İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Araştırma Makalesi / Research Article

KAOTİK HARİTA TABANLI ÇOK KATMANLI GÖRÜNTÜ STEGANOGRAFİSİ İLE HASSAS VERİLERİN GİZLENMESİ VE KORUNMASI

HIDING AND PROTECTING SENSITIVE DATA WITH CHAOTIC MAP-BASED MULTILAYER IMAGE STEGANOGRAPHY

Sevgül TOKATLIOĞLU[1] **Erdal GÜVENOĞLU**[2]

https://doi.org/10.55071/ticaretfbd.1705157

Sorumlu Yazar (Corresponding Author)	*Geliş Tarihi (Received)*	*Revizyon Tarihi (Revised)*	*Kabul Tarihi (Accepted)*
erdalguvenoglu@maltepe.edu.tr	*11.06.2025*	*19.08.2025*	*02.09.2025*

Öz

Son yıllarda internet ve mobil cihazlar üzerinden veri paylaşımının artmasıyla birlikte bilgi güvenliği sorunları da önemli ölçüde artmıştır. Bu bağlamda, verilerin yetkisiz erişimden korunması amacıyla steganografi ve kriptografi gibi yöntemler üzerine yoğun araştırmalar yapılmaktadır. Bu çalışma, geleneksel En Düşük Bite Ekleme (LSB) steganografi yönteminin güvenlik açıklarını gidermek amacıyla Kaotik Çadır Haritası (CTM) ve SHA-256 hash algoritmasını kullanan yeni bir veri gizleme tekniği sunmaktadır. Önerilen yöntemde, gizli anahtar SHA-256 ile işlenmekte, mesaj uzunluğu bu hash değeri içerisine gizlenmektedir. CTM kullanılarak hem verinin gömüleceği piksel konumları rastgele bir şekilde belirlenmekte hem de gizlenecek veri kaotik dizi ile XOR işlemine tabi tutularak şifrelenmektedir. Yöntemin performansı, standart test görüntüleri üzerinde histogram analizi, entropi, korelasyon, SSIM, PSNR, MSE, NPCR, UACI ve NIST gibi çeşitli güvenlik ve kalite metrikleri kullanılarak değerlendirilmiştir. Deneysel sonuçlar, yöntemin veri gizlenmiş görüntünün görsel kalitesini ve algılanamazlığını üst düzeyde koruduğunu göstermektedir. Ortalama 70.6318 dB PSNR, 0.99997 SSIM ve 0.075 MSE değerleri, görsel bozulmanın minimum seviyede olduğunu kanıtlamaktadır. Benzer şekilde, orijinal ve veri gizlenmiş görüntüler arasındaki düşük diferansiyel değişim oranları olan NPCR değerinin ortalama 0.0054 ve UACI değerinin ortalama $2{,}2348 \times 10^{-5}$ olmasıda bu durumu desteklemektedir. Yöntemin güvenliği ise, orijinal ve veri gizlenmiş görüntülerin birbirine çok yakın entropi ve korelasyon değerleri sergilemesi ve tüm NIST istatistiksel testlerinden başarıyla geçmesiyle teyit edilmiştir. Bu bulgular, yöntemin steganaliz saldırılarına karşı dirençli olduğunu göstermektedir.

Anahtar Kelimeler: Kaotik haritalar, veri gizleme, steganografi, veri güvenliği.

Abstract

In recent years, with the increase in data sharing over the internet and mobile devices, information security problems have also increased significantly. In this context, intensive research is being conducted on methods such as steganography and cryptography to protect data from unauthorized access. This study proposes a new data hiding technique using the Chaotic Tent Map (CTM) and the SHA-256 hash algorithm to address the security vulnerabilities of the traditional Least Bit Addition (LSB) steganography method. In the proposed method, the secret key is processed with SHA-256, and the message length is hidden within this hash value. Using CTM, the pixel locations where the data will be embedded are randomly determined, and the hidden data is encrypted by subjecting it to the XOR operation with a chaotic array. The performance of the method is evaluated using various security and quality metrics, such as histogram analysis, entropy, correlation, SSIM, PSNR, MSE, NPCR, UACI, and NIST, on standard test images. Experimental results demonstrate that the method maintains a high level of visual quality and imperceptibility of the hidden image. Average PSNR of 70.6318 dB, SSIM of 0.99997, and MSE of 0.075 demonstrate minimal visual degradation. Similarly, the low differential change rates between the original and data-hidden images, with an average NPCR value of 0.0054 and an average UACI value of $2{,}2348 \times 10^{-5}$, support this finding. The security of the method is confirmed by the very similar entropy and correlation values of the original and data-hidden images, and by successfully passing all NIST statistical tests. These findings demonstrate the method's resistance to steganalysis attacks.

Keywords: Chaotic maps, data hiding, steganography, data security.

[*] *Bu yayın Sevgül Tokatlıoğlu isimli öğrencinin İstanbul Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Tezli Yüksek Lisans Programındaki Yüksek Lisans tezinden üretilmiştir.*

[1] Maltepe Üniversitesi, Lisanüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul, Türkiye. sevgul.tokatlioglu1968@gmail.com.

[2] Maltepe Üniversitesi, Meslek Yüksekokulu, Bilgisayar Programcılığı Programı, İstanbul, Türkiye. erdalguvenoglu@maltepe.edu.tr.

1. GİRİŞ

Son 20-30 yılda internet kullanımı önemli ölçüde artmıştır. Bununla birlikte, bilginin çeşitli yollarla paylaşılması, özellikle mobil cihazların çok yaygın olması ve bu cihazlar aracılığıyla resim, ses ve metin göndermenin son derece kolay olması nedeniyle, bilgi güvenliği sorunları da önemli ölçüde artış göstermiştir. Günümüzde bilgi güvenliğini sağlamak ve verilerin yetkisiz erişimden korunmasını temin etmek amacıyla farklı teknikler geliştirilmektedir. Bu bağlamda, veri iletiminde güvenliği artırmak için steganografi ve kriptografi gibi yöntemler üzerine yoğun araştırmalar yapılmaktadır.

Steganografi, veri gizleme tekniklerinden en popüleri ve en yaygınıdır. Eski Yunanca'da "steganografi" terimi gizli, örtülü yazı olarak ifade edilmektedir (Dalal & Juneja, 2021b). Başka bir deyişle, bir tür kapsüllemede denebilecek bilgiler örtülerek gizlenmekte ve bu şekilde iletilmektedir. Steganografinin temel amacı iletişimi gizli tutmaktır. Böylece gönderilen mesajın başlangıç noktası ile hedef arasında gizlenmiş verinin anlaşılmadan iletilmesini sağlanmaktadır. Verinin günümüzde üçüncü kişilerin eline geçmesini engellemenin bir yolu verinin şifrelenmesidir. Şifrelemenin temel amacı verileri güvende tutmaktır. Bu çerçevede ileri düzeyde etkili ve güvenli bir iletişimi sağlamak için steganografi ve kriptografi disiplinleri bir arada kullanılabilmektedir (Dalal & Juneja, 2021a). Kriptografide verinin şifrelendiği açıktır ve yalnızca yetkili kişiler tarafından çözülebilirken, steganografide veri gizlenir ve üçüncü taraflar onun varlığından habersizdir. Bu nedenle, kriptografi güvenliği ve steganografi ise gizliliği sağlamaktadır. Dijital medyanın hızla çeşitlenmesi ve yaygınlaşmasına paralel olarak steganografik yöntemlerin uygulama alanları da genişlemiştir. Görüntü, ses, video, metin vb. farklı dosya türlerinin artan kullanımı ve bu ortamlarda veri gizleme potansiyelinin fark edilmesi, steganografik tekniklerin çeşitlenmesine ve her bir taşıyıcı ortama özgü yöntemlerin geliştirilmesine zemin hazırlamıştır. Bu gelişmeler sonucunda steganografi, temel olarak verinin gizlendiği taşıyıcı ortamın türüne göre görüntü, ses ve metin steganografisi gibi ana kategorilere ayrılmıştır. Her bir kategori, gizlenen verinin algılanamazlığını ve taşıyıcı dosyanın bütünlüğünü koruma hedefine yönelik özgün yaklaşımlar ve algoritmalar içermektedir.

Bu çalışmada, geleneksel LSB yönteminin güvenlik açıklarını gidermek amacıyla kaotik haritaların rastgelelik ve deterministik kaos özelliklerinden faydalanılarak geliştirilmiş yeni bir veri gizleme tekniği sunulmaktadır. Kaotik sistemlerin öngörülemez ve duyarlı doğası, verinin piksellere dağıtılmasını daha düzensiz hale getirerek steganaliz saldırılarına karşı dayanıklılığı artırmaktadır. Önerilen yöntem, mevcut kaotik steganografi literatürüne aşağıdaki temel katkıları sunarak benzer yaklaşımlardan ayrılmaktadır.

- Literatürdeki birçok yaklaşım, yüksek hesaplama maliyeti gerektiren çok boyutlu, hibrit veya bağlantılı kaotik sistemler kullanırken önerilen yöntem tek boyutlu ve verimli bir harita olan Kaotik Çadır Haritası'nı (CTM) temel almaktadır. Bu sayede, aşırı karmaşıklıktan kaçınarak hem uygulama kolaylığı sağlanmış hem de yüksek güvenlik performansı korunmuştur.
- Yöntem, tek bir güvenlik mekanizmasına dayanmak yerine gizli anahtarın kriptografik hash fonksiyonu (SHA-256) ile işlenmesi, mesaj konumlarının CTM ile kaotik olarak belirlenmesi ve gizlenecek verinin yine CTM dizisiyle XOR işlemine tabi tutularak şifrelenmesi gibi üçlü bir koruma yapısı

sunmaktadır. Bu bütünleşik yapı, sadece konumları rastgele hale getirmekle kalmamakta aynı zamanda mesaj içeriğini de koruyarak sistemi daha dayanıklı kılmaktadır.

- Geleneksel LSB ve bazı temel kaotik uygulamalar, veriyi öngörülebilir veya basit desenlerle gizleyerek istatistiksel analizlere karşı zayıf kalabilmektedir. Önerilen yöntem, piksel seçimini tamamen anahtara bağlı kaotik bir yörüngeye devrederek veri gizleme izlerini kapak görüntüye homojen bir şekilde dağıtmaktadır. Bu sayede, histogram tabanlı steganaliz saldırılarına karşı belirgin bir üstünlük sağlamaktadır.
- Literatürdeki bazı karmaşık yöntemler güvenliği artırırken görsel kaliteyi düşürme veya hesaplama yükünü artırma eğilimindedir. Bu çalışmada sunulan basit ve etkili mimari sayesinde hem çok yüksek görsel kalite metriklerine ulaşılmakta hem de NIST gibi standart testleri geçerek istatistiksel olarak güvenli olduğunu da kanıtlamaktadır. Bununla birlikte, yöntemin pratik olarak uygulanabilirliğini önemli ölçüde artırmaktadır.

2. LİTERATÜR ARAŞTIRMASI

Steganografi, gizli verilerin görsel veya sesli medyada saklanmasını sağlayan önemli bir alandır. Bu alanda yapılan çalışmalar, yeni yöntemler, teknolojiler ve güvenlik önlemleri ile sürekli olarak evrilmektedir. Bu çalışmaların başında kaotik sistemler gelmektedir. Kaotik sistemler, deterministik ancak hassas başlangıç koşullarına dayalı, tahmin edilemez bir davranış sergileyen matematiksel modellerdir. Bu sistemler, özellikle steganografi ve kriptografi gibi alanlarda güvenli veri gizleme ve şifreleme tekniklerinin geliştirilmesinde önemli bir rol oynamaktadır. Kaotik sistemlerin, özellikle rastgelelik ve düzensizlik özellikleri, verilerin güvenliğini artırmak ve gizliliğini sağlamak için kullanılmaktadır. Aşağıda, farklı yöntemleri içeren çalışmaların bir derlemesi sunulmaktadır.

