FEN BİLİMLERİ ENSTİTÜSÜ

GÖRÜNTÜLER İÇİN KAOTİK ŞİFRELEME SİSTEMİ VE PERFORMANS ANALİZİ

Gizem SEVAL

Danışman
Doç. Dr. Mustafa Cem KASAPBAŞI

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
İSTANBUL - 2023

KABUL VE ONAY SAYFASI

Gizem SEVAL tarafından hazırlanan **"Görüntüler için kaotik şifreleme sistemi ve performans analizi"** adlı tez çalışması 19/01/2023 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Bilgisayar Mühendisliği Anabilim Dalı**'nda **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Danışman	**Doç. Dr. Mustafa Cem KASAPBAŞI** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Doç. Dr. Önder DEMİR** Marmara Üniversitesi	.....
Jüri Üyesi	**Dr. Öğr. Üyesi Ali AKMAN** İstanbul Ticaret Üniversitesi	.....

Onay Tarihi: 27.01.2023

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsünün 27.01.2023 tarih ve 2023/373 numaralı Yönetim Kurulu Kararının 15. maddesi gereğince, ders yüklerini ve tez yükümlülüğünü yerine getirdiği belirlenen "Gizem SEVAL" adlı öğrencinin mezun olmasına oy birliği ile karar verilmiştir.

Prof. Dr. Doğan KAYA
Enstitü Müdürü

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

27.01.2023

Gizem SEVAL

İÇİNDEKİLER

Sayfa

ÖZET

Yüksek Lisans Tezi

GÖRÜNTÜLER İÇİN KAOTİK ŞİFRELEME SİSTEMİ VE PERFORMANS ANALİZİ

Gizem SEVAL

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Mustafa Cem KASAPBAŞI

2023, 45 sayfa

Teknoloji yıllar içinde çok hızlı bir şekilde ilerlemiş ve bu ilerleyişine hızla devam etmektedir. Bu süreçte verilerin güvenliğini sağlama konusu da her alanda önemini arttırmıştır. Bu çalışmada kullanılan veri kaynağı görüntü olarak seçilmiştir. Görüntü şifrelemede histogram, korelasyon, diferansiyel saldırı, anahtar uzay, anahtar hassasiyet, zaman karmaşıklığı, entropi başarı analizleri ve istatiksel analizlere yönelik NIST testleri kullanılmıştır. Tanımlanan analiz ve testler doğrultusunda gerçekleştirilen analiz sonuçları karşılaştırılarak görüntü şifrelemede kullanılan bu yöntemlerin çıktı olarak doğru sonuçları ve beklenen performansları verip vermediği değerlendirilmiştir. Önerilen şifreleme yönteminin çıktı olarak başarılı sonuç ve performansları verdiği gözlemlenmiştir.

Anahtar Kelimeler: Görüntü şifreleme, kaotik, performans analizi.

ABSTRACT

M.Sc. Thesis

CHAOTIC ENCRYPTION SYSTEM FOR IMAGES AND PERFORMANCE ANALYSIS

Gizem SEVAL

Istanbul Commerce University
Graduate School of Applied and Natural Sciences
Department of Computer Engineering

Supervisor: Assoc. Prof. Dr. Mustafa Cem KASAPBAŞI

2023, 45 pages

Technology has progressed very rapidly over the years and this progress continues rapidly. In this process, the issue of ensuring the security of data has increased its importance in every field. The data source used in this study was chosen as an image. In image encryption, histogram, correlation, differential attack, key space, key sensitivity, time complexity, entropy for success analysis and NIST tests for statistical analysis were used. By comparing the analysis results performed in line with the defined analysis and tests, it has been evaluated whether these methods used in image encryption give the correct results and expected performances as output. It has been observed that the proposed encryption method gives successful results and performances as output.

Keywords: Chaotic, image encryption, performance analysis.

TEŞEKKÜR

Çalışma boyunca analizlerin sonuçlarını değerlendirerek makale ve tez yorumlarıyla yardımcı olmasından ötürü tez danışman hocam Doç. Dr. Mustafa Cem KASAPBAŞI'na teşekkür ederim.

Rehberliğiyle bu zamana kadar yol gösteren ve bundan sonrasında da desteğini esirgemeyeceğini düşündüğüm ablam İrem SEVAL'e teşekkür ederim.

Beni yetiştiren, düşünce yapımın ve çalışmalarımın temelde mimarı olan babam Haşmet SEVAL ve annem Nebahat SEVAL'e sonsuz sevgi ve saygılarımı sunarım.

Gizem SEVAL
İSTANBUL, 2023

ŞEKİLLER

Sayfa

ÇİZELGELER

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

AES	Gelişmiş şifreleme standard (Advanced encryption standard)
CPU	Merkezi işlem birimi (Central process unit)
DES	Veri şifreleme standard (Data encryption standard)
H	Uzunluk (Height)
LFSR	Doğrusal geri bildirim kaydırma yazmacı (Linear-feedback shift register)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
NPCR	Piksel sayısı değişim oranı (Number of changing pixel rate)
RGB	Kırmızı, yeşil, mavi (Red, green, blue)
UACI	Birleşik ortalama değişen yoğunluk (Unified averaged changed intensity)
W	Genişlik (Width)

1. GİRİŞ

Verilerin güvenliğinin sağlanması konusunun önem düzeyi teknolojinin hızla gelişmesinin sonucu olarak artış göstermiştir. Şifreleme veri güvenliğinin sağlanmasında kullanılan yöntemlerdir. Önem düzeyine bağlı olarak veriler şifreli olarak kaydedilebilmekte veya aktarılabilmektedir. Son kullanıcılar için ihtiyaç haline gelen şifreleme, verileri okunamaz duruma getirerek korumayı sağlamaktadır. Dolayısıyla verilere yetkisi olan kişiler haricinde kimse erişememekte böylece verilerin hem gizliliği hem de güvenliği sağlanmış olmaktadır. Yetkili kişiler şifre çözme yöntemlerini kullanarak verilere erişim sağlayabilmektedir.

Verilerin şifrelenmesi için en çok kullanılan bazı klasik ve modern şifreleme algoritmaları Vigenere, DES (Data Encryption Standart – Veri Şifreleme Standardı), AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı) RC4, RC5, Blowfish, IDEA olarak örnek verilebilir. (Atalay vd., 2019) (Ceyhan ve Yolaçan, 2021) Verilerin şifrelerinin çözülmesiyse şifre çözme algoritmaları kullanılarak gerçekleştirilmektedir. Bu çalışmada veri kaynağı olarak görüntü seçilmiştir çünkü multimedya kullanımı dijital çağda giderek artmakta ve kullanılan multimedyaların da gizlilik ve güvenliği önemli hale gelmektedir. Görüntü şifrelemelerin görüntüdeki bilgilerin korelasyonlarından dolayı farklı zorlukları vardır.

Bölüm 1'de görüntü şifreleme konusu hakkında gerçekleştirilen çalışmaların literatür taraması yapılmıştır. Bölüm 2'de görüntü şifrelemede kullanılan başarı analizleri tanımlanmıştır. Bölüm 3'te Bölüm 2'de tanımlanan analiz yöntemleri kullanılarak gerçekleştirilen analizlerin sonuçları sunulmuştur. Bölüm 4'te bu çalışmanın sonucunda görüntü şifrelemede kullanılan başarı analizlerinin uygulanmasıyla birlikte performansları değerlendirilerek analizlerin karşılaştırılmaları yapılmıştır.

2. LİTERATÜR ÖZETİ

İnternet üzerinden bilgi aktarımı ses, görüntü ve diğer yollarla sağlanabilmektedir. Bu sebeple bilgilerin aktarım esnasında, bilgilerin saklanması esnasında ya da bilgilere erişim esnasında güvenliklerini sağlamanın önemi artmaktadır. Literatür taraması konusu olarak görüntü şifreleme, görüntü işleme, şifreleme algoritmaları ve şifre çözme algoritmaları hakkında yapılan çalışmalara bu bölümde yer verilmiştir.

