Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi
Afyon Kocatepe University – Journal of Science and Engineering
https://dergipark.org.tr/tr/pub/akufemubid

Araştırma Makalesi / Research Article
e-ISSN: 2149-3367
DOI: https://doi.org/10.35414/akufemubid.1704583
CITE: Afyon Kocatepe University Journal of Science and Engineering 26(2) (2026) 354-363

Görüntü Şifrelemede RC4 ve Kaotik RC4 Yöntemlerinin Karşılaştırmalı Performans Analizi

*Makale Bilgisi / Article Info
Alındı/Received: 22.05.2025
Kabul/Accepted: 10.01.2026
Yayımlandı/Published: 08.04.2026

Performance Analysis of Chaotic RC4 and Traditional RC4 Encryption Methods in Image Encryption

Muhammed Baki KARHAN [1*], Funda AKAR [2]

[1] *Erzincan Binali Yıldırım Üniversitesi, Fen Bilimleri Enstitüsü, Yapay Zeka ve Robotik ABD, Erzincan, Türkiye*
[2] *Erzincan Binali Yıldırım Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Erzincan, Türkiye*

Öz

Dijital görüntülerin güvenli biçimde iletilmesi, günümüzün kritik bilgi güvenliği gereksinimleri arasında yer almaktadır. Bu çalışmada, geleneksel RC4 şifreleme algoritması ile Lojistik Map tabanlı kaotik sistem kullanılarak güçlendirilmiş RC4 yönteminin görüntü şifrelemedeki performansları karşılaştırılmıştır. Çalışmada her iki yöntem için renkli görüntüler üzerinde şifreleme ve deşifreleme işlemleri gerçekleştirerek işlem süresi, histogram analizi, bitişik pikseller arasındaki korelasyon, entropi, MSE, PSNR, NPCR ve UACI gibi kriptografik güvenlik metrikleri değerlendirilmiştir. Bulgular RC4 algoritmasının şifreleme ve çözme süresi açısından daha hızlı olduğunu, buna karşın Kaotik RC4 yönteminin histogram dağılımındaki homojenlik, korelasyonun düşürülmesi, entropi değerlerinin artırılması ve diferansiyel saldırılara karşı dayanıklılık açısından daha yüksek performans sergilediğini göstermektedir. NPCR ve UACI sonuçları, Kaotik RC4'ün piksel düzeyindeki değişimlere daha duyarlı olduğunu ve güvenlik açısından RC4'ten üstün olduğunu ortaya koymuştur. Elde edilen bulgular, kaotik sistemlerle güçlendirilmiş akış şifreleme yöntemlerinin görüntü verilerinde güvenlik düzeyini artırmada etkili bir alternatif olduğunu göstermektedir.

Anahtar Kelimeler: *Veri güvenliği; Kriptoloji; Kaotik; RC4; Görüntü şifreleme.*

Abstract

The secure transmission of digital images is among today's critical information security requirements. In this study, the performance of the traditional RC4 stream cipher and the Logistic Map–based chaotic RC4 method is comparatively analyzed for image encryption. For both methods, encryption and decryption operations were performed on RGB images, and several cryptographic metrics including processing time, histogram analysis, adjacent pixel correlation, entropy, MSE, PSNR, NPCR and UACI were evaluated. The findings indicate that the RC4 algorithm is faster in terms of encryption and decryption time, while the Chaotic RC4 method demonstrates higher performance in terms of histogram homogeneity, decreasing correlation, increasing entropy values, and resistance to differential attacks. NPCR and UACI results further indicate that the chaotic RC4 method is more sensitive to slight pixel changes, offering stronger security compared to traditional RC4. These findings show that chaos-enhanced stream cipher methods are effective alternatives for improving the security of image data.

Keywords: *Data security; Cryptology; Chaotic; RC4; Image encryption*

1. Giriş

Dijital görüntülerin güvenliği, günümüzün yoğun veri paylaşımı gerektiren teknolojik ekosisteminde kritik bir öneme sahiptir. İnternet üzerinden aktarılan görüntülerin yetkisiz erişime, manipülasyona veya kopyalamaya karşı korunması hem bireysel hem de kurumsal uygulamalarda temel bir gereklilik haline gelmiştir. Bu nedenle görüntülerin şifrelenerek güvenli biçimde iletilmesi, modern bilgi güvenliği yaklaşımlarının önemli bir parçasını oluşturur.

Açık haberleşme kanalları üzerinden veri iletimi sırasında bilginin yetkisiz kişiler tarafından dinlenmesi, değiştirilmesi veya bozulması riski, ciddi bir sorun oluşturmaktadır. İki nokta arasındaki iletişimde ya da sistemler arasındaki veri transferlerinde güvenliğin sağlanması kritik bir öneme sahiptir. Bu nedenle veri, açık haberleşme kanalları üzerinden iletilmeden önce şifrelenerek güvence altına alınır (Gençoğlu ve Yerlikaya 2019). Şifreleme, hassas bilgilerin korunmasını sağlamak için kullanılan temel yöntemlerden biridir (Singh ve Supriya 2013).

Şifre çözme işlemi ise şifrelenmiş verilerin orijinal ve anlaşılır formuna geri döndürülmesini ifade eder. Bu süreçte, sistem hatalı verileri filtreleyerek düzenler ve ardından hem insan hem de bilgisayar tarafından kolayca anlaşılabilecek metin ya da görseller oluşturur. Genel olarak şifre çözme manuel, otomatik veya belirli anahtar ve şifre kombinasyonlarıyla gerçekleştirilebilir (Ayushi 2010). Günümüzde yazılım geliştiricilerden, deneyim

*Sorumlu Yazar/Corresponding Author: Muhammed Baki KARHAN e-posta/e-mail: muhammed.karhan@ogr.ebyu.edu.tr

seviyeleri ne olursa olsun, uygulamalarını kriptografik yöntemlerle güvence altına almaları beklenmektedir (Buhurcu 2022). Başka bir deyişle, kriptografi artık yalnızca belirli uygulamalar için gizli iletişim sağlamaya yönelik basit teknikler bütünü olmaktan çıkmış, dünya genelinde sistem güvenliğini sağlamada kritik bir bilim dalına dönüşmüştür (Katz Lindell 2020).

Görüntü şifrelemede yaygın olarak kullanılan yöntemler arasında simetrik anahtar tabanlı akış ve blok şifreleme algoritmaları yer almaktadır (Biswas ve Basuli 2012). Simetrik şifreleme yöntemleri, tek bir gizli anahtarın hem şifreleme hem de şifre çözme işlemlerinde kullanılması sebebiyle yüksek hız ve düşük hesaplama maliyeti sunmaktadır. AES, RC4, DES ve Blowfish gibi algoritmalar bu sınıfta değerlendirilmektedir (Dibas ve Sabri, 2021). Asimetrik şifreleme algoritmaları ise iki ayrı anahtar (açık ve gizli anahtar) kullanarak daha yüksek güvenlik sağlamakta ancak görüntü gibi yüksek boyutlu verilerde performans düşüklüğü nedeniyle sınırlı kullanılmaktadır.

Son yıllarda kaotik sistemlerin kriptografi alanında kullanımı büyük ilgi görmektedir. Kaotik sistemler, deterministik olmalarına rağmen başlangıç koşullarına yüksek duyarlılık ve rastgeleliğe yakın karmaşık davranışlar sergilemeleri nedeniyle güçlü anahtar dizileri üretebilmektedir. Bu özellikleri, özellikle görüntü şifreleme gibi yüksek güvenlik gerektiren uygulamalarda önemli avantajlar sağlamaktadır. Logistic map, Tent map, Henon map gibi kaotik fonksiyonlar akış şifreleme algoritmalarına entegre edilerek güvenliği artıran hibrit yöntemler geliştirilmiştir.

Görüntü verilerinin doğasında yüksek piksel korelasyonu ve bölgesel benzerlikler bulunduğundan, güvenli bir şifreleme algoritmasının bu yapıları mümkün olduğunca bozması ve şifreli görüntüde rastgeleliğe yakın bir dağılım üretmesi beklenir. Bu nedenle histogram düzleşmesi, bitişik piksel korelasyonunun azaltılması, entropi artışı, NPCR ve UACI gibi ölçütler görüntü güvenliği açısından kritik değerlendirme metrikleridir (Feng ve Yun 2016; Ye vd. 2016; Zhou vd. 2015).

Bu çalışmada, klasik RC4 akış şifreleme algoritması ile Logistic map tabanlı kaotik sistemle güçlendirilmiş RC4 yöntemi görüntü şifreleme uygulaması üzerinde karşılaştırılmıştır. RC4, basit yapısı ve düşük hesaplama maliyeti nedeniyle geçmişte yaygın olarak kullanılmış bir algoritmadır ancak literatürde çeşitli güvenlik açıkları tespit edilmiştir. Kaotik sistemle güçlendirilmiş RC4 ise, anahtar akışının istatistiksel yapısını iyileştirerek güvenlik seviyesini artırmayı amaçlamaktadır. Bu kapsamda her iki algoritma renkli görüntüler üzerinde uygulanarak işlem süresi, histogram, korelasyon, entropi, PSNR, MSE, NPCR ve UACI gibi kapsamlı güvenlik metrikleri ile karşılaştırma yapılmıştır. Elde edilen bulgular, RC4'ün hız açısından avantajlı olmasına karşın kaotik sistem entegrasyonunun rastgelelik ve güvenlik parametrelerinde belirgin iyileşme sağladığını ortaya koymaktadır.

2. İlgili Çalışmalar

Görüntü şifreleme alanında yapılan çalışmalar hem klasik simetrik şifreleme algoritmalarını hem de kaotik sistemlere dayalı modern yöntemleri kapsamaktadır. RC4, AES ve DES gibi geleneksel algoritmalar uzun yıllardır kullanılmakta olup özellikle hız ve düşük hesaplama maliyeti açısından avantaj sağlamaktadır. 2006 yılında yapılan bir çalışmada RC4 algoritmasının performansının anahtar uzunluğu ve veri boyutuna bağlı olarak değiştiği ortaya koyulmuştur (Mousa ve Hamad 2006). Simetrik şifreleme algoritmalarından biri olan RC4 ise 1987 yılında Rivest tarafından veri güvenliğini sağlamak amacıyla geliştirilmiştir (Rivest vd. 1978; Singhal ve Raina 2011; Yüksel vd. 2021). RC4, veriyi şifrelerken her bir bit için sürekli olarak bir anahtar akışı üretir ve bu anahtar akışını verinin her bir bitine XOR işlemi ile ekler. Bu işlem şifreli verinin açık veriden tamamen farklı bir formda olmasını sağlar. RC4, hızlı ve verimli olması nedeniyle birçok uygulamada, özellikle internet güvenliği ve veri şifreleme alanlarında yaygın olarak kullanılmıştır (Alsharida vd. 2021; Sujatha vd. 2024; Zhang vd. 2020).

2011 yılında yapılan bir çalışmada, Discrete Wavelet Transform (DWT) ve RC4 Akış Şifreleme algoritması kullanılarak hızlı bir kısmi görüntü şifreleme sistemi önerilmiştir (Sasidharan ve Philip 2011). Çalışmada, görüntünün yaklaşık matrisinin (en düşük frekans bandı) şifrelenmesi sağlanmıştır çünkü bu bölüm görüntü verilerinin çoğunu içermektedir. Sadece görüntünün bir kısmı şifrelenip geri kalan kısmı karıştırılarak şifreleme süresi azaltılmış, bu sayede yüksek güvenlik seviyesi korunmuştur. Büyük hacimli görüntüler için hesaplama gereksinimlerini azaltma amacıyla geliştirilen bu şifreleme yöntemi, hızlı bir görüntü şifreleme algoritması olarak tanımlanmıştır. Ancak, şifrelenmiş görüntülerin PSNR (Pik sinyal-gürültü oranı) değerlerinin daha düşük olduğu ve bu nedenle istatistiksel saldırılara karşı daha savunmasız olabileceği belirtilmiştir.

2012 yılında sıkıştırılmış görüntülerin şifrelenmesi için yeni bir yöntem önerilmiştir (Al-Maadeed vd. 2012). Bu çalışmada, şifreleme işlemi kaotik haritalara dayalı bir algoritma kullanılarak gerçekleştirilmiştir. Araştırmanın sonuçlarına göre, şifreleme sırasında kullanılan harici anahtar sayılarının artması, orijinal görüntü ile şifrelenmiş görüntü arasındaki korelasyonu azaltarak güvenlik

seviyesini yükseltmiştir. 2016 yılında yapılan bir tez çalışmasında, kaotik sistemlerin farklı özellikleri ile modern şifreleme algoritmaları birleştirilerek kaos tabanlı yöntemlerin güvenlik seviyesini belirgin şekilde artırdığı gösterilmiştir (Çavuşoğlu 2016). 2019 yılında yapılan bir çalışmada, DES, AES ve RC4 gibi klasik algoritmalar görüntü üzerinde değerlendirilmiş, AES'in güvenlik metriklerinde daha başarılı olduğu raporlanmıştır (Atalay vd. 2019). 2020 yılında yapılan bir tez çalışmasında ise RC4 şifreleme algoritması ve Haar dalgacık dönüşümünü bir araya getirerek bir görüntü şifreleme yöntemi önerilmiştir (Yasin ve Saraçoğlu 2020).

Kaotik sistemler ile güçlendirilmiş RC4 şifreleme yöntemi, RC4'ün klasik özelliklerine ek olarak kaotik sistemlerin rastgelelik ve güvenlik özelliklerini entegre eder. Bu yaklaşım, şifreleme sürecinin güvenliğini artırır, verilerin daha zor çözülmesini sağlar ve daha düşük korelasyonlu şifreli veriler üretir. Bu, özellikle yüksek güvenlik gereksinimlerine sahip uygulamalarda önemli avantajlar sunar. Son yıllarda kaotik sistem temelli görüntü şifreleme üzerine yapılan çalışmaların sayısı önemli ölçüde artmıştır. 2022 yılında yayımlanan bir araştırmada, kaotik harita ve rastgele ikame stratejisini kullanan hafif bir şifreleme algoritması geliştirilmiş ve NPCR, UACI, PSNR gibi metrikler üzerinden kapsamlı performans değerlendirmeleri yapılmıştır. Sonuçlar, kaotik tabanlı yöntemlerin RGB görüntülerde yüksek rastgelelik ve düşük korelasyon değerleri ürettiğini göstermiştir (Alghamdi vd. 2022). 2023 yılında yayımlanan bir çalışmada, görüntü şifrelemesi için yeni bir kaotik permütasyon mekanizması önerilmiş ve kaotik sistemin özellikle piksel permütasyonu aşamasında güvenliği önemli ölçüde artırdığı gösterilmiştir (Alawida 2023). 2023 yılında yayımlanan kapsamlı bir derleme çalışmasında, kaos tabanlı görüntü şifreleme yöntemlerinin temel prensipleri, uygulama alanları ve güvenlik analizleri detaylı biçimde sunulmuş histogram, korelasyon, entropi ve diferansiyel saldırı metriklerinin güvenlik değerlendirmesinde kritik öneme sahip olduğu vurgulanmıştır (Zhang ve Liu 2023). Bu çalışma, kaotik sistemlere dayalı yaklaşımların literatürde güçlü bir yer edindiğini göstermektedir. 2025 yılında yapılan çalışma ise kaotik görüntü şifreleme yöntemlerinin klasik yöntemlere göre çok daha yüksek rastgelelik ve saldırı dayanımı sunduğunu göstermektedir (Salih ve Zeebaree 2025).

3. Materyal ve Metot

Bu çalışmada, RC4 ve Logistic Map tabanlı kaotik RC4 yöntemleri kullanılarak görüntü şifreleme ve çözme işlemleri gerçekleştirilmiştir. Çalışma Intel Core i5 12. nesil 12 çekirdekli işlemci, 16 GB RAM ve 8 GB GPU'ya sahip bir bilgisayarda, Windows işletim sistemi üzerinde gerçekleştirilmiştir. Uygulamalar, Python programlama dili kullanılarak geliştirilmiş ve OpenCV, NumPy ve PyCryptodome kütüphaneleri ile desteklenmiştir.

3.1 RC4 Algoritması ile Görüntü Şifreleme

RC4, 1987 yılında Ron Rivest tarafından geliştirilen, değişken uzunlukta anahtar kullanan bir simetrik akış şifreleme algoritmasıdır. Algoritmanın temel prensibi, bir durum tablosu (S-Box) oluşturarak bu tabloyu anahtar bilgisiyle karıştırarak rastgele görünümlü bir anahtar akışı üretmektir (Rivest vd. 1978). Üretilen anahtar akışı, düz veri ile bit düzeyinde XOR işlemi uygulanarak şifreleme ve şifre çözme işlemlerinde kullanılır. RC4 algoritmasının yapısı hem şifreleme hem de şifre çözme işlemlerinin aynı mekanizma ile simetrik şekilde gerçekleştirilmesine olanak tanır. Basit ve hızlı yapısı nedeniyle özellikle düşük işlem gücüne sahip sistemlerde yaygın olarak tercih edilmiştir; ancak ilerleyen yıllarda algoritmanın bazı güvenlik açıkları tespit edilmiş ve kullanımında dikkat edilmesi gerektiği anlaşılmıştır.

Görüntü şifreleme sürecinde RC4 algoritmasının kullanımı sırasında, ilk olarak görüntü verisi RGB kanallarına ayrılarak tek boyutlu (düz) veri akışına dönüştürülmektedir. Bu işlem için:

- Giriş: renkli görüntü Iboyutları $H \times W \times 3$(yükseklik H, genişlik W). Her pikselin üç kanalı vardır: R, G, B. Kanal değerleri $\{0, \dots, 255\}$aralığında 8-bit tamsayılardır.

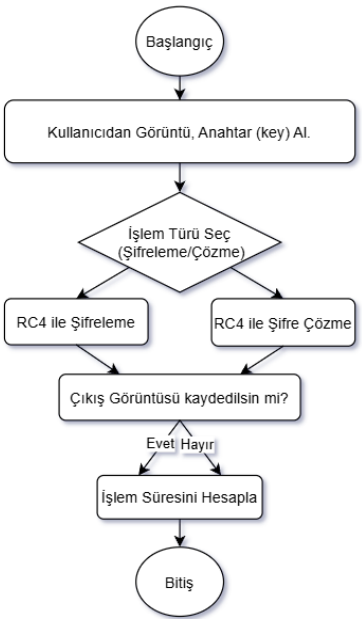
- Piksel sıralaması: görüntü satır-satır okunur yani önce üst satırın sol-üst pikselinden başlayarak sağa doğru, sonra bir sonraki satıra geçilir. Her piksel için kanallar (R, G, B) sırasıyla alınır. Yani çıktı dizisi şu sırayı takip eder:

$$[R_{0,0}, G_{0,0}, B_{0,0}, R_{0,1}, G_{0,1}, B_{0,1}, \dots, R_{H-1,W-1}, G_{H-1,W-1}, B_{H-1,W-1}]$$

- Elde edilen tek boyutlu vektörün uzunluğu $N = H \times W \times 3$ bayttır. Bu vektör şifreleme işlemine doğrudan girer ve her giriş baytı şifreleyici keystream ile XORlanır.

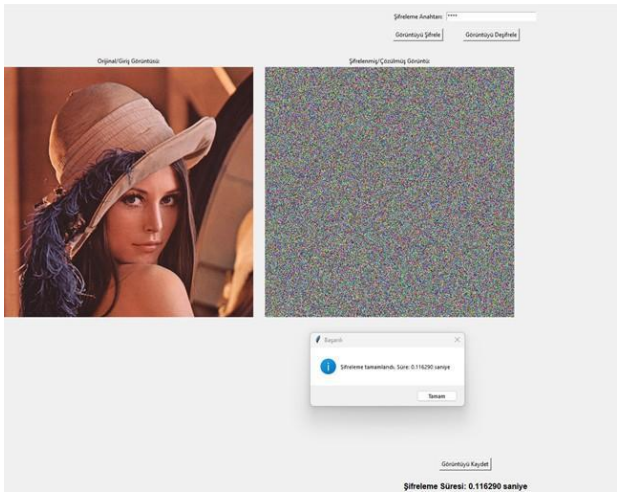
RC4, 256 baytlık bir S-box (permutation) üzerinden anahtar tabanlı karıştırma ile bir keystream üretir. Anahtar Planlama Algoritması KSA (Key Scheduling Algorithm) S-box'u başlatır ve anahtara göre permütasyonu oluşturur. Sahte Rastgele Üretim Algoritması PRGA (Pseudo-Random Generation Algorithm) ise bu S-box'u kullanarak ardışık keystream baytları üretir. Ardından, şifreleme işlemi için belirlenen anahtar yardımıyla bir durum tablosu oluşturulmakta ve bu tablo kullanılarak rastgele bir anahtar akışı elde edilmektedir. Elde edilen bu anahtar akışı, görüntü verisi

ile bit düzeyinde XOR işlemine tabi tutularak şifrelenmiş görüntü oluşturulmaktadır. Şifre çözme işlemi ise aynı anahtar kullanılarak gerçekleştirilmekte ve şifrelenmiş veri ile anahtar akışı arasında yeniden XOR işlemi uygulanarak orijinal görüntü verisi geri elde edilmektedir. Bu çalışmada, RC4 algoritması kullanılarak görüntü şifreleme ve şifre çözme işlemlerini gerçekleştiren iki farklı uygulama geliştirilmiştir. Geliştirilen ilk uygulamada, RC4 algoritması kullanılarak görüntü verisinin şifrelenmesi ve deşifre edilmesi sağlanmıştır. Sürecin akış diyagramı Şekil 1'de gösterilmiştir.



Şekil 1. RC4 ile görüntü şifreleme/deşifreleme gerçekleştirilmesi akış diyagramı.

Geliştirilen uygulama, kullanıcı dostu bir arayüz sunarak şifreleme ve şifre çözme işlemleri için farklı butonlar içermektedir. İşlem tamamlandığında, işlem süreleri ekranda görüntülenirken, şifrelenen veya deşifrelenen görüntülerin kaydedilmesine de olanak tanımaktadır. RC4 algoritması, düşük işlemci gücü gerektirmesi sayesinde hızlı şifreleme ve çözme imkânı sunarken, XOR tabanlı yapısı sayesinde basit ve kolay uygulanabilir bir yöntemdir. Ayrıca, farklı görüntü formatlarına kolayca uyarlanabilir olması ile geniş bir kullanım alanına sahiptir. İlk uygulamanın arayüzü Şekil 2'de verilmiştir. Uygulama kullanıcı dostu ve sade bir tasarıma sahiptir. Kullanıcı, öncelikle bir şifreleme anahtarı girerek işlem yapmak istediği görüntüyü klasörden seçer. Arayüzde sol tarafta, orijinal veya giriş görüntüsü yer alırken, sağ tarafta şifrelenmiş ya da şifre çözülmüş görüntü gösterilir. Kullanıcı, "Görüntüyü Şifrele" düğmesine basarak seçilen görüntüyü RC4 algoritması ile şifreleyebilir veya "Görüntüyü Deşifrele" düğmesini kullanarak şifrelenmiş görüntüyü tekrar orijinal haline getirebilir. İşlem tamamlandığında, ekrana bir bilgilendirme penceresi açılarak şifreleme süresi kullanıcıya gösterilir. Ayrıca, arayüzde yer alan "Görüntüyü Kaydet" butonu sayesinde kullanıcı, şifrelenmiş veya şifresi çözülmüş görüntüyü kaydedebilir.



Şekil 2. RC4 ile görüntü şifreleme/deşifreleme uygulama arayüzü.

3.2 Kaotik Yöntem ile Güçlendirilmiş RC4 Algoritması ile Görüntü Şifreleme

Kaotik sistemler, deterministik yapıda olmalarına rağmen başlangıç koşullarına son derece duyarlı olmaları ve uzun vadede rastgele gibi görünen bir davranış sergilemeleriyle bilinirler. Bu özellikleri sayesinde kriptografi ve özellikle görüntü şifreleme alanında güçlü ve karmaşık anahtar dizileri üretmek amacıyla sıklıkla kullanılmaktadırlar. Kaotik sistemler, küçük bir başlangıç değeri değişiminin bile büyük farklılıklara yol açabilmesi nedeniyle, şifreleme sistemlerinde öngörülemezlik ve güvenlik seviyesini artırmak için etkili bir araç sunmaktadır.

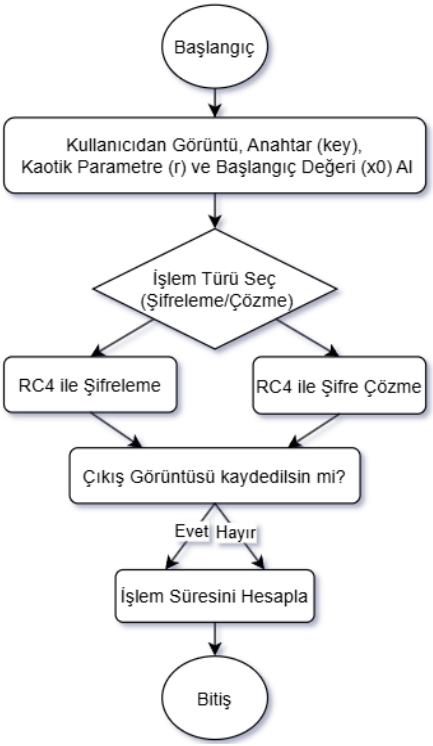
Logistic map, kaotik bir sıra üretmek için kullanılan deterministik bir sistemdir. r (kaotik parametre) ve x0 (başlangıç değeri) ile belirlenen bu dizi, rastgele gibi görünen bir yapı oluşturur. RC4 algoritmasında anahtar karıştırma ve akış üretme aşamalarına entegre edilerek güvenlik artırılır. Logistic map, Kaotik denklem formülü Eşitlik 1'de ifade edilmektedir.

$$x_{n+1} = r.x_n.(1 - x_n) \qquad (1)$$

Burada r kaotik parametre ($0 < r \leq 4$) ve x başlangıç değeri ($0 < x < 1$) olup, iteratif şekilde yeni değerler üretilir.

İkinci uygulamada kaotik yöntemle güçlendirilmiş RC4 algoritması ile şifreleme/deşifreleme işlemleri yapılır. Geleneksel RC4 algoritması üzerine kaotik davranış eklenerek, sistemin güvenliği artırılır ve algoritmanın tahmin edilebilirliği düşürülür. Bu uygulamaya ait akış diyagramı Şekil 3'te verilmiştir.

Çalışmada Logistic map için r = 3.9 ve x = 0.5 değerleri seçilmiştir. r = 3.9, Logistic map'in tam kaotik bölgede çalışmasını sağlayarak üretilen dizinin rastgelelik düzeyini artırır. Başlangıç değeri olarak x = 0.5 seçilmesi ise sistemin hızlıca kaotik davranış göstermesine ve geniş bir değer aralığında dağılmasına katkı sağlar. Böylece hem şifreleme güvenliği artırılmış hem de anahtar üretim süreci daha güçlü hale getirilmiştir.

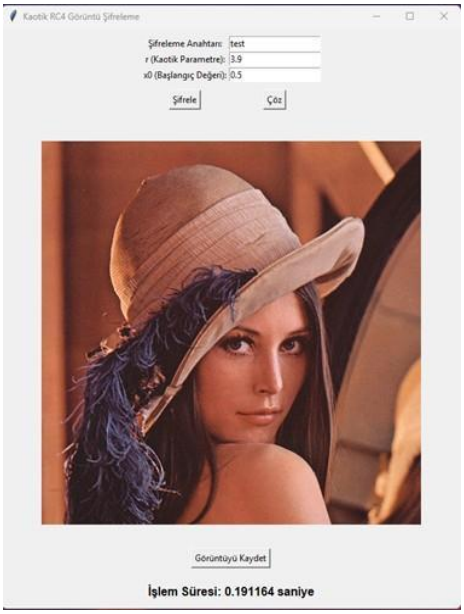


Şekil 3. Kaotik sistemle güçlendirilmiş RC4 ile görüntü şifreleme/deşifreleme gerçekleştirilmesi akış diyagramı.

Şekil 4'te gösterilen kullanıcı dostu bir arayüzle Kaotik RC4 ile hem şifreleme hem de çözme işlemleri hızlı ve etkili bir şekilde gerçekleştirilebilir. Üst kısımda, kullanıcıdan gerekli girişleri almayı sağlayan üç metin kutusu bulunmaktadır. Bunlar sırasıyla şifreleme anahtarı (key), kaotik parametre (r) ve başlangıç değeri (x0) için ayrılmıştır. Kullanıcı, bu değerleri girerek "Şifrele" veya "Çöz" butonları ile işlemi başlatabilir. İşlem tamamlandığında, orijinal veya şifrelenmiş görüntü arayüzde görüntülenir. Çıkış ekranının alt kısmında, elde edilen görüntüyü kaydetmek için "Görüntüyü Kaydet" düğmesi yer alırken, hemen altında da işlem süresini gösteren bir metin alanı bulunmaktadır.

4. Bulgular

Bu bölümde RC4 ve Kaotik RC4 algoritmalarının Lena görüntüsü üzerinde gerçekleştirilmiş şifreleme ve şifre çözme işlemlerine ilişkin deneysel sonuçlar kapsamlı şekilde sunulmaktadır. Analiz sürecinde işlem süresi, histogram dağılımı, bitişik piksel korelasyonu, entropi, MSE, PSNR, NPCR ve UACI gibi kriptografik ve istatistiksel değerlendirme ölçütleri kullanılmıştır. Bu ölçütler, görüntü tabanlı şifreleme algoritmalarının güvenliğini çok yönlü şekilde değerlendirmeye olanak tanımakta ve algoritmalar arasındaki performans farklarını daha net bir biçimde ortaya koymaktadır.



Şekil 4. Kaotik sistemle güçlendirilmiş RC4 görüntü şifreleme/deşifreleme uygulama arayüzü.

4.1 İşlem Süresi Analizi

RC4 ve Kaotik RC4 algoritmalarının işlem süreleri Çizelge 1'de sunulmuştur. İşlem süreleri, her iki yöntemin pratik kullanım açısından değerlendirilmesinde kritik bir ölçüt olup, özellikle gerçek zamanlı uygulamalarda performansı doğrudan etkilemektedir.

Çizelge 1. Yöntemlerin çalışma süresi.

Şifreleme Yöntemi	Şifreleme Süresi (saniye)	Şifre Çözme Süresi (saniye)
RC4	0.114479	0.117975
Kaotik RC4	0.209017	0.191164

Görüntü verileri, içerdikleri yüksek miktarda piksel bilgisi nedeniyle metin ya da ses verilerinden çok daha büyük veri hacmine sahiptir. Bu sebeple görüntü şifreleme sürecinde işlemsel yük önemli bir faktördür. RC4 algoritması, yapısının basit olması ve ek matematiksel hesaplama gerektirmemesi sebebiyle oldukça hızlı çalışmakta; şifreleme ve çözme işlemlerinde düşük işlem süresi sunmaktadır. RC4, iki temel aşamadan oluşmaktadır: KSA (Key Scheduling Algorithm – Anahtar Zamanlama Algoritması), verilen gizli anahtarı kullanarak 256 elemanlı durum tablosunu (S-Box) karıştıran ve başlangıç permütasyonunu oluşturan aşamadır. PRGA (Pseudo Random Generation Algorithm – Sözde Rastgele Akış Üretim Algoritması) ise bu durum tablosunu

kullanarak şifrelemede kullanılacak sözde rastgele anahtar akışını üreten aşamadır. RC4'ün yüksek hız sunmasının temel sebeplerinden biri, bu iki aşamanın tamamen hafif ve XOR tabanlı işlemlerle çalışmasıdır.

Kaotik RC4 algoritmasında ise Logistic Map'ten türetilen kaotik dizinin hem KSA hem de PRGA aşamalarına entegre edilmesi hesaplama maliyetini artırmaktadır. Buna rağmen söz konusu ek maliyet, güvenlik kazanımlarıyla karşılaştırıldığında kabul edilebilir düzeydedir. Kaotik RC4 zaman açısından RC4'ten daha yavaş olsa da özellikle yüksek güvenlik gerektiren görüntü şifreleme uygulamalarında bu fark göz ardı edilebilir.

4.2 Histogram Analizi

Histogram analizi, şifrelenen görüntülerin istatistiksel özelliklerini değerlendirmede kullanılan temel yöntemlerden biridir. Güvenli bir görüntü şifreleme algoritmasının, şifreli görüntüdeki piksel değerlerini mümkün olduğunca geniş bir aralığa yayması ve her renk kanalında homojen bir yoğunluk dağılımı oluşturması beklenir. Bu nedenle histogram analizi yalnızca birleşik histogram üzerinden değil, R, G ve B kanallarının ayrı ayrı incelenmesiyle daha anlamlı sonuçlar vermektedir.

Bu çalışmada RC4 ve Kaotik RC4 algoritmaları için her bir renk kanalına ait histogram korelasyon değerleri hesaplanmış ve değerlendirme sonuçları Çizelge 2'de sunulmuştur. RC4 algoritması için kırmızı, yeşil ve mavi kanallarında elde edilen korelasyon değerleri sırasıyla 0.0501, 0.0026 ve 0.0188'dir. Bu değerler RC4'ün özellikle R kanalında istatistiksel bağımsızlığı tam olarak sağlayamadığını, bazı yoğunluk bölgelerinde kümelenmeler oluştuğunu ve histogram yapısının tam anlamıyla üniform olmadığını göstermektedir.Kaotik RC4 algoritması için histogram korelasyon değerleri R: 0.0271, G: 0.0081 ve özellikle B: –0.0894 olarak elde edilmiştir. B kanalındaki negatif korelasyon değeri, kaotik sistemin RC4'ün karıştırma sürecine eklediği doğrusal olmayan etkinin güçlü bir istatistiksel ayrışma yarattığını ve piksel yoğunluklarının bağımsızlaştığını göstermektedir. Ayrıca Kaotik RC4'ün üç kanal için de daha homojen bir histogram yapısı ürettiği, belirgin tepe noktalarının ortadan kalktığı ve orijinal görüntüye ait istatistiksel izlerin çok daha etkili biçimde maskelendiği gözlemlenmiştir.

Çizelge 2'de sunulan sonuçlar genel olarak değerlendirildiğinde, RC4 algoritmasının düşük işlem maliyetine sahip olması nedeniyle belirli düzeyde rastgelelik sağlasa da histogram tabanlı saldırılara karşı sınırlı koruma sunduğu anlaşılmaktadır. Buna karşın Kaotik RC4 algoritması, kanal bazlı histogram düzeyinde sunduğu daha güçlü rastgelelik, daha yüksek uniformluk ve daha düşük korelasyon değerleriyle istatistiksel güvenlik açısından belirgin bir üstünlük göstermektedir. Bu bulgular, kaotik sistemlerin RC4 yapısına entegre edilmesinin şifreleme güvenliğini anlamlı ölçüde artırdığını doğrulamaktadır.

Çizelge 2. RC4 ve Kaotik RC4 Algoritmalarının RGB Kanal Bazlı Histogram Analizi Sonuçları.

Kriter	RC4	Kaotik RC4	Yorum
R Kanalı Histogram korelasyonu	0.0501	0.0271	Kaotik RC4, R kanalında daha düşük korelasyon üreterek daha güçlü rastgelelik sağlar.
G Kanalı Histogram Korelasyonu	0.0026	0.0081	Her iki yöntem de düşük korelasyon gösterse de RC4 daha düşük değer üretmiştir; ancak fark minimaldir.
B Kanalı Histogram Korelasyonu	0.0188	–0.0894	Kaotik RC4'ün negatif korelasyonu, istatistiksel bağımlılığın en güçlü şekilde kırıldığını gösterir.
Histogram Üniformluğu	Orta düzey, bazı tepe noktaları görülür.	Yüksek düzeyde uniform, tepe noktaları yoktur.	Kaotik RC4, daha homojen histogram yapısı üretir.
Renk Kanal Bağımsızlığı	Bazı kanallarda yoğunluk kümelenmesi devam eder	Kanallar arası bağımsızlık daha yüksektir.	Kaotik RC4'ün karıştırma etkisi daha güçlüdür.
Kriptanaliz Dayanıklılığı	Sınırlı	Yüksek	Kaotik RC4 histogram tabanlı saldırılara karşı daha dirençlidir.

4.3 Bitişik Piksel Korelasyon Analizi

Bir şifreleme yönteminin güvenliğini değerlendirirken şifrelenmiş görüntünün bitişik pikseller arasındaki korelasyon değerinin sıfıra mümkün olduğunca yakın olması ideal olarak kabul edilir. Bu, bitişik piksellerin bağımsız hale geldiğini ve dolayısıyla şifreleme yönteminin güçlü olduğunu gösterir. Görüntü üzerinde 5000 adet rastgele piksel çifti seçilerek, Yatay–dikey–diyagonal korelasyonun bu piksel çiftleri üzerinden hesaplanmıştır. İki yöntem için korelasyon değerlendirilmesi Çizelge 3'te verilmiştir. Kaotik RC4, birçok renk kanalında standart RC4 algoritmasına kıyasla daha düşük korelasyon değerleri sağlayarak şifreleme güvenliğini artırmaktadır.

Çizelge 3. Korelasyon oranlarının değerlendirilmesi.

Kanal	Yön	RC4 Korelasyon Değeri	Kaotik RC4 Korelasyon Değeri	Yorum
Kırmızı	Yatay	0.0030	0.0051	RC4 daha düşük bir korelasyon değeri sağlar.
	Dikey	-0.0007	0.0021	RC4, kaotik RC4'e göre daha düşük korelasyon göstermektedir.
	Diyagonal	0.0017	-0.0038	Kaotik RC4, diyagonal yön için daha iyi sonuç vermektedir.
Yeşil	Yatay	-0.0027	0.0001	Kaotik RC4'ün korelasyonu neredeyse sıfıra yakın ve RC4'e kıyasla daha iyi performans sergiler.
	Dikey	0.0032	-0.0019	Kaotik RC4, korelasyonu ters yönde azaltarak daha iyi bir bağımsızlık sağlar.
	Diyagonal	-0.0013	0.0040	RC4, bu yön için kaotik RC4'e göre daha düşük korelasyon gösterir.
Mavi	Yatay	0.0009	-0.0046	Kaotik RC4, korelasyon değerini negatif ve daha düşük seviyeye çekerek üstünlük sağlar.
	Dikey	0.0037	-0.0029	Kaotik RC4, dikey korelasyonu azaltarak daha iyi sonuç verir.
	Diyagonal	-0.0026	-0.0016	RC4, diyagonal yönde kaotik RC4'e göre daha iyi performans göstermektedir.

Bununla birlikte, RC4 bazı durumlarda, özellikle kırmızı kanalın yatay ve dikey yönlerinde, daha düşük korelasyon değerleri sağlayabilmektedir. Ancak genel olarak değerlendirildiğinde, kaotik RC4'ün korelasyon değerlerinin sıfıra daha yakın olması, şifrelenmiş görüntüde bitişik pikseller arasındaki ilişkinin zayıfladığını ve bu sayede şifreleme sürecinin daha güvenli hale geldiğini göstermektedir. Bu durum, kaotik sistemlerin RC4 algoritmasına entegre edilmesinin güvenlik açısından önemli avantajlar sunduğunu kanıtlamaktadır.

4.4 Entropi Analizi

Entropi analizi, bir şifreleme algoritmasının rastgelelik seviyesini ölçmek için kullanılan bir yöntemdir. Yüksek entropi değeri (genellikle 8'e yakın), şifrelenmiş verinin daha rastgele olduğunu ve bilgi sızıntısının düşük olduğunu gösterir. Şifreleme sürecinde entropi ne kadar yüksekse, saldırganlar için veriyi tahmin etmek o kadar zor hale gelir. Kullanılan iki yöntemin entropi değerlendirmesi Çizelge 4'te verilmiştir.

Çizelge 4. Entropi Değerlendirme Tablosu.

Yöntem	Entropi (bit)	Yorum
RC4	7.6347	Entropi değeri yüksek, ancak mükemmel rastgelelik (8 bit) seviyesine ulaşmamıştır.
Kaotik RC4	7.6457	RC4'e kıyasla daha yüksek bir entropi değeri sağlayarak daha iyi rastgelelik göstermektedir.

4.5 MSE ve PSNR Analizi

Şifreli görüntülerin orijinal görüntüden ne kadar ayrıştığını değerlendirmek amacıyla Ortalama Karesel Hata MSE (Mean Squared Error), Tepe Sinyal-Gürültü Oranı PSNR (Peak Signal-to-Noise Ratio) ve Yapısal Benzerlik İndeksi SSIM (Structural Similarity Index) metrikleri hesaplanmıştır. MSE değeri ne kadar düşükse, orijinal görüntü ile şifrelenip geri elde edilen görüntü arasındaki fark o kadar azdır. PSNR görüntü kalitesinin ölçüsüdür, yüksek PSNR daha iyi kalite anlamına gelir. SSIM görüntülerin yapısal benzerliğini ölçer, 1'e ne kadar yakınsa o kadar benzediğini gösterir. Çizelge 5' te her iki yöntem için bu metriklerin sonuçları verilmiştir.

Kaotik RC4'ün MSE değeri RC4'e göre biraz daha düşüktür. Bu durum, kaotik yapı eklemenin hata miktarını az da olsa iyileştirdiğini gösterir. Kaotik RC4'ün PSNR değeri RC4'e göre çok az daha yüksektir. Bu da yine kaotik versiyonun bir miktar daha iyi koruma/geri elde etme performansı sunduğunu gösterir. Kaotik RC4, SSIM açısından RC4 ile aynı performansı göstermiştir. Yapısal benzerlik üzerinde kaotik eklemenin etkisi görülmemektedir.

Çizelge 5. RC4 ve Kaotik RC4 algoritmalarının MSE, PSNR ve SSIM değerleri.

Yöntem	MSE	PSNR (dB)	SSIM
RC4	9424.0	8.3849	0.0086
Kaotik RC4	9397.0	8.3965	0.0086

Bu sonuçlar hem RC4 hem de Kaotik RC4 algoritmalarının orijinal görüntüyü görsel olarak güçlü biçimde bozduğunu ve yapısal bilgiyi başarıyla maskelediğini göstermektedir.

SSIM değerlerinin her iki yöntem için 0.01'in altında çıkması, şifreleme sonrası görüntünün orijinaliyle yapısal benzerlik taşımadığını ve maskelemenin güçlü olduğunu doğrulamaktadır.

4.6 NPCR ve UACI Analizi

Diferansiyel saldırılara karşı dayanıklılığı değerlendirmek amacıyla Piksel Sayısı Değişim Oranı NPCR (Number of Pixels Change Rate) ve Birleşik Ortalama Değişim Yoğunluğu UACI (Unified Average Changing Intensity) metrikleri kullanılmıştır. NPCR, düz görüntüdeki tek bir pikselin değiştirilmesi sonucunda şifreli görüntüde kaç pikselin farklılaştığını gösterirken; UACI, aynı koşul altında şifreli görüntülerin ortalama parlaklık farkını yüzde cinsinden ifade eder. Teorik olarak güçlü bir görüntü şifreleme algoritması için NPCR değerinin %99'un üzerinde, UACI değerinin ise yaklaşık %33 civarında olması beklenmektedir. RC4 algoritması için NPCR değeri %79,62, UACI değeri ise %33,54 olarak elde edilmiştir. UACI değeri kabul edilebilir aralıkta olsa da NPCR'nin %80'in altında kalması, RC4 algoritmasının girişteki tek bir piksel değişikliğini şifreli görüntünün tamamına etkin şekilde yayamadığını göstermektedir. Bu durum RC4'ün diferansiyel saldırılara karşı zayıf bir güvenlik seviyesi sunduğunu ortaya koymaktadır. Çizelge 6' da her iki yöntem için bu metriklerin sonuçları verilmiştir.

Çizelge 6. RC4 ve Kaotik RC4 algoritmaları için NPCR ve UACI sonuçları.

Yöntem	NPCR(%)	UACI (%)
RC4	79.62	33.54
Kaotik RC4	99.61	30.99

Kaotik RC4, %99,61 ile ideal değere çok yakın bir performans göstermektedir. RC4 ise %79,62 ile oldukça düşük kalmaktadır, bu da klasik RC4'ün diferansiyel saldırılara karşı zayıf olduğunu gösterir. NPCR'nin %99'un üzerine çıkması, kaotik dizinin RC4 algoritmasının yayılma (diffusion) mekanizmasını önemli ölçüde güçlendirdiğini ve küçük giriş değişimlerinin şifreli görüntüde küresel bir etkiye dönüştüğünü ortaya koymaktadır. UACI değerinin %30 civarında olması ise parlaklık değişiminin literatürde kabul edilen aralıkta gerçekleştiğini ve kaotik yapının şifreleme sürecine eklediği doğrusal olmayan etkinin tutarlı bir değişim sağladığını göstermektedir. UACI açısından RC4 biraz daha iyi gözükse de fark büyük değildir. Bu sonuçlar Kaotik RC4'ün diferansiyel saldırılara karşı RC4'e kıyasla belirgin şekilde daha yüksek güvenlik sunduğunu açıkça ortaya koymaktadır.

5. Tartışma

Bu çalışmada RC4 ve Kaotik RC4 algoritmalarının görüntü şifreleme performansları zaman, istatistiksel rastgelelik ve diferansiyel saldırı dayanıklılığı açısından kapsamlı biçimde değerlendirilmiştir.

Zaman performansı değerlendirildiğinde RC4'ün hem şifreleme hem de şifre çözme aşamalarında Kaotik RC4'e göre daha hızlı çalıştığı görülmektedir. Bu durum RC4'ün düşük hesaplama maliyetinden kaynaklanmakta olup zaman açısından kritik uygulamalarda RC4'ün avantaj sağladığını göstermektedir. Kaotik RC4 ise lojistik harita entegrasyonu nedeniyle ek işlem yükü oluştursa da bu fark, güvenlik kazanımlarıyla karşılaştırıldığında kabul edilebilir düzeydedir.

Histogram analizi sonuçları, RC4 algoritmasının özellikle R kanalında belirgin yoğunluk kümeleri oluşturduğunu ve tam anlamıyla uniform bir dağılım sağlayamadığını göstermiştir. Kaotik RC4 yöntemi ise üç kanal için de daha homojen bir histogram yapısı üretmiş, B kanalında negatif korelasyon değerine ulaşarak renk kanalları arasındaki istatistiksel bağımlılığı büyük ölçüde ortadan kaldırmıştır. Bu durum Kaotik RC4'ün histogram tabanlı saldırılara karşı daha dirençli olduğunu göstermektedir.

Korelasyon analizinde doğal görüntülerde yüksek düzeyde bulunan bitişik piksel bağımlılığının kırılması amaçlanmaktadır. Kaotik RC4 hem yatay hem dikey hem de diyagonal yönlerde RC4'e kıyasla daha düşük korelasyon değerleri üretmiş, bazı kanallarda korelasyonu sıfırın altına düşürerek güçlü bir decorrelation etkisi sağlamıştır. Bu sonuçlar, kaotik yapının RC4'ün karıştırma kapasitesini belirgin biçimde artırdığını doğrulamaktadır.

MSE, PSNR ve SSIM sonuçları iki algoritmanın da orijinal görüntüyle görsel benzerliği önemli ölçüde azalttığını göstermektedir. PSNR değerlerinin 8–9 dB aralığında düşük çıkması ve SSIM değerlerinin 0.01'in altında olması, her iki yöntemin de görüntü içeriğini etkili şekilde maskelediğini göstermektedir. Kaotik RC4'ün biraz daha yüksek MSE ve biraz daha düşük PSNR değerleri üretmesi, maskeleme etkisinin RC4'e kıyasla daha güçlü olabileceğini göstermektedir.

Diferansiyel analiz sonuçları çalışmanın güvenlik açısından en belirleyici bulgularını sunmaktadır. RC4 için NPCR değeri %79,62'de kalırken Kaotik RC4 için bu değer %99,61'e ulaşmıştır. Bu fark, kaotik yapının RC4'ün yayılma mekanizmasını büyük ölçüde güçlendirdiğini ve girişteki küçük değişikliklerin şifreli görüntünün tamamına hızlı bir şekilde yayılmasını sağladığını göstermektedir. UACI değerlerinin literatürde beklenen aralıklara yakın gerçekleşmesi de bu sonucu desteklemektedir.

Tüm analizler birlikte değerlendirildiğinde RC4 algoritması hız açısından avantajlı olsa da istatistiksel rastgelelik, korelasyon kırma kapasitesi ve diferansiyel saldırı dayanıklılığı açısından sınırlı kalmaktadır. Kaotik RC4 yöntemi ise özellikle güvenliğin öncelikli olduğu uygulamalarda daha tutarlı, daha rastgele ve daha dayanıklı bir şifreleme yapısı sunarak RC4'e göre anlamlı bir üstünlük göstermektedir.

6. Sonuç ve Öneriler

Bu çalışmada RC4 ve Kaotik RC4 algoritmaları görüntü şifreleme bağlamında kapsamlı biçimde değerlendirilmiş ve elde edilen bulgular, kaotik sistemlerin şifreleme güvenliğini anlamlı ölçüde artırdığını ortaya koymuştur. RC4 algoritması hesaplama açısından hızlı olmasına rağmen istatistiksel rastgelelik, korelasyon kırma kapasitesi ve diferansiyel saldırı dayanıklılığı bakımından sınırlı kalmıştır. Buna karşılık Logistic Map ile güçlendirilmiş Kaotik RC4 yöntemi, histogram dağılımının daha homojen olması, korelasyon değerlerinin sıfıra çok yaklaşması, SSIM değerlerinin düşmesi ve özellikle NPCR ile UACI ölçütlerinde elde edilen üstün sonuçlar sayesinde güvenlik açısından daha yüksek performans sergilemiştir. Bu sonuçlar, kaotik yapının RC4 algoritmasına entegre edilmesinin hem rastgelelik hem de saldırı dayanımı açısından belirgin iyileşme sağladığını göstermektedir.

Gelecek çalışmalar kapsamında güvenliğin daha da artırılması için farklı kaotik haritaların (Henon, Tent, Lorenz, Arnold vb.) RC4 ve diğer simetrik şifreleme algoritmalarıyla birleştirilmesi değerlendirilebilir. Ayrıca hibrit yaklaşımlarla hem yüksek hız hem de yüksek güvenlik sunan yeni yöntemlerin tasarlanması önem taşımaktadır. Algoritmaların gerçek zamanlı video işleme sistemlerinde, düşük güçlü gömülü donanımlarda veya IoT cihazlarında performanslarının test edilmesi, pratik uygulanabilirlik açısından kritik bir araştırma alanı olarak görülmektedir. Bunun yanı sıra gelecekte yapay zekâ tabanlı saldırı ve savunma modelleriyle şifreleme yöntemlerinin karşılaştırılması, özellikle adversarial analiz bağlamında önemli katkılar sağlayacaktır.

Elde edilen bulgular, kaotik sistemlerin görüntü şifreleme algoritmalarının güvenlik seviyesini anlamlı şekilde yükselttiğini ve gelecekte yapılacak çalışmalar için güçlü bir temel oluşturduğunu göstermektedir.

Etik Standartlar Bildirgesi

Bu çalışmanın hazırlanma sürecinde bilimsel ve etik ilkelere uyulduğu ve yararlanılan tüm çalışmaların kaynakçada belirtildiği beyan olunur.

Bu çalışma Dr. Öğretim Üyesi Funda AKAR danışmanlığında Muhammed Baki KARHAN tarafından 10.02.2026 tarihinde tamamlanan "Kaotik Sistemle Güçlendirilmiş Hibrit RC4 ve RSA Algoritmaları ile Görüntü Şifreleme: Güvenlik ve Performans Analizi" başlıklı yüksek lisans tezinden türetilmiştir.

Yazarlık Katkı Beyanı

Yazar 1: Kaynaklar, Araştırma, Uygulama, Yazma – orijinal taslak Görselleştirme, Analiz ve yorumlama

Yazar 2: Fikir Sahibi, Araştırma, Biçimsel analiz, Doğrulama, Metodoloji, Görselleştirme, Denetleme/danışmanlık, Yazma/inceleme ve düzenleme

Çıkar Çatışması Beyanı

Yazarların bu makalenin içeriğiyle ilgili olarak beyan edecekleri hiçbir çıkar çatışması yoktur.

Verilerin Kullanılabilirliği

Bu çalışma sırasında oluşturulan veya analiz edilen tüm veriler, yayınlanan bu makaleye dahil edilmiştir.

7. Kaynaklar

Alawida, M., 2023. A novel chaos-based permutation for image encryption. *Journal of King Saud University – Computer and Information Sciences*, **35(6)**, 101595. https://doi.org/10.1016/j.jksuci.2020.10.008

Alghamdi, Y., Munir, A. and Ahmad, J., 2022. A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy*, **24(10)**, 1344. https://doi.org/10.3390/entropy24101344

Al-Maadeed, S., Al-Ali, A. and Abdalla, T., 2012. A new chaos-based image-encryption and compression algorithm. *Journal of Electrical and Computer Engineering*, 2012, **1–12**. https://doi.org/10.1155/2012/179693

Alsharida, R., Hammood, M., Ahmed, M.A., Thamer, B. and Shakir, M., 2021. RC4D: A new development of RC4 encryption algorithm. *Lecture Notes in Networks and Systems*, **180**, 19–30. https://doi.org/10.1007/978-3-030-64758-2_2

Atalay, N.S., Doğan, Ş., Tuncer, T. and Akbal, E., 2019. İmge şifreleme yöntem ve algoritmaları. *DÜMF Mühendislik Dergisi*, **10(3)**, 815–831. https://doi.org/10.24012/dumf.478877

Ayushi, M., 2010. A symmetric key cryptographic algorithm. International *Journal of Computer Applications*, **1(15)**, 1–6. https://doi.org/10.5120/331-502

Biswas, B. and Basuli, K., 2012. A novel process for key exchange avoiding man-in-middle attack. *IJART*, **1(4)**, 75–79.

Buhurcu, H., 2022. Kriptoloji ve Steganografiyle Güvenli İletişim Sistemi Tasarımı. Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Konya.

Çavuşoğlu, Ü., 2016. Kaos tabanlı hibrit simetrik ve asimetrik şifreleme algoritmaları tasarımı ve uygulaması. Doktora Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya, 180 s.

Dibas, H. and Sabri, K.E., 2021. A comprehensive performance empirical study of symmetric algorithms: AES, 3DES, *Blowfish and Twofish. International Conference on Information Technology*, 344–349. https://doi.org/10.1109/ICIT52682.2021.9491644

Diffie, W. and Hellman, M., 1976. New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Feng, Z.W. and Yun, H., 2016. A novel multi-wing chaotic system and circuit simulation. *International Journal*

of Multimedia and Ubiquitous Engineering, **11(7)**, 385–390. https://doi.org/10.14257/ijmue.2016.11.7.38

Gençoğlu, H. and Yerlikaya, T., 2019. Three part hybrid encryption schema. Balkan *Journal of Electrical and Computer Engineering*, **7(4)**, 384–390. https://doi.org/10.17694/bajece.616893

Katz, J. and Lindell, Y., 2020. Introduction to Modern Cryptography. *CRC Press*.

Mousa, A. and Hamad, A., 2006. Evaluation of the RC4 algorithm for data encryption. *International Journal of Computer Science & Applications*, **3**, 44–56.

Rivest, R., Shamir, A. and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21(2)**, 120–126. https://doi.org/10.1145/359340.359342

Sasidharan, S. and Philip, D.S., 2011. A fast partial image encryption scheme with wavelet transform and RC4. *International Journal of Advances in Engineering & Technology*, **1(4)**, 322–331.

Singh, G. and Supriya, S., 2013. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, **67(19)**, 33-38. https://doi.org/10.5120/11507-7224

Salih, M. S., & Zeebaree, S. R. (2025). Enhanced Image Encryption Using Pixel-Block Permutation and Multi-Chaotic Maps with DNA-Based Diffusion. *Journal of Soft Computing and Data Mining*, ***6*(1)**, 347-358.

Singhal, N. and Raina, J.P.S., 2011. Comparative analysis of AES and RC4 algorithms. *International Journal of Computer Trends and Technology*, **1(3)**, 177–182.

Sujatha, M.S., Reddy, M.G.M., Reddy, C.B., Sriyesh, V.S., Sofiya, K. and Sulthan, E.T., 2024. *RC4 cipher based securing of data exchange in smart grid*. 2024 2nd International Conference on Smart Technologies for Power and Renewable Energy (SPECon 2024). https://doi.org/10.1109/SPECON61254.2024.10537563

Yasin, E. and Saraçoğlu, R., 2020. Haar wavelet transformation and RC4 algorithm based image encryption. *International Journal of Applied Mathematics Electronics and Computers*, **8(3)**, 45–49. https://doi.org/10.18100/ijamec.763283

Ye, C.H., Xiong, Z.G., Ding, Y.M., Zhang, X., Wang, G. and Xu, F., 2016. A secure fingerprinted multimedia distribution using social network analysis. *International Journal of Security and Its Applications*, **10(4)**, 209–220. https://doi.org/10.14257/IJSIA.2016.10.4.20

Yüksel, T., Özgün, B. and Güvenliği, B., 2021. RSA ve RC4 algoritmalarının performans karşılaştırması. *Aurum Journal of Engineering Systems and Architecture*, **5(1)**, 29–40. https://doi.org/10.53600/ajesa.864348

Zhang, J., Liu, H. and Ni, L., 2020. A secure energy-saving communication and encrypted storage model based on RC4 for EHR. *IEEE Access*, **8**, 38995–39012. https://doi.org/10.1109/ACCESS.2020.2975208

Zhang, B. and Liu, L., 2023. Chaos-based image encryption: review, application, and challenges. *Mathematics*, **11**, 2585. https://doi.org/10.3390/math11112585

Zhou, G., Zhang, D., Liu, Y., Yuan, Y. and Liu, Q., 2015. A novel image encryption algorithm based on chaos and line map. *Neurocomputing*, **169**, 150–157. https://doi.org/10.1016/j.neucom.2014.08.071