T.C.
ERZİNCAN BİNALİ YILDIRIM ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YAPAY ZEKA VE ROBOTİK ANABİLİM DALI

KAOTİK SİSTEMLE GÜÇLENDİRİLMİŞ HİBRİT RC4 VE RSA ALGORİTMALARI İLE GÖRÜNTÜ ŞİFRELEME: GÜVENLİK VE PERFORMANS ANALİZİ

Muhammed Baki KARHAN

Danışman: Dr. Öğr. Üyesi Funda AKAR

TEZ JÜRİ ÜYELERİ
Dr. Öğr. Üyesi Funda AKAR
Doç. Dr. İsmail AKGÜL
Dr. Öğr. Üyesi Faruk Baturalp GÜNAY

YÜKSEK LİSANS TEZİ
ERZİNCAN, 2026

Kabul ve Onay Sayfası

Dr. Öğr. Üyesi Funda AKAR danışmanlığında, Muhammed Baki Karhan tarafından hazırlanan bu çalışma 22.01.2026 tarihinde aşağıdaki jüri tarafından Yapay Zekâ ve Robotik Anabilim Dalı'nda Yüksek Lisans Tezi olarak oybirliği ile kabul edilmiştir.

Başkan	:	Dr. Öğr. Üyesi Funda AKAR	İmza:
Üye	:	Doç. Dr. İsmail AKGÜL	İmza:
Üye	:	Dr. Öğr. Üyesi Faruk Baturalp GÜNAY	İmza:

Bu tez Enstitü Yönetim Kurulunun …./…./ 20.... tarih ve …../…….. sayılı kararı ile onaylanmıştır.

Doç. Dr. Kemal Volkan ÖZDOKUR
Enstitü Müdür V.

Not: Bu tezde kullanılan özgün ve başka kaynaklardan yapılan bildirişlerin, şekil ve tabloların kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

Bilimsel Etiğe Uygunluk Sayfası

“Kaotik Sistemle Güçlendirilmiş Hibrit RC4 ve RSA Algoritmaları ile Görüntü Şifreleme: Güvenlik ve Performans Analizi” isimli “Yüksek Lisans/ Doktora” tezim tarafımca intihal tespit programı ile incelenmiştir. Buna göre tezimde bilimsel etik ihlali ve intihal olarak nitelendirilebilecek herhangi bir durum olmadığını taahhüt ederim.

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir biçimde elde edildiğini; aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi beyan ederim. 22/01/2026

(İmza)

Muhammed Baki
KARHAN

ÖZET

KAOTİK SİSTEMLE GÜÇLENDİRİLMİŞ HİBRİT RC4 VE RSA ALGORİTMALARI İLE GÖRÜNTÜ ŞİFRELEME: GÜVENLİK VE PERFORMANS ANALİZİ

Muhammed Baki KARHAN

Yüksek Lisans Tezi
Erzincan Binali Yıldırım Üniversitesi, Fen Bilimleri Enstitüsü,
Yapay Zeka ve Robotik Anabilim Dalı
Danışman: Dr. Öğr. Üyesi Funda AKAR
2026, 62 sayfa

Bu tez çalışması, dijital görüntülerin güvenliğinin sağlanmasında şifreleme algoritmalarının rolünü inceleyerek, özellikle kaotik sistemlerle güçlendirilmiş hibrit yaklaşımların güvenlik ve performans üzerindeki etkilerini ortaya koymayı amaçlamaktadır. Günümüzde bireysel ve kurumsal düzeyde artan veri güvenliği ihtiyacı, görüntülerin hem hızlı hem de güvenli bir şekilde korunmasını zorunlu hâle getirmekte; bu durum yeni nesil şifreleme yöntemlerinin geliştirilmesini gerekli kılmaktadır. Bu kapsamda, RC4 algoritması Logistic Map tabanlı kaotik bir sistemle birleştirilerek hibrit bir şifreleme yöntemi önerilmiş; ayrıca klasik RC4, AES ve kaotik AES algoritmaları ile karşılaştırmalı olarak değerlendirilmiştir. Çalışmada, renkli ve gri ölçekli görüntüler üzerinde şifreleme ve şifre çözme işlemleri gerçekleştirilmiş; elde edilen sonuçlar süre bazlı performans ölçütleri ile analiz edilmiş ve histogram, korelasyon ve entropi testleri aracılığıyla güvenlik değerlendirmeleri yapılmıştır. Elde edilen bulgular, RC4 algoritmasının işlem hızı açısından daha avantajlı olduğunu, buna karşın kaotik tabanlı hibrit yöntemlerin güvenlik metrikleri bakımından daha başarılı sonuçlar sunduğunu göstermektedir. Sonuçlar, kaotik hibrit şifreleme yaklaşımlarının görüntü güvenliği alanında daha dirençli ve güvenilir bir alternatif oluşturabileceğini ortaya koymakta; bu yönüyle çalışma hem akademik literatüre hem de pratik uygulamalara önemli katkılar sağlamaktadır.

Anahtar Kelimeler: Görüntü şifreleme, kaotik sistemler, Rc4, Kaotik rc4, Aes, Kaotik aes, Hibrit şifreleme, Histogram analizi, Korelasyon analizi, Entropi analizi, Performans değerlendirmesi

ABSTRACT

IMAGE ENCRYPTION WITH CHAOTIC SYSTEM-ENHANCED HYBRID RC4 AND RSA ALGORITHMS: SECURITY AND PERFORMANCE ANALYSIS

Muhammed Baki KARHAN

Master's Thesis
Erzincan Binali Yıldırım University, Institute of Science and Technology,
Department of Artificial Intelligence and Robotics
Advisor: Asst. Prof. Dr. Funda AKAR
2026, 62 pages

This thesis investigates the role of encryption algorithms in ensuring the security of digital images, with a particular focus on the effects of hybrid approaches strengthened by chaotic systems on both security and performance. The increasing demand for data protection at both individual and organizational levels makes it essential to safeguard images not only rapidly but also securely, thereby emphasizing the need for advanced encryption techniques. Within this scope, a hybrid method is proposed by combining the RC4 algorithm with a Logistic Map-based chaotic system. In addition, the proposed approach is comparatively evaluated against classical RC4, AES, and chaotic AES algorithms. Experimental studies are conducted on both color and grayscale images, and the obtained results are analyzed in terms of encryption and decryption times to evaluate performance. Furthermore, security robustness is assessed using histogram analysis, pixel correlation, and entropy measurements. The findings indicate that although RC4 demonstrates superior performance in terms of computational speed, chaotic-based hybrid approaches achieve more effective results with respect to security metrics. This study demonstrates that chaotic hybrid encryption methods provide a more resilient and reliable alternative for image security, contributing to both academic research and practical applications.

Keywords: Image encryption, Chaotic systems, Rc4, Chaotic rc4, Aes, Chaotic aes, Hybrid encryption, Histogram analysis, Correlation analysis, Entropy analysis, Performance evaluation

TEŞEKKÜR

Yüksek lisans eğitimim süresince bilgi ve birikimiyle çalışmalarımı yönlendiren, akademik gelişimime değerli katkılar sağlayan danışmanım Dr. Öğr. Üyesi Funda AKAR'a teşekkür ederim. Her zaman yanımda olan, sevgisi ve desteğiyle beni bugünlere getiren kıymetli anneme ve babama teşekkürü borç bilirim. Bu süreçte sabrı, anlayışı ve moral veren desteğiyle her zaman yanımda olan sevgili eşime gönülden teşekkür ederim. Ayrıca, desteklerini esirgemeyen değerli iş arkadaşlarıma da teşekkür ederim.

Muhammed Baki KARHAN
Ocak, 2026

İÇİNDEKİLER

ÖZET i
ABSTRACT ii
TEŞEKKÜR iii
İÇİNDEKİLER iv
TABLOLAR DİZİNİ vi
ŞEKİLLER DİZİNİ vii
SİMGELER VE KISALTMALAR DİZİNİ viii
1. GİRİŞ 1
1.1. Araştırmanın Amacı 2
1.2. Araştırmanın Önemi 4
1.3. Varsayımlar 5
2. KAVRAMSAL ÇERÇEVE VE İLGİLİ ÇALIŞMALAR 7
2.1. Kriptoloji 7
2.1.1 Kriptografi 8
2.1.2 Kriptoanaliz 8
2.1.3. Simetrik şifreleme algoritmaları 9
2.1.4. Asimetrik şifreleme algoritmaları 10
2.2. Kaotik Sistemler 11
2.3. Hibrit Şifreleme Yöntemleri 12
2.4. Görüntü Şifreleme 13
2.4.1. Görüntü şifrelemenin uygulama perspektifleri 15
2.4.2. Askeri ve uydu görüntülerinde şifreleme 15
2.4.3. Bulut sistemlerinde görüntü güvenliği 16
2.4.4. Sağlık ve tıbbi görüntülerde şifreleme 16
2.4.5. Biyometrik verilerin şifrelenmesi 16
2.4.6. Eğitim ve e-öğrenmede görüntü güvenliği 17
2.5. Görüntü şifreleme güvenlik ve performans ölçütleri 17
2.5.1. Histogram analizi 18
2.5.2. Korelasyon katsayısı 19
2.5.3. Entropi 20
2.5.4. Npcr ve uacı 21
2.5.5. Psnr ve mse 22
2.6. Ölçütlerin Önemi ve Literatürdeki Kullanımı 24

2.7. İlgili Çalışmalar 26
3. YÖNTEM 31
3.1. Araştırmanın Amacı ve Yaklaşımı 32
3.2. Yazılım ve Donanım Ortamı 33
3.3. Sistem Mimarisi ve Modüller 35
3.3.1. Şifreleme modülü 37
3.3.2. Deşifreleme modülü 43
3.4. Performans ve Güvenlik Analizleri 46
4. BULGULAR 49
4.1. 512 × 512 Renkli Görüntü Şifreleme Sonuçları 49
4.2. 512 × 512 Gri Görüntü Şifreleme Sonuçları 50
4.3. 765 × 603 Renkli Görüntü Şifreleme Sonuçları 51
4.4. 765 × 603 Gri Görüntü Şifreleme Sonuçları 53
4.5. Genel Karşılaştırmalı Değerlendirme 54
5. SONUÇ VE ÖNERİLER 56
KAYNAKÇA 59

TABLOLAR DİZİNİ

Tablo 1. Yazılım Ortamı 34
Tablo 2. Donanım Ortamı 35
Tablo 3. 512 x 512 Renkli Görüntü Şifreleme Performans Tablosu 50
Tablo 4. 512 x 512 Gri Görüntü Şifreleme Performans Tablosu 51
Tablo 5.765 x 603 Renkli Görüntü Şifreleme Performans Tablosu 52
Tablo 6. 765 x 603 Gri Görüntü Şifreleme Performans Tablosu 53

ŞEKİLLER DİZİNİ

Şekil 1. Kriptoloji Bilimi (Sabonchı vd., 2016) 7
Şekil 2. Şifreleme Teknikleri (Yogi vd., 2025) 15
Şekil 3. Şifrelemede Performans Metrikleri (Yogi vd., 2025) 18
Şekil 4. Görüntü Şifreleme Uygulamasının Ana sayfası 36
Şekil 5. Şifreleme Aşamasında Orijinal Görüntünün Arayüz Üzerinde Önizlenmesi 37
Şekil 6. Şifreleme Sonrası Elde Edilen Şifreli Görüntünün Arayüz Üzerinde Gösterimi 38
Şekil 7. Şifreleme Akış Diyagramı 42
Şekil 8. Deşifreleme Aşamasında Şifreli Görüntünün Arayüz Üzerinden Yüklenmesi 44
Şekil 9. Deşifreleme Sonrası Elde Edilen Orijinal Görüntünün Arayüz Üzerinde Gösterimi . 44
Şekil 10. Deşifreleme Akış Diyagramı 45
Şekil 11. Kaotik RC4 + RSA Hibrit Modelinde Şifreleme ve Deşifreleme İşlemlerinin Aynı Arayüz Üzerinde Gösterimi 47
Şekil 12. Klasik RC4 ve Kaotik RC4 Uygulama Arayüz Gösterimi 48
Şekil 13. Klasik AES ve Kaotik AES Uygulama Arayüz Gösterimi 48

SİMGELER VE KISALTMALAR DİZİNİ

H	Entropi değeri
ρ	Korelasyon katsayısı
μ	Ortalama değer
Σ	Toplam sembolü
C	Cipher Image (Şifreli görüntü)
K	Anahtar
r	Logistic Map kontrol parametresi
x_0	Başlangıç değeri (initial condition)
AES	Advanced Encryption Standard
RC4	Rivest Cipher 4
RSA	Rivest–Shamir–Adleman
KRC4+RSA	Kaotik RC4 + RSA Hibrit Algoritması
LM	Logistic Map (Lojistik Harita)
RGB	Red–Green–Blue (Renkli görüntü)
GS	Gray-Scale (Gri seviye görüntü)
HST	Histogram
PSNR	Peak Signal-to-Noise Ratio
SSIM	Structural Similarity Index Measure
GUI	Graphical User Interface
PNG	Portable Network Graphics
JPG/JPEG	Joint Photographic Experts Group Formatı
TKinter	Python GUI Arayüz Kütüphanesi
PSNR	Peak Signal-to-Noise Ratio
SSIM	Structural Similarity Index
T	İşlem Süresi

1. GİRİŞ

Teknolojik gelişmelerin hızla ilerlemesiyle birlikte dijital ortamda üretilen, depolanan ve paylaşılan veri miktarı her geçen gün artmaktadır. Bu artış, bilgiye erişimi kolaylaştırırken aynı zamanda veri güvenliği konusunda ciddi riskleri de beraberinde getirmektedir. Özellikle internet altyapısı üzerinden gerçekleşen veri iletimlerinde, bilgilerin üçüncü şahıslar tarafından izinsiz olarak ele geçirilmesi, değiştirilmesi veya kötüye kullanılması olasılığı, güvenlik zafiyetlerini kaçınılmaz hâle getirmektedir. Bu durum, bireylerden ulusal güvenlik kurumlarına kadar geniş bir yelpazede önemli bir sorun olarak karşımıza çıkmaktadır.

Dijitalleşmenin etkisiyle birlikte Nesnelerin İnterneti (IoT), yapay zekâ tabanlı sistemler, bulut bilişim ve büyük veri uygulamaları gibi alanlar hızla yaygınlaşmıştır. Bu teknolojiler, veri miktarının üstel şekilde artmasına neden olurken, aynı zamanda bu verilerin güvenliğinin sağlanmasını daha da zorlaştırmıştır (Zhang vd., 2020). Özellikle açık ağlar üzerinden veri paylaşımı yapılan durumlarda, verinin gizliliği ve bütünlüğü kritik bir öneme sahiptir.

Görüntü tabanlı veriler, içerdiği zengin bilgi ve yüksek duyarlılık nedeniyle diğer veri türlerine kıyasla daha fazla korunma gerektirmektedir. Günümüzde kişisel fotoğraflar, sağlık verileri, askeri uydu kayıtları, biyometrik veriler, güvenlik kameraları kayıtları ve adli bilişim materyalleri gibi birçok bilgi türü görüntü biçiminde saklanmakta ve iletilmektedir (Ceyhan ve Yolaçan, 2021). Bu nedenle dijital görüntülerin korunması, yalnızca bireysel gizlilik açısından değil; aynı zamanda kamu güvenliği, savunma teknolojileri ve kritik altyapıların güvenliği bakımından da son derece önemlidir.

Veri güvenliğinin sağlanmasında en temel yöntemlerden biri kriptografi, yani şifreleme teknikleridir. Şifreleme, bilgiyi matematiksel işlemler yoluyla anlaşılmaz bir biçime dönüştürerek yalnızca yetkili kullanıcıların erişebilmesini sağlayan bir süreçtir (Kumari vd., 2017). Bu bağlamda kriptografi, modern bilgi güvenliği sistemlerinin en temel bileşenlerinden biri hâline gelmiştir.

Kriptografik algoritmalar genel olarak iki ana grupta incelenmektedir: simetrik (gizli anahtarlı) ve asimetrik (açık anahtarlı) yöntemler. Simetrik sistemlerde aynı anahtar hem şifreleme hem de çözme işlemlerinde kullanılır. Bu durum işlem hızını artırsa da anahtar paylaşımı sırasında güvenlik risklerini beraberinde getirebilir. Asimetrik algoritmalarda ise farklı anahtarlar (açık

ve özel) kullanıldığından güvenlik seviyesi artmakta, ancak işlem süresi uzamaktadır (Katz ve Lindell, 2020). Bu nedenle son yıllarda araştırmacılar, her iki yöntemin güçlü yönlerini bir araya getiren hibrit şifreleme sistemleri üzerine yoğunlaşmıştır (Bermani vd., 2013).

Ayrıca kaotik sistemlerin doğasındaki doğrusal olmayan yapı ve başlangıç koşullarına duyarlılık özellikleri, kriptografi alanında yeni bir araştırma yönü olarak öne çıkmaktadır. Kaotik haritalar sayesinde yüksek düzeyde rastgelelik üretilebilmekte ve düşük hesaplama maliyetiyle güçlü güvenlik seviyeleri sağlanabilmektedir (Benaissi vd., 2023). Literatürde yer alan birçok çalışma, kaotik sistemlerin geleneksel şifreleme algoritmalarına entegre edilmesiyle hem performansın hem de güvenliğin anlamlı biçimde iyileştirilebildiğini göstermektedir (Lan vd., 2018).

1.1. Araştırmanın Amacı

Bu tez çalışmasının temel amacı, mevcut şifreleme yöntemlerinin performans ve güvenlik açısından sahip olduğu sınırlılıkları aşabilecek, daha etkin ve dengeli bir hibrit şifreleme yaklaşımı geliştirmektir. Günümüzde kullanılan birçok klasik şifreleme algoritması, güvenlik ile performans arasında ideal bir denge kurmakta zorlanmaktadır. Bazı yöntemler yüksek güvenlik sağlarken işlem süresi bakımından yavaş çalışmakta, bazıları ise hız avantajına rağmen saldırılara karşı zayıf kalmaktadır. Özellikle yüksek boyutlu görüntü verilerinin güvenli şekilde saklanması ve iletilmesi gereken uygulamalarda bu denge büyük önem taşımaktadır.

Bu araştırmada önerilen hibrit model, hem simetrik hem de asimetrik kriptografik yöntemlerin avantajlarını bir araya getirmeyi hedeflemektedir. Bu kapsamda, simetrik bir akış şifreleme algoritması olan RC4, kaotik tabanlı bir yapı ile güçlendirilmiş ve ardından RSA algoritması ile hibrit biçimde birleştirilmiştir. Geliştirilen yapıda kaotik davranışın elde edilmesi amacıyla Logistic Map fonksiyonu kullanılmıştır. Logistic Map; basit matematiksel yapısına rağmen başlangıç koşullarına karşı yüksek duyarlılık göstermesi, geniş kaotik parametre aralığı sunması ve düşük hesaplama maliyeti gibi özellikleri sayesinde kriptografik uygulamalarda sıklıkla tercih edilen bir modeldir.

RC4 algoritmasının temel avantajı olan yüksek hız korunurken, Logistic Map tarafından üretilen rastgele diziler kullanılarak anahtar akışının öngörülemezliği ve istatistiksel rastgeleliği artırılmıştır. Bu sayede RC4 algoritmasının klasik formunda görülen anahtar tekrarları, düşük

entropi değerleri ve yüksek piksel korelasyonu gibi zayıflıkların giderilmesi amaçlanmıştır. Logistic Map tabanlı bu yapı, RC4 algoritmasının anahtar akışını dinamik olarak etkileyerek her şifreleme oturumunda farklı ve karmaşık bit dizilerinin oluşmasını sağlamaktadır.

Elde edilen bu kaotik RC4 yapısı, daha sonra RSA algoritması ile hibrit bir biçimde birleştirilmiştir. RSA'nın güvenli anahtar paylaşımı ve kimlik doğrulama avantajı, RC4'ün hız performansını tamamlayacak şekilde kullanılmıştır. Bu sayede simetrik şifreleme sistemlerinde karşılaşılan anahtar dağıtımı problemi ortadan kaldırılmış, aynı zamanda sistemin genel güvenlik seviyesi artırılmıştır.

Çalışmada önerilen hibrit yapı yalnızca teorik olarak değil, uygulamalı olarak da test edilmiştir. Python programlama dili kullanılarak geliştirilen sistem, açık kaynak kütüphanelerle desteklenmiş ve farklı boyutlardaki renkli ve gri ölçekli görüntüler üzerinde kapsamlı performans ölçümleri gerçekleştirilmiştir. Bu uygulama süreci, geliştirilen yöntemin hem akademik hem de pratik açıdan uygulanabilirliğini ortaya koymayı amaçlamaktadır.

Bu kapsamda araştırmanın temel hedefleri şu şekilde özetlenebilir:

- Logistic Map kullanılarak RC4 algoritmasının anahtar üretim sürecini iyileştirmek ve daha güçlü bir akış şifreleme yapısı oluşturmak,
- RSA algoritmasıyla hibrit bir yapı kurarak güvenli anahtar paylaşımı ve yetkilendirme sorunlarını ortadan kaldırmak,
- Geliştirilen hibrit RC4–RSA yönteminin performansını ve güvenlik düzeyini AES, kaotik AES, RC4 ve kaotik RC4 algoritmaları ile karşılaştırmalı olarak analiz etmek,
- Elde edilen sonuçlar üzerinden yöntemin dijital görüntü güvenliği açısından uygulanabilirliğini göstermek ve literatüre katkı sunmak.

Sonuç olarak, bu tez çalışması ile Logistic Map tabanlı kaotik yapıların hibrit şifreleme sistemlerine entegrasyonu sağlanmış; hem simetrik hem de asimetrik algoritmaların avantajlarını bir araya getiren yeni bir yaklaşım geliştirilmiştir. Önerilen bu yaklaşım, özellikle yüksek güvenlik ve düşük hesaplama maliyeti gerektiren tıbbi, askeri, biyometrik ve adli bilişim gibi alanlarda kullanılabilecek etkili bir alternatif çözüm olarak tasarlanmıştır.

1.2. Araştırmanın Önemi

Bu çalışmanın önemi birden fazla açıdan değerlendirilebilir. Günümüzde dijital verilerin güvenliği, özellikle görüntü tabanlı bilgilerin korunması, bireysel ve kurumsal düzeyde kritik bir gereklilik hâline gelmiştir. Tıbbi görüntüler, biyometrik veriler, askeri uydu kayıtları, adli bilişim materyalleri ve güvenlik kameralarından elde edilen veriler gibi hassas nitelikteki bilgiler, genellikle internet veya bulut altyapıları üzerinden iletilmekte ve depolanmaktadır. Bu nedenle bu verilerin gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) ilkeleri çerçevesinde korunması, siber güvenlik açısından büyük önem taşımaktadır (NIST, 2017).

Geleneksel şifreleme algoritmaları çoğunlukla hız, anahtar yönetimi ve güvenlik düzeyi arasında etkin bir denge kurma sorunu yaşamaktadır. Simetrik algoritmalar (örneğin RC4 ve AES) yüksek hız sağlarken, anahtar paylaşımı konusunda güvenlik zafiyetleri barındırmaktadır. Buna karşılık asimetrik algoritmalar (örneğin RSA ve ElGamal) güvenli anahtar değişimi imkânı sunsa da işlem karmaşıklığı ve performans açısından çeşitli sınırlılıklara sahiptir (Katz ve Lindell, 2020). Bu tezde önerilen hibrit RC4–RSA yapısı, söz konusu iki yöntemin güçlü yönlerini bir araya getirerek hem güvenliği hem de verimliliği artırmayı amaçlamaktadır. Böylece görüntü tabanlı verilerin korunmasında hem güvenlik seviyesi hem de işlem performansı açısından dengeli ve etkin bir çözüm sunulması hedeflenmiştir.