Son yıllarda, steganografi alanında birçok yenilikçi yaklaşım geliştirilmiştir. Bu yaklaşımlardan en yaygın kullanılan teknik LSB tekniğidir. (Khalil ve ark., 2024) tarafından LSB tekniği ve 2D kaotik haritalar tabanlı bir görüntü steganografisi yöntemi önermiştir. Bu çalışmada, kaotik haritalar kullanılarak veri gizleme süreci karmaşık hale getirilmiştir. Bu durum saldırganların verileri tespit etmesini zorlaştırmaktadır. Kaotik harita tabanlı pek çok steganografi tekniği bulunmaktadır. Kaotik haritalar tabanlı görüntü güvenlik teknikleri üzerine sistematik bir literatür taraması (Singh ve ark., 2024) tarafından yapılmıştır. Çalışmada mevcut yöntemlerin etkinliği ve eksikleri vurgulanarak literatüre önemli katkılar sağlamışlardır. Bu tarama, kaotik haritalar kullanılarak geliştirilen yöntemlerin gereksinimlerini belirlemiş ve yönlendirme sağlamıştır. Benzer bir literatür araştırması (Al-Sulami & Hashim, 2021) tarafından yapılmıştır. Çalışmada çevrimiçi çoklu medya verilerini korumak amacıyla kaotik haritalar ve steganografi teknikleri üzerine kapsamlı bir inceleme yapılarak bu alanda önemli bir literatür kaynağı oluşturulmuştur. Kaotik haritalar ve steganografi farklı pek çok bilim analında kullanılmaktadır. (Zhang ve ark., 2024), tıbbi görüntüler için birleştirilmiş kaotik haritalar (CCM, Coupled Chaotic Maps) ve steganografi tabanında geri dönüşümlü seçici şifreleme (RSE, Reversibly selective encryption) yöntemini geliştirmiştir. Bu yöntem, tıbbi verilerin güvenliğini artırarak sağlık alanında veri transferinin korunmasına yönelik bir çözüm sunmaktadır. RSE, kullanıcıların yalnızca gerekli olduğunda verileri çözmesine olanak tanıyarak veri güvenliğini

pekiştirmiştir. Tıp alanında bir başka bir çalışma (Karawia, 2021) tarafından yapılmıştır. Çalışmada modifiye edilmiş LSB yöntemi ve kaotik harita kullanarak tıbbi görüntüler için bir steganografik algoritma önermiştir. Bu yöntem tıbbi verilerin korunması amacıyla geliştirilmiştir. (Yakut, 2024) ise kaotik haritalar ve XOR işlemleri kullanarak verileri gizlemek için geliştirdiği yöntemle, veri gizleme alanında yeni bir yaklaşım önermiş ve bu yöntemle %95'e kadar veri gizlilik oranı elde etmiştir. (Yamni ve ark., 2024), adaptif bir dinamik kaotik sistem kullanarak renkli görüntü steganografisi tekniği geliştirmişlerdir. Yöntemde şifreleme ve veri gizleme sonrasında elde edilen görüntü kalitesinin korunması hedeflenmiştir. Ancak her ne kadar kalitenin korunması hedeflenmiş olsa da piksel değişimlerinden dolayı bozulmalar meydana gelebilecektir. (Salim ve ark., 2024) Lorenz kaotik sistemi ve bloom filtresi tabanlı bir teknik geliştirerek, veri güvenliğini artırmayı hedefleyen bir yöntem önermişlerdir. Önerilen yöntemle, verilerin şifrelenmesi ve izlenebilirliğinin azaltılması amacıyla bir şifreleme mekanizması sunulmuştur. (Aparna & Madhumitha, 2023), çoklu kaotik haritaları kullanarak görüntü şifreleme ve steganografiyi birleştiren yeni bir teknik önermektedir. Amaç, hem güvenliği artırmak hem de verinin gizliliğini korumaktır. Birden fazla kaotik harita (Logistic Map, Henon Map, Tent Map) kullanılarak rastgele anahtarlar üretilmektedir. Bu kaotik haritalar, hem görüntü şifreleme hem de steganografi sürecinde farklı aşamalarda uygulanmaktadır. (Ramzan & Khan, 2023), lineer kesirli dönüşüm ve kaotik haritalarla oluşturulan steganografik algoritmalarının belirginlik ve kapasite sağlama açısından önemli başarılar elde ettiğini belirtmiştir. Diğer bir ifade ile kaotik haritaların steganografi ve şifreleme de önemli bir yer sahip olduğunu vurgulamıştır. (Elshoush & Mahmoud, 2023), parçalı lineer kaotik harita (piecewise linear chaotic map) ile LSB tekniğini birleştirerek, %98'e varan kaplama kapasitesi ve güvenlik sunan bir sistem geliştirmiştir. (Nagarajegowda & Krishnan, 2023) geliştirilmiş hiper-kaotik Henon haritası ve fraktal tromino kullanarak bir görüntü steganografisi yöntemi önermişlerdir. Amaç, veri gizleme sürecinin güvenliğini artırmak ve stego-görüntünün tespit edilmesini zorlaştırmaktır. Tromino bölme tekniği, görüntüyü L şeklindeki fraktal bloklara ayırarak veri gömmek için kullanılmaktadır. Fraktal bölme yöntemleri, geleneksel steganografi tekniklerine kıyasla daha fazla işlem gücü gerektirmektedir. (Hematpour ve ark., 2022), CCM ve yeni bir kaotik S-box ile bir steganografik algoritma geliştirerek, verilerin gizlenmesi amacıyla kullanmıştır. Amaç, gizli veriyi yüksek güvenlikli bir şekilde taşıyıcı görüntüye gömmek ve stego-görüntüdeki bozulmayı en aza indirerek algılanabilirliğini zorlaştırmaktır. (Abd & Hussein, 2022) ise duffing kaotik haritası ve steganografi ile güvenli çok seviyeli bir iletişim sistemi tasarlamıştır. Sistem, veri iletimi sırasında güvenliği artırmak için kaotik sistemlerin dinamiklerinden faydalanmakta ve aynı zamanda steganografi ile verinin gizliliğini korumaktadır. (Sharafi ve ark., 2021), hibrit kaotik harita ve ayrık dönüşümler (discrete transforms) kullanarak geliştirilen bir görüntü steganografi yöntemi önermektedir. Amaç, gizli veriyi güvenli ve düşük algılanabilirlik ile saklamak, aynı zamanda görsel kaliteyi koruyarak saldırılara karşı dirençli bir sistem oluşturmaktır. (Hameed ve ark., 2021), 3D Cat Haritası kullanan kaos tabanlı renkli görüntü steganografisi ile bir veri koruma yöntemi geliştirmiştir. 3D Cat Map, kaotik bir sistem olup, görüntü piksellerini rastgele dağıtarak şifreleme ve veri gizleme işlemlerini gerçekleştiren bir dönüşümdür. Taşıyıcı görüntüye 3D Cat Map dönüşümü uygulanarak piksellerin kaotik olarak dağıtılması ile verilerin gizlenmesi sağlanmıştır. (Liu ve ark., 2022), yüksek boyutlu kaotik haritalar ve steganografi ile görüntü şifreleme algoritmaları geliştirmiştir. Bu da verilerin güvenliği

açısından steganografi ve kaotik haritaların bu alanda önemli bir yere sahip olduğunu göstermiştir.

Steganografi sadece görüntü alanında değil farklı ortam ve multimedyalarda da kullanılmaktadır. Farklı kaotik haritaların kullanımıyla görüntü şifrelemesi ile desteklenen bir ses steganografisi tekniği (Nasr ve ark., 2024) tarafından geliştirmiştir. Bu teknik, ses verilerinin güvenliğini artırarak, sesli iletişimdeki hassas bilgilerin korunmasını önemli ölçüde iyileştirmiştir. Çalışmada, ses verilerinin güvenliğini artırmak için kaotik harita tabanlı şifreleme yöntemleri ve görüntü şifreleme yaklaşımları bir arada kullanılmıştır. (Khaleel & Abduljaleel, 2021), ses sinyalinde gizli mesajları korumak için steganografi ve şifreleme tekniklerini kullanarak, verilerin güvenliğini sağlamıştır. (Huo ve ark., 2024) ise kaotik haritalama ve üretici karşıt ağlar (GAN, Generative Adversarial Networks) kullanarak bir görüntü steganografisi ağı geliştirmiştir. Bu yaklaşım, görüntülerde veri saklama kapasitesini ve güvenliğini artırarak, doküman güvenliğini arttırmayı hedeflemiştir. (Bhandari ve ark., 2022), üçgen kaotik harita ile karınca kolonisi optimizasyonunun birleşimiyle bir görüntü steganografi yöntemi önermiştir. Karınca kolonisi optimizasyonu, yol bulma algoritmalarından ilham alınarak, taşıyıcı görüntüde veri gömme işlemini optimize etmek için kullanılmıştır. (Durafe & Patidar, 2024), fraktal kaplama (fractal cover) ve karma-chaos-DNA tabanlı şifreleme kombinasyonunu kullanarak görüntü steganografisi için bir yöntem önermektedir. Fraktal kaplama, gizlenecek verinin karmaşık ancak kendini tekrarlayan fraktal desenler kullanılarak gömülmesini sağlamaktadır. İlk olarak, veriler kaotik haritalar ve DNA kodlamasıyla şifrelenmekte ve ardından fraktal kaplama ile görüntüye gömülmektedir. (Alabaichi & Altameemi, 2022), DNA kodlama ve kaotik haritaları kullanarak video rasterlerinde gizli mesajları şifreleyen bir steganografi yöntemi önermektedir. Yöntemin amacı, yüksek güvenlikli veri gizleme sağlayarak gizli mesajların tespit edilmesini zorlaştırmaktır. Gizli mesajlar, DNA kodlaması kullanılarak şifrelenmekte ve ardından steganografi ile verilerin gizlenmesi sağlanmaktadır. (Vivek & Gadgay, 2021), Yüksek Verimli Video Kodlama (HEVC - High Efficiency Video Coding) ve Kaotik Şifreleme Algoritmalarını birleştirerek video steganografi yöntemi geliştirilmiştir. HEVC, modern video sıkıştırma teknolojisi olarak veri boyutunu küçültüp kaliteyi korurken, kaotik şifreleme algoritması gizli verinin güvenliğini artırarak steganaliz saldırılarına karşı koruma sağlamaktadır. (Rostam ve ark., 2022) steganografi ve kaotik haritalar ile IoT cihazlarında (internet of things) gizlilik koruma yöntemlerine odaklanmış, böylece IoT cihazları için güvenliği artıran teknikler geliştirmiştir. Bu teknik, IoT sistemlerinin gizliliğini artırmayı hedeflemektedir. (Kustov & Krasnov, 2021), steganografi problemlerinde gürültü altına gizlenmiş mesajları maskeleme tekniklerini ele almaktadır. Günümüzde steganografi, dijital ortamda gizli mesajları tespit edilmeden iletmek için sıkça kullanılmaktadır. Ancak, saldırganlar tarafından yapılan analizler (steganaliz teknikleri), gizli verileri tespit edebilmektedir. Çalışmada, gürültü temelli maskeleme teknikleri kullanılarak gizli mesajların tespit edilmesini zorlaştıran yöntemler incelenmektedir. Literatür çalışmalarında kullanılan yöntemler ve dezavantajları Tablo 1' de özetlenmiştir.

Tablo 1. Literatür Çalışmalarının Özeti

Yayın	**Kullanılan Yöntemler**	**Dezavantajlar**
(Khalil ve ark., 2024)	LSB Tekniği, 2D Kaotik Haritalar	LSB yönteminin zayıflıkları, yüksek görünürlük riski vardır.
(Nasr ve ark., 2024)	Kaotik Haritalar, Görüntü Şifrelemesi	Uygulamanın karmaşıklığı, performansı etkileyebilir.
(Singh ve ark., 2024)	Literatür Taraması	Yenilikçi bir yaklaşım bulunmamaktadır.
(Huo ve ark., 2024)	Kaotik Haritalar, Üretici Karşıt Ağlar (GAN)	Eğitim süresi ve hesaplama maliyeti yüksektir.
(Zhang ve ark., 2024)	Bağlantılı Kaotik Haritalar, Steganografi	Kullanılması karmaşık olabilir, uygulama zorluğu bulunmaktadır.
(Yakut, 2024)	Kaotik Fonksiyonlar, XOR İşlemleri	XOR işlemine dayalı olarak güvenlik zafiyeti olabilir.
(Durafe & Patidar, 2024)	Fraktal Kapak, Kaos-DNA Tabanlı Şifreleme	Uygulama zorluğu ve karmaşıklık mevcuttur.
(Yamni ve ark., 2024)	Adaptif Kaotik Dinamik Sistem, Ayrık Ortogonal Momentum Dönüşümleri	Yüksek hesaplama gücü gereksinimi söz konusudur
(Salim ve ark., 2024)	Lorenz Kaotik Sistemi, Bloom Filtresi	Yanlış kullanım durumunda veri kaybı riski vardır.
(Aparna & Madhumitha, 2023)	Çoklu Kaotik Haritalar, Görüntü Şifreleme, Steganografi	Sistem karmaşık yapıya sahiptir.
(Ramzan & Khan, 2023)	Lineer Kesirli Dönüşüm, Kaotik Haritalar	Gelişmiş kurulum ve uygulama gerektirir.
(Elshoush & Mahmoud, 2023)	Parçalı Lineer Kaotik Harita, Tek Kullanımlık Şifre	Verimliliği etkileyen karmaşıklıklar bulunmaktadır.
(Nagarajegowda & Krishnan, 2023)	Geliştirilmiş Hiper-Kaotik Henon Haritası, Fraktal Tromino	Uygulaması güç ve sistemsel zorluklar içerebilir.
(Liu ve ark., 2022)	Yüksek Boyutlu Kaotik Harita, Steganografi	Yüksek hesaplama gücü gerektirir.
(Hematpour ve ark., 2022)	Bağlantılı Kaotik Haritalar, Yeni Kaotik S-kutu	Gelişmiş hesaplama kaynakları gerektirir.

