Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 44, S. 13-20, Aralık 2022

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 44, pp. 13-20, December 2022

Research Article

Görüntüler İçin Kaotik Şifreleme Sistemi Ve Performans Analizi

Gizem Seval[1*], Mustafa Cem Kasapbaşı[2]

[1*] İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Anabilim Dalı Siber Güvenlik Bölümü, İstanbul, Türkiye (ORCID: 0000-0001-8869-4198), gizem.seval@istanbulticaret.edu.tr

[2] İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye (ORCID: 0000-0001-6444-6659), mckasapbasi@ticaret.edu.tr

(6th International Symposium on Innovative Approaches in Smart Technologies (ISAS) 2022 – 8-10 December 2022)

(**DOI:** 10.31590/ejosat.1216797)

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

Öz

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: Kaotik, Performans Analizi, Görüntü Şifreleme

Chaotic Encryption System For Images And Performance Analysis

Abstract

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.

[*] Sorumlu Yazar: gizem.seval@istanbulticaret.edu.tr

1. Giriş

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.

Verilen 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, DOĞAN, TUNCER, & AKBAL, 2019) (CEYHAN & 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 resimdeki 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.

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.

2012 yılında gerçekleştirilen bir çalışmada (Al-Maadeed, Al-Ali, & Abdalla, 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.

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.

Nursin Catak ve arkadaşı tarafından yapılan araştırma çalışmasında (ELMACI & 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.

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.

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.

Zhongyun Huaa ve arkadaşları bu soruna odaklanarak kosinüs dönüşümüyle ilgili kaotik sistem (CTBCS) üzerinde çalışma (Hua, Zhou, & Huang, 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.

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.

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

Zahir Muhammed Ziad Muhammad ve Fatih Özkaynak aynı şekilde güvenlik sorunları üzerine çalışmıştır. Yaptıkları çalışmada (Muhammad & 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.

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

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.

Serdar Solak ve Umut Altınışık yaptıkları çalışmada (Solak & 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.

2. Materyal ve Metot

2.1. Resim Şifrelemede Kullanılan Başarı Analizleri

Belirli metrikler kullanılarak görüntü şifreleme (SAKAL & YILDIRIM, 2016) işlemi gerçekleştirilmektedir. İmge şifreleme analizi (Fadhel, Shafry, & Farook, 2017) olarak da adlandırılan görüntü şifreleme başarı analizleri bu metrikler doğrultusunda sonuçlandırılmaktadır. Bu çalışmada kullanılan analiz yöntemlerine ve gerçekleştirilen testlere aşağıda yer verilmiştir.

2.1.1. 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 resmin histogram analizi grafiğiyle resmin aslının histogram analizi grafiği farklı olmalıdır. Histogram dağılımlarının standardının tekdüze bir yapıda olmasının gerekliliği şifreleme teknikleri için kriptanaliz risklerinin bulunmasından dolayıdır.

2.1.2. 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. Aşağıdaki verilen denklemlerle korelasyon katsayıları hesaplanabilmektedir.

$$r_{\alpha\beta} = \frac{cov(\alpha,\beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}} \quad (1)$$

$$E(\alpha) = \frac{1}{N}\sum_{i=1}^{N}\alpha_i \quad (2)$$

$$D(\alpha) = \frac{1}{N}\sum_{i=1}^{N}\left(\alpha_{i-E(\alpha)}\right)^2 \quad (3)$$

$$cov(\alpha,\beta) = \frac{1}{N}\sum_{i=1}^{N}(\alpha_i - E(\alpha))(\beta_i - E(\beta)) \quad (4)$$

2.1.3. Diferansiyel Saldırı Analizi

Pikseldeki küçük veya büyük herhangi bir değişiklik ile resmin aslıyla şifrelenmiş görüntüdeki değişiklikleri görüntülemek için yapılan analizler diferansiyel saldırı analizi olarak adlandırılmaktadır. Bu analizin yapılabilmesi için resmin aslı ile değiştirilmiş olan resmin 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, resmin aslıyla pikseli değiştirilmiş olan resmin karşılaştırılması sonucunda şifreli resmin 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 resmin yükseklik ve genişlik değerlerini ifade etmektedir. D değeri, C1 ile C2 görüntülerine eş büyüklükteki diziyi belirtmektedir ve 0 veya 1 bileşenleri kullanılmaktadır.

$$NPCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D(i,j)}{W \times H} \times 100\% \quad (5)$$

$$D(i,j) = \begin{pmatrix} 0 & C1(i,j) = C2(i,j). \\ 1 & C1(i,j) \neq C2(i,j) \end{pmatrix} \quad (6)$$

UACI oranı, resmin 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 resmin pikselini belirten bit sayısıdır.

$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|C1(i,j) - C2(i,j)|}{2^L - 1}\right]100\% \quad (7)$$

2.1.4. 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 tabloda (Tablo 1) genel olarak görüntü şifreleme algoritmalarında kullanılan anahtar uzay aralıkları verilmiştir.

Tablo 1. Anahtar Uzay Aralıkları

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

2.1.5. Anahtar Hassasiyet Analizi

Resmi şifrelerken kullanılan algoritmalardaki anahtarda oluşan değişimleri belirlemek amacıyla yapılan analiz anahtar hassasiyet analizi olarak tanımlanmaktadır. Anahtara hassas olarak bağımlı sistemler kaotik şifreleme sistemleridir. Anahtar hassasiyeti pikseller karşılaştırılarak analiz edilmektedir. Analizde resmin şifrelenmiş halinin piksel karşılaştırması ve NPCR oranıyla anahtar değerindeki değişiklikler incelenmektedir. Analizin beklentisi, meydana gelen değişikliklerin kötü niyetli saldırılara karşı güvenli şifrelemeyi gerçekleştirebilmesidir.

2.1.6. Zaman Karmaşıklığı Analizi

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

2.1.7. Entropi Analizi

Entropi analizi, resmin şifreli halinin karmaşıklığının analiz edilebilmesini sağlamaktadır. Karmaşıklık şifrelemenin kaliteli olduğunu göstermektedir. Resmin 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.

2.1.8. İstatiksel Analiz

Şifreleme sistemlerinde yaygın olarak kullanılan analiz yöntemi istatiksel analizdir. İstatistiksel analiz resmin 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.

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.

2. Blok İçi 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. 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.

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.

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.

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.

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.

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.

9. Maurer'in Evrensel İstatistik 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.

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.

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.

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.

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.

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.

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.

2.2 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 xorlanarak şifreleme yapılmıştır.

Algoritma 1'de görüntülerde kaotik şifre üretmeye yönelik algoritma tanımlanmıştır.

ALGORİTMA 1: GÖRÜNTÜLERDE KAOTİK ŞİFRE ÜRETMEK İÇİN ALGORİTMA

Girdi: *a, b, key1, key2*

Çıktı: *işlem sonuçlarının modunun alınması*

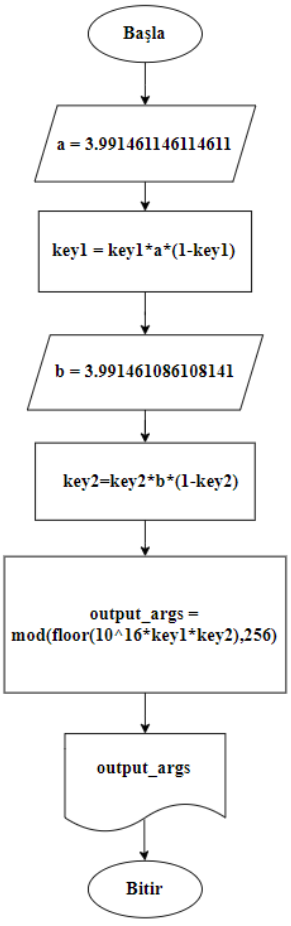
1 ***keygenerate*** ← *anahtar üretmek için kullanılan keyfenerate fonksiyonu*

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 1'de kaotik şifre üretmeye yönelik akış diyagramı gösterilmiştir.



Şekil 1: Şifre Üretme Akış Diyagramı

Algoritma 2'de görüntülerde kaotik şifre üretildikten sonra şifrelemeyi oluşturmak için algoritma tanımlanmıştır.

ALGORİTMA 2: KAOTİK ŞİFRELEMEYİ OLUŞTURMAK İÇİN ALGORİTMA

Girdi: *image, key1, key2*

Çıktı: *modu alınmış denklemlerden çıkan sonuçların xorlanması*

1 ***image dosyası*** *←başlangıçta seçilen resmin 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*

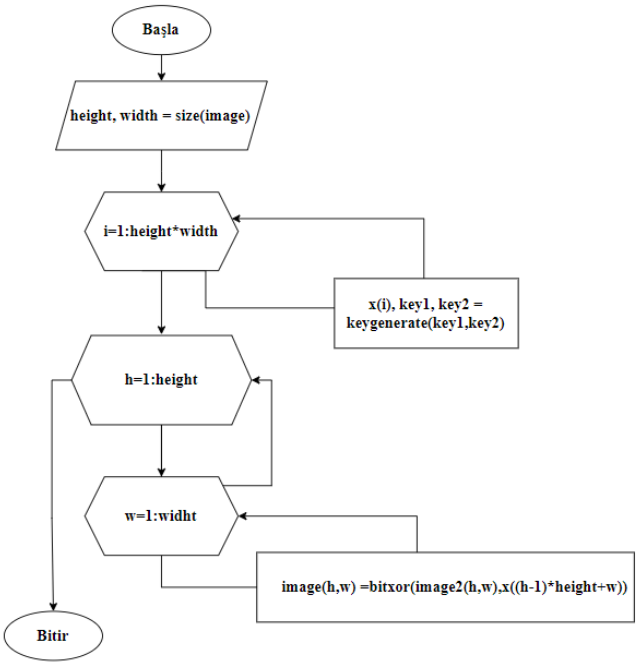
10 *bir sonraki w değişkenine atla*

11 ***end***

12 *bir sonraki h değişkenine atla*

13 ***end***

Şekil 2'de görüntülerde kaotik şifre üretildikten sonra kaotik şifrelemeyi oluşturmak için kullanılan algoritmaya yönelik akış diyagramı gösterilmiştir.

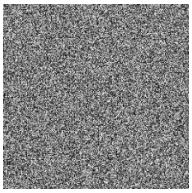


Şekil 2: Kaotik Şifre Oluşturma Akış Diyagramı

3. Araştırma Sonuçları ve Tartışma

Bu çalışmada görüntü şifreleme yöntemlerinin analiz ve test çıktılarını incelemek için MATLAB uygulaması kullanılmıştır. Çalışmada kullanılan 0.50000001 ve 0.50000002 anahtarlarıyla kameraman resminin orijinal, şifrelenmiş ve şifresi çözülmüş görüntüsü Şekil 3, Şekil 4, ve Şekil 5'te verilmiştir.

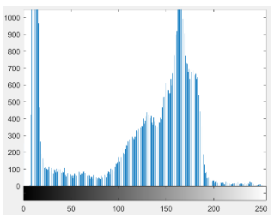
Şekil 3: Orijinal



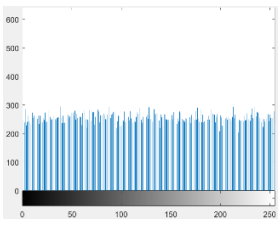
Şekil 4: Şifrelenmiş

Şekil 5: Şifre Çözülmüş

Gerçekleştirilen histogram analizi sonucunda beklendiği gibi histogram grafiğinin tekdüze bir dağılıma sahip olduğu gözlemlenmiştir. Şifrelenmiş resmin histogram analizi grafiği (Şekil 6) ile resmin aslının histogram analizi grafiği (Şekil 7) farklıdır.



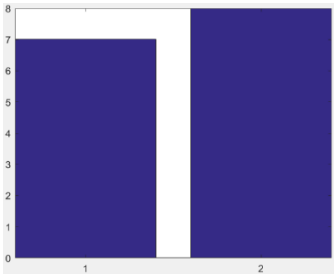
Şekil 6: Orijinal Histogram



Şekil 7: Şifrelenmiş Histogram

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

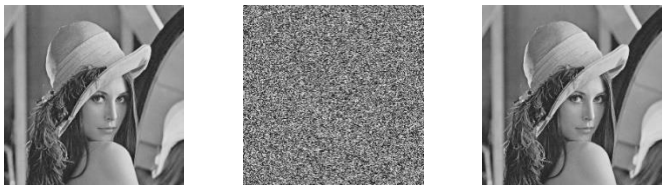
Şekil 8'de resmin orijinal görüntüsünün (1) ve resmin şifrelenmiş görüntüsünün (2) entropi analizi sonuçlarının grafiği verilmiştir.



Şekil 8: Entropi Analizi

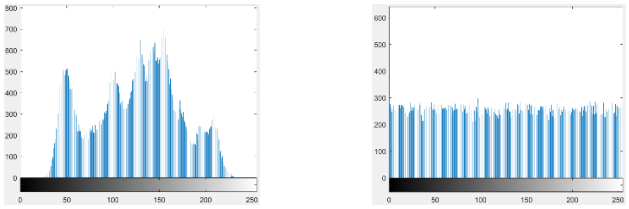
Gerçekleştirilen diferansiyel saldırı analizi sonucunda beklenildiği gibi analiz sonuçları UACI oranı 0.3354, NPCR oranı 0.9962 olarak bulunmuştur. Gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.056462, şifre çözme süresi 0.060088 olarak bulunmuştur. 1.1161 MB/s şifreleme kapasitesiyle çalışmaktadır.

Çalışmada kullanılan 0.50000001 ve 0.50000002 anahtarlarıyla Lena resminin orijinal, şifrelenmiş ve şifresi çözülmüş görüntüsü Şekil 9, Şekil 10, ve Şekil 11'de verilmiştir.



Şekil 9: Orijinal *Şekil 10: Şifrelenmiş* *Şekil 11: Şifre Çözülmüş*

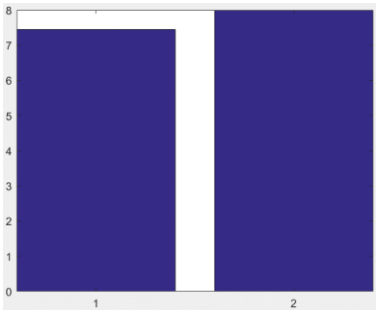
Gerçekleştirilen histogram analizi sonucunda beklendiği gibi histogram grafiğinin tekdüze bir dağılıma sahip olduğu gözlemlenmiştir. Şifrelenmiş resmin histogram analizi grafiği (Şekil 12) ile resmin aslının histogram analizi grafiği (Şekil 13) farklıdır.



Şekil 12: Orijinal Histogram *Şekil 13: Şifrelenmiş Histogram*

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

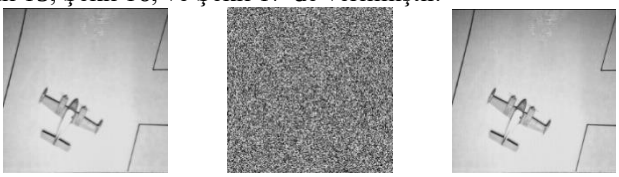
Şekil 14'te resmin orijinal görüntüsünün (1) ve resmin şifrelenmiş görüntüsünün (2) entropi analizi sonuçlarının grafiği verilmiştir.



Şekil 14: Entropi Analizi

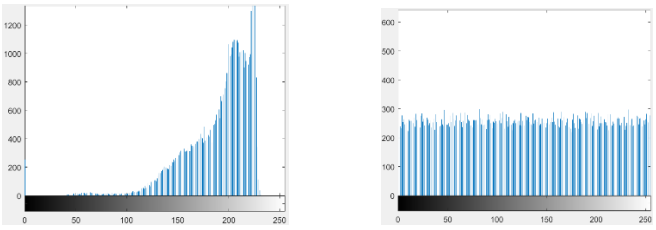
Gerçekleştirilen diferansiyel saldırı analizi sonucunda beklenildiği gibi analiz sonuçları UACI oranı 0.3354, NPCR oranı 0.9962 olarak bulunmuştur. Gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.056903, şifre çözme süresi 0.058524 olarak bulunmuştur.

Çalışmada kullanılan 0.50000001 ve 0.50000002 anahtarlarıyla uçak resminin orijinal, şifrelenmiş ve şifresi çözülmüş görüntüsü Şekil 15, Şekil 16, ve Şekil 17'de verilmiştir.



Şekil 15: Orijinal *Şekil 16: Şifrelenmiş* *Şekil 17: Şifre Çözülmüş*

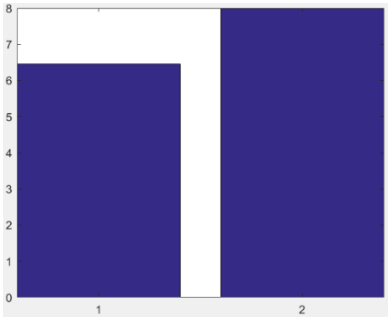
Gerçekleştirilen histogram analizi sonucunda beklendiği gibi histogram grafiğinin tekdüze bir dağılıma sahip olduğu gözlemlenmiştir. Şifrelenmiş resmin histogram analizi grafiği (Şekil 18) ile resmin aslının histogram analizi grafiği (Şekil 19) farklıdır.



Şekil 18: Orijinal Histogram *Şekil 19: Şifrelenmiş Histogram*

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

Şekil 20'de resmin orijinal görüntüsünün (1) ve resmin şifrelenmiş görüntüsünün (2) entropi analizi sonuçlarının grafiği verilmiştir.



Şekil 20: Entropi Analizi

Gerçekleştirilen diferansiyel saldırı analizi sonucunda beklenildiği gibi analiz sonuçları UACI oranı 0.3333, NPCR oranı 0.9960 olarak bulunmuştur. Gerçekleştirilen zaman karmaşıklığı analizi sonucunda görüntünün şifreleme süresi 0.058946, şifre çözme süresi 0.063232 olarak bulunmuştur.

Gerçekleştirilen anahtar uzay analizi sonucu;

log2(10^16)	log2(10^28)	log2(10^56)
= 53.1508	= 93.0140	= 186.0280

İstatiksel analizlere yönelik test sonuçları Tablo 2'de verilmiştir.

Tablo 2. P Değerleri

İstatiksel Testler	Kameraman P Değeri	Lena P Değeri	Uçak P Değeri
Frequency	0.350485	0.066882	0.066882
BlockFrequency	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	0.213309	0.035174	0.122325
Universal	0.000000	0.000000	0.000000
ApproximateEntropy	0.911413	0.000199	0.122325
Serial	0.739918	0.066882	0.017912
LinearComplexity	0.017912	0.017912	0.122325

4. Sonuç

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. 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. Görüntü şifrelemede kullanılan bu yöntemlerin çıktı olarak başarılı sonuç ve performansları verdiği gözlemlenmiştir.

5. Teşekkür

Çalışma boyunca analizlerin sonuçlarını değerlendirerek makale ve tez yorumlarıyla yardımcı olmasından ötürü Mustafa Cem Kasapbaşı'na teşekkürlerimi sunarım.

Kaynakça

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.

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

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

Çavuşoğlu, Ü. (2016). Kaos Tabanlı Hibrit Simetrik ve Asimetrik Şifreleme Algoritmaları Tasarımı ve Uygulaması. *Sakarya: Sakarya Üniversitesi Fen Bilimleri Enstitüsü*.

ELMACI, D., & CATAK, N. B. (2019). Higher Dimensional Chaotic Linear Transformations of Colored Image Encryptions. *Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi*.

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

Guodong, Y. (2015). Design and Analysis of Some New Chaotic Image Encryption Schemes. *Hong Kong: City University of Hong Kong*.

Hartman, S. (2005). Chaos Theory and the Mandelbrot Set. *Muncie, Indiana: Ball State University*.

Hua, Z., Zhou, Y., & Huang, H. (2018). Cosine-transform-based chaotic system for image encryption. *Web of Science*.

Keleş, C. (2012). Kaotik Haritalar Kullanarak Görüntü Şifreleme. *Trabzon: Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü*.

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.

Muhammad, Z. M., & Özkaynak, F. (2017). Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique. *IEEE Access*.

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

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.

Peker, M. (2009). Görüntü İşleme Tekniği Kullanılarak Gerçek Zamanlı Hareketli Görüntü Tanıma. *Sakarya: Sakarya Üniversitesi Fen Bilimleri Enstitüsü*.

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

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.