Samuel Hartman 2005 yılında yaptığı tez çalışmasında (Hartman, 2005) rastgeleliğe yeni bir bakış açısı yaratan bilim dalı olan kaos teorisini ve evrensel fonksiyon sınıfına göre oluşturulan Mandelbrot kümesini konu olarak ele almıştır. Dinamik davranışlar sergilemeyen bazı kaotik şifreleme sistemlerinin güvenlik açığı olduğu tespit edilmiştir.

Musa Peker yaptığı tez çalışmasında (Peker, 2009) kamera görüntülerinde hareket analizi için kullanılan teknikleri analiz ederek uygulamış ayrıca uygulama sonuçlarını tartışmıştır. Görüntü şifrelemede kullanılan görüntü işleme ve RGB (Kırmızı, yeşil, mavi) konularına değinilmiştir. Kullanılan yöntem basit fark alma olarak adlandırılan hareket tespit segmentasyonudur. Bu segmentasyon koordinatlardaki piksel farklarının eşik değeriyle kıyaslanmasından elde edilen sonuçla belirlenmektedir. Çalışma sonucunda bilgisayara bağlı web kamerası hareket eden nesnelerin takibi için yönlendirilmiştir.

2012 yılında gerçekleştirilen bir çalışmada (Al-Maadeed vd., 2012) sıkıştırma yoluyla birleştirilmiş görüntülerin şifrelenmesi için yöntem önerilmiştir. Şifreleme için, kaotik haritaya dayalı algoritma kullanılmıştır. Sonuç olarak harici şifreleme anahtar sayıları fazlalaştıkça asıl görüntüyle şifrelenmiş görüntü arasındaki korelasyonun azaldığı bu sayede güvenliğin arttığı belirlenmiştir.

Cihat Keleş 2012 yılında yaptığı tez çalışmasında (Keleş, 2012) kriptografinin temellerini, çoklu ortam içeriklerinin şifreleme sorunlarını, kaos teorisini ve kaos teorisinin kriptografiyle ortak noktalarını araştırmıştır. Güvenlik analizleri ile

istatiksel analizler gerçekleştirildiğinde çıkan sonuca göre bit tabanlı kaotik karıştırma piksel tabanlıya göre yayılma aşamasını daha çok etkilediği belirlenmiştir.

Ye Guodong yaptığı tez çalışmasında (Guodong, 2015) kaos tabanlı görüntü şifreleme şemalarını konu olarak ele almıştır. Çalışmada Shannon teoremiyle tasarlanan difüzyon yapısıyla birlikte klasik karışıklık kullanılmıştır. Güvenlik analizlerinin sonucunda beklenen görüntü şifreleme şemalarının güvenlik seviyelerine ulaşılmıştır.

2016 yılında Ümit Çavuşoğlu yaptığı tez çalışmasında (Çavuşoğlu, 2016), güvenliği yüksek ve kaos tabanlı hibrit tasarımları gerçekleştirmek amacıyla kaotik sistemlerin çeşitli özelliklerini ve modern şifreleme algoritmalarını harmanlamıştır. Bu harmanlamanın sonucunda geliştirilen kaos tabanlı şifreleme algoritmalarının görüntü şifrelemede kullanılmasının güvenilir olacağı kanıtlanmıştır.

Zahir Muhammed Ziad Muhammad ve Fatih Özkaynak aynı şekilde güvenlik sorunları üzerine çalışmıştır. Yaptıkları çalışmada (Muhammad ve Özkaynak, 2017) şifreleme algoritmalarında bulunan güvenlik açıklıklarının analizini gerçekleştirerek analiz sonuçlarının sağlaması olarak algoritmaları bozmuşlardır. Çalışma için yazılan senaryoda algoritma geliştirilirken hedeflenen SHA-3 algoritmasına dayalı anahtar planlamadır. Çalışmanın sonucunda hesaplama makinesi değiştirilerek algoritmanın kırılabileceği kanıtlanmıştır.

Chengqing Li ve arkadaşları bilgi entropisi kaotik algoritmalarının güvenliği ve güvenlik değerlendirmelerinin geçerlilikleri üzerine çalışma (LI vd., 2018) yapmışlardır. Yanlış sonuçların çıkabildiğini belirlemişler bu sebeple güvenli bir multimedya şifrelemesi için kapsamlı düşünülerek kriptanalitik çalışmaların artırılmasının gerekli olduğu sonucuna ulaşmışlardır.

Serdar Solak ve Umut Altınışık yaptıkları çalışmada (Solak ve Altınışık, 2018) görüntü işleme tekniklerini fındık meyvesine uygulamışlardır. Kullanılan teknik ve sınıflandırmaları karşılaştırmışlardır sonuç olarak kullanılan yöntemlerin maliyeti düşük, performansı yüksek olarak gerçekleştirilen analiz sonuçlarında belli bir oranda benzerlik gösterdiğini tespit etmişlerdir.

Zhongyun Huaa ve arkadaşları bu soruna odaklanarak kosinüs dönüşümüyle ilgili kaotik sistem (CTBCS) üzerinde çalışma (Hua vd., 2018) yapmışlardır. Performans değerlendirmeleriyle birlikte güvenlik analizlerinden çıkan sonuca göre kosinüs dönüşümüyle ilgili kaotik sistem haritaları farklı yöntemler kullanılarak üretilen kaotik haritalardan daha üstün kaos performansı sergilemiştir.

Nursin Catak ve arkadaşı tarafından yapılan araştırma çalışmasında (Elmacı ve Catak, 2019), iki boyutlu dönüşümü iki boyutlu dönüşümden daha yüksek dönüşümlere çevirmek adına kaotik dönüşüm olan Arnold'ın CAT dönüşümünü kullanılmıştır. CAT dönüşümünün şifrelenmiş görüntüdeki şifrenin çözümü için daha çok güvenlik sağlayan karışık sonuçlar sağladığı belirlenmiştir. Çalışma sonucunda şifrenin çözülmesiyse doğru bir şekilde ve kolayca sağlanmıştır.

Osemwegie Omoruyi ve arkadaşları yaptıkları çalışmada (Omoruyi vd., 2019) bir başka şifrreleme algoritması olan Hill Cipher algoritmasını kullanarak görüntü izleme uygulamaları için algoritmanın şifreleme kalitesini değerlendirmişlerdir. Değerlendirme sonucunda, diğer algoritmalara göre Hill şifreleme algoritmasının daha etkin bulmuşlardır.

3. MATERYAL VE METOT

3.1. Görüntü Şifrelemede Kullanılan Başarı Analizleri

Belirli metrikler kullanılarak görüntü şifreleme (Sakal ve Yıldırım, 2016) işlemi gerçekleştirilmektedir. Görüntü şifreleme analizi (Fadhel vd., 2017) olarak da adlandırılan görüntü şifreleme başarı analizleri bu metrikler doğrultusunda sonuçlandırılmaktadır.

Bu çalışmada kullanılan analiz yöntemlerine ve gerçekleştirilen testlere aşağıda yer verilmiştir.

3.2. Histogram Analizi

Grafiksel bir gösterim olan histogram, dijital görüntüde var olan piksel yoğunluk değerlerinin frekans dağılımını belirtir. Bu analiz sonucunda beklenti histogram grafiğinin tekdüze bir dağılıma sahip olmasıdır. Şifrelenmiş görüntünün histogram analizi grafiğiyle görüntünün aslının histogram analizi grafiği farklı olmalıdır. Histogram dağılımlarının standardının tekdüze bir yapıda olmasının gerekliliği şifreleme teknikleri için kriptanaliz risklerinin bulunmasından dolayıdır.

3.3. Korelasyon Analizi

Şifrelenmiş görüntü üzerindeki bitişik piksellerde korelasyon bulunmamalıdır. Bitişik piksellerde korelasyon bulunması kötü niyetli herhangi bir kullanıcının resmi tekrar oluşturabilmesine ya da görüntü üzerinde değişiklikler yapabilmesine yol açabilmektedir. Korelasyon katsayıları –1 ve +1 arasındadır. -1 mükemmel negatif, +1 pozitif doğrusal ilişkiyi belirtmektedir. Bu analiz sonucunda beklenti analiz sonucunun 0'a yakın olmasıdır.