(Bhandari ve ark., 2022)	Karınca Kolonisi Optimizasyonu, Üçgen Kaotik Harita	Uygulama zorluğu ve zaman alıcı süreçler mevcuttur.
(Abd & Hussein, 2022)	Duffing Kaotik Haritası, Steganografi	Hedef uygulama gereklilikleri olabilir.
(Alabaichi & Altameemi, 2022)	DNA ve Kaotik Harita	Karmaşık yapısı nedeniyle güvenlik açıkları olabilir.
(Rostam ve ark., 2022)	Steganografi, Kaotik Fonksiyonlar	IoT ortamlarındaki değişken güvenlik açıkları vardır.
(Sharafi ve ark., 2021)	Hibrit Kaos Haritası, Ayrık Dönüşümler	Uygulama karmaşası ve tasarım zorlukları vardır.
(Al-Sulami & Hashim, 2021)	Kaotik Haritalar, Steganografi Teknikleri	Literatür taraması sınırlı yenilikçi çözümler sunabilir.
(Karawia, 2021)	Modifiye LSB Yöntemi, Kaotik Harita	Yüksek görünürlük sorunu olabilir.
(Khaleel & Abduljaleel, 2021)	Steganografi Madenciliği, Şifreleme	Ekstra hesaplama gereksinimleri artırabilir.
(Kustov & Krasnov, 2021)	Parazit Altında Gizli Mesajlar Maskeleme	Daha düşük güvenlik seviyelerine yol açabileceğinden dikkat edilmelidir.
(Hameed ve ark., 2021)	3D Cat Haritası Kullanarak Kaos Tabanlı Renkli Görüntü Steganografisi	Hesaplama yükü ve eğitme süresi yüksek olabilir.
(Vivek & Gadgay, 2021)	Kaos Şifreleme Algoritması, Yüksek Verimlilikte Video Steganografisi	Video kalitesinde kayıplar görülebilir.

3. MATERYAL VE YÖNTEM

3.1. En Düşük Bite Ekleme Yöntemi

En sık kullanılan steganografik yöntem görüntü steganografisidir. Bu metodoloji iki dosya kullanır. İlk görüntünün örtü verisi veya kapak resmi (Cover Image) olarak bilinen verinin saklanacağı resim dosyasıdır. Diğer bir dosya ise mesaj dosyasıdır. En Düşük Bite Ekleme Yöntemi (LSB, Least Significant Bit) görüntü steganografisinde en yaygın yöntemdir. Görüntü piksellerinin en küçük bitleri, girilecek veri bitlerinin yerini almaktadır. LSB yönteminin en büyük avantajı, gizli verinin görüntüye dahil edilmesinin ardından insan gözünün algılayamayacağı kadar küçük değişiklikler yapmasıdır. LSB yöntemi tipik olarak yüksek kaliteli görsel dosyalarda çok yüksek miktarlarda veri gizleme işlemini sağlayabilmektedir. Bununla birlikte, kullanımının yaygınlığı ve tanınması nedeniyle bu yöntem saldırıya karşı dayanıksızdır. Şekil 1'de

bir görüntü pikselleri içerisine tek bir karakterlik metin verisinin LSB ile nasıl eklendiğini gösteren bir örnek verilmiştir (Güvenoğlu & Razbonyalı, 2019).

Şekil 1. Görüntü Piksellerine Metin Verisinin Eklenmesi ve Çıkarılması

Bu yöntem, her bir fotoğraf pikselinin en düşük bitlerine gizli verinin sekiz bitinin sırasıyla eklenmesi yoluyla gerçekleştirilmektedir. Gizlenmek istenen veri ASCII tablosundaki 89 değerine karşılık gelen Y karakteri Şekil 2'de gösterilmektedir. Bu karakterin ikili sistemde karşılığı 01011001'dir. İkili bit dizisinin her bir bitinin görüntü piksellerine ait en düşük bitleri ile yer değiştirmesi sırasıyla gerçekleşmektedir. Alıcı tarafından gönderilen görüntüye tersine işlem uygulanmaktadır. Bu nedenle, resim piksellerinin ikili sayı sistemindeki karşılığı bulunmaktadır. En düşük bitler bir araya getirilerek 8'erli olarak gruplandırılmıştır. Gruplanan bu ifadelerin ASCII karşılıkları alındıktan sonra gizlenmiş metin verisi elde edilebilmektedir. Örnekteki en düşük bit grubu 01011001'dir. Bu değerin ASCII karşılığı 89'dur ve Y karakterini temsil etmektedir.

3.2. Kaotik Haritalar

Kaotik haritalar, kriptografi ve steganografi alanlarında güvenliği artırmak ve rastgelelik sağlamak amacıyla önemli bir rol oynamaktadır. Özellikle kaos tabanlı şifreleme sistemlerinde, doğrusal olmayan dinamik yapıları sayesinde yüksek güvenlik seviyesi sunarak şifreleme anahtarlarının tahmin edilmesini zorlaştırmaktadır (Mowafy ve ark., 2024). Bunun yanı sıra, steganografi uygulamalarında da kaotik haritalar kullanılarak gizli verinin konumlandırılması ve dağıtılması rastgele hale getirilmekte, böylece saldırılara karşı direnç artırılmaktadır. Kaotik sistemlerin duyarlılık özelliği sayesinde, küçük başlangıç değişiklikleri bile büyük farklılıklara yol açarak veri güvenliğini güçlendirmektedir. Hem kriptografik hem de steganografik yöntemlerde kaotik haritaların entegrasyonu, bilgi gizleme ve koruma süreçlerinde etkili bir strateji olarak değerlendirilmektedir. Bu bağlamda, kaos tabanlı yaklaşımlar modern güvenlik protokollerinde önemli bir bileşen olarak görülmektedir (Nasr ve ark., 2024; Yakut, 2024).

3.2.1. Kaotik çadır harita

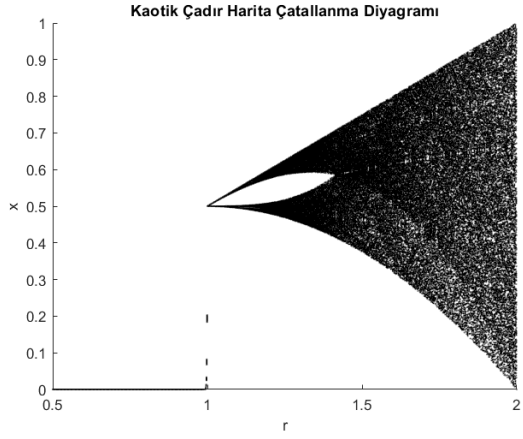
Kaotik Çadır Harita (CTM, Chaotic Tent Map), basit ve tek boyutlu kaotik bir haritadır. En yaygın kullanılan kaotik haritalardan biridir. Literatürde optimizasyon yöntemleri, rastgele sayı üretimi ve şifrelemede anahtar üretimi için kullanılmaktadır. CTM, Denklem 1 ile ifade edilmektedir (Odeh ve ark., 2025).

$$x_{n+1} = \begin{cases} r \cdot x_n & eğer\ x_n < 0{,}5 \\ r \cdot (1 - x_n) & eğer\ x_n \geq 0{,}5 \end{cases} \quad (1)$$

Burada $x_n \in [0, 1]$ başlangıç değerini, $r \in [0, 2]$ sistem kontrol parametrelerini ve x_{n+1} bir sonraki iterasyon değerini temsil etmektedir.

3.2.2. Bifurcation diagram

Dinamik sistemlerin parametrelerinde meydana gelen değişiklikler ve sistemin davranışında meydana gelen değişiklikler, bir bifurcation (Çatallanma) diyagramıyla gösterilebilir. Bu diyagramlarda, parametrelerin değerleri, sistemin kaotik davranışını, periyodik çözümlerini ve sabit noktalarını nasıl değiştirdiğini göstermektedir. Bifurcation diyagramları, özellikle kaotik sistemlerde, sistemin hangi parametrelerde kaotik hale geldiğini ve hangi parametrelerde düzenli veya kalıcı çözümler görüldüğünü analiz etmek için kullanılır (Sriram ve ark., 2024). Bifurcation diyagramları, tipik olarak parametrenin yatay eksende ve sistemin çözüm değerlerinin dikey eksende gösterildiği bir grafik şeklinde çizilir. Bu diyagramlara göre, sistemin uzun vadeli performansı, çok küçük parametre değişikliklerinden etkilenebilir (Karimov ve ark., 2021). Bifurcation diyagramları, özellikle kaotik sistemlerde, sistemin davranışının önemli geçiş noktalarını görselleştirerek kaotik davranışın nasıl ortaya çıktığını anlamamıza yardımcı olur. Parametredeki küçük bir değişiklik, sistemin çözümünü önemli ölçüde etkileyen noktalardır. Bu ayrım noktalarından sonra, kaotik sistemlerde sistemin davranışı deterministik olmaktan çıkar ve küçük bir değişiklik çok önemli sonuçlara yol açmaktadır. Çalışmada kullanılan yöntemde kaotik haritadan elde edilen değerlere ait bifurcation grafiği Şekil 2' de verilmiştir.

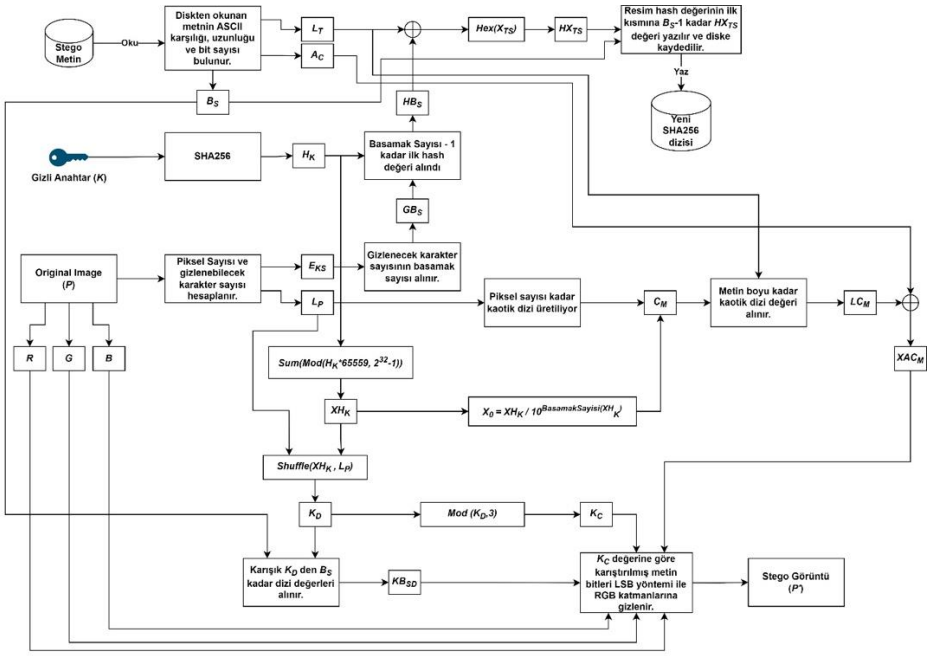


Şekil 2. Kaotik Çadır Haritasının Bifurcation Diyagramı

Çalışmada kullanılan çatallanma diyagramı, r kontrol parametresinin değişimiyle sistemin uzun vadeli x durum değişkeni davranışındaki geçişleri göstermektedir. Sistem $r < 1$ için $x = 0$ noktasına yakınsarken, $r = 1$ civarında durağanlığını yitirmektedir. Sistem yaklaşık $1 < r < 1{,}414$ aralığında düzenli bir davranış sergilemektedir. Sistem 1,414' ten sonra ise kaotik yapı sergilemeye başlayarak x değeri rastgele bir dağılım sergilemeye başlamaktadır. $r = 2$ olması durumunda ise tam olarak kaotik bir yapıya dönüşmektedir. Bu noktada kaotik bir yapıya ulaşması ve düzgün bir dağılım sergilememesinden dolayı steganografi gibi pek çok bilim alanı için büyük önem taşımaktadır. Bu teorik çerçeve doğrultusunda, önerilen steganografi algoritmasının tekrar üretilebilirliğini ve güvenliğini sağlamak amacıyla kullanılan parametreler net bir şekilde tanımlanmıştır. Önerilen yöntemin uygulanmasında, sistemin tam kaotik bölgede çalışmasını ve maksimum öngörülemezlik sağlamasını temin etmek için kontrol parametresi $r = 2$ olarak belirlenmiştir. Sistemin başlangıç koşullarına olan yüksek duyarlılığından faydalanarak güvenliği artırmak amacıyla, algoritmanın gizli anahtarı olarak işlev gören başlangıç koşulu ise $x_0 = [0, 1]$ aralığında seçilmiştir. x_0 değeri önerilen yöntemde kullanıcıya ait gizli anahtar yardımıyla dinamik bir şekilde elde edilmekte ve bu aralıkta olması garantilenmektedir. Bu parametreler altında CTM tarafından üretilen kaotik dizi, mesaj bitlerinin gizleneceği piksel koordinatlarının belirlenmesinde kullanılmıştır. Bu değerlerin açıkça belirtilmesi, yöntemin bilimsel geçerliliğini artırmakta ve sonuçların doğrulanabilirliğini sağlamaktadır.

3.3. Önerilen Yöntem

Bu çalışmada, güvenli veri iletimi için LSB yöntemi ile birlikte CTM fonksiyonunu kullanan güvenli bir steganografi yöntemi önerilmiştir. Yöntem, veri gizleme ve gömülü veriyi taşıyıcı veriden çıkarma olmak üzere iki temel bileşenden oluşmaktadır. Veri gizleme yöntemine ait tüm adımları gösteren blok diyagram Şekil 3' te gösterilmektedir.



Şekil 3. Veri Gizleme Blok Diyagramı

Önerilen yöntem ard arda gelen yedi adımdan meydana gelmektedir. Her adımda gerçekleşen veri gizleme adımları aşağıda detaylı olarak verilmiştir.

