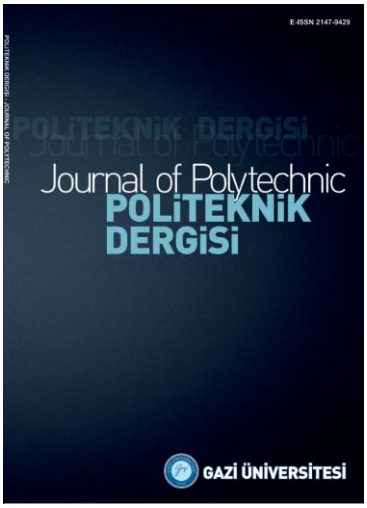


POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

K-en az anlamlı bitlere dayalı kaotik bir harita kullanan renkli görüntü steganografisi

A color image steganography using a chaotic map based on k-least significant bits

***Yazar(lar) (Author(s))**: Hidayet ÇELİK[1], Nurettin DOĞAN[2]*

ORCID[1]: 0000-0002-9898-6925

ORCID[2]: 0000-0002-8267-8469

To cite to this article: Çelik H. ve Doğan N., "K-en az anlamlı bitlere dayalı kaotik bir harita kullanan renkli görüntü steganografisi", ***Journal of Polytechnic***, 26(2): 679-692, (2023).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Çelik H. ve Doğan N., "K-en az anlamlı bitlere dayalı kaotik bir harita kullanan renkli görüntü steganografisi", ***Politeknik Dergisi***, 26(2): 679-692, (2023).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: **10.2339/politeknik.1008594**

K-En Az Anlamlı Bitlere Dayalı Kaotik Bir Harita Kullanan Renkli Görüntü Steganografisi

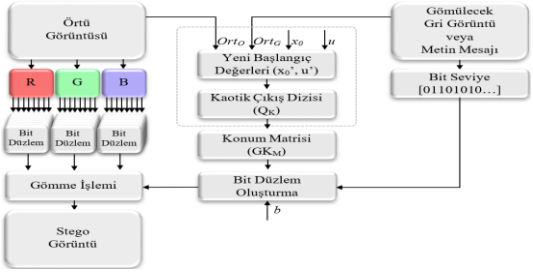
A Color Image Steganography Using A Chaotic Map Based On K-Least Significant Bits

Önemli noktalar (Highlights)

- *1B lojistik harita ile kaotik yapı oluşturma / Creation of chaotic structure with 1D logistic map*
- *Renkli görüntü kanallarına yazı veya görüntü gizleme / Hiding text or image in channels of color image*
- *En az önemli k-bitleriyle gizli veri taşıma / Carrying secret data with the least significant k-bits*

Grafik Özet (Graphical Abstract)

Bu çalışmada, kaotik harita kullanılarak bir renkli görüntü steganografisi önerilmiş ve bu yöntem uygulamalı olarak anlatılmıştır. / In this study, a color image steganography using a chaotic map has been proposed and this method has been descriped with application.



Şekil. Önerilen yöntemin blok diyagramı **/ Figure.** Block diagram of the proposed method

Amaç (Aim)

Renkli bir görüntü üzerine yüksek veri gömme kapasitesine sahip saldırıya dayanıklı bir steganografi yöntemi amaçlanmaktadır. / An attack-resistant steganography method with high data embedding capacity on a color image is aimed.

Tasarım ve Yöntem (Design & Methodology)

Gizlenecek veri genişletilmiş 1 boyutlu lojistik harita kullanılarak rastgele dağıtılır ve ardından renkli kapak görüntüsünde en az anlamlı k-bit ile değiştirilir. / The data to be hidden is randomly distributed using the expanded 1D logistic map and then replaced with the least significant k-bit in the colored cover image.

Özgünlük (Originality)

Bit düzlem sayısı algoritmanın başında seçilmektedir. Maksimum 4 bit düzlemde veri gömme işlemi yapılabilmektedir. Kaotik haritanın başlangıç değerleri hem kapak görüntüsüne hem de gizlenecek veriye göre ayarlanır. / The number of bit planes is selected at the beginning of the algorithm. Data embedding can be done in a maximum of 4 bit planes. The initial values of the chaotic map are set according to both the cover image and the data to be hidden.