Aşağıda verilen denklemlerle korelasyon katsayıları hesaplanabilmektedir.

$$r_{\alpha\beta} = \frac{cov(\alpha.\beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}} \quad (3.3)$$

$$E(\alpha) = \frac{1}{N}\sum_{i=1}^{N} \alpha_i$$

(3.3)

$$D(\alpha) = \frac{1}{N}\sum_{i=1}^{N}(\alpha_{i-E(\alpha)})^2 \quad (3.3)$$

$$cov(\alpha,\beta) = \frac{1}{N}\sum_{i=1}^{N}(\alpha_i - E(\alpha))(\beta_i - E(\beta)) \quad (3.3)$$

3.4. Diferansiyel Saldırı Analizi

Pikseldeki küçük veya büyük herhangi bir değişiklik ile görüntünün aslıyla şifrelenmiş görüntüdeki değişiklikleri görüntülemek için yapılan analizler diferansiyel saldırı analizi olarak adlandırılmaktadır. Bu analizin yapılabilmesi için görüntünün aslı ile değiştirilmiş olan görüntünün aynı şifreleme tekniğiyle şifrelenmiş olması gerekmektedir. NPCR (Number of changing pixel rate) ve UACI (Unified averaged changed intensity) en çok kullanılan diferansiyel saldırı analizi yöntemlerindendir. UACI oranı, görüntü şifreleme için kullanılan tekniklere karşı gerçekleştirilen kötü niyetli saldırılara dayanıklılık oranıdır. NPCR oranı, görüntünün aslıyla pikseli değiştirilmiş olan görüntünün karşılaştırılması sonucunda şifreli görüntünün piksel sayısındaki değişim oranını belirten orandır. Bu analiz sonucundaki beklenti aşağıdaki denklem kullanılarak bulunan NPCR oranının 0.99 olmasıdır. Denklemdeki H (Height) ile W (Width) değerleri görüntünün yükseklik ve genişlik değerlerini ifade etmektedir. D değeri, C1 ile C2 görüntülerine eş büyüklükteki diziyi belirtmektedir ve 0 veya 1 bileşenleri kullanılmaktadır.

$$NPCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D(i,j)}{W \times H} \times 100\% \quad (3.4)$$

$$D(i,j) = \begin{pmatrix} 0 & C1(i,j)=C2(i,j), \\ 1 & C1(i,j)\neq C2(i,j) \end{pmatrix} \quad (3.4)$$

UACI oranı, görüntünün aslıyla şifrelenmiş görüntü arasındaki ortalama yoğunluk farkı olarak tanımlanmaktadır. Bu analiz sonucundaki beklenti aşağıdaki denklem kullanılarak bulunan UACI oranının 0.34 olmasıdır. Denklemdeki L parametresi görüntünün pikselini belirten bit sayısıdır.

$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|C1(i,j)-C2(i,j)|}{2^{L}-1}\right]100\% \quad (3.4)$$

3.5. Anahtar Uzay Analizi

Kaba kuvvet saldırılarına karşı dayanıklı şifreleme oluşturulabilmesi için anahtar uzayının fizibilitesi için belirlenen kombinasyonların yeterli olması gerekmektedir. Görüntü şifreleme algoritmalarından bazıları küçük anahtar alanlara sahiptir bu nedenle kaba kuvvet saldırılarına karşı savunmasızdır. Aşağıdaki çizelgede (Çizelge 3.5.1) genel olarak görüntü şifreleme algoritmalarında kullanılan anahtar büyüklüklerine örnekler verilmiştir. (Atalay vd., 2019)

Çizelge 3.1. Anahtar uzay aralıkları

Anahtar Büyüklüğü	**Algoritma**
2^{128}	AES
2^{128}	RC5
2^{128}	Vigenere
2^{128}	IDEA
2^{64}	Blowfish
2^{56}	DES
2^{256}	RC4

3.6. Zaman Karmaşıklığı Analizi

Şifrelenmiş görüntünün şifreleme ve şifre çözme süresi zaman karmaşıklığı analizindeki zaman miktarıyla ifade edilmektedir. Analiz sonuçları farklı faktörlere (sistem konfigürasyonu, kullanılan görüntü vb.) bağlı olarak değişebilmektedir.

3.7. Entropi Analizi

Düzensizlik veya belirsizlik kelimeleriyle ifade edilen entropi bu kavramların nicel ölçüsü olarak nitelendirilmektedir. Düzensizlik ve entropi arasında doğrusal bir ilişki bulunmaktadır. Bir sistemde düzensizlik arttığında entropi de artar. Entropi analizi, görüntünün şifreli halinin karmaşıklığının analiz edilebilmesini sağlamaktadır.

Karmaşıklık şifrelemenin kaliteli olduğunu göstermektedir. Görüntünün şifreli verileri ne kadar karmaşıksa görüntü o kadar iyi şifrelenmiş demektir. Bu analiz sonucundaki beklenti entropi değerinin 8'e yakın olmasıdır. Entropi değerinin 8'e yakınlığı şifrelemenin iyi bir entropi değerine sahip olduğunu göstermektedir.

3.8. İstatiksel Analiz

Şifreleme sistemlerinde yaygın olarak kullanılan analiz yöntemi istatiksel analizdir. İstatistiksel analiz görüntünün aslıyla şifreli hali arasındaki ilişkiyi belirler.

Rastgelelik: Madeni parayla yapılan birbirinden bağımsız atışlar sonucunda her atışta 0 ya da 1 üretilme olasılığı ½'dir. Üretilen 0 ile 1 değerleri rastgele dağıtılacağından madeni para rastgelelik için örnek olarak verilebilir. Bu çalışmada rastgeleliğin testi için NIST Test Suite tarafından geliştirilmiş aşağıdaki 15 test (NIST, 2010) kullanılmıştır.

3.8.1. Frekans testi

Frekans testi, dizi içindeki 0 ve 1'lerin oranını test eder. Amaç 0 ve 1'lerin sayısının rastgele dizi için beklenilen şekilde yaklaşık olarak aynı olup olmadığını gözlemlemektir. Testin beklentisi dizideki 0 ve 1'lerin sayısının yaklaşık olarak aynı olmasıdır.

3.8.2. Blok içi frekans testi

Rastgelelikte M-bit bloğundakilerin frekansının yaklaşık olarak M/2 olması beklenmektedir. Beklenildiği şekilde frekansın yaklaşık olarak M/2 olup olmadığını tespit etmek bu testin amacıdır.

3.8.3. Koşu testi

Dizideki toplam çalıştırma sayısına odaklanan test koşu testi olarak tanımlanmaktadır. k uzunluğundaki bir dizi k tane özdeş bitten oluşmaktadır. Bu testin amacı, uzunlukları değişiklik gösterebilen 0 ve 1'lerin rastgele dizi için

beklendiği gibi mi olduğunu tespit etmektir. Ayrıca, 0 ve 1'ler arasındaki salınımın hızlı ya da yavaş olduğu da tespit edilebilmektedir.

3.8.4. Bir bloktaki en uzun süreli testler

Testi gerçekleştirilen dizideki en uzun koşunun uzunluğunun, rastgele dizide beklenen en uzun koşunun uzunluğuyla tutarlı olup olmadığının tespit edilebilmesi amacıyla bu test yapılmaktadır.

3.8.5. İkili matris sıra testi

İkili matris sıra testi, dizinin ayrık alt matrislerinin sıralanmasına odaklanır. Bu test, asıl diziyle sabit uzunluktaki alt dizileri arasındaki doğrusal bağımlılığı kontrol etmek amacıyla kullanılmaktadır.