Adım 1: İlk adımda gizlenecek metin okunarak her bir karakterin ASCII karşılığı (A_C) elde edilmektedir. Ardından metnin uzunluğu (L_T) ile toplam bit sayısı (B_S) hesaplanmaktadır. Bu aşamada elde edilen her bir değer sonraki adımların gerçekleştirilmesinde kullanılmaktadır.

Adım 2: Verilerin üçünücü taraflardan gizlenebilmesi için kullanıcıya ait kişisel gizli anahtarlar kullanılması veri güvenliği açısından da iyi olmaktadır. Bundan dolayı bu adımda kullanıcının kişisel gizli anahtarı olan K değerinin gizliliğininde sağlanabilmesi açısından SHA-256 hash algoritmasından geçirilmektedir. SHA-256 hash algoritması ile elde edilen gizli anahtarın karşılığı H_K elde edilmektedir. Veri şifreleme alanında, SHA-256 hash algoritması en çok tercih edilen anahtarlama algoritmaları arasındadır. Bu aşamada, SHA-256 hash algoritması yöntemde hem anahtarın gizliliğini hem de sonraki adımlarda kaotik haritanın başlangıç değerini elde etmek için kullanılmaktadır.

Adım 3: Önerilen veri gizleme yöntemi RGB renkli görüntüler üzerinde uygulanmaktadır. İlk olarak P orijinal görüntüsü veri gizleme aşamasında kullanılacağından öncelikli olarak RGB kanallarına ayrılmaktadır. Ayrıca bu aşamada görüntünün toplam piksel sayısı L_P ve eklenebilecek karakter sayısı E_{KS} değeri elde edilmektedir. Gizlenebilecek karakter sayısı olan E_{KS} değeri Denklem 2 yardımıyla elde edilmektedir.

$$E_{KS} = \frac{L_P}{8} \tag{2}$$

Bu aşamada, E_{KS} değerinin basamak sayısı olan GB_S değeri de elde edilmektedir. Elde edilen bu değer toplam metin uzunluğunun veri elde etme aşamasında ve yöntemin sonraki adımlarında kullanılmak üzere hash değeri içerisine gizlenebilmesi amacıyla elde edilmektedir. Bunun ana nedeni, verinin tekrar elde edilmesi için metin uzunluğuna ihtiyaç duyulmasıdır. Metnin uzunluğunun da üçüncü taraflardan gizlenmesi son derece önemlidir.

Adım 4: Bu adım, Adım 3' te elde edilen metin uzunluğunun gizlenmesi aşamalarını içermektedir. Adım 2' de elde edilmiş olan SHA-256 anahtarlama değer dizisinin ilk GB_S-1 adet değeri alınarak HB_S değeri Denklem 3 ile elde edilmektedir.

$$HB_s = SHA256\ (1 : GB_s - 1) \tag{3}$$

Ek olarak, Adım 1' de elde edilmiş olan L_T değeri ile HB_S değeri XOR işlemine tabi tutularak onaltılık sayı sisteminde bu değerlerin karşılığı elde edilmektedir. Denklem 4' te bu süreç işlemi verilmiştir.

$$HX_{Ts} = Hex(L_T \oplus HB_s) \tag{4}$$

Elde edilmiş olan onaltılık sayı sistemindeki bu değer ile H_K anahtarlama dizisinin en başındaki GB_S-1 kadarlık kısmı yer değiştirmektedir. Buradaki yer değiştirme işleminde SHA-256 anahtarlama dizisi boyu sabit kalmaktadır. Elde edilen yeni SHA-256 anahtarlama değer dizisi diske yazılmaktadır. Bu değerin geri dönüşü mümkün olmadığından herkese açık olmasında da herhangi bir sakınca bulunmamaktadır. Bu durum hash algoritmalarının doğal bir sonucudur.

Adım 5: Adım 2' deki H_K anahtarlama değeri yardımıyla XH_K gizli anahtarı değeri elde edilmektedir. Gizli anahtar XH_K değerinin elde edilmesi Denklem 5 yardımı ile gerçekleştirilmektedir.

$$XH_K = SUM\ (Mod(H_K \times 65559, 2^{32} - 1) \tag{5}$$

Bu aşamada ayrıca kaotik harita değerleri de paralel olarak elde edilmektedir. Bunun için toplam piksel sayısı L_P adeti kadar kaotik dizi değeri elde edilmektedir. Kaotik bir haritada dizi değerlerinin elde edilebilmesi ancak kaotik denklemin X_0 başlangıç değeri ile mümkün olabilmektedir. Bu nedenle X_0 değerinin elde edilebilmesi amacıyla Denklem 6 kullanılmaktadır.

$$X_0 = XH_K\ \ / (10^{BasamakSayısı(XH_K)} \tag{6}$$

Adım 6: Kaotik dizi değerlerinin elde edilmesinin ardından bu dizinin ilk L_T adeti kadar dizi değeri alınmaktadır. Gizlenecek metin uzunluğuna göre bu L_T değeri değişmektedir. Adım 1'deki metinin ASCII karşılığı elde edilen A_C ile kaotik diziden alınan LC_M kadar dizi değeri XOR işlemine tabi tutulmaktadır. Bu işlemin temel amacı, gizlenecek olan her bir karakterin anlaşılamaz hale getirilmesidir. Bu da bilgilerin korunmasını sağlamaktadır. Bu sürece ait işlem Denklem 7' de gösterilmektedir.

$$XAC_M = LC_M \oplus A_C \quad (7)$$

Adım 7: Adım 5'teki süreçte elde edilen XH_K gizli anahtarı ile bu adımda karışık bir yamsayı dizisi elde edilmektedir. Bu karışık dizi değerleri, resmin piksel sayısı kadardır ve 1 … ($M \times N$) arasında yer alan tamsayılardan oluşmaktadır. Bu prosedürün amacı, gizlenecek olan metine ait bit değerlerinin hangi RGB katmanlarına ekleneceğini belirlemektir. 1 … ($M \times N$) arasındaki tamsayıların karıştırılmasında aşağıdaki verilen adımlar kullanılmaktadır.

Adım 7.1: $M \times N$ adet kadar rastgele sayı üretilir. Burada rastgele sayı üretecinin görevini yerine getirebilmesi için başlangıç değeri (seed) olarak Adım 5' te elde edilmiş olan XH_K değeri kullanılmaktadır.

Adım 7.2:Üretilen rastgele tamsayılar bir dizide tutulmaktadır.

Adım 7.3: Üretilen rastgele sayılar kendi içinde küçükten büyüğe doğru sıralanmaktadır. Bu sıralama sırasında dizi indis değerleri de farklı bir diziye değiştirme sırasıyla yazılarak K_D karışık dizisi elde edilmektedir. Belirtilen bu süreçlere ait bir karıştırma işlemi örneği Tablo 2' de verilmiştir.

Tablo 2. Karışık Dizinin Elde Edilme Işlemi Örneği

Dizi indisi	1	2	3	4	5	6	7	8	9	10
Rastgele üretilen sayılar	6	1	5	8	7	10	9	2	4	3
Sıralanan rastgele sayılar	1	2	3	4	5	6	7	8	9	10
Karışık dizi ile konumları değişen dizi indisleri	2	8	10	9	3	1	5	4	7	6

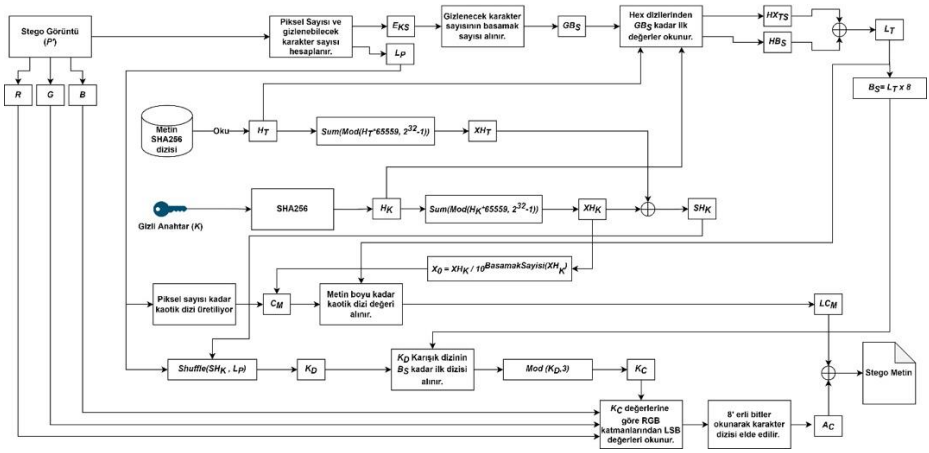
Karıştırılmış dizi değerleri, RGB kanal sayısı olan 3 ile mod işlemine tabi tutulmaktadır. Gizlenecek veri bitinin hangi RGB kanallarına ekleneceğini belirlemek için bu yöntem kullanılmaktadır. Denklem 8 ve Denklem 9, karışık dizinin ve metin veri bitlerinin hangi RGB kanallara gizleneceğine dair gerçekleştirilen işlemleri göstermektedir.

$$K_D = Shuffle(XH_K, L_P) \quad (8)$$
$$K_C = mod(K_D, 3) \quad (9)$$

K_D karışık dizisinin ilk değerinden itibaren B_S adeti kadar sayı alınarak KB_{SD} dizisine yazılmaktadır. Bu dizi değerleri, metin bitlerinin görüntüdeki hangi koordinattaki piksele veri ekleneceğini belirlemektedir. Bu koordinat değerleri yardımıyla önceden karıştırılmış olan XAC_M metin bitleri LSB yöntemi kullanılarak veri gizlenmiş P' stego görüntüsü elde edilmektedir. Elde edilen görüntünün boyutlarında ve veri büyüklüğünde bir değişiklik olmamaktadır.

3.4. Gizli Verinin Elde Edilmesi

Gizlenmiş olan verinin elde edilebilmesi için veri gizleme işleminin tersten çalıştırılması gerekmektedir. Gizlenmiş olan verinin elde edilmesi Şekil 4' de verilen blok diyagram takip edilerek gerçekleştirilmektedir.



Şekil 4. Gizli Verinin Elde Edilme Süreçlerini Gösteren Blok Diyagram

Stego-görüntü içerisine gizlenmiş olan verinin alıcı tarafından hatasız bir şekilde elde edilebilmesi, veri gizleme sürecinde gerçekleştirilen algoritmik adımların tam tersi sırada ve doğru parametrelerle uygulanmasını gerektirmektedir. Bu süreç, alıcının stego-görüntüye (P'), kişisel gizli anahtara (K) ve veri gizleme aşamasında oluşturulup diske yazılmış olan modifiye edilmiş SHA-256 hash değerine sahip olmasını zorunlu kılmaktadır. Gizli verinin elde edilme süreci, Şekil 4'te blok diyagramı verilen ve aşağıda detaylandırılan adımlardan oluşmaktadır.

Adım 1: Başlangıç Parametrelerinin ve Anahtarların Hazırlanması

Veri çıkarma sürecinin ilk adımında, alıcı kendi kişisel gizli anahtarını (K) kullanarak sistemin temelini oluşturan parametreleri yeniden üretilmektedir. Kişisel gizli anahtar K, veri gizleme aşamasında olduğu gibi SHA-256 hash algoritmasından geçirilmektedir. Bu işlem sonucunda, metin uzunluğunun gizlenmemiş olduğu orijinal hash değeri (H_K) elde edilmektedir. Bu H_K değeri, sonraki adımlarda hem metin uzunluğunu deşifre etmek hem de kaotik diziyi ve piksel konumlarını üretmek için kritik öneme sahiptir. Stego görüntü P' okunarak boyutları ($M \times N$) ve toplam piksel sayısı (L_P) tespit edilmektedir.

Adım 2: Gizli Metin Uzunluğunun (L_T) Geri Elde Edilmesi

Verinin tamamının ne kadar olduğunun bilinmesi, çıkarma işleminin nerede duracağını belirlemek için son derece önemlidir. Bu bilgi, modifiye edilmiş hash değeri içerisinden aşağıdaki adımlarla elde edilmektedir.

- Stego-görüntünün toplam piksel sayısı (L_P) kullanılarak, Denklem 2'de verilen formül aracılığıyla gizlenebilecek maksimum karakter sayısı (*EKS*) ve bu sayının basamak adedi (GB_S) yeniden hesaplanmaktadır.
- Diske yazılmış olan modifiye edilmiş hash değeri (H_K) okunmaktadır. Bu hash değerinin ilk GB_S-1 karakteri, Denklem 4'te şifrelenmiş metin uzunluğunu temsil eden HX_{TS} değerini içermektedir.
- Adım 1'de üretilen orijinal hash değerinin (H_K) ilk GB_S-1 karakteri alınarak HB_S değeri elde edilmektedir.
- Veri gizleme aşamasındaki Denklem 4' te verilen XOR işleminin tersi uygulanarak orijinal metin uzunluğu (L_T) Denklem 10'da gösterildiği gibi hesaplanır.

$$L_T = HexToDec(HX_{Ts} \oplus HB_s) \tag{10}$$

- Elde edilen L_T değeri, çıkarılacak toplam bit sayısını ($B_S = L_T \times 8$) belirlemek için kullanılmaktadır.