Bu araştırmanın özgün yönlerinden biri, hibrit şifreleme yapısının kaotik sistemlerle desteklenmiş bir biçimde ele alınmasıdır. Kaotik sistemlerin en belirgin özellikleri olan başlangıç koşullarına aşırı duyarlılık ve doğrusal olmayan yapı, kriptografik süreçlerde rastgelelik üretimi ve anahtar çeşitliliği açısından önemli avantajlar sunmaktadır (Şahin, 2024). Özellikle Logistic Map tabanlı kaotik sistemlerin, düşük hesaplama maliyetiyle yüksek güvenlik seviyesi sağlamada etkili olduğu literatürde çeşitli çalışmalarda gösterilmiştir (Hamadi vd., 2025).

Bu çalışma ayrıca Python programlama dili ve açık kaynak kütüphaneler kullanılarak geliştirilmiş olması bakımından da önem taşımaktadır. Python'un geniş kütüphane desteği, yüksek prototipleme hızı ve güçlü topluluk desteği sayesinde geliştirilen bu yapı, yalnızca akademik düzeyde değil, pratik sistemlerde de uygulanabilir niteliktedir. Bu durum araştırmanın erişilebilirliğini artırmakta ve gelecekte yapılacak çalışmalara kolayca entegre

edilebilmesini sağlamaktadır. Böylelikle tez çalışması, hem akademik literatüre katkı sağlamakta hem de uygulamalı kriptografi alanında yeniden üretilebilir ve genişletilebilir bir model sunmaktadır.

Sonuç olarak, bu araştırma;
Yüksek hacimli görüntü verilerinin güvenli biçimde iletilmesi, şifreleme performansı ile güvenlik arasında etkin bir dengenin sağlanması, kaotik sistemlerin hibrit şifreleme yapılarına entegrasyonu ve açık kaynaklı, uygulanabilir bir modelin geliştirilmesi açısından önemli bir katkı niteliği taşımaktadır. Bu yönüyle çalışma, hem literatürdeki mevcut boşlukların doldurulmasına hem de gelecekte gerçekleştirilecek hibrit ve kaotik tabanlı görüntü şifreleme araştırmalarına yol gösterici bir kaynak olma potansiyeline sahiptir.

1.3. Varsayımlar

Bu araştırmada, geliştirilen hibrit şifreleme yönteminin tasarımı, uygulanması ve değerlendirilmesi sürecinde birtakım varsayımlar yapılmıştır. Bu varsayımlar, çalışmanın kapsamını netleştirmek ve elde edilen sonuçların yorumlanmasında metodolojik bir çerçeve oluşturmak amacıyla belirlenmiştir.

Veri Güvenliği Varsayımı: Çalışmada kullanılan görüntülerin yalnızca şifreleme tabanlı yöntemlerle korunacağı; buna ek olarak herhangi bir ağ güvenlik protokolü, VPN tünelleme yöntemi veya SSL/TLS gibi üst seviye koruma mekanizmalarının devreye alınmadığı varsayılmıştır. Böylece geliştirilen algoritmanın, doğrudan veri düzeyinde sağladığı güvenlik katkısının izole biçimde değerlendirilmesi amaçlanmıştır.

Test Ortamı Varsayımı: Uygulama ve performans analizlerinin Python programlama dili kullanılarak standart donanım ve yazılım koşullarında gerçekleştirildiği kabul edilmiştir. Bu nedenle elde edilen test sonuçlarının, kullanılan donanımın işlem gücü, bellek kapasitesi ve sistem yükü gibi değişkenlerden bağımsız olarak algoritmanın genel performans eğilimini temsil ettiği varsayılmıştır.

Karşılaştırma Parametreleri Varsayımı: Geliştirilen hibrit yöntem, literatürde yaygın olarak kullanılan AES, RC4, kaotik AES ve kaotik RC4 algoritmaları ile karşılaştırılmıştır. Bu karşılaştırmalarda ilgili algoritmaların, literatürde önerilen optimum parametreler ve

konfigürasyon değerleriyle çalıştırıldığı varsayılmıştır. Böylece karşılaştırmalı analizlerin adil ve nesnel biçimde gerçekleştirilmesi hedeflenmiştir (Malik vd., 2020).

Veri Bütünlüğü Varsayımı: Şifreleme işlemleri öncesinde kullanılan görüntü dosyalarının ön işleme adımlarında (yeniden boyutlandırma, format dönüşümü vb.) herhangi bir bilgi kaybı, bozulma veya manipülasyonun meydana gelmediği kabul edilmiştir. Bu varsayım, analizlerin yalnızca şifreleme algoritmasının performansı ve güvenliği üzerine odaklanabilmesi açısından önem taşımaktadır (El-Latif vd., 2022).

Matematiksel Model Varsayımı: Logistic Map tabanlı kaotik sistemin doğrusal olmayan yapısının, rastgelelik ve anahtar çeşitliliği açısından ideal koşullarda çalıştığı varsayılmıştır. Bu kapsamda başlangıç değerleri ve kontrol parametrelerinin uygun biçimde seçildiği ve sistemin deterministik kaotik davranışını koruduğu kabul edilmiştir (Luo vd., 2019).

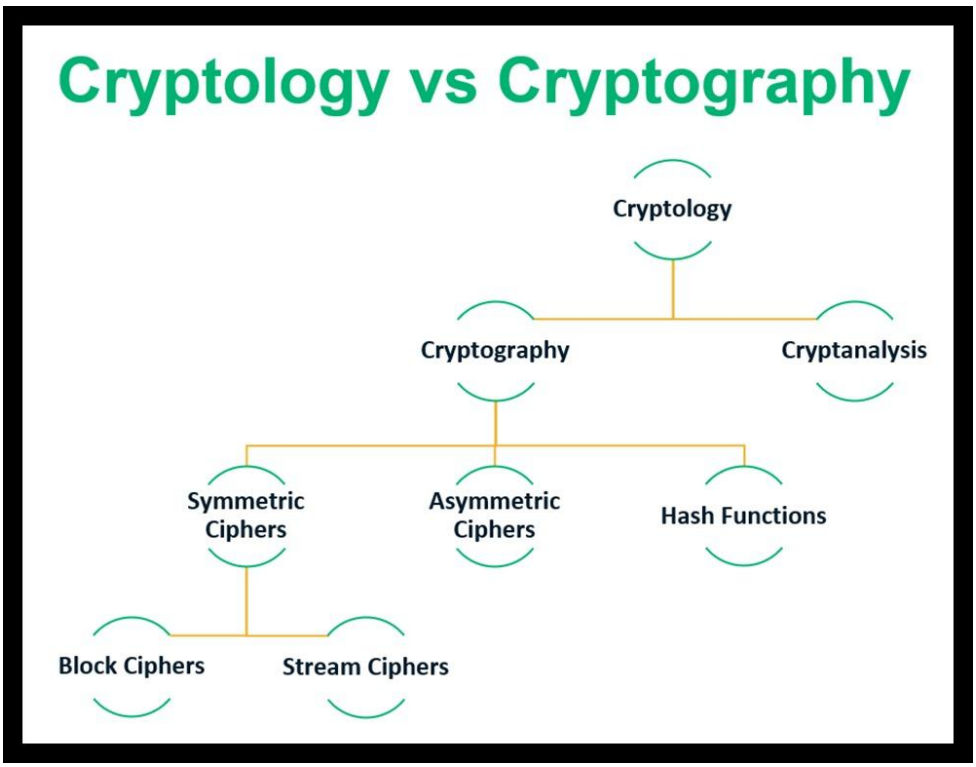
Sonuç olarak, bu varsayımlar çalışmanın sınırlarını belirlemekte ve deneysel bulguların yalnızca tanımlanan koşullar altında geçerli olduğunu ifade etmektedir. Farklı donanım ortamları, veri türleri veya ek güvenlik katmanlarının kullanıldığı senaryolarda elde edilecek sonuçlar, bu araştırmada sunulan bulgulardan farklılık gösterebilir.

2. KAVRAMSAL ÇERÇEVE VE İLGİLİ ÇALIŞMALAR

2.1. Kriptoloji

Kriptoloji, bilgilerin gizliliğini, bütünlüğünü ve doğruluğunu sağlamak amacıyla kullanılan yöntemleri inceleyen bilim dalıdır. Temel olarak, verilerin yetkisiz kişiler tarafından okunmasını engelleyen şifreleme (encryption) ve bu verilerin yetkili kullanıcılar tarafından tekrar anlaşılabilir hâle getirilmesini sağlayan şifre çözme (decryption) süreçlerini kapsamaktadır. Kriptoloji yalnızca verilerin gizliliğini korumakla sınırlı değildir; aynı zamanda iletim sırasında verilerin değiştirilmesini, bozulmasını veya yetkisiz müdahalelere maruz kalmasını önlemeyi de hedeflemektedir. Bu yönüyle kriptoloji, modern bilgi güvenliği sistemlerinin temel yapı taşlarından biri olarak kabul edilmektedir.

Modern kriptoloji çalışmaları; simetrik ve asimetrik şifreleme algoritmaları, hibrit kriptografik yapılar ve kaotik sistemler gibi yenilikçi teknikleri de kapsamaktadır. Özellikle son yıllarda artan veri hacmi ve güvenlik tehditleri, bu yöntemlerin birlikte kullanıldığı daha güçlü ve esnek kriptografik çözümlerin geliştirilmesini gerekli kılmıştır (Christensen, 2010).



Şekil 1. Kriptoloji Bilimi (Sabonchı vd., 2016)

2.1.1 Kriptografi

Kriptografi, verilerin yetkisiz erişimlere karşı korunması amacıyla, anlaşılabilir biçimden (açık metin) anlaşılmaz biçime (şifreli metin) dönüştürülmesini sağlayan bilim dalıdır. Kriptografinin temel amaçları gizlilik, bütünlük, kimlik doğrulama ve inkâr edilemezliktir (Stallings, 2017). Kriptografik yöntemler yalnızca metin tabanlı verilerde değil; ses, video ve görüntü gibi multimedya içeriklerinin korunmasında da etkin biçimde kullanılmaktadır.

Multimedya kriptografisinde temel hedef yalnızca verinin gizliliğini sağlamak değil, aynı zamanda bilginin bütünlüğünü ve orijinalliğini de korumaktır (Kaur ve Kumar, 2020). Son yıllarda yapılan araştırmalar, klasik kriptografik yapıların kaotik sistemler veya makine öğrenmesi tabanlı mekanizmalarla birleştirilmesiyle daha güçlü ve dayanıklı güvenlik yapılarının elde edilebildiğini göstermektedir.

Örneğin, Fang vd. (2023), eliptik eğri kriptografisini (ECC) Hill tabanlı bir sistemle birleştirerek yüksek entropi ve düşük korelasyon değerleri sunan etkili bir görüntü şifreleme mekanizması önermiştir. Benzer biçimde, Alghamdi ve Munir (2024), kriptografik yapılara kaotik sistemlerin entegrasyonunun özellikle renkli görüntüler üzerinde güvenlik düzeyini önemli ölçüde artırdığını ortaya koymuştur.

2.1.2 Kriptoanaliz

Kriptoanaliz, şifrelenmiş verilerden anahtar bilgisi olmaksızın anlamlı sonuçlar elde etmeyi veya kullanılan şifreleme algoritmasının zayıf yönlerini ortaya çıkarmayı amaçlayan bir inceleme alanıdır. Kriptolojinin tamamlayıcı bir parçası olan kriptoanaliz, herhangi bir şifreleme yönteminin gerçek güvenlik düzeyinin değerlendirilmesinde temel bir role sahiptir. Bu nedenle, bir şifreleme algoritmasının yalnızca teorik olarak değil, aynı zamanda pratik saldırı senaryoları altında da test edilmesi gerekmektedir (Paar ve Pelzl, 2009).

Kriptoanaliz; istatistiksel yöntemler, matematiksel çözümleme, frekans analizi, korelasyon incelemeleri, diferansiyel ve lineer saldırılar ile anahtar uzayı araştırmaları gibi çok çeşitli teknikleri kapsamaktadır. Bu yöntemler aracılığıyla, şifreli verilerdeki olası desenler, rastgelelik düzeyi ve algoritmanın belirli giriş değişimlerine verdiği tepkiler ayrıntılı biçimde analiz edilmektedir. Modern kriptografik sistemlerin tasarım sürecinde, söz konusu saldırı

türlerine karşı yüksek direnç gösterebilen yapılar geliştirmek temel hedeflerden biridir (Christensen, 2010).

Günümüzde kriptoanaliz yalnızca teorik çalışmalardan ibaret değildir; görüntü güvenliğinden kablosuz ağlara, Nesnelerin İnterneti (IoT) cihazlarından askeri haberleşme sistemlerine kadar geniş bir uygulama alanında kullanılan şifreleme yöntemlerinin pratik dayanıklılığını ölçmek için de kritik bir gereklilik hâline gelmiştir. Bu bağlamda kriptoanaliz, yeni algoritmalar geliştirilirken hem güvenlik hem de performans dengesi açısından yol gösterici bir değerlendirme aracı olarak kabul edilmektedir.

2.1.3. Simetrik şifreleme algoritmaları

Simetrik şifreleme algoritmalarında, hem şifreleme hem de şifre çözme işlemleri aynı gizli anahtar kullanılarak gerçekleştirilmektedir. Bu yöntemler, hızlı çalışmaları ve düşük hesaplama maliyetleri sayesinde özellikle büyük veri setlerinin şifrelenmesinde önemli avantajlar sunmaktadır. Simetrik şifreleme algoritmaları genel olarak iki ana kategoriye ayrılmaktadır: blok şifreleme ve akış şifreleme yöntemleri (Daemen ve Rijmen, 2002).

Simetrik yapıda geliştirilen başlıca algoritmalar arasında DES, 3DES, AES, RC2, RC4, RC5, RC6, IDEA (International Data Encryption Algorithm), Blowfish, Twofish, Serpent ve Camellia gibi yaygın olarak kullanılan yöntemler yer almaktadır. Bu algoritmalar; anahtar uzunluğu, blok boyutu, işlem hızı ve saldırılara karşı dayanıklılık gibi teknik özellikler bakımından farklılık göstermekte olup, kullanım alanları uygulama gereksinimlerine göre değişmektedir.

RC4, 1987 yılında Ron Rivest tarafından geliştirilen bir akış şifreleme algoritmasıdır. Basit yapısı ve yüksek işlem hızı sayesinde uzun yıllar boyunca SSL/TLS gibi kritik güvenlik protokollerinde yaygın biçimde tercih edilmiştir. Ancak daha sonraki araştırmalar, RC4 algoritmasının anahtar başlangıç aşamasında belirli istatistiksel önyargılar içerdiğini ve bu durumun saldırganlar için önemli bir güvenlik zafiyeti oluşturabileceğini ortaya koymuştur (Mousa ve Hamad, 2006). Bu nedenle RC4, modern güvenlik uygulamalarında tek başına kullanımı önerilmeyen algoritmalar arasında yer almaktadır.

AES (Advanced Encryption Standard), 2001 yılında ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından DES algoritmasının yerine geçmek üzere modern bir şifreleme standardı olarak kabul edilmiştir. Rijndael mimarisine dayanan AES, sabit boyutlu bloklar üzerinde güçlü karıştırma, permütasyon ve difüzyon işlemleri uygulayarak yüksek güvenlik seviyesi sağlamaktadır. Ayrıca donanım ve yazılım ortamlarında kolay uygulanabilirliği, düşük hata yayılımı ve güçlü kriptografik yapısı sayesinde günümüzde en yaygın kullanılan simetrik şifreleme algoritmalarından biri hâline gelmiştir (Daemen ve Rijmen, 2002).

2.1.4. Asimetrik şifreleme algoritmaları

Asimetrik şifreleme sistemleri, birbirinden farklı iki anahtarın kullanıldığı bir yapıya sahiptir: veriyi şifrelemek için kullanılan açık anahtar ve yalnızca yetkili kullanıcıda bulunan gizli anahtar. Bu iki anahtar matematiksel olarak birbiriyle ilişkili olsa da, gizli anahtarın açık anahtardan elde edilmesi hesaplama açısından pratikte mümkün değildir. Bu özellik, asimetrik şifreleme yöntemlerini özellikle güvenli anahtar değişimi, kimlik doğrulama ve dijital imza gibi kritik süreçlerde vazgeçilmez hâle getirmektedir (Shah ve Gor, 2025).

Günümüzde kullanılan temel asimetrik şifreleme yöntemleri arasında RSA, ElGamal, ECC (Elliptic Curve Cryptography), DSA (Digital Signature Algorithm) ve güvenli anahtar paylaşımında önemli bir rol oynayan Diffie–Hellman protokolü yer almaktadır. Bu algoritmaların ortak amacı, güvenlik gereksinimlerini yüksek matematiksel karmaşıklığa sahip problemler üzerinden sağlamaktır.

Bu yöntemler içerisinde en yaygın kullanılan algoritma RSA'dır. Rivest, Shamir ve Adleman tarafından 1978 yılında geliştirilen RSA algoritması, güvenliğini büyük asal sayıların çarpanlara ayrılmasının zorluğuna dayandırmaktadır (Rivest vd., 1978). RSA algoritması yüksek güvenlik seviyesi sunmasına rağmen, hesaplama maliyeti simetrik algoritmalara kıyasla oldukça fazladır. Bu nedenle büyük boyutlu veri setlerinin doğrudan RSA ile şifrelenmesi verimli değildir. Bunun yerine RSA, çoğunlukla hibrit şifreleme sistemlerinde simetrik algoritmalarla birlikte kullanılarak, yalnızca simetrik anahtarın güvenli biçimde iletilmesi amacıyla tercih edilmektedir.

Literatürde hibrit şifreleme yaklaşımlarının hem güvenlik hem de performans açısından önemli avantajlar sunduğu çeşitli çalışmalarla ortaya konmuştur. Örneğin Hakim ve Budiman (2024),

RSA ve RC4 algoritmalarını bir araya getirerek hızlı anahtar üretimi ve güvenli veri iletimi sağlayan bir hibrit model önermiştir. Benzer şekilde Khalaf ve Lakhtaria (2023), RSA ve AES tabanlı hibrit mimarilerin özellikle büyük boyutlu veri şifreleme uygulamalarında etkili performans sunduğunu göstermiştir. Bu çalışmalar, RSA'nın doğrudan veri şifreleme yerine güvenli anahtar yönetimi ve dağıtımı açısından kritik bir rol üstlendiğini açıkça ortaya koymaktadır.

Son dönem araştırmalarda ise RSA algoritmasının temel zayıf yönlerinden biri olarak kabul edilen yüksek hesaplama maliyetini azaltmaya yönelik çeşitli iyileştirmeler önerilmiştir. Modüler üs alma işlemlerinde optimizasyon sağlayan yöntemler, paralel işlem desteğiyle hızlandırılmış RSA uygulamaları ve büyük asal sayı üretiminde daha verimli algoritmalar bu iyileştirmelere örnek olarak verilebilir (Liu vd., 2022). Bu gelişmeler, asimetrik şifreleme yöntemlerinin modern güvenlik gereksinimlerine daha uygun hâle getirilmesini hedeflemektedir.

2.2. Kaotik Sistemler

Kaotik sistemler, başlangıç koşullarına karşı yüksek duyarlılık, doğrusal olmayan davranış ve pseudo-rastgelelik özellikleri ile karakterize edilmektedir. Bu özellikler, kaotik sistemleri kriptografi ve özellikle dijital görüntü şifreleme alanında güçlü bir araç hâline getirmektedir. Kaotik haritalar deterministik yapıda olmalarına rağmen tahmin edilemez davranışlar sergileyebilmekte ve yüksek düzeyde rastgelelik üretebilmektedir. Bu sayede şifreleme algoritmalarında güvenli anahtar dizilerinin oluşturulması, piksel karıştırma (permutation) ve veri yayma (diffusion) işlemlerinde etkin biçimde kullanılmaktadır (Pareek vd., 2006).

Günümüzde yaygın olarak kullanılan kaotik fonksiyonlar arasında Logistic Map, Tent Map, Henon Map, Lorenz Map, Sine Map ve Baker Map yer almaktadır. Bu haritalar, klasik rastgele sayı üreteçlerine kıyasla daha geniş bir anahtar uzayı ve dinamik bir yapı sunmaktadır. Böylece şifreleme süreçlerinde hem yüksek güvenlik seviyesi hem de saldırılara karşı daha güçlü bir direnç sağlanmaktadır. Örneğin Al-Maadeed vd. (2012), kaotik haritaların şifreleme algoritmalarına entegre edilmesinin histogram düzgünlüğünü artırdığını ve şifreli görüntülerdeki piksel dağılımını daha homojen hâle getirdiğini göstermiştir. Benzer şekilde Benaissi vd. (2023), Logistic ve Tent haritalarını birleştiren hibrit bir yapı kullanarak entropi değerlerini 7.998 seviyesine yükseltmiş ve şifreleme rastgeleliğinin önemli ölçüde arttığını

rapor etmiştir.

Kaotik sistemlerin şifreleme alanındaki kullanımı yalnızca temel kaotik haritalarla sınırlı değildir. Son yıllarda geliştirilen hibrit kaotik yöntemler, birden fazla kaotik haritanın bir araya getirilmesiyle daha karmaşık ve saldırılara karşı daha dayanıklı yapılar oluşturmayı amaçlamaktadır. Bu tür hibrit modeller, tek haritalı yapılarda görülebilen doğrusal zayıflıkları azaltarak daha güvenli anahtar dizileri ve daha etkili piksel karıştırma mekanizmaları sunmaktadır. Bu kapsamda Umar vd. (2024) tarafından önerilen Modified Skew Tent Map (M-STM) modeli, klasik skew tent haritasında görülen kararsızlıkları gidererek daha geniş bir kaotik aralık, daha kararlı dinamik davranış ve kriptografik uygulamalar için daha güvenilir pseudo-rastgele çıktılar üretmiştir.

Kaotik yöntemler yalnızca rastgele anahtar üretimi ile sınırlı kalmayıp, aynı zamanda piksel karıştırma (pixel shuffling), bit düzeyi permütasyon ve modül tabanlı yayma (diffusion) gibi işlemlerde de etkin biçimde kullanılmaktadır. Bu yaklaşımlar, şifreli görüntülerin istatistiksel özelliklerini iyileştirerek komşu pikseller arasındaki korelasyonu önemli ölçüde azaltmakta ve diferansiyel saldırılara karşı yüksek direnç sağlamaktadır. Ayrıca kaotik haritalar, düşük hesaplama maliyetleriyle yüksek güvenlik sunmaları nedeniyle gömülü sistemler ve gerçek zamanlı uygulamalar için de avantajlı bir çözüm olarak öne çıkmaktadır.