3.8.6. Ayrık Fourier dönüşümü testi

Ayrık Fourier dönüşümü testi, dizinin dönüşümdeki tepe yüksekliklerine odaklanır. Amaç test edilen dizideki rastgelelikte meydana gelen sapmaları gösterecek tekrarlayan ve birbirine yakın modelleri belirlemektir. Modelleri belirlemekteki amaçsa, eşik olarak %95'i aşan tepe noktalarının sayısı %5'ten farklı mı bunu gözlemlemektir.

3.8.7. Örtüşmeyen şablon eşleştirme testi

Önceden tespit edilmiş dizilerin oluşum sayısına odaklanan testler örtüşmeyen şablon eşleştirme testleri olarak adlandırılmaktadır. Örtüşmeyen şablon eşleştirme testinin amacı periyodik olmayan modellerin fazla tekrarla üreten üreticileri belirlemektir. M-bit penceresi kullanan bu testte model bulunamazsa pencere bir bit konumuna kaymaktadır. Test sonucunda model bulunursa pencere bulunan modelden sonraki bite sıfırlanarak arama devam etmektedir.

3.8.8. Örtüşen şablon eşleştirme testi

Önceden tespit edilmiş dizilerin oluşum sayısına odaklanan testler örtüşen şablon eşleştirme testleri olarak adlandırılmaktadır. M-bit penceresi kullanan bu testte model bulunamazsa pencere bir bit konumuna kaymaktadır. Test sonucunda model bulunursa aramaya devam etmeden önce pencere yalnızca bir bit kaymaktadır.

3.8.9. Maurer'in evrensel istatistik testi

Evrensel istatistik testi eşleşen desenler arasındaki bit sayısına odaklanmaktadır. Bu test, bilgi kaybı olmadan dizi sıkıştırılabilir mi bunu belirlemeyi amaçlamaktadır. Eğer dizi sıkıştırılabilirse kabul edilen tez dizinin rastgele olmadığıdır.

3.8.10. Doğrusal karmaşıklık testi

Doğrusal karmaşıklık testi LFSR (Linear-feedback shift register) uzunluğuna odaklanmaktadır. Bu test, dizinin karmaşıklığını belirleyerek rastgele olarak kabul edilip edilmeyeceğini tespit etmeyi amaçlamaktadır. Rastgele dizilerde LFSR'nin uzunluğu daha fazla olmaktadır.

3.8.11. Seri test

Seri testi dizi boyunca örtüşen m-bit modellerinin frekanslarına odaklanmaktadır. Bu test, 2m m-bit örtüşen modellerin oluşum sayısı rastgele diziler için beklenen oluşum sayısıyla yaklaşık olarak aynı mı bunu tespit etmeyi amaçlamaktadır. Diziler rastgeleyse tekdüzedir.

3.8.12. Yaklaşık entropi testi

Yaklaşık entropi testi dizi boyunca örtüşen m-bit modellerinin frekanslarına odaklanmaktadır. Bu test, m ve m+1 gibi iki ardışık uzunlukta örtüşen blokların sıklığını, rastgele dizi için beklenen sıklık sonucuyla karşılaştırmayı amaçlamaktadır.

3.8.13. Kümülatif toplamlar testi

Dizideki hanelerin kümülatif toplamı tarafından tanımlanan rastgele yürüyüşün maksimum sapmasına odaklanan testler kümülatif toplamlar testi olarak tanımlanmaktadır. Bu test, dizide meydana gelen kısmi dizilerin kümülatif toplamın, rastgele diziler için beklenen davranışına göre büyüklük ya da küçüklüğünü tespit etmeyi amaçlamaktadır. Rastgele yürüyüş bu kümülatif toplamdır dolayısıyla test için beklenen sonuç yürüyüşün sıfıra yakın olmasıdır.

3.8.14. Rastgele geziler testi

Kümülatif toplam rastgele yürüyüşlerinde döngü sayısına odaklanan testler rastgele geziler testi olarak adlandırılmaktadır. Rastgele yürüyüş döngüsü, başlangıç noktasından başlayarak orijine geri dönmektedir. Bu dönüşte rastgele birim uzunluklar alınmaktadır. Rastgele geziler testi, bir döngü içinde gerçekleşen durumların sayısı rastgele dizi için beklenen durumların sayısından farklı mı bunu tespit etmeyi amaçlamaktadır.

3.8.15. Rastgele geziler varyant testi

Kümülatif toplam rastgele yürüyüşlerinde gerçekleşen durumların toplam sayısına odaklanan testler rastgele geziler varyant testleri olarak adlandırılmaktadır. Bu test, rastgele yürüyüşteki beklenen durum sayılarından sapma olup olmadığını tespit etmeyi amaçlamaktadır.

3.9 Metodoloji

Bu çalışmada kullanılan ve önerilen şifreleme yöntemi bitxor yapısıyla oluşturulmuştur. Aşağıdaki denklemler kullanılarak 2 anahtar üretilmiştir.

```
a = 3.991461146114611;
key1 = key1*a*(1-key1);
b = 3.991461086108141;
key2 = key2*b*(1-key2);
```

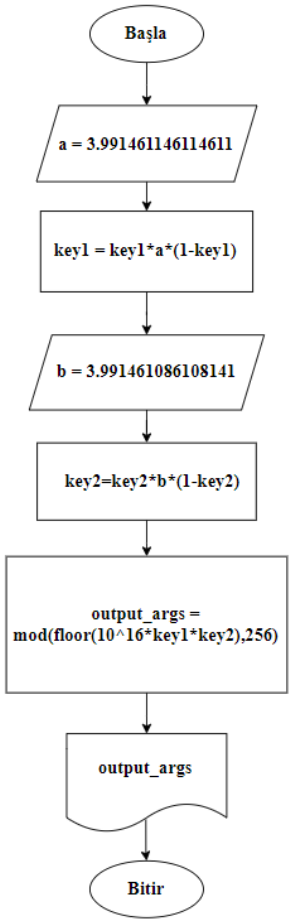
Üretilen bu iki anahtar birbirleriyle ve 10^16 ile çarpıldıktan sonra modu alınmış bu denklemlerden çıkan sonuçlar Ex-Or lanarak şifreleme yapılmıştır.

Algoritma 1'de (Çizelge 3.2) görüntülerde kaotik şifre üretmeye yönelik algoritma tanımlanmıştır.

Çizelge 3.2. Görüntülerde kaotik şifre üretmek için algoritma

ALGORİTMA 1: GÖRÜNTÜLERDE KAOTİK ŞİFRE ÜRETMEK İÇİN ALGORİTMA	
	Girdi: *a, b, key1, key2*
	Çıktı: *işlem sonuçlarının modunun alınması*
1	***keygenerate*** ← *anahtar üretmek için kullanılan keyfenerate fonksiyonu*
2	***Değişkenlerin başlatılması:*** *a ve b değişkenlerine sayı ata*
3	***İşlemler:*** *key1'i a ve 1-key1 ile çarp, key2'yi b ve 1-key2 ile çarp*
4	***Çıktı değerleri:*** *10^16 ile key1 ve key2'yi çarpıp 256'ya göre modunu al*

Şekil 3.9.1’de kaotik şifre üretmeye yönelik akış diyagramı gösterilmiştir.



Şekil 3.1. Şifre üretme akış diyagramı

Algoritma 2'de (Çizelge 3.3) görüntülerde kaotik şifre üretildikten sonra şifrelemeyi oluşturmak için algoritma tanımlanmıştır.

Çizelge 3.3. Kaotik şifrelemeyi oluşturmak için algoritma

ALGORİTMA 2: KAOTİK ŞİFRELEMEYİ OLUŞTURMAK İÇİN ALGORİTMA

Girdi: *image, key1, key2*

Çıktı: *modu alınmış denklemlerden çıkan sonuçların xorlanması*

1 ***image dosyası*** *←başlangıçta seçilen görüntünün bulunduğu dosya*

2 ***Değişkenlerin başlatılması:*** *height ve width değişkenlerine image'in boyutunu ata*

3 ***for (i=1:height*width)*** *// height ve width değerlerini çarparak 1'e ata for döngüsünü başlat*

4 ***işlemler*** *← key1 ve key2 kullanılarılak keygenerate fonksiyonuyla üretilen anahtarı x(i), key1, key2 değişkenlerine ata*

5 *bir sonraki i değişkenine atla*

6 ***End***

7 ***for(h=1:height)*** *// height değerini h değişkenine ata*

8 ***for (w=1:width) // width değerini w değişkenine ata***

9 *işlemler ← image(h,w), x((h-1)*height+w)) işleminden çıkan sonucu xorla ve image(h,w)'ye ata*

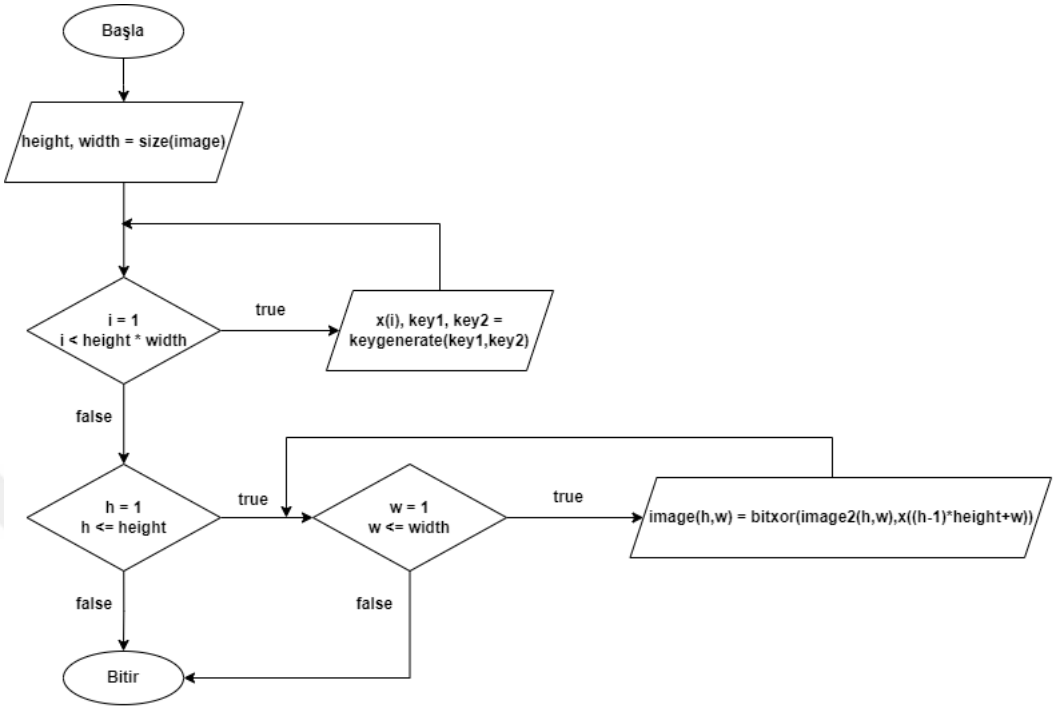
10 *bir sonraki w değişkenine atla*

11 ***End***

12 *bir sonraki h değişkenine atla*

13 ***End***

Şekil 3.2’de görüntülerde kaotik şifre üretildikten sonra kaotik şifrelemeyi oluşturmak için kullanılan algoritmaya yönelik akış diyagramı gösterilmiştir.

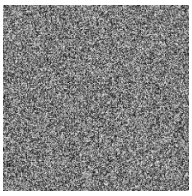


Şekil 3.2. Kaotik şifre oluşturma akış diyagramı

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Bu çalışmada görüntü şifreleme yöntemlerinin analiz ve test çıktılarını incelemek için MATLAB uygulaması kullanılmıştır. Çalışmada kullanılan 0.50000001 ve 0.50000002 anahtarlarıyla kameraman görüntüsünün orijinal, şifrelenmiş ve şifresi çözülmüş görüntüsü Şekil 4.1, Şekil 4.2, ve Şekil 4.3'te verilmiştir.

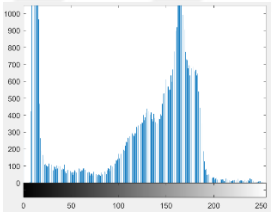
Şekil 4.1. Orijinal



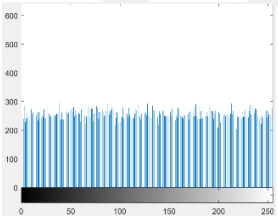
Şekil 4.2. Şifrelenmiş

Şekil 4.3. Şifre çözülmüş

Gerçekleştirilen histogram analizi sonucunda beklendiği gibi histogram grafiğinin tekdüze bir dağılıma sahip olduğu gözlemlenmiştir. Şifrelenmiş görüntünün histogram analizi grafiği (Şekil 4.4) ile görüntünün aslının histogram analizi grafiği (Şekil 4.5) farklıdır.



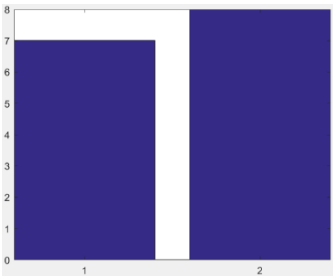
Şekil 4.4. Orijinal histogram



Şekil 4.5. Şifrelenmiş histogram

Gerçekleştirilen korelasyon analizi sonucunda beklenildiği gibi şifrelenmiş görüntünün analiz sonucu 0'a yakın olarak bulunmuştur. Görüntünün orijinal görüntüsünün korelasyon analizi sonucu 0.9846'dır. Görüntünün şifrelenmiş görüntüsünün korelasyon analizi sonucu 0.2806'dır. Gerçekleştirilen entropi analizi sonucunda beklenildiği gibi entropi değeri 8'e yakın olarak bulunmuştur. Görüntünün orijinal görüntüsünün entropi analizi sonucu 7.0134'tür. Görüntünün şifrelenmiş görüntüsünün entropi analizi sonucu 7.9970'tir.

Şekil 4.6’da görüntünün orijinal görüntüsünün (1) ve görüntünün şifrelenmiş görüntüsünün (2) entropi analizi sonuçlarının grafiği verilmiştir.



Şekil 4.6. Entropi analizi

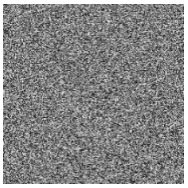
Gerçekleştirilen diferansiyel saldırı analizi sonucunda beklenildiği gibi analiz sonuçları UACI oranı 0.3354, NPCR oranı 0.9962 olarak bulunmuştur.

256x256 boyutlu kameraman görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.056462, şifre çözme süresi 0.060088, 512x512 boyutlu uçak görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.276390, şifre çözme süresi 0.229176, 128x128 boyutlu uçak görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.014538, şifre çözme süresi 0.014087 olarak bulunmuştur.

1.1161 MB/s şifreleme kapasitesiyle çalışmaktadır.
Analizler gerçekleştirilirken kullanılan cihazın özellikleri;
İşlemci: Intel® Core™ i5-8265U CPU @ 1.60GHz 1.80GHz,
Takılı RAM: 16,0 GB (kullanılabilir: 15,9 GB),
Sistem türü: 64 bit işletim sistemi, x64 tabanlı işlemci.
Windows özellikleri;
Edisyon: Windows 10 Pro,
Sürüm: 22H2.

Çalışmada kullanılan 0.50000001 ve 0.50000002 anahtarlarıyla Lena görüntüsünün orijinal, şifrelenmiş ve şifresi çözülmüş görüntüsü Şekil 4.7, Şekil 4.8, ve Şekil 4.9'da verilmiştir.

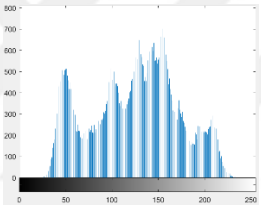
Şekil 4.7. Orijinal



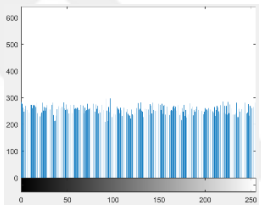
Şekil 4.8. Şifrelenmiş

Şekil 4.9. Şifre çözülmüş

Gerçekleştirilen histogram analizi sonucunda beklendiği gibi histogram grafiğinin tekdüze bir dağılıma sahip olduğu gözlemlenmiştir. Şifrelenmiş görüntünün histogram analizi grafiği (Şekil 4.10) ile görüntünün aslının histogram analizi grafiği (Şekil 4.11) farklıdır.



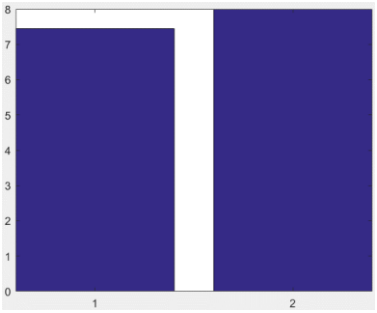
Şekil 4.10. Orijinal histogram



Şekil 4.11. Şifrelenmiş histogram

Gerçekleştirilen korelasyon analizi sonucunda beklenildiği gibi şifrelenmiş görüntünün analiz sonucu 0'a yakın olarak bulunmuştur. Görüntünün orijinal görüntüsünün korelasyon analizi sonucu 0.9856'dır. Görüntünün şifrelenmiş görüntüsünün korelasyon analizi sonucu 0.2874'tür. Gerçekleştirilen entropi analizi sonucunda beklenildiği gibi entropi değeri 8'e yakın olarak bulunmuştur. Görüntünün orijinal görüntüsünün entropi analizi sonucu 7.4429'dur. Görüntünün şifrelenmiş görüntüsünün entropi analizi sonucu 7.9971'dir.

Şekil 4.12'de görüntünün orijinal görüntüsünün (1) ve görüntünün şifrelenmiş görüntüsünün (2) entropi analizi sonuçlarının grafiği verilmiştir.

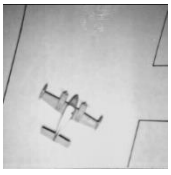


Şekil 4.12. Entropi analizi

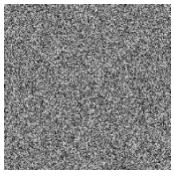
Gerçekleştirilen diferansiyel saldırı analizi sonucunda beklenildiği gibi analiz sonuçları UACI oranı 0.3354, NPCR oranı 0.9962 olarak bulunmuştur.

256x256 boyutlu Lena görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.056903, şifre çözme süresi 0.058524, 512x512 boyutlu uçak görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.251949, şifre çözme süresi 0.238874, 128x128 boyutlu uçak görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 00.014547, şifre çözme süresi 0.014573 olarak bulunmuştur.

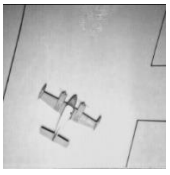
Çalışmada kullanılan 0.50000001 ve 0.50000002 anahtarlarıyla uçak görüntüsünün orijinal, şifrelenmiş ve şifresi çözülmüş görüntüsü Şekil 4.13, Şekil 4.14, ve Şekil 4.15'te verilmiştir.



Şekil 4.13. Orijinal

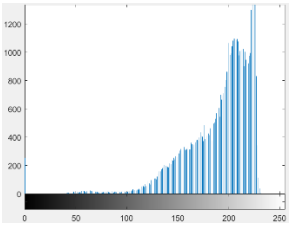


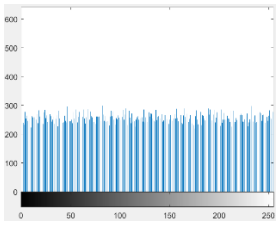
Şekil 4.14. Şifrelenmiş



Şekil 4.15. Şifre çözülmüş

Gerçekleştirilen histogram analizi sonucunda beklendiği gibi histogram grafiğinin tekdüze bir dağılıma sahip olduğu gözlemlenmiştir. Şifrelenmiş görüntünün histogram analizi grafiği (Şekil 4.16) ile görüntünün aslının histogram analizi grafiği (Şekil 4.17) farklıdır.

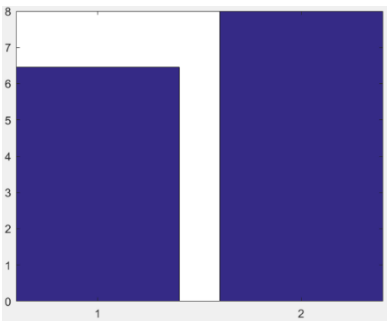




Şekil 4.16. Orijinal histogram Şekil 4.17. Şifrelenmiş histogram

Gerçekleştirilen korelasyon analizi sonucunda beklenildiği gibi şifrelenmiş görüntünün analiz sonucu 0'a yakın olarak bulunmuştur. Görüntünün orijinal görüntüsünün korelasyon analizi sonucu 0.9910'dur. Görüntünün şifrelenmiş görüntüsünün korelasyon analizi sonucu 0.2892'dir. Gerçekleştirilen entropi analizi sonucunda beklenildiği gibi entropi değeri 8'e yakın olarak bulunmuştur. Görüntünün orijinal görüntüsünün entropi analizi sonucu 6.4523'tür. Görüntünün şifrelenmiş görüntüsünün entropi analizi sonucu 7.9970'tir.

Şekil 4.18'de görüntünün orijinal görüntüsünün (1) ve görüntünün şifrelenmiş görüntüsünün (2) entropi analizi sonuçlarının grafiği verilmiştir.



Şekil 4.18. Entropi analizi

Gerçekleştirilen diferansiyel saldırı analizi sonucunda beklenildiği gibi analiz sonuçları UACI oranı 0.3333, NPCR oranı 0.9960 olarak bulunmuştur.

256x256 boyutlu uçak görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.058946, şifre çözme süresi 0.063232, 512x512 boyutlu uçak görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.228803, şifre çözme süresi 0.220626, 128x128 boyutlu uçak görüntüsünde gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.016799, şifre çözme süresi 0.014315 olarak bulunmuştur.

Gerçekleştirilen anahtar uzay analizi sonucu;

$\log_2(10^{16})$ $\log_2(10^{28})$ $\log_2(10^{56})$
= 53.1508 = 93.0140 = 186.0280

Bu sonucun hesaplanışı aşağıda verilmiştir.
a = 3.99xxxxxxxxxxxxx; 10^{13}
b = 3.99xxxxxxxxxxxxx; 10^{13}
Virgülden sonra 15 hane olduğundan;
15+15=30 → 10^{30}
3.99 logistic map değeridir. Bu değerden sonrası;
15 – 2 = 13
13+13=26 → 10^{26}
$10^{26} + 10^{30} = 10^{56}$

İstatistiksel testlerde kullanılan varsayılan parametreler Çizelge 4.1'de verilmiştir.

Çizelge 4.1. Kullanıcı tarafından belirlenen istatistiksel test parametreleri

Kaynak Kod Parametresi	Varsayılan Parametre	Açıklama
ALPHA	0.01	Anlamlılık düzeyi
MAXNUMOFTEMPLATES	40	Örtüşmeyen Şablonlar testi
NUMOFTESTS	16	Maksimum test sayısı
NUMOFGENERATORS	12	Maksimum PRNG sayısı

Alpha parametresi, kabul bölgesini belirleyen önem derecesini ifade eder ve NIST, Alpha'nın [0.001, 0.01] aralığında olmasını önerir.

Maxnumoftemplates parametresi, periyodik olmayan şablonların maksimum sayısını belirtir. Örtüşmeyen şablon eşleştirmeleri testiyle yürütülebilir. m = 9 boyutunda şablonlar için, 148'e kadar olası periyodik olmayan şablonlar uygulanabilir.

Numoftests ve Numofgenerators parametreleri maksimum test sayısına karşılık gelir. İstatiksel analizlere yönelik test sonuçları Çizelge 4.2'de verilmiştir.

Çizelge 4.2. P değerleri

İstatiksel Testler	Kameraman P Değeri	Lena P Değeri	Uçak P Değeri
Frequency	0.350485	0.066882	0.066882
BlockFrequency *(m = 128)*	0.213309	0.000439	0.002043
CumulativeSums	0.534146	0.017912	0.122325
Runs	0.534146	0.035174	0.008879
LongestRun	0.534146	0.066882	0.066882
Rank	0.911413	0.017912	0.122325
FFT	0.213309	0.035174	0.008879
OverlappingTemplate *(m = 9)*	0.213309	0.035174	0.122325
Universal	0.000000	0.000000	0.000000
ApproximateEntropy *(m = 10)*	0.911413	0.000199	0.122325
Serial (m = 16, $\nabla\Psi_m^2$)	0.739918	0.066882	0.017912
LinearComplexity (M = 500)	0.017912	0.017912	0.122325

5. SONUÇ VE ÖNERİLER

Teknolojinin yıllar geçtikçe hız kesmeden ilerleyişine devam etmesi sonucunda her alanda veri güvenliği kavramı önemini arttırmıştır. Verilerin güvenliği kapsamında görüntü şifreleme üzerine yapılan bu çalışmada kullanılan veri kaynağı görüntü olarak seçilmiştir. Görüntü şifreleme başarı analizleri ve istatiksel analizlere yönelik testler tanımlanmış ve uygulama üzerinden analizler gerçekleştirilmiştir. Analizler gerçekleştirilirken MATLAB uygulaması üzerinde kodlama yapılmıştır. Öncelikle görüntülerin önceki bölümlerde anlatıldığı şekilde şifrelenmesi sağlanmış ve sonra şifrelenmiş görüntülerin şifrelerini çözme işlemleri için kod yazılmıştır. Testler gerçekleştirilirken, yazılan kodlarla öncelikle görüntülerin pixel değerlerinin binary olarak çevrilmesi sağlanmıştır. Bu çevrilen değerler NIST testleri için kullanılmıştır. Tanımlanan analiz ve testler doğrultusunda gerçekleştirilen histogram, korelasyon, diferansiyel saldırı, anahtar uzay, anahtar hassasiyet, zaman karmaşıklığı, entropi başarı analizleri ve istatiksel analizlere yönelik frekans, blok içi frekans, koşu, bir bloktaki en uzun süreli, ikili matris sıra, ayrık Fourier dönüşümü, örtüşmeyen şablon eşleştirme, örtüşen şablon eşleştirme, Maurer'in evrensel istatistik, doğrusal karmaşıklık, seri, yaklaşık entropi, kümülatif toplamlar, rastgele geziler, rastgele geziler varyant testlerinin sonuçları karşılaştırılmıştır. Gerçekleştirilen histogram analizi sonucunda kullanılan 3 görüntü için beklenildiği gibi histogram grafiğinin tekdüze bir dağılıma sahip olduğu gözlemlenmiştir. Histogram analizlerini incelediğimizde 0 siyah 250 beyaz rengi, 0-250 arası gri tonları gösterir. Şifrelenmiş görüntünün tekdüze histogram grafiği vermesi grafiğe bakıldığında görüntünün ne olduğu hakkında bir ipucu elde edilememesini sağlamıştır. Gerçekleştirilen korelasyon analizi sonucunda beklenildiği gibi şifrelenmiş görüntülerin analiz sonuçları şifrelenmeden önce 0.9 değerlerindeyken şifrelendikten sonra 0'a yakın olarak 0.2 değerlerinde bulunmuştur. Bitişik piksellerde korelasyon bulunması görüntünün tekrar oluşturabilmesine ya da görüntü üzerinde değişiklikler yapabilmesine yol açabildiğinden korelasyon katsayılarının -1 ve +1 arasında ilişki belirttiği göze alındığında şifrelenmiş görüntülerin 0'a yakın bulunmasıyla beklenilen sonuç elde edilmiştir. Pikseldeki değişiklik ile görüntünün aslıyla şifrelenmiş görüntüdeki değişiklikleri görüntülemek için yapılan diferansiyel saldırı analizinde UACI ve NPCR oranları beklenilen değerlerde sonuçlar vermiştir.

Anahtar uzayının fizibilitesinin yeterliliğinin belirlenmesi için gerçekleştirilen anahtar uzay analizinde yeterli sonuca ulaşılmıştır. Anahtar hassasiyet analizi sonucu anahtarın 1.1161 MB/s şifreleme kapasitesiyle çalıştığı belirlenmiştir. Zaman karmaşıklığı analiziyle elde edilen şifre oluşturma ve çözme süreleriyle şifreleme kapasitesine yönelik bu sonuçların performanslarının çalıştırılan makine göze alındığında başarılı olduğu gözlemlenmiştir. Görüntünün boyutları değiştirilerek şifre oluşturma ve şifre çözme süreleri tekrar test edilmiştir. Yapılan testler sonucunda bu sonuçların çalıştırılan makine özellikleri (işletim sistemi, RAM kapasitesi vb.) göze alındığında başarılı olduğu gözlemlenmiştir. Entropi analizinde özellikle uçak görüntüsünün orijinal halinin entropi sonucu 6.4 değerindeyken, şifrelenmiş görüntüsünün entropi değeri 8'e yakın bir değer olarak 7.9 değerinde bulunmuştur. Entropi görüntünün karmaşıklığını ifade ettiğinden entropi arttıkça karmaşıklık artar dolayısıyla şifrelenmiş görüntünün karmaşıklığının arttığı analiz sonucuyla gözlemlenmiştir. İstatistiksel testlerin tümü uygulanmış ve sonuçlar çizelgeye kaydedilmiştir. 15 testin 12'sinde sonuç alınmıştır. Özetle, bu çalışmada şifrelenmiş görüntüler ve görüntülerin asılları kullanılarak gerçekleştirilen testler sonucunda beklenilen değerlerin elde edilmesi, oluşturulan şifrelemenin performansının değerlendirilmesi amaçlanmıştır. Görüntü şifrelemede kullanılan ve bu çalışmada açıklanan yöntemlerin çıktı olarak başarılı sonuç ve performansları verdiği gözlemlenmiştir.

KAYNAKLAR

Al-Maadeed, S., Al-Ali, A., Abdalla, T., 2012. A New Chaos-Based Image-Encryption and Compression Algorithm. Hindawi Publishing Corporation Journal of Electrical and Computer Engineering, 1-11, Katar, Irak.

Atalay, N. S., Doğan, Ş., Tuncer, T., Akbal, E., 2019. İmge Şifreleme Yöntem ve Algoritmaları. DÜMF Mühendislik Dergisi, 815-831, Diyarbakır.

Ceyhan, M., Yolaçan, E. N., 2021. Görüntü Dosyalarının Şifrelenerek Güvenli Şekilde Saklanması. ESOGÜ Mühendislik Mimarlık Fakültesi Dergisi, 28-42, Eskişehir.

Çavuşoğlu, Ü., 2016. Kaos Tabanlı Hibrit Simetrik ve Asimetrik Şifreleme Algoritmaları Tasarımı ve Uygulaması. Sakarya Üniversitesi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi, 141, Sakarya.

Elmacı, D., Catak, N. B., 2019. Higher Dimensional Chaotic Linear Transformations of Colored Image Encryptions. Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 687-694, Erzincan.

Fadhel, S., Shafry, M., Farook, O., 2017. Chaos Image Encryption Methods: A Survey Study. Bulletin of Electrical Engineering and Informatics, 99-104, Malaysia.

Guodong, Y., 2015. Design and Analysis of Some New Chaotic Image Encryption Schemes. City University of Hong Kong, Department of Electrical Engineering, Doktora Tezi, 125, Hong Kong.

Hartman, S., 2005. Chaos Theory and the Mandelbrot Set. Ball State University, Bitirme Tezi, 51, Muncie, Indiana.

Hua, Z., Zhou, Y., Huang, H., 2018. Cosine-transform-based chaotic system for image encryption. Web of Science, 403–419, China.

Keleş, C., 2012. Kaotik Haritalar Kullanarak Görüntü Şifreleme. Karadeniz Teknik Üniversitesi, Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü. Yüksek Lisans Tezi, 76, Trabzon.

Li, C., Lin, D., Feng, B., Lü, J., Hao, F., 2018. Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy. IEEE Access, 2-9. China.

Muhammad, Z. M., Özkaynak, F., 2017. Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique. IEEE Access, 9, Elazığ.

NIST, 2010. A Statistical Test Suite for Cryptographic Applications. National Institute of Standarts and Technology, 23-87, Hindistan.

Omoruyi, O., Okereke, C., Okokpujie, K., Noma-Osaghae, E., Okoyeigbo, O., John, S., 2019. Evaluation of the quality of an image encrytion scheme. Telkomnika, 2968-2974, Nigeria.

Peker, M., 2009. Görüntü İşleme Tekniği Kullanılarak Gerçek Zamanlı Hareketli Görüntü Tanıma. Sakarya Üniversitesi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 105, Sakarya.

Sakal, H., Yıldırım, M., 2016. Görüntü Şifreleme İçin Scan Paternlerini Kullanan Hibrit Bir Yöntem. Selçuk-Teknik Dergisi, 264-283, Konya.

Solak, S., Altınışık, U., 2018. Görüntü işleme teknikleri ve kümeleme yöntemleri kullanılarak fındık meyvesinin tespit ve sınıflandırılması. Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 56-65, Sakarya.

EKLER

EK A. Şifreleme

EK B. Şifre çözme

EK C. Entropinin hesaplanması

EK D. NPCR oranının hesaplanması

EK E. UACI oranının hesaplanması

EK F. Korelasyonun ve histogramın hesaplanması

EK G. Görüntüleri binary olarak yazma

EK H. Anahtar oluşturma

EK I. Dosyadan görüntü yükleme ve fonksiyonları çalıştırma

EK İ. Sözlük

EK A. Şifreleme

```
function [image2] = bitxor_operation(image2,key1,key2)
[height, width] = size(image2);
for i = 1:height*width
[x(i),key1,key2]=keygenerate(key1,key2);
end
tic
for h = 1:height
   for w = 1:width
         image2(h,w)=bitxor(image2(h,w),x((h-1)*height+w));
   end
end
toc
```

EK B. Şifre çözme

```
function [image3] = bitxor_operation_reverse(image3,key1,key2)
[height, width] = size(image3);
for i = 1:height*width
[x(i),key1,key2]=keygenerate(key1,key2);
end
tic
for h = 1:height
   for w = 1:width
         image3(h,w)=bitxor(image3(h,w),x((h-1)*height+w));
   end
end
toc
```

EK C. Entropinin hesaplanması

```
function [ output_args, I,I2 ] = calculate_entropy( ~,~ )
I=imread('plane.tiff');
I2=imread('plane_enc.png');
x=entropy(I)
x2=entropy(I2)
bar([x x2]);
set(gca,'xticklabel');
end
```

EK D. NPCR oranının hesaplanması

```
function calculate_npcr(image1,image2)
[height, width, page] = size(image1);
resolution = height*width*page;
d = 0;
same = 0;
different = 0;
for h = 1:height
   for w = 1:width
      for p = 1:page
         if image1(h,w) ~= image2(h,w)
            d = d + 1;
            different = different +1;
         elseif image1(h,w) == image2(h,w)
            same = same+1;
         end
      end
   end
end

d = d / resolution;
disp(same);
disp(different);
disp(d)
```

EK E. UACI oranının hesaplanması

```
function calculate_uaci(image1,image2)
[height, width, page] = size(image1);
resolution = height*width;
d = 0;
for h = 1:height
   for w = 1:width
         pixel1 = double(image1(h,w));
         pixel2 = double(image2(h,w));
         val = abs((pixel1-pixel2))/255;
         d = d + val;
   end
end
```

EK F. Korelasyonun ve histogramın hesaplanması

```
function [ output_args, I,J,R ] = correlation( I,J,R )
I = imread('plane_enc.png');
J = medfilt2(I);
R = corr2(I,J)
End

function [ output_args, I ] = histogram( I )
I = imread('plane_enc.png');
figure;
imhist(I);
end
```

EK G. Görüntüleri binary olarak yazma

```
function [ output_args,a ] = dec2binn( a )
I = imread('cam_enc.png');
[m n] = size(I);
for i=1:m
    for j=1:n
     t=(i-1)*m+j;
      a(t,:)=dec2bin(I(i,j),8);
      %save('plane.txt','a', '-ascii');
      new=cellstr(a);
      fileID = fopen('cam.txt','w');
      fprintf(fileID,'%s\n',new{:});
      fclose(fileID);
    end
```

EK H. Anahtar oluşturma

```
function [ output_args,key1,key2 ] = keygenerate( key1,key2 )
a = 3.991461146114611; 10^13
key1 = key1*a*(1-key1);
b = 3.991461086108141; 10^13
key2 = key2*b*(1-key2);
output_args = mod(floor(10^16*key1*key2),256);
end
```

EK I. Dosyadan görüntü yükleme ve fonksiyonları çalıştırma

```
[file, path] = uigetfile('*.tiff');
image = imread(fullfile(path, file));
%image=my_reverse_logistic(image,0.41,0.76);
image2=bitxor_operation(image,0.50000001,0.50000002);
image3=bitxor_operation_reverse(image2,0.50000001,0.50000002);
%image=my_logistic(image,0.76,0.41);
selected_folder = uigetdir('C:\Users\Lenovo\Desktop\dosyalar\şuankiler\');
imwrite(image2, fullfile(selected_folder,'plane_enc.png'));
imwrite(image3, fullfile(selected_folder,'plane_dec.png'));
figure(1);
subplot(1,3,1);
imshow(image);
title('Original');
figure(1);
subplot(1,3,2);
imshow(image2);
title('Encrypted');
subplot(1,3,3);
imshow(image3);
title('Decrypted');
test;
```

EK İ. Sözlük

AES: Şifreleme ve şifre çözme yöntemlerinde aynı anahtarın kullanıldığı simetrik şifreleme algoritmasıdır.
Blowfish: 64 bitlik bloklarla şifreleme yapan simetrik şifreleme algoritmasıdır.
DES: Büyük boyutlu verileri şifrelemek için gönderenin ve alıcının aynı benzersiz anahtara sahip olduğu simetrik şifreleme algoritmasıdır.
Hill Cipher: Şifrelenecek verinin bloklara bölünerek şifrelendiği şifreleme algoritmasıdır.
IDEA: 128 bitlik anahtarla 52 adet 16 bitlik alt anahtarlar kullanarak şifrelemeyi gerçekleştiren şifreleme algoritmasıdır.
MATLAB: Matematiksel işlemler için kullanılan programlama dilidir.
RC4: Anahtar akışlarını rasgele üreterek şifreleme ve şifre çözme süreçleri esnasında veriye/mesaja uygulayan akış şifresidir.
RC5: Değişken blok, anahtar ve tur sayısına sahip simetrik, basit ve hızlı anahtar blok şifresidir.
SHA-3: Secure hash algorithm açılımıyla NSA tarafından geliştirilmiş olan kriptografik fonksiyondur.

ÖZGEÇMİŞ

Adı Soyadı : Gizem SEVAL

Eğitim Durumu

Lise: Bandırma Anadolu Lisesi, 2013

Lisans: Doğuş Üniversitesi, Mühendislik Fakültesi, Bilişim Sistemleri Mühendisliği Bölümü, 2018

Yüksek Lisans: İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı

Yayınları

Seval G., Kasapbaşı M.C., 2022. Görüntüler İçin Kaotik Kriptografi Sistemi ve Performans Analizi. Avrupa Bilim ve Teknoloji Dergisi, (44), 13-20.

Seval G., Kasapbaşı M.C., 2022. Chaotic Encryption System for Images and Performance Analysis, ISAS2022 Winter, Türkiye.