Adım 3: Kaotik Dizinin ve Karışık Konum Dizisinin Yeniden Üretilmesi

Metin uzunluğu elde edildikten sonra gizli veriyi elde etmek ve bitlerin konumlarını bulmak için gerekli olan diziler yeniden oluşturulmaktadır. Bu süreç aşağıdaki adımlar izlenerek gerçekleştirilmektedir.

- Adım 1'de üretilen orijinal H_K değeri kullanılarak, Denklem 5 yardımıyla XH_K gizli anahtarı tekrar hesaplanmaktadır.
- XH_K değeri, Denklem 6'ya göre kaotik haritanın başlangıç değeri olan X_0'ı üretmek için kullanılmaktadır.
- Bu X_0 başlangıç değeri ile Tent Haritası (CTM), L_T iterasyon kadar çalıştırılarak, veri gizleme aşamasında kullanılan kaotik dizinin (LC_M) aynısı elde edilmektedir. Bu dizi, bir sonraki adımda verileri elde etmek için kullanılmaktadır.
- Aynı XH_K değeri, rastgele sayı üretecinin başlangıç değeri (seed) olarak kullanılarak, piksellerin karıştırılma sırasını belirleyen karışık dizi (K_D) Denklem 8'e göre yeniden oluşturulmaktadır. Ardından, Denklem 9 ile her piksel için hangi renk kanalının (R, G veya B) kullanıldığı bilgisi de elde edilmektedir.

Adım 4: Gizli Bitlerin Stego-Görüntüden Çıkarılması

Bu aşamada piksellerin hangi renk kanallarından, kaç adet bit çıkarılacağı bilgisi elde edilmiş olmaktadır. Ardından aşağıdaki adımlar izlenerek stego görüntü içerisindeki karıştırılmış hale getirilen bit dizisine ulaşılmaktadır.

- K_D dizisinin ilk B_S adet elemanı, gizli bitlerin bulunduğu piksel koordinatlarını; K_C dizisinin ilk B_S adet elemanı ise ilgili renk kanallarını göstermektedir.
- Elde edilen koordinat ve kanal bilgileri takip edilerek, stego-görüntü P' üzerindeki ilgili piksellerin belirtilen renk kanallarından en düşük bitleri

sırasıyla okunmakta ve bir bit dizisi haline getirilmektedir. Bu bit dizisi, şifrelenmiş metin olan XAC_M'yi temsil etmektedir.

Adım 5: Orijinal Metnin Deşifre Edilmesi

Son adımda, elde edilen karıştırışmış bit dizisi çözülerek orijinal metne ulaşılmaktadır.

- Elde edilen XAC_M bit dizisi, 8'erli gruplara (byte) ayrılır ve her bir grubun ASCII sayısal karşılığı bulunmaktadır.
- Bu ASCII değerleri, Adım 3'te yeniden üretilen kaotik dizi LC_M ile Denklem 7'nin tersi olan XOR işlemine tabi tutulmaktadır. Yapılan işlemin tersi Denklem 11'de verilmiştir.

$$A_C = LC_M \oplus XAC_M \tag{11}$$

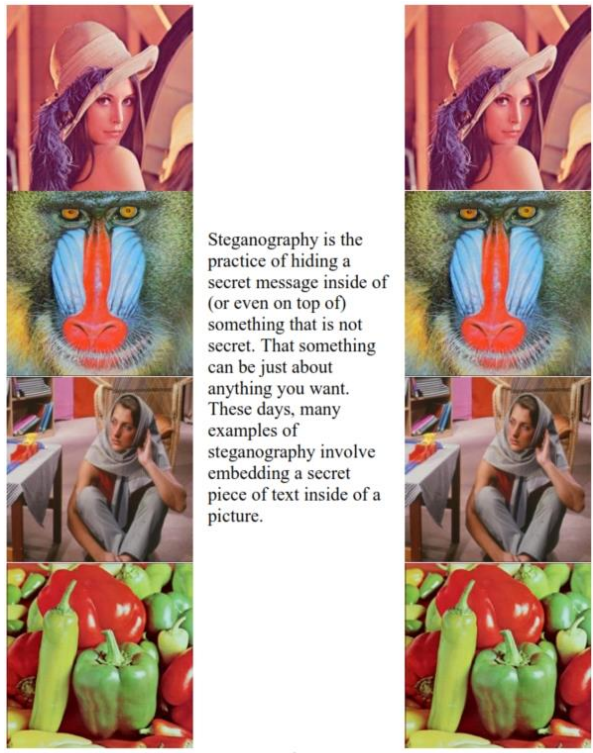
- XOR işlemi sonucunda elde edilen yeni ASCII değerleri (A_C), karakter karşılıklarına dönüştürülerek orijinal gizli metin başarıyla elde edilmiş olmaktadır.

4. DENEYSEL SONUÇLAR VE DETAYLI GÜVENLİK ANALİZLERİ

Bu bölümde, ayrıntıları önceki bölümde verilen veri gizleme yöntemine ait deneysel sonuçlar ve güvenlik analizlerinin detaylarına yer verilmiştir.

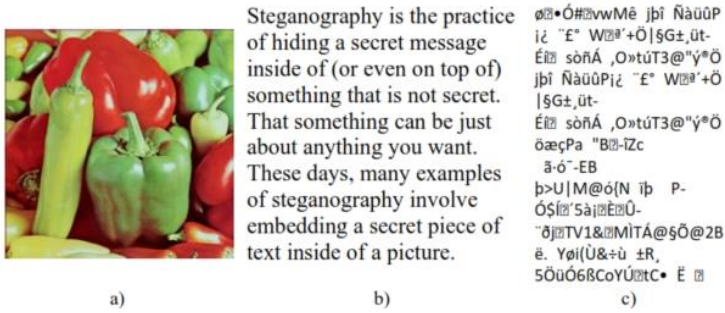
4.1. Veri Gizleme ve Gizlenmiş Verinin Elde Edilmesi

Önerilen yöntemin 256 × 256 boyutlarında "Lena", "Pepper", "Barbara" ve "Baboon" görüntüleri üzerinde deneysel çalışmalar yapılmıştır. Önerilen yöntem, gri seviye görüntüler ve RGB renkli üzerinde başarılı bir şekilde çalışmaktadır. Önerilen yöntem, Intel Core i7-4700 CPU ve 2,4 GHz 4 çekirdek işlemcili, MS Windows 10 Professional 64 bit işletim sistemi ve 16 GB RAM kapasiteli bir bilgisayar üzerinde test edilmiştir. Şekil 5' de rastgele seçilmiş bir metnin yukarıda isim ve ölçüleri verilen görüntüler içerisine gizlenmiş sonuçlarına yer verilmiştir.



Şekil 5. Veri Gizlenmiş Görüntüler ve Görsel Analizi
a) Orijinal Görüntüler, b) Gizlenen Metin, c) Metin Gizlenmiş Görüntüler

Şekil 5'e dikkatle bakıldığında, veri gizlenmiş görüntülerde belirgin bir farkın bulunmadığı görülmektedir. Bu durum önerilen yaklaşımın veri gizlemede oldukça etkili olduğunu göstermektedir. Bununla birlikte veri gizlenmiş görüntülerden doğru ve yanlış şifre ile verilerin elde edilip edilemediği de test edilmiştir. Örnek bir deneysel sonuç Şekil 6' da gösterilmiştir.

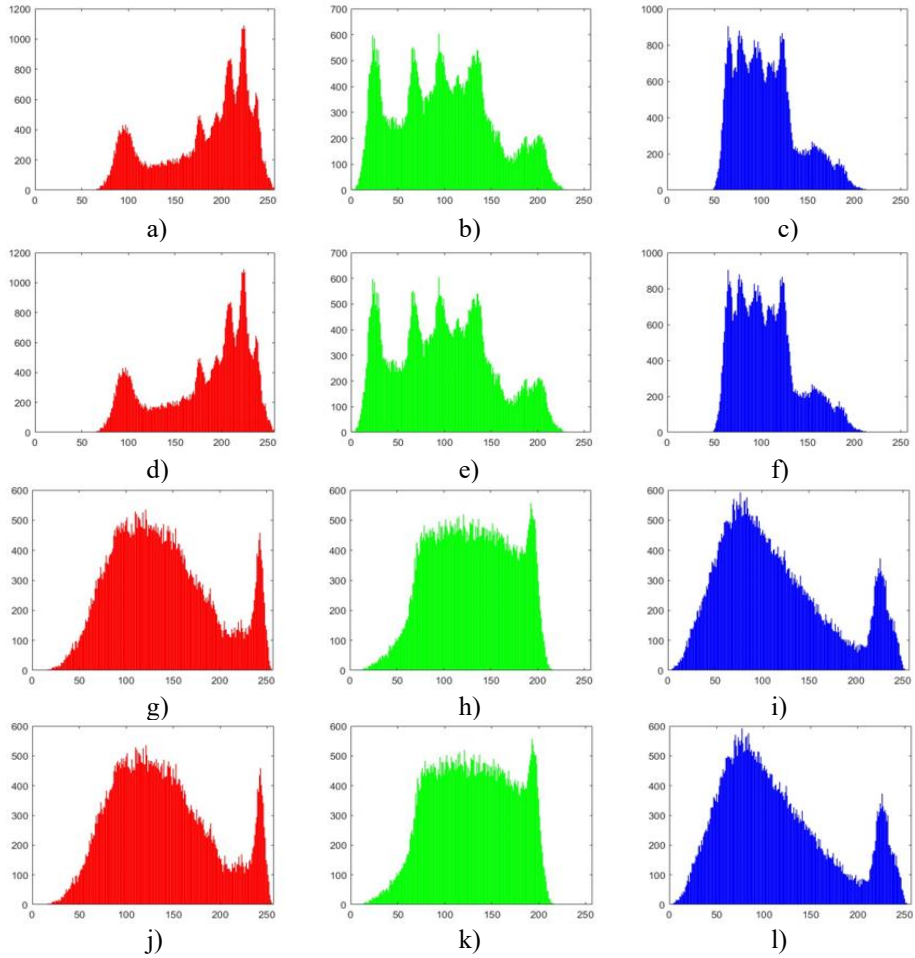


Şekil 6. Doğru ve Yanlış Şifre ile Metnin Elde Edilmesi a) Veri Gizlenmiş Görüntü, b) Doğru Şifre Ile Elde Edilen Metin, c) Yanlış Şifre Ile Elde Edilen Metin

Kullanıcıya ait doğru şifrenin girilmesi durumunda verilerin tam ve eksiksiz olarak elde edildiği, şifrenin yanlış girilmesi durumunda ise orijinal metin ile ilgisi olmayan anlamsız verilerin elde edildiği görülmektedir. Yöntemin doğru şifre ile doğru verinin elde edilmesinde başarılı olduğu sonucuna varılabilmektedir.

4.2. Histogram Analizi Testi

Histogram analizi, gri seviye bir görüntüde piksel değerlerinin nasıl dağıldığını göstermek ve bir görüntüde verinin gizlenip gizlenmediğini belirlemek için kullanılmaktadır (Xie ve ark., 2022). Başka bir deyişle, orijinal görüntüdeki piksel değerleri ve veri gizlenmiş piksel değerleri arasında bir karşılaştırma sağlamaktadır. Renkli görüntü olması durumunda, RGB kanallarının her biri için histogramlar ayrı ayrı oluşturulmaktadır. Başka bir deyişle, renkli bir görüntünün karşılaştırılması RGB kanalları kullanılarak gerçekleştirilmektedir. Verinin gizlenmesinde kullanılan bazı test görüntülerine ait orijinal ve veri gizlenmiş görüntülerin histogram dağılımları Şekil 7' de verilmiştir.



Şekil 7. Histogram analizi testi, a) Orijinal Lena Red histogramı, b) Orijinal Lena Green histogramı, c)Orijinal Lena Blue histogramı, d) Veri Gizlenmiş Lena Red Histogramı, e) Veri Gizlenmiş Lena Green Histogramı, f) Veri Gizlenmiş Lena Blue Histogramı, g) Orijinal Baboon Red histogramı, h) Orijinal Baboon Green histogramı, i)Orijinal Baboon Blue histogramı, j) Veri Gizlenmiş Baboon Red Histogramı, k) Veri Gizlenmiş Baboon Green Histogramı, l) Veri Gizlenmiş Baboon Blue Histogramı

Histogram analizinde orijinal görüntü histogramları ve veri gizlenmiş görüntü histogramlarının aynı olması beklenmektedir. Şekil 7'ye dikkat edildiğinde orijinal ve veri gizlenmiş görüntü histogramları arasında bir farklılığın olmadığı görülmektedir. Bu durum ise önerilen yöntemin histogram analizi testinde oldukça başarılı bir sonuç ortaya koyduğu anlamına gelmektedir.

4.3. Entropi Testi

Entropi testi, bir verideki rastgelelik ve düzensizlik düzeyini ölçmek için kullanılmaktadır. Veri gizlenmiş görüntülerde, entropi değerinin işlenmemiş orijinal görüntünün entropi değerine oldukça yakın olması beklenmektedir. Bu durum görüntü pikselleri arasında bir düzensizliğinde olmadığı anlamı taşımaktadır. Bir görüntünün entropisi Denklem 12 ile hesaplanmaktadır (El-Khamy ve ark., 2020).

$$H(S) = -\sum_{S}(P(S_i)\ x\ \log_2 P(S_i)) \tag{12}$$

Burada *S*, mesaj bilgisini temsil ederken, *H(S)* bu mesajın entropisini ifade etmektedir. S_i, görüntü veri dizisindeki belirli bir sembol veya piksel değerini, $P(S_i)$ ise bu sembolün olasılığını göstermektedir. Entropi değeri genellikle [0, 8] arasında değişmektedir. Veri gizlenmiş 8 bitlik bir görüntüde, beklenen entropi değeri orijinal görüntünün entropisine yakın olmalıdır. Önerilen yöntemin entropi analizi sonuçları Tablo 3' de verilmiştir.

Tablo 3. Entropi Testi Sonuçları

	Orijinal Görüntü			**Veri Gizlenmiş Görüntü**		
Görüntüler	**R**	**G**	**B**	**R**	**G**	**B**
Lena	7,2427	7,5765	6,9181	7,2428	7,5765	6,9183
Baboon	7,6048	7,3521	7,6655	7,6038	7,3520	7,6652
Barbara	7,5528	7,3746	7,4772	7,5538	7,3746	7,4772
Pepper	7,3006	7,5671	7,0924	7,3006	7,5675	7,0935

Entropi testi neticesinde orijinal ve veri gizlenmiş görüntü entropi değerlerinin birbirlerine çok yakın olduğu görülmektedir. Bu test neticesinde önerilen yöntemin veri gizleme süreçlerinde oldukça başarılı olduğu söylenebilmektedir.

4.4. Korelasyon Analizi Testi

İki görüntü arasındaki ilişkinin belirlenmesi amacıyla korelasyon teknikleri kullanılmaktadır. Veri gizlenmiş görüntülerdeki pikseller arasındaki korelasyonlar yatay, dikey ve çapraz yönlerdeki birbirlerine komşu piksellerden faydalanılarak elde edilmektedir (Güvenoğlu & Tüysüz, 2015). Farklı yönlerdeki korelasyon değerleri *N* seçilen piksel çiflerinin sayıyı, *x* ve *y* komşu piksel değerleri olmak üzere Denklem 13, 14, 15 ve 16 yardımıyla hesaplanmaktadır (Güvenoğlu, 2024).

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{14}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{15}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{16}$$

Bu çalışmada, orijinal görüntüler ve veri gizlenmiş görüntüler arasında birbirlerine komşu 5000 adet rastgele piksel seçilmiş ve üç farklı yönde korelasyon testlerine tabii tutulmuştur. Yöntem farklı görüntüler üzerinde test edilmiş ve test sonuçları Tablo 4 ve Tablo 5'te verilmiştir.

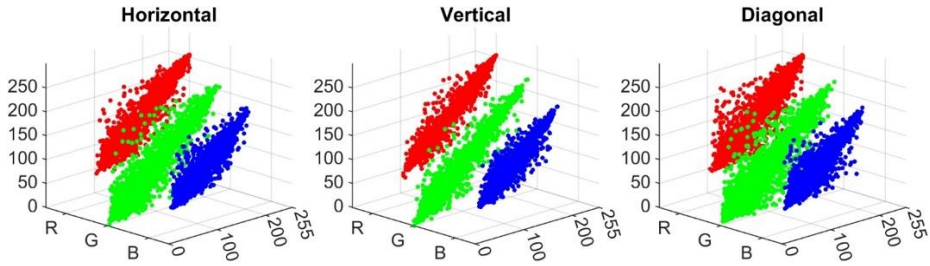
Tablo 4. Orijinal Görüntü Pikselleri Arasındaki Korelasyon

	Yatay			Dikey			Diagonal		
Görüntüler	R	G	B	R	G	B	R	G	B
Lena	0,9565	0,9416	0,9254	0,9790	0,9724	0,9529	0,9344	0,9203	0,8922
Baboon	0,9488	0,8724	0,9204	0,9214	0,8419	0,9127	0,9010	0,8051	0,8765
Barbara	0,9555	0,9449	0,9519	0,9617	0,9564	0,9626	0,9195	0,9022	0,9137
Pepper	0,9651	0,9692	0,9540	0,9716	0,9750	0,9675	0,9305	0,9499	0,9293

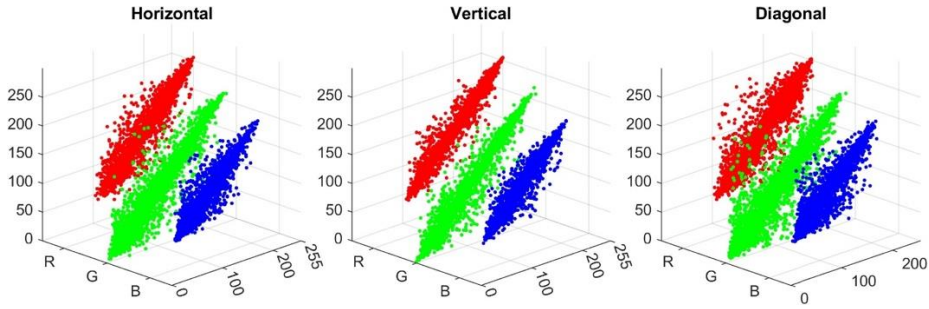
Tablo 5. Veri Gizlenmiş Test Görüntü Pikselleri Arasındaki Korelasyon

	Yatay			Dikey			Diagonal		
Görüntüler	R	G	B	R	G	B	R	G	B
Lena	0,9597	0,9395	0,9256	0,9790	0,9724	0,9527	0,9304	0,9138	0,8937
Baboon	0,9463	0,8654	0,9250	0,9247	0,8375	0,9046	0,8991	0,7932	0,8782
Barbara	0,9528	0,9439	0,9523	0,9606	0,9557	0,9611	0,9205	0,8975	0,9106
Pepper	0,9677	0,9749	0,9579	0,9660	0,9765	0,9689	0,9349	0,9469	0,9277

Tablo 4 ve Tablo 5'te görüldüğü gibi, orijinal görüntüler ile veri gizlenmiş görüntüler arasındaki ilişkinin düşük olduğu görülmektedir. Başka bir deyişle, sonuçlar birbirlerine oldukça yakın değerlere sahiptir. Bu, veri gizleme tekniğinin oldukça etkili olduğunu ve ayrıca veri gizlenmiş görüntünün gözle algılanabilir bir zarar görmediğini göstermektedir. Başka bir ifadeyle üçüncü şahıslar tarafından görüntü içerisinde bir verinin gizlendiğinin anlaşılması oldukça güçtür. Korelasyon testinin orijinal ve veri gizlenmiş Lena görüntüleri üzerindeki dağılımları Şekil 8 ve Şekil 9' da gösterilmiştir. Grafiklerin karşılaştırılmasında da gözle görülür bir zararın olmadığı ve yöntemin oldukça başarılı olduğu anlaşılmaktadır.



Şekil 8. Orijinal Lena Görüntüsüne Ait Korelasyon Dağılım Grafiği



Şekil 9. Veri Gizlenmiş Lena Görüntüsüne Ait Korelasyon Dağılım Grafiği

4.5. Yapısal Benzerlik İndeksi Testi

Yapısal benzerlik indeksi testi (SSIM, Structural Similarity Index Measure), bir görüntünün bozulup bozulmadığının ölçüldüğü bir testtir (Mudeng ve ark., 2022). Orjinal görüntü ile veri gizlenmiş görüntü arasında benzerliği ölçmek ve veri gizlenmiş olan görüntüdeki kaliteyi değerlendirilmek amacıyla kullanılmaktadır. SSIM ile benzerlik ölçümünün yapılabilmesi için orijinal ve veri gizlenmiş görüntülerin ölçülerinin aynı olması beklenmektedir. SSIM, Denklem 17 ile gösterilmektedir (Arabboev ve ark., 2024).

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (17)$$

Burada *x* ve *y* parametreleri sırasıyla orijinal ve veri gizlenmiş görüntüleri, $\mu_x ve\ \mu_y$, x ve y görüntü piksellerinin ortalamalarını, σ_x^2 ve σ_y^2, x ve y görüntülerinin varyanslarını, σ_{xy} ise kovayanslarını temsil etmektedir. Ayrıca C_1 ile C_2, orijinal ve veri gizlenmiş görüntülerin dengeli hale getirilmesi amacıyla kullanılan kontrol değişkenlerini temsil etmektedir (Arabboev ve ark., 2024). SSIM, [-1, 1] değer aralığındadır. SSIM değerinin 0 olması görüntüler arasında benzerliği olmadığı, 1 ise her iki görüntünün çok benzer olduğunu ifade etmektedir. Orijinal görüntü ile veri gizlenmiş görüntünün kalite değerlendirmesi SSIM yöntemi kullanılarak gerçekleştirilmiştir. Tablo 6'da SSIM sonuçlara yer verilmiştir.

Tablo 6. Bit Bazında Gerçekleştirilmiş Yapısal Benzerlik Testi Sonuçları

Görüntüler	**R**	**G**	**B**
Lena	0,99995	0,99996	0,99996
Baboon	0,99998	0,99998	0,99998
Barbara	0,99997	0,99997	0,99997
Pepper	0,99996	0,99996	0,99996

SSIM ile benzerlik ölçümü yapılan görüntülerde, SSIM ölçüm sonuçlarının aynı veya 1' e çok yakın olması beklenmektedir. Tablo 6' ya dikkat edildiğinde bit bazında gerçekleştirilen test sonuçlarına göre orijinal ve veri gizlenmiş görüntülerin çok benzer olduğu, gözle algılanabilir bir farkın olmadığı ve yöntemin oldukça başarılı olduğu söylenebilecektir.

4.6. PSNR ve MSE Testi

Veri gizleme işleminden sonra veri gizlenmiş bir görüntünün kalitesini ve orijinal görüntüye olan benzerliğini değerlendirmek amacıyla, literatüründe yaygın olarak kullanılan Tepe Sinyal Gürültü Oranı (PSNR, Peak Signal to Noise Ratio) ve Ortalama Kare Hata (MSE, Mean Squared Error) metrikleri kullanılmaktadır. Bu metrikler, orijinal görüntü ile veri gizlenmiş görüntü arasındaki farkı ölçerek gizleme işleminin neden olduğu bozulmanın derecesini belirlemektedir. MSE, orijinal *I* görüntü ve *K* veri gizlenmiş görüntü pikseller değerlerinin farklarının karlerinin ortalamasını ölçmektedir. *M*×*N* boyutlarındaki bir görüntü için MSE Denklem 18 ile temsil edilmektedir (Cheddad ve ark., 2010).

$$MSE = \frac{1}{MxN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I(i,j) - K(i,j)]^2 \quad (18)$$

Düşük bir MSE değeri, veri gizlenmiş görüntünün orijinal görüntüye daha yakın olduğunu ve daha az bozulmaya uğradığını göstermektedir. Bir diğer ölçüm metriği olan PSNR, bir görüntünün ulaşabileceği maksimum olası piksel değerinin, görüntüyü bozan hatanın gücüne oranıdır ve genellikle desibel (dB) cinsinden ifade edilmektedir.

PSNR, n piksel başına düşen bit sayısını temsil etmek üzere ve MSE kullanılarak Denklem 19' daki gibi ifade edilmektedir.

$$PSNR = 10\log_{10}\frac{(2^n-1)^2}{MSE} \tag{19}$$

Yüksek bir PSNR değeri, veri gizlenmiş görüntünün kalitesinin yüksek olduğunu ve orijinal görüntüye çok benzediğini, dolayısıyla gizlenen verinin insan gözüyle tespit edilmesinin zor olduğunu göstermektedir. Genellikle, 30 dB üzerindeki PSNR değerleri kabul edilebilir bir kaliteyi işaret etmektedir. Steganografi uygulamalarında ise 50 dB üzerindeki çok daha yüksek değerler hedeflenmektedir (Cheddad ve ark., 2010). Bu durum gizlenen verinin algılanmasının zorlaştığını göstermektedir. Tablo 7' de önerilen yöntem ile veri gizlenmiş görüntülere ait test sonuçları verilmiştir. Sonuçlara dikkat edildiğinde önerilen yöntemin oldukça iyi sonuçlar verdiği anlaşılmaktadır.

Tablo 7. PSNR Ve MSE Testi Sonuçları

	MSE			**PSNR (dB)**		
Görüntüler	R	G	B	R	G	B
Lena	0,0764	0,0751	0,0735	70,4523	70,6253	70,8179
Baboon	0,0740	0,0745	0,0744	70,7202	70,6482	70,7215
Barbara	0,0739	0,0708	0,0739	70,7316	70,1912	70,7025
Pepper	0,0749	0,0731	0,0765	70,6029	70,8159	70,4397

4.7. NPCR ve UACI Testi

Diferansiyel saldırıları analiz etmek için literatürde iki yöntem çok yaygın olarak kullanılmaktadır. Kullanılan iki yöntem, Birleşik Ortalama Değişen Yoğunluk (UACI, Unified Averaged Changed Intensity) ile Piksel Değişim Oranı (NPCR, Number Of Changing Pixel Rate) parametreleridir. Diferensiyel saldırının yukarıda belirtilen yöntemleri, steganografi algoritmalarının standart düz ham görüntülerdeki en ufak değişikliklere karşı hassasiyetini test etmek için kullanılmaktadır. Saldırılar genellikle başlangıç görüntülerini çok küçük bir şekilde değiştirmektedir. Daha sonra orijinal ve değiştirilmiş görüntüler ortak gizli anahtar kullanılarak veriler gizlenmektedir. En son aşamada, değiştirilmiş ve orijinal görüntü arasındaki bağlantı bulunmaya çalışılmaktadır. NPCR testi, orijinal görüntü ile veri gizlenmiş görüntü arasındaki rastgelelik farkını değerlendiren bir yöntemdir. UACI testi ise görüntü steganografisinde performansın değerlendirilmesini sağlanmaktadır. Bu test ile orijinal ve veri gizlenmiş olan görüntü arasındaki değişiklikler gözlemlenmektedir. Orijinal görüntü ile veri gizlenmiş görüntü arasındaki farkın, insan gözüyle fark edilmesi neredeyse imkansız derecede çok ince olduğunu göstermek amacıyla kullanılmaktadır. Birbirlerinden tamamen farklı iki görüntüde NPCR değerinin %99,61'e ve UACI değerinin ise %33,46' ya yakın olması istenmektedir (Ping ve ark., 2018). Ancak steganografide ise orijinal görüntü ve veri gizlenmiş görüntü arasındaki benzerliğin 0' ya çok yakın olması beklenmektedir. Düşük NPCR ve UACI değeri, içerisine veri gizlenen görüntülerin piksel değerlerinde çok az değişiklik olduğu anlamına gelmektedir. Görüntünün kalitesinin korunması amacıyla tercih edilmektedir. NPCR ve UACI, Denklem 20 ve 21 ile ifade edilmektedir (Mansoor & Parah, 2023).

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{MxN} x100 \quad D(i,j) = \begin{cases} 0, & eğer\ C_1 = C_2 \\ 1, & eğer\ C_1 \neq C_2 \end{cases} \tag{20}$$

$$UACI = \frac{1}{MxN}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_1(i,j)-C_2(i,j))}{255}\right] x100 \tag{21}$$

M ve *N*, veri gizlenmiş görüntünün genişlik ve yüksekliğini ifade ederken; C_1 piksel değişikliği yapılmadan önceki veri gizlenmiş görüntüyü, C_2 ise piksel değişikliğinin ardından oluşan veri gizlenmiş görüntüyü göstermektedir. NPCR hesaplamasında, her iki görüntüde aynı koordinattaki piksel değerleri eşit ise 0, farklı ise 1 değeri atanmaktadır. Tablo 8' de, veri gizlenmiş test görüntülerine ait NPCR ve UACI sonuçları sunulmaktadır.

Tablo 8. NPCR ve UACI Sonuçları

	NPCR			**UACI**		
Görüntüler	R	G	B	R	G	B
Lena	0,0057	0,0052	0,0053	$2{,}2972x10^{-5}$	$2{,}2070x10^{-5}$	$2{,}1103x10^{-5}$
Baboon	0,0053	0,0057	0,0052	$2{,}1599x10^{-5}$	$2{,}1951x10^{-5}$	$2{,}1502x10^{-5}$
Barbara	0,0051	0,0042	0,0057	$2{,}1532x10^{-5}$	$1{,}9378x10^{-5}$	$2{,}1651x10^{-5}$
Pepper	0,0059	0,0051	0,0055	$2{,}2201x10^{-5}$	$2{,}1103x10^{-5}$	$2{,}3198x10^{-5}$

Tablo 8' de verilen değerler dikkate alındığında NPCR ve UACI değerlerinin oldukça düşük ve orijinal görüntüden gözle ayırt edilemeyecek kadar küçük farklar olduğu görülmektedir. Bu nedenle önerilen yöntem oldukça başarılı sonuçlar sergilemiştir.

4.8. NIST Analizi Testi

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST, National Institute of Standards and Technology) tarafından geliştirilen testler, kaotik sistemlerde rastgele sayı üreten kaynakların sayı dizilerinin rastgelelik derecesini değerlendirmek için kullanılan istatistiksel yöntemlerdir. NIST test paketi, toplamda 15 ayrı testten oluşmaktadır. Bu testler sayesinde bit dizileri kapsamlı ve güçlü analizlere tabi tutulur. Bir bit dizisinin rastgele kabul edilmesi, bu 15 testin tamamından başarılı sonuçlar alınmasına bağlıdır. Her bir test sonucunda bir P-değeri hesaplanır ve bu değer, test edilen sayı dizisinin rastgelelik seviyesinin bir göstergesi olarak değerlendirilir. P değeri 0,01 olarak seçilmektedir. Bu değerin 0,01' den büyük olması önerilen sistemin rastgele olduğu sonucunu çıkarmaktadır. Başka bir ifadeyle, teste tabi tutulan yöntemin rastgelelik durumunun %99 oranında güvenilir olduğunu göstermektedir. Önerilen yöntemde kaotik haritadan elde edilen değerler ve ardarda gelen adım sonucunda elde edilmiş olan karıştırılmış değerler NIST testine tabii tutulmuştur. Elde edilen test sonuçları Tablo 9' da yer almaktadır.

Tablo 9. Veri Gizlenmiş "Lena" Görüntü İçin NIST Testi Sonuçları

No	Test Adı	P Değeri	Sonuç
1	Frequency (Monobits) Test	0,6471	Rastgele
2	Frequency Test within a Block	0,6760	Rastgele
3	Runs Test	0,6346	Rastgele
4	Test for the Longest Run of Ones in a Block	0,0242	Rastgele
5	Binary Matrix Rank Test	0,7318	Rastgele
6	Discrete Fourier Transform Test	0,6190	Rastgele
7	Non-Overlapping Template Matching Test	0,8728	Rastgele
8	Overlapping Template Matching Test	0,0359	Rastgele
9	Maurer's "Universal Statistical" Test	0,5746	Rastgele
10	Linear Complexity Test	0,9394	Rastgele
11	Serial Test	0,9125	Rastgele
12	Approximate Entropy Test	0,1843	Rastgele
13	Cumulative Sums Test	0,2948	Rastgele
14	Random Excursions Test	0,9146	Rastgele
15	Random Excursions Variant Test	0,6317	Rastgele

Testler neticesinde elde edilen sonuçların 0,01 değerinden yüksek olması önerilen yöntemdeki karıştırılmış dizinin rastgelelik durumunun %99 güvenilir olduğu anlamına gelmektedir. Bu durum önerilen veri gizleme yönteminin 15 testten başarılı olarak geçtiği anlamına gelmektedir.

4.9. Önerilen Yöntemin Karşılaştırılması

Önerilen yöntem literatürdeki diğer yöntemler ile standart kullanılan metrikler üzerinden değerlendirilmiştir. Karşılaştırma yapılırken literatür çalışmalarında tek değer verildiğinden benzer bir biçimde önerilen yöntem içinde RGB değerlerinin ortalaması alınmış ve karşılaştırma yapılmıştır. Literatür karşılaştırması yapılırken hem CTM kullanan yöntemler hemde son yıllarda yapılmış ve LSB kullanan teknikler ile karşılaştırmalar yapılmıştır. Elde edilen değerlendirme sonuçları Tablo 10' da verilmiştir.

Tablo 10. Literatür Yöntemleri ile Metrikler Üzerinden Karşılaştırma Sonuçları

Metrik		Yöntem (Ortalama)	(Sandhu ve ark., 2024)	(Dey ve ark., 2025)	(He ve ark., 2024)	(Aiswarya & Gomathi, 2023)	(Aparna & Madhumitha, 2023)	(Wu ve ark., 2024)	(Abdulijalel ve ark., 2022)	(Ghosh ve ark., 2025)
Entropi		7,2459	7,9981	7,4524	-	-	7,4818	7,9944	7,4467	-
Korelasyon	**Yatay**	0,9416	-	0,9607	0,8786	0,9320	0,9088	-	-0,9980	-
	Dikey	0,9680	-	0,9790	0,6764	0,9542	0,9170	-	-0,9710	-

	Diagonal	0,9126	-	0,9366	0,9106	0,9001	0,8571	-	-0,9690	-
SSIM		0,99996	-	0,9994	-		0,9975	0,9894	0,9994	0,9980
NPCR (%)		99,4375	-	99,97	-	99,7988	99,6277	99,6089	-	24,912
UACI (%)		33,9978	-	32,2094	-	28,2563	33,5462	33,5712	-	0,0980
PSNR (dB)		70,6318	78,871	52,07	62,440	46,8371	55,8591	43,0618	58,7705	54,1700
MSE		0,0750	0,0001	0,0048	-	0,0715	0,1687	-	0,0863	0,2500
Görüntü Boyutu		256x256	024x1024	512x512	12x768	256x256	512x512	512x512	512x512	512x512

Önerilen yöntemde, PSNR değeri açısından 70,6318 dB gibi oldukça yüksek bir skor elde edilmiştir. Bu değer, karşılaştırılan yöntemlerin büyük çoğunluğundan önemli ölçüde daha başarılıdır. Sadece (Sandhu ve ark., 2024) tarafından sunulan 78.871 dB'lik değer, önerilen yöntemden daha başarılı olmuştur. Ancak önerilen yöntemdeki yüksek PSNR değeri, veri eklenmiş görüntü ile orijinal görüntü arasında çok düşük bir bozulma olduğunu ve dolayısıyla veri eklenmiş görüntüde yüksek bir kalitenin olduğunu işaret etmektedir. Bununla birlikte MSE değeri 0,0750 olarak hesaplanmıştır. MSE değerinin düşük olması yöntemin oldukça başarılı olmasına işarettir. Yöntemde elde edilen MSE değeri bazı yöntemlere göre oldukça düşük çıkmıştır. Bu durumda yöntemin oldukça başarılı olduğu anlamına gelmektedir. SSIM metriği ile elde edilen 0,99996 değeri literatürdeki yöntemler ile karşılaştırıldığında oldukça başarılı bir sonuç elde edilmiştir. Bu durum veri gizlenmiş görüntünün orijinal görüntüde oldukça benzer olduğunu ve insan gözüyle fark edilmesinin son derece güç olduğunu işaret etmektedir.

NPCR değeri %99,4375 olarak bulunmuştur. Bu değer, ideal %99,61 değerine oldukça yakındır ve önerilen yöntemin, orijinal görüntüdeki küçük bir değişikliğe karşı veri gizlenmiş görüntüde yüksek oranda piksel değişikliği ürettiğini göstermektedir. Bu özellik, diferansiyel saldırılara karşı iyi bir direnç sapladığı anlamına gelmektedir. Bununla birlikte UACI değeri %33,9978 olarak hesaplanmıştır. Bu değer, ideal %33,46 değerine oldukça yakındır ve veri gizlenmiş görüntüdeki değişimlerin ortalama yoğunluğunun istenen seviyede olduğunu göstermektedir. Literatür çalışmalarına bakıldığında bazı yöntemlerin ideal değerden oldukça uzak olduğu görülmektedir. Önerilen yöntemindeki UACI değeri ise ideal değere çok yakın ve oldukça başarılıdır.

Önerilen yöntem entropi testi üzerinden karşılaştırıldığında yöntemde 7,2459 olarak elde edilmiştir. Elde edilen değer veri gizlenmiş görüntüden elde edilen değerdir. Bu değer Tablo 3'de verilen değerler ile karşılaştırıldığında veri gizlenmiş görüntünün orijinal görüntü ile oldukça benzer olduğu ve yöntemin başarılı olduğu anlamına gelmektedir. Entropi karşılaştırmasının ilgili yöntemdeki orijinal görüntüler ve veri gizlenmiş görüntüler arasında yapılması daha doğru olacaktır. Bu nedenle literatürde yer alan yöntemlerde de oldukça başarılı sonuçlar elde edilmiştir.

Korelasyon katsayıları incelendiğinde, önerilen yöntemin değerleri benzer çalışmalara göre oldukça başarılı olduğu görülmektedir. İdeal olarak, güvenli bir veri gizleme yönteminde komşu pikseller arasındaki korelasyonun düşük olması beklenmektedir. Bununla birlikte istatistiksel saldırılara karşı dayanıklı olabilmesi içinde orijinal ve ver gizlenmiş görüntülerin korelasyon değerlerinin birbirlerine çok yakın olması beklenmelidir. Önerilen yöntemin korelasyon katsayıları, literatürde yer alan benzer çalışmalar incelendiğinde bazı yöntemlerden oldukça iyi bazı yöntemlerden ise daha düşük olduğu görülmektedir. Bununla birlikte orijinal ve veri gizlenmiş görüntülere ait Tablo 4 ve Tablo 5' de verilen katsayılar karşılaştırıldığında ise çok ciddi farkların olmadığı ve istatistiksel saldırılara karşı oldukça dayanıklı olduğu söylenebilecektir.

Sonuç olarak önerilen yöntem, özellikle SSIM, PSNR, NPCR ve UACI metriklerinde son derece başarılı sonuçlar ortaya koymaktadır. SSIM değerinde en iyi performansı sergilemesi ve PSNR değerinin literatürdeki birçok çalışmadan üstün olması, önerilen yöntemin yüksek kalitede ve fark edilemez veri gizlenmiş görüntüler üretebildiğini göstermektedir. UACI değerinin ideale çok yakın olması da önemli bir avantajdır. Bununla birlikte, entropi değerinin bazı yöntemlere göre daha düşük olması ve özellikle komşu pikseller arası korelasyon katsayılarının yüksekliği, yöntemin istatistiksel özelliklerinin ve dolayısıyla bazı istatistiksel saldırılara karşı direncini artırma potansiyeli olduğunu göstermektedir. Önerilen yöntem, yüksek algılanamazlık ve iyi bir sağlamlık profili sunarak umut verici bir performans sergilemektedir. Gelecekteki çalışmalarda, entropi ve korelasyon metriklerinde iyileştirmeler hedeflenerek yöntemin güvenlik özellikleri daha da güçlendirilebilir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada, dijital görüntülerde veri gizleme amacıyla kullanılan geleneksel LSB yönteminin güvenlik açıklarını gidermek ve performansını artırmak için Kaotik Çadır Haritası (CTM) ve SHA-256 algoritmasını entegre eden yeni bir steganografi tekniği önerilmiştir. Önerilen yaklaşım, kullanıcıya ait gizli anahtarın SHA-256 ile anahtarlanması, gizlenecek mesajın uzunluğunun bu anahtar değeri içerisine gömülmesi, CTM ile üretilen kaotik dizilerin hem mesaj bitlerinin gömüleceği piksel konumlarını rastgele seçmek hem de mesaj bitlerini XOR işlemiyle şifrelemek için kullanılması gibi çok katmanlı bir güvenlik mekanizması sunmaktadır. Yapılan kapsamlı deneysel analizler, önerilen yöntemin başarısını birçok açıdan doğrulamıştır. Histogram analizleri ve SSIM değerleri, veri gizleme işlemi sonrasında veri gizlenmiş görüntülerde insan gözüyle algılanabilir bir bozulma olmadığını, görsel kalitenin yüksek seviyede korunduğunu göstermiştir. Entropi ve komşu pikseller arası korelasyon testleri, orijinal ve veri gizlenmiş görüntülerin istatistiksel özelliklerinin birbirine çok yakın olduğunu, bu durumun da yöntemin steganaliz saldırılarına karşı direncini artırdığını ortaya koymuştur. NPCR ve UACI test sonuçları, yöntemin diferansiyel saldırılara karşı duyarlılığının düşük olduğunu, yani görüntüdeki minimal değişikliklerin bile öngörülemeyen sonuçlar doğurduğunu ve veri güvenliğini sağladığını kanıtlamıştır. Ayrıca,

yöntemde kullanılan kaotik süreçlerin rastgeleliği NIST test paketi ile teyit edilmiş ve tüm testlerden başarıyla geçmiştir. Doğru anahtar olmadan gizli veriye erişimin mümkün olmadığı da gösterilmiştir. Sonuç olarak, sunulan bu yeni steganografi tekniği, LSB yönteminin basitliği ve yüksek gömme kapasitesi avantajlarını korurken, kaotik sistemlerin öngörülemezlik ve rastgelelik özelliklerinden faydalanarak güvenlik seviyesini önemli ölçüde artırmaktadır. Bu çalışma, görüntü steganografisi alanında daha güvenli ve dayanıklı veri gizleme yöntemleri geliştirilmesine katkı sağlamakta ve kaotik sistemlerin bu alandaki potansiyelini bir kez daha vurgulamaktadır. Gelecek çalışmalarda, önerilen yöntemin farklı kaotik haritalarla ve daha karmaşık steganaliz tekniklerine karşı performansı incelenebilir.

Yazarların Katkısı
Yazarların makaleye katkıları eşit orandadır

Çıkar Çatışması Beyanı
Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır.

Araştırma ve Yayın Etiği Beyanı
Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

KAYNAKÇA

Abd, A., & Hussein, E. (2022). Design secure multi-level communication system based on duffing chaotic map and steganography. *Indonesian Journal of Electrical Engineering Computer Science*, *25*(1), 238-246.

Abduljaleel, I. Q., Abduljabbar, Z. A., Al Sibahee, M. A., Ghrabat, M. J. J., Ma, J., & Nyangaresi, V. O. (2022). A lightweight hybrid scheme for hiding text messages in colour images using LSB, Lah transform and Chaotic techniques. *Journal of Sensor Actuator Networks*, *11*(4), 66.

Aiswarya, S., & Gomathi, R. (2023). Chaos Based Cryptography and Rectangular Shape Based Steganography Technique Using LSB. *Malaysian Journal of Computer Science*, *36*(4), 368-380.

Al-Sulami, Z. A., & Hashim, H. S. (2021, May, 26–27). Review of secure the online multimedia data using chaotic map and steganography techniques. AIP Conference Proceedings, Al-Samawa, Iraq.

Alabaichi, A., & Altameemi, A. A. (2022). Steganography encryption secret message in video raster using DNA and chaotic map. *Iraqi Journal of Science*, 5534-5548.

Aparna, H., & Madhumitha, J. (2023). Combined image encryption and steganography technique for enhanced security using multiple chaotic maps. *Computers Electrical Engineering*, *110*, 108824.

Arabboev, M., Begmatov, S., Rikhsivoev, M., Nosirov, K., & Saydiakbarov, S. (2024). A comprehensive review of image super-resolution metrics: classical and AI-based approaches. *Acta IMEKO*, *13*(1), 1-8.

Bhandari, M., Panday, S., Bhatta, C. P., & Panday, S. P. (2022, February, 23-25). Image steganography approach based ant colony optimization with triangular chaotic map. 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Gautam Buddha Nagar, India

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), 727-752.

Dalal, M., & Juneja, M. (2021a). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. *Multimedia Tools Applications*, *80*(4), 5723-5771.

Dalal, M., & Juneja, M. (2021b). A survey on information hiding using video steganography. *Artificial Intelligence Review*, *54*(8), 5831-5895.

Dey, D., Jana, D. K., & Bhunia, P. (2025). A Novel Approach to Steganography Security: Embedding Encrypted Text in Color Images Using Langton's Ant Cellular Automaton and Hybrid Chaotic Map. *SN Computer Science*, *6*(5), 402.

Durafe, A., & Patidar, V. (2024). Image steganography using fractal cover and combined chaos-DNA based encryption. *Annals of Data Science*, *11*(3), 855-885.

El-Khamy, S. E., Korany, N. O., & Mohamed, A. G. (2020). A new fuzzy-DNA image encryption and steganography technique. *IEEE Access*, *8*, 148935-148951.

Elshoush, H. T., & Mahmoud, M. M. (2023). Ameliorating LSB using piecewise linear chaotic map and one-time pad for superlative capacity, imperceptibility and secure audio steganography. *IEEE Access*, *11*, 33354-33380.

Ghosh, B. R., Mandal, J. K., & Banerjee, S. (2025). A high capacity multi-level LSB image steganographic technique using integer wavelet transform and tent map. *International Journal of Computers Applications*, 1-33.

Güvenoğlu, E. (2024). An image encryption algorithm based on multi-layered chaotic maps and its security analysis. *Connection Science*, *36*(1), 2312108.

Güvenoğlu, E., & Razbonyalı, C. (2019). The creation of maze in order to hide data, and the proposal of method based on AES data encryption algorithm. *El-Cezeri*, *6*(3), 668-680.

Güvenoğlu, E., & Tüysüz, M. A. A. (2015, May, 16-19). An improvement for Knutt/Durstenfeld algorithm based image encryption. 23nd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey.

Hameed, S. M., Ali, Z. H., AL-Khafaji, G. K., & Ahmed, S. (2021). Chaos-based Color Image Steganography Method Using 3 D Cat Map. *Iraqi Journal of Science*, 3220-3227.

He, D., Cai, Z., Zhou, D., & Chen, Z. (2024). Inter-channel correlation modeling and improved skewed histogram shifting for reversible data hiding in color images. *Mathematics*, *12*(9), 1283.

Hematpour, N., Ahadpour, S., Sourkhani, I. G., & Sani, R. H. (2022). A new steganographic algorithm based on coupled chaotic maps and a new chaotic S-box. *Multimedia Tools Applications*, *81*(27), 39753-39784.

Huo, L., Chen, R., Wei, J., & Huang, L. (2024). A high-capacity and high-security image steganography network based on chaotic mapping and generative adversarial networks. *Applied Sciences*, *14*(3), 1225.

Karawia, A. (2021). Medical image steganographic algorithm via modified LSB method and chaotic map. *IET Image Processing*, *15*(11), 2580-2590.

Karimov, T. I., Druzhina, O. S., Andreev, V. S., Tutueva, A. V., & Kopets, E. E. (2021, January, 26-29). Bifurcation spectral diagrams: A tool for nonlinear dynamics investigation. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia.

Khaleel, A. H., & Abduljaleel, I. Q. (2021). Secure image hiding in speech signal by steganography-mining and encryption. *Indonesian Journal of Electrical Engineering Computer Science*, *21*(3), 1692-1703.

Khalil, N., Sarhan, A., & Alshewimy, M. A. (2024). A secure image steganography based on LSB technique and 2D chaotic maps. *Computers Electrical Engineering*, *119*, 109566.

Kustov, V., & Krasnov, A. (2021, July, 26-28). Masking Hidden Messages under Noise in Steganography Problems. 44th International Conference on Telecommunications and Signal Processing (TSP), Brno, Czech Republic.

Liu, J., Wang, Y., Han, Q., & Gao, J. (2022). A sensitive image encryption algorithm based on a higher-dimensional chaotic map and steganography. *International Journal of Bifurcation Chaos*, *32*(01), 2250004.

Mansoor, S., & Parah, S. A. (2023). HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing. *Multimedia Tools Applications*, *82*(19), 28769-28796.

Mowafy, W. S., Zayyan, M. H., & El-Henawy, I. M. (2024). On Cryptanalysis Techniques in Chaos-based Cryptography. *Mansoura Journal for Computer Information Sciences*, *19*(1), 43-62.

Mudeng, V., Kim, M., & Choe, S.-w. (2022). Prospects of structural similarity index for medical image analysis. *Applied Sciences*, *12*(8), 3754.

Nagarajegowda, S., & Krishnan, K. (2023). An image steganography using improved hyper-chaotic Henon map and fractal tromino. *International Journal of Electrical Computer Engineering*, *13*(6), 6836-6846.

Nasr, M. A., El-Shafai, W., El-Rabaie, E.-S. M., El-Fishawy, A. S., El-Hoseny, H. M., Abd El-Samie, F. E., & Abdel-Salam, N. (2024). A robust audio steganography technique based on image encryption using different chaotic maps. *Scientific Reports*, *14*(1), 22054.

Odeh, A., Taleb, A. A., Alhajahjeh, T., Navarro, F., & Ayesh, A. (2025). Lightweight secure image encryption: a tent map chaos theory approach. *Multimedia Tools Applications*, 1-20.

Ping, P., Fan, J., Mao, Y., Xu, F., & Gao, J. (2018). A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access*, *6*, 67581-67593.

Ramzan, M., & Khan, M. F. (2023). A Robust Steganographic Algorithm based on Linear Fractional Transformation and Chaotic Maps. *International Journal of Advanced Computer Science Applications*, *14*(3).

Rostam, H. E., Motameni, H., & Enayatifar, R. (2022). Privacy-preserving in the Internet of Things based on steganography and chaotic functions. *Optik*, *258*, 168864.

Salim, A., Abdulbasit Mohammed, K., Maath Jasem, F., & Makki Sagheer, A. (2024). Image steganography technique based on lorenz chaotic system and bloom filter. *International Journal of Computing Digital Systems*, *16*(1), 851-859.

Sandhu, M., Ahmed, M., Hussain, M., & Khan, I. (2024). Protecting Sensitive Images with Improved 6-D Logistic Chaotic Image Steganography. *International Arab Journal of Information Technology*, *21*(6).

Sharafi, J., Khedmati, Y., & Shabani, M. (2021). Image steganography based on a new hybrid chaos map and discrete transforms. *Optik*, *226*, 165492.

Singh, D., Kaur, S., Kaur, M., Singh, S., Kaur, M., & Lee, H.-N. (2024). A systematic literature review on chaotic maps-based image security techniques. *Computer Science Review*, *54*, 100659.

Sriram, G., Ali, A. M. A., Natiq, H., Ahmadi, A., Rajagopal, K., & Jafari, S. (2024). Dynamics of a novel chaotic map. *Journal of Computational Applied Mathematics*, *436*, 115453.

Vivek, J., & Gadgay, B. (2021). Video steganography using chaos encryption algorithm with high efficiency video coding for data hiding. *International Journal of Intelligent Engineering Systems*, *14*(5), 15-24.

Wu, W., Dong, Y., & Wang, G. (2024). Image Robust Watermarking Method Based on DWT-SVD Transform and Chaotic Map. *Complexity*, *2024*(1), 6618382.

Xie, H.-w., Gao, Y.-j., Liu, X.-l., Zhang, J., & Zhang, H. (2022). A novel exploiting modification direction scheme and its application in quantum color image steganography. *Quantum Information Processing*, *21*(7), 249.

Yakut, S. (2024). An Efficient Steganography Method Based on Chaotic Functions and XOR Operation for Data Hiding. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, *5*(2), 58-65.

Yamni, M., Daoui, A., & Abd El-Latif, A. A. (2024). Efficient color image steganography based on new adapted chaotic dynamical system with discrete orthogonal moment transforms. *Mathematics computers in simulation*.

Zhang, L., Song, X., El-Latif, A. A. A., Zhao, Y., & Abd-El-Atty, B. (2024). Reversibly selective encryption for medical images based on coupled chaotic maps and steganography. *Complex Intelligent Systems*, *10*(2), 2187-2213.