Genel olarak kaotik sistemlerin kriptografide kullanımı, klasik simetrik veya asimetrik algoritmalarla hibrit yapıların oluşturulmasına olanak tanımaktadır. Bu sayede hem hız hem de güvenlik açısından dengeli ve etkin şifreleme sistemleri geliştirilebilmektedir. Literatürdeki çalışmalar, kaotik sistemlerin modern şifreleme yöntemlerinde stratejik bir rol üstlendiğini ve özellikle dijital görüntü güvenliği uygulamalarında giderek daha merkezi bir yaklaşım hâline geldiğini ortaya koymaktadır (Pareek vd., 2006; Umar vd., 2024).

2.3. Hibrit Şifreleme Yöntemleri

Hibrit şifreleme yöntemleri, simetrik ve asimetrik şifreleme tekniklerinin güçlü yönlerini bir araya getirerek dengeli ve etkin güvenlik çözümleri sunmayı amaçlamaktadır. Simetrik algoritmalar yüksek işlem hızı ve düşük hesaplama maliyeti sağlarken; asimetrik algoritmalar güvenli anahtar dağıtımı, kimlik doğrulama ve güvenli anahtar paylaşımı gibi önemli avantajlar sunmaktadır. Bu nedenle hibrit şifreleme sistemleri, AES–RSA ve ECC–AES gibi

kombinasyonlarla hem performans hem de güvenlik gereksinimlerini karşılayacak biçimde yaygın olarak tercih edilmektedir (Subedar & Araballi, 2020; Alkady & Habib, 2013).

Hibrit şifrelemenin temel çalışma prensibi, büyük veri bloklarının veya multimedya içeriklerinin simetrik algoritmalar kullanılarak hızlı bir şekilde şifrelenmesi ve kullanılan simetrik anahtarların asimetrik algoritmalar aracılığıyla güvenli biçimde iletilmesine dayanmaktadır. Bu yaklaşım, özellikle veri iletimi ve depolama süreçlerinde etkin bir güvenlik sağlamaktadır. Örneğin RC4 veya AES gibi simetrik algoritmalar, verileri yüksek hızda şifrelerken; RSA veya ECC gibi asimetrik algoritmalar, bu simetrik anahtarların güvenli bir şekilde paylaşılmasını mümkün kılmaktadır (Alkady vd., 2013).

Hibrit şifreleme yöntemleri yalnızca işlem hızını artırmakla kalmayıp, aynı zamanda istatistiksel ve diferansiyel saldırılara karşı daha güçlü bir direnç sunmaktadır. Son yıllarda yapılan çalışmalar, hibrit modellerin özellikle dijital görüntü şifreleme uygulamalarında yüksek güvenlik seviyesi ile birlikte düşük işlem süresi sağladığını ortaya koymaktadır. Örneğin AES ve RSA'nın birlikte kullanıldığı hibrit sistemler, simetrik algoritmaların hız avantajını asimetrik algoritmaların güvenli anahtar yönetimi yetenekleriyle birleştirmektedir (Alkady & Habib, 2013). Benzer şekilde Arab vd. (2019), kaotik sistemlerle desteklenmiş hibrit AES yapılarının büyük veri ve multimedya içeriklerinde yüksek güvenlik ve pratik uygulanabilirlik sunduğunu göstermiştir.

Hibrit şifreleme yaklaşımları günümüzde görüntü güvenliği, kablosuz iletişim sistemleri, IoT tabanlı uygulamalar ve bulut tabanlı veri depolama platformları gibi birçok alanda yaygın olarak kullanılmaktadır. Bu yöntemler yalnızca veri gizliliğini korumakla kalmayıp, aynı zamanda verinin bütünlüğünün ve orijinalliğinin güvence altına alınmasına da katkı sağlamaktadır. Hibrit şifreleme tekniklerinin esnek ve modüler yapısı, farklı algoritmaların farklı veri türleri ve uygulama senaryolarına kolayca uyarlanabilmesini mümkün kılmaktadır.

2.4. Görüntü Şifreleme

Görüntü şifreleme, dijital görüntülerin yetkisiz erişimlere karşı korunmasını amaçlayan özel bir kriptografik uygulama alanıdır. Metin tabanlı verilerle karşılaştırıldığında, görüntülerin yüksek piksel yoğunluğuna sahip olması ve komşu pikseller arasında güçlü bir korelasyon bulunması, bu alanda özel şifreleme tekniklerinin kullanılmasını zorunlu kılmaktadır (Chen vd., 2004).

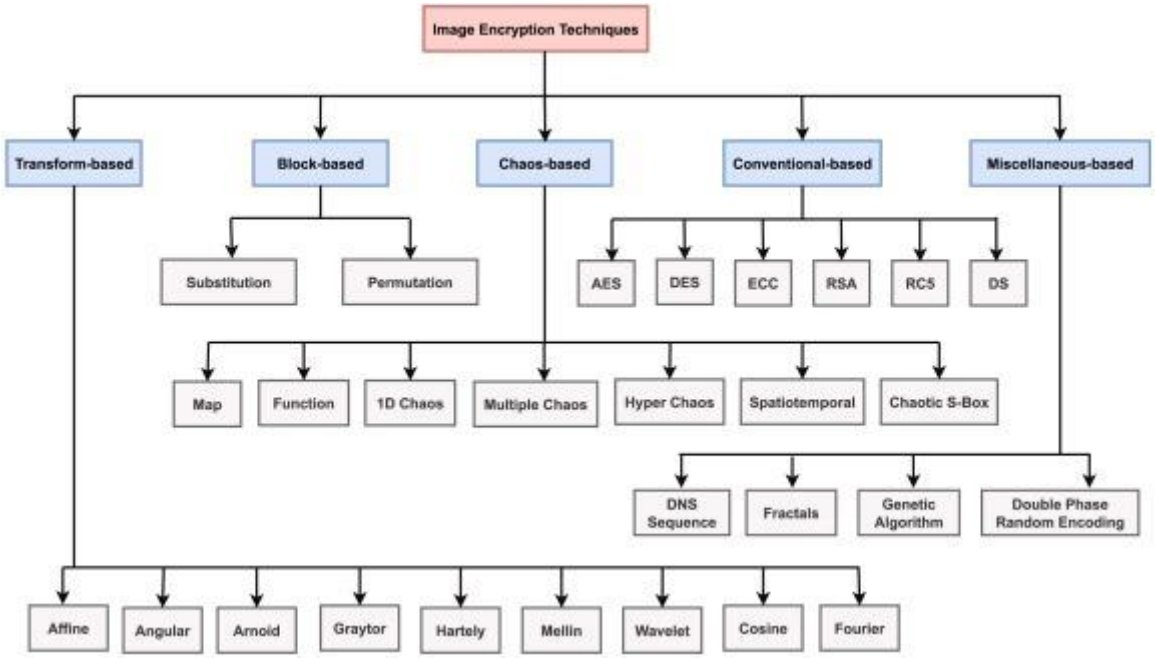
Özellikle renkli görüntülerde üç kanallı (RGB) yapı ve yüksek veri tekrar oranı, klasik metin tabanlı şifreleme yöntemlerinin görüntü verileri üzerinde yeterli performans göstermemesine yol açmaktadır.

Görüntü şifreleme yöntemleri genellikle iki temel aşamaya dayanmaktadır: karıştırma (confusion) ve yayma (diffusion). Karıştırma aşamasında, piksellerin konumları ve/veya değerleri değiştirilerek şifreli görüntüdeki yapısal desenler gizlenir. Yayma aşamasında ise, görüntüde yapılan küçük bir değişikliğin tüm görüntüye yayılması sağlanarak güvenlik seviyesi artırılır. Bu iki temel ilke sayesinde, şifreli görüntü rastgele bir görünüm kazanmakta ve orijinal görüntüye dair herhangi bir anlamlı bilgi taşımamaktadır.

Görüntü şifreleme algoritmalarının güvenlik ve performans düzeyi çeşitli ölçütler aracılığıyla değerlendirilmektedir. Bu ölçütler aşağıda özetlenmiştir:

- Histogram analizi: Piksel dağılımının üniform olup olmadığı incelenir.
- Korelasyon katsayısı: Şifreli görüntüde komşu pikseller arasındaki ilişkinin sıfıra yakın olması beklenir.
- Entropi: Görüntüdeki rastgelelik derecesi; ideal olarak 8 bit görüntülerde 8'e yakın olmalıdır.
- NPCR ve UACI: Küçük değişikliklerin şifreli görüntüye etkisini ölçer; yüksek değerler iyi yayılımı gösterir.
- PSNR ve MSE: Şifreli görüntünün çözülmesinin ardından orijinal görüntüye yakınlığını değerlendirir.

Son yıllarda yapılan çalışmalar, klasik uzamsal alan tabanlı yöntemlerin yanı sıra hibrit-domain tabanlı görüntü şifreleme algoritmalarının hem güvenlik hem de kalite açısından daha başarılı sonuçlar sunduğunu ortaya koymuştur (Wang & Zhang, 2018). Bu yaklaşımlar, uzamsal alan ve dönüşüm alanı işlemlerini birleştirerek saldırılara karşı daha dayanıklı yapılar geliştirmeyi hedeflemektedir. Ayrıca artan güvenlik gereksinimleri doğrultusunda, tıbbi görüntüler, biyometrik veriler ve kritik altyapılarda kullanılan görüntülerin korunması için gelişmiş ve hibrit şifreleme tekniklerinin önemi giderek artmaktadır (Ghorbani & Yadollahi, 2024).
Görüntü şifreleme süreçlerinin genel işleyişi ve temel aşamaları Şekil 2'de şematik olarak gösterilmiştir.



Şekil 2. Şifreleme Teknikleri (Yogi vd., 2025)

2.4.1. Görüntü şifrelemenin uygulama perspektifleri

Görüntü şifreleme, dijital çağda bilgi güvenliğinin kritik bir bileşeni hâline gelmiştir. Dijital verilerin giderek artan hacmi, yüksek çözünürlüklü multimedya içerikleri ve internet tabanlı paylaşım mekanizmaları, güvenli veri iletimini zorunlu kılmaktadır. Bu bağlamda görüntü şifreleme yalnızca kişisel fotoğrafların gizliliğini sağlamakla kalmaz; sağlık, askeri sistemler, uydu görüntüleri, bulut depolama, biyometrik kimlik doğrulama ve eğitim gibi kritik alanlarda veri bütünlüğünün korunması ve yetkisiz erişimlerin önlenmesi açısından stratejik bir rol üstlenir. Şifreleme süreçlerinin hem veri bütünlüğünü koruması hem de hızlı ve pratik biçimde uygulanabilir olması gerekmektedir (SaberiKamarposhti vd., 2024).

2.4.2. Askeri ve uydu görüntülerinde şifreleme

Askeri ve uydu görüntüleri, ulusal güvenlik ve stratejik istihbarat açısından son derece kritik bilgiler içermektedir. Bu tür verilerde yüksek güvenlik seviyesine sahip şifreleme algoritmalarının kullanılması zorunludur. Uydu görüntüleri genellikle yüksek çözünürlüklü, büyük boyutlu ve dinamik yapıda olduğundan, işlem süresi ve performans da güvenlik kadar önem taşımaktadır. Bu nedenle yüksek performanslı simetrik algoritmalar (AES, RC4) ile kaotik sistem tabanlı hibrit yaklaşımlar sıklıkla tercih edilmektedir (Rashid vd., 2024).

Örneğin Zhao vd. (2024), uydu görüntülerinin korunması amacıyla yedi boyutlu karmaşık kaotik sistem ve RNA kodlamaya dayalı bir şifreleme algoritması önermiş ve önerilen yapının hem güçlü istatistiksel güvenlik sağladığını hem de yüksek çözünürlüklü uydu görüntülerinde pratik olarak uygulanabilir olduğunu göstermiştir (Zhai vd., 2024).

2.4.3. Bulut sistemlerinde görüntü güvenliği

Bulut tabanlı depolama sistemlerinde kullanıcı verilerinin üçüncü taraf hizmet sağlayıcılar tarafından yönetilmesi, gizlilik ve güvenlik endişelerini artırmaktadır. Bu nedenle bulut ortamına yüklenen görüntülerin önceden şifrelenmesi temel bir güvenlik gerekliliği hâline gelmiştir. Elhoseny ve Shankar (2020), görüntü verilerinin bulut ortamına aktarılmadan önce hibrit şifreleme modelleriyle korunmasının, yetkisiz erişimlerin önlenmesi ve veri gizliliğinin sağlanması açısından kritik bir rol oynadığını ortaya koymuştur.

2.4.4. Sağlık ve tıbbi görüntülerde şifreleme

Tıbbi görüntüler (MR, BT, ultrason, röntgen vb.), hastalara ait son derece hassas bilgiler içermekte olup gizlilik açısından özel koruma gerektirmektedir. Bu tür verilerin yetkisiz erişimlere karşı korunması, hasta mahremiyeti ve yasal düzenlemeler açısından büyük önem taşımaktadır. Literatürde, tıbbi görüntülerin kaotik ve hibrit şifreleme yöntemleriyle korunmasının hem veri gizliliğini artırdığı hem de tanısal görüntü kalitesini koruduğu rapor edilmiştir. Bu nedenle sağlık alanında kullanılan görüntü şifreleme sistemlerinin hem yüksek güvenlik hem de düşük bilgi kaybı sağlayacak biçimde tasarlanması gerekmektedir.

2.4.5. Biyometrik verilerin şifrelenmesi

Biyometrik veriler, kişisel kimlik doğrulamada kritik öneme sahip olup gizlilik açısından son derece hassastır. Parmak izi, yüz, iris veya retina verilerinin ele geçirilmesi, kimlik hırsızlığı ve veri suiistimali riskini ciddi biçimde artırmaktadır. Bu nedenle biyometrik sistemlerin yalnızca tanıma doğruluğu açısından değil, aynı zamanda şablon güvenliği ve veri gizliliği açısından da güçlü kriptografik mekanizmalarla desteklenmesi gerekmektedir (Jain vd., 2008).

Literatürde biyometrik şablon koruma kapsamında; iptal edilebilir biyometri, biyokryptosistemler ve şifreleme tabanlı yaklaşımlar gibi çeşitli yöntemler önerilmiştir. Son

dönemde, özellikle homomorfik şifreleme gibi gelişmiş kriptografik tekniklerin biyometrik sistemlere entegre edilmesiyle, verilerin şifreli hâlde depolanıp işlenmesi hedeflenmektedir (Yang vd., 2023).

2.4.6. Eğitim ve e-öğrenmede görüntü güvenliği

E-öğrenme platformlarında öğrenci kimlik bilgileri, sınav görüntüleri ve dijital eğitim materyalleri yoğun biçimde paylaşılmaktadır. Bu durum, veri gizliliğinin sağlanması için etkili şifreleme yöntemlerini zorunlu kılmaktadır. Rafee ve Nema (2022), sıfır bilgi ispatı (ZKP) ve AES tabanlı güvenli bir e-öğrenme sistemi tasarlayarak, kullanıcı verilerinin yetkisiz erişimlere karşı korunabildiğini göstermiştir.

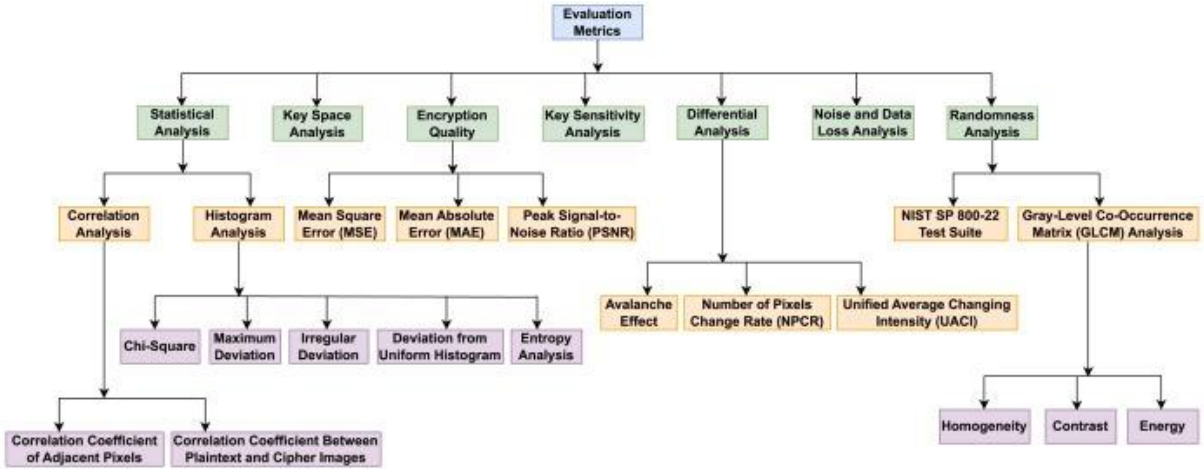
Benzer şekilde Shadmanova vd. (2024), internet tabanlı bir e-öğrenme sistemi için AES ve RSA algoritmalarını bütünleştiren entegre bir şifreleme yaklaşımı önermiş ve ders içerikleri ile sınav verilerinin bulut altyapısı üzerinde güvenli biçimde saklanmasını sağlamıştır. Bu çalışmalar, eğitim teknolojilerinde hibrit şifreleme yaklaşımlarının hem gizlilik hem de erişim kontrolü açısından etkili çözümler sunduğunu ortaya koymaktadır.

2.5. Görüntü şifreleme güvenlik ve performans ölçütleri

Görüntü şifreleme algoritmalarının etkinliği yalnızca algoritmanın teorik yapısıyla sınırlı değildir; aynı zamanda şifrelenmiş görüntünün güvenlik düzeyini ve şifre çözme işlemi sonrasında elde edilen görüntünün kalitesini değerlendiren çeşitli ölçütler aracılığıyla nicel olarak analiz edilir. Bu ölçütler, şifreleme işleminin rastgelelik, yayılım (diffusion) ve güvenlik özelliklerini ortaya koyarak algoritmanın pratik uygulamalardaki dayanıklılığını objektif biçimde değerlendirmeye olanak tanır.

Literatürde histogram analizi, korelasyon katsayısı, entropi, NPCR, UACI, PSNR, MSE ve SSIM gibi metrikler; görüntü şifreleme algoritmalarının güvenlik ve performans analizlerinde yaygın olarak kullanılan standart değerlendirme ölçütleri olarak kabul edilmektedir (Alghamdi & Munir, 2024). Bu ölçütler sayesinde şifreleme algoritmalarının istatistiksel saldırılara, diferansiyel saldırılara ve görsel analizlere karşı gösterdiği direnç ayrıntılı biçimde incelenebilmektedir.

Bu çalışmada kullanılan temel güvenlik ve performans ölçütleri, Şekil 3'te genel bir çerçeve içerisinde sunulmuştur. Aşağıda, görüntü şifreleme algoritmalarının güvenlik ve performansını değerlendirmede yaygın olarak kullanılan başlıca ölçütler ayrıntılı biçimde açıklanmaktadır.



Şekil 3. Şifrelemede Performans Metrikleri (Yogi vd., 2025)

2.5.1. Histogram analizi

Histogram analizi, bir görüntüdeki piksel değerlerinin dağılımını görselleştirerek şifreleme algoritmasının istatistiksel saldırılara karşı direncini değerlendiren temel yöntemlerden biridir. Orijinal görüntüler genellikle belirli renk ve yoğunluk değerlerinde kümelenmeler içerir ve histogramlarında belirgin piklere sahip dağılımlar gözlemlenir. Bu durum, görüntüdeki yapısal ve istatistiksel bilgilerin açığa çıkmasına neden olabilir.

Etkili bir şifreleme algoritmasında ise, şifreleme sonrasında piksel değerlerinin histogram dağılımının mümkün olduğunca uniform (düzgün) bir yapıya sahip olması beklenir. Uniform histogram yapısı, görüntüdeki öngörülebilir desenlerin ve istatistiksel bağıntıların ortadan kaldırıldığını, dolayısıyla şifreli görüntüden orijinal içeriğe ilişkin herhangi bir anlamlı çıkarım yapılmasının zorlaştığını göstermektedir.

Bu özellik, özellikle tıbbi, askeri ve biyometrik görüntülerin korunmasında kritik bir öneme sahiptir. Çünkü histogram temelli istatistiksel analizler, saldırganlar tarafından orijinal görüntüye dair bilgi elde etmek amacıyla sıklıkla kullanılan yöntemler arasındadır (Alghamdi & Munir, 2024).

Sonuç olarak histogram analizi, görüntü şifreleme algoritmalarının temel güvenlik düzeyini hızlı, sezgisel ve görsel olarak değerlendirmeye imkân tanıyan etkili bir performans ölçütü olarak kabul edilmektedir.

2.5.2. Korelasyon katsayısı

Korelasyon katsayısı, bir görüntüde yatay, dikey ve çapraz yöndeki komşu pikseller arasındaki doğrusal ilişkiyi nicel olarak ölçen istatistiksel bir ölçüttür. Bu çalışmada kullanılan korelasyon katsayısı, ilk kez Karl Pearson tarafından tanımlanan ve literatürde Pearson korelasyon katsayısı olarak bilinen istatistiksel ölçüt temel alınarak hesaplanmıştır (Pearson, 1895).

Orijinal görüntülerde komşu pikseller genellikle benzer renk ve yoğunluk değerlerine sahip olduğundan, korelasyon katsayısı yüksek değerlere (1'e yakın) sahiptir. Buna karşılık, başarılı bir görüntü şifreleme algoritması sonrasında komşu pikseller arasındaki ilişkinin zayıflaması ve korelasyon katsayısının sıfıra yakın değerlere düşmesi beklenir. Bu durum, görüntüdeki örüntülerin ve istatistiksel bağımlılıkların etkili biçimde gizlendiğini göstermektedir. Korelasyon katsayısı aşağıdaki matematiksel ifade ile hesaplanmaktadır (Pearson, 1895):

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.1}$$

Burada kovaryans ve varyans terimleri şu şekilde tanımlanmaktadır:

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{2.2}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{2.3}$$

Bu ifadelerde $x_i$ve y_i, komşu iki pikselin yoğunluk değerlerini; $E(x)$ve $E(y)$ortalama değerleri; Nise seçilen piksel çiftlerinin sayısını temsil etmektedir. Görüntü şifreleme literatüründe, yatay, dikey ve çapraz yönlerde hesaplanan korelasyon katsayılarının sıfıra yakın olması, algoritmanın istatistiksel saldırılara karşı güçlü bir direnç sergilediğini göstermektedir (Zhang vd., 2024).

2.5.3. Entropi

Entropi, bir bilgi kaynağındaki belirsizlik ve rastgelelik düzeyini ölçen temel bir ölçüttür. Görüntü şifreleme alanında entropi, şifreli görüntüdeki piksel değerlerinin ne derece rastgele dağıldığını nicel olarak değerlendirmek amacıyla kullanılmaktadır. Bu çalışmada kullanılan entropi ölçütü, bilgi kuramının temellerini atan Claude E. Shannon tarafından tanımlanan bilgi entropisi kavramına dayanmaktadır (Shannon, 1948).

Bir dijital görüntü için entropi değeri aşağıdaki matematiksel ifade ile hesaplanmaktadır (Shannon, 1948):

$$H = -\sum_{i=0}^{L-1} p(i) \log_2 p(i) \tag{2.4}$$

Burada;

- **H**, görüntünün entropi değerini,
- **p(i)**, görüntüdeki *i* piksel değerinin gerçekleşme olasılığını,
- **L**, olası piksel değerlerinin sayısını ifade etmektedir.