Bulgular (Findings)

Yüksek veri gömme kapasitesi ve veri güvenliği sağlanmıştır. Düşük kapasiteli veri, maksimum gömme kapasitesi kullanılmadan gizlendiğinde, stego görüntüde yüksek algılanamazlık elde edilmiştir. / High data embedding capacity and data security have been offered. When the data with a low capacity is hidden without using the maximum embedding capacity, high imperceptibility has been achieved in the stego image.

Sonuç (Conclusion)

Elde edilen test sonuçları doğrultusunda önerilen algoritmanın görüntü steganografi işlemlerinde kullanılabileceği uygun görülmektedir. / According to test results, it seems appropriate that the proposed algorithm can be used in image steganography operations.

Etik Standartların Beyanı (*Declaration of Ethical Standards*)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler. / The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

K-En Az Anlamlı Bitlere Dayalı Kaotik Bir Harita Kullanan Renkli Görüntü Steganografisi

Araştırma Makalesi / Research Article

Hidayet ÇELİK, Nurettin DOĞAN*

Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Selçuk Üniversitesi, Türkiye

(Geliş/Received : 12.10.2021 ; Kabul/Accepted : 30.12.2021 ; Erken Görünüm : 12.01.2022)

ÖZ

Günümüzde dijital iletişim içerisinde bilginin güvenliği çok önemli bir yer tutmaktadır. Uçtan uca iletişimlerde önemli bilgilerin şifrelenmesi veya bir taşıyıcı üzerine gömülerek gizlenmesi bilgi güvenliği için kullanılan yöntemlerinin başında gelir. Bazı durumlarda güvenliği artırmak için yöntemler karma bir şekilde kullanılıp bilgi iletişim kanalları içerisine bırakılabilir. Bu yöntemlerdeki ortak amaç, kaynaktan çıkan önemli bilgilerin, iletişimde ilgisi olmayan kişilerin eline geçmeden veya anlaşılmaz şekle dönüştürülerek hedefe gönderilmesidir. Bu çalışmada, steganografi ile ilgili temel bilgiler verildikten sonra önerilen renkli görüntü gizleme yöntemi anlatılmıştır. Yöntemde, önce gizlenecek görüntü veya metindeki veriler genişletilmiş 1B lojistik harita kullanılarak rastgele dağıtılmış ardından renkli örtü görüntüsündeki en az anlamlı k-bit ile değiştirilmiştir. Gizlenmek istenen bilgi şifrelenerek bilgi güvenliğinin artırılması hedeflenmiştir. Yöntemin başarısı, bilginin saklanacağı bit düzlem sayısına göre farklı boyutlarda görsel ve metinler üzerinde denenmiştir. Önemli güvenlik değerlendirme kriterlerinden PSNR ve MSE ölçütleri incelenmiştir. 1 bit düzlemin kullanıldığı 75x100 boyutlarındaki görselin gizlendiği işlemde PSNR 54.4359, MSE 0.23415, 7500byte metnin gizlendiği işlemde PSNR 56.7213, MSE 0.13834 olarak hesaplanmıştır. 4 bit düzlemin kullanıldığı 150x150 boyutlarındaki görselin gizlendiği işlemde PSNR 36.503, MSE 14.5472, 22500byte metnin gizlendiği işlemde PSNR 38.657, MSE 8.8585 olarak hesaplanmıştır. Deneysel sonuçlarla, algoritmanın iyi bir performansa sahip olduğu, istatistiksel analiz saldırılarına karşı iyi bir performans gösterdiği kanıtlanmıştır.

Anahtar Kelimeler: Steganografi, renkli görüntü şifreleme, en önemsiz bit, kaotik harita, veri güvenliği.

A Color Image Steganography Using A Chaotic Map Based On K-Least Significant Bits

ABSTRACT

Nowadays, information security has a very important place in digital communication. Encrypting important information in end-to-end communications or hiding it by embedding it on a carrier is one of the methods used for information security. In some cases, methods are used in a mixed manner to increase security. An encrypted information can be hidden on the carrier or a hidden information can be encrypted and released into communication channels. The common purpose of these methods is to send the important information from the source to the target by transforming it into an incomprehensible form or before it gets into the hands of unrelated people.In this study, after giving brief information about steganography, the proposed color image hiding method is explained. In this method, first the data in the image or text to be hidden is randomly distributed using an expanded 1D logistic map, and then replaced with the least significant k-bits (K-LSB) in the colored cover image. It is aimed to increase information security by encrypting the information that is desired to be hidden. The success of the method is tested on images and texts of different sizes according to the number of bit planes in which the information will be stored. PSNR and MSE criteria, which are important safety evaluation criteria, are examined. PSNR and MSE are calculated as 54.4359, 0.23415 respectively in the process of hiding the 75x100 image using 1 bit plane, by the way PSNR and MSE are calculated as 56.7213, 0.13834 respectively in the process of hiding the 7500byte. PSNR and MSE are calculated as 36.503, 14.5472 respectively in the process of hiding the 150x150 image using 4 bit plane, by the way PSNR and MSE are calculated as 38.657, 8.8585 respectively in the process of hiding the 22500byte. With experimental results, it is proven that the algorithm has good performance, good performance against statistical analysis attacks.

Keywords: Steganography, color image encryption, least significant bit, chaotic map, data security.

1. GİRİŞ (INTRODUCTION)

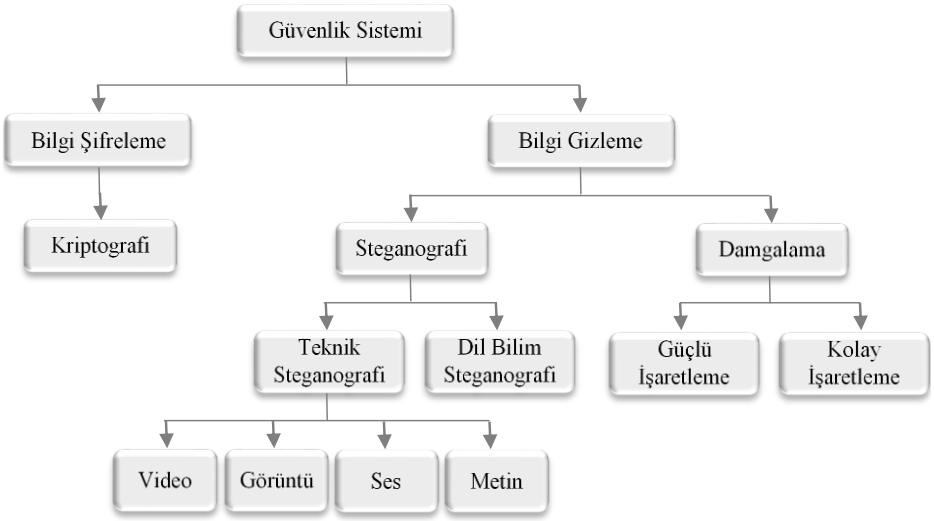
Günümüz internet çağında bilgiye erişim eskisi gibi zor ve zaman alan bir süreç olmaktan çıkıp alakalı alakasız milyonlarca sonucun saniyeler içinde ekranlarımıza düştüğü bir yenilik olarak karşımıza gelmiştir. Teknolojinin insan yararına olan her gelişiminde işler biraz daha kolaylaşmış, emek ve çaba harcamadan işleryoluna koyulmuştur. En basitinden bir örnek ile anlatmak gerekirse, haberleşmede posta kutularının dijital ortama taşınmasıyla, gönderen ve alıcı arasındaki iletişimde mektup ve postane gibi somut kavramlar ortadan kalkmış, saniyeler içinde iletişimlerin gerçekleştiği, yazılı mesajın yanı sıra ses ve görüntülerin de anlık bir şekilde ilgili hedeflere yönlendirildiği bir hale evrimleşmiştir.

*Sorumlu Yazar (Corresponding Author)
e-posta : ndogan@ymail.com

Çoğu zaman bu mesajların içerisinde önemli bilgi içeren veriler de gönderilmektedir. Tabi ki göndericinin, herkesin ortak kullandığı iletişim kanallarında önemli verilerinin bulunmasını veya erişilmesini istememesi gibi doğal bir hakkı vardır. Çünkü bu ortamda kötü niyetli saldırganların bulunduğu gerçeği kadar, saldırganların da o önemli bilgi içeren veriye ulaşmak ve önemli bilgiyi elinde bulundurmak isteyeceği de tartışmasız kesindir.

Bu durumda önemli bilginin güvenliğini sağlamak için bilgiyi şifreleme ya da gizleme işlemlerine başvurulur [1]. Kriptoloji, kriptografiyi (şifre bilimi) ve kripto analizi (şifre analizi) içeren bir bilim dalıdır [2]. Bilgi şifreleme temelde Yunanca Crypto ve Logos kelimelerinden meydana gelen ve anlamca gizleme bilimi olan Kriptoloji ana başlığında toplanmaktadır. Kriptografinin ana amacı bilgi güvenliğinin sağlamak için verileri gizli verilere dönüştürme işleminin yapılmasıdır [2,3]. Bilgi gizleme steganografi ve damgalama olarak iki grup altında toplanır. Yunanca Stegos ve Grapha kelimelerinden oluşan steganografi, mesajın varlığını kendi içinde saklayan örtülü yazı anlamındadır [4-6]. Uygulama yöntemleri aynı olmasına rağmen steganografi ve damgalamanın kullanım amaçları farklıdır. Steganografide bilginin gizlenmesi esas iken, damgalama dijital içeriklerin fikri mülkiyet haklarını korumak için uygulanır [1,4,7-9]. Kriptografi ve steganografide ise uygulamada farklı yöntemler kullanılsa da, sonuçta bilgi gizleme amaçlanmaktadır [4, 10-12]. Kriptografide şifrelenmiş bilgi açıkça belli olduğu için bu durum saldırganların dikkatini çekecek ve saldırganlar gizli bilgiye ulaşma arzusunda olacaklardır. Steganografide ise bilgi bir taşıyıcı içerisine gömüldüğü için çoğu zaman saldırganların dikkatinden kaçma ihtimali yüksektir.

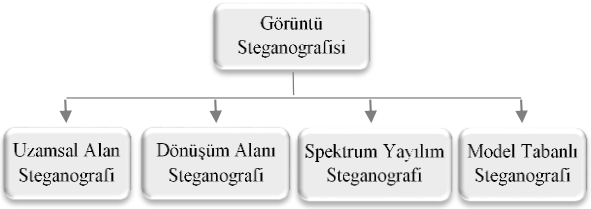
Bilgi güvenliği için kullanılan yöntemleri Şekil 1'deki ana başlıklar altında gruplandırabiliriz [8,13].



Şekil 1. Temel Güvenlik Sistemi (Basic Security System)

Steganografide iletim ortamı yani taşıyıcı, bir görüntü, video, ses veya metin dosyası olabileceği gibi, ağ protokolü veya DNA yapısı da olabilir. Bu ortamlar bilgiyi gizlemek için kendilerine ait karakteristik özelliklerini kullanırlar. Örneğin, ses dosyalarında faz veya spektrum yayılması, ağ protokolünde paket içeriği veya paket başlığı, görüntü dosyalarında piksel değerleri bilgi gizlemek için kullanılan özelliklerdir [8]. Bu ortamlar arasında literatürde üzerinde en çok çalışılan görüntü dosyalarıdır. Bu çalışmada da görüntü içerisine bilgi gizleme üzerinde durulacaktır.

Görüntü steganografisinde, gizli bilgiyi taşıyan ortam bir görüntü dosyasıdır. Şekil 2'de gösterildiği gibi, uzamsal alanı, dönüşüm alanı, spektrum yayılımı ve model tabanlı olmak görüntü içerisinde bilgi gizleme teknikleri kullanılmaktadır [8].



Şekil 2. Görüntü Steganografi Teknikleri (Image Steganography Techniques)

Uzamsal alan steganografisinde, gizli bilgi doğrudan görüntünün piksel değerlerine gömülmektedir. Dönüşüm alanı steganografisinde, görüntü dönüşüm yöntemlerinden birisi ile uzamsal alandan frekans alanına dönüştürüldükten sonra gizli bilgi gömme işlemi gerçekleştirilir. Spektrum yayılım steganografisinde, görüntüyü elde etme sürecine özgü gürültünün içine gizli bilgi yerleştirilir. Model tabanlı steganografi ise

görüntünün istatistiksel özellikleri dikkate alınır ve buna göre gizli bilgi gömme işlemi yapılır [8]. Görüntü steganografisinde bilgi gizleme yöntemi üç başlık altında değerlendirilir: **Kapasite;** maksimum veri gömme yoğunluğu, **Algılanamazlık;** gizli bilgi içeren görüntünün, taşıyıcı görüntüye benzerlik oranı, **Sağlamlık;** gizli bilgi içeren görüntünün saldırılara karşı direnci. İdeal bir steganografi yönteminin, bu üç başlığı aynı anda yerine getirmesi beklenir. Fakat bunu sağlamak zor bir olaydır. Çoğu zaman yüksek veri gömülen bir görüntü, hem benzerlik açısından taşıyıcı görüntüsünden uzaklaşabilmekte hem de saldırılara karşı savunmasız kalabilmektedir. Aynı zamanda taşıyıcı görüntüyle yüksek benzerlik sunan bir bilgi gizleme işleminde gömülecek veri kapasitesi düşük olabilmektedir.

Bu çalışmada yüksek veri gömme kapasitesi sağlayan LSB (Least Significant Bit - En Az Anlamlı Bit) yöntemi üzerinde çalışılacaktır. Gizli veri gömülecek örtü görüntüsü RGB kanallarında bit düzlemlere ayrılacak ve verinin gömüleceği bit düzlemleri seçilecektir. Gizli verinin maksimum en az anlamlı 4 bite gömülmesine izin verilecektir. Steganografi ile birlikte kriptografi de kullanılarak gizli verilerin güvenliğini artırmak hedeflenmiştir. Bunu gerçekleştirebilmek için veri gömülmeden önce genişletilen 1B lojistik harita ile oluşturan rasgele konumlara gizli verinin biti ve bit düzlemdeki bit XOR işlemine tabi tutularak işlem gerçekleştirilecektir. Deneysel sonuçlarla performans analizi ve literatürdeki bazı yöntemlerle kıyaslamalar yapılacaktır.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

Bu bölümde, son 10 yılda literatürdeki bazı LSB ve BPCS (Bit Plane Complexity Segmentation - Bit Düzlemi Karmaşıklık Dilimleme) steganografi yöntemleri üzerine çalışılmış algoritmalara ve bu algoritmaların özelliklerine değinilmiştir.

Wang vd., gizli verilerin kapasitesini geliştirmek ve algılanamayan gizli görüntü kalitesi sağlamak için, LSB değiştirme ve Hamming koduna (HLAH) dayalı hibrit bir steganografi yöntemi önerdiler. Bu yöntemde, görüntünün kenar bölgelerine daha fazla bilgi gömülürken, pürüzsüz bölgelere daha az bilgi gömüldü. Diğer yöntemlerden daha fazla gömme kapasitesine ve yüksek görüntü kalitesine ulaşıldı [14].

Elharrouss vd., LSB kodlamasına dayalı olarak, görüntüyü gizlemek için en az k bit kullanan k-LSB tabanlı bir yöntem önerdiler. Gizli görüntüyü çözme işleminde, blokların gizli görüntüyü içerdiğini bilmek için bir bölge algılama işlemi kullanıldı. Önerilen yaklaşımın etkinliği bazı LSB yöntemleriyle karşılaştırıldı [15].

Rachael vd., tatmin edici bir gizlilik ve güvenlik önlemi sunmak için steganografi ile kriptografiyi birleştirdiler. 1 baytlık en az anlamlılık tekniğini geliştiren en az anlamlı bit steganografisi için yeni bir yaklaşım önerildi [16].

Shehzad ve Dag, blok matris determinant yöntemine dayalı bir görüntü steganografi tekniği önerdiler. Örtü görüntüsünü 2x2 bloklara böldükten sonra, her bloğun determinantını hesaplandı. Determinant değerlerinin ve karşılık gelen veri bitlerinin karşılaştırılması, veri bitlerinin gömülmesi için hassas bir yol sağladı. Önerilen teknikle, örtü görüntü kalitesini etkilemeden bir görüntü içinde gizli verilerin gizlenmesi amaçlandı [17].

Ali vd., gizli bilginin bir pikselin rastgele bit pozisyonuna gömüldüğü en az anlamlı bit yer değiştirmesi ile bir görüntü steganografisi yaklaşımı önerdiler. Yüksek PSNR (Peak Signal to Noise Ratio - Tepe Sinyal Gürültü Oranı) ve MSE (Mean Squared Error - Ortalama Kare Hata) değerleri ile algılanamazlık ve sağlamlık açısından yüksek performans sağlandı [18].

Bhuiyan vd., görüntü steganografisi için uzamsal alanda oldukça güvenli bir veri gizleme tekniği önerdiler. Yöntemde, mesaj biti ve her RGB bileşeninin 7. biti XOR işlemine tabi tutulduktan sonra üretilen çıktı, her RGB bileşeninin 8. biti içine gömüldü. Deneysel sonuçlarda, daha az algılanamazlık ve daha fazla güvenlik anlamına gelen çok iyi PSNR ve MSE oranı elde edildi [19].

Kuşuma vd., görüntü güvenliğini artırmak için kriptografi ve steganografi tekniğini birlikte kullandılar. Arnold (ACM-Arnold Cat Map) algoritmasını RSA (Rivers Shamir Adleman) algoritmasıyla birleştirip, ardından örtü görüntüsünün bit düzlemindeki iki biti mesaj bitleriyle değiştirdi. Geliştirilen yöntemle iki katı kapasite sağlandı. PSNR ve entropi parametreleri ile stego görüntülerin kalitesi değerlendirildi [20].

Zhou vd., kuantum görüntülerinin NEQR temsiline ve en az anlamlı bit şemasına dayanan bir kuantum görüntü steganografi yöntemi önerdiler. Önce, orijinal bilgi görüntüsünü karıştırmak için bit düzlemi karıştırma yöntemi kullanıldı. Ardından, karıştırılan görüntü, yalnızca operatörün bildiği anahtar ile örtü görüntüsüyle aynı boyuta getirildi ve Arnold karıştırma ile anlamsız bir görüntü olacak şekilde karıştırıldı. Gömme işlemi ve çıkarma işlemi operatör kontrolünde olan iki anahtarla gerçekleştirildi. Deneylerle yöntemin iyi bir görsel kaliteye sahip olduğu ve güvenliğin mükemmel olduğu söylendi [21].

Nguyen vd., örtü görüntüsünün düzgün bölgelerine ait piksellere gizli mesaj gömüldüğünde görsel olarak meydana gelen bozulmadan yola çıkarak stego görüntülerin kalitesini iyileştirmek için kenar tabanlı yaklaşım üzerine çalıştılar. Geliştirdikleri yöntemde birden fazla bit düzlemi kullandı ve örtü görüntüsünün karmaşık bölgelerini seçmek için uyarlanabilir karmaşıklık eşiği hesaplaması uygulandı. Sonuç olarak gömme kapasitesini ve güvenlik performansını önceki yaklaşımlara kıyasla iyileştirildi [22].

Zhou vd., çalışmalarında bilgi gizleme güvenliğini artırmak için, bilgi gizleme ve kriptografiyi kullanarak, dijital imza ve şifreleme teknolojisine dayalı kimlik doğrulamayı birleştiren, gelişmiş bir LSB bilgi gizleme algoritması önerdiler. Deneysel sonuçlarda geliştirdikleri yöntemin daha iyi güvenlik ve daha yüksek tepe-sinyal

gürültü oranı (PSNR) ile genel LSB görüntü steganografi yönteminden iyi olduğu gösterildi [23].

Patel ve Meena, çalışmalarında taşıyıcı görüntünün en az anlamlı bitinin (LSB) modifikasyonu, gizli görüntünün en anlamlı biti (MSB-Most Significant Bit) tarafından yaptılar. Bilgi gizlemenin yanı sıra dinamik anahtar şifrelemesi ile güvenlik de sağlandı. Anahtarın dinamik özelliği, anahtarın döndürülmesiyle etkinleştirildi ve anahtarın her dönüşü yeni anahtar üretildi. Bu teknikte, stegano analitik saldırısına karşı çift katmanlı güvenlik sağlayan sözde rastgele sayı (PRN-Pseudo Random Number) bazında taşıyıcı görüntü ve gizli görüntünün piksel seçimi yapıldı [24].

Singh ve Singh, verileri gizlemek için kullanılan çoğu steganografi yöntemin gömme kapasitesinin az olduğunu, daha fazla veri gizlendiğinde görüntü kalitesinde ve gizli verinin güvenliğinde problemler olduğunu söyleyerek, bu problemlerin üstesinden gelmek için bilgiyi, görüntü kalitesini artıracak ve yüksek gömme kapasitesi sağlayacak şekilde RGB görüntüsünün üç düzlemine gömerek renkli görüntüler için geliştirilmiş bir LSB tekniği önerdiler [25].

Sun, çalışmasında BPCS steganografisinde, örtü görüntüsünde gürültülü bölgelerin yerleştirilmesi için siyah-beyaz kenar karmaşıklığı yönteminin kolay uygulanabilir olduğunu fakat özellikle periyodik desenler için her zaman kullanışlı olmadığını belirtti. Bu sorunu çözmek için çalışma uzunluğu düzensizliği ve kenar gürültüsü üzerinde durdu. Önerdiği yöntemde, nihai gömülü görüntünün orijinal görüntü ile aynı olduğu ve örtü görüntüsüne gürültü benzeri bölgelerin daha kesin olarak yerleştirildiği gösterildi [26].

Kumar vd, herhangi bir veri kaybı olmadan bit-düzlemleri kullanarak bilgiyi gizlemek ve mesajı son kullanıcıya ulaştırmak için bir teknik sundular. Kullanılan yöntemde, en düşük 3 veya 4 LSB, mesaj bitleri veya görüntü verileriyle değiştirildi. Steganaliz aracını kullanarak yöntem test edildi. Çözümleyicinin, son kullanıcıya gönderilen metni algılayamaması üzerine yöntemlerinin verimli olduğu söylendi [27].

Bansod vd., büyük miktarda veriyi depolamak için veri şifreleme RSA ve sıkıştırma DES (Data Encryption Standard - Veri Şifreleme Standardı) algoritmalarına dayalı hibrit şifreleme önerdiler. Önerdikleri algoritma, örtü görüntüsünün tüm bit düzlemlerindeki "gürültü benzeri" bölgeleri görüntü kalitesini bozmadan gizli verilerle değiştirebilen modifiye edilmiş BPCS steganografi tekniğidir. Yapılan deneylere göre, mesajlar örtü görselinde başarılı bir şekilde gizlendi. Ayrıca, yöntem büyük gömü kapasitesine sahip ve orijinal görüntü olmadan stego-görüntüden gizli bilgi çıkarılabilmektedir [28].

Daneshkhah vd., dijital görüntüye uzamsal alanda mesajı gizlemek için yeni bir yaklaşım sundular. Bu yaklaşımla, verilerin en az anlamlı bit dışındaki yerlere gömülmesinin mümkün olduğunu ve buna iyi bir plan eşlik ederse, steganaliz yöntemleriyle gizli verilerin tespitini çok daha zor hale getirebileceği öne sürüldü [29].

Bui vd., çalışmalarında piksel değeri farklılaştırma PVD (Pixel Value Differencing - Piksel Değeri Farklılaştırma) steganografisi ve BPCS steganografisinin, düz alanlarda bloklu efektler, gürültü üretme ve steganaliz ile tespit edilebilir olma zayıflığından bahsederek, bu zayıflıkların üstesinden gelmek için, gürültülü blokları seçerken sağlam bir ölçü kullanan, uzamsal alanda güvenli bir bit düzlemi tabanlı steganografi yöntemi sundular. Örtü görüntülerinin değişimini azaltmak için bir matris gömme tekniği de uygulandı. Önerilen yöntem, PVD ve BPCS steganografi yöntemleri ile karşılaştırıldı. Deneysel sonuçlar, önerilen yöntemin olası saldırılara karşı güvenli olduğu doğrulandı [30].

Kalita vd, iyi bir veri gizleme yöntemi sağlamak için görüntüyü dört alt banda ayıran IWT (Integer Wavelet Transform - Tamsayı Dalgacık Dönüşümü) kullandılar. Stego görüntüsünün kalitesini belirleyen LL (Low-Low - Düşük-Düşük) bandına dokunmadan diğer üç band ile işlem yapıldı. Gömülecek gizli bitlerin sayısını belirlemek için katsayı değeri farklılaştırma yaklaşımı uygulandı. Algoritmanın, yüksek kapasite, algılanamazlık ve sağlamlık açısından iyi bir performansa sahip olduğu gösterildi [31].

Nazari ve Ahmedi, renkli ve gri görüntüler üzerinde DCT (Discrete Cosine Transform-Ayrık Kosinüs Dönüşümü) kullanan bir steganografi yöntemi önerdiler. Yüksek kapasitesi ile çalışmaları ön plana çıkmıştır. Gömme işlemini önce orta frekansta (MF-Middle Frequency), sonra kapasiteyi artırmak için ortadan yükseğe (MHF-Middle to High) ve yüksekten ortaya (HMF-High to Middle) olmak üzere iki farklı zikzak tarama yöntemi ile yüksek frekansta yaptılar. Sonuçta, MF algoritmasıyla yüksek sağlamlık elde edilirken, HMF ve MHF algoritmalarında yüksek gömme kapasitesi elde edildi. Bunun yanında MHF algoritmasının gürültülere ve saldırılara karşı daha sağlam olduğunu gösterdiler [32].

Literatürdeki çalışmalardan da görülebileceği gibi görüntü üzerine veri gizlenirken farklı yöntemlere başvurulmuştur. LSB yöntemi yüksek veri gömme kapasitesi ve kolay kullanımı açısından çoğunlukla tercih edilmiş, bununla beraber araştırmacılar gömülecek bit seçimini ya da gömme işlemini yaparken çalışmalarını farklılaştıracak yöntemler kullanmışlardır. Bazı araştırmacılar çalışmalarında görüntü üzerinde bölge ya da kenar algılama yöntemlerini [14,15,22] kullanırken, bazıları rasgele sayı üreterek [18,24] seçilen piksellerin LSB bitine ya da bit düzlemlerine [21,22,26-28,30] gömme işlemi üzerine çalışmışlardır. Gri seviyeli örtü görüntüler üzerine [21,22,26] olduğu kadar renkli örtü görüntüleri üzerine de [18-20,23-25,28] veri gömme işlemi yapılmıştır. Bazı çalışmalarda gömü verisi bir metinken [18,19,22,25,28], bazı çalışmalarda bir görüntü [15,20,21,23,24,26] olmuştur. Kaotik yapılar kullanarak [20,21], kriptografi yöntemleriyle şifrelenerek [23,24,28] ya da frekans düzleminde [31,32] veri gömme işlemleri de gerçekleştirilmiştir.

Önerdiğimiz yöntemde, stego görüntüsünü elde etmek için gizli mesaj bitlerinin lojistik harita ile şifrelendikten sonra örtü görüntüsünün seçilen bit düzlemlerine XOR işlemiyle gizleneceği bir LSB değiştirme yaklaşımı sunulmuştur. Literatürdeki çalışmalardan farklı olarak, gizlenecek verinin, metin ya da görüntü verisi olacağı algoritma başında gömü işlemini yapacak kişi tarafından seçilecektir. Ayrıca gömme işleminde kullanılacak LSB bit sayısı da algoritma başında seçilecektir. Kullanılan kaotik harita ile oluşturulan konum matrisine göre gizlenecek verinin bitleri rasgele konumlandırılacaktır. Bu sayede bit düzlem incelenmesinde gizli verinin gürültü olarak görülmesi sağlanacaktır. Saldırganlar bit düzlemlerden gizli veriye dair açık bilgiye ulaşamayacaktır. Kaotik haritada kullanılan başlangıç değerleri, hem örtü görüntüