidir.

Görüntü Şifre Çözme (image decryption): Giriş olarak anahtar/özel anahtar kullanılarak şifreli görüntünün düz görüntüye dönüştürülme işlemidir.

Kriptografide bilgi güvenliği, bilginin izinsiz eişimden, kullanımından, ifşasından, değiştirilmesinden veya zarar görmesinden korunması işleminin genel adıdır. Bilgi güvenliğinin temel işlevleri şekil 4.1'deki gibi özetlenebilir. Bilgi güvenliğinin sağlanabilmesi için şifreleme adımlarının CIA üçlemesini sağlaması gereklidir.

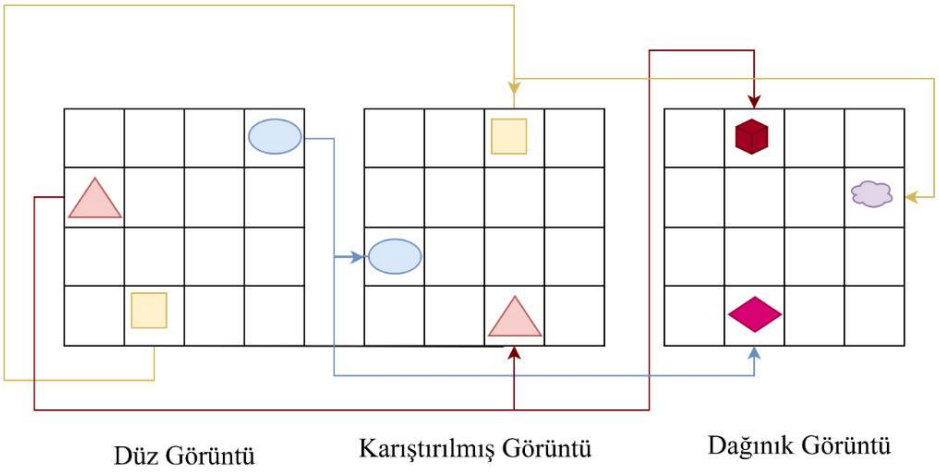


Şekil 4.1: Görüntü şifrelemede CIA üçlemesi.

4.3. Temel Görüntü Şifreleme Adımları

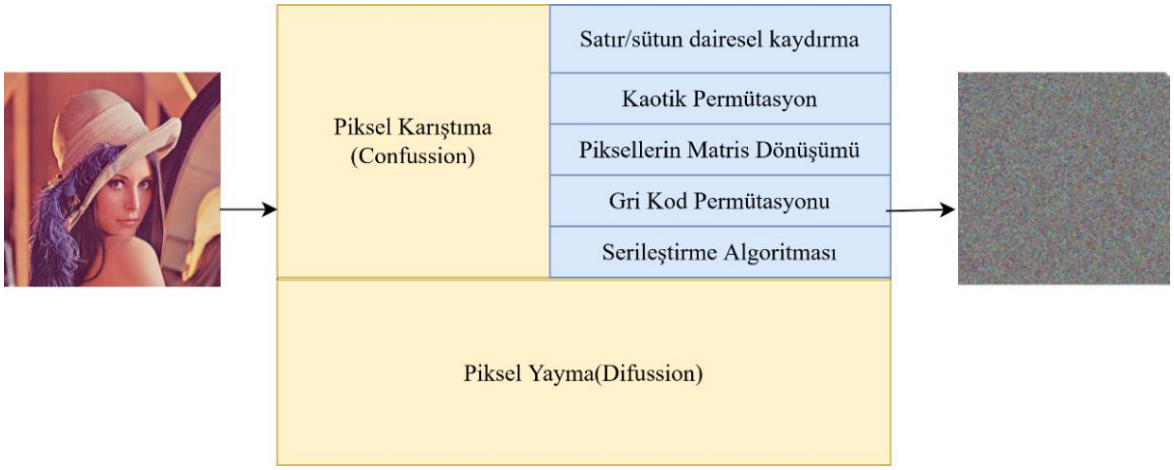
Temel olarak düz bir görüntüyü yalnızca hedeflenen alıcı tarafından deşifre edilebilecek kodlanmış bir forma dönüştürme işlemi olarak tanımlanan görüntü şifreleme veri türünün ve ilgili uygulamaların artan yaygınlığına ve ağ üzerinden güvenli şekilde iletilmesine yanıt olarak giderek önem kazanmıştır(Kolivand et al., 2024).

Görüntü şifreleme işlemleri genel olarak iki süreçten oluşur. Bunlar piksel konumlarının çeşitli yöntemlerle karıştırılması ve piksel değerlerinin difüzyon işlemiyle dağıtılması olarak özetlenebilir. Bu adımlardan karıştırma adımındaki amaç düz görüntüyü karışık görüntüyle değiştimek iken; yayma adımının amacı pikselleri değiştirmektir. İyi bir permütasyon işlemi, iyi bir karıştırma etkisi göstermeli ve iyi bir yayılma işlemi, düz görüntüdeki görsel olarak anlamsız seviyedeki küçük bir değişikliğin şifreli görüntü üzerinde büyük bir değişikliğe öncülük etmesi beklenir(Xing yuan Wang et al., 2010). Temel olarak karıştırma ve yayma adımları piksel değişikliği Şekil 4.2'de örneklendirilmiştir. Tabiki araştırmacılar karıştırma ve yayma adımlarını iç içe kullanarak, karıştırma sırasında değişiklik yapabilir. Bu anlamda Şekil 4.2 sembolik bir gösterimdir.



Şekil 4.2: Düz görüntü piksellerinin karıştırma ve yayma adımlarındaki değişikliğinin örneklenmesi.

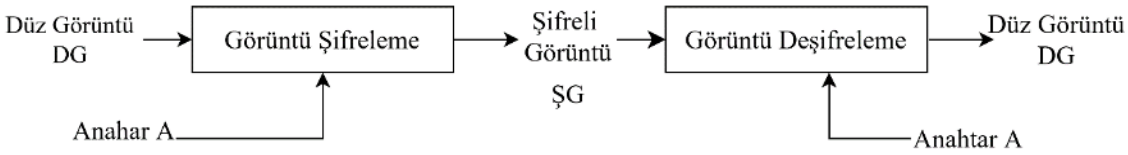
Görüntü şifreleme karıştırma adımında farklı algoritmalar kullanan birçok çalışma gerçekleştirilmiştir (X. Zhang et al., 2023; X. Zhang et al., 2023; X. Zhang et al., 2022). Yaygın kullanılan dönüşüm algoritmalardan sık kullanılanları zigzag ve spiral dönüşüm algoritmaları ve varyasyonlarıdır (S. Li et al., 2021; H. Li et al., 2022). Bu tür dönüşüm algoritmasının arkasındaki temel fikir, piksel matrisini algoritmanın önerdiği şekilde serileştirmek ve daha sonra serileştirilmiş diziden matrisi başlangıç boyutlarında yeniden oluşturmaktır (İnce et al., 2024). Bu algoritmaların en önemli görevi pikseller arasındaki korelasyonu zayıflatmaktır. Görüntü şifreleme adımlarının örnek resim üzerinde gösterimi Şekil 4.3' deki gibidir.



Şekil 4.3: Görüntü Şifreleme Temel Adımları (Köşe geçiş algoritması uygulanması sonrası Lena görüntüsü).

4.3.1. Simetrik görüntü şifreleme

Simetrik şifreleme sistemi, geleneksel şifreleme sisteminin tipik biçimi olarak kabul edilir çünkü yüzyıllarca tek şifreleme yöntemi olarak kullanılmaktaydı. Simetrik görüntü şifreleme, bir şifreleme Ş işlemi, düz görüntü D ve anahtar A olmak üzere iki parametreli ve çıkış olarak Şifrelenmiş Görüntü ŞG'yi üreten bir fonksiyondur. Şifre çözme işlemi ise şifreleme adımlarının tersten sürdürülmesi prensibine bağlı olarak D, giriş parametreleri şifreli görüntü ŞG ve anahtar A olmak üzere çıktı olarak düz görüntü D'yi üreten bir fonksiyondur. İşlemin tamamı Şekil 4.4'te gösterilmiştir. Ayrıca simetrik şifreleme fonksiyonları Denklem 4.1 ve 4.2'de sunulmuştur



Şekil 4.4: Simetrik görüntü şifreleme.

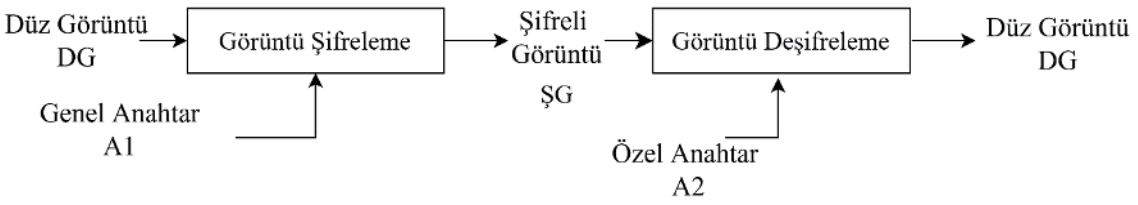
$$ŞG = Ş(DG, A) \tag{4.1}$$

$$DG = D(ŞG, A) \tag{4.2}$$

Burada hem şifrelemede hem de şifre çözme işleminde aynı anahtar alan değeri kullanılır. Şifreleme için düz görüntü ve anahtar alan değerleri kullanılırken, deşifreleme işleminde şifrelemenin tersi işlemi uygulanarak şifreli görüntü ve anahtar alan değerleri kullanılarak düz görüntü elde edilir.

4.3.2. Asimetrik görüntü şifreleme

Asimetrik görüntü şifreleme olarak adlandırılan bu yöntem, şifreleme ve deşifreleme işleminde farklı anahtar değeri kullanılan şifreleme yöntemidir ve şekil 4.5'deki gibi görsel olarak ifade edilebilir. Ayrıca şifreleme ve şifre çözme işlemlerinin fonksiyonları denklem 4.3 ve 4.4 'deki gibi ifade edilir.



Şekil 4.5: Asimetrik görüntü şifreleme.

$$ŞG = e\,(D, A_1) \tag{4.3}$$

$$DG = d(ŞG, A_2) \tag{4.4}$$

Burada A_1 ve A_2 farklı anahtarlardır. Genel ve özel anahtarlar daha sonra görüntü şifreleme ve görüntü şifre çözme anahtarları rolünde kullanılır. Gönderen, A_1 genel anahtarını elinde tutar, A_2 özel anahtarının gizliliği ise alıcının sorumluluğundadır. Çizelge 4.1, simetrik ve asimetrik şifrelemenin güvenlik gereksinimleri çizelgesidir.

Çizelge 4.1: Simetrik ve asimetrik görüntü şifreleme güvenlik kriterleri tablosu.

Kriterler	Simetrik Görüntü Şifreleme	Asimetrik Görüntü Şifreleme
Anahtarların kullanımı	Hem görüntü şifrelemede, hem de deşifrelemede aynı anahtar kullanılır.	Görüntü şifreleme ve deşifreleme için farklı anahtarlar kullanılır.
Şifreli görüntüyü kırma	Başka veri yoksa bir görüntüyü deşifre etmek sonuçsuz olmalıdır	Genel anahtar mevcut olsa bile bir görüntünün şifresini çözmek sonuçsuz olmalıdır.
Güvende tutulması gereken anahtar	Kullanılan tek anahtarın güvenli bir şekilde paylaşılması gerekir	Açık anahtar zaten açık iken gizli anahtar hiçbir şekilde paylaşılmamalıdır
Kriptoanaliz imkanı	Görüntü şifreleme ve örnek şifre görüntüsü bilgisi, anahtarı belirlemek için geçersizdir.	Görüntü şifreleme ve genel anahtar ve örnek şifre görüntüsü bilgisi, özel anahtarı belirlemek için geçersizdir.

Görüntü kriptanalizi, şifreli bir görüntüden düz görüntüyü elde etme işlemidir. Şifreli bir görüntü kriptanaliz yöntemleri ile analiz edilirken farklı senaryolar kullanılmakla birlikte en temel olarak, anahtar bilinmeden düz görüntünün bir kısmını veya tamamını matematiksel ve bilgisayar tabanlı yöntemler kullanarak elde etmeye çalışmaktır. Kriptanalist, anahtarı bilmese de, kriptosistemin diğer tüm parametrelerine hâkim olduğu kabul edilir.

Bir şifreleme sisteminin sağlamlığını değerlendirirken dört temel saldırı türü göz önünde bulundurulur:

- *Yalnızca Şifreli Görüntü Saldırısı:* Saldırgan, tıpkı bir casus gibi, sadece şifrelenmiş görüntülere erişebilir. Bu görüntülerdeki gizli mesajı çözmek için matematiksel ve bilgisayar tabanlı araçları kullanır.

- *Bilinen Düz Görüntü Saldırısı:* Saldırgan, hem şifrelenmiş hem de orijinal metnin bir kısmına sahip olur. Bu eşleşmeleri kullanarak, şifreleme algoritması ve anahtar hakkında bilgi edinmeye çalışır.
- *Seçilmiş Düz Görüntü Saldırısı:* Saldırgan, kendi seçtiği metinleri şifreleyip, şifreli metinleri kullanarak şifreleme algoritmasını ve anahtar hakkında daha fazla bilgi edinmeye çalışabilir. Bu, bir dedektifin ipuçlarını kullanarak bir gizemi çözmesine benzetilebilir.
- *Seçilmiş Şifreli Görüntü Saldırısı:* Saldırgan, bilinçli olarak bir dizi şifreli görüntü seçip, bu görüntülerin orijinal piksellerini gözlemleyebilir. Bu, algoritmanın zayıflıklarını bulmak ve şifreyi çözmek için kullanılabilir.

4.4. Görüntü Şifreleme Yöntemleri Kategorizasyonu

Şifreli bir görüntü, bir bakışta sıradan bir piksel karmaşası gibi görünebilir. Fakat bu piksellerin ardında, gizlenmiş bir mesaj saklıdır. Bu mesaj, özel bir anahtarla elde edilebilen bir içeriktir. İdeal bir şifreli görüntüde aşağıdaki özelliklerin olması gerekmektedir:

Piksellerin bağımsızlığı: Şifreli bir görüntüdeki pikseller, orijinal görüntünün aksine, birbirleriyle bağlantılı değildir. Bu da, şifrelenmiş görüntüyü sadece piksellerine bakarak çözmeyi imkânsız hale getirir.

Azaltılmış gürültü: Şifreleme işlemi, orijinal görüntüdeki gürültüyü ve fazlalıkları ortadan kaldırır. Bu da, şifreli görüntüyü daha kompakt ve analiz edilmesi daha zor hale getirir.

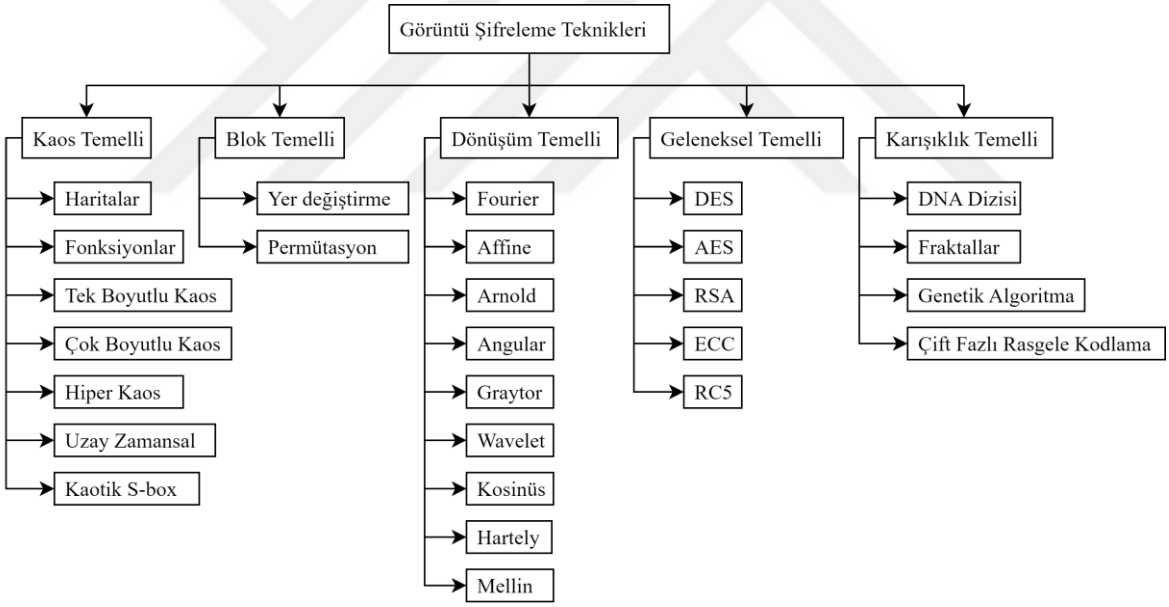
Güvenlik: Şifreleme algoritması, anahtar olmadan şifreli görüntüden orijinal görüntüyü çıkarmayı imkânsız hale getirmelidir. Bu da, mesajın yetkisiz kişiler tarafından ele geçirilmesini engeller.

Görüntü şifreleme işlemi için birçok farklı yöntem ve algoritma geliştirilmiştir. Mevcut metin şifreleme algoritmaları DES, AES, RSA gibi algoritmalar güvenli olsa da zaman karmaşıklıkları yüksek olan algoritmalar olduğu görülmüş ve veri yoğunluğu fazla olan görüntü verileri için farklı yöntem arayışlarına girilmiştir. Bu arayış sonrası dönüşüm tabanlı şifreleme teknikleri geliştirilmiş ve veriler tek tek işlenmek yerine blok blok işlenerek işlem hızı arttırma çabası blok tabanlı şifreleme algoritmalarının geliştirilmesine olanak sağlamıştır. Görüntü verilerinin şifrelenmesi sırasında öngörülebilirlik ve rasgelelik

arttırılarak şifreleme algoritmalarının kalitesinin arttırılması çabası da şifreleme algoritmalarında kaos tabanlı şifreleme algoritmalarının geliştirilmesinde önemli rol oynamıştır. Görüntü şifreleme işlemi için kullanılan yöntem ve algoritmaların genel sınflandırılması aşağıdaki gibidir.

- *Kaos tabanlı:* Kaotik matematiksel fonksiyonlar, pikselleri rastgele bir şekilde dağıtarak şifrelemeyi gerçekleştirir.
- *Blok tabanlı:* Görüntü, şifrelenebilecek küçük parçalara bölünür ve her blok ayrı ayrı şifrelenir.
- *Dönüşüm tabanlı:* Görüntü, Fourier transformasyonu gibi matematiksel işlemler kullanılarak farklı bir alana dönüştürülür ve şifrelenir.
- *Geleneksel teknikler:* AES ve RSA gibi klasik şifreleme algoritmaları görüntüyü şifrelemek için kullanılabilir.

Bu kategorizasyonun geniş şematik gösterimi Şekil 4.6. te verilmiştir.



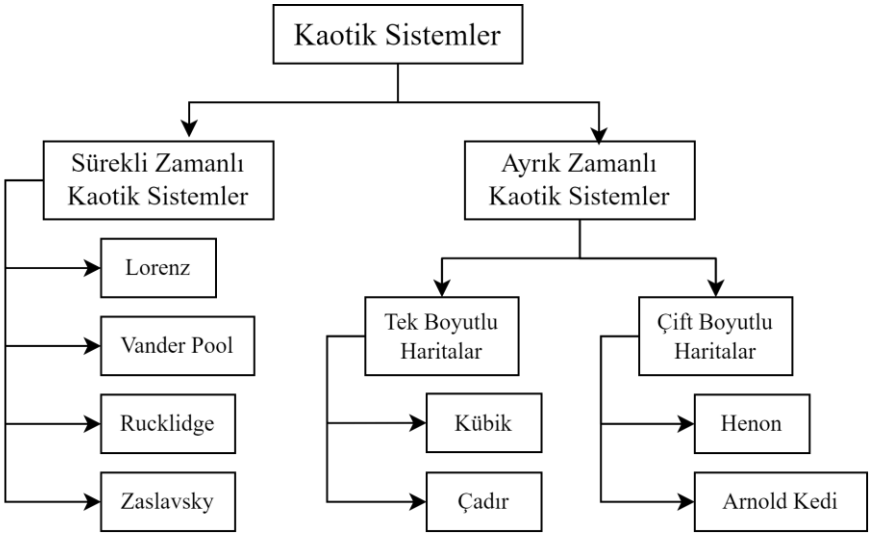
Şekil 4.6: Görüntü şifreleme teknikleri.

4.5. Görüntü Şifrelemede Kullanılan Kaotik Haritalar

Kaos teorisi, peryodik, doğrusal olmayan(non-linear), dinamik ve bağlı öğelerden elde edilen karmaşık yapıları ele almaya imkan tanıyan kavramsal, matematiksel, geometrik yöntemlerin birleşimidir (Gökmen A., 2009). Bu tür sistemlere örnek olarak hava koşulları, hisse senetleri değişimi, kalp ritm ölçümü, beyin dalgalarının hareketleri, türbülans kontrolü, desen tanıma ve bulma, rasgele sayı üreticiler, nüfus artış şekilleri gibi örnekler verilebilir (H. Xu et al., 2016; Aihara & Suzuki, 2010; Thesis & Engineering, 1997; X. Zhou et al., 2012; İnce, 2023).

Deterministik modeller, hiçbir rastgelelik olmayan sistemlerdir. Kaotik sistemler tahmin edilmesi zor deterministik sistemlerdir. Bir sistemin kaotiklik özellikli olup olmadığını anlamak için bazı özelliklerine bakılması gerekir. Bunlar en temel anlamada başlangıç şartlarına hassasiyet, rasgele olmama, frekans spekturumu, Lyapunov üstelleri gibi özelliklerdir. Kaotik sistemler düzensizlik içinde bir düzene sahiptirler. Literatürde çok sayıda kaotik sistem önerilmiş olup üzerinde en çok çalışma yapılan kaotik sistemler Lorenz, Rössler, Chen, Arnold Cat, Tent, Rikitake kaotik sistemleridir (Bourekouche et al., 2024 ;Hermann et al., 2022; İnce et al., 2024; Pehlivan, 2007).

Kaotik sistemler matematiksel modellendirilmelerine göre sürekli zamanlı kaotik sistemler ve ayrık zamanlı kaotik sistemler olarak sınıflandırılabilirler. Kaotik haritaların sınıflandırması Şekil 4.7' deki gibidir.



Şekil 4.7: Kaotik haritaların sınıflandırılması.

Kaotik sistemler dinamik yapıya sahiptirler bu da zamana göre değişim anlamına gelmektedir. Aynı zamanda bu sistemler değişken ve periyodik olmayan yapılardır. Böylece kendilerini tekrar etmezler.

Matematiksel olarak kaotik yapılar modellendiğinde güç spekturumlarının gürültü spekturuma benzer yapıda olması, Lyapunov üstellerinden en az birinin pozitif değer alması, Poincare kesitinin bir bölümünün yada tamamının düzensiz olması gözlemlenir.

4.5.1. Sürekli Zamanlı Kaotik Sistemler

Sürekli zamanlı kaotik sistemler, $x(t)$ bir vektör olmak üzere;

$$f(x(t)) = \frac{d(x(t))}{dt} \tag{4.5}$$

olacak şekilde adi diferansiyel denklem olarak ifade edilen sistemlerdir. Sürekli zamanlı bir denklemin üçüncü dereceden bir denklem olması ve nonlineer yapıda olması gerekmektedir (Chua et al., 1993).

Lorenz Haritası: Lorenz, üç boyutlu kaotik, dinamik bir haritadır. Bu bileşik diferansiyel denklem ilk olarak 1963 yılında Edward Lorenz tarafından geliştirilmiştir (Almeida et al., 2016). Bu kaotik sistem denklem 4.6'daki gibi ifade edilir:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= rx - rz - y \\ \frac{dz}{dt} &= xy - bz \end{aligned} \tag{4.6}$$

Sistem büyük ölçüde r ve b kontrol parametrelerine bağlıdır. Sistem matematiksel runge kutta yöntemi ile diferensiyel denklemi elde edilir (İNCE et al., 2021). Burada $\sigma = 10, r = 28\ ve\ b = 8/3$ parametreleri ve $x_0 = 0, y_0 = -0.1\ ve\ z_0 = 9$ başlangıç şartları için sistem kaotiklik göstermeye başlar. En temel kaotik sistem Lorenz kaotik sistemidir.

Rucklidge Kaotik Harita: Doğrusal olmayan dinamiklere sahip bir diğer sürekli zamanlı kaotik harita da rucklidge kaotik haritasıdır**.** Hesaplanması denklem 4.7'deki gibidir.

$$\begin{aligned} x &= -kx + \lambda y - yz \\ y &= x \\ z &= -z + y^2 \end{aligned} \tag{4.7}$$

Bu denklemlerdeki x, y, z değişkenleri durum değişkenleri, k ve λ değişkenleri ise sistemin parametreleridir.

4.5.2. Ayrık Zamanlı Kaotik Sistemler

Ayrık zamanlı kaos sistem, f(x) nonlineer fonksiyonunun iterasyonu ile elde edilen, geri beslemeli kaotik dizilerden oluşan sistemdir. Ayrık zamanlı bir sistem denklem 4.8'deki gibi ifade edilir.

$$X_{n+1} = f(X_n) \tag{4.8}$$

Seçilen f(x) fonksyonunun kaotik özellik göstermesi için başlangıç koşullarına aşırı hassasiyet göstermesi gerekir. Literatürde sıklıkla kullanılan ayrık zamanlı kaotik haritalar aşağıdadır.

Çadır Kaotik Harita: Doğrusal olmayan deterministik sistemlerden biri çadır kaotik haritalardır. Değişmez yoğunluk ve güç spekturumu açısından kaotik bölgenin tamamını kapsayan çadır haritasının kaotik davranışları ilk olarak 1983'te Yosidaa vd. (Yoshida et al., 1983) tarafından sunulmuştur. Yapılan incelemelerde çadır haritasının topolojik olarak eşlenik oduğu ve haritanın yinelemeler sonucu aynı şekilde davrandığı tespit edilmiştir. Kaotik çadır haritalarının matematiksel denklemi denklem 4.9'da verilmiştir.

$$x_{i+1} = f(x_i, \mu)$$
$$f(x_i, \mu) = \begin{cases} \mu \times x_i & x_i < 0.5 \\ \mu \times (1 - x_i) & diğer \end{cases} \tag{4.9}$$

Burada μ [0, 2] kapalı aralığında kaotiklik özellik gösterir.

Henon Kaotik Haritası: İki boyutlu ayrık zamanlı dinamik sistemlerden biridir. İkinci dereceden doğrusal olmayan iki boyutlu bir harita sunar. Basit uygulanabilirliği nedeniyle sayısal çalışmalarda yaygın kullanılan Henon haritası IoT ortamlarında kullanılmaya imkan tanıyan sayısal işlemlerle elde edilir (W. Bin Chen & Zhang, 2009). Henon kaotik harita hesabı denklem 4.10'da verilmiştir.

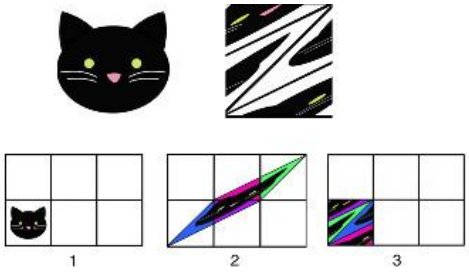
$$x_{i+1} = 1 - ax_i^2 + y_i$$
$$y_{i+1} = bx_i, i = 0,1,2,3, \ldots \tag{4.10}$$

Henon kaotik haritasında a=0.3 ve b=1.4 değerlerinde sistem kaotiklik göstermeye başlar.

Arnold Kedi Haritası: Arnold'un kedi haritası, kendi içinde kaotik bir haritadır ve adını 1960'larda bir kedi resmi kullanarak etkilerini gösteren Vladimir Arnold'dan almıştır (Dachlan 2014:1, 2014).

Arnold'un kedi haritası, alanı bir yönde bir birim, diğer yönde iki birim uzatan iki boyutlu torus T2'nin kendisine dönüşümüdür. Daha sonra, her birim karedeki kısmi

görüntüler alınarak ve bunların Şekil 4.8'de gösterilen orijinal simidin karşılık gelen kısmına çevrilmesiyle görüntü, orijinal simitin karesinde yeniden birleştirilir.



Şekil 4.8: Arnold Kedi Haritası dönüşümü

Arnold'un kedi haritası matematiksel ifadesi denklem 4.11'de verilmiştir.

$$\begin{bmatrix} x_{k+1} \\ y_{k+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_k \\ y_k \end{bmatrix} \tag{4.11}$$

Zavslavsky Kaotik Haritası: Zavslavsky haritası, kaotik sistemleri modellemek ve görüntü şifreleme gibi alanlarda kullanılmak üzere geliştirilmiş sürekli zamanlı kaotik haritadır. Bu haritanın matemtiksel ifadesi denklem 4.12'deki gibidir

$$X_{n+1} = f(X_n) + \mu \times X_n \times \sin(\pi \times X_n) \tag{4.12}$$

Chebyshev Kaotik Haritası: Chebyshev kaotik haritası, kaotik sistemleri modellemek ve görüntü şifreleme gibi alanlarda kullanılmak üzere geliştirilmiş sürekli zamanlı kaotik haritadır. 1989 yılında Rus matematikçi Sergey Smirnov tarafından tanıtılmıştır (Shiryaev, 2012). Chebyshev kaotik haritası, denklem 4.13'de verilmiştir.

$$x_{n+1} = f(X_n) + \mu \times cos\ (\pi \times xn) \tag{4.13}$$

4.6. Kaotiklik Ölçme Kriterleri

Bir sistemin kaotiklik gösterip göstermediğini tespit için birçok yöntem mevcuttur. Bunlar faz portreleri, denge noktaları, lyapunov üstelleri, çatallanma diyagramları, zaman serileri analizi gibi yöntemler bunlardan en çok kullanılanlarıdır (J. Wen et al., 2021).

Faz Portreleri Analizi: Durum değişkenlerinin ve türevlerinden meydana gelen uzay alanıdır. Bu analizde sistemin yörüngesi takip edilir. Zaman sonsuza giderken izlenen yörünge yani sistemin almış olduğu değerler kümesi sistemin faz portresidir. Bir sistem, kararlı peryodik bir yapıya sahip olması durumunda zaman sonsuza giderken kapalı bir şekil oluşur. Kaotik sistemlerin defalarca tekrarlanmasına rağmen yörüngelerin aynı noktalardan geçmediği gözlemlenmiştir.

Denge Noktaları Analizi: Denge noktaları etrafında kalan sistem kararlıdır. Denge noktalarını bulmak için sistem denklemleri sıfıra eşitlenir ve denklemler çözülür. Daha sonra bulunan değerler Jacobian matrisi ile çözülerek $|J - \lambda I|=0$ denklemi ile sistemin özdeğerleri bulunur. Bu değerlerden en az biri pozitifse sistem kaotiktir çıkarımı yapılabilir (Tez, 2016).

Zaman Serileri Analizi: Kaotik sistemde bulunan değişkenlerin zamanla nasıl değiştiğini tespit etmek için kullanılan analizdir. Bu yöntem bir sistemin kaotikliğini tek başına tespit edemez. Çünkü değerlerin sadece belli aralıklardaki değerleri gözlemlenmektedir. Bu yöntem kaotikliği tek başına belirleyemese de başlangıç koşullarına hassasiyeti ölçmede etkin bir yöntemdir. Giriş değerlerinde yapılan en ufak bir değişiklik çıkış değerlerini tamamen değiştirip değiştirememe durumuna göre kaotikliğin kontrolü gerçekleştirilebilir (Uzel, 2008).

Lyopunov Üstelleri Analizi: Kaotik sistemlerin kaotiklikliklerini ölçmede kullanılan en önemli yöntem Lyopunov üstelleri yöntemleridir. Bu yöntem, başlangıç şartlarındaki değişime sistemin tepkisini tespit etmektir.

Lyapunov üstelinin (λ) matematiksel hesabı denklem 4.14'te verilmiştir.

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=1}^{N} \log_2 \frac{d(t_k)}{d_{(k-1)}}, \quad \mathrm{d}\,(\mathrm{t}) = d_0 e^{\lambda \mathrm{t}} \tag{4.14}$$

Bu denklemdeki d (t) uzaklık değeridir. Üç boyutlu sürekli zamanlı sistemlerde kaotik davranışı belirten tek durum "-, 0, +" durumudur ($\lambda 1 < 0$, $\lambda 2 = 0$, $\lambda 3 > 0$). Dört boyutlu sistemlerde ise işaretlere göre kaotiklik durumları şu şekilde yorumlanır:

1. (+, +, 0, -) ise bu sistem hiperkaos (Awrejcewicz et al., 2012)
2. (+, 0, -, -) ise bu sistem kaos (tuhaf çekici) (Uzel, 2008)
3. (+, 0, 0, -) ise bu sistem torus kaostur (W. Wu et al., 2009).

Çatallaşma Analizi: Sistemde bir parametre değişikliğinin toplam sistem üzerindeki etkisini görebilmek için kullanılan yöntemlerden birisi çatallaşma diyagramlarıdır. Bu analizle sistemin kaosa girdiği ve çıktığı aralık tespit edilir. Yerel maksimum değerlerinin çizdirilmesi ile çatallaşma diyagramı elde edilir. Sistem kaotikliği ve kararlılığı çatallaşma diyagramlarıyla gözlemlenebilir (Lin et al., 2006).

Başlangıç Koşullarına Duyarlılık Analizi: Kaotik sistemler başlangıç koşullarına aşırı hassas sistemlerdir. Sistemin durum değişkenlerinden herhangi birisinin başlangıç değerinin

çok küçük oranda bile değişmesi, sistemin bütün durum değişkenlerinin çözüm kümesini değiştirir.

4.7. Değerlendirme Metrikleri

Görüntü şifreleme işleminin kullanılabilirliğini ve şifrelemenin kalitesini belirlemek için şifreleme değerlendirme metrikleri mevcuttur. Bu değerlendirme metrikleri şifreleme işlemini istatistiki, kalite, diferansiyel, gürültü, anahtar alan, rasgelelik gibi kriterlere göre kıyaslanabilir bir rapor sunar. Genel bir değerlendirme metrikleri kategorizasyonu Şekil 4.9'da verilmiştir

4.7.1. İstatistiki analizler

4.7.1.1. Korelasyon analizi analizi

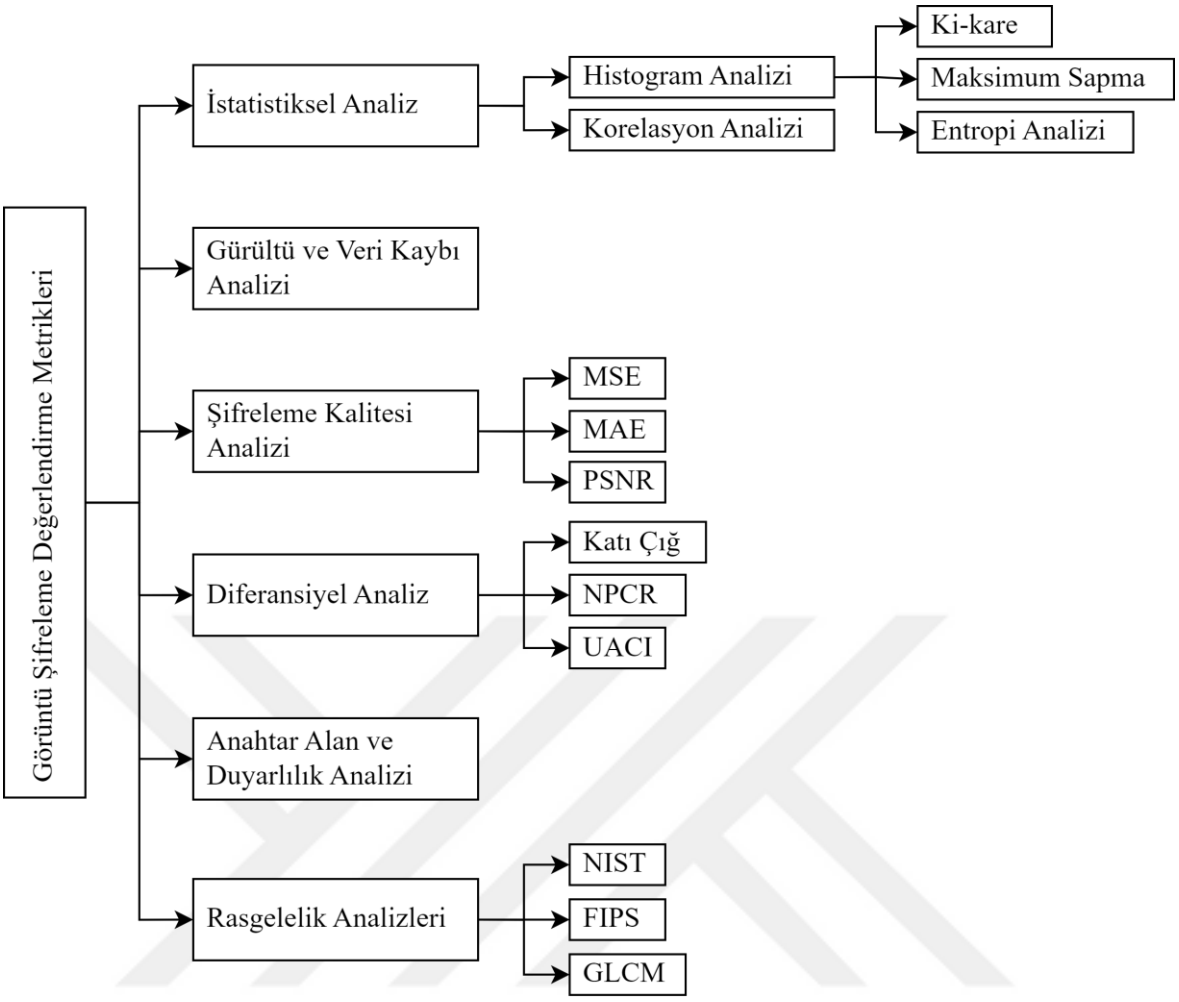
Korelasyon katsayısı, hem düz görüntüdeki hem de şifreli görüntüdeki bitişik pikseller arasında geçerli olan korelasyonu inceler ve görüntü şifreleme sisteminin kalitesinin bir tahminidir (Cohen & Handy, 2001). Korelasyon değerinin sıfıra yaklaşması şifreleme işleminin başarısını gösterir. X: düz görüntü, Y: şifreli görüntü, L:piksel sayısı olmak üzere korelasyon denklem 4.15-4.18'deki gibi hesaplanır:

$$E(X) = \frac{1}{L}\sum_1^L X_i \tag{4.15}$$

$$D(X) = \frac{1}{L}\sum_1^L (X_i - E(x))^2 \tag{4.16}$$

$$cov(X,Y) = \frac{1}{L}\sum_1^L \big(X_i - E(X)\big)\,(Y_i - E(Y)) \tag{4.17}$$

$$r_{XY} = \frac{cov(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}} \tag{4.18}$$



Şekil 4.9: Görüntü şifreleme işleminde kullanılan değerlendirme metrikleri.

4.7.1.2. Histogram analizi

Görüntüler, hassas bilgiler içeren dijital veri denizinde önemli bir yer tutar. Bu değerli görselleri korumak için güçlü şifreleme yöntemleri devreye girer. Histogram analizi de bu yöntemlerin güvenliğini ve sağlamlığını ölçmek için kullanılan kritik bir araçtır. Basitçe histogram, bir görüntünün piksellerinin renk ve parlaklık değerlerinin dağılımını gösteren bir grafiktir. Düzgün bir histogram, görüntünün rastgele ve şifreli olduğunu gösterir. Bu da saldırganların görüntüyü anlamlı bir şekilde yorumlamasını zorlaştırır. Histogram analizi için ki-kare, maksimum sapma, düzensiz sapma, tekdüze histogramdan sapma gibi ölçümler mevcuttur. Bu ölçümlerin işlevi kısaca şu şekilde özetlenebilir:

4.7.1.3. Ki-kare analizi

Ki-kare χ2, şifre görüntüsünün histogram değerlerini tekdüze bir histogramın beklenen dağılımıyla karşılaştırarak, bir algoritma tarafından üretilen şifre görüntülerinin rastgeleliğini ve tekdüzeliğini test etmek için görüntü şifrelemede kullanılan istatistiksel bir testtir (Ma et al., 2019). Ki-kare, piksel değerlerinin dağılımının tekdüze olup olmadığını belirlemek için şifre görüntüsünün her pikselini test eder. Ki-kare (χ2) matematiksel olarak denklem 4.19 ve 4.20'deki gibi ifade edilir.

$$X^2 = \sum_0^{255} \frac{(f_i - \varepsilon)^2}{\varepsilon} \tag{4.19}$$

$$\varepsilon = \frac{H \times W}{256} \tag{4.20}$$

Denklem 4.19'daki f şifreli görüntünün histogramı, f_i, şifreli görüntüdeki *i* indeksinin histogramı değeridir. Denklem 4.20'daki H ve W görüntünün yüksekliği ve genişliğidir. Düzgün dağılmış bir histogramın $\chi 2$ değeri 0'dır. $\chi 2$ değerinin düşük olması şifreli görüntünün histogram dağılımının düzgün bir dağılıma yakın olduğunu gösterir. Ayrıca, χ2 değeri daha yüksek olduğunda histogram düzgün değildir.

4.7.1.4. Maksimum sapma anlizi

İki histogramın piksel değerleri arasındaki ortalama sapmasını gösterir.

Tekdüze histogramdan sapma: Şifrelenmiş görüntü histogramının ideal düz çizgiden ne kadar sapma gösterdiğini gösterir.

Düzensiz sapma: iki histogramın piksel değerlerinin ortalama sapmasını gösterir.

4.7.1.5. Entropi analizi

Bilgi entropisi, iletişim sistemlerindeki belirsizliği ve rastgeleliği tahmin eden istatistiksel bir testtir. İlk kez 1948'de Claude Shannon tarafından tanıtılmıştır (Shannon, 1948). Görüntü şifrelemede entropi, şifreli görüntüdeki piksellerin dağılımının rastgeleliğini ölçmek için kullanılır. Yüksek bir entropi değeri, düz metnin daha iyi gizlendiğini ve herhangi bir fark edilebilir modelin bulunmadığını gösterir. Bir şifreleme algoritmasının öngörülemezliğini ve rastgeleliğini değerlendirmek için araştırmacılar, küresel entropi ve yerel entropi olmak üzere iki tür entropi testine güvenirler. Küresel entropi olarak da bilinen

Shannon entropisi, tam görüntünün piksel bilgisini hesaplarken, yerel entropi, rastgele seçilen örtüşmeyen blokların ortalama entropisini ölçer. Shannon entropisi denklem 4.21 kullanılarak hesaplanabilir.

$$H(m) = -\sum_{0}^{2^n-1} p(m_i) log_2[\, p(m_{i)}\,] \tag{4.21}$$

Denklem 4.21'deki n, bit sayısını temsil ederken p(m_i), m_i sembolünün olasılığını temsil eder. p(m_i), görüntüdeki her yoğunluk değeri için normalleştirilmiş histogram sayımlarını temsil eder. 8 bitlik bir gösterimde bir pikselin mümkün olan maksimum yoğunluk değerinin 256 olduğu ve bir piksel değerinin oluşma olasılığının 1/256 olduğu göz önüne alındığında, bir görüntü için ideal entropi değeri denklem 4.22'de verilen eşitlikle hesaplanır:

$$H_{ideal} = -\sum_{0}^{255} \frac{1}{256} \times log_2 \frac{1}{256} \tag{4.22}$$

Denklem 4.22 matematiksel ifadesi sonucu incelendiğinde ideal histogram değerinin 8 bulunduğu görülür.

4.7.2. Şifreleme kalite analizi

Bir görüntü şifreleme algoritmasının kalitesi, düz metin görüntülerinin piksel değerleri ve ilgili şifreleri karşılaştırılarak çeşitli ölçümler kullanılarak analiz edilir. Düz metin görüntüler ve ilgili şifreler arasında piksel değerlerinde yüksek bir değişiklik olduğunda şifreleme algoritmasının iyi kalitede olduğu kabul edilir. Görüntü şifreleme araştırmacıları, şifreleme kalitesini ölçmek için MSE, MAE, PSNR gibi bir dizi ölçüm kullanır. Bu ölçümlerin her biri aşağıda daha ayrıntılı olarak verilmiştir.

4.7.2.1. MSE analizi

Kalite değerlendirme ölçümlerinden biridir. Düz görüntü ile şifreli görüntü arasındaki piksel değerlerinin ortalama kare farkını hesaplar (Qayyum et al., 2020). Daha düşük bir MSE değeri, düz metin görüntüsü ile şifresi arasında daha büyük bir benzerliği belirtirken, daha yüksek bir MSE değeri, düz metin görüntüsü ile şifresi arasında daha düşük bir benzerlik anlamına gelir. Bu nedenle daha yüksek bir MSE değeri, daha yüksek kaliteli

şifreleme anlamına gelir. Düz metin görüntüsü ile şifreli görüntüsü arasındaki MSE denklem 4.23'teki denklemle hesaplanabilir.

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} [P(i,j) - C(i,j)]^2 \quad (4.23)$$

MSE'nin minimum değerini hesaplamak için başlangıçtaki görüntü ile şifreli görüntünün aynı olduğu durumu hesaplarsak piksel değerleri farkı 0 olacağından MSE değeri 0 olacaktır. MSE'nin maksimum değeri ise iki görüntü piksellerinin birbirinden tamamen farklı olduğu durumdur yani piksel değerleri farkı 255'tir. Maksimum MSE hesaplanması denklem 4.24'te verilmiştir.

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} [255 - 0]^2 \quad (4.24)$$

$$MSE = \frac{1}{H \times W} \times H \times W \times [255]^2$$

$$MSE = 65.025$$

4.7.2.2.MAE analizi

MAE, bir görüntü şifreleme algoritmasının kalitesini değerlendirmek için kullanılan başka bir istatistiksel ölçümdür. Düz metin görüntüsünün piksel değerleri ile şifreli görüntüsü arasındaki ortalama mutlak farkı ölçer (Fan et al., 2023). Daha düşük bir MAE değeri, düz metin görüntüsü ile şifresi arasında daha büyük bir benzerliğe işaret ederken, daha yüksek bir MAE değeri, düz metin görüntüsü ile onun şifresi arasında daha düşük bir benzerliğe işaret eder; bu nedenle daha yüksek bir MAE değeri, daha yüksek kalitede şifreleme anlamına gelir. MAE denklem 4.25 kullanılarak hesaplanabilir.

$$AE = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} |P(i,j) - C(i,j)| \quad (4.25)$$

MAE'nin minimum değeri için iki görüntünün aynı olduğunu varsayarsak P(i, j) − C(i, j) 0 olacaktır. Dolayısıyla MAE minimum değeri 0'dır. Maksimum değer için iki görüntünün birbirinden tamamen farklı olduğunu varsayılırsa (biri 255 piksel değerinde, diğeri 0 piksel değerinde), mümkün olan maksimum MAE denklem 4.26 ve 4.27 bulunark hesaplanır.

$$MAE = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} |255 - 0)| \quad (4.26)$$

$$\frac{1}{H \times W} \times H \times W \times 255 \quad (4.27)$$

Maksimum MAE değerinin de 255 olduğu matematiksel olarak elde edilmiştir.

4.7.2.3.PSNR analizi

Görüntü şifrelemede, PSNR metriği düz metin görüntüsü ile şifreli görüntüsü arasındaki gürültü oranını ölçmek için kullanılır (Qayyum et al., 2020). 0'lık bir PSNR değeri, test edilen görüntünün rastgele gürültüye eşdeğer olduğunu gösterir ve daha yüksek bir değer, düz metin görüntüsüne daha yakın olan daha yüksek kaliteli bir görüntü anlamına gelir. Bir şifreleme algoritması tarafından üretilen şifre görüntülerinin PSNR değeri ne denli düşük olursa, şifrelemenin kalitesi de o denli iyi olur. PSNR denklem 4.28 kullanılarak hesaplanabilir.

$$PSNR = 10\ log_{10} \frac{MAX_p}{MSE} \quad (4.28)$$

Burada MAXp, bir pikselin sahip olabileceği maksimum değerdir, MSE ise ortalama kare hatasıdır.

4.7.3. Gürültü ve veri kaybı analizi

İletişim ağları üzerinden iletilen dijital görüntüler genellikle gürültüden ve veri kaybından etkilenir ve bu da şifreli görüntüleri şifrelenemez hale getirebilir. Bu tür bozulmalar, şifreli görüntüleri bozmayı amaçlayan saldırganlar tarafından da oluşturulabilir. Bu saldırılara gürültü ve tıkanma saldırıları adı verilmektedir (Bakker et al., 2003) Bir görüntü şifreleme algoritmasının güvenilirliğini sağlamak için, bu tür saldırılara dayanma ve düz metin görüntüsünün değiştirilmiş şifre görüntüsünden şifresini çözme yeteneğinin test edilmesi gerekir (Shafique et al., 2021). Bir şifreleme algoritmasının gürültü saldırılarına karşı dayanıklılığını değerlendirmek için araştırmacılar, şifre görüntüsüne değişken yoğunluklarda gürültü katılır ve etkilenen şifre görüntülerinin şifresini çözmeye çalışır. Tıkanma saldırılarına karşı direnç sağlamak için araştırmacılar, şifreleme algoritmasının, değişen şiddet derecelerinde kırpılmış bölümlere sahip bir şifre görüntüsünün şifresini çözme yeteneğini değerlendiriyor. Ayrıca, ileriki bölümlerde bahsedilecek olan PSNR metriği, şifresi çözülmüş bozuk görüntünün PSNR'sini düz metin görüntüsüyle karşılaştırarak, bozuk bir görüntünün şifresini çözerken şifreleme algoritmalarının kalitesini

ölçmek için kullanılabilir (J. Zhou et al., 2020). Orijinal düz metin görüntüsüyle karşılaştırıldığında şifresi çözülmüş görüntünün daha yüksek bir PSNR'si, şifresi çözülmüş bozuk görüntünün orijinal düz metin görüntüsüne daha yakın olduğunu gösterir.

4.7.4. Diferansiyel analizler

4.7.4.1. Katı Çığ Etkisi analizi

Görüntü şifrelemede çığ etkisi, anahtarda veya görüntü verisinde yapılan küçük bir değişikliğin, önemli ölçüde farklı bir şifreli görüntü üretmesine neden olduğu durumlarda meydana gelen olguyu ifade eder. Bir şifreleme algoritması, düz görüntüdeki veya anahtarındaki bir piksel değişikliği, şifreli görüntüdeki piksellerin %50'sinden fazlasının değişmesine neden olduğunda, diferansiyel saldırılara karşı güvenli kabul edilir (Himthani et al., 2022). Çığ etkisi, bir düz görüntünün ve yalnızca bir piksel değiştirilmiş aynı düz görüntünün şifrelenmesiyle üretilen iki şifreli görüntü arasındaki ortalama kare farkını hesaplamak için MSE metriği kullanılarak analiz edilebilir. Çığ etkisi MSE (MSEav) denklem 4.29 ile hesaplanır.

$$MSE_{av} = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} [C_1(i,j) - C_2(i,j)]^2 \tag{4.29}$$

4.7.4.2. NPCR analizi

NPCR metriği, yalnızca bir pikseli farklı olan iki düz görüntünün şifrelenmesiyle üretilen iki şifreli görüntü arasındaki farkların yüzdesini ölçer; diğer tüm pikseller iki düz görüntüde aynı olur (Yu et al., 2023). Daha yüksek bir NPCR değeri, algoritmanın düz görüntüdeki veya anahtarındaki değişikliklere karşı daha fazla yanıt verdiğini ve dolayısıyla diferansiyel saldırılara karşı daha iyi direnç gösterdiğini bildirir. Başka bir deyişle, iyi bir şifreleme algoritmasının bu tür saldırılara karşı koyabilmesi için anahtardaki veya düz görüntüdeki küçük değişikliklere karşı son derece duyarlı olması gerekir. İdeal NPCR değerinin ≥%99,6094 olduğunu hesaplamıştır. NPCR değeri denklem 4.30 ile hesaplanır.

$$NPCR = \sum_{i=1}^{H} \sum_{j=1}^{W} \frac{D(i,j)}{H \times W} \times 100\% \tag{4.30}$$

$$\text{öyleki: } D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases}$$

Denklem 4.30'da $D(i,j),(i,j)$ konumundaki C1 ve C2 arasındaki farklı piksellerin sayısının toplamıdır. (i,j) konumundaki C1 ve C2 piksel değerleri farklı olduğunda $D(i,j)$, 1 değerine sahiptir; aksi durumda 0 değerine sahiptir.

4.7.4.3. UACI analizi

UACI, aynı olan ancak yalnızca bir piksel açısından farklı olan iki düz görüntünün şifrelenmesiyle üretilen iki şifreli görüntü arasındaki ortalama değişim yoğunluğunu ölçer. Bir şifreleme algoritmasının diferansiyel saldırılara direnme yeteneğini değerlendirmek için kullanılan bir ölçümdür (Yu et al., 2023). NPCR'ye benzer şekilde, daha yüksek bir UACI değeri, farklı saldırılara karşı daha iyi bir direnç gösterir. UACI için ideal değer, UACI değeri≥ %33,4635 'dir (Y. Wu et al., 2014). UACI hesaplanması denklem 4.31'de verilmiştir.

$$UACI = \frac{1}{H \times W}\left[\frac{\sum_{i=1}^{H}\sum_{j=1}^{W}|C_1(i,j)-C_2(i,j)|}{255}\right] \times 100\% \quad (4.31)$$

4.7.5. Anahtar alan ve anahtar duyarlılık analizi

Anahtar alanı, bir şifreleme algoritmasının kullanabileceği tüm olası anahtarların kümesini temsil eder. Kaba kuvvet saldırılarına karşı daha güçlü bir güvenlik düzeyi sağlamak için bir görüntü şifreleme algoritmasının anahtar alanı değeri 2^{100}'den büyük olmalıdır (Y. Wu et al., 2014). Anahtar duyarlılığı analizi, görüntü şifreleme algoritmasının anahtardaki küçük değişikliklere karşı duyarlılığını değerlendirir. Sağlam ve güvenli bir algoritma, yalnızca bir bit farklı iki anahtarla şifrelendiğinde tamamen farklı iki şifreli görüntü üretmelidir. Ayrıca, bir şifreli görüntünün şifresini çözememeli ve bir biti değiştirilmiş bir anahtarla görüntü elde edilememelidir (Himthani et al., 2022). Bir şifreleme algoritmasının şifrelemeye yönelik anahtar hassasiyetini değerlendirmek için araştırmacılar, düz görüntünün yalnızca bir bitte farklılık gösteren iki anahtarla (k1 ve k2) şifreler ve elde edilen şifre görüntülerini karşılaştırır. Şifre çözme için anahtar duyarlılığının değerlendirilmesi durumunda, yalnızca bir bitte farklılık gösteren k2 anahtarını kullanarak k1 anahtarıyla şifrelenmiş bir görüntünün şifresini çözmeye çalışır. Algoritma anahtardaki değişikliklere duyarlıysa, değiştirilen anahtarla şifreli görüntünün şifresi çözülememelidir.

4.7.6. Görüntü şifreleme değerlendirme metrikleri optimum değerleri

Yapılan görüntü şifreleme işleminin güvenlik kriterleri açısından uygunluğunun belirlenmesi için gerekli ve öncelikli kriterlere bu bölümde değinilmiştir. Bu tez çalışmasında göz önünde bulundurulan görüntü şifreleme performans kriterlerinin optimum değerleri Çizelge 4.2.'de verilmiştir.

Çizelge 4.2: Görüntü şifrelemede kullanılan önemli metrikler ve optimum değerleri

No	Metrikler	Tercih edilen değerler
1	Histogram	Tek düze (uniform) dağılım göstermesi
2	Korelasyon katsayısı	Sıfıra yakın
3	Entropi	8 (8 bit kodlamalı görüntü için)
4	Anahtar alan	$>2^{100}$
5	Çığ etkisi	>50% (bitlerin %50 si)
6	NPCR	99.609%
7	UACI	33.464%
8	PSNR	Düşük olması şifreleme kalitesini arttırır
9	Hesaplama süresi	Minimum (tercih edilen).

5. UYGULAMA

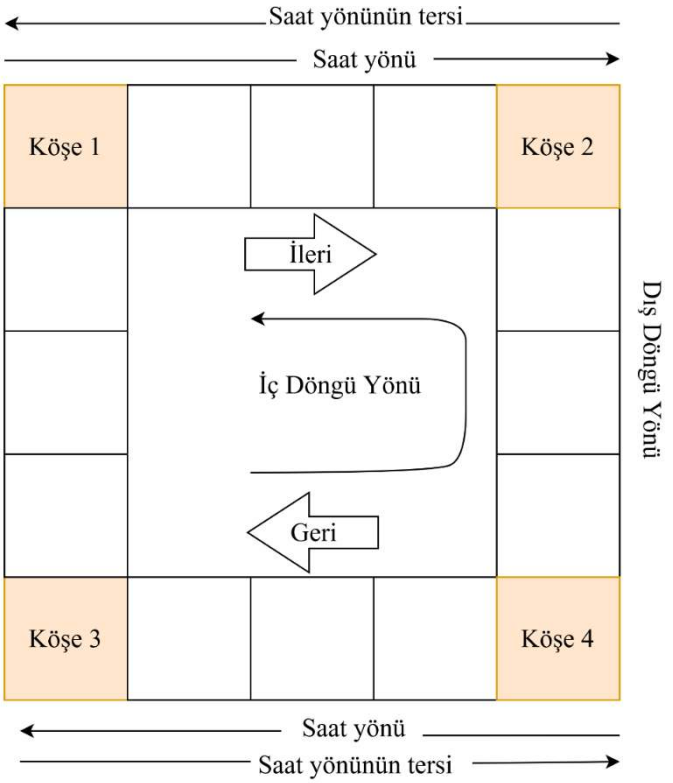
Bu tez çalışmasında IoT sistemlerde görüntü şifreleme uygulamalarına katkı sağlamak amacı ile iki farklı görüntü şifreleme algoritması yaklaşımı önerilmiştir. Birinci yaklaşımda kaos temelli piksel karıştırma işlemi ile geliştirilen bir algoritma, ikinci yaklaşımda ise literatürde genellikle tek aşamada uygulanan matris haritalama yaklaşımlarına doğrusal olmama özelliğini arttıran değişken adımlı kaotik haritalama algoritması önerilmiştir. Bu bölümde bu önerilen algoritmalar detaylandırılacaktır. Algoritmalar sunulurken çalışma detayları, görüntü şifreleme sonuçları ve metrik değerlendirmeleri verilecektir. Aynı zamanda literatürde yer alan benzer algoritmalar ile kıyaslama sonuçları da sunulacaktır. Ek bir adım olarak serileştirme algoritmalarının kullanımının ve doğrusal olmayan matris haritalama yöntemlerinin kıyaslaması incelenmiş olacaktır.

5.1. Köşe Geçiş Algoritması

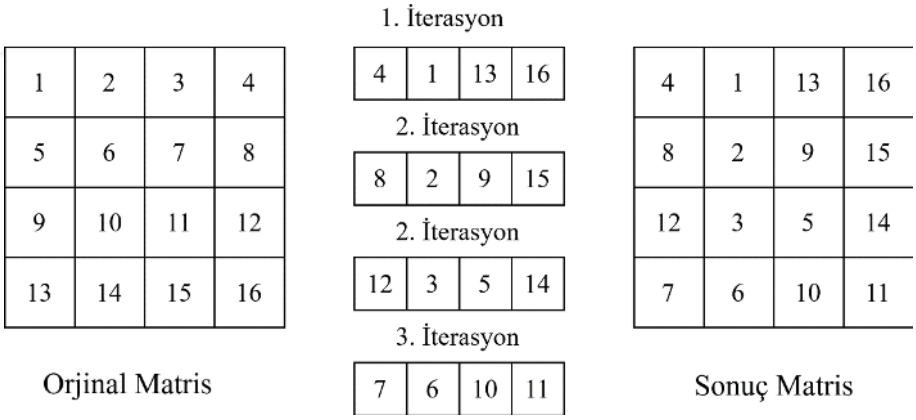
Köşe geçiş algoritması (KGA), temel olarak deterministik bir piksel karıştırma algoritmasıdır. Diğer deterministik piksel karıştırma algoritmaları gibi iki boyutlu görüntüyü farklı gezintiler ile renk düzlemlerine göre serileştirir, daha sonra karışık olarak tek boyuta indirgenmiş bu seri diziyi ilk boyutlarına göre tekrar matrise dönüştürür.

5.1.1. Algoritma adımları

Önerilen KGA'nın temel çalışma prensibi Şekil 5.1'de sunulmuştur. Algoritmanın görüntünün kendisi dışında üç giriş parametresi vardır: başlangıç köşesi, dönüş yönü ve ilerleme yönü. KGA algoritması iki boyutlu verinin en dış katmanını verilen giriş parametrelerine göre serileştirir. Daha sonra bir iç katmana geçer ve devam eder. Şekil 5.2'te başlangıç köşesi 2, dönüş yönü saat yönünün tersine ve ilerleme yönü geri yönde olan sembolik bir görüntünün piksel değerlerinin KGA ile nasıl değiştirildiği gösterilmiştir. Bu algoritmanın temel avantajı, her yinelemede mümkün olan en uzak pikselleri seçerek pikseller arasındaki korelasyonu alternatiflerinden daha iyi azaltmasıdır. Sonuç olarak pikselleraras korelasyon koparılarak düzenli dağılım sağlanmıştır.



Şekil 5.1: Köşe geçiş algoritması parametreleri.



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

4	1	13	16

8	2	9	15

12	3	5	14

7	6	10	11

4	1	13	16
8	2	9	15
12	3	5	14
7	6	10	11

Şekil 5.2: KGA ‘nın hesaplanma örneği , (başlangıç parametreleri başlangıç köşesi:2, yönü: saat yönünün tersine dönüş ve geriye doğru ilerleme).

5.1.2. Şifreleme Şemasının Uygulanması

Önerilen şifreleme algoritma adımları Algoritma 1’de sunulmuştur. Görüntü şifreleme iki temel adımdan oluşur: karıştırma ve dağıtma. Öncelikle piksel konumlarını değiştirmek için bu çalışmada önerilmiş olan KGA’yı kullanılmıştır. Önerilen şifreleme algoritması IoT sistemlerinde kullanılmak üzere tasarlandığı için yüksek boyutlu kaotik haritalar yerine bir

boyutlu logistik harita kullanılmıştır. Bu harita, dağıtım ve anahtar oluşturma aşamalarında kullanılır. Önerilen simetrik şifreleme algoritması temel olarak üç adımdan oluşur.

1. Lojistik harita tabanlı iki boyutlu haritalama
2. Kaotik Xoring
3. KGA uygulaması

KGA'nın şifreleme aşamaları algoritma1'de verilmiştir. Ayrıca, algoritmayı daha iyi açıklayabilmek için tüm adımların sembolik sayısal bir matris üzerinde yürütülmesi Şekil 5.4'te gösterilmiştir. Şekil 5.3'te X*Y, matris bu dizilerin nokta çarpımıdır. Önerilen şifreleme şemasında, şifrelenecek görüntünün boyutu MxN olarak kabul edilirse Algoritma 1'de görülebileceği gibi, M ve N boyutunda iki rastgele dizi oluşturmak için lojistik harita kullanılır. Bu matrisler iki işlemde kullanılır: biri piksel permütasyonu, ikincisi ise difüzyon aşaması içindir. Bu şekilde lojistik harita kullanılarak oluşturulan X[1,3,0,2] ve Y[3,0,2,1] dizileri Şekil 5.3'te görülmektedir. Ayrıca piksellerin yayılımını arttırmak için görüntü piksellerinin ortalaması lojistik haritanın başlangıç parametrelerine eklenmiştir.

Algoritma 1. Önerilen görüntü şifreleme algoritması

Giriş:

image: Şifrelenecek görüntü MxN boyutunda görüntü.

KEY: KGA ve Lojistik Haritanın parametrelerini tanımlamak için şifreleme şeması anahtarı

Çıkış:

eImage: Şifreli görüntü

procedure encryption (image, KEY):

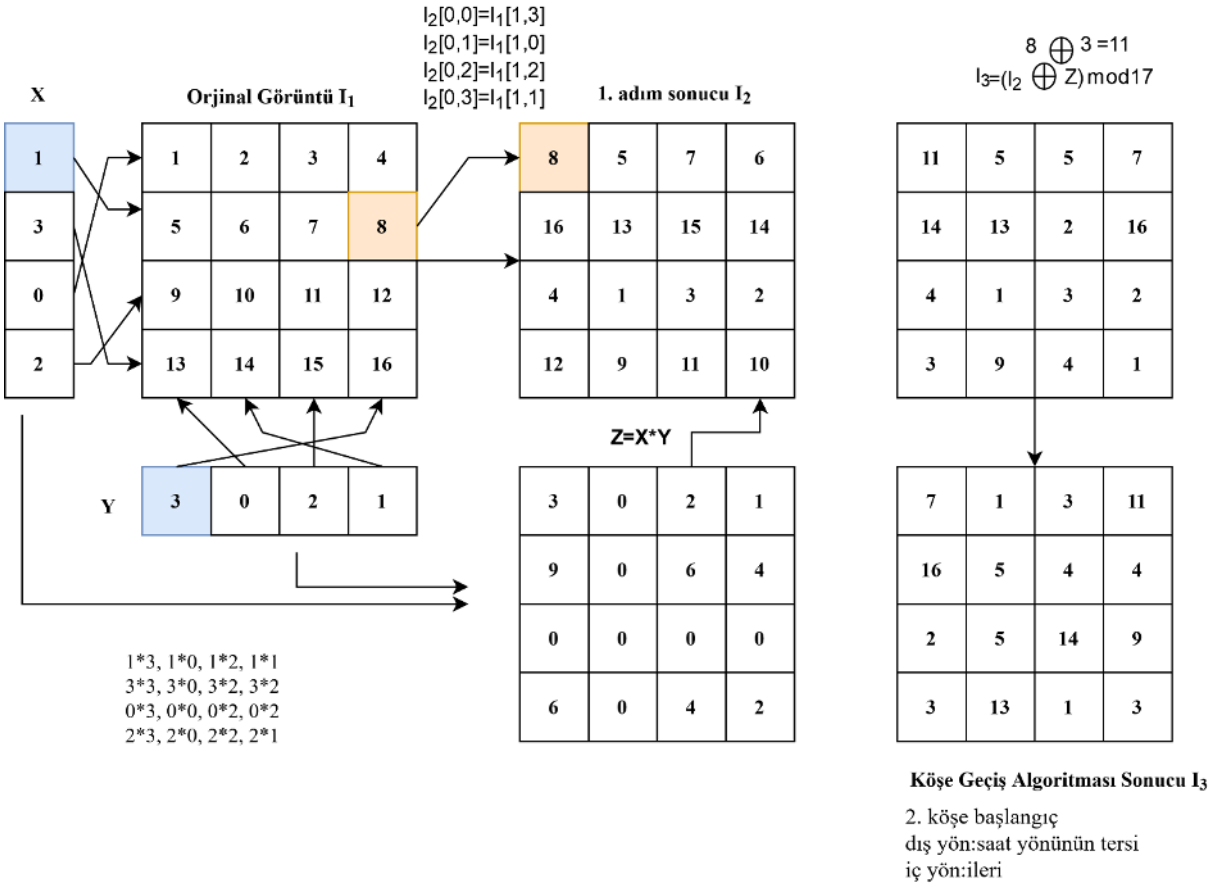
M: görüntünün yüksekliği

N: görüntünün genişliği

$eImage[M][N]$: şifreli çıkış görüntüsü

$i = 0, j = 0$: döngü parametreleri

1. Generate $X[M]$ //satır dizisi, Lojistik Harita ile oluşturulan
2. Generate $Y[N]$ //sütun dizisi, Lojistik Harita ile oluşturulan
3. $while\ i < M$
4. $\quad while\ j < N$
5. $\quad\quad eImage[i][j] = image[X[i]][Y[j]]$
6. $\quad\quad eImage[i][j] = eImage[i][j] \oplus (X[i] * Y[i])\ mod\ 256$
7. $eImage = Cornering(eImage)$
8. $return\ eImage$



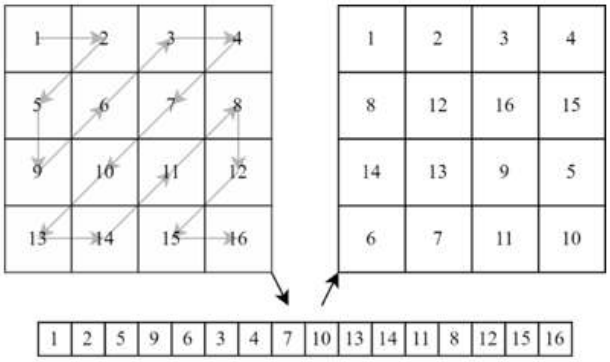
Şekil 5.3: Şifreleme işleminin örnek matris üzerinde gösterimi.

KGA 'nın tüm aşamalar için uygulanması şeması Şekil 5.4'te verilmiştir. Burada P: Plain image, K:key, E: encrypted image temsil etmektedir.

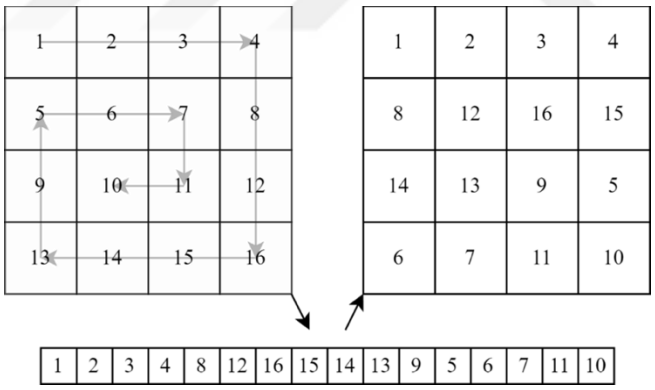
Şekil 5.4: Düz görüntüden şifreli görüntü elde edilmesi (E), şifreli görüntüden düz görüntü elde edilmesi (P).

5.1.3. Serileştirme Algoritmaları

Serileştirme algoritmaları temel olarak 2 boyutlu MxN renkli veya gri tonlamalı bir görüntüye tersinir bir geçiş işleminin uygulanmasını, elde edilen yolun bir diziye dönüştürülmesini ve son olarak bu diziden orijinal görüntü boyutunun yeniden oluşturulmasını içerir. Literatürdeki en popüler serileştirme algoritmaları ZigZag (Xingyuan Wang & Chen, 2021; Buyukcolak, 2019) ve Spiral (Farrukh et al., 2023; İnce et al., 2024) vb. dönüşüm algoritmalarıdır. Standart ZigZag ve spiral dönüşümler sırasıyla Şekil 5.5 ve 5.6'da sunulmuştur.



Şekil 5.5: Standart Zigzag Algoritması.

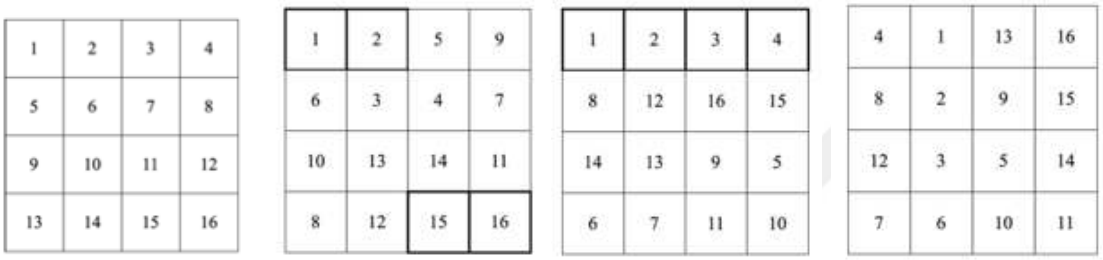


Şekil 5.6: Standart Spiral Algoritması.

Standart zizgzag algoritması ile spiral algoritmaları incelendiğinde ortak dezavantajları, değişmeyen piksel değerleri sayısının fazla olmasıdır. Serileştirme algoritmalarına alternatif olarak köşe geçiş algoritması geliştirilmiştir ve bölüm 5.1.4'te sunulmuştur.

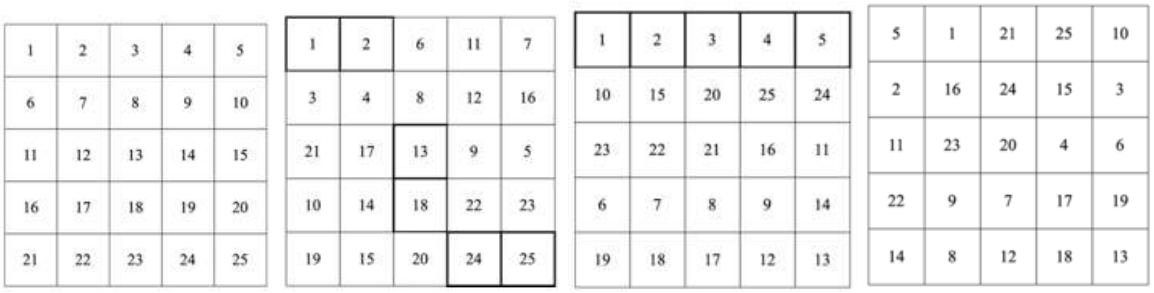
5.1.4. KGA, Zigzag ve Spiral Algoritmalarının Kıyaslanması

Şekil 5.7'de üç serileştirme algoritması görsel olarak karşılaştırmıştır. Kalın kenarlıklar, ortaya çıkan görüntüdeki değişmeyen piksel değerlerini temsil eder. Şekil 5.8'de gösterildiği gibi, hem Spiral hem de ZigZag algoritmaları değişmeyen piksel değerleri sergiler. Ancak Spiral algoritması, özellikle I[0,0] noktasından başlayarak orijinal MxN görüntünün genişliği boyunca değişmeyen piksel değerleri ile sonuçlandığından, karşılaştırmaya I[0,N] noktasından başlayan spiral algoritması da kıyaslama tablosuna Çizelge 5.1'de spiral 2 olarak eklenmiştir. Değişmeyen piksel sayıları Çizelge 5.1'de verilmiştir.



Orijinal matris | Zigzag sonrası | Spiral sonrası | KGA sonrası

Şekil 5.7: 4*4 matis örneği için zigzag, spiral ve KGA uygulanması sonucu elde edilen yeni matrisler.



Orijinal matris | Zigzag sonrası | Spiral sonrası | KGA sonrası

Şekil 5.8: 5*5 matris örneği için zigzag, spiral ve KGA uygulanması sonucu elde edilen yeni matrisler.

Çizelge 5.1: Zigzag, spiraller ve KGA için değişmeyen piksel sayıları

Test edilen görüntü	Değişmeyen piksel sayısı			
	ZigZag	**Spiral 1**	**Spiral 2**	**KGA**
Baboon (Gri)	8	512	1	1
Barbara (Gri)	12645	12730	12451	12032
Boat (Gri)	5011	4816	4324	4194
Lenna (Renkli)	10	514	5	4
Peppers (Renkli)	22	523	9	11
Grapes (Renkli)	111	574	61	65

Çizelge5.1'de sunulan sonuçlara göre KGA diğer iki algoritmadan daha üstün görünse de, böyle bir karşılaştırma bile görüntülere uygulandığında yanıltıcı olabilir. Çünkü aynı değerdeki iki piksel yer değiştirse bile bu senaryo değişmeden değerlendirilecektir. Bu sınırlamayı gidermek için algoritmalar arasındaki gerçek farkları ortaya çıkarmak amacıyla sayısal bir karşılaştırma yapılmıştır. Bu değerlendirmede çeşitli boyutlardaki matrisler, matris boyutlarını temsil eden 1'den başlayıp MxN'ye kadar art arda artan tamsayı değerlerle doldurulur. Bu, tüm nominal piksel değerlerinin farklı olmasını sağlar. Bu sayısal karşılaştırmanın sonuçları Çizelge 5.2 'de sunulmuştur.

Çizelge 5.2: Fakrklı boyutlu matrisler için değişmeyen piksel sayıları

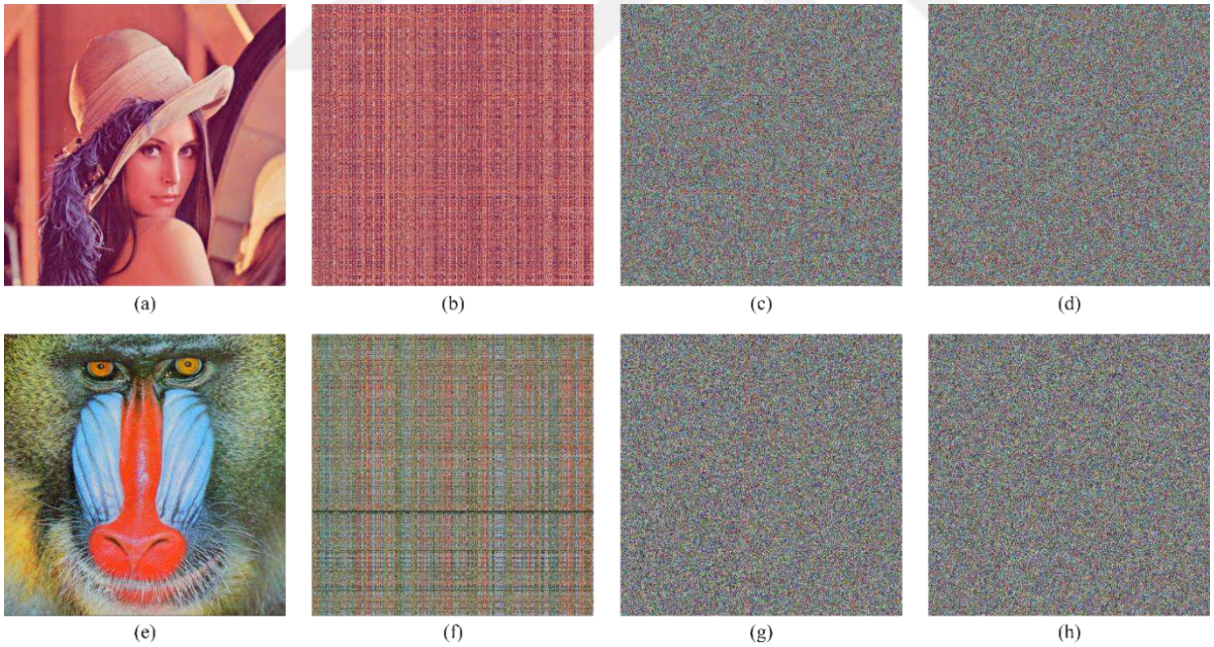
Matris Boyutu	**Değişmeyen Hücre Sayısı**			
	ZigZag	**Spiral**	**Spiral 2**	**KGA**
16x16	4	17	1	1
32x32	8	32	1	2
64x64	4	65	1	1
128x128	4	128	2	1
256x256	4	257	2	1
512x512	8	512	1	1
1024x1024	6	1026	3	3
2048x2048	10	2048	1	1

Görüntü boyutu büyük olduğunda da KGA algoritmasının pikselleri değiştirme oranı olarak zigzag ve spiralden çok daha başarılı olduğu görülmüştür.

5.1.5. KGA Uygulaması

Önerilen şifreleme şemasının uygulama adımları sırasıyla açıklanacaktır. Yapılan uygulama çalışmaları sonuçları işlemcisi i9 9980HK@ 2.4 Ghz işlemci ve 32 GB RAM özellikleri olan bir laptopta, IoT uygulamaları da PI 4 Model B ARM V8@ 1.8 Ghz (4 GB) özellikli donanımlar kullanılmıştır. Uygulama program kodları java ortamı kullanılarak geliştirilmiştir. Metrik değerlerin hesaplanması ve görselleştirilmesi için Matlab R2019b versiyonu kullanılmıştır. Kaotik harita olarak lojistik harita ile üretilen kaotik dizilere KGA uygulanarak görüntü şifreleme işlemi tamamlanmıştır.

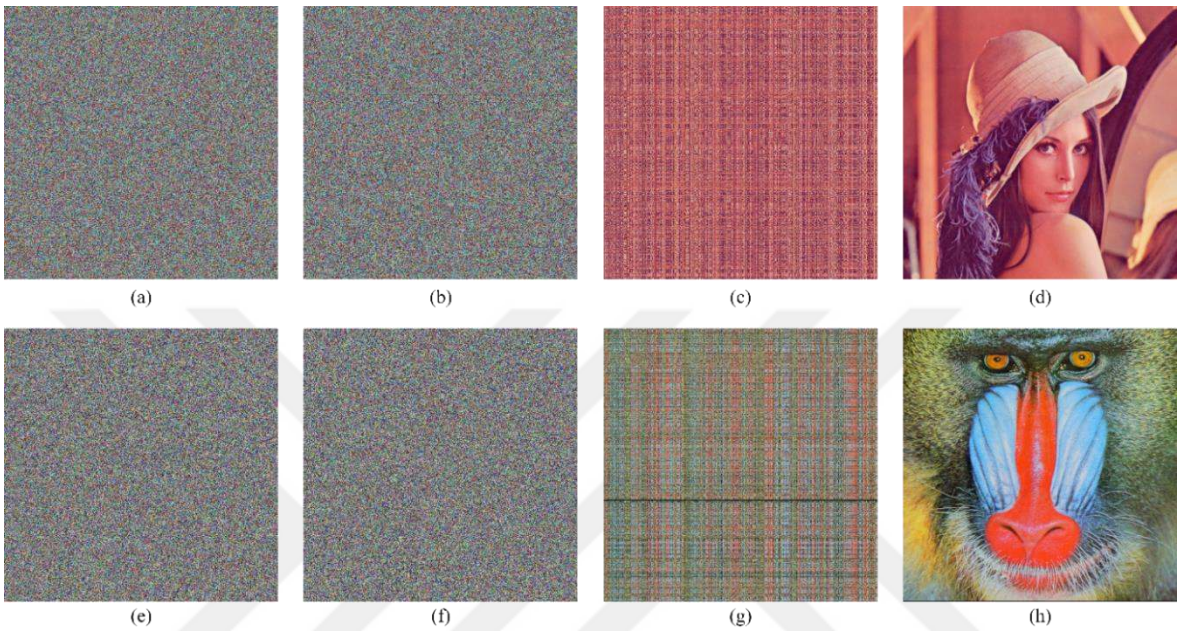
Şifrelemenin tüm adımları Şekil 5.9 'da gösterilmektedir. Şifreleme işlemi sırasında yapılan işlemler değerlendirildiğinde işlem sırasının önemli olmadığı görülecektir. Çünkü temelde tüm adımlar anahtar güvenliğine bağlı olan deterministik süreçlerdir. Kriptografinin Kerckhoff prensibine göre anahtar, şifreleme işleminin güvenliğidir. Çünkü anahtar dışında algoritmanın bütün detayları bilinse bile kırılamaz olması gerekir. Ancak şifreleme ve şifre çözme işlemlerinde bu işlem sırası tersine olacağından şifre çözmenin doğru yapılması önemlidir. Hatta güvenliği artırmak için bu işlemlerin sırası farklı bir anahtar alanı olarak eklenebilir.



Şekil 5.9 (a) Orijinal Lena görüntüsü, (b) Lena'nın 2D kaotik haritalama sonucu , (c) Lena görüntüsünün chaotic XORlama sonucu, (d) Köşe geçiş algoritması uygulanması sonrası Lena görüntüsü, (e) Orijinal Baboon görüntüsü, (f) Baboon'un 2D kaotik haritalama sonucu, (g) Baboon'un kaotik XORlama sonucu, (h) Köşe geçiş algoritması sonucu Baboon'un şifreli görüntüsü

5.1.6. Görüntü Deşifreleme Uygulamaları

Şifre Çözme adımları, şifreleme adımları tersten çalıştırılarak gerçekleştirilir. İlk adım ters KGA, ikinci adım kaotik XORing, üçüncü adım ise kaotik 2 boyutlu haritalamadır. Şekil 5.10'da sunulan şifrelenmiş görüntülerin şifre çözme adımları verilmiştir. Bu şekilde tüm şifre çözme adımlarının ara sonuçları sunulmaktadır.



Şekil 5.10: (a) Şifrelenmiş Lena görüntüsü (b) Şifrelenmiş Lenna'nın Ters Köşelenme sonucu (c) Önceki sonucun Kaotik XORing sonucu (d) Ters 2D haritalama ve ortaya çıkan orijinal Lenna görüntüsü (e) Şifreli Babun görüntüsü (f) Şifrelenmiş Babun'un Ters Köşelenme sonucu (g) Kaotik XORing sonucu önceki sonuç (h) Ters 2 boyutlu haritalama ve elde edilen orijinal Babun görüntüsü

5.1.7. Performans Analizleri

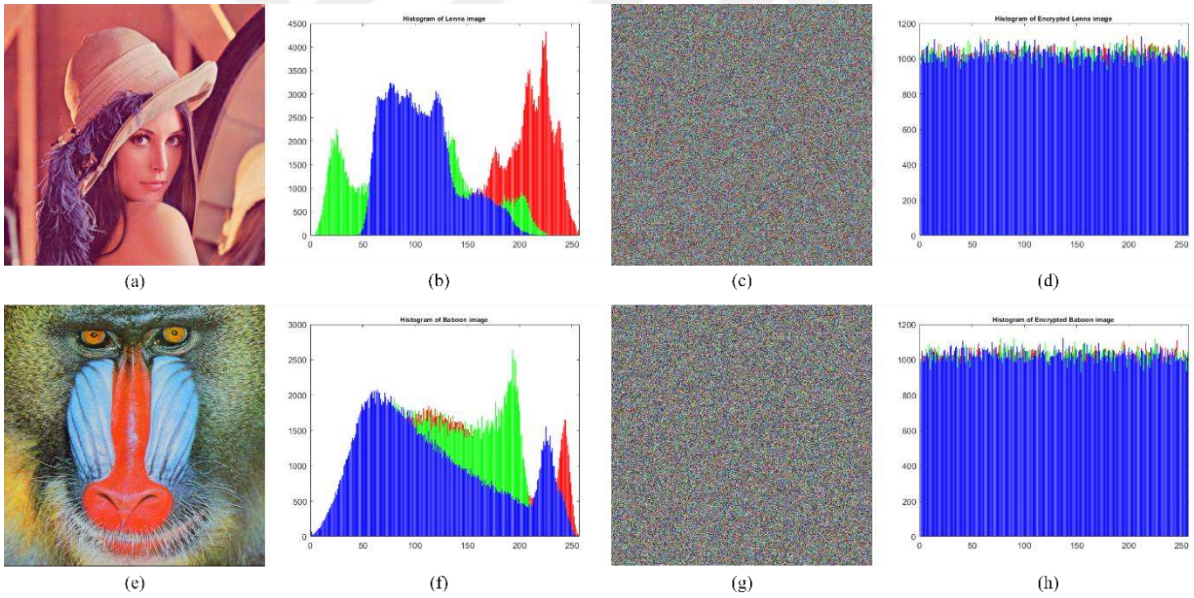
5.1.7.1. Anahtar alan analizi sonuçları

Anahtar alanı, kriptosistemde kullanılabilecek farklı gizli anahtarların toplam sayısıdır. İyi bir şifreleme şemasının kaba kuvvet saldırısına direnmek için geniş bir anahtar alanına sahip olması gerekir. Önerilen şifreleme şemasında 9 farklı anahtar alanı bulunmaktadır. Bunlardan yedisi 2^{64} hassasiyetine göre kayan noktalardır. Ayrıca, iki ikili sonuçtaki sayı da dâhil edilmiştir. Sonuç olarak, tahmini anahtar alanı yaklaşık 2^{450}'dir. Bu anahtar uzay çok boyutlu kaotik sistemlerle veya kesirli dereceli sistemler yardımıyla daha

da artırılabilir. Ancak bu çalışmanın amacı kapsamında Köşe Geçiş Algoritmasının kabul edilebilir hafif bir şifreleme şemasıyla sunulması istenmektedir.

5.1.7.2. Histogram analizi sonuçları

Histogram, bir görüntünün veya dijital sinyalin piksel değerlerinin dağılımını gösterir. Şekil 5.11'de şifreleme işleminin histogram analizini göstermektedir. Metin, video, resim gibi her türlü veride belirli bilgiler diğerlerinden daha fazla tekrarlanır. Örneğin herhangi bir dilin sözlüğü incelendiğinde bazı karakterlerin frekansının diğerlerine göre daha yüksek olduğu görülecektir. Güçlü bir şifreleme algoritması, diğer şeylerin yanı sıra bu bilgiyi de gizleyebilmelidir. Görüntü verileri söz konusu olduğunda histogram, görüntüde her bir farklı renk kodunun kaç kez kullanıldığıdır. Doğal olarak şifrelenmiş görüntüde orijinal görüntüdeki renk frekanslarının bozulması ve tüm piksel değerlerinin normal dağılıma sahip olması beklenir. Şekil 5.11 incelendiğinde önerilen algoritma orijinal görüntünün histogramını başarılı bir şekilde normalleştirmektedir.



Şekil 5.11: Orijinal ve şifrelenmiş test görüntülerinin histogramı (a) Lenna görüntüsü (b) Lenna görüntüsünün histogramı (c) Lenna'nın şifrelenmiş görüntüsü (d) Şifrelenmiş Lenna görüntüsünün histogramı (e) Baboon görüntüsü (f) Baboon görüntüsünün histogramı (g) Baboon'un şifrelenmiş görüntüsü (h) Baboon'un histogramı şifrelenmiş Babun görüntüsü

5.1.7.3. MSE analizi sonuçları

MSE, istatistikte hata olarak adlandırılan, olası tahmin değeri ile gerçek değer arasındaki farkın karelerinin toplamıdır. Görüntü şifrelemede, orijinal görüntü ile şifrelenmiş görüntünün ortak piksel değerlerinin farkının karesi olarak kullanılır. MSE belirli bir değerin üzerindeyse orijinal görüntü ile şifrelenmiş görüntü arasındaki mesafeyi belirtir. Sonuç olarak MSE değerinin istatistiklerde düşük olması hedeflenirken, görüntü şifrelemede yüksek olması hedeflenmektedir. Bu, anahtardaki veya orijinal görüntüdeki herhangi bir değişikliğin şifreli metinde yaratacağı farkı analiz edecektir. Önerilen KGA ile şifrelenmiş görüntülerden hesaplanan MSE değerleri Çizelge 5.3'te verilmiştir.

5.1.7.4. PSNR analizi sonuçları

PSNR, bir sinyalin en yüksek gücü ile temsilinin güvenilirliğini etkileyen rahatsız edici gürültünün gücü arasındaki orandır. Bu oran, gerçek göüntü ile şifrelenmiş görüntü arasındaki kalitenin ölçüsü olarak kullanılır. PSNR ne kadar yüksek olursa şifreleme şemasının kalitesi de o kadar yüksek olur. Önerilen KGA ile şifrelenmiş görüntülerden hesaplanan PSNR değerleri Çizelge 5.3'te verilmiştir

5.1.7.5. UACI analizi sonuçları

İki görüntü arasındaki yoğunluk farkı olarak ifade edilen UACI, şifreleme algoritmasının diferansiyel saldırılara karşı dayanıklılığını ifade eder. Daha yüksek bir UACI değeri, daha güçlü şifreleme anlamına gelir. Önerilen KGA ile şifrelenmiş görüntülerden hesaplanan UACI değerleri Çizelge 5.3'te verilmiştir**.**

5.1.7.6. NPCR analizi sonuçları

Şifrelenmiş görüntüdeki piksellerin varyans değeri olarak tanımlanır. Varyans, yani standart sapma, ortalamadan farkların karesinin ortalama ölçüsüdür. Bu bilgi, UACI gibi bir şifreleme sisteminin görüntü şifrelemede diferansiyel saldırılara karşı ne kadar güçlü olduğunu ifade eder. Yüksek bir NPCR değeri, güçlü bir şifreleme yöntemine işaret eder. Önerilen KGA ile şifrelenmiş görüntülerden hesaplanan NPCR değerleri Çizelge 5.3'te verilmiştir**.**

5.1.7.7. Entropi analizi sonuçları

Entropi, düzensizliğin veya rastgeleliğin ölçüsüdür. Önerilen KGA ile şifrelenmiş görüntülerden hesaplanan entropi değerleri Çizelge 5.3'de verilmiştir**.**

Çizelge 5.3: Bazı şifreli görüntülerin MSE değerleri

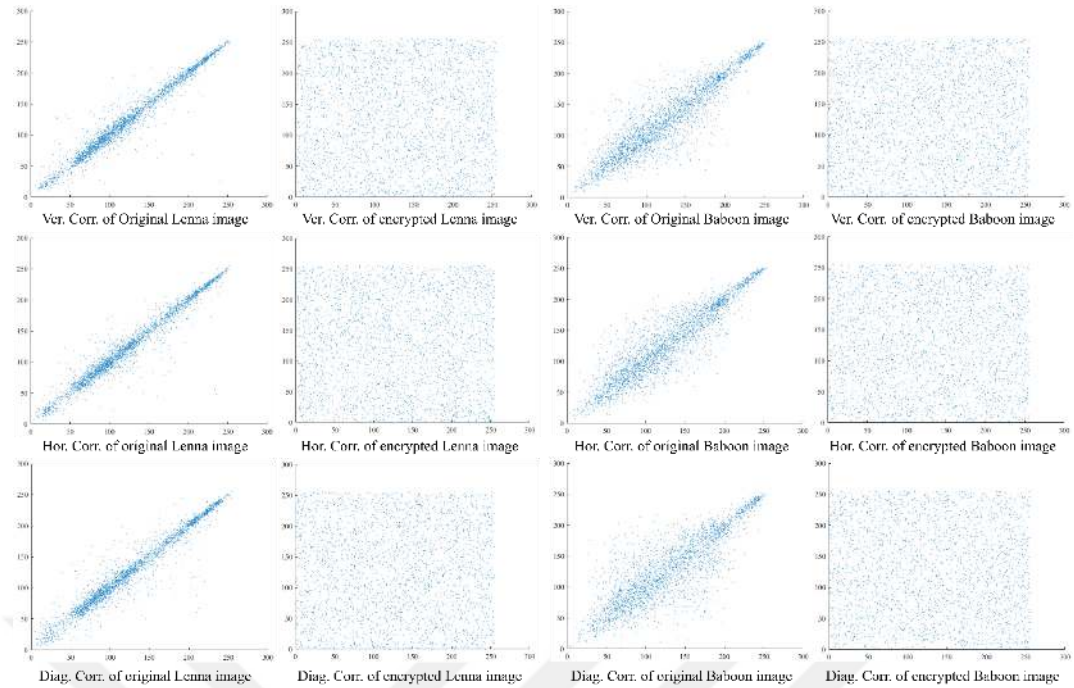
Görüntü Adı	MSE	PSNR	UACI	NPCR	Entropi
Lena	8602	8.6358	33.49	99.99	33.24
Baboon	8602	8.78	33.45	99.98	33.55
Cameraman	9273	8.45	33.46	99.63	8.0739
Peppers	14583	6.49	33.57	99.96	23.12

5.1.7.8. Korelasyon katsayısı analizi

Korelasyon, iki değişken arasındaki doğrusal korelasyonu analiz eder. Görüntü şifrelemede kullanım alanı, orijinal görüntü ile şifrelenmiş görüntü arasındaki ilişkinin gücünün hesaplanmasıdır. Standart görüntülerde piksel değerleri arasındaki korelasyon yüksektir. Görüntü şifrelemenin temel amacı, görüntü pikselleri arasındaki güçlü korelasyonu ortadan kaldırmaktır. Önerilen KGA ile şifrelenmiş görüntülerden hesaplanan yatay, dikey, çapraz korelasyon değerleri Çizelge 5.4'te verilmiştir

Çizelge 5.4: Bazı görüntülerin yatay, dikey, çapraz korelasyon değerleri

Görüntü	Yatay Korelasyon		Dikey Korelasyon		Çapraz Korelasyon	
	Düz Görüntü	Şifreli Görüntü	Düz Görüntü	Şifreli Görüntü	Düz Görüntü	Şifreli Görüntü
Lenna	0.9776	0.0142	0.9770	0.0197	0.9723	-0.0099
Baboon	0.8948	0.0120	0.9079	-0.0087	0.8329	-0.0260
Cameraman	0.9142	0.0030	0.9028	-0.0081	0.8915	0.0168
Peppers	0.9849	-0.0253	0.9853	0.0302	-0.0339	0.9731



Şekil 5.12: Lenna ve Baboon görüntülerinin dikey, yatay ve çapraz yönlerde korelasyonu

5.1.7.9. KGA'nın mevcut algoritmalarla performans kıyaslanması

Aşağıdaki tabloda bazı görüntü şifreleme yöntemeriyle mevcut çalışmada tanıtılan KGA'nın korelasyon katsayısı sonuçları kıyaslama tablosu Çizelge 5.5'de verilmiştir.

Çizelge 5.5: Önerilen yöntemle literatürdeki diğer çalışmaların korelasyon katsayısı kıyaslaması

Görüntü	**Yön**	**Önerilen Şema**	**(Mondal & Singh, 2022)**	**(Xingyuan Wang et al., 2019)**	**(Xingyuan Wang et al., 2016)**	**(Jiang et al., 2023)**	**(Xingyuan Wang & Guo, 2014)**
Lenna	Yatay	0.0142	0.10468	−0.001327	0.0113	0.00059	0.0152
	Dikey	0.0197	0.000029777	0.002319	−0.0013	0.00127	0.0145
	Çapraz	-0.0099	0.0014162	0.001843	0.0310	0.00109	0.0163
Baboon	Yatay	0.0120	0.012925	-	−0.00026	−0.00026	0.0063
	Dikey	-0.0087	0.0029121	-	0.00102	0.00102	0.0062
	Çapraz	-0.0260	0.00043698	-	0.00060	0.00060	0.0069
Cameraman	Yatay	0.0030	-	-	-	-	-
	Dikey	0.0302	-	-	-	-	-
	Çapraz	0.0168	-	-	-	-	-
Peppers	Yatay	0.0253	0.057748	−0.007583	−0.0044	−0.00081	0.0038
	Dikey	0.0302	0.0030312	0.004022	−0.0168	0.00122	0.0048
	Çapraz	0.9731	0.00079301	−0.005094	0.0198	0.00398	0.0044

Çizelge 5.5 incelendiğinde bazı hücrelerin boş olduğu görülmektedir. Literatürde ortak kullanılan görüntüler üzerinde verilen sonuçların kıyaslanması hedef alınmış, kıyaslama tabloları mevcut literatürde kullanılan örnek görüntüler üzerinden verilmeye çalışılmıştır. Ortak görüntüler üzerinde kıyaslama çizelge 5.5'deki gibi eksik değer içeren hücrelerle oluşturulabilmiştir.

5.1.7.10. KGA sonuçları

Bir şifreleme algoritmasının diferansiyel saldırılara karşı gücü, NPCR ve UACI değerlerine bakılarak anlaşılabilir (L. Xu et al., 2016). Diferansiyel analiz sonuçları UACI>%33,33 ve NPCR>%99,6 ise bu şifreleme algoritmasının genel olarak diferansiyel saldırılara karşı dayanıklı olduğu söylenebilir (Susanto et al., 2020). Önerilen yöntemin diferansiyel saldırılara karşı dayanıklılığı elde edilen NPCR ve UACI değerleriyle açıkça görülmektedir. Ayrıca entropi değeri mümkün olduğu kadar 8'e yakın olmalıdır (Setiadi et al., 2018). PSNR değerinin mümkün olduğu kadar düşük olması, daha iyi şifreleme anlamına gelir. Çizelge 5.6 incelendiğinde UACI ve NPCR değerlerinde ise önerilen yöntemlere göre daha başarılı sonuçlar elde edilmiştir. Entropi değeri ise ideal değere oldukça yakındır. Sadece PSNR değerinde karşılaştırılan yöntemlere göre biraz daha kötü sonuçlar verdiği görülmektedir.

Çizelge 5.6: Önerilen yöntemle bazı çalışmaların metrik değerleri kıyaslaması

Görüntü	Metrik	Önerilen Şema	Referans (Mondal & Singh, 2022)	Referans (Essaid et al., 2019)	Referans (Suri & Vijay, 2019)
Lenna	UACI	33.49	30.701	33.4733	30.4620
	NPCR	99.99	99.587	99.6453	99.6090
	PSNR	8.63	7.9989	8.6173	-
	Entropy	8.005	7.9989	7.9998	7.9971
Baboon	UACI	33.4568	27.866	33.4542	29.4007
	NPCR	99.9998	99.616	99.6372	99.6010
	PSNR	8.78	44.636	11.8866	-
	Entropy	8.006	7.3719	7.9997	7.9972

IoT sistemleri sınırlı bilgi işlem kaynaklarına sahip sistemlerdir. Bu nedenle IoT ağlarının güvenliği için geliştirilen şifreleme algoritmalarının hafif olması gerekmektedir. Bu çalışmada bir matris yapısını serileştirmek için yeni bir yaklaşım önerilmektedir. Bu yöntem bir görüntü şifreleme şeması olarak sunulmaktadır. Bu yaklaşımın, görüntü matrisi piksel karıştırma seviyeleri ve iki farklı sistem üzerinde yürütme süreleri açısından alternatiflerine göre daha verimli olduğu gösterilmiştir. Sonuç olarak etkili bir hafif

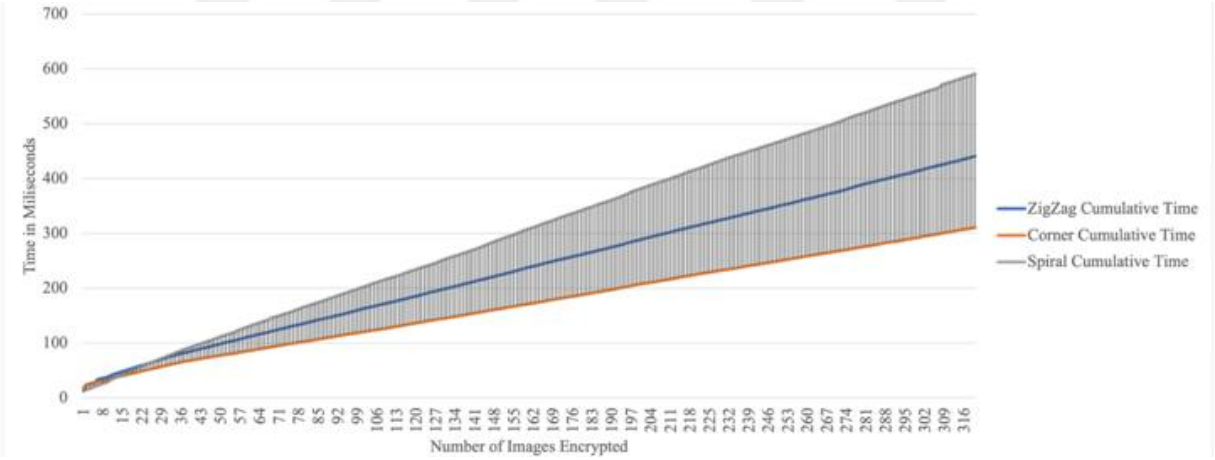
şifreleme algoritması önerilmiştir. Gerçekleştirilen güvenlik testleri, önerilen şemanın güvenlik ihtiyacı olan sistemlerde kullanılabilecek düzeyde bir güvenlik sunduğunu göstermiştir.

5.1.7.11. Zaman karmaşıklığı kıyaslanması

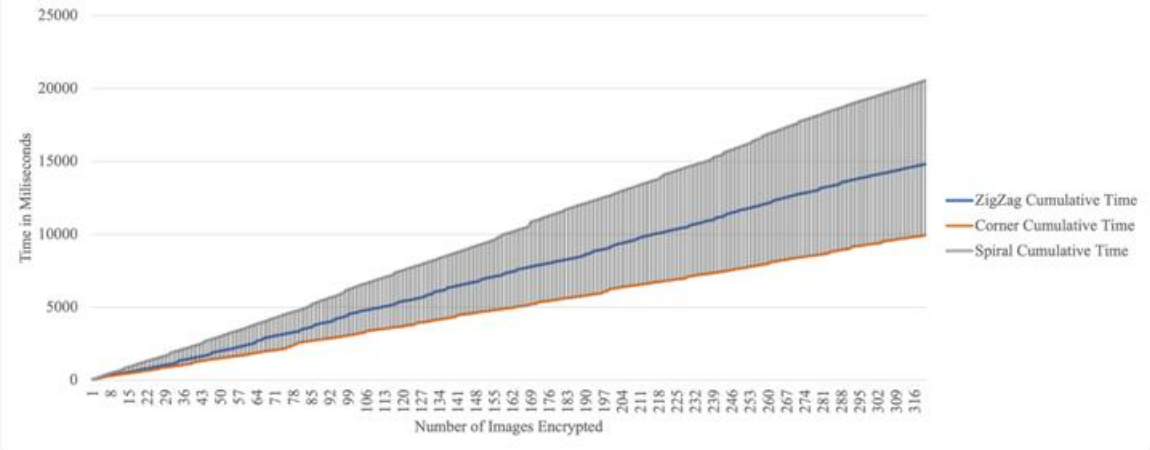
Bir algoritma seçiminde bir diğer önemli faktör, zaman karmaşıklığıdır. Şekil 5.11'de standart laptop için ve Şekil 5.13'te ise IoT cihazı için hesaplanan kümülatif şifreleme sürelerini göstermektedir. Şekillerden de anlaşılacağı üzere KGA en iyi zaman karmaşıklığı sonuçlarını göstermektedir. Çizelge 5.7'de bu analiz için kullanılan iki test ortamının özellikleri verilmektedir.

Çizelge 5.7: Test ortamlarının özellikleri

System	CPU	Memory
Test System 1 (Standard Laptop)	i9 9980HK @2.4 Ghz	32 GB
Test System 2 (Raspberry Pi 4 Model B)	ARM V8 @1.8 Ghz	4 GB



Şekil 5.13: İlk ortam standart laptop için Zigzag, spiral ve KGA kümülatif işlem süreleri



Şekil 5.14: İkinci ortam Raspberry PI için Zigzag, spiral ve KGA kümülatif işlem süreleri

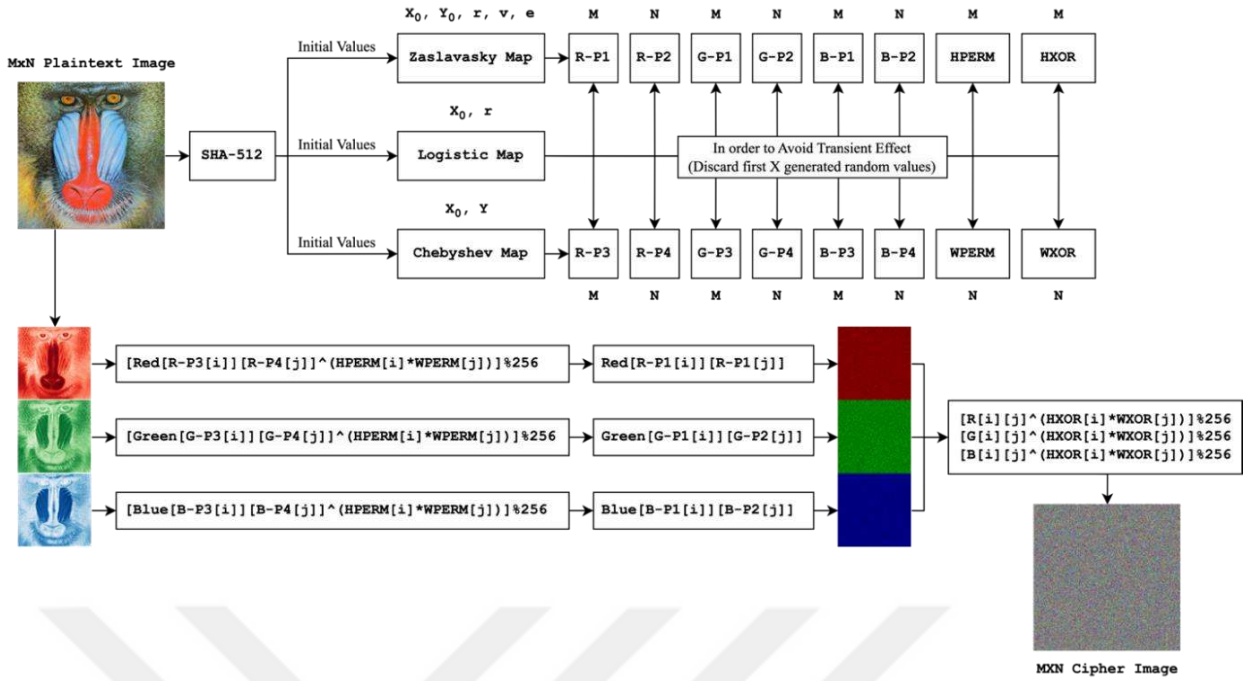
5.2. Uygulama 2: Doğrusal Olmayan Permütasyon Çatısı (DOPÇ)

Genel olarak matris temelli haritalama yöntemlerinde rasgele oluşturulan sayı dizilerine göre piksel konumları değiştirilir. Bu yöntem doğrusal bir yaklaşımdır ve gücünü tamamen kullanılan rasgelelik kaynağının gücünden alır. Bu çalışmada DOPÇ algoritmasında değişken adım sayılı matris permütasyonu önerilmektedir. Bu sayede permütasyon karmaşıklığı arttırılmıştır.

Önerilen algoritmanın görsel özeti Şekil 5.15'de gösterilmektedir. Bu yaklaşımda 2B Zaslavsky haritası, 1B Chebyshev haritası ve 1B Lojistik haritası olmak üzere üç farklı kaotik harita kullanılmaktadır. Bu haritaların çeşitli adım ve şekillerde kullanılmasıyla doğrusallık büyük ölçüde bozulmaktadır. Şekil 5.15 'te M ve N, oluşturulan rastgele dizilerin boyutlarını temsil eder. Zaslavsky haritası kullanılarak 5 adet M boyutlu ve 3 adet N boyutlu rastgele dizi üretilir. Benzer şekilde Chebyshev haritası 3 adet M boyutlu ve 5 adet N boyutlu rastgele diziler üretmek için kullanılır. Son olarak Lojistik harita 16 rastgele sayı üretir. Bu 16 sayı, diğer rastgele sayı üreteçlerinin çıkış uzunluğunu belirler, üretilen tüm dizilerin geçici etkilerini etkili bir şekilde kontrol eder ve güvenliği artırır.

5.2.1. Öncüller

Önerilen DOPÇ algoritması temel olarak bir dizi kaotik harita ve değişken adım sayılı matris haritalama yöntemini kullanmaktadır. Bu bölümde bu kavramlar algoritma özelinde tanıtılacaktır.



Şekil 5.15: Önerilen RGB görüntü şifreleme şemasının grafiksel özeti

Önerilen yaklaşımda biri 2 boyutlu ikisi 1 boyutlu olmak üzere üç farklı kaotik harita kullanılmaktadır. Başlangıç koşullarına ve kontrol parametrelerine oldukça duyarlı olan kaotik haritalar, matematiksel formüller tarafından oluşturulan öngörülemeyen dizilerdir. Doğasında var olan rastgelelik ve mevcut çok çeşitli seçenekler nedeniyle bu çalışma, güçlü güvenliği korurken hesaplama verimliliğine (veya odağa bağlı olarak şifreleme hızına) öncelik vermek için düşük boyutlu kaotik haritalar kullanır. Çıktıları, Şekil 5.13'de gösterildiği gibi, görüntünün karıştırma ve yayılma aşamalarında birlikte kullanılır. Bu sayede yüksek karmaşıklık sunarken verimlilikten taviz verilmez.

Zaslavsky haritası dört parametreli 2 boyutlu kaotik bir haritadır ve uygun özellikleri nedeniyle seçilmiştir. Zavslavsky denklemi Denklem 5.1, 5.2 ve 5.3'te sunulmaktadır.

$$x_{n+1} = [x_n + v(1 + \mu y_n) + \epsilon v\mu \cos(2\pi x_n)] mod 1 \quad (5.1)$$

$$y_{n+1} = e^{-r}(y_n + \epsilon \cos(2\pi x_n)) \quad (5.2)$$

$$\mu = \frac{1-e^{-r}}{r} \quad (5.3)$$

Bu denklemde $\epsilon, v, \mu, and\ e$ kontrol paametreleri, $x_n\ ve\ y_n$ başlangıç parametreleridir.

Kullanılan diğer kaotik harita Chebyshev haritası matematiksel denklemi denklem 5.4'te verilmiştir.

$$X_{n+1} = \cos(\gamma \cos^{-1}(X_n)) \quad (5.4)$$

Chebyshev haritasında γ control parametresi ve X_n başlangıç değeridir. $\gamma > 1$ olduğu zaman Chebyshev haritası kaotiklik gösterir.

Son olarak kullanılan kaotik harita lojistik haritadır ve lojistik haritanın matematiksel ifadesi denklem 5.5.'te verilmiştir.

$$X_{n+1} = \mu X_n(1 - X_n) \tag{5.5}$$

Burada $0 < \mu \leq 4$ ve $0 < x_0 < 1$ aralığında sistem kaotiklik gösterir.

5.2.2. DOPÇ Analitik İfadesi

Geliştirilmiş güvenlik için önerilen görüntü şifreleme algoritması stratejik bir yaklaşım benimser: her RGB kanalında benzersiz rastgele diziler kullanılır ve bu da şemanın genel doğrusal olmama özelliğini artırır. Denklem 5.6, 5.7, 5.8, 5.9 ve 5.10, algoritmanın matematiksel temeline açılan bir pencere sunar.

$$A_{red}[R - P1[i]][R - P2[j]] = \left(I_{red}[R - P3[i]][R - P4[j]] \oplus (HPERM[i] * WPERM[j])\right) \%256 \tag{5.6}$$

$$A_{green}[G - P1[i]][G - P2[j]] = \left(I_{green}[G - P3[i]][G - P4[j]] \oplus (HPERM[i] * WPERM[j])\right) \%256 \tag{5.7}$$

$$A_{blue}[B - P1[i]][B - P2[j]] = \left(I_{blue}[B - P3[i]][B - P4[j]] \oplus (HPERM[i] * WPERM[j])\right) \%256 \tag{5.8}$$

$$Cipher_{red}[i][j] = (A_{red} \oplus \big(HXOR[i] * WXOR(j)\big) \%256 \tag{5.9}$$

$$Cipher_{green}[i][j] = (A_{green} \oplus \big(HXOR[i] * WXOR(j)\big) \%256 \tag{5.10}$$

$$Cipher_{blue}[i][j] = (A_{blue} \oplus \big(HXOR[i] * WXOR(j)\big) \%256 \tag{5.11}$$

Bu 6 adet denklem, görüntüyü iki iç içe döngüyle bir kez geçerek $M \times N$ (görüntü boyutları) verimli bir şekilde kullanır. Bu, yüksek düzeyde doğrusal olmayan basit, uygulanabiir net ve zarif bir çözümle sonuçlanır.

5.2.3. Uygulamanın Değerlendirme Sonuçları

Bu çalışmada SIPI veriseti kullanılmış ve şifreli görüntüleri elde edilmiştir. Bütün sonuçlar kullanılan test görüntülerinden elde edilen değerlerin ortalaması şeklinde kıyaslamaya sokulmuştur. Elde edilen kıyaslama sonuçları önerilen çatının güçlü ve verimli bir yaklaşım olduğunu göstermektedir.

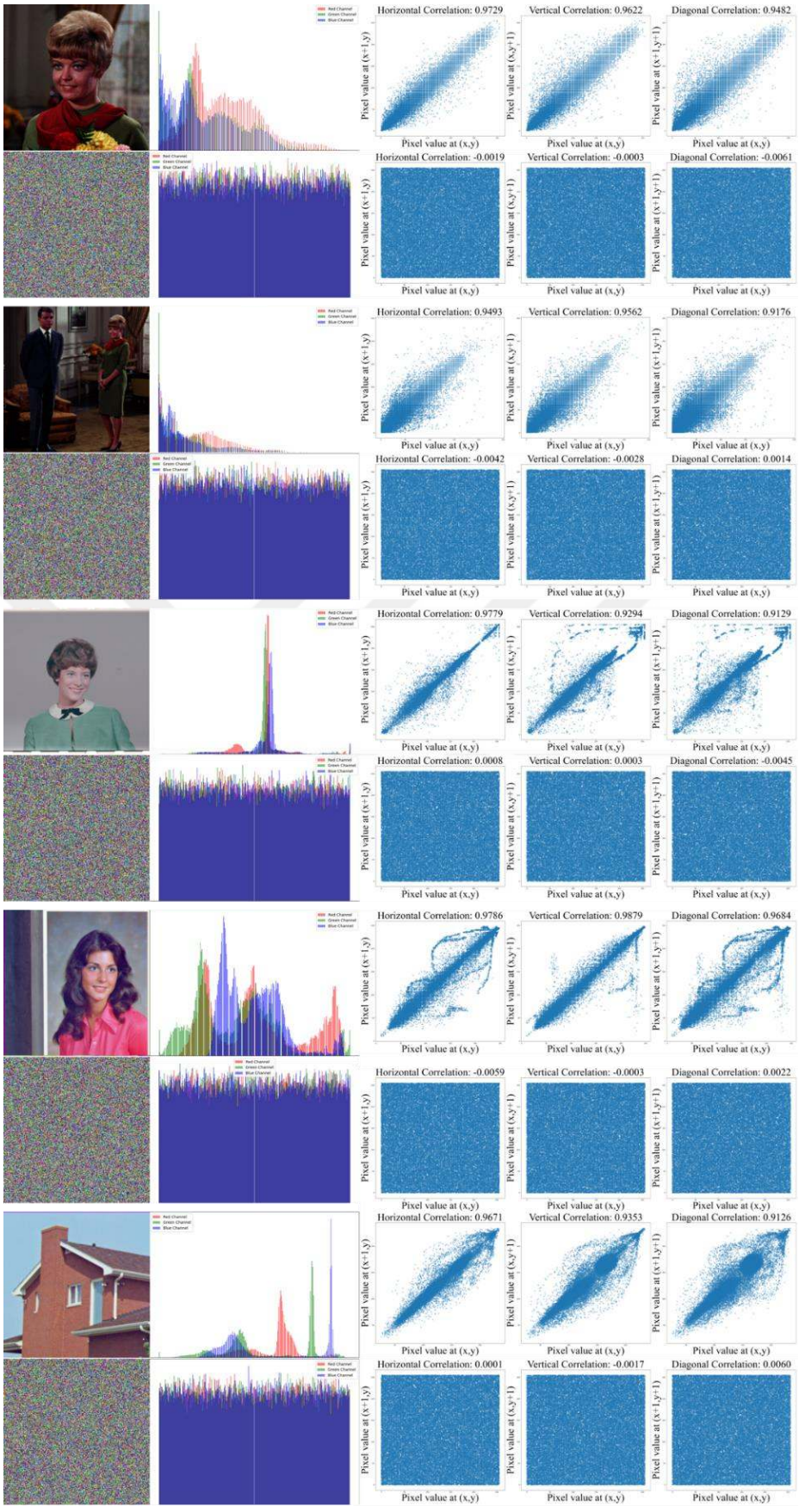
5.2.3.1. Histogram analizi sonuçları

Dijital bir görüntünün histogramı piksel değerlerinin dağılımını temsil eder. Görsel görüntüler için piksel değerlerinin dağılımı belirli bir ayırt edilebilir modeli takip eder.

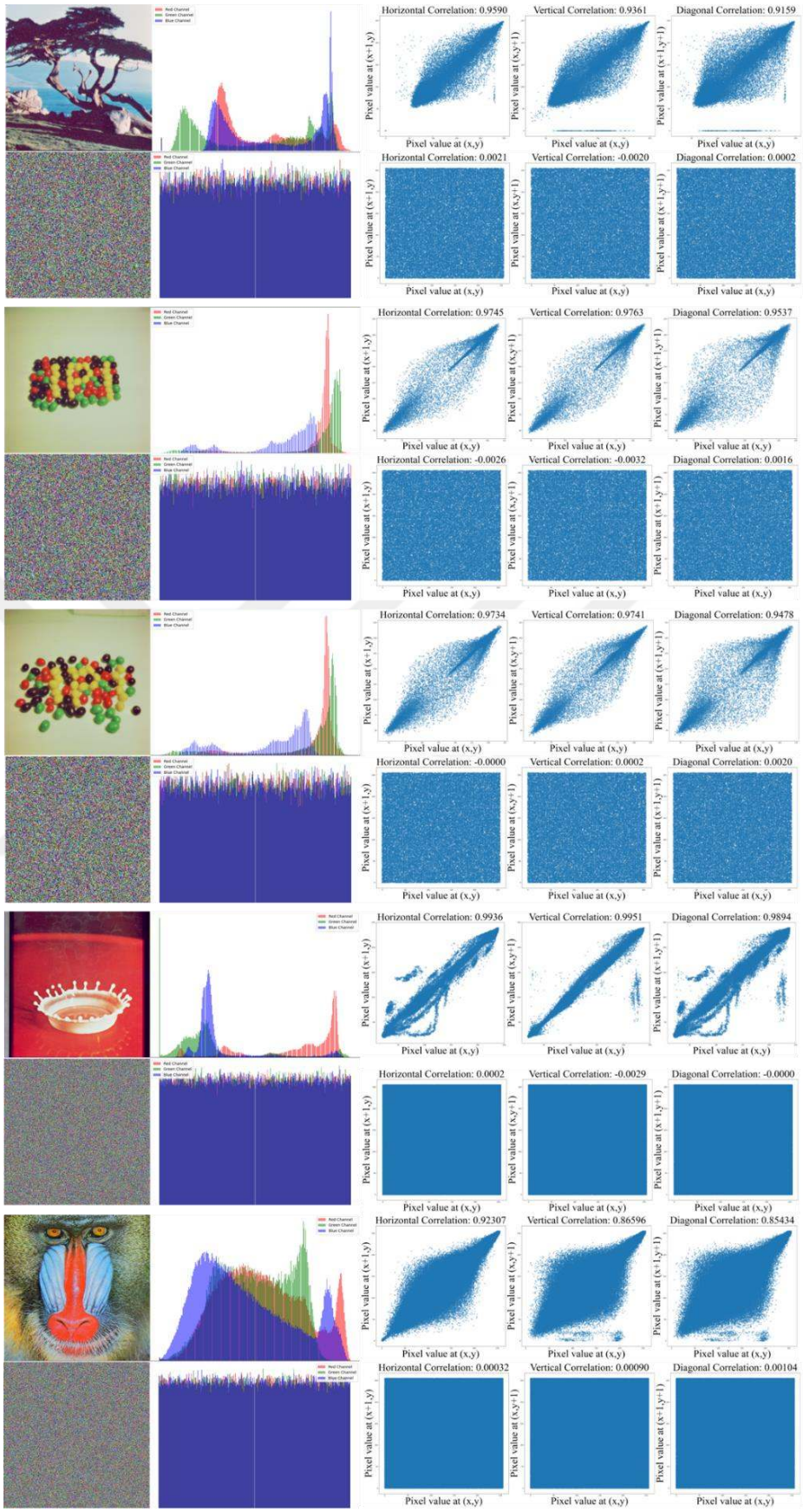
İstatistiksel saldırı, bir kriptosistemi kırmak için istatistiksel ipuçları bulmanın yaygın bir yöntemidir. Güvenli bir şifreleme sistemi, şifrelenmiş görüntünün tekdüze bir frekans dağılımına sahip olmasını ve mümkün olduğunca az istatistiksel bilgi sağlamasını sağlamalıdır. Şekil 5.16, 5.17, 5.18 'de sunulan uygulama sonuç görsellerinin ikinci sütunu, düz metin ve şifrelenmiş görsellerin histogram sonuçlarını göstermektedir. Bu şekillerden de görülebileceği gibi, önerilen algoritma, şifrelenecek düz metin görüntünün histogramının ne kadar farklı olduğuna bakılmaksızın, tüm şifrelenmiş görüntüler için benzer grafikler üretmektedir. Dolayısıyla önerilen yöntemin histogram analizinde başarılı olduğu sonucuna varılabilir.

5.2.3.2. Korelasyon katsayısı analizi sonuçları

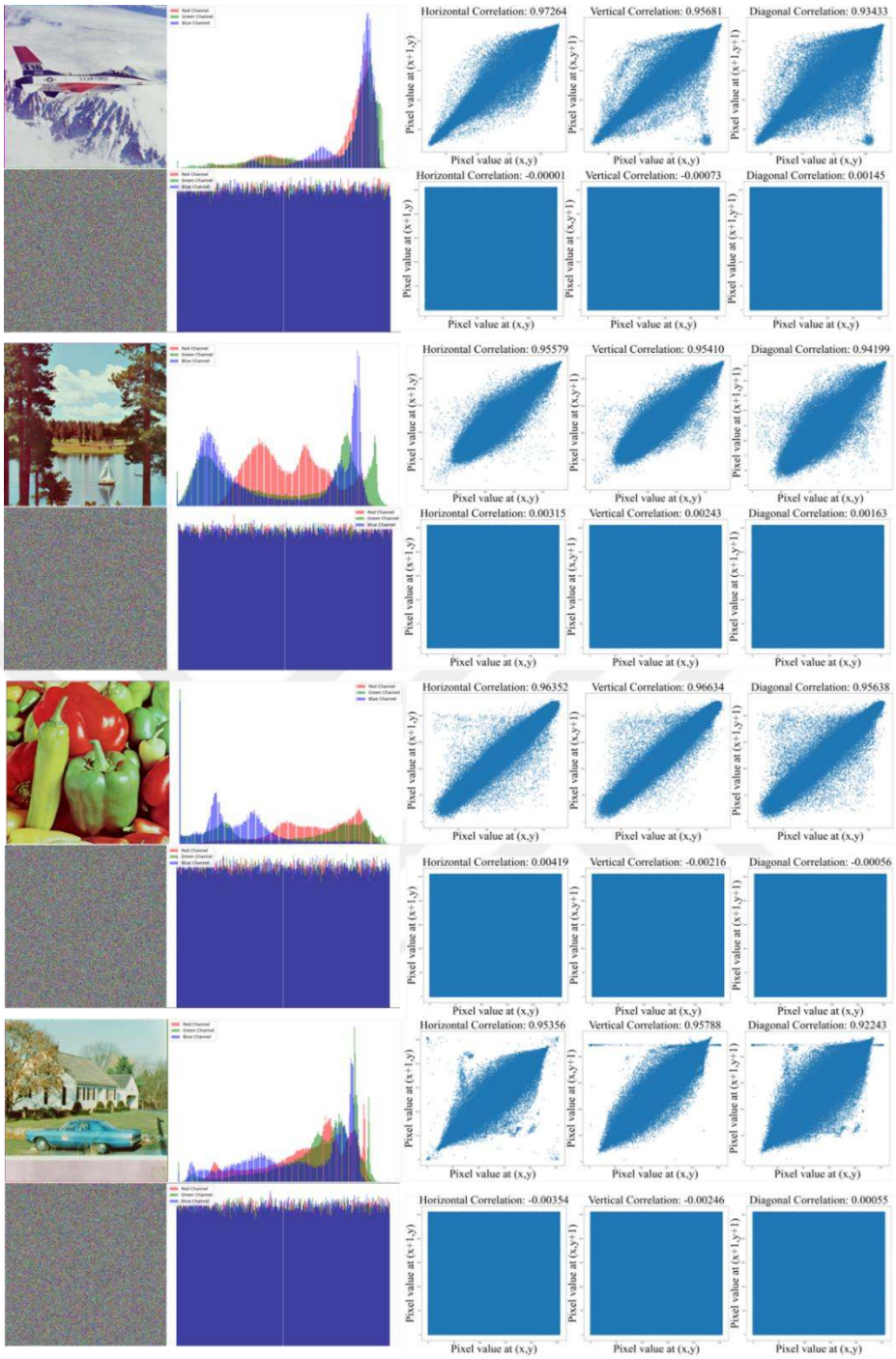
Görüntülerin doğası gereği bitişik pikselleri, yüksek korelasyon sergiler. Korelasyon katsayısı, iki değişken arasındaki istatistiksel ilişkiyi ölçmek için kullanılan sayısal bir ölçüdür. Yüksek korelasyon, saldırganların olasılık teorisini kullanarak bitişik piksel değerlerini tahmin etmeye çalışabilecekleri anlamına gelir. Mükemmel bir görüntü şifreleme algoritması, bitişik pikseller arasındaki korelasyonu azaltmalı ve minimum korelasyon katsayısı sağlamalıdır. Şekil 5.16, 5.17, 5.18 'de sunulan uygulama sonuç görsellerinin üçüncü sütunu, düz metin ve şifrelenmiş görsellerin korelasyon sonuçlarını göstermektedir. SIPI datasetini oluşturan görüntüler üç parçaya ayrılarak ilk satırda ele alınan düz görüntünün ilk sütun değerini oluşturmuştur. İlk satırın ikinci sütun değeri düz görüntünün histogram grafiğini, diğer son üç sütun ise sırasıyla yatay, dikey, çapraz korelasyon grafiklerini göstermektedir. İlk satırın altındaki ikinci satır ise birinci satırda yer alan düz görüntünün şifreli görüntüsü için yeniden histogram ve korelasyon grafiklerini içermektedir. Şekillerdeki şifreli görüntülerin histogram ve korelasyon dağılımları incelendiğinde piksellerin tamamen düzgün dağılımlı olduğu görülmektedir. Şekil 5.16, Şekil 5.17, Şekil 5.18 görsellerindeki tüm görseller için teker teker düz görüntü ve şifreli görüntü değerleri için histogram analizi ve korelasyon analizleri yapılmış olup 14 görüntü ve 14 şifreli görüntü için histogram ve korelasyon sonuçları elde edilmiştir.



Şekil 5.16: SIPI veriseti histogram ve korelasyon analizleri



Şekil 5.17: SIPI veriseti histogram ve korelasyon analizleri



Şekil 5.18: SIPI veriseti histogram ve korelasyon analizi

5.2.3.3. Bilgi entropisi analizi

Görüntü şifrelemede, rastgeleliğin bir ölçüsü olan entropi hayati bir rol oynar. Bilgilerin yetkisiz erişime karşı gizlenmesine yardımcı olur. Algoritma, şifreleme işlemi aracılığıyla görüntünün entropisini artırmayı hedefleyerek görüntüyü daha öngörülemez bir duruma dönüştürürür ve saldırganların içeriğin şifresini çözmesini önemli ölçüde zorlaştırır.

Bir veri kümesinin maksimum entropi değeri, içerdiği benzersiz olayların (veya sınıfların) sayısına bağlıdır. Bilgi teorisinde belirsizliğin veya rastgeleliğin bir ölçüsü olan entropi, maksimum değerine tüm olayların eşit olasılıkta olduğu durumlarda ulaşır. Çizelge 5.8'de SIPI verisetinin düz resim entropi değerleri ve şifreli resim için entropi değerleri verilmiştir.

Çizelge 5.8: SIPI veriseti düz görüntü ve şifreli görüntü bilgi entropisi değerleri

SIPI veriseti	**Entropi**		**Entropi Sapma**
	Düz resim	**Şifreli resim**	
4.1.01	6.8981	7.9984	0.0016
4.1.02	6.2945	7.9991	0.0009
4.1.03	5.9709	7.9990	0.0010
4.1.04	7.4269	7.9990	0.0010
4.1.05	7.0686	7.9990	0.0010
4.1.06	7.5371	7.9989	0.0011
4.1.07	6.5835	7.9991	0.0009
4.1.08	6.8527	7.9991	0.0009
4.2.01	7.2428	7.9997	0.0003
4.2.03	7.7624	7.9998	0.0002
4.2.05	6.6639	7.9998	0.0002
4.2.06	7.7622	7.9998	0.0002
4.2.07	7.6698	7.9997	0.0003
house	7.4858	7.9998	0.0002
Ortalama	**7.0871**	**7.9993**	**0.0007**

5.2.3.4. Yatay, dikey ve çapraz korelasyon analizi

Rastgele seçilen piksellerden oluşan bir alt kümeyle (örneğin, 3000, 5000...) korelasyon katsayılarını hesaplayan tipik uygulamaların aksine, bu yaklaşım, görüntünün tam korelasyon özelliklerini yakalamak için tüm piksel değerlerini analiz eder. Şekil 5.16, 5.17, ve 5.18'in üçüncü sütundaki düz metin ve şifre görüntülerinin yatay, dikey ve çapraz korelasyon grafikleri sunulmaktadır. Ek olarak Çizelge 5.9'te sayısal korelasyon analizi sonuçları verilmektedir. Çizelge 5.9, SIPI veri kümesindeki tüm renkli görüntüler için korelasyon katsayılarını sunmaktadır. Netliği artırmak için son satırda 14 görüntünün ortalama korelasyon değerleri verilmiştir. Bu sonuçların incelenmesiyle önerilen algoritmanın istatistiksel saldırılara karşı etkinliği daha da belirgin hale gelmektedir.

Çizelge 5.9: SIPI veri seti yatay, dikey, çapraz korelasyon katsayıları sayısal değerleri

SIPI Image	Yatay Korelasyon		Dikey Korelasyon		Köşegen Korelasyon	
	Düz görüntü	**Şifreli**	**Düz görüntü**	**Şifreli**	**Düz görüntü**	**Şifreli**
4.1.01	0.9629	-0.0019	0.9622	-0.0003	0.9482	-0.0061
4.1.02	0.9493	-0.0042	0.9562	-0.0028	0.9176	0.0014
4.1.03	0.9779	0.0008	0.9294	0.0003	0.9129	-0.0045
4.1.04	0.9786	-0.0059	0.9879	-0.0003	0.9684	0.0022
4.1.05	0.9671	0.0001	0.9353	-0.0017	0.9126	0.0060
4.1.06	0.9590	0.0021	0.9361	-0.0020	0.9159	0.0002
4.1.07	0.9745	-0.0026	0.9763	-0.0032	0.9537	0.0016
4.1.08	0.9734	-0.0000	0.9741	0.0002	0.9478	0.0020
4.2.01	0.9936	0.0002	0.9951	-0.0029	0.9894	-0.0000
4.2.03	0.9231	0.0003	0.8660	0.0009	0.8543	0.0010
4.2.05	0.9726	-0.0000	0.9568	-0.0007	0.9343	0.0015
4.2.06	0.9558	0.0032	0.9541	0.0024	0.9420	0.0016
4.2.07	0.9635	0.0041	0.9663	-0.0021	0.9564	-0.0006
house	0.9536	-0.0035	0.9579	-0.0024	0.9224	0.0005
Ortalama	**0.9646**	**-0,0005**	**0,9538**	**-0,001**	**0,9339**	**0,0004**

5.2.3.5. Diferansiyel analiz

Diferansiyel analizde kullanılan en yaygın iki yöntem NPCR ve UACI değerlendirmeleridir. UACI, iki görüntünün karşılık gelen pikselleri arasındaki ortalama yoğunluk farkını ölçer. Orijinal görüntüdeki tek bir piksel değişikliğinin şifrelenmiş görüntüyü ne kadar etkilediğini gösterir. Bunun tersine, NPCR, orijinal görüntüdeki tek bir bit değişiminden sonra şifrelenmiş görüntünün değiştiği piksel konumlarının yüzdesini yansıtır. Saldırganların orijinal görüntüyü hafifçe değiştirerek bilgileri kurtarmaya çalıştığı diferansiyel saldırılara karşı algoritmanın direncinin bir ölçüsü olarak hizmet eder. Önerilen şemanın NPCR ve UACI değerleri Çizelge 5.10'te NPCR Piksel ve UACI piksel olarak sunulmaktadır. Diğer NPCR Anahtarı ve UACI Anahtarı değerleri, önerilen şemanın temel duyarlılık analizi sonuçlarıdır. İdeal NPCR ve UACI değerlerini sırasıyla %99,6094070 ve %33,4635070 olarak belirleyen FIPS'in bulgularına dayanarak Çizelge 5.10, önerilen çerçevenin bu referans değerlerine yakın performans ölçümlerine ulaştığını göstermektedir. Bu yakınlık güçlü şifreleme yeteneklerini akla getiriyor. Ortalama NPCR ve UACI değerleri beklenen değerlerden sırasıyla 0,0028 ve 0,0055 sapmaktadır ve ideale yakındır.

Çizelge 5.10: SIPI veriseti diferansiyel analiz sonuçları

SIPI Image	NPCR Piksel	UACI Piksel	NPCR Anahtar	UACI Anahtar
4.1.01	99.5895	33.4347	99.6220	33.3791
4.1.02	99.6098	33.5497	99.5981	33.4934
4.1.03	99.6185	33.5128	99.6058	33.4923
4.1.04	99.6089	33.4365	99.5819	33.4341
4.1.05	99.5967	33.4517	99.6089	33.5056
4.1.06	99.6144	33.3184	99.5966	33.3930
4.1.07	99.6205	33.4366	99.6114	33.4796
4.1.08	99.6170	33.4806	99.6124	33.4764
4.2.01	99.6206	33.4769	99.6049	33.4162
4.2.03	99.6288	33.4559	99.6215	33.4799
4.2.05	99.6081	33.4997	99.6117	33.4637
4.2.06	99.6135	33.5064	99.6173	33.5072
4.2.07	99.6236	33.5133	99.6055	33.5188
house	99.6009	33.4934	99.6044	33.4326
Ortalama	**99,6122**	**33,4690**	**99,6073**	**33,4622**

5.2.3.6. Anahtar hassasiyeti analizi

İyi bir görüntü şifreleme sistemi, anahtarın düz metinle tam olarak karıştırılmasını sağlamak için yüksek anahtar duyarlılığı gerektirir. Şemamız dokuz anahtar kullanıyor. Anahtar hassasiyeti, herhangi bir anahtar alandaki bir dakikalık değişikliğin (10-15 seviye) şifrelenmiş görüntü üzerindeki etkisi ile ölçülür. Burada, Zaslavsky haritasının x_0 parametresinde 10-15'lik bir değişiklikle oluşturulan şifre görüntüsü ile orijinal şifrelenmiş görüntü (Çizelge 5.10'te NPCR Anahtarı ve UACI Anahtarı olarak sunulan) arasındaki NPCR ve UACI değerlerini hesaplıyoruz. Sonuçlar, önerilen sistemin güçlü anahtar duyarlılığını ve kapsamlı saldırı direncini göstermektedir. Ortalama NPCR ve UACI değerleri beklenen değerlerden sırasıyla 0,0021 ve 0,0068 sapmaktadır.

Anahtar Alan Analizi: Görüntü şifrelemede anahtar alanı boyutu genellikle anahtarda kullanılan toplam bit sayısıyla tanımlanır. Bu şema iki parçalı bir anahtar kullanır: farklı kaotik haritaların başlangıç değerleri ve düz metin görüntüsünün SHA-512 karma değeri. Başlangıç değerleri çift duyarlıklı olduğundan uzayları 2^{288}'dir. 512 bitlik SHA-512 hash değerinin uzayı 2^{512}'dir. Dolayısıyla tüm şemanın anahtar uzayı 2^{800} olur. 2^{800} bir anahtar uzayı ile önerilen şema önemli ölçüde aşmaktadır. 2^{256}'lık minimum (Amina et al., 2024; Fetteha et al., 2023; Mckay & Cooper, 2001) eşiğin (Amina et al., 2024), (Fetteha et al., 2023), (Mckay & Cooper, 2001) kaba kuvvet saldırılarına karşı dirençli olduğu kabul edilir. Bu geniş anahtar alanı, kaba kuvvet

saldırılarını etkili bir şekilde hesaplama açısından olanaksız hale getirerek bu tür girişimlere karşı yüksek düzeyde güvenlik sağlar.

Sağlamlık Analizi: Güvenli bir görüntü şifreleme algoritmasının sağlamlığı genellikle aşırı durumlardaki performansı kullanılarak değerlendirilir. Burada siyah beyaz görüntüler için şifreleme ve şifre çözme performansını analiz ediyoruz. Şekil 5.19 sonuçları göstermektedir. Özel olarak tasarlanmış 256x256 siyah-beyaz görüntülerin şifrelenmesini ve şifresinin çözülmesini, bunlara karşılık gelen histogram grafikleriyle birlikte gösterir. Şekil 5.19'dan da görülebileceği gibi önerilen yöntem bu tür görüntüleri başarılı bir şekilde ele almaktadır.

5.2.3.7. Literatürdeki çalışmalarla DOPÇ kıyaslaması

Yaklaşım, uygulama alanı ve test görüntülerindeki farklılıklardan kaynaklanan görüntü şifreleme algoritmalarındaki doğal değişkenlik nedeniyle, görüntü bazında karşılaştırmalar zor olabilir. Bunu ele almak için Çizelge 5.11, bu çalışmada sunulan değerlendirme kriterlerinin ortalama değerlerine dayalı bir karşılaştırma sunmaktadır. Çizelge 5.11, bu çalışmada önerilen yöntemin değerlendirme metriklerinin yanı sıra en son teknolojiye sahip görüntü şifreleme algoritmalarından elde edilen sonuçları içerir. Bu çalışmada adil bir karşılaştırma sağlamak için diğer görüntü şifreleme algoritmalarının değerlendirmeleri, bu çalışmada kullanılan yöntemlerin aynısı kullanılarak hesaplanan ölçümlere dayandırılmıştır. Bu yaklaşım, karşılaştırmalar arasında tutarlılık sağlar. Ortalamalar, karşılaştırılan her çalışmada kullanılan test görüntülerinin sayısı dikkate alınarak hesaplanmıştır. Örneğin korelasyon değerleri mutlak değerler olarak toplanmış ve her çalışma için ortalama sonuç elde edilmiştir.

Önerilen algoritmanın sağlamlığı, sadece şifreleme yeteneğiyle sınırlı değildir. Veri kaybı ve gürültü gibi zorlu koşullarda bile şifreli görüntülerin çözülmesinde de oldukça başarılıdır. Bunu kanıtlamak için iki test gerçekleştirilmiştir:

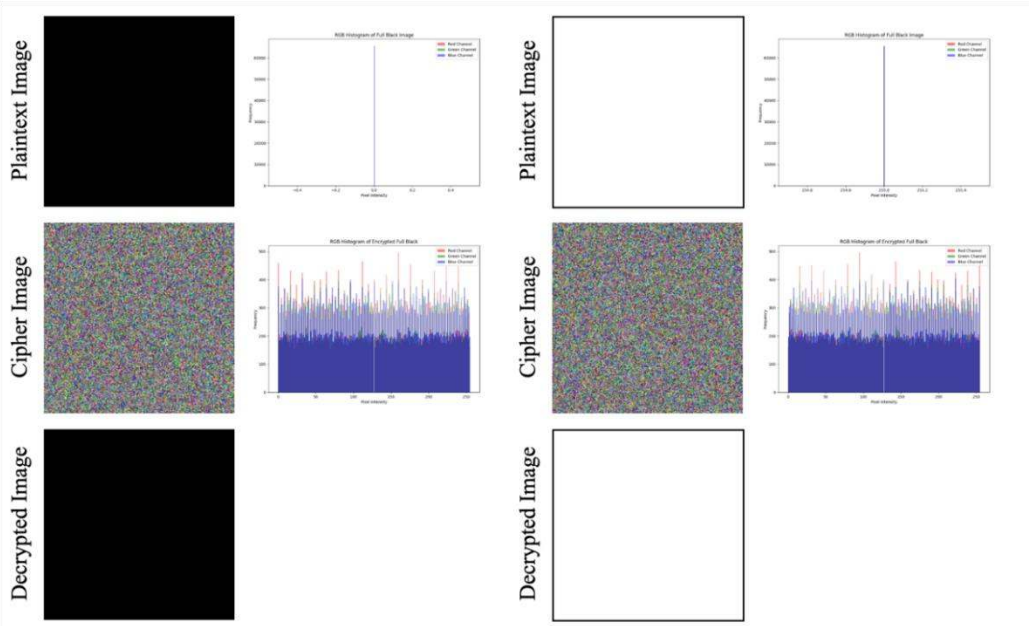
Veri Kaybına Karşı Dayanıklılık: Rastgele veri kaybı %10 ila %90 arasında değişen şifrelenmiş görüntüler çözülmüştür. Şekil 5.20 'de da görülebileceği gibi, %90 veri kaybı gibi ekstrem bir durumda bile orijinal görüntünün silueti hala fark edilebilir durumdadır.

Gürültüye Karşı Dayanıklılık: Değişen derecelerde tuz ve biber gürültüsü (0,1 ila 0,9) eklenmiş şifrelenmiş görüntüler çözülmüştür. Şekil 5.21'de gösterilen sonuçlar, algoritmanın 0,9 seviyesine kadar yüksek gürültü seviyelerinde bile sağlamlığını koruduğunu göstermektedir.

Genelleştirilebilirlik: Bu testlerde, test setinden en sık kullanılan iki görüntü (Babun ve Uçak) kullanılmıştır. Farklı görüntü türleri üzerinde de benzer sonuçlar elde edilmiştir. Bu durum önerilen çalışmanın görüntü verisini yüksek seviyede anlamsızlaştırdığını göstermektedir.

Çizelge 5.11: Literatürde yapılmış çalışmalarla DOPÇ değerlendirme metrik sonuçları kıyaslama

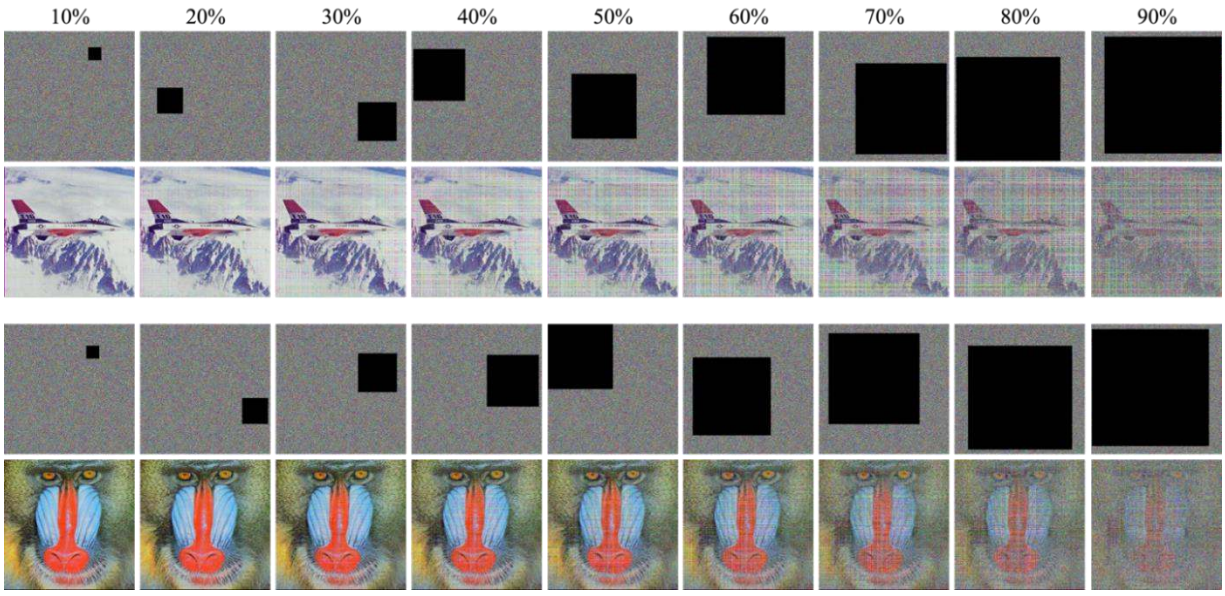
Değerlendirme Metrikleri	**(Alghamdi et al., 2022)**	**(Amina et al., 2024)**	**(Es-sabry et al., 2024)**	**(Chai, Gan, et al., 2017)**	**(Buyukcolak, 2019)**	**(Z. Li et al., 2021)**	**(Yu et al., 2023)**	**(Sayed & Radwan, 2020)**	DOPÇ
Korelasyon	0.3645	0.0009	0.0069	0.0047	0.0036	0.004	0.0046	0.0018	0.00063
PSNR	9.2098	8.6267	6.5690	-	-	-	-	-	8.2635
Entropy	7.9987	7.9983	7.9987	7.9964	7.9985	7.9025	7.9981	7.9971	7.9993
NPCR Pixel	99.6153	99.5211	99.6520	-	99.6089	99.7272	98.3051	99.6143	99,6122
UACI Pixel	33.4718	33.1778	33.5244	-	33.4658	33.4730	32.4134	33.5002	33,4690
NPCR Key	-	-	-	-	-	-	-	-	99,6073
UACI Key	-	-	-	-	-	-	-	-	33,4622
Anahtar Uzayı	2^{256}	2^{1116}	-	2^{600}	2^{471}	-	2^{384}	-	2^{800}



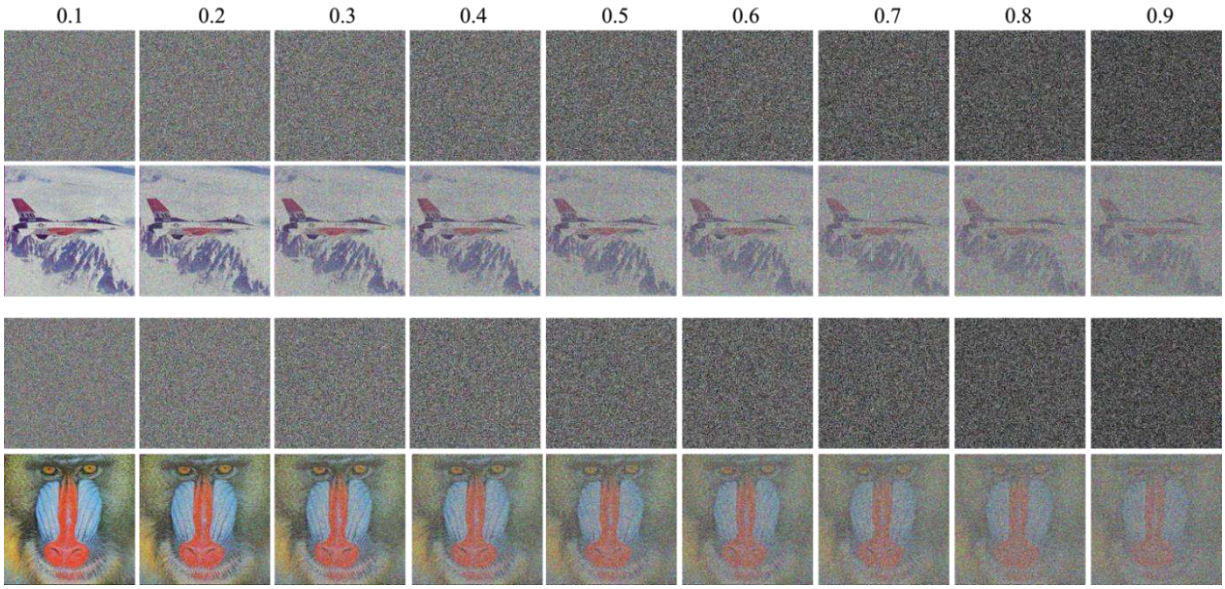
Şekil 5.19: Önerilen şemanın tam siyah beyaz görüntü şifreleme, şifre çözme ve histogram sonuçları; sağlamlık analizi

5.2.3.8. DOPÇ gürültü ve veri kaybı analizi sonuçları

Önerilen algoritma, sadece zarif, verimli ve güvenli olmakla kalmayıp, veri kaybı ve gürültüye karşı da oldukça dayanıklıdır. Bu sayede, algoritma daha geniş bir yelpazede uygulama imkânı bulmaktadır.



Şekil 5.20: Şifre görüntüsünde farklı yüzdesel veri kaybı için şifre çözme sonucu



Şekil 5.21: Şifre görüntüsündeki farklı yüzde Salt & Peppers gürültüsü için şifre çözme sonucu

5.2.3.9. DOPÇ algoritmasının karmaşıklık analizi

Önerilen görüntü şifreleme şeması, zaman karmaşıklığı açısından olağanüstü verimlilik göstermektedir. Tüm işlemler aynı anda gerçekleştirilebilir, böylece işlem süresi en aza indirilir. 2,4 GHz işlemci üzerinde yapılan testler, 100 çalıştırma için ortalama şifreleme süresinin 29 ms ve ortalama şifre çözme süresinin 25 ms olduğunu ortaya çıkardı. Bu özellikli sonuçlar, nesnellik açısından resmi karşılaştırmaların dışında bırakılırken, yöntem, verimli çalışmasını gösteren uygun bir $O(MxN)$ zaman karmaşıklığına sahiptir.

5.2.3.10. Değerlendirme

Güvenlik ve Verimlilik: Bu çalışma, üç farklı kaotik haritanın stratejik kullanımıyla hem güvenliği hem de verimliliği artıran hafif bir görüntü şifreleme algoritması önermektedir. Bu, uygulama basitliği ve düşük bellek kullanımıyla birlikte yüksek güvenlik sağlamaktadır.

Bellek Kullanımı: Temel konfigürasyonda 16 dizi kullanılması bellek kullanımıyla ilgili endişelere yol açabilir. Fakat bu konfigürasyonda bile sistemin bellek alanı yaklaşık 16 MB'tır. Bu, günümüzdeki standartlara göre oldukça düşük bir rakamdır.

Düşük Boyutlu Kaotik Haritaların Kullanımı: Düşük boyutlu kaotik haritaların kullanımı, anahtar alanı ve sistem karmaşıklığı açısından avantajlar sunmaktadır. Bu da onları kaynak kısıtlı cihazlar için ideal hale getirir.

Doğrusallık Sorunu: Düşük boyutlu haritaların doğrusallık eğilimi, şifreleme algoritmasının güvenliğini zayıflatabilir. Önerilen yöntem, doğrusal olmayan matris geçişleri kullanarak bu sorunu etkili bir şekilde ortadan kaldırır.

Anahtar Alanı: 2^{800} bitlik anahtar alanı, IoT sistemleri için fazlasıyla yeterlidir.

Önerilen algoritma, kaynak kısıtlı cihazlar için ideal olan hafif, güvenli ve verimli bir görüntü şifreleme çözümü sunmaktadır.

- Düşük boyutlu kaotik haritaların kullanımıyla ilgili endişeler, doğrusal olmayan matris geçişleri ve geniş anahtar alanı ile giderilmiştir.
- Bellek kullanımıyla ilgili endişeler, 16 MB'lık düşük bellek alanı ile ortadan kalkmaktadır.
- Gelecekteki geliştirmeler, daha yüksek güvenlik gereksinimlerini karşılamak için sistem karmaşıklığını ve anahtar alanını artırmaya odaklanacaktır.

Önerilen DOPÇ, hafif ve verimli yapısıyla, kaynak kısıtlı cihazlar için ideal bir görüntü şifreleme çözümü sunmaktadır.

6. SONUÇLAR

Bu tez çalışmasında kaynak kısıtlı cihazları hedefleyen şifreleme algoritmaları üzerine bir araştırma gerçekleştirilmiş ve önerilen KGA ve DOPÇ olarak isimlendirilen iki yeni yaklaşım ile kullanışlı sonuçlar elde edilmiştir. Her iki yaklaşımda rasgelelik kaynağı olarak kaotik haritalar kullanılmıştır. Görüntü şifreleme işlemlerinde kaotik haritalar yaygın kullanılan yöntemlerdendir. Kaotik haritaların öngörülmezliği, başlangıç koşullarına hassasiyeti, ergodiklik gibi bazı özellikleri kaotik haritaları vazgeçilmez kılmaktadır. Bu tezde düşük boyutlu Lojistik, Zaslavsky ve Chebyshev haritaları kullanılarak düşük zaman karmaşıklığı ve iyi karıştırma ve yayma adımları geliştirmek hedeflenmiştir. Kaotik haritaların farklı kombinasyonlar ile kullanılması sayesinde düşük dereceli haritalar kullanılmasına rağmen güvenli minimum anahtar alan uzayından çok daha yüksek değerler sağlamıştır. Deneysel sonuçlar gerçekleştirlen uygulamaların iyi dinamik özellikleri gösterdiğini; gürültüye ve küçük dış etkenlere karşı dayanıklı olduğunu, gürültü varlığında görüntülerdeki filigranları kurtarmamıza olanak tanıdığını göstermektedir.

Birinci yaklaşım görüntü piksel karıştırma algoritmalarına alternatif hafif ve verimli bir piksel serileştirme algoritması KGA'yı sunarken, ikinci yaklaşım birçok algoritmanın ara adımlarında kullanılabilecek değişken adımlı matris haritalama yaklaşımını kullanan yeni bir şifreleme çerçevesi (DOPÇ) sunmaktadır.

Çalışmanın ilk aşamasında KGA gerçekleştirilmiş olup, önerilen algoritma kriptanalize karşı yüksek güvenlik ve sağlamlık sunmaktadır. İyi bir anahtar uzayı sayesinde kaba kuvvet saldırılarına karşı, düzgün dağılımlı histogramlara ve sıfıra yakın korelasyon değerleri ile istatistiksel saldırılara karşı, ideale çok yakın NPCR ve UACI değerleri ile de diferansiyel saldırılara karşı yüksek dayanıklığa sahiptir. Sunulan güvenlik analizleri, IoT uygulamaları için şifreleme algoritmasının etkinliğini doğrulamıştır. Önerilen algoritmanın performansı kişisel bir bilgisayar ve Raspberry Pi 4 üzerinde test edilmiştir. Düşük donanım özelliklerine sahip IoT cihazlarda çalışma süresinin optimum değerlere yakın olması hafif siklet şifreleme algoritmaları sınıfında alternatif bir yöntem olduğunu göstermektedir. Güvenlik analizi sonuçlarına göre, şifreleme algoritmasında güvenliği garanti etmek için kaotik haritada daha büyük bir boyutun gerekli olmadığı görülmüştür. Raspberry Pi 4 Model B ortamında gerçekleştirilen testlerde 316 adet 256x256 görüntülerden oluşan veri kümesinin tamamını 1 saniye gibi çok kısa bir sürede şifrelenmektedir. Buna karşın aynı kategorideki rakipleri 1,5 ve 2 katı daha uzun süre almıştır. Sonuçlar değerlendirildiğinde

KGA ‘nın ilgili kategoride gerçekleştirilen diğer algoritma sonuçları ile rekabet edebilir düzeyde olduğu görülmektedir.

Önerilen ikinci algoritma DOPÇ’de, yeni bir değişken adımlı permütasyon yaklaşımı önerilmiştir. Tez çalışmasında ardışık iki permütasyon adımı şeklinde uygulanan şifreleme çatısı bütün adımları tek bir görüntü gezintisi içerisinde gerçekleştirerek hem mühendislik hem de zaman karmaşıklığı bakımından temiz kod (clean code) bir yaklaşım sunmaktadır. Algoritmanın zaman karmaşıklığının $O(MxN)$ olmasıyla verimlilik açısından hafif sıklet kategorisinde öne çıkmaktadır. Ayrıca algoritma sonuçlarından entropi, NPCR ve UACI değerlerinde ideal değerlerden sırasıyla 0,0007, 0,0021 ve 0,0068 sapma göstermiştir. Zaman karmaşıklığı ile elde edilen sonuçlar birlikte değerlendirildiğinde önerilen çerçevenin hafif sıklet görüntü şifreleme kategorisindeki etkinliği görülmüştür.

Sonuç olarak bu tez çalışmasında hafif sıklet görüntü şifreleme kategorisinde iki farklı verimli yaklaşım önerilmiştir. Her iki yaklaşım değerlendirme metrik sonuçları ve benzer algoritmalar ile kıyaslama raporları sunulmuş ve her iki algoritmanın yüksek verimlilik sunan alternatif şifreleme şemaları olduğu gösterilmiştir.

Tez çerçevesinde geliştirilmiş olan KGA ve DOPÇ algoritmaları ileriki süreçlerde geliştirilerek güvenlik analizleri ile şifreleme bakımından daha güçlü algoritmaların elde edilmesi hedeflenmektedir. Mevcut görüntü şifreleme algoritmalar ile kıyaslanmasını sağlamak amacıyla data platformlarında paylaşılarak geliştirilmesi hedeflenmektedir.

REFERANSLAR

Abbas, N. A. (2016). Image encryption based on Independent Component Analysis and Arnold's Cat Map. *Egyptian Informatics Journal*, *17*(1), 139–146. https://doi.org/10.1016/j.eij.2015.10.001

Abou elazm, L. A., Ibrahim, S., Egila, M. G., Shawky, H., Elsaid, M. K. H., El-Shafai, W., & Abd El-Samie, F. E. (2020). Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. *Multimedia Tools and Applications*, *79*(19–20), 14053–14078. https://doi.org/10.1007/s11042-019-08462-8

Abuturab, M. R. (2024). Multiple single - channel cryptosystem based on QZ decomposition , CMYK color space fusion and wavelength multiplexing. *Optical and Quantum Electronics*, *56*(3), 1–22. https://doi.org/10.1007/s11082-023-06001-2

Ahmad, J. (2015). An Efficient Image Encryption Scheme Based on : Henon Map , Skew Tent Map and S-Box. *2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*, 1–6. https://doi.org/10.1109/ICMSAO.2015.7152261

Aihara, K., & Suzuki, H. (2010). Theory of hybrid dynamical systems and its applications to biological and medical systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *368*(1930), 4893–4914. https://doi.org/10.1098/rsta.2010.0237

Akhavan, A., Samsudin, A., & Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm based on DNA encoding. *Optics and Laser Technology*, *95*, 94–99. https://doi.org/10.1016/j.optlastec.2017.04.022

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys and Tutorials*, *22*(3), 1646–1685. https://doi.org/10.1109/COMST.2020.2988293

Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications*, *78*(23), 32633–32657. https://doi.org/10.1007/s11042-018-6801-z

Alghamdi, Y., Munir, A., & Ahmad, J. (2022). A Lightweight Image Encryption

Algorithm Based on Chaotic Map and Random Substitution. *Entropy*, *24*(10), 1–25. https://doi.org/10.3390/e24101344

Almeida (2016). *an Intelligent Selection System Development for the Use of*. *2*, 18–28.

Amina, Y., Bekkouche, T., Daachi, M. E. H., & Diffellah, N. (2024). A novel trigonometric 3D chaotic map and its application in a double permutation-diffusion image encryption. *Multimedia Tools and Applications*, *83*(3), 7895–7918. https://doi.org/10.1007/s11042-023-15858-0

Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocessors and Microsystems*, *80*(September 2020). https://doi.org/10.1016/j.micpro.2020.103301

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Awrejcewicz, J., Krysko, A. V., Papkova, I. V., & Krysko, V. A. (2012). Routes to chaos in continuous mechanical systems. Part 3: The Lyapunov exponents, hyper, hyper-hyper and spatial-temporal chaos. *Chaos, Solitons and Fractals*, *45*(6), 721–736. https://doi.org/10.1016/j.chaos.2012.02.002

Aziz, T., & Haq, E. (2018). Security Challenges Facing IoT Layers and its Protective Measures. *International Journal of Computer Applications*, *179*(27), 31–35. https://doi.org/10.5120/ijca2018916607

Baeza, I., Verdoy, J. A., Villanueva-Oller, J., & Villanueva, R. J. (2009). ROI-based procedures for progressive transmission of digital images: A comparison. *Mathematical and Computer Modelling*, *50*(5–6), 849–859. https://doi.org/10.1016/j.mcm.2009.05.014

Bakker, F. C., Klijn, C. J. M., Jennekens-Schinkel, A., Van Der Tweel, I., Tulleken, C. A. F., & Kappelle, L. J. (2003). Cognitive impairment in patients with carotid artery occlusion and ipsilateral transient ischemic attacks. *Journal of Neurology*, *250*(11), 1340–1347. https://doi.org/10.1007/s00415-003-0222-1

Bembe, M., Abu-Mahfouz, A., Masonta, M., & Ngqondi, T. (2019). A survey on low-power wide area networks for IoT applications. *Telecommunication Systems*, *71*(2), 249–274. https://doi.org/10.1007/s11235-019-00557-9

Benazer, S. S., Dawood, M. S., Ramanathan, S. K., & Saranya, G. (2021). Efficient model for IoT based railway crack detection system. *Materials Today: Proceedings*, *45*, 2789–2792. https://doi.org/10.1016/j.matpr.2020.11.743

Bhatia, A., Goyal, N., Yadav, J., & Jain, E. (2017). Internet of Things (IOT): Confronts and Applications. *SJ Impact Factor:6*, *887*(Viii), 1226–1231. www.ijraset.com1226

Bhowmik, S., & Acharyya, S. (2023). Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm. *Journal of Information Security and Applications*, *72*(December 2022), 103391. https://doi.org/10.1016/j.jisa.2022.103391

Bourekouche, H., Belkacem, S., & Messaoudi, N. (2024). *Lightweight Medical Image Encrypting and Decrypting Algorithm Based on the 3D Intertwining Logistic Map*. *6*(2), 46–62.

Bukhari, S., Arif, M. S., Anjum, M. R., & Dilbar, S. (2017). Enhancing security of images by Steganography and Cryptography techniques. *2016 6th International Conference on Innovative Computing Technology, INTECH 2016*, 531–534. https://doi.org/10.1109/INTECH.2016.7845050

Buyukcolak, O. S. (2019). Simultaneous Image Encryption and Compression Using Modified Huffman Tables. *Proceedings - 2019 7th International Conference on Digital Information Processing and Communications, ICDIPC 2019*, 47–51. https://doi.org/10.1109/ICDIPC.2019.8723751

Callebaut, G., Leenders, G., Van Mulders, J., Ottoy, G., De Strycker, L., & Van der Perre, L. (2021). The art of designing remote iot devices—technologies and strategies for a long battery life. *Sensors (Switzerland)*, *21*(3), 1–37. https://doi.org/10.3390/s21030913

Cao, F., Huang, H. K., & Zhou, X. Q. (2003). Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics*, *27*(2–3), 185–196. https://doi.org/10.1016/S0895-6111(02)00073-3

Cao, Y. (2013). A new hybrid chaotic map and its application on image encryption and hiding. *Mathematical Problems in Engineering*, *2013*. https://doi.org/10.1155/2013/728375

Capra, M., Peloso, R., Masera, G., Roch, M. R., & Martina, M. (2019). Edge computing:

A survey on the hardware requirements in the Internet of Things world. *Future Internet*, *11*(4), 1–25. https://doi.org/10.3390/fi11040100

Carter, B., & Magoc, T. (2007). Classical Ciphers and Cryptanalysis. *Space*, *1000*, 1–10.

Chahal, R. K., Kumar, N., & Batra, S. (2020). Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Computer Communications*, *150*(September 2019), 13–46. https://doi.org/10.1016/j.comcom.2019.10.034

Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in Engineering*, *88*, 197–213. https://doi.org/10.1016/j.optlaseng.2016.08.009

Chai, X., Gan, Z., Yang, K., Chen, Y., & Liu, X. (2017). An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Processing: Image Communication*, *52*(December 2016), 6–19. https://doi.org/10.1016/j.image.2016.12.007

Chelliah, B., Subramanian, S., & Subbiah, G. (2013). High payload image steganography with reduced distortion using octonary pixel pairing scheme. *Multimedia Tools and Applications*, *73*, 2223–2245. https://doi.org/10.1007/s11042-013-1640-4

Chen, W. Bin, & Zhang, X. (2009). Image encryption algorithm based on henon chaotic system. *Proceedings of 2009 International Conference on Image Analysis and Signal Processing, IASP 2009*, 94–97. https://doi.org/10.1109/IASP.2009.5054653

Chen, Jialun, Chen, L., Lin, S., Liu, C., & Cheung, P. C. K. (2015). Preparation and structural characterization of a partially depolymerized beta-glucan obtained from Poria cocos sclerotium by ultrasonic treatment. *Food Hydrocolloids*, *46*, 1–9. https://doi.org/10.1016/j.foodhyd.2014.12.005

Chen, Junxin, Chen, L., & Zhou, Y. (2020). Cryptanalysis of a DNA-based image encryption scheme. *Information Sciences*, *520*, 130–141. https://doi.org/10.1016/j.ins.2020.02.024

Chen, Q., & Lv, X. (2024). Designing a novel image encryption algorithm based on a 2D - SCLC hyperchaotic map. *Multimedia Tools and Applications*, *0123456789*. https://doi.org/10.1007/s11042-023-17755-y

Chua, L. O., Wu, C. W., Huang, A., & Zhong, G. Q. (1993). A Universal Circuit for Studying and Generating Chaos—Part II: Strange Attractors. *IEEE Transactions on*

Circuits and Systems I: Fundamental Theory and Applications, *40*(10), 745–761. https://doi.org/10.1109/81.246150

Cohen, A. J., & Handy, N. C. (2001). Dynamic correlation. *Molecular Physics*, *99*(7), 607–615. https://doi.org/10.1080/00268970010023435

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks*, *144*, 17–39. https://doi.org/10.1016/j.comnet.2018.07.017

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., Kalker, T., Jones, W. P., Witten, I. H., Gori, M. (2013), & Numerico, T. (2008). *and Steganography The Morgan Kaufmann Series in Multimedia Information and Systems*.

Dachlan (2014). Arnold's cat map: an exposition Geneva. *Angewandte Chemie International Edition, 6(11), 951–952.*, 22–31.

DeMaria, A. N. (2003). A structure for deoxyribose nucleic acid. *Journal of the American College of Cardiology*, *42*(2), 373–374. https://doi.org/10.1016/S0735-1097(03)00800-3

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight Cryptography: A Solution to Secure IoT. In *Wireless Personal Communications* (Vol. 112, Issue 3). Springer US. https://doi.org/10.1007/s11277-020-07134-3

Dua, M., Wesanekar, A., Gupta, V., Bhola, M., & Dua, S. (2020). Differential evolution optimization of intertwining logistic map-DNA based image encryption technique. *Journal of Ambient Intelligence and Humanized Computing*, *11*(9), 3771–3786. https://doi.org/10.1007/s12652-019-01580-z

Dwivedi, A. D., & Srivastava, G. (2023). Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK. *Internet of Things (Netherlands)*, *21*(December 2022), 100677. https://doi.org/10.1016/j.iot.2022.100677

Electronics, R. R. T. (2023). *Image Encryption Using Imitating Jigsaw Method*. *14*(05), 700–708.

Es-sabry, M., El, N., Khrissi, L., Satori, K., El-shafai, W., Altameem, T., & Singh, R. (2024). An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers. *Egyptian Informatics Journal*, *25*(January), 100449. https://doi.org/10.1016/j.eij.2024.100449

Essaid, M., Akharraz, I., Saaidi, A., & Mouhib, et A. (2019). Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps. *Journal of Information Security and Applications*, *47*, 173–187. https://doi.org/10.1016/j.jisa.2019.05.006

Fan, W., Li, T., Wu, J., & Wu, J. (2023). *Chaotic Color Image Encryption Based on Eight-Base DNA-Level Permutation and Diffusion*.

Farrukh, Y. A., Wali, S., Khan, I., & Bastian, N. D. (2023). SeNet-I: An approach for detecting network intrusions through serialized network traffic images. *Engineering Applications of Artificial Intelligence*, *126*(PD), 107169. https://doi.org/10.1016/j.engappai.2023.107169

Fetteha, M. A., Sayed, W. S., & Said, L. A. (2023). A Lightweight Image Encryption Scheme Using DNA Coding and Chaos. *Electronics (Switzerland)*, *12*(24), 1–15. https://doi.org/10.3390/electronics12244895

Gaffar, A. F. O., Malani, R., & Putra, A. B. W. (2020). Magic cube puzzle approach for image encryption. *International Journal of Advances in Intelligent Informatics*, *6*(3), 290–302. https://doi.org/10.26555/ijain.v6i3.422

Gangadhar, Y., Giridhar Akula, V. S., & Reddy, P. C. (2018). An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. *Biomedical Signal Processing and Control*, *43*, 31–40. https://doi.org/10.1016/j.bspc.2018.02.007

Gao, H., Zhang, Y., Liang, S., & Li, D. (2006). *A new chaotic algorithm for image encryption*. *29*, 393–399. https://doi.org/10.1016/j.chaos.2005.08.110

Geetha, S., Kabilan, V., Chockalingam, S. P., & Kamaraj, N. (2011). Varying radix numeral system based adaptive image steganography. *Information Processing Letters*, *111*(16), 792–797. https://doi.org/10.1016/j.ipl.2011.05.013

Gökmen A. (2009). Kaos Teorisinin Genel Değelendirmesi. *Hitit Üniversitesi Sosyal Bilimler Dergisi*, *2*(2), 61–77.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Gündüz, M. Z., & Daş, R. (2022). Kişisel Siber Güvenlik Yaklaşımlarının

Değerlendirilmesi. *DÜMF Mühendislik Dergisi*, *3*, 429–438. https://doi.org/10.24012/dumf.1122997

Hariyanto, E., & Rahim, R. (2013). Arnold's Cat Map Algorithm in Digital Image Encryption. *International Journal of Science and Research*, *5*(10), 2319–7064. https://doi.org/10.21275/ART20162488

Hermann, D., Gildas, G. G., Fouda, J. S. A. E., & Koepf, W. (2022). On the implementation of large period piece-wise linear Arnold cat map. *Multimedia Tools and Applications*, *81*(27), 39003–39020. https://doi.org/10.1007/s11042-022-13175-6

Himthani, V., Dhaka, V. S., Kaur, M., Singh, D., & Lee, H.-N. (2022). Systematic Survey on Visually Meaningful Image Encryption Techniques. *IEEE Access*, *10*, 98360–98373. https://doi.org/10.1109/ACCESS.2022.3203173

Holland J. H. (1975). *Adaptation in Natural and Artificial Systems, University of Michigan Press*.

Hua, Z., Yi, S., & Zhou, Y. (2018). Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Processing*, *144*, 134–144. https://doi.org/10.1016/j.sigpro.2017.10.004

Hwang, H. (2012). Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain. *OPTICS*, *285*(5), 567–573. https://doi.org/10.1016/j.optcom.2011.11.007

Hwang, H. E. (2012). Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain. *Optics Communications*, *285*(5), 567–573. https://doi.org/10.1016/j.optcom.2011.11.007

Iera, A., Floerkemeier, C., Mitsugi, J., & Morabito, G. (2010). The Internet of things. *IEEE Wireless Communications*, *17*(6), 8–9. https://doi.org/10.1109/MWC.2010.5675772

Ince, C., İnce, K., & Hanbay, D. (2024). Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices. *Multimedia Tools and Applications*, *0123456789*. https://doi.org/10.1007/s11042-024-18620-2

Ince C., Ince, K., & Hanbay, D. (2021). Randomness Analysis With Runge Kutta Methods. *Computer Science*. https://doi.org/10.53070/bbd.990990

Ince, K. (2023). Exploring the potential of deep learning and machine learning techniques

for randomness analysis to enhance security on IoT. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00783-y

Jamgekar, R. S., & Joshi, G. S. (2013). File Encryption and Decryption Using Secure RSA. *International Journal of Emerging Science and Engineering (IJESE)*, *1*(4), 11–14.

Javadikasgari, H., Soltesz, E. G., & Gillinov, A. M. (2019). Chapter 28 - Surgery for Atrial Fibrillation. In F. W. Sellke & M. Ruel (Eds.), *Atlas of Cardiac Surgical Techniques (Second Edition)* (Second Edi, pp. 479–488). Elsevier. https://doi.org/https://doi.org/10.1016/B978-0-323-46294-5.00028-5

Jiang, X., Xie, Y., Liu, B., Chai, J., Ye, Y., Song, T., Feng, M., & Yuan, H. (2023). Image encryption based on actual chaotic mapping using optical reservoir computing. *Nonlinear Dynamics*, *111*(16), 15531–15555. https://doi.org/10.1007/s11071-023-08666-6

Kansal, S., & Mittal, M. (2014). Performance evaluation of various symmetric encryption algorithms. *Proceedings of 2014 3rd International Conference on Parallel, Distributed and Grid Computing, PDGC 2014*, 105–109. https://doi.org/10.1109/PDGC.2014.7030724

Kaur, H., & Kakkar, A. (2017). Comparison of different image formats using LSB Steganography. *4th IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2017*, *2017-Janua*, 97–101. https://doi.org/10.1109/ISPCC.2017.8269657

Kaur, M., Singh, S., Kaur, M., Singh, A., & Singh, D. (2022). A Systematic Review of Metaheuristic-based Image Encryption Techniques. *Archives of Computational Methods in Engineering*, *29*(5), 2563–2577. https://doi.org/10.1007/s11831-021-09656-w

Kengnou Telem, A. N., Feudjio, C., Ramakrishnan, B., Fotsin, H. B., & Rajagopal, K. (2022). A Simple Image Encryption Based on Binary Image Affine Transformation and Zigzag Process. *Complexity*, *2022*. https://doi.org/10.1155/2022/3865820

Khan, R., & Mian, A. N. (2020). Sustainable IoT sensing applications development through graphQL-based abstraction layer. *Electronics (Switzerland)*, *9*(4), 1–23. https://doi.org/10.3390/electronics9040564

Kim, A., Miller, K., Jo, J., Kilimnik, G., Wojcik, P., & Hara, M. (2009). Islet architecture:

A comparative study. *Islets*, *1*(2), 129–136. https://doi.org/10.4161/isl.1.2.9480

Kocak, O., Erkan, U., Toktas, A., & Gao, S. (2024). PSO-based image encryption scheme using modular integrated logistic exponential map. *Expert Systems with Applications*, *237*(May 2023). https://doi.org/10.1016/j.eswa.2023.121452

Kolivand, H., Hamood, S. F., Asadianfam, S., & Rahim, M. S. (2024). Image encryption techniques: A comprehensive review. In *Multimedia Tools and Applications* (Issue 0123456789). Springer US. https://doi.org/10.1007/s11042-023-17896-0

Kumari, D., Parmar, A. S., Goyal, H. S., Mishra, K., & Panda, S. (2024). HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data. *Computer Networks*, *241*(March 2023), 110223. https://doi.org/10.1016/j.comnet.2024.110223

Li, H., Hu, Y., Shi, Z., Wang, B., & Zheng, P. (2022). An Image Encryption Algorithm Based on Improved Lifting-Like Structure and Cross-Plane Zigzag Transform. *IEEE Access*, *10*(August), 82305–82318. https://doi.org/10.1109/ACCESS.2022.3194730

Li, S., Zhao, L., & Yang, N. (2021). Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/6624809

Li, X., Wang, L., Yan, Y., & Liu, P. (2016). An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. *Optik*, *127*(5), 2558–2565. https://doi.org/10.1016/j.ijleo.2015.11.221

Li, Y., Wang, W., Zhou, J., Chen, H., & Zhang, P. (2017). 10B areal density: A novel approach for design and fabrication of B4C/6061Al neutron absorbing materials. *Journal of Nuclear Materials*, *487*, 238–246. https://doi.org/10.1016/j.jnucmat.2017.02.020

Li, Z., Peng, C., Tan, W., & Li, L. (2021). *An Effective Chaos-Based Image Encryption Scheme Using Imitating Jigsaw Method*. *2021*.

Lin, W., Qiao, N., & Yuying, H. (2006). Bifurcations and chaos in a forced cantilever system with impacts. *Journal of Sound and Vibration*, *296*(4–5), 1068–1078. https://doi.org/10.1016/j.jsv.2006.03.015

Liu, G., Xie, H., Wang, W., & Huang, H. (2024). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. *Journal of*

Cloud Computing, *13*(1). https://doi.org/10.1186/s13677-024-00608-w

Liu, H., & Nan, H. (2013). Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform. *Optics and Laser Technology*, *50*, 1–7. https://doi.org/10.1016/j.optlastec.2013.02.003

Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., & Liu, S. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Optics Communications*, *284*(1), 123–128. https://doi.org/10.1016/j.optcom.2010.09.013

Ma, S., Zhang, Y., Yang, Z., Hu, J., & Lei, X. (2019). A New Plaintext-Related Image Encryption Scheme Based on Chaotic Sequence. *IEEE Access*, *7*, 30344–30360. https://doi.org/10.1109/ACCESS.2019.2901302

Madushanka, T., Kumara, D. S., & Rathnaweera, A. (2024). SecureRights: A Blockchain-Powered Trusted DRM Framework for Robust Protection and Asserting Digital Rights. http://arxiv.org/abs/2403.06094

Mali, K., Chakraborty, S., & Roy, M. (2015). A Study on Statistical Analysis and Security Evaluation Parameters in Image Encryption. *IJSRD-International Journal for Scientific Research & Development*|, *3*(08), 2321–0613. www.ijsrd.com

Mao, Y., Chen, G., & Lian, S. (2004). A novel fast image encryption scheme based on 3D chaotic baker maps. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, *14*(10), 3613–3624. https://doi.org/10.1142/S021812740401151X

Mardon, A., Barara, G., Chana, I., Di Martino, A., Falade, I., Harun, R., Hauser, A., Johnson, J., Li, A., Pham, J., & Varghese, N. (2021). *Cryptography online*.

Maver, D. (2011). Criminalistics in Slovenia: an Overview of Research. In *International sceintific conference "'Archibald Reiss days.'"*

Mckay, K. A., & Cooper, D. A. (2001). *Withdrawn NIST Technical Series Publication*. *2001*, 27–28.

Mishra, M. (2012). Image Encryption Using Fibonacci-Lucas Transformation. *International Journal on Cryptography and Information Security*, *2*(3), 131–141. https://doi.org/10.5121/ijcis.2012.2312

Mondal, B., & Singh, J. P. (2022). A lightweight image encryption scheme based on chaos

and diffusion circuit. *Multimedia Tools and Applications*, *81*(24), 34547–34571. https://doi.org/10.1007/s11042-021-11657-7

Noshadian, S., Ebrahimzade, A., & Kazemitabar, S. J. (2018). Optimizing chaos based image encryption. *Multimedia Tools and Applications*, *77*(19), 25569–25590. https://doi.org/10.1007/s11042-018-5807-x

Ott, E. (1993). *Chaos in Dynamical Systems. CUP, Cambridge.* https://10.1017/CB09780511803260.

Ouedraogo, C. A., Medjiah, S., Chassot, C., Drira, K., & Aguilar, J. (2021). A Cost-Effective Approach for End-to-End QoS Management in NFV-Enabled IoT Platforms. *IEEE Internet of Things Journal*, *8*(5), 3885–3903. https://doi.org/10.1109/JIOT.2020.3025500

Pehlivan, İ. (2007). *Yenİ Kaotik Sistemler : Elektronik Devre Gerçeklemeleri , Senkroni Zasyon Ve Güvenliği*. 19.

Petrellis, N., Birbas, M., & Gioulekas, F. (2019). On the design of low-cost IoT sensor node for e-health environment. *Electronics (Switzerland)*, *8*(2). https://doi.org/10.3390/electronics8020178

Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Arshad, Masood, F., Khan, F., & Buchanan, W. J. (2020). Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution. *IEEE Access*, *8*, 140876–140895. https://doi.org/10.1109/ACCESS.2020.3012912

Rahmani, A. M., Bayramov, S., & Kiani Kalejahi, B. (2022). Internet of Things Applications: Opportunities and Threats. *Wireless Personal Communications*, *122*(1), 451–476. https://doi.org/10.1007/s11277-021-08907-0

Rajashree, S., Gajkumar Shah, P., & Murali, S. (2018). Security Model for Internet of Things End Devices. *Proceedings - IEEE 2018 International Congress on Cybermatics*, 219–221. https://doi.org/10.1109/Cybermatics_2018.2018.00066

Rauscher, J., & Bauer, B. (2018). Safety and security architecture analyses framework for the internet of things of medical devices. *2018 IEEE 20th International Conference on E-Health Networking, Applications and Services, Healthcom 2018*, 1–3. https://doi.org/10.1109/HealthCom.2018.8531121

Rejewski, M. (1982). Mathematical solution of the enigma cipher. *Cryptologia*, *6*(1), 1–18.

https://doi.org/10.1080/0161-118291856731

Samie, F., Tsoutsouras, V., Bauer, L., Xydis, S., Soudris, D., & Henkel, J. (2016). Computation offloading and resource allocation for low-power IoT edge devices. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 7–12. https://doi.org/10.1109/WF-IoT.2016.7845499

Sani, M. S., Iranmanesh, S., Salarian, H., Raad, R., & Jamalipour, A. (2024). BIDS: Blockchain-Enabled Intrusion Detection System in Smart Cities. *IEEE Internet of Things Magazine*, *7*(2), 107–113. https://doi.org/10.1109/iotm.001.2300191

Sayed, W. S., & Radwan, A. G. (2020). International Journal of Electronics and Communications (AEÜ) Generalized switched synchronization and dependent image encryption using dynamically rotating fractional-order chaotic systems. *AEUE - International Journal of Electronics and Communications*, *123*, 153268. https://doi.org/10.1016/j.aeue.2020.153268

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*. https://doi.org/10.1155/2017/9324035

Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., Susanto, A., & Doheir, M. (2018). A Comparative Study of Image Cryptographic Method. *Proceedings - 2018 5th International Conference on Information Technology, Computer and Electrical Engineering, İcitacee 2018*, 336–341. https://doi.org/10.1109/ICITACEE.2018.8576907

Shafique, A., Ahmed, J., Rehman, M. U., & Hazzazi, M. M. (2021). Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain. *IEEE Access*, *9*, 59108–59130. https://doi.org/10.1109/ACCESS.2021.3071535

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, *27*(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Shao, Z., Shu, H., Wu, J., Dong, Z., Coatrieux, G., & Coatrieux, J. L. (2014). Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain. *Optics Express*, *22*(5), 4932. https://doi.org/10.1364/oe.22.004932

Shashikiran, B. S., Shaila, K., & Venugopal, K. R. (2021). Minimal Block Knight's Tour

and Edge with LSB Pixel Replacement Based Encrypted Image Steganography. *SN Computer Science*, *2*(3), 1–9. https://doi.org/10.1007/s42979-021-00542-7

Shini, S. G., Thomas, T., & Chithraranjan, K. (2012). Cloud based medical image exchange-security challenges. *Procedia Engineering*, *38*, 3454–3461. https://doi.org/10.1016/j.proeng.2012.06.399

Shiryaev, B. (2012). *Kolmogorov : Life and Creative Activities Author (s): A . N . Shiryaev Reviewed work (s): Source : The Annals of Probability , Vol . 17 , No . 3 (Jul ., 1989), pp . 866-944*

Simmons, G. J. (1979). Symmetric and Asymmetric Encryption. *ACM Computing Surveys (CSUR)*, *11*(4), 305–330. https://doi.org/10.1145/356789.356793

Singh, M., Kakkar, A., & Singh, M. (2015). Image Encryption Scheme Based on Knight's Tour Problem. *Procedia Computer Science*, *70*, 245–250. https://doi.org/10.1016/j.procs.2015.10.081

Smith, A. R. (1995). A pixel is not a little square. *Pixar Technical Memo*, *6*, 1–11.

Society, A. P., & Society, A. P. (2010). *Blaise de Vigenère and the " Chiffre Carré " Author (s): Charles J . Mendelsohn Published by : American Philosophical Society Stable .* *82*(2), 103–129.

Solachidis, V., & Pitas, I. (2001). Circularly symmetric watermark embedding in 2-D DFT domain. *IEEE Transactions on Image Processing*, *10*(11), 1741–1753. https://doi.org/10.1109/83.967401

Sui, L., Duan, K., & Liang, J. (2015). Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. *Optics Communications*, *343*, 140–149. https://doi.org/10.1016/j.optcom.2015.01.021

Suri, S., & 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. https://doi.org/10.1007/s12652-018-0825-0

Susanto, A., Setiadi, D. R. I. M., Rachmawanto, E. H., Mulyono, I. U. W., Sari, C. A., Sarker, M. K., & Sazal, M. R. (2020). Triple layer image security using bit-shift, chaos, and stream encryption. *Bulletin of Electrical Engineering and Informatics*, *9*(3), 980–987. https://doi.org/10.11591/eei.v9i3.2001

Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning

algorithm. *Information (Switzerland)*, *11*(5). https://doi.org/10.3390/INFO11050279

Tang, L., Lee, N., & Russo, S. (n.d.). *Breaking Enigma*. 1–15.

Çavuşoğlu Ü. (2016). *Kaos tabanli hibrit simetrik ve asimetrik şifreleme algoritmalari tasarimi ve uygulamasi*.

Thesis, A., & Engineering, E. (1997). *synchronization of chaotic systems by using occasional coupling submitted to the department of electrical and m oez Feki*. *June*.

Tsui, T. K., Zhang, X. P., & Androutsos, D. (2008). Color image watermarking using multidimensional fourier transforms. *IEEE Transactions on Information Forensics and Security*, *3*(1), 16–28. https://doi.org/10.1109/TIFS.2007.916275

Uhl, A., & Pommer, A. (2005). Image and Video Encryption: From Digital Rights Management to Secured Personal Communication. *Advances in Information Security*, *15*. https://doi.org/10.1007/b101495

Umar, T., Nadeem, M., & Anwer, F. (2024). Computer Standards & Interfaces A new modified Skew Tent Map and its application in pseudo-random number generator. *Computer Standards & Interfaces*, *89*(November 2023), 103826. https://doi.org/10.1016/j.csi.2023.103826

Ur, A., Jan, R., & Khan, S. (2020). A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps. *3D Research*, *February 2016*. https://doi.org/10.1007/s13319-016-0084-9

Venkatraman, S., Abraham, A., & Paprzycki, M. (2004). Significance of steganography on data security. *International Conference on Information Technology: Coding Computing, ITCC*, *2*, 347–351. https://doi.org/10.1109/ITCC.2004.1286660

Wang, Jie, & Liu, L. (2022). A Novel Chaos-Based Image Encryption Using Magic Square Scrambling and Octree Diffusing. *Mathematics*, *10*(3). https://doi.org/10.3390/math10030457

Wang, Jingya, Song, X., & El-Latif, A. (2022). Single-Objective Particle Swarm Optimization-Based Chaotic Image Encryption Scheme. *Electronics (Switzerland)*, *11*(16). https://doi.org/10.3390/electronics11162628

Wang, M., Fu, X., Yan, X., & Teng, L. (2024). *A New Chaos-Based Image Encryption Algorithm Based on Discrete Fourier Transform and Improved Joseph Traversal*.

Wang, Xing yuan, Chen, F., & Wang, T. (2010). A new compound mode of confusion and diffusion for block encryption of image based on chaos. *Communications in Nonlinear Science and Numerical Simulation*, *15*(9), 2479–2485. https://doi.org/10.1016/j.cnsns.2009.10.001

Wang, Xingyuan, & Chen, X. (2021). An image encryption algorithm based on dynamic row scrambling and Zigzag transformation. *Chaos, Solitons and Fractals*, *147*, 110962. https://doi.org/10.1016/j.chaos.2021.110962

Wang, Xingyuan, & Guo, K. (2014). A new image alternate encryption algorithm based on chaotic map. *Nonlinear Dynamics*, *76*(4), 1943–1950. https://doi.org/10.1007/s11071-014-1259-7

Wang, Xingyuan, Liu, C., & Zhang, H. (2016). An effective and fast image encryption algorithm based on Chaos and interweaving of ranks. *Nonlinear Dynamics*, *84*(3), 1595–1607. https://doi.org/10.1007/s11071-015-2590-3

Wang, Xingyuan, & Sun, H. (2019). A chaotic image encryption algorithm based on zigzag-like transform and DNA-like coding. *Multimedia Tools and Applications*, *78*(24), 34981–34997. https://doi.org/10.1007/s11042-019-08085-z

Wang, Xingyuan, Wang, Y., Zhu, X., & Unar, S. (2019). Image encryption scheme based on Chaos and DNA plane operations. *Multimedia Tools and Applications*, *78*(18), 26111–26128. https://doi.org/10.1007/s11042-019-07794-9

Wen, H., feng, zhaoyang, Chixin, B., Lin, Y., Zhang, X., & Feng, W. (2024). Frequency-domain image encryption based on IWT and 3D S-box. *Physica Scripta*, *99*. https://doi.org/10.1088/1402-4896/ad30ec

Wen, J., Feng, Y., Tao, X., & Cao, Y. (2021). Dynamical Analysis of a New Chaotic System: Hidden Attractor, Coexisting-Attractors, Offset Boosting, and DSP Realization. *IEEE Access*, *9*, 167920–167927. https://doi.org/10.1109/ACCESS.2021.3136249

Wu, W., Chen, Z., & Yuan, Z. (2009). The evolution of a novel four-dimensional autonomous system: Among 3-torus, limit cycle, 2-torus, chaos and hyperchaos. *Chaos, Solitons and Fractals*, *39*(5), 2340–2356. https://doi.org/10.1016/j.chaos.2007.07.016

Wu, X., Wang, D., Kurths, J., & Kan, H. (2016). A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Information Sciences*, *349–350*,

137–153. https://doi.org/10.1016/j.ins.2016.02.041

Wu, Y., Member, S., Noonan, J. P., & Member, L. (2014). *NPCR and UACI Randomness Tests for Image Encryption*. *April 2011*.

Xiong, G., Zheng, S., Wang, J., Cai, Z., & Qi, D. (2018). Local Negative Base Transform and Image Scrambling. *Mathematical Problems in Engineering*, *2018*. https://doi.org/10.1155/2018/8087958

Xu, H., Tong, X., & Meng, X. (2016). An efficient chaos pseudo-random number generator applied to video encryption. *Optik*, *127*(20), 9305–9319. https://doi.org/10.1016/j.ijleo.2016.07.024

Xu, L., Li, Z., Li, J., & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering*, *78*, 17–25. https://doi.org/10.1016/j.optlaseng.2015.09.007

Yadav, P. K., & Prajapati, N. L. (2012). An Overview of Genetic Algorithm and Modeling. *International Journal of Scientific and Research Publications*, *2*(9), 1–4.

Yang, X., Zhang, K., Jia, K., & Zhao, P. (2024). A personalized and efficient EMR sharing and management scheme based on smart contracts. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-024-01669-z

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., & Mardini, W. (2017). *Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms*.

Yingbing, Z., & Yongzhen, L. (2014). The design and implementation of a symmetric encryption algorithm based on des. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, 517–520. https://doi.org/10.1109/ICSESS.2014.6933619

Yoshida, T., Mori, H., & Shigematsu, H. (1983). Analytic study of chaos of the tent map: Band structures, power spectra, and critical behaviors. *Journal of Statistical Physics*, *31*(2), 279–308. https://doi.org/10.1007/BF01011583

Yu, F., Shen, H., Yu, Q., Kong, X., Sharma, P. K., & Cai, S. (2023). Privacy Protection of Medical Data Based on Multi-Scroll Memristive Hopfield Neural Network. *IEEE Transactions on Network Science and Engineering*, *10*(2), 845–858. https://doi.org/10.1109/TNSE.2022.3223930

Zeadally, S., Shaikh, F. K., Talpur, A., & Sheng, Q. Z. (2020). Design architectures for

energy harvesting in the Internet of Things. *Renewable and Sustainable Energy Reviews*, *128*(April), 109901. https://doi.org/10.1016/j.rser.2020.109901

Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics*, *11*(11). https://doi.org/10.3390/math11112585

Zhang, H., & Hu, H. (2024). An image encryption algorithm based on a compound-coupled chaotic system. *Digital Signal Processing*, *146*, 104367. https://doi.org/10.1016/j.dsp.2023.104367

Zhang, H., Hu, H., & Ding, W. (2024). VSDHS-CIEA : Color image encryption algorithm based on novel variable-structure discrete hyperchaotic system and cross-plane confusion strategy. *Information Sciences*, *665*(February), 120332. https://doi.org/10.1016/j.ins.2024.120332

Zhang, Q. Y., Wu, G. R., Yang, R., & Chen, J. Y. (2024). Digital image copyright protection method based on blockchain and zero trust mechanism. In *Multimedia Tools and Applications* (Issue 0123456789). Springer US. https://doi.org/10.1007/s11042-024-18514-3

Zhang, X., Liu, M., Tian, J., & Gong, Z. (2022). Color Image Encryption Algorithm Based on Dynamic Block Zigzag Transformation and Six-Sided Star Model. *Electronics (Switzerland)*, *11*(16). https://doi.org/10.3390/electronics11162512

Zhang, X., Liu, M., & Yang, X. (2023). Color Image Encryption Algorithm Based on Cross-Spiral Transformation and Zone Diffusion. *Mathematics*, *11*(14), 3228. https://doi.org/10.3390/math11143228

Zhang, Y. (2018). The image encryption algorithm based on chaos and DNA computing. *Multimedia Tools and Applications*, *77*(16), 21589–21615. https://doi.org/10.1007/s11042-017-5585-x

Zhou, G., Zhang, D., Liu, Y., Yuan, Y., & Liu, Q. (2015). Neurocomputing A novel image encryption algorithm based on chaos and Line map. *Neurocomputing*, *169*, 150–157. https://doi.org/10.1016/j.neucom.2014.11.095

Zhou, J., Zhou, N., & Gong, L. (2020). Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix. *Optics and Laser Technology*, *131*(July), 106437. https://doi.org/10.1016/j.optlastec.2020.106437

Zhou, N., Hu, L., Huang, Z., Wang, M., & Luo, G. (2024). Novel multiple color images

encryption and decryption scheme based on a bit-level extension algorithm. *Expert Systems With Applications*, *238*(PC), 122052. https://doi.org/10.1016/j.eswa.2023.122052

Zhou, X., Li, J., & Ma, Y. (2012). Chaos phenomena in DC-DC converter and chaos control. *Procedia Engineering*, *29*, 470–473. https://doi.org/10.1016/j.proeng.2011.12.744

Zhou, Y., Cao, W., & Philip Chen, C. L. (2014). Image encryption using binary bitplane. *Signal Processing*, *100*, 197–207. https://doi.org/10.1016/j.sigpro.2014.01.020

ÖZGEÇMİŞ

Ad Soyad **:** Cemile İNCE

ÖĞRENİM DURUMU

Lisans **:**Fırat Üniversitesi Mühendislik Fakütesi Bilgisayar Mühendisliği, 2009

Yüksek Lisans **:**Munzur Üniversitesi Mühendislik Fakültesi Elektrik Elektronik Mühendisliği, 2019

Doktora **:**İnönü Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Donanım Anabilim Dalı, 2024

MESLEKİ DENEYİM

2009-2010 Tunceli Üniversitesi Bilgi İşlem Daire Başkanlığı, Bilgisayar Mühendisi

2010-2012 İnönü Üniversitesi Bilgi İşlem Daire Başkanlığı, Bilgisayar Mühendisi

2012-2013 İnönü Üniversitsi Uzaktan Eğitim Uygulama ve Araştırma Merkezi, Bilgisayar Mühendisi

2014-2021 İnönü Üniversitesi Bilgi İşlem Daire Başkanlığı, Bilgisayar Mühendisi

2021-Devam İnönü Üniversitesi Uzaktan Eğitim Uygulama ve Araştırma Merkezi, Bilgisayar Mühendisi

TEZDEN ÜRETİLEN YAYINLAR / SUNUMLAR

1. İnce, C., İnce, K. & Hanbay, D. Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices. *Multimed Tools Appl* (2024). https://doi.org/10.1007/s11042-024-18620-2
2. İnce, C., İnce, K. & Hanbay, D. A Multilayer Permutation Framework for Lightweight Image Encryption. (2024) (In review)
3. İnce, K., İnce, C. & Hanbay, D. RSP: A novel lightweight image encryption framework for IoT devices based on color planes stripe permutation (2024). (In review)

4. İnce, C., İnce, K. & Hanbay, D. (2022). SecureRandom Kütüphanesi Kullanarak Yazılımsal Trivium Oluşturma. *Avrupa Bilim ve Teknoloji Dergisi*, (34), 639-644. DOI:10.31590/ejosat.1084005

5. İnce, C., İnce, K. & Hanbay, D. (2021). Randomness Analysis with Runge Kutta Methods. Computer Science, DOI:10.53070/bbd.990990

6. İnce *Et Al.*, "Saldırı Tespit Sistemlerinde Sınıflandırma Yöntemlerinin Kıyaslanması," *Anatolian Journal of Computer Science*, vol.6, no.1, pp.1-10, 2021

7. 10^{th} Ankara International Congress on ScientificResearch held onJune 25-27,2024/ Ankara, Türkiye with the paper entitled “Multı-layer Nonlınear Permutatıon Framework for Lightweıght İmage Encryption Algorithms”

8. 4^{th} International Conference on Innovatite Academic Studies March 12-13 in 2024 at Konya/Turkey with the paper entitled “A Novel RGB Color Plane Chaotic Scrambling-Based İmage Encryption Algorithm”