8-bit bir görüntü için $L = 256$ olup, entropi değerinin teorik olarak 8'e yakın olması, piksel değerlerinin uniform ve yüksek derecede rastgele bir dağılıma sahip olduğunu göstermektedir. Bu durum, şifreli görüntü üzerinden istatistiksel bilgi elde edilmesini zorlaştırarak, şifreleme algoritmasının güvenlik seviyesinin yüksek olduğunu ifade eder.

Literatürde entropi analizi, özellikle tıbbi, askeri ve biyometrik görüntülerin şifrelenmesinde, algoritmanın güvenliğini nicel olarak değerlendirmek amacıyla yaygın biçimde kullanılmaktadır (Alghamdi & Munir, 2024). Yüksek entropi değerleri, istatistiksel saldırılar ve kaba kuvvet saldırıları gibi yaygın saldırı yöntemlerine karşı daha etkin bir koruma sağlandığını göstermektedir. Bu nedenle entropi, görüntü şifreleme algoritmalarının güvenlik performansını değerlendirmede temel ölçütlerden biri olarak kabul edilmektedir.

2.5.4. Npcr ve uacı

NPCR (Number of Pixels Change Rate) ve UACI (Unified Average Changing Intensity), görüntü şifreleme algoritmalarının diferansiyel saldırılara karşı dayanıklılığını değerlendirmek amacıyla yaygın olarak kullanılan iki temel istatistiksel ölçüttür. Bu ölçütler, orijinal görüntüde yapılan çok küçük bir değişikliğin (örneğin tek bir pikselin veya bir bitin değiştirilmesi) şifreli görüntü üzerinde ne ölçüde yaygın ve etkili bir değişime yol açtığını nicel olarak analiz etmektedir.

NPCR, iki şifreli görüntü arasındaki piksel değişim oranını ölçerek, algoritmanın yayılım (diffusion) özelliğini değerlendirmektedir. Yüksek NPCR değeri, şifreleme algoritmasının girişteki küçük değişikliklere karşı yüksek hassasiyet gösterdiğini ve diferansiyel saldırılara karşı güçlü bir direnç sağladığını ifade eder.

NPCR değeri aşağıdaki matematiksel ifade ile hesaplanmaktadır (Biham & Shamir, 1997):

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100 \tag{2.5}$$

$$D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & \text{aksi halde} \end{cases} \tag{2.6}$$

Burada;

- C_1ve C_2, yalnızca bir piksel veya bir bit farkı bulunan iki şifreli görüntüyü,
- $M \times N$, görüntünün boyutunu ifade etmektedir.

UACI (Unified Average Changing Intensity), iki şifreli görüntü arasındaki piksel yoğunluğu değişimlerinin ortalama şiddetini ölçmektedir. Yüksek UACI değeri, tek bir pikselde yapılan değişikliğin tüm görüntü geneline güçlü bir biçimde yayıldığını ve şifreleme algoritmasının etkinliğini göstermektedir.

UACI değeri aşağıdaki formül ile hesaplanmaktadır (Wu, Noonan & Agaian, 2011). Burada 255 değeri, 8-bit görüntüler için maksimum piksel yoğunluğunu temsil etmektedir.

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{| C_1(i,j) - C_2(i,j) |}{255} \times 100 \quad (2.7)$$

NPCR ve UACI ölçütleri birlikte değerlendirildiğinde, bir görüntü şifreleme algoritmasının diferansiyel saldırılara karşı dayanıklılığı hakkında kapsamlı bilgi sunmaktadır. Literatürde bu ölçütlerin, özellikle tıbbi, askeri ve biyometrik görüntülerin güvenlik performansını analiz etmek için standart değerlendirme kriterleri olarak kullanıldığı belirtilmektedir (Alghamdi & Munir, 2024). Yüksek NPCR ve UACI değerleri, algoritmanın küçük giriş değişikliklerine karşı güçlü bir difüzyon etkisi sergilediğini ve görüntü verilerinin güvenli biçimde korunduğunu göstermektedir.

2.5.5. Psnr ve mse

MSE (Mean Squared Error) ve PSNR (Peak Signal-to-Noise Ratio), görüntü şifreleme algoritmalarında **geri çözme (deşifre) doğruluğunu ve görüntü kalitesini** nicel olarak değerlendirmek amacıyla yaygın şekilde kullanılan iki temel ölçüttür. Bu ölçütler, özellikle şifre çözme işlemi sonrasında elde edilen görüntünün orijinal görüntüye ne ölçüde yakın olduğunu analiz etmeye olanak tanımaktadır.

MSE (Mean Squared Error), orijinal görüntü ile şifre çözülmüş görüntü arasındaki piksel farklarının karesinin ortalamasını ifade etmektedir. MSE değeri aşağıdaki matematiksel ifade ile hesaplanmaktadır (Gonzalez & Woods, 2002):

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I'(i,j)]^2 \quad (2.8)$$

Burada;

- $I(i,j)$: orijinal görüntünün i,jpiksel değerini,
- $I'(i,j)$: şifre çözülmüş görüntünün i,jpiksel değerini,
- $M \times N$: görüntü boyutunu temsil etmektedir.

Düşük MSE değeri, şifre çözme işlemi sonrasında elde edilen görüntünün orijinal görüntüye yüksek derecede benzer olduğunu ve görüntü kalitesinin başarılı biçimde korunduğunu göstermektedir.

PSNR (Peak Signal-to-Noise Ratio), MSE değerine bağlı olarak hesaplanan ve iki görüntü arasındaki farkı desibel (dB) cinsinden ifade eden bir kalite ölçütüdür. PSNR değeri aşağıdaki formül ile hesaplanmaktadır (Huynh-Thu & Ghanbari, 2008):

$$\text{PSNR} = 10\log_{10}\left(\frac{MAX^2}{\text{MSE}}\right) \tag{2.9}$$

Bu ifadede **MAX**, görüntüdeki maksimum piksel değerini temsil etmekte olup, 8-bit görüntüler için bu değer 255'tir. PSNR değerinin yüksek olması, orijinal görüntü ile şifre çözülmüş görüntü arasındaki farkın düşük olduğunu ve şifreleme–çözme sürecinde görüntü kalitesinin başarılı bir şekilde korunduğunu göstermektedir.

Görüntü şifreleme literatüründe, PSNR ve MSE ölçütleri iki farklı amaçla değerlendirilmektedir. Şifreli görüntü ile orijinal görüntü arasındaki karşılaştırmalarda düşük PSNR ve yüksek MSE değerleri, şifrelemenin güçlü olduğunu ve görsel bilginin etkin biçimde gizlendiğini göstermektedir. Buna karşılık, şifre çözülmüş görüntü ile orijinal görüntü arasındaki karşılaştırmalarda yüksek PSNR ve düşük MSE değerleri, geri çözme işleminin doğru ve kayıpsız biçimde gerçekleştirildiğini ifade etmektedir.

Bu nedenle PSNR ve MSE ölçütleri, yalnızca şifreleme algoritmasının güvenliğini değil, aynı zamanda geri çözme doğruluğunu, görüntü kalitesini ve uygulama verimliliğini değerlendirmek açısından da büyük önem taşımaktadır. Özellikle tıbbi görüntülerin şifrelenmesinde, yüksek PSNR ve düşük MSE değerleri, tanısal bilgilerin kaybolmaması ve klinik doğruluğun korunması açısından kritik öneme sahiptir (Zhang vd., 2024). Ayrıca bu ölçütlerin optimize edilmesi, görüntü şifreleme algoritmalarının gerçek zamanlı ve pratik uygulamalarda kullanılabilirliğini artırmaktadır.

2.6. Ölçütlerin Önemi ve Literatürdeki Kullanımı

Görüntü şifreleme algoritmalarının etkinliği, tek bir ölçüte dayanarak değerlendirilemez; farklı kriterlerin birlikte incelenmesi gerekmektedir. Literatürde histogram, korelasyon katsayısı, entropi, NPCR, UACI, PSNR ve MSE gibi ölçütler, şifreleme algoritmalarının güvenliğini ve performansını bütüncül bir biçimde analiz etmek amacıyla yaygın olarak kullanılmaktadır (Alghamdi & Munir, 2024; Zhang vd., 2024).

Bu ölçütler, algoritmanın rastgelelik, yayılım, güvenlik ve şifre çözme kalitesi gibi temel özelliklerini sayısal olarak ortaya koymaktadır. Örneğin histogram ve korelasyon katsayıları, şifrelemenin istatistiksel saldırılara karşı direncini gösterirken; NPCR ve UACI ölçütleri diferansiyel saldırılara karşı dayanıklılığı değerlendirmektedir. Entropi, algoritmanın belirsizlik ve rastgelelik düzeyini ölçerken; PSNR ve MSE değerleri ise şifre çözme sonrasında elde edilen görüntünün orijinal görüntüye olan benzerliğini nicel olarak ifade etmektedir.

Ayrıca bu ölçütler, sağlık, askeri, biyometrik ve bulut tabanlı sistemler gibi farklı uygulama alanlarında algoritmaların karşılaştırmalı performans analizlerinde standart bir referans olarak kabul edilmektedir. Böylece araştırmacılar, farklı şifreleme yöntemlerinin güçlü ve zayıf yönlerini sistematik biçimde ortaya koyabilmekte ve pratik uygulamalar için en uygun yöntemleri seçebilmektedir.

Kaotik sistemler, deterministik denklemlere dayalı olmalarına rağmen başlangıç koşullarına son derece duyarlı ve öngörülemez davranışlar sergileyen dinamik yapılardır. Bu özellikleri sayesinde, rastgeleye benzer karmaşık diziler üreterek şifreleme algoritmalarında yüksek güvenlik seviyesinin sağlanmasında etkin bir araç olarak kullanılmaktadır (Pareek vd., 2006). Kaosun temel özellikleri arasında başlangıç koşullarına hassas bağımlılık, ergodiklik, deterministik yapı ve rassallık benzeri davranışlar yer almaktadır. Bu nitelikler, özellikle dijital görüntülerin şifrelenmesinde yüksek güvenlik elde edilmesi açısından kritik öneme sahiptir.

Kriptografide yaygın olarak kullanılan kaotik haritalar arasında Logistic Map, Tent Map, Henon Map, Lorenz attractor ve Chen sistemi bulunmaktadır. Logistic Map, basit matematiksel yapısına rağmen güçlü doğrusal olmayan özellikler sergilemesi nedeniyle sık tercih edilmektedir. Bu fonksiyon aşağıdaki denklem ile tanımlanmaktadır:

$$x_{n+1} = r * x_n(1 - x_n) \tag{2.10}$$

(2.10) nolu denklemde r parametresi sistemin kaotik davranış yoğunluğunu belirlemekte olup, özellikle $3.57 < r \leq 4$aralığında sistem tamamen kaotik hâle gelerek öngörülemez diziler üretmektedir (Kocarev, 2002).

Kaotik sistemlerin şifrelemede kullanılmasının önemli avantajlarından biri, geniş anahtar uzayları oluşturarak kaba kuvvet (brute-force) saldırılarını zorlaştırmasıdır. Kaotik dizilerin yüksek entropi üretmesi ve komşu pikseller arasındaki korelasyonu azaltması sayesinde istatistiksel saldırılara karşı güçlü bir koruma sağlanmaktadır. Örneğin Al-Maadeed vd. (2012), kaos tabanlı görüntü şifreleme algoritmalarında genişletilmiş anahtar uzayı ve düşük piksel korelasyonları elde ederek güvenlik seviyesini önemli ölçüde artırmıştır.

Ayrıca kaotik sistemlerin entropi, NPCR ve UACI gibi istatistiksel güvenlik metriklerinde yüksek performans gösterdiği birçok çalışmada ortaya konmuştur. Chen vd. (2004), kaotik harita tabanlı algoritmaların entropi, korelasyon, NPCR ve UACI sonuçlarında güçlü bir güvenlik seviyesi sağladığını göstermiştir. Bu yönüyle kaotik sistemler, hem yüksek güvenlik hem de hesaplama verimliliği sunarak özellikle büyük boyutlu görüntülerin şifrelenmesinde etkili bir çözüm oluşturmaktadır.

Hibrit şifreleme sistemleri, simetrik ve asimetrik algoritmaların güçlü yönlerini bir araya getirerek modern kriptografide yaygın biçimde kullanılan güvenlik yaklaşımlarıdır. Simetrik algoritmalar (örneğin AES, RC4, DES) yüksek hız ve düşük hesaplama maliyeti sayesinde büyük boyutlu veri veya görüntü işleme uygulamalarında avantaj sağlarken; asimetrik algoritmalar (örneğin RSA, ECC, ElGamal) güvenli anahtar yönetimi ve dağıtımı açısından güçlüdür. Bu nedenle hibrit yapılarda simetrik ve asimetrik yöntemlerin birlikte kullanılması, performans ve güvenlik açısından dengeli bir çözüm sunmaktadır (Singh & Supriya, 2013).

Hibrit modellerde veri genellikle hızlı işlem kapasitesi nedeniyle simetrik bir algoritma ile şifrelenmekte; kullanılan simetrik anahtar ise RSA veya ECC gibi bir asimetrik algoritma ile şifrelenerek güvenli biçimde saklanmakta veya iletilmektedir. Bu yaklaşım hem işlem maliyetini azaltmakta hem de anahtar güvenliğini artırmaktadır. Özellikle güvenli iletişimde kullanılan RSA–AES tabanlı hibrit yapılar hem yüksek performans hem de güçlü güvenlik sağlamaktadır.

Görüntü şifreleme alanında hibrit yöntemler, güçlü rastgelelik özellikleri ve yüksek istatistiksel güvenlik düzeyi nedeniyle literatürde sıklıkla tercih edilmektedir. AES gibi simetrik yöntemlerin işlem hızını kaotik fonksiyonlar veya asimetrik anahtar mekanizmaları ile birleştiren hibrit yaklaşımlar; düşük korelasyon, yüksek entropi ve diferansiyel saldırılara karşı direnç gibi önemli avantajlar sunmaktadır. Nitekim hibrit kaos–AES temelli yöntemlerin görüntü güvenliği açısından yüksek performans gösterdiği çeşitli çalışmalarda rapor edilmiştir (Zhang vd., 2020).

Bu avantajlar sayesinde hibrit şifreleme yapıları; bulut depolama, biyometrik görüntü güvenliği, tıbbi görüntü iletimi ve askeri haberleşme gibi hassas veri barındıran uygulamalarda yaygın olarak tercih edilmektedir. Hem güçlü anahtar yönetimi hem de yüksek şifreleme hızı sunan bu sistemler, modern veri güvenliğinde kritik bir rol üstlenmektedir.

Kaotik hibrit yaklaşımlar ise klasik hibrit şifreleme sistemlerine ek olarak kaotik dizilerin entegrasyonu ile rastgelelik ve güvenlik düzeyini daha da artırmayı amaçlamaktadır. Kaotik haritalar, başlangıç koşullarına yüksek duyarlılık ve doğrusal olmayan dinamikleri sayesinde geniş anahtar uzayları ve güçlü pseudo-rastgelelik üretmektedir. Bu nedenle simetrik algoritmaların anahtarlarının veya başlangıç vektörlerinin kaotik dizilerle oluşturulması, şifreleme sürecinin öngörülemezliğini artırmakta ve saldırılara karşı ek bir güvenlik katmanı sağlamaktadır (Pareek vd., 2006).

Kaotik yapıların hibrit sistemlere entegrasyonunda kaotik diziler genellikle simetrik şifreleme aşamasını güçlendirmek amacıyla kullanılmaktadır. Özellikle kaotik haritaların entropi, NPCR ve UACI gibi güvenlik ölçütlerinde yüksek performans gösterdiği ve diferansiyel saldırılara karşı güçlü bir direnç sağladığı çeşitli çalışmalarda doğrulanmıştır (Chen vd., 2004).

2.7. İlgili Çalışmalar

Kriptografi literatürü hem klasik hem de modern yaklaşımlarla zenginleşmiş özellikle kaotik sistemlerin ve hibrit kriptografi modellerinin şifreleme güvenliğini artırmaya yönelik potansiyeli giderek daha fazla ön plana çıkmıştır. Bu bölümde, simetrik ve asimetrik yöntemler, kaotik haritalar, hibrit sistemler ve güncel kaotik hibrit yaklaşımlar bağlamında gerçekleştirilen önemli çalışmalara yer verilmektedir.

Kriptografinin klasik temelleri, asimetrik anahtar yöntemleri ile atılmıştır. Diffie ve Hellman (1976), simetrik anahtar paylaşımındaki güvenlik problemlerine çözüm olarak açık anahtar değişim protokolünü tanıtmış ve böylece asimetrik kriptografinin temelini oluşturmuştur. Bunu izleyen yıllarda Rivest, Shamir ve Adleman (1978) tarafından geliştirilen RSA algoritması, büyük asal sayıların çarpanlara ayrılmasının zorluğuna dayalı güvenlik yapısı sayesinde yüksek bir güvenlik seviyesi sunmuştur. RSA, güvenli anahtar değişimi ve kimlik doğrulama gibi kritik senaryolarda yaygın biçimde benimsenmiş; ancak yüksek hesaplama maliyeti ve büyük veri boyutlarında doğrudan kullanımda ortaya çıkan verimlilik sınırlamaları nedeniyle tek başına büyük veri şifreleme uygulamalarında dezavantajlı hâle gelmiştir (Katz & Lindell, 2020; Stallings, 2017).

Simetrik kriptografide ise RC4, AES ve DES gibi algoritmalar temel bir rol oynamıştır. RC4, basit akış şifreleme yapısı ve her bit için dinamik anahtar akışı üretme yeteneği sayesinde uzun yıllar boyunca popülerliğini korumuştur (Singhal & Raina, 2011). Özellikle SSL/TLS gibi internet güvenliği protokollerinde yaygın olarak kullanılması, RC4'ün performans avantajlarını açıkça ortaya koymuştur. Ancak zamanla RC4 algoritmasında tespit edilen anahtar akışı önyargıları ve çeşitli güvenlik açıkları, algoritmanın savunmasız yönlerini gün yüzüne çıkarmıştır (Mousa & Hamad, 2006). Bu zafiyetler, araştırmacıları RC4'ün güvenliğini artırmaya yönelik yeni yöntemler geliştirmeye yönlendirmiştir.

RC4'ün performans özelliklerini ve güvenlik eksiklerini gidermeye yönelik çalışmalar literatürde geniş yer bulmuştur. RC4'ün pratik uygulamalardaki hız avantajı, özellikle anahtar uzunluğu ve şifrelenen veri boyutu arttıkça nasıl etkilendiği açısından sistematik biçimde incelenmiştir. Bu kapsamda Mousa ve Hamad (2006), RC4'ün performansını farklı veri büyüklükleri üzerinde değerlendirerek algoritmanın hız–güvenlik dengesi hakkında kapsamlı bulgular sunmuştur.

RC4'ün güvenlik boyutunda ise özellikle anahtar akışı üretiminde ortaya çıkan önyargılar önemli bir araştırma konusu olmuştur. Mironov (2002), RC4 keystream'inin ilk yüzlerce baytında gözlemlenen istatistiksel sapmaları ayrıntılı biçimde analiz etmiş ve bu önyargıların şifreleme güvenliğini ciddi ölçüde zayıflatabileceğini göstermiştir. Bu çalışmalar, RC4'ün modern güvenlik protokollerindeki kullanımının terk edilmesine ve daha güvenli varyantların geliştirilmesine zemin hazırlamıştır.

Geleneksel kriptografik yaklaşımların ortaya koyduğu sınırlamalara alternatif olarak, kaotik sistemler son yıllarda şifreleme alanında artan bir ilgi görmüştür. Kaotik sistemler deterministik denklemlere dayalı olmalarına rağmen başlangıç koşullarına karşı yüksek duyarlılık, ergodiklik ve pseudo-rastgelelik davranışı sergilemektedir. Bu özellikler, kaotik sistemleri anahtar üretimi ve karıştırma işlemleri için son derece uygun hâle getirmektedir (Pareek vd., 2006). Logistic Map, Tent Map, Henon Map, Lorenz çekicisi ve Chen sistemi, literatürde en sık kullanılan kaotik modeller arasında yer almakta ve hem anahtar üretimi hem de karıştırma mekanizmalarında etkin biçimde kullanılmaktadır.

Logistic Map, kaotik sistemler içerisinde en çok tercih edilen haritalardan biridir. Basit matematiksel yapısına rağmen uygun parametre aralığında deterministik fakat pseudo-rastgele davranış sergilemesi, bu haritayı kriptografik anahtar üretimi açısından avantajlı kılmaktadır. Logistic Map; rastgele anahtar dizileri üretmek, simetrik algoritmaların anahtarlarını dinamik hâle getirmek veya başlangıç vektörü olarak kullanılmak amacıyla literatürde yaygın şekilde uygulanmıştır. Kaotik sistemlerin kriptografide sunduğu en önemli avantajlardan biri, anahtar uzayını genişleterek kaba kuvvet (brute-force) saldırılarını zorlaştırmasıdır. Ayrıca kaotik diziler, düşük piksel korelasyonu ve yüksek entropi değerleri sağlayarak istatistiksel saldırılara karşı güçlü bir koruma sunmaktadır (Pareek, Patidar & Sud, 2006).

Kaotik sistemlere dayalı şifreleme yaklaşımlarının özellikle görüntü güvenliği uygulamalarında güçlü bir alternatif sunduğu birçok çalışmada gösterilmiştir. Kaotik haritalar, başlangıç koşullarına aşırı duyarlılıkları ve yüksek pseudo-rastgelelik özellikleri sayesinde hem anahtar çeşitliliğini artırmakta hem de şifreli görüntülerde korelasyon katsayılarının önemli ölçüde düşmesine katkı sağlamaktadır. Örneğin Pareek vd. (2006), Logistic Map ve benzeri kaotik fonksiyonları kullanarak geliştirdikleri görüntü şifreleme algoritmasında düşük piksel korelasyonu, yüksek entropi ve güçlü diferansiyel güvenlik elde etmişlerdir.

Benzer şekilde Chen, Mao ve Chui (2004), üç boyutlu kaotik haritaları simetrik şifreleme süreçleriyle birleştirerek hem karıştırma (confusion) hem de yayma (diffusion) aşamalarında kaotik davranışın güvenliği belirgin biçimde artırdığını göstermiştir. Bu çalışmalar, kaotik sistemlerin simetrik şifreleme yapılarını güçlendirmede etkili bir yöntem olduğunu ortaya koymaktadır.

Hibrit kriptografi, simetrik ve asimetrik yöntemlerin avantajlarını bir araya getirerek performans ve güvenlik dengesini sağlamayı amaçlamaktadır. Bu yapılarda veri genellikle simetrik bir algoritma ile şifrelenirken, simetrik anahtar asimetrik algoritmalar aracılığıyla güvenli biçimde iletilmektedir (Singh & Supriya, 2013).

RC4 ve RSA'nın birlikte kullanıldığı hibrit şifreleme yaklaşımları, hızlı veri işleme ihtiyacı ile güvenli anahtar yönetimi gereksinimini aynı anda karşılaması nedeniyle literatürde önemli bir yer edinmiştir. Bala vd. (2019), RC4–RSA tabanlı hibrit bir modelde RC4'ün veri şifreleme sürecini, RSA'nın ise yalnızca oturum anahtarını şifreleyerek güvenli anahtar dağıtımını sağladığını göstermiştir. Deneysel sonuçlar, hibrit modelin işlem süresi ve kaynak kullanımı açısından tek başına RC4 veya RSA kullanımına kıyasla daha dengeli bir performans sunduğunu ortaya koymuştur.

Benzer biçimde Yüksel ve Özgün (2021), RC4 ve RSA algoritmalarını performans, işlem süresi ve uygulama uygunluğu açısından karşılaştırmış; RC4'ün yüksek veri yoğunluğuna sahip uygulamalarda RSA'ya kıyasla çok daha hızlı çalıştığını göstermiştir. Çalışma, RSA'nın tek başına büyük veri veya görüntü işleme uygulamalarında verimli olmadığını; ancak RC4 ile birlikte hibrit bir yapıda kullanıldığında güvenliği artıran etkili bir bileşen hâline geldiğini vurgulamaktadır. Bu bulgular, RC4–RSA hibrit yöntemlerinin bulut depolama, multimedya aktarımı, IoT sistemleri ve gerçek zamanlı veri işleme gibi alanlarda uygulanabilir ve ölçeklenebilir çözümler sunduğunu göstermektedir.

Son yıllarda kaotik-hibrit sistemler, görüntü şifreleme uygulamalarında hem rastgelelik hem de güvenlik düzeyini artırması nedeniyle önemli ölçüde dikkat çekmektedir. Bu yaklaşımlarda simetrik algoritmalar (AES veya RC4 gibi), kaotik haritalar tarafından üretilen yüksek doğrusal olmayan anahtar dizileriyle desteklenmekte; böylece anahtar uzayı genişlemekte ve istatistiksel saldırılara karşı dayanıklılık artırılmaktadır. Chen vd. (2004) tarafından önerilen kaotik confusion–diffusion yapısı, bu alandaki öncü çalışmalardan biri olarak kabul edilmektedir. Pareek vd. (2006) ise Logistic Map tabanlı kaotik anahtar türetme yönteminin düşük piksel korelasyonu ve yüksek entropi açısından güçlü bir performans sunduğunu göstermiştir. Ayrıca Çavuşoğlu vd. (2016), hibrit kaotik yapıları modern blok şifreleme algoritmalarıyla birleştirerek hem güvenlik hem de hesaplama verimliliğini artıran yeni modeller önermiştir.

2020 sonrası dönemde yapılan çalışmalar, hiper-kaotik sistemler ve gelişmiş hibrit confusion–diffusion yapılarının görüntü şifreleme performansını önemli ölçüde iyileştirdiğini ortaya koymuştur. Wang vd. (2021), dört boyutlu hiper-kaotik Lorenz sistemine dayalı hibrit bir görüntü şifreleme yöntemi önererek yüksek entropi, düşük korelasyon ve güçlü diferansiyel saldırı dayanımı elde etmiştir. Benzer şekilde Liu ve Wang (2022), hiper-kaotik Chen sistemi ile AES'in birlikte kullanıldığı hibrit bir yapıda NPCR ve UACI değerlerinin geleneksel yöntemlere kıyasla belirgin şekilde yükseldiğini rapor etmiştir. Zhang vd. (2023) ise kaotik harita tabanlı anahtar üretimi ile blok tabanlı AES yapısını birleştirerek hem güvenlik hem de performans açısından iyileştirilmiş bir görüntü şifreleme modeli geliştirmiştir.

Sonuç olarak literatür, RC4, AES ve RSA gibi temel algoritmaların avantaj ve dezavantajlarını ayrıntılı biçimde ortaya koymakta; kaotik sistemlerin entegrasyonu ile güvenlik seviyesinin artırılabileceğini ve hibrit yapıların performans–güvenlik dengesini başarılı biçimde sağlayabildiğini göstermektedir. Bu tez çalışması da literatürdeki bu eğilim doğrultusunda, kaotik RC4 algoritmasını RSA ile hibritleştirerek hem güvenlik hem de performans analizlerini kapsamlı bir şekilde sunmayı amaçlamaktadır.

3. YÖNTEM

Bu tez çalışmasında geliştirilen sistem, kaotik sistemlerle güçlendirilmiş hibrit RC4 ve RSA algoritmaları kullanılarak dijital görüntülerin güvenli biçimde şifrelenmesi ve deşifre edilmesi esasına dayanmaktadır. Önerilen hibrit yapı, simetrik RC4 algoritmasının yüksek hız ve düşük hesaplama maliyeti avantajını, asimetrik RSA algoritmasının güvenli anahtar yönetimi özellikleriyle birleştirmekte; buna ek olarak kaotik Logistic Map tabanlı bir sistem ile anahtar akışının rastgeleliğini ve öngörülemezliğini artırmaktadır. Bu yaklaşım, özellikle yüksek çözünürlüklü ve büyük boyutlu görüntülerin güvenli şekilde işlenmesi gereken uygulamalarda hem performans hem de güvenlik açısından önemli avantajlar sunmaktadır.

RC4 algoritması, büyük veri setlerini hızlı bir biçimde işleyebilme yeteneği sayesinde şifreleme ve deşifreleme süreçlerinde zaman verimliliği sağlamaktadır. Ancak RC4'ün bilinen istatistiksel zayıflıkları göz önünde bulundurulduğunda, bu algoritmanın tek başına kullanımı güvenlik açısından yeterli değildir. Bu nedenle çalışmada RC4 algoritması, kaotik Logistic Map tabanlı bir sistem ile güçlendirilerek anahtar akışının dinamik ve tahmin edilemez hâle getirilmesi amaçlanmıştır. Ayrıca RSA algoritması, simetrik anahtarın güvenli biçimde iletilmesini sağlayarak yalnızca yetkili kullanıcıların şifreli veriye erişebilmesini garanti altına almaktadır. Bu üç bileşenin birlikte kullanılmasıyla çok katmanlı ve güçlü bir güvenlik yapısı oluşturulmuştur.

Uygulama, Python programlama dili kullanılarak geliştirilmiş olup kullanıcı etkileşimini artırmak amacıyla Tkinter kütüphanesi ile grafiksel bir kullanıcı arayüzü tasarlanmıştır. Geliştirilen arayüz sayesinde kullanıcılar; şifrelenecek görüntüyü seçebilmekte, RC4 şifreleme anahtarını belirleyebilmekte ve kaotik sistem parametreleri olan r ve x_0 değerlerini doğrudan sisteme girebilmektedir. Girilen bu parametreler kullanılarak Logistic Map tabanlı kaotik bir dizi üretilmekte ve elde edilen dizi RC4 algoritmasının anahtar akışı sürecine entegre edilerek şifreleme işlemi güçlendirilmektedir. Kullanıcıya sunulan bu esnek yapı, sistemin hem akademik deneysel çalışmalar hem de pratik kullanım senaryoları için uygulanabilirliğini artırmaktadır.

Sistem, şifreleme ve deşifreleme sürelerini otomatik olarak hesaplayarak kullanıcıya görsel olarak sunmaktadır. Bu özellik sayesinde, farklı anahtar ve kaotik parametre kombinasyonlarının sistem performansı üzerindeki etkileri kolaylıkla analiz edilebilmektedir.

Ayrıca uygulama kapsamında histogram analizi, entropi analizi ve korelasyon katsayısı hesaplamaları otomatik olarak gerçekleştirilmekte ve elde edilen sonuçlar kullanıcıya sunulmaktadır. Histogram analizi, orijinal ve şifreli görüntüler arasındaki piksel dağılımlarının karşılaştırılmasını sağlarken; entropi analizi, şifreli görüntünün rastgelelik düzeyini nicel olarak değerlendirmektedir. Korelasyon analizi ise şifreleme işlemi sonrasında komşu pikseller arasındaki ilişkinin ne ölçüde azaltıldığını ortaya koyarak algoritmanın istatistiksel saldırılara karşı dayanıklılığını değerlendirmeye olanak tanımaktadır.

Bu tez kapsamında geliştirilen yöntem, yalnızca şifreleme hızını artırmayı değil, aynı zamanda anahtar yönetimi ve güvenlik seviyesini optimize eden bütüncül bir hibrit yapı sunmayı hedeflemektedir. RC4 algoritmasının yüksek performansı, kaotik sistemlerin sağladığı güçlü rastgelelik özellikleri ve RSA algoritmasının güvenli anahtar paylaşım mekanizması bir araya getirilerek hem güvenli hem de verimli bir görüntü şifreleme sistemi oluşturulmuştur. Elde edilen bu yapı, akademik araştırmaların yanı sıra gerçek dünyadaki görüntü güvenliği uygulamalarında da kullanılabilecek güçlü ve ölçeklenebilir bir çözüm sunmaktadır.

3.1. Araştırmanın Amacı ve Yaklaşımı

Günümüzde dijital görüntülerin güvenliği, özellikle internet üzerinden iletilen medya içeriklerinin yetkisiz erişim, kopyalama ve manipülasyondan korunması açısından kritik bir öneme sahiptir. Gelişen teknoloji ve artan dijital içerik paylaşımı ile birlikte, klasik şifreleme yöntemleri bazı senaryolarda yeterli güvenlik sağlayamayabilir veya yüksek çözünürlüklü veriler üzerinde performans sorunlarına yol açabilir. Bu tez çalışmasının temel amacı, yüksek performanslı ve güvenli bir hibrit görüntü şifreleme yöntemi geliştirmektir. Önerilen yöntem, simetrik ve asimetrik şifreleme tekniklerini kaotik sistemlerle birleştirerek hem veri güvenliğini hem de işlem hızını optimize etmeyi hedeflemektedir. Bu çalışmada RC4 algoritması yüksek işlem hızı avantajı nedeniyle, RSA algoritması simetrik anahtarın güvenli biçimde iletilmesini sağlamak amacıyla ve kaotik lojistik harita ise anahtar uzayını genişleterek rastgeleliği artırmak ve RC4'ün bilinen istatistiksel zayıflıklarını azaltmak amacıyla tercih edilmiştir.

Bu amaç doğrultusunda benimsenen yaklaşım üç ana bileşen üzerine inşa edilmiştir:

1. Simetrik Şifreleme (RC4): RC4 algoritması, görüntü verilerinin hızlı bir şekilde şifrelenmesini sağlayarak, özellikle büyük boyutlu görüntülerin kısa sürelerde işlenmesine imkân tanır. Bu sayede şifreleme ve deşifreleme süreçlerinde zaman

maliyeti minimum seviyede tutulur. RC4'ün akış tabanlı yapısı, verilerin byte düzeyinde işlenmesine ve piksel değerlerinin dinamik bir şekilde dönüştürülmesine olanak sağlar.

2. Asimetrik Şifreleme (RSA): RC4 anahtarının güvenli bir biçimde yönetilmesi, sistemin bütünlüğü ve yetkisiz erişimlerin önlenmesi açısından kritik öneme sahiptir. RSA algoritması, kamu ve özel anahtar yapısı sayesinde, RC4 anahtarının yalnızca yetkili kullanıcılar tarafından çözülmesini sağlar. Böylece, şifreleme sürecinde kullanılan anahtarın iletimi veya saklanması sırasında ortaya çıkabilecek güvenlik açıkları ortadan kaldırılır.
3. Kaotik Sistem: Kaotik lojistik harita, RC4 anahtar akışını güçlendirerek öngörülemezliği artırır ve saldırılara karşı ek bir güvenlik katmanı oluşturur. Kaotik sistem, deterministik ama yüksek hassasiyetli bir rastgelelik sunar; küçük başlangıç değer değişiklikleri, şifreleme sonucunda tamamen farklı bir çıktıya yol açar. Bu özellik hem sistemin güvenlik seviyesini artırır hem de anahtarın tahmin edilemez olmasını sağlar.

Bu üç bileşenin birleşimi, hibrit bir şifreleme yaklaşımı oluşturur. Önerilen yöntem sayesinde, şifreleme ve deşifreleme süreleri optimize edilmiş, anahtar güvenliği sağlanmış ve görüntülerin gizliliği üst düzeye çıkarılmıştır. Ayrıca, kaotik sistemin deterministik yapısı sayesinde aynı parametreler kullanılarak şifreleme ve deşifreleme işlemleri tekrar edilebilir ve doğrulanabilir.

Bu yaklaşım, akademik araştırmalarda performans ve güvenlik analizlerinin yapılabilmesi, pratik uygulamalarda ise yüksek çözünürlüklü görüntülerin güvenli bir şekilde iletilmesi için ideal bir altyapı sunmaktadır. Sistem ayrıca, histogram, entropi ve korelasyon analizleri ile şifreleme güvenliğinin sayısal olarak değerlendirilmesine imkân tanır, böylece hem teorik hem de uygulamalı güvenlik ölçütleri karşılanmış olur.

3.2. Yazılım ve Donanım Ortamı

Bu çalışmada geliştirilen hibrit şifreleme sistemi hem yazılım hem de donanım ortamının uygunluğu doğrultusunda tasarlanmış ve test edilmiştir. Sistemin performansı ve güvenlik analizi, kullanılan yazılım kütüphaneleri ile donanım bileşenleri sayesinde optimum düzeyde sağlanmıştır.

Uygulama Python 3.11 programlama dili kullanılarak geliştirilmiştir. Python, açık kaynak yapısı, geniş kütüphane desteği ve bilimsel hesaplamalara uygunluğu sayesinde hem şifreleme algoritmalarının uygulanması hem de görsel veri işleme süreçlerinin etkin bir biçimde yürütülmesi için tercih edilmiştir. Kullanılan başlıca kütüphaneler ve işlevleri Tablo 1'de özetlenmiştir.

Bu kütüphanelerin kombinasyonu, yüksek çözünürlüklü görüntülerin hızlı bir şekilde işlenmesini ve güvenli bir şekilde şifrelenmesini mümkün kılmaktadır. Ayrıca, uygulamanın Tkinter arayüzü üzerinden kullanıcı dostu bir deneyim sunması hem akademik analiz hem de pratik kullanım açısından önem arz etmektedir.

Tablo 1. Yazılım ortamı

Kütüphane	Kullanım Alanı
Tkinter	Kullanıcı arayüzü tasarımı, giriş ve çıktı alanlarının yönetimi, buton ve metin alanları ile etkileşimlerin sağlanması
Pillow (PIL)	Görüntülerin yüklenmesi, RGB kanallarına ayrılması, dönüştürülmesi, kaydedilmesi ve şifrelenmiş/deşifrelenmiş görüntülerin görselleştirilmesi
NumPy	Görüntü verilerinin matris ve dizi işlemleri ile hızlı şekilde işlenmesi, piksel bazlı RC4 ve kaotik harita hesaplamalarının yapılması
PyCryptodome	RSA algoritması ile RC4 anahtarının güvenli bir şekilde şifrelenmesi ve çözülmesi
Matplotlib	Orijinal ve şifreli görüntülere ait histogramların oluşturulması, entropi ve korelasyon analizlerinin görselleştirilmesi
Time	Şifreleme ve deşifreleme sürelerinin ölçülmesi ve kullanıcı arayüzünde raporlanması

Sistem, performans analizlerinin doğru ve güvenilir bir biçimde yapılabilmesi için yeterli donanım kaynaklarına sahip bir bilgisayarda geliştirilmiş ve test edilmiştir. Kullanılan donanım bileşenleri ve özellikleri Tablo 2'de gösterilmiştir.

Tablo 2. Donanım ortamı

Donanım Bileşeni	Özellik
İşlemci (CPU)	Intel® Core™ i5 12th Gen, 12 çekirdek, 2.5 GHz
Ekran Kartı (GPU)	16 GB DDR4
NumPy	NVIDIA GeForce RTX 4060
Depolama Alanı	512 GB SSD
İşletim Sistemi	Windows 11 64-bit

Bu donanım yapısı, özellikle yüksek çözünürlüklü görüntülerin şifrelenmesi ve şifre çözülmesi sırasında işlem sürelerinin ölçülmesi ve algoritmaların performans karşılaştırmalarının yapılabilmesi açısından yeterli bir altyapı sunmaktadır. İşlemci ve grafik işlem biriminin sağladığı hesaplama gücü, kaotik dizilerin üretilmesi ve RC4 algoritmasının uygulanması sırasında oluşabilecek gecikmeleri minimize etmektedir. SSD depolama birimi ise görüntü dosyalarının hızlı bir şekilde yüklenmesini ve kaydedilmesini mümkün kılmaktadır.

Sonuç olarak, kullanılan yazılım ve donanım ortamı, geliştirilen hibrit şifreleme sisteminin hem güvenilir hem de yüksek performanslı bir şekilde çalışmasını sağlamış; gerçekleştirilen deneysel analizlerin tutarlı ve tekrarlanabilir olmasına katkıda bulunmuştur.

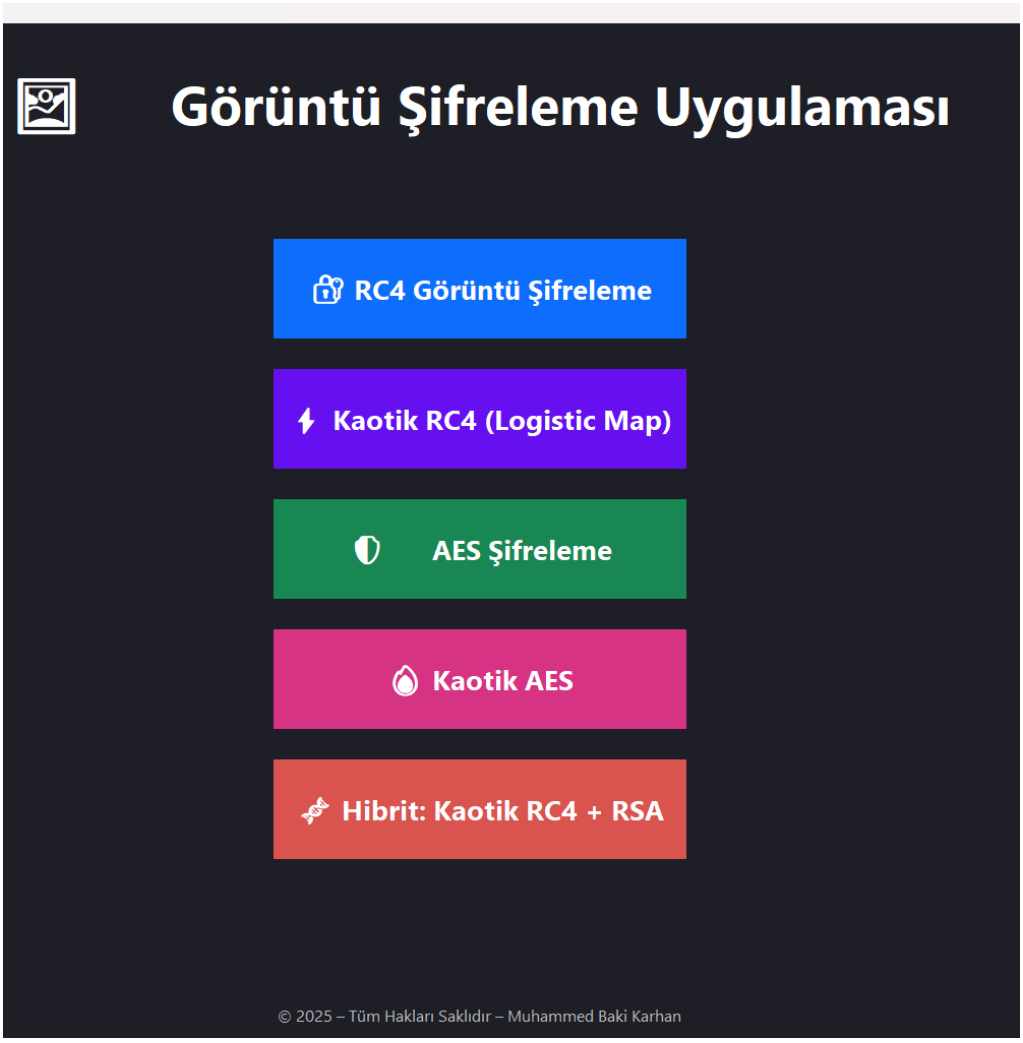
3.3. Sistem Mimarisi ve Modüller

Bu çalışmada geliştirilen görüntü şifreleme sistemi, farklı şifreleme algoritmalarını ve analiz yöntemlerini tek bir çatı altında toplayan, modüler ve kullanıcı etkileşimli bir mimari yapıda tasarlanmıştır. Sistem mimarisi, grafiksel kullanıcı arayüzü (GUI) üzerinden yönetilen ve her biri belirli bir işlevi yerine getiren bağımsız modüllerden oluşmaktadır. Bu yaklaşım, sistemin hem genişletilebilirliğini hem de farklı algoritmaların karşılaştırmalı olarak incelenebilmesini mümkün kılmaktadır.

Sistemin ana menü ekranı (Şekil 4), kullanıcıya RC4, Kaotik RC4 (Logistic Map), AES, Kaotik AES ve Hibrit Kaotik RC4 + RSA olmak üzere farklı şifreleme seçeneklerini sunmaktadır. Kullanıcı, bu ekran üzerinden çalışmak istediği algoritmayı seçerek doğrudan ilgili şifreleme

ve deşifreleme modülüne yönlendirilir. Bu yapı, sistemin algoritma bağımsız ve ölçeklenebilir bir mimariye sahip olmasını sağlamaktadır.

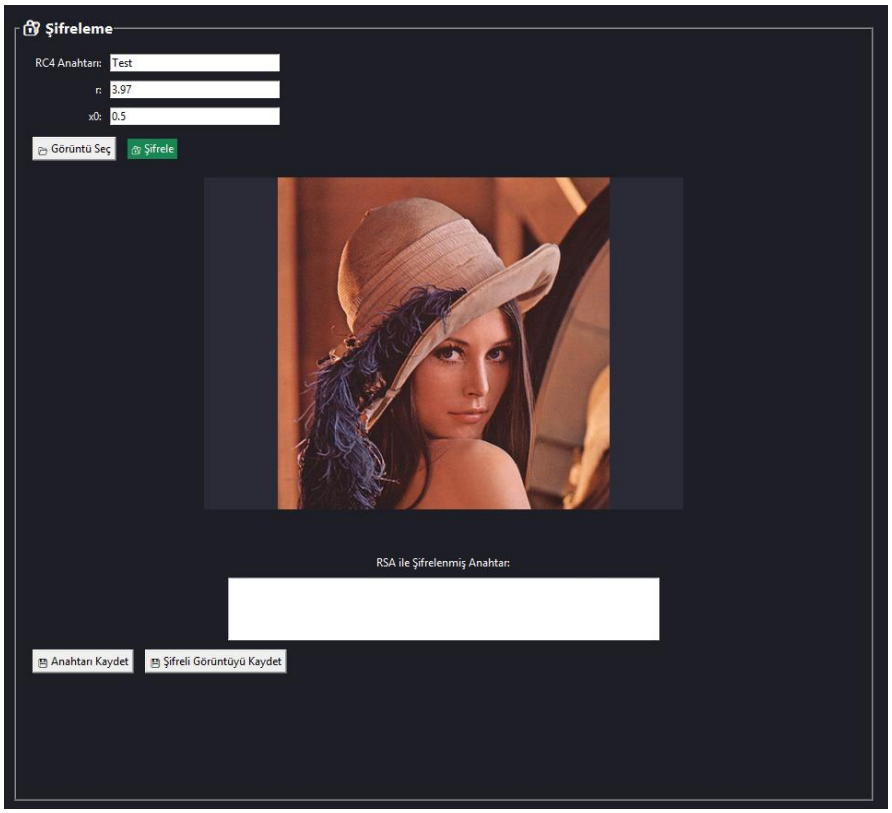
Bu tez çalışmasının ana odağı, Kaotik RC4 algoritmasının RSA ile hibrit bir yapıda birleştirilmesine dayandığından, sistem mimarisi kapsamında şifreleme ve deşifreleme süreçleri Kaotik RC4 + RSA hibrit modeli için ayrıntılı biçimde ele alınmıştır. Diğer şifreleme algoritmaları ise geliştirilen sistemin çoklu algoritma desteğini ve karşılaştırmalı analiz yeteneğini göstermek amacıyla uygulamaya entegre edilmiş olup, ilgili arayüz ekranları özet biçimde sunulmuştur.



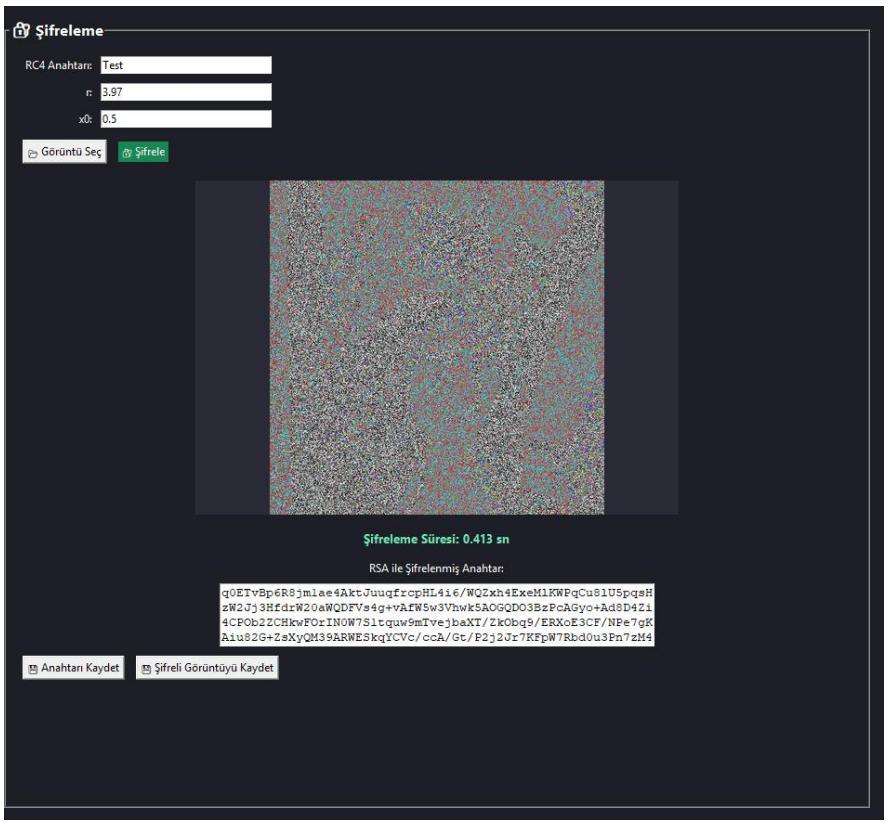
Şekil 4. Görüntü Şifreleme Uygulamasının Ana sayfası

3.3.1. Şifreleme modülü

Geliştirilen hibrit görüntü şifreleme sistemi, modüler bir yapıya sahiptir ve kullanıcı dostu bir arayüz üzerinden çalışacak şekilde tasarlanmıştır. Sistem, güvenlik ve performans gereksinimlerini karşılamak amacıyla farklı işlevsel bileşenlerden oluşmaktadır. İlk aşamada kullanıcı, bilgisayarından .png, .jpg, .jpeg veya .bmp formatındaki görüntü dosyasını seçer. Yüklenen görüntü, işleme hazır hale getirilir ve arayüzde önizleme olarak gösterilir. Bu sayede kullanıcı, doğru görüntüyü seçtiğinden emin olabilir ve şifreleme sürecine doğrudan başlayabilir. Uygulamanın şifreleme aşamasına ait arayüz ekran görüntüleri, orijinal görüntü ön izlemesi ve şifreleme sonrası elde edilen çıktı olmak üzere Şekil 5 ve Şekil 6'da sırasıyla gösterilmiştir.



Şekil 5. Şifreleme Aşamasında Orijinal Görüntünün Arayüz Üzerinde Önizlenmesi



Şekil 6. Şifreleme Sonrası Elde Edilen Şifreli Görüntünün Arayüz Üzerinde Gösterimi

Güvenlik altyapısının temelini kaotik anahtar üretimi oluşturur. Kullanıcı tarafından girilen parametreler (r ve x_0), kaotik bir sayı dizisinin oluşturulmasını sağlar. Bu diziler, RC4 anahtar akışını güçlendirerek öngörülemezliği artırır ve sistemin deterministik yapısı sayesinde deşifreleme sırasında aynı parametreler kullanılarak yeniden üretilebilir. Böylece hem güvenlik hem de veri bütünlüğü sağlanmış olur.

RC4 algoritması, simetrik şifreleme yöntemi olarak görüntü verilerini hızlı bir şekilde şifreler. Sistem, görüntüyü RGB kanallarına ayırır ve her kanal üzerinde kaotik dizi ile güçlendirilmiş RC4 algoritmasını uygular. Bu yöntem, piksel bazlı şifreleme yaparken yüksek performans sağlar. Şifrelenmiş görüntü, kullanıcıya arayüz üzerinden gösterilir ve kaydedilebilir. RC4 anahtarı, sistemin güvenlik seviyesini artırmak amacıyla RSA algoritması ile şifrelenir. Anahtar, public key kullanılarak şifrelenir ve yalnızca private key ile çözülebilir. Bu yöntem, anahtar yönetimini güvence altına alır ve kullanıcıların güvenli bir biçimde anahtarı saklamasını veya iletmesini sağlar.

Kaotik sistemler, deterministik bir yapıya sahip olmalarına rağmen öngörülemez ve rastgele gibi görünen diziler üretebilirler. Bu özellikleri nedeniyle kriptografi ve veri güvenliği alanında özellikle anahtar güçlendirme amacıyla yaygın olarak kullanılmaktadır. Kaotik sistemler, geleneksel rastgele sayı üreteçlerinden farklı olarak başlangıç parametreleri ve kaotik parametreye bağlı deterministik diziler üretir; bu diziler, algoritmanın tekrarlandığında aynı sonucu vermesini sağlar ancak dışarıdan gözlemlendiğinde tamamen öngörülemez görünür.
Bu tez çalışmasında kullanılan kaotik yapı, Logistic Map (Lojistik Harita) olarak adlandırılan matematiksel model üzerinden oluşturulmuştur. Lojistik harita, basit bir doğrusal olmayan denklem ile her iterasyonda bir önceki değeri kullanarak yeni değer üretir ve kaotik davranış sergiler. Lojistik harita matematiksel olarak şu şekilde ifade edilir:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n) \tag{3.1}$$

Burada;
r: Kaotik parametre olup, 3.57 ile 4 arasında seçildiğinde sistem kaotik davranış gösterir.
x_0: Başlangıç değeri, 0 ile 1 arasında rastgele seçilir.
x_n: n. iterasyondaki kaotik değer.
Sistem, kullanıcıdan alınan r ve x_0 değerlerini kullanarak deterministik bir kaotik dizi üretir. Bu diziler, görüntü verisinin şifrelenmesinde kullanılan RC4 anahtar akışını güçlendirmek için 0–255 aralığına dönüştürülür. Her piksel için yapılan XOR işlemlerinde bu kaotik diziler kullanıldığında, aynı RC4 anahtarı bile farklı kaotik diziler ile birleştirilerek şifreleme sırasında değişkenlik yaratır ve anahtar tahminini son derece güçleştirir.

Kaotik sistemin bir diğer önemli avantajı, deterministik yapı sayesinde deşifreleme sırasında aynı r ve x_0 değerleri kullanılarak aynı kaotik dizinin yeniden üretilebilmesidir. Bu sayede sistem hem güvenli hem de geri döndürülebilir bir şifreleme süreci sağlar. Ayrıca, kaotik dizilerin kullanımı, RC4 algoritmasının doğal zayıflıklarını minimize ederek daha güçlü bir hibrit şifreleme yöntemi oluşturur.

Görselleştirme açısından, üretilen kaotik diziler histogram ve dağılım analizleri ile incelenebilir. Bu analizler, dizinin öngörülemezliğini ve kriptografik dayanıklılığını doğrulamak için önemlidir. Kaotik dizilerin özellikleri, sistemin genel güvenlik seviyesi ve performansı üzerinde doğrudan etkili olduğundan, kullanıcı tarafından belirlenen r ve x_0 değerlerinin önemi büyüktür.

Bu yöntem, yüksek hız ve düşük gecikme sağlayarak gerçek zamanlı veya büyük boyutlu görüntü işleme gerektiren uygulamalarda etkilidir. Ayrıca, kaotik sistem ile güçlendirilmiş RC4 akışı, klasik RC4'ün öngörülebilir zayıflıklarını minimize eder ve daha güvenli bir akış şifreleme mekanizması sunar. Önerilen hibrit sistemde RC4 şu adımlarla uygulanır:

1. Görüntü Kanallarının Ayrılması: Orijinal görüntü RGB (Red, Green, Blue) kanallarına ayrılır. Her kanal, ayrı bir matris olarak işlenir.
2. Düzleştirme ve Kaotik Anahtar Akışı: Her kanal, tek boyutlu bir diziye dönüştürülür ve kaotik logistic map ile güçlendirilmiş RC4 anahtarı ile birleştirilir. Bu sayede her piksel için farklı ve öngörülemez bir anahtar akışı oluşturulur.
3. XOR İşlemi ile Şifreleme: Kaotik anahtar akışı ile piksel değerleri XOR işlemine tabi tutulur ve şifrelenmiş pikseller elde edilir.
4. RGB Matrisine Dönüştürme: Şifrelenmiş pikseller tekrar orijinal RGB formatında matrise dönüştürülür ve şifrelenmiş görüntü elde edilir.

Simetrik şifrelemenin bir zayıf noktası, anahtar yönetimidir. RC4 ile şifreleme sırasında kullanılan anahtarın güvenli bir şekilde iletilmesi ve saklanması gereklidir. Bu çalışma, RC4 anahtarının güvenliğini sağlamak için RSA asimetrik şifreleme yöntemini kullanır.
Şifreleme işleminde RC4 anahtarı, RSA'nın public key kullanılarak şifrelenir:

$$K_{\text{enc}} = \text{RSA}_{\text{pub}}(\text{RC4 key}) \tag{3.2}$$

Deşifreleme işleminde şifrelenmiş RC4 anahtarı yalnızca RSA'nın private key kullanılarak çözülebilir:

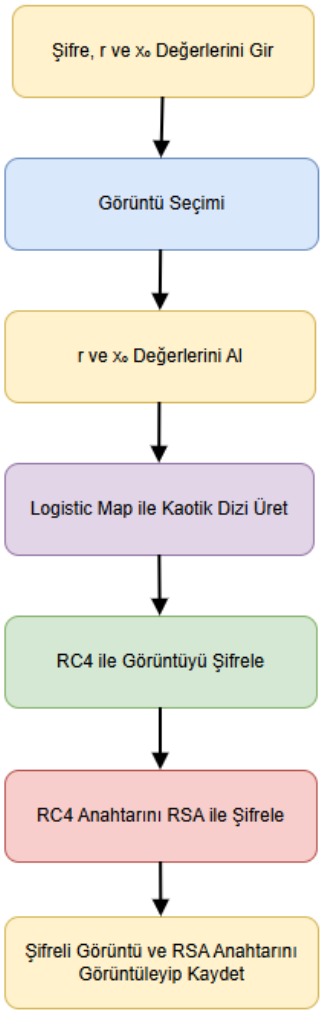
$$\text{RC4 key} = \text{RSA}_{\text{priv}}^{-1}(K_{\text{enc}}) \tag{3.3}$$

Bu işlem, RC4 anahtarının güvenli bir şekilde iletilmesini sağlar. Şifrelenmiş anahtar dosyaları base64 formatında saklanır ve kullanıcı arayüzünde görüntülenebilir.

Önerilen sistemde kaotik RC4 ve RSA algoritmaları hibrit bir yapıda birleştirilmiştir. Bu yapı hem simetrik hem de asimetrik şifrelemenin avantajlarını aynı anda kullanır:

1. Performans ve Hız: RC4 algoritması, görüntü verilerini hızlı bir şekilde şifreleyerek yüksek performans sağlar.
2. Güvenli Anahtar Yönetimi: RC4 anahtarı, RSA public key ile şifrelenerek güvenli bir şekilde saklanır ve iletilir. Anahtarın yalnızca private key ile çözülmesi, üçüncü şahısların veriye erişimini engeller.
3. Kaotik Sistem Güçlendirmesi: RC4 anahtar akışı, kaotik logistic map ile güçlendirilir. Bu sayede aynı RC4 anahtarı bile kaotik dizilerle birleştirildiğinde farklı bir şifreleme çıktısı üretir ve öngörülemezlik artar.
4. Hibrit yapı sayesinde sistem hem yüksek güvenlik seviyesi sağlar hem de yüksek performans ile hızlı şifreleme gerçekleştirir. Bu yöntem, özellikle büyük boyutlu ve yüksek çözünürlüklü görüntülerin korunmasında etkili bir çözüm sunmaktadır.

Sistemin işleyişi akış diyagramı ile özetlenebilir. Akış, görüntü yükleme, kaotik dizi üretimi, RC4 şifreleme, RSA ile anahtar şifreleme, deşifreleme ve performans ölçüm modüllerinin birbirini takip eden adımlarını gösterir. Bu yapı, modüller arası veri akışını net bir şekilde ortaya koyarak sistemin bütünlüğünü ve işlevselliğini açıklar. Şifreleme modülünün akış diyagramı Şekil 7'te verilmiştir.



Şekil 7. Şifreleme Akış Diyagramı

Görüntü Seçimi: Kullanıcı, bilgisayarından desteklenen formatlarda (.png, .jpg, .bmp) bir görüntü seçer. Sistem, seçilen görüntüyü önizleme amacıyla arayüzde gösterir.

R ve x_0 Değerlerinin Alınması: Kullanıcı, kaotik logistic map'in çalışması için gerekli olan r (kaotik parametre) ve x_0 (başlangıç değeri) parametrelerini girer. Bu parametreler algoritmanın deterministik fakat öngörülemez kaotik diziler üretmesini sağlar.

Kaotik Dizi Üretimi (Logistic Map): Girilen r ve x_0 değerleri kullanılarak her piksel için kaotik bir dizi üretilir. Üretilen dizi, RC4 anahtar akışının çeşitli noktalarında kullanılarak sürece ek bir rastgelelik kazandırır.

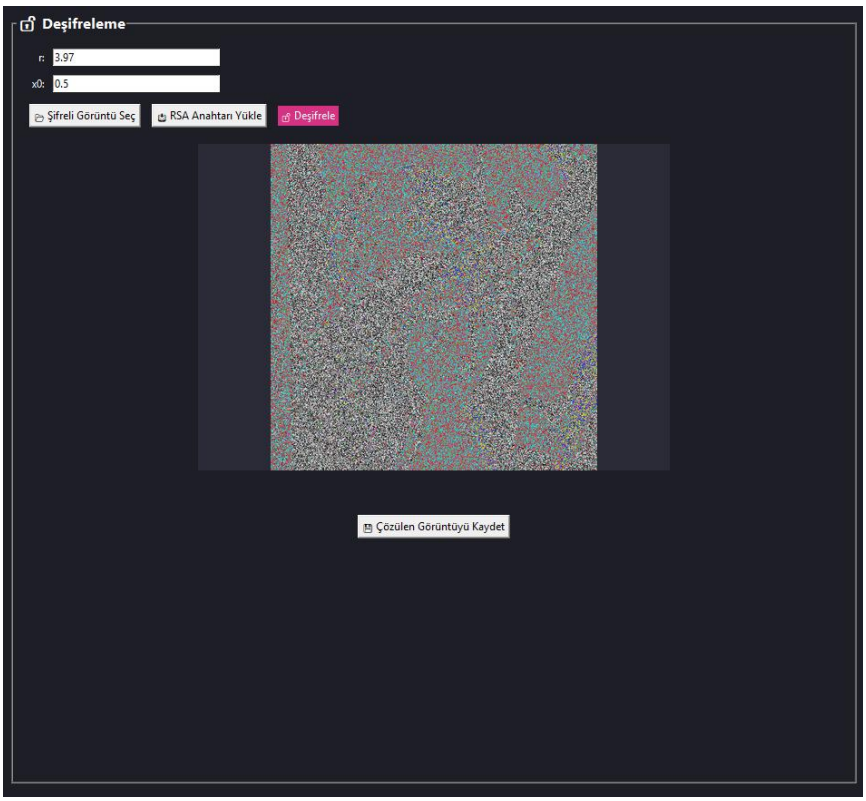
RC4 Şifreleme (Kaotik Sistem ile Birlikte): Görüntü R, G ve B kanallarına ayrılır. RC4 anahtar akışı elde edilir. Her piksel, kaotik dizi ile güçlendirilmiş RC4 akışıyla XOR işlemine tabi tutulur. Bu işlem sonucunda şifrelenmiş piksel matrisi oluşturulur.

RSA ile RC4 Anahtarının Şifrelenmesi**:** Şifrelemede kullanılan RC4 anahtarı, RSA public key kullanılarak şifrelenir. Böylece RC4 anahtarı güvenli şekilde saklanabilir veya başka bir tarafa güvenli biçimde iletilebilir.

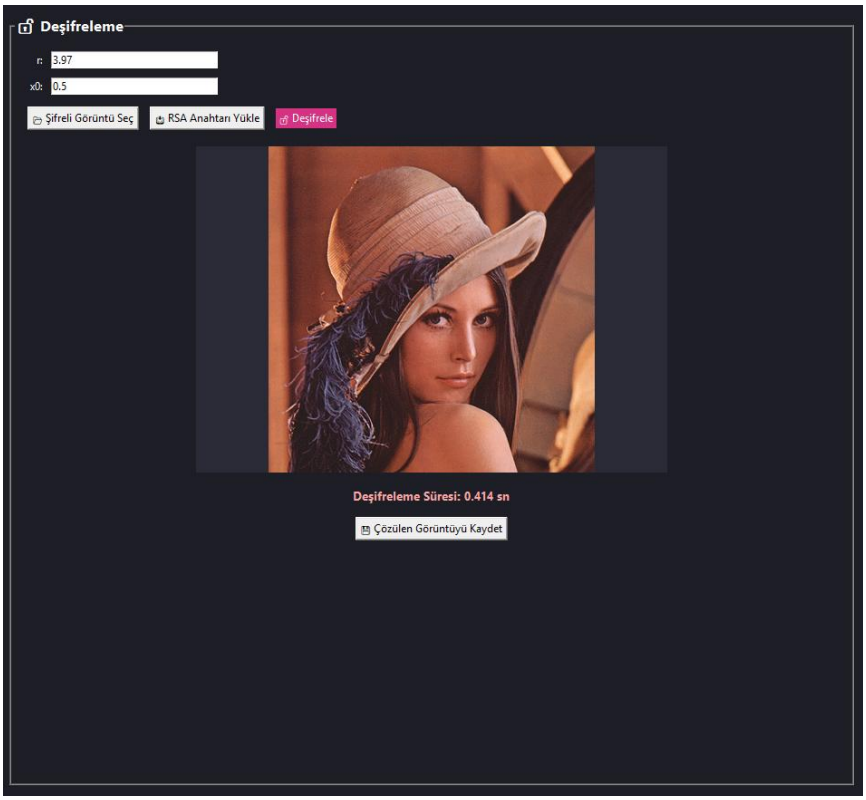
Şifreli Görüntü ve Anahtar Kaydı: Şifrelenmiş görüntü dosyası kaydedilir. RSA ile şifrelenmiş RC4 anahtarı da aynı klasöre veya belirlenen konuma kaydedilir. Böylece görüntü hem güvenli hem de geri çözülebilir bir biçimde saklanmış olur.

3.3.2. Deşifreleme modülü

Deşifreleme sürecinde, şifrelenmiş görüntü ve RSA ile şifrelenmiş anahtar kullanılarak orijinal görüntü yeniden oluşturulur. RSA private key ile RC4 anahtarı çözülür ve kaotik diziler tekrar üretilir. Daha sonra RC4 algoritması kullanılarak görüntü RGB kanalları bazında geri dönüştürülür. Bu süreç, sistemin deterministik yapısını ve güvenli veri aktarımını garanti eder. Sistem, şifreleme ve deşifreleme sürelerini otomatik olarak ölçer ve kullanıcıya görsel olarak sunar. Ayrıca, şifrelenmiş ve orijinal görüntüler arasında histogram, entropi ve korelasyon analizleri yapılabilir. Bu sayede hem akademik analiz hem de pratik kullanım açısından kapsamlı bir değerlendirme imkânı sağlanır. Uygulamanın deşifreleme aşamasına ait arayüz ekran görüntüleri, şifreli görüntünün sisteme yüklenmesi ve deşifreleme sonrası elde edilen orijinal görüntünün gösterimi olmak üzere Şekil 8 ve Şekil 9'da sırasıyla sunulmuştur.



Şekil 8. Deşifreleme Aşamasında Şifreli Görüntünün Arayüz Üzerinden Yüklenmesi



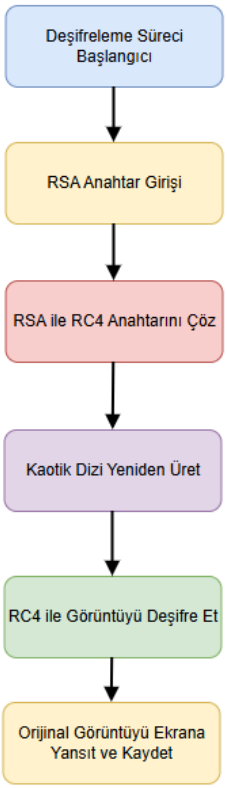
Şekil 9. Deşifreleme Sonrası Elde Edilen Orijinal Görüntünün Arayüz Üzerinde Gösterimi

RSA Private Key ile RC4 Anahtarının Çözülmesi: Kayıtlı RSA şifreli RC4 anahtarı, RSA private key kullanılarak çözülür. Böylece şifrelemede kullanılan gerçek RC4 anahtarı elde edilir.

Kaotik Dizinin Yeniden Üretilmesi: Şifreleme sırasında kullanılan r ve x_0 parametreleri, deşifrelemede tekrar girilir. Aynı logistic map iterasyonu yeniden çalıştırılarak şifreleme sırasında oluşan kaotik dizinin birebir aynısı elde edilir.

RC4 ile Görüntünün Deşifre Edilmesi: RC4 akışı yeniden oluşturulur. RGB kanalları üzerinde XOR işlemi uygulanır ve Kaotik dizinin etkisi de hesaba katılarak şifre çözme işlemi gerçekleştirilir. Sonuç olarak orijinal piksel matrisi elde edilir.

Orijinal Görüntünün Ekrana Yansıtılması ve Kaydedilmesi: Deşifre edilen piksel matrisi yeniden görüntü formatına dönüştürülür ve arayüzde gösterilir. Böylece kullanıcı orijinal görüntüyü eksiksiz şekilde görebilir. Deşifreleme modülünün akış diyagramı Şekil 10'da verilmiştir



Şekil 10. Deşifreleme Akış Diyagramı

3.4. Performans ve Güvenlik Analizleri

Önerilen görüntü şifreleme algoritmasının güvenlik düzeyi ve işlem performansı çeşitli analitik yöntemlerle kapsamlı şekilde değerlendirilmiştir. Yapılan analizler hem şifreleme yapısının rastgelelik ve dayanıklılık açısından güçlü olduğunu hem de performans açısından kullanıcı gereksinimlerini karşıladığını göstermektedir. Bu kapsamda incelenen temel ölçütler aşağıda özetlenmiştir:

- Entropi Analizi: Şifrelenmiş görüntüdeki piksellerin rastgelelik seviyesi ölçülmüştür. Yaklaşık ideal değerlere yakın entropi oranları, algoritmanın yüksek düzeyde bilgi gizleme kapasitesine sahip olduğunu kanıtlamaktadır.

- Histogram Analizi: Orijinal ve şifrelenmiş görüntülerin histogramları karşılaştırılmıştır. Şifrelenmiş görüntünün histogramının tamamen farklı ve düzensiz bir dağılıma sahip olması, algoritmanın istatistiksel saldırılara karşı başarılı bir koruma sağladığını göstermektedir.

- Korelasyon Katsayısı Analizi: Şifreleme öncesi komşu pikseller arasında yüksek olan korelasyon, şifreleme işleminden sonra neredeyse sıfıra yakın değerlere düşmüştür. Bu durum, komşu piksel ilişkilerinin etkili biçimde bozulduğunu ve algoritmanın diferansiyel saldırılara karşı dayanıklı olduğunu ortaya koymaktadır.

- PSNR ve SSIM Analizleri: Şifrelenmiş görüntü ile orijinal görüntü arasındaki fark nicel olarak değerlendirilmiştir.

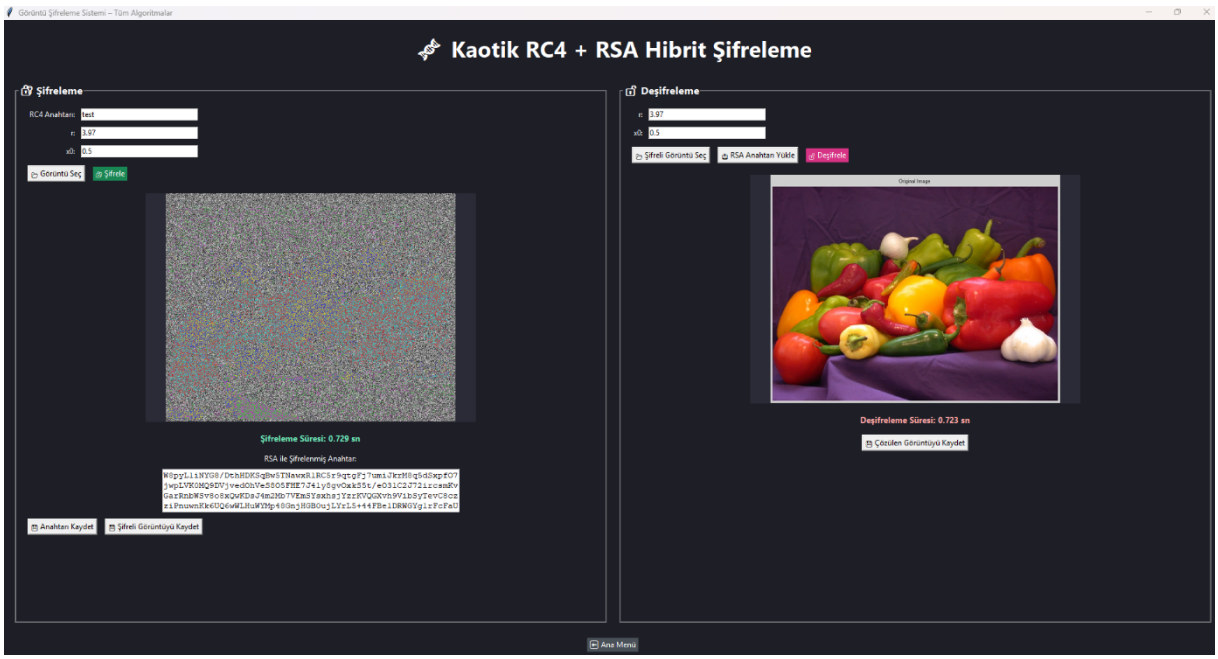
    - Düşük PSNR değerleri, şifreleme işleminin görüntüyü tamamen bozduğunu ve orijinal bilgiyi gizlediğini,
    - Düşük SSIM değerleri ise yapısal benzerliğin ortadan kalktığını ve şifrelemenin etkin şekilde uygulandığını göstermektedir.

- Şifreleme ve Deşifreleme Süreleri: Algoritmanın işlem hızı değerlendirilmiş, şifreleme ve deşifreleme süreleri karşılaştırmalı olarak sunulmuştur. Elde edilen sürelerin gerçek zamanlı uygulamalar için yeterli olduğu gözlemlenmiştir.

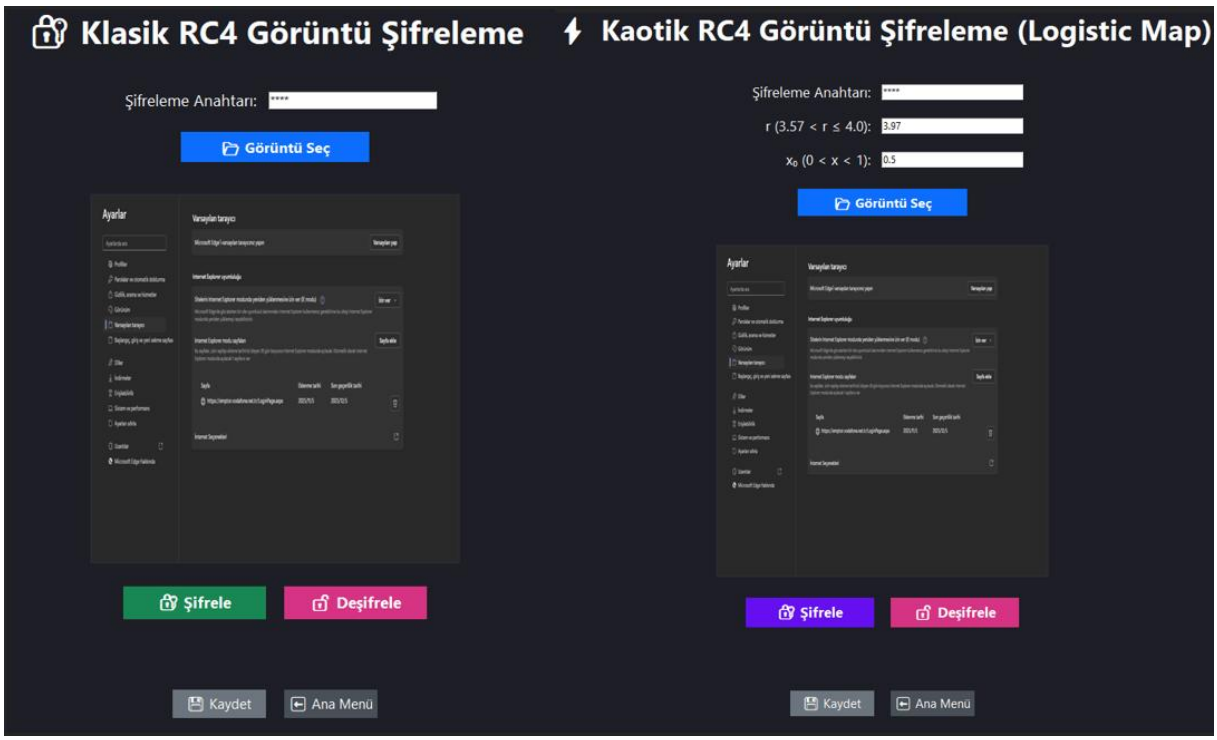
Bu değerlendirmeler sonucunda geliştirilen algoritmanın hem kriptografik açıdan güçlü bir yapıya sahip olduğu hem de işlem performansı bakımından verimli çalıştığı sonucuna varılmıştır. Bu bütüncül analizler, sistemin güvenlik ve hız açısından dengeli bir şifreleme çözümü sunduğunu göstermektedir. Önerilen sistem sayesinde:

- Kaotik sistem rastgelelik ve anahtar güçlendirme sağlar.
- RC4 algoritması hızlı ve verimli şifreleme sunar.
- RSA algoritması güvenli anahtar yönetimi gerçekleştirir.

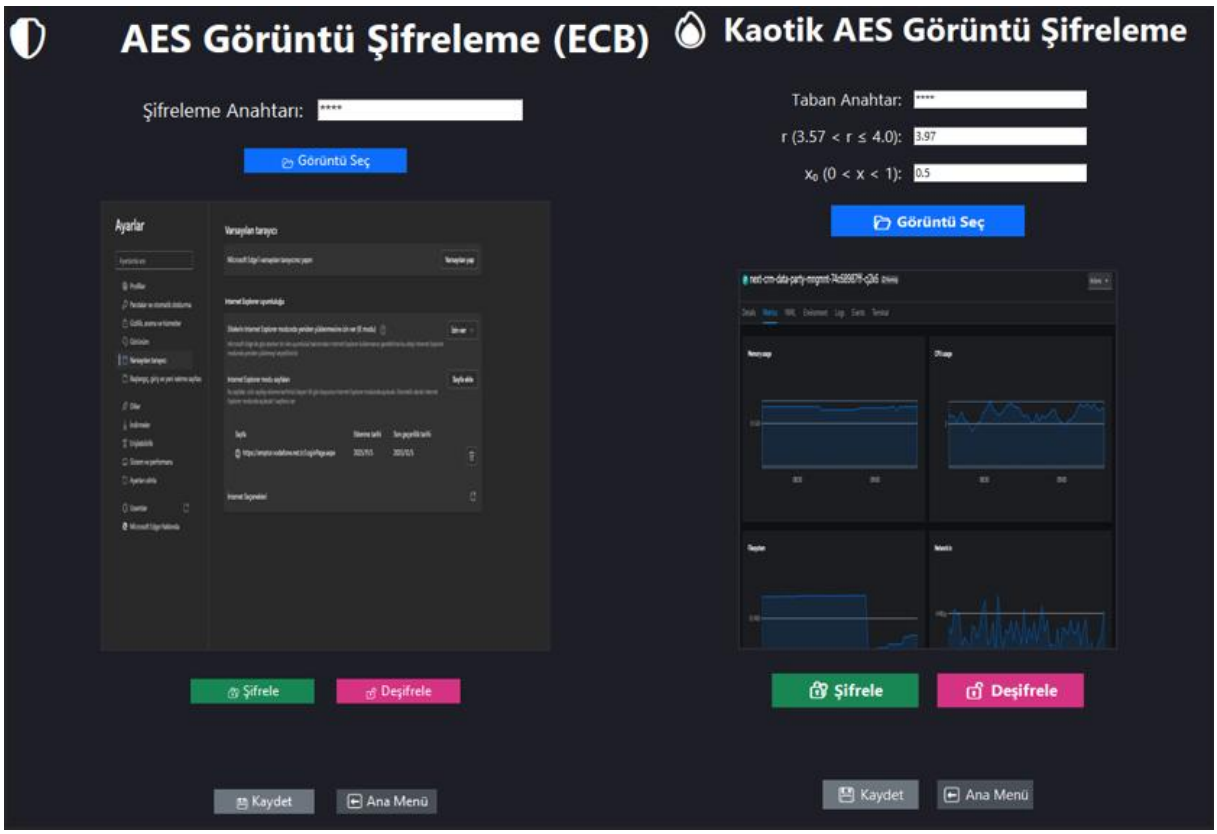
Sonuç olarak, geliştirilen sistem hem akademik analizler hem de pratik kullanım senaryoları için uygun, hibrit bir görüntü şifreleme ortamı sunmaktadır. Kullanıcı dostu Tkinter tabanlı arayüz, veri görselleştirme ve performans ölçümleri ile sistemin uygulanabilirliğini artırmaktadır. Şekil 11'de, Kaotik RC4 + RSA hibrit modeline ait şifreleme ve deşifreleme işlemlerinin aynı arayüz üzerinde eş zamanlı olarak gerçekleştirildiği uygulama ekranı sunularak, sistemin analiz düzeyinin ötesinde gerçek kullanım ortamında da etkin biçimde çalıştığı görsel olarak ortaya konmuştur. Şekil 12 ve Şekil 13'te diğer şifreleme yöntemlerine ait uygulama arayüz gösterimleri verilmiştir.



Şekil 11. Kaotik RC4 + RSA Hibrit Modelinde Şifreleme ve Deşifreleme İşlemlerinin Aynı Arayüz Üzerinde Gösterimi



Şekil 12. Klasik RC4 ve Kaotik RC4 Uygulama Arayüz Gösterimi



Şekil 13. Klasik AES ve Kaotik AES Uygulama Arayüz Gösterimi

4. BULGULAR

Bu bölümde, geliştirilen kaotik tabanlı hibrit görüntü şifreleme sisteminin performansı farklı çözünürlükler ve renk formatları altında kapsamlı biçimde değerlendirilmiştir. Sistem; AES, Kaotik AES, RC4, Kaotik RC4 ve Kaotik RC4 + RSA hibrit modelleri kullanılarak test edilmiş; her bir algoritma için histogram korelasyonu, entropi, PSNR, SSIM ve şifreleme/deşifreleme işlem süreleri ayrı ayrı analiz edilmiştir.

Analizler hem renkli hem de gri seviyeli görüntüler üzerinde iki farklı çözünürlükte (512×512 ve 765×603) gerçekleştirilmiş ve algoritmalar güvenlik, performans ve kalite ölçütleri açısından karşılaştırılmıştır. Elde edilen bulgular, şifrelenmiş görüntülerin rastgelelik düzeylerini, yapısal benzerlikten sapma oranlarını ve şifreleme işlemi sonucu oluşan bozulma seviyelerini ayrıntılı biçimde ortaya koymakta; aynı zamanda hibrit yaklaşımın tekil yöntemlere kıyasla sunduğu avantajları açık biçimde göstermektedir.

Gerçekleştirilen 10 tekrar sonucunda, güvenlik metrikleri olan histogram dağılımı, korelasyon katsayısı, entropi, PSNR ve SSIM değerlerinin genel eğilim açısından kararlılık gösterdiği ve tekrarlar arasında anlamlı bir farklılık oluşturmadığı gözlemlenmiştir. Buna karşın, şifreleme ve deşifreleme sürelerinde sistemsel etkenlere bağlı olarak milisaniye düzeyinde değişiklikler meydana gelmiştir. Bu doğrultuda, bulgular bölümünde sunulan zaman performansına ilişkin sonuçlar ortalama değerler esas alınarak raporlanmıştır.

4.1. 512 × 512 Renkli Görüntü Şifreleme Sonuçları

512×512 çözünürlüğündeki renkli görüntü üzerinde gerçekleştirilen analizler, özellikle entropi ve histogram korelasyonu açısından tüm şifreleme yöntemlerinin oldukça başarılı sonuçlar ürettiğini göstermektedir. Şifreli görüntülerin entropi değerleri yaklaşık 7.999 seviyesinde olup, teorik maksimum değer olan 8'e oldukça yakındır. Bu durum, tüm algoritmaların rastgelelik açısından neredeyse ideal performans sergilediğini göstermektedir.

Histogram korelasyonu açısından en düşük değer Kaotik RC4 yönteminde elde edilmiş ve negatif korelasyon değeri gözlemlenmiştir. Bu sonuç, şifreli görüntü ile orijinal görüntü arasında neredeyse tamamen rastlantısal bir ilişki bulunduğunu ve kaotik RC4 yönteminin rastgelelik üretme kapasitesini belirgin biçimde artırdığını doğrulamaktadır.

PSNR değerleri tüm algoritmalarda yaklaşık 8–8.4 dB aralığında olup, şifreli görüntü ile orijinal görüntü arasında büyük bir fark bulunduğunu göstermektedir. SSIM değerlerinin de oldukça düşük çıkması (0.007–0.009 aralığı), şifreleme işleminin yapısal benzerliği neredeyse tamamen ortadan kaldırdığını göstermektedir. Bu bulgular, şifreleme işleminin başarılı olduğunu ve şifreli görüntünün orijinal görüntüye ait anlamlı herhangi bir bilgi taşımadığını açıkça ortaya koymaktadır.

İşlem süreleri açısından RC4, yaklaşık 0.09 sn ile en hızlı yöntem olarak öne çıkmaktadır. Kaotik RC4 ve RC4+RSA hibrit yöntemleri orta seviyede işlem süresi sunarken, AES tabanlı yöntemlerin daha yavaş çalıştığı gözlemlenmiştir (0.27–0.29 sn). Buna karşın hibrit RC4+RSA modeli, RSA anahtar işlemi içermesine rağmen AES tabanlı yöntemlerden daha hızlı çalışmış ve işlem performansı açısından rekabetçi bir yapı sergilemiştir. Bu değerlendirmelere ilişkin sayısal sonuçlar, farklı şifreleme algoritmalarının histogram korelasyonu, entropi, PSNR, SSIM ve işlem süreleri bakımından karşılaştırmalı olarak Tablo 3'te sunulmuştur.

Tablo 3. 512 x 512 Renkli görüntü şifreleme performans tablosu

Algoritma Adı	Histogram Korelasyonu	Entropi	PSNR	SSIM	Şifreleme (sn)	Deşifreleme (sn)
AES	0.0252	7.993	8.3984	0.0078	0.27286	0.26286
Kaotik AES	0.0229	7.9993	8.3939	0.0084	0.28391	0.29320
RC4	0.0239	7.9992	8.3849	0.0086	0.09898	0.09944
Kaotik RC4	-0.01181	7.9993	8.3965	0.0086	0.18294	0.18033
Kaoitik RC4+RSA Hibrit Şifreleme	0.0031	7.9993	8.3881	0.0079	0.22100	0.21800

4.2. 512 × 512 Gri Görüntü Şifreleme Sonuçları

512×512 çözünürlüğündeki gri seviyeli görüntülerde elde edilen sonuçlar, renkli görüntülerdeki bulgularla büyük ölçüde paralellik göstermektedir. Entropi değerleri yine 7.999 civarında olup, şifreli görüntünün yüksek rastgelelik özelliğini koruduğunu göstermektedir.

Histogram korelasyon değerleri genel olarak renkli görüntülere kıyasla daha düşük çıkmıştır. Bu durum, gri görüntülerin tek kanallı yapısı nedeniyle şifreleme etkisinin daha belirgin hâle geldiğini göstermektedir. Özellikle AES algoritmasında negatif korelasyon değerinin elde edilmesi, şifreli görüntü ile orijinal görüntü arasında istatistiksel bir ilişkinin kalmadığını ortaya koymaktadır.

PSNR değerleri gri görüntülerde yaklaşık 9 dB seviyesine yükselmiş olup, bu durum gri görüntülerin renkli görüntülere kıyasla şifreleme sonrası biraz daha az bozulma ürettiğini göstermektedir. SSIM değerleri ise tüm algoritmalarda oldukça düşük seviyelerde kalmış (0.009–0.010 aralığı) ve yapısal bilginin tamamen yok edildiğini doğrulamıştır.
İşlem süreleri açısından RC4 algoritması yine en hızlı yöntem olarak öne çıkmıştır. Kaotik RC4 yöntemi RC4'e kıyasla daha yavaş çalışsa da, RC4+RSA hibrit yöntemi gri görüntülerde dahi AES tabanlı yöntemlerden daha düşük işlem süresi sunarak hibrit yapının pratik uygulamalar açısından uygunluğunu göstermiştir. 512×512 çözünürlüğündeki gri seviyeli görüntüler üzerinde elde edilen performans ve güvenlik ölçütleri, renkli görüntülerle benzer eğilimler sergilemektedir. Entropi, histogram korelasyonu, PSNR, SSIM ve işlem sürelerine ait sayısal sonuçlar Tablo 4'te sunulmuştur.

Tablo 4. 512 x 512 Gri Görüntü Şifreleme Performans Tablosu

Algoritma Adı	Histogram Korelasyonu	Entropi	PSNR	SSIM	Şifreleme (sn)	Deşifreleme (sn)
AES	-0.0165	7.9991	9.1329	0.0098	0.25813	0.25394
Kaotik AES	0.0054	7.9991	9.1310	0.0103	0.26024	0.26126
RC4	0.0720	7.9993	9.1389	0.0093	0.12974	0.12987
Kaotik RC4	0.0463	7.9994	9.1298	0.0094	0.15604	0.15238
Kaoitik RC4+RSA Hibrit Şifreleme	0.0410	7.9993	9.1208	0.0100	0.21800	0.22400

4.3. 765 × 603 Renkli Görüntü Şifreleme Sonuçları

765×603 çözünürlüğündeki daha büyük boyutlu renkli görüntüler üzerinde yapılan analizlerde, tüm algoritmaların entropi değerlerinin yine hedeflenen maksimuma oldukça yakın olduğu görülmüştür. Özellikle RC4 ve hibrit RC4+RSA yöntemleri 7.9996 gibi ideal bir entropi

değerine ulaşarak yüksek çözünürlükte dahi mükemmel bir rastgelelik performansı sergilemiştir.

Histogram korelasyon değerleri tüm algoritmalarda 0.03–0.07 aralığında ölçülmüş ve bu değerler, orijinal görüntü ile şifreli görüntü arasında anlamlı bir ilişkinin kalmadığını göstermiştir.

PSNR değerleri bir önceki çözünürlüğe kıyasla bir miktar düşerek 7.4–7.5 dB aralığında gerçekleşmiştir. Bu durum, yüksek çözünürlüklü görüntülerde şifreleme kaynaklı bozulmaların daha belirgin olduğunu göstermektedir. SSIM değerleri ise tüm algoritmalar için oldukça düşük çıkmış ve yapısal benzerliğin tamamen yok edildiği doğrulanmıştır.

İşlem süreleri incelendiğinde RC4 yine en hızlı yöntem olarak öne çıkmıştır (≈0.17 sn). AES ve Kaotik AES yöntemleri çözünürlük arttıkça daha yavaş çalışmış, Kaotik AES özellikle 0.35 sn üzerindeki süreleriyle düşük hız performansı sergilemiştir. Hibrit RC4+RSA yöntemi ise RSA anahtar işlemleri nedeniyle en yavaş yöntem olmakla birlikte, sunduğu güvenlik seviyesiyle bu maliyeti dengelemektedir. Daha yüksek çözünürlüklü (765×603) renkli görüntüler üzerinde gerçekleştirilen analizler, algoritmaların ölçeklenebilirliğini değerlendirmek açısından önem taşımaktadır. Bu çözünürlükte elde edilen histogram korelasyonu, entropi, PSNR, SSIM ve işlem süresi değerleri Tablo 5'te ayrıntılı olarak verilmiştir.

Tablo 5.765 x 603 Renkli görüntü şifreleme performans tablosu

Algoritma Adı	Histogram Korelasyonu	Entropi	PSNR	SSIM	Şifreleme (sn)	Deşifreleme (sn)
AES	0.0775	7.9907	7.4340	0.0075	0.29242	0.29986
Kaotik AES	0.0417	7.9899	7.4915	0.0076	0.35711	0.36248
RC4	0.0338	7.9996	7.5151	0.0075	0.17223	0.17242
Kaotik RC4	0.0417	7.9899	7.4915	0.0076	0.31663	0.31626
Kaoitik RC4+RSA Hibrit Şifreleme	0.0313	7.9996	7.5097	0.0075	0.39400	0.39500

4.4. 765 × 603 Gri Görüntü Şifreleme Sonuçları

765×603 çözünürlüğündeki gri görüntülerde, histogram korelasyonunun en düşük değerleri RC4 ve Kaotik AES algoritmalarında elde edilmiştir. Özellikle RC4 algoritmasında negatif korelasyonun yüksek çözünürlükte de devam etmesi, tek kanallı verilerin rastgeleleştirilmesinde algoritmanın oldukça etkili olduğunu göstermektedir.

Entropi değerleri tüm algoritmalarda 7.999 seviyesine ulaşmış ve rastgelelik en üst düzeye taşınmıştır. PSNR değerleri yaklaşık 8 dB seviyesinde olup, şifreli görüntülerin orijinal görüntüden ciddi biçimde farklılaştığını göstermektedir. SSIM değerlerinin tüm algoritmalarda 0.008 civarında olması, yapısal bilginin tamamen yok edildiğini doğrulamaktadır.

İşlem süreleri açısından RC4, büyük gri görüntülerde de en hızlı yöntem olarak öne çıkarken (≈0.16 sn), hibrit RC4+RSA yöntemi en yüksek işlem süresine sahiptir. Kaotik RC4 yöntemi RC4'e kıyasla daha yavaş çalışsa da güvenlik metrikleri açısından oldukça başarılı sonuçlar üretmiştir. 765×603 çözünürlüğündeki gri seviyeli görüntüler üzerinde yapılan deneysel çalışmalar, algoritmaların tek kanal veriler üzerindeki davranışını ortaya koymaktadır. Bu kapsamda elde edilen performans ve güvenlik ölçütlerine ait karşılaştırmalı sonuçlar Tablo 6'da sunulmuştur.

Tablo 6. 765 x 603 Gri görüntü şifreleme performans tablosu

Algoritma Adı	Histogram Korelasyonu	Entropi	PSNR	SSIM	Şifreleme (sn)	Deşifreleme (sn)
AES	0.1469	7.9754	7.9674	0.0078	0.25686	0.26950
Kaotik AES	-0.0353	7.9732	8.0446	0.0079	0.35686	0.34543
RC4	-0.0772	7.9996	8.1089	0.0084	0.16764	0.16813
Kaotik RC4	0.0383	7.9996	8.1006	0.0083	0.30750	0.30808
Kaoitik RC4+RSA Hibrit Şifreleme	0.0043	7.9996	8.0876	0.0079	0.38100	0.38800

4.5. Genel Karşılaştırmalı Değerlendirme

Bu çalışmada gerçekleştirilen tüm performans ve güvenlik analizleri, literatürde yaygın olarak kullanılan standart test görüntüleri üzerinde yürütülmüştür. 512×512 boyutundaki deneyler Lena görüntüsü üzerinde, 765×603 çözünürlüğündeki deneyler ise Peppers görüntüsü üzerinde uygulanmıştır. Bu görüntülerin tercih edilme nedeni; yüksek detay seviyeleri, farklı kontrast dağılımları ve zengin renk içerikleri sayesinde şifreleme algoritmalarının hem istatistiksel güvenlik çıktılarının hem de performans metriklerinin karşılaştırılabilir biçimde analiz edilmesine olanak sağlamasıdır. Bu yaklaşım, geliştirilen yöntemin literatürdeki benzer çalışmalarla uyumlu biçimde değerlendirilebilirliğini artırmaktadır.

Tüm çözünürlüklerde ve her iki renk formatında elde edilen sonuçlar birlikte değerlendirildiğinde, geliştirilen kaotik RC4+RSA hibrit yönteminin, güvenlik açısından en güçlü şifreleme yapılarından biri olduğu açıkça görülmektedir. Özellikle entropi ve histogram korelasyon değerleri, hibrit yöntemin rastgelelik kapasitesinin oldukça yüksek olduğunu ve klasik AES ile RC4 gibi yöntemlere kıyasla daha güçlü bir güvenlik seviyesi sunduğunu göstermektedir. Histogram korelasyon değerlerinin sıfıra yakın olması, şifreli görüntü ile orijinal görüntü arasındaki ilişkinin neredeyse tamamen ortadan kalktığını ve şifrelemenin istatistiksel saldırılara karşı güçlü bir direnç sağladığını ortaya koymaktadır.

Entropi değerleri incelendiğinde, hibrit RC4+RSA ve kaotik RC4 yöntemlerinin tüm çözünürlüklerde en yüksek rastgelelik seviyelerine ulaştığı tespit edilmiştir. Bu durum, kaotik lojistik haritanın RC4 anahtar akışına entegre edilmesinin rastgelelik seviyesini önemli ölçüde artırdığını ve şifreli görüntülerin istatistiksel olarak tahmin edilmesini zorlaştırdığını göstermektedir.

Benzer şekilde, histogram korelasyonu açısından en düşük değerler kaotik RC4 ve hibrit RC4+RSA yöntemlerinde elde edilmiştir. AES ve kaotik AES algoritmaları da yüksek güvenlik sağlamakla birlikte, kaotik RC4 tabanlı yaklaşımlar piksel korelasyonunun daha etkin biçimde zayıflatılması bakımından daha başarılı sonuçlar sunmuştur.

PSNR değerleri, tüm algoritmalarda şifreli görüntü ile orijinal görüntü arasında belirgin bir fark olduğunu ve şifreleme işleminin görüntüyü güçlü biçimde bozduğunu göstermektedir. Düşük PSNR değerleri, şifreli görüntülerin orijinal görüntüye dair anlamlı herhangi bir bilgi

taşımadığını doğrulamaktadır. SSIM değerlerinin tüm testlerde oldukça düşük çıkması ise yapısal benzerliğin tamamen ortadan kalktığını ve algoritmaların görüntünün geometrik ve yapısal özelliklerini etkin biçimde bozduğunu göstermektedir.

Performans açısından değerlendirildiğinde, RC4 algoritması en hızlı yöntem olarak öne çıkmaktadır. RC4'ün basit anahtar akışı üretim yapısı sayesinde hem renkli hem de gri görüntülerde en düşük şifreleme ve deşifreleme sürelerine ulaştığı gözlemlenmiştir. AES, blok tabanlı yapısı nedeniyle RC4'e kıyasla daha yavaş çalışmaktadır. Kaotik yapıların algoritmalara eklenmesi işlem süresini belirli ölçüde artırmış; RSA kullanılarak anahtarın şifrelenmesiyle hibrit yöntemde işlem süresinin en yüksek seviyeye çıktığı görülmüştür.

Bununla birlikte, RSA'nın yalnızca anahtar şifreleme amacıyla kullanıldığı dikkate alındığında, hibrit yöntemin işlem maliyetindeki artışa rağmen anahtar güvenliği açısından en güçlü yaklaşımı sunduğu açıktır. Bu bağlamda geliştirilen hibrit mimari; askeri sistemler, kritik altyapılar, tıbbi görüntüleme ve dijital arşivleme gibi yüksek güvenlik gerektiren uygulama alanlarında tercih edilebilir, güvenilir ve etkili bir çözüm olarak değerlendirilmektedir.

5. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, görüntü güvenliğini artırmaya yönelik olarak geliştirilen kaotik sistemle güçlendirilmiş hibrit RC4+RSA algoritması, farklı çözünürlük ve görüntü türleri üzerinde kapsamlı biçimde test edilmiştir. Elde edilen deneysel bulgular literatürle ilişkilendirilmiş; sistemin güvenlik, performans ve ölçeklenebilirlik özellikleri çok yönlü olarak değerlendirilmiştir. Çalışmanın temel amacı, klasik şifreleme algoritmalarının (AES, RC4) tek başına sunamadığı yüksek rastgelelik, saldırı dayanıklılığı ve anahtar güvenliğini tek bir mimari içerisinde birleştiren hibrit bir yapı geliştirmektir. Bu doğrultuda önerilen kaotik RC4+RSA sistemi, kaotik haritaların başlangıç koşullarına duyarlı yapısından kaynaklanan yüksek rastgelelik üretme kapasitesi ile RSA'nın güçlü anahtar yönetim mekanizmasını bir araya getirerek literatürde sınırlı biçimde ele alınan bütüncül bir hibrit yaklaşım sunmaktadır**.**

Bu çalışma, literatürdeki benzer görüntü şifreleme yaklaşımlarından farklı olarak, RC4 algoritmasının hız avantajını kaotik sistemlerle güçlendirmiş ve bu yapıyı RSA tabanlı güvenli anahtar yönetimi ile bütünleştirerek hem güvenlik hem de performansı birlikte ele alan bütüncül bir hibrit mimari önermektedir. Literatürde genellikle kaotik sistemler veya hibrit şifreleme yapıları ayrı ayrı değerlendirilirken, bu tez kapsamında kaotik RC4 ve RSA algoritmaları tek bir çatı altında birleştirilmiş; önerilen yapı farklı çözünürlük ve görüntü türleri üzerinde deneysel olarak doğrulanmıştır. Bu yönüyle çalışma, yalnızca teorik değil, uygulamalı ve karşılaştırmalı analizlerle desteklenen özgün bir katkı sunmaktadır.

Çalışmadan elde edilen bulgular, literatürdeki pek çok araştırma ile uyum göstermektedir. Kaotik sistemlerin şifreleme algoritmalarına entegre edilmesinin rastgeleliği artırdığı, histogram dağılımını düzleştirdiği ve istatistiksel saldırıların etkisini azalttığı daha önceki çalışmalarda da vurgulanmıştır. Bu tez kapsamında özellikle kaotik RC4 ve hibrit RC4+RSA yöntemlerinde histogram korelasyon değerlerinin sıfıra ya da negatif değerlere oldukça yakın olduğu gözlemlenmiştir. Bu sonuç, şifreli görüntü ile orijinal görüntü arasında istatistiksel herhangi bir bağıntının kalmadığını ve saldırganın orijinal içerik hakkında anlamlı bir çıkarım yapmasının neredeyse imkânsız hâle geldiğini göstermektedir. Literatürde RC4 algoritmasının hız avantajına sahip olduğu ancak tek başına kullanıldığında yeterli güvenlik sunamadığı belirtilmektedir. Bu çalışmada RC4'ün kaotik sistemle güçlendirilmesiyle hem rastgelelik seviyesinin hem de histogram düzleşmesinin belirgin biçimde artması, kaotik yapıların RC4 için etkili bir güvenlik güçlendirici olduğunu açıkça ortaya koymuştur.

Diferansiyel saldırılara karşı dayanıklılığı değerlendirmek amacıyla gerçekleştirilen NPCR ve UACI analizlerinde, orijinal görüntüde yalnızca tek bir pikselin bir biti değiştirilmiş ve her iki görüntü aynı anahtar ve kaotik parametreler kullanılarak ayrı ayrı şifrelenmiştir. Elde edilen sonuçlarda NPCR değerinin %99.60, UACI değerinin ise %33.42 seviyesinde olduğu belirlenmiştir. Bu değerler, literatürde diferansiyel saldırılara karşı güçlü kabul edilen eşiklerle uyumludur ve önerilen kaotik RC4 tabanlı hibrit yapının yüksek difüzyon özelliği sergilediğini açıkça göstermektedir.

Entropi analizleri incelendiğinde, kaotik RC4 ve hibrit RC4+RSA yöntemlerinin teorik maksimum değer olan 8'e en yakın sonuçları ürettiği görülmüştür. Literatürde 7.5 üzerindeki entropi değerleri yüksek güvenlik göstergesi olarak kabul edilirken, bu çalışmada elde edilen 7.97–7.999 aralığındaki sonuçlar hem renkli hem de gri görüntülerde güçlü bir rastgelelik üretildiğini doğrulamaktadır. Özellikle hibrit RC4+RSA yapısında kaotik lojistik harita ile desteklenen RC4 anahtar akışının piksel dağılımını tamamen homojen hâle getirdiği tespit edilmiştir.

Yapısal benzerliği ölçen SSIM değerlerinin 0.007–0.01 aralığında olması, şifreli görüntülerin orijinal görüntüyle herhangi bir yapısal benzerlik taşımadığını göstermektedir. Literatürde güçlü görüntü şifreleme sistemlerinde SSIM değerlerinin 0.01'in altında olması hedeflenirken, bu çalışmada tüm yöntemlerin bu eşiği sağlaması şifreleme başarımının yüksek olduğunu kanıtlamaktadır. PSNR değerlerinin 7–9 dB aralığında elde edilmesi de şifreli görüntülerin orijinal görüntüden ciddi biçimde ayrıştığını ve şifreli veriden görsel bilginin geri kazanılamadığını göstermektedir.

Performans değerlendirmeleri, RC4 algoritmasının tüm senaryolarda en hızlı yöntem olduğunu ortaya koymuştur. Bu sonuç literatürle tamamen uyumludur; RC4 düşük hesaplama maliyeti sayesinde gerçek zamanlı uygulamalarda avantaj sağlamaktadır. Kaotik RC4 yönteminde işlem süresi bir miktar artmış olsa da bu artış, sağlanan güvenlik kazanımı dikkate alındığında kabul edilebilir düzeydedir. AES ve kaotik AES yöntemleri blok tabanlı yapıları nedeniyle RC4'e kıyasla daha yavaş çalışmıştır. Hibrit RC4+RSA yönteminin en yavaş yöntem olmasının temel nedeni RSA'nın anahtar üretim ve çözme aşamalarındaki yüksek matematiksel işlem maliyetidir. Buna karşın hibrit yapı, anahtar güvenliği açısından en güçlü yaklaşımı sunmaktadır.

Çalışmanın önemli katkılarından biri, farklı çözünürlük ve formatlarda yapılan testlerle yöntemlerin ölçeklenebilirliğinin ortaya konmuş olmasıdır. 512×512 ve 765×603 çözünürlüklerde elde edilen sonuçlar, çözünürlük arttıkça güvenlik ve performans metriklerinin genel eğilimlerinin korunduğunu göstermiştir. Bu durum, önerilen hibrit modelin farklı boyut ve türdeki görüntülerde kararlı ve güvenilir sonuçlar üretebildiğini ortaya koymaktadır.

Genel değerlendirme sonucunda; kaotik RC4 ve hibrit RC4+RSA yöntemleri güvenlik açısından en güçlü sonuçları üretmiş, RC4 ise performans açısından öne çıkmıştır. Bu durum, güvenlik–performans dengesinin uygulama alanına göre değiştirilebileceğini göstermektedir. Gerçek zamanlı görüntü iletimi, gömülü sistemler ve yüksek hız gerektiren uygulamalar için RC4 ve kaotik RC4 yöntemleri uygunken; askeri sistemler, kritik altyapılar ve tıbbi görüntüleme gibi yüksek güvenlik gerektiren alanlarda hibrit RC4+RSA yaklaşımı daha uygun bir çözüm sunmaktadır.

Gelecek çalışmalarda, Tent, Henon, Ikeda, Sine gibi farklı kaotik haritaların entegrasyonu, rastgelelik performansını daha da artırabilir. Ayrıca DNA tabanlı kodlama, piksel permütasyonu, blok tabanlı kaotik karıştırma gibi ileri seviye tekniklerin hibrit modele eklenmesi güvenlik seviyesini daha da yükseltebilir. RSA yerine Eliptik Eğri Kriptografisi (ECC) gibi daha hızlı anahtar yönetim algoritmalarının kullanılması performans açısından önemli bir iyileştirme sağlayabilir. Video akışlarının gerçek zamanlı kaotik hibrit yöntemlerle şifrelenmesi de gelecek çalışmalar için önemli bir araştırma alanı sunmaktadır.

Sonuç olarak bu tez çalışması, kaotik tabanlı hibrit şifreleme yaklaşımlarının görüntü güvenliği alanında son derece etkili olduğunu ortaya koymuş; geliştirilen RC4+RSA hibrit modeli ile yüksek güvenlik ve güçlü rastgelelik bir arada sağlanmıştır. Elde edilen sonuçların hem akademik literatüre katkı sunacağı hem de pratik uygulamalarda güvenli görüntü iletimi için yol gösterici olacağı değerlendirilmektedir.

KAYNAKÇA

Alghamdi, Y., & Munir, A. (2024). Image encryption algorithms: A survey of design and evaluation metrics. Journal of Cybersecurity and Privacy, 4(1), 126–152.

Alkady, Y., Habib, M. I., & Rizk, R. Y. (2013, December). A new security protocol using hybrid cryptography algorithms. In 2013 9th International Computer Engineering Conference (ICENCO) (pp. 109–115). IEEE.

Al-Maadeed, S., Al-Ali, A., & Abdalla, T. (2012). A new chaos-based image-encryption and compression algorithm. Journal of Electrical and Computer Engineering, 2012, 179693.

Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. Journal of Supercomputing, 75(10).

Benaissi, S., Chikouche, N., & Hamza, R. (2023). A novel image encryption algorithm based on hybrid chaotic maps using a key image. Optik, 272, 170316.

Bermani, A. K., Murshedi, T. A. K., & Abod, Z. A. (2021). A hybrid cryptography technique for data storage on cloud computing. Journal of Discrete Mathematical Sciences & Cryptography, 24(6), 1613–1624.

Ceyhan, M., & Yolaçan, E. N. (2021). Görüntü dosyalarının şifrelenerek güvenli şekilde saklanması. Eskişehir Osmangazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 29(1), 28–42.

Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749–761.

Chen, S. H., & Chou, C. (1999). Development of Chinese Internet addiction scale in Taiwan. Poster session presented at the 107th American Psychology Annual Convention, Boston, USA.

Christensen, C. (2010). Review of cryptography and network security: Principles and practice. Cryptologia, 35(1), 97–99.

Daemen, J., & Rijmen, V. (2002). The design of Rijndael. Springer-Verlag.

El-Latif, A. A. Abd, et al. (2022). A novel chaos-based cryptography algorithm and its performance analysis. Mathematics, 10(14), 2434.

Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT healthcare systems. IEEE Access, 6, 20596–20608.

Fang, J., Zhao, K., & Liang, W. (2023). A novel color image encryption scheme using elliptic curve cryptography and hyperchaotic system. Physica Scripta, 98(11), 115257.

Hakim, A. R., Budiman, M. A., & Nasution, M. K. M. (2024). Hybrid cryptosystem enhanced RSA and RC4 chaotic map: A tutorial. AIP Conference Proceedings, 3222(1), 030005.

Hamadi, S. J., & Mohammed, E. A. (2025). Chaotic systems in cryptography: An overview of feature-based methods. Al-Salam Journal for Engineering and Technology, 4(1), 164–172.

Katz, J., & Lindell, Y. (2020). Introduction to modern cryptography (3rd ed.). Chapman & Hall/CRC.

Kaur, M., & Kumar, V. (2020). A comprehensive review on image encryption techniques. Archives of Computational Methods in Engineering, 27(1).

Khalaf, A. M., & Lakhtaria, K. (2023). Enhancing hybrid system based mixing AES and RSA cryptography algorithms. Journal of Natural and Applied Sciences URAL, 3(2).

Kocarev, L. (2002). Chaos-based cryptography: A brief overview. IEEE Circuits and Systems Magazine, 1(3), 6–21.

Kumari, M., Gupta, S., & Sardana, P. (2017). A study on image encryption algorithms. 3D Research, 8, 37.

Lan, R., He, J., Wang, S., Gu, T., & Luo, X. (2018). Integrated chaotic systems for image encryption. Signal Processing, 147, 133–145.

Liu, J. J., Tsang, K. T., & Deng, Y. H. (2022). A variant RSA acceleration with parallelisation. International Journal of Parallel, Emergent and Distributed Systems, 37(3), 318–332.

Luo, Y., Yu, J., Lai, W., & Liu, L. (2019). A chaotic image encryption algorithm based on improved Baker and logistic maps. Multimedia Tools and Applications, 78(15), 22023–22043.

Malik, A., Gupta, S., & Dhall, S. (2020). Analysis of traditional and modern image encryption algorithms under realistic ambience. Multimedia Tools and Applications, 79(37), 27941–27993.

Mironov, I. (2002). (Not so) random shuffles of RC4. In Annual International Cryptology Conference (pp. 304–319). Springer.

Mousa, A., & Hamad, A. (2006). Evaluation of the RC4 algorithm for data encryption. International Journal of Computer Science Applications, 3(2), 44–56.

Nagar, A., Nandakumar, K., & Jain, A. K. (2008). Securing fingerprint templates: Fuzzy vault with minutiae descriptors. 19th International Conference on Pattern Recognition, 1–4.

NIST. (2017). An introduction to information security (NIST SP 800-12 Rev.1). National Institute of Standards and Technology.

Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926–934.

Paar, C., & Pelzl, J. (2009). Understanding cryptography. Springer.

Rashid, F. B., Rankothge, W., Sadeghi, S., Mohammadian, H., & Ghorbani, A. (2024). Privacy-preserving for images in satellite communications: A review. arXiv:2410.21177.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126.

SaberiKamarposhti, M., Ghorbani, A., & Yadollahi, M. (2024). A comprehensive survey on image encryption. Chaos, Solitons & Fractals, 178, 114361.

Şahin, D. (2024). AES tabanlı parametrik resim şifreleme Java uygulaması (Yayımlanmamış yüksek lisans tezi). İstanbul Gelişim Üniversitesi.

Shah, M., & Gor, A. (2025). Comprehensive survey of symmetric and public-key cryptographic algorithms. International Journal of Informative Research, 12(10).

Singh, G., & Supriya. (2013). A study of encryption algorithms (RSA, DES, 3DES & AES). International Journal of Computer Applications, 67, 33–38.

Singhal, N., & Raina, J. P. S. (2011). Comparative analysis of AES and RC4 algorithms. International Journal of Computer Trends and Technology, 2(6), 177–181.

Subedar, Z., & Araballi, A. (2020). Hybrid cryptography: Performance analysis of various cryptographic combinations. International Journal of Mathematical Sciences and Computing, 6(4), 35–41.

Umar, T., Nadeem, M., & Anwer, F. (2024). Modified skew tent map PRNG. Computer Standards & Interfaces, 89, 103826.

Wang, M., Wang, X., Zhang, Y., & Gao, Z. (2018). Chaotic encryption based on image segmentation. Optics & Laser Technology, 108, 558–573.

Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A review of homomorphic encryption for biometrics. Sensors, 23(7), 3566.

Yogi, B., & Khan, A. K. (2025). Advancements in image encryption. Computer Science Review, 57, 100759.

Yüksel, T., & Özgün, B. (2021). RSA ve RC4 algoritmalarının performans karşılaştırması. AURUM Journal of Engineering Systems and Architecture, 5(1), 29–40.

Zhang, H., Wang, X., Xie, H., Wang, C., & Wang, X. (2020). Secure image encryption with non-adjacent coupled maps. IEEE Access, 8, 122104–122120.

Zhang, L., Song, X., El-Latif, A. A. A., Zhao, Y., & Abd-El-Atty, B. (2024). Selective medical image encryption using chaotic maps. Complex & Intelligent Systems, 10(2), 2187–2213.

Zhang, Y., Xiao, D., & Wang, X. (2020). A survey on image encryption techniques based on chaotic systems. IEEE Access, 8, 182176–182201.

Zhao, L., Zhao, L., Cui, F., & Sun, T. (2024). Satellite image encryption based on RNA and 7D chaotic system. The Visual Computer, 40(8), 5659–5679.

Pearson, K. (1895). Notes on Regression and Inheritance in the Case of Two Parents Proceedings of the Royal Society of London.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal*, *27*(3), 379-423.

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, *1*(2), 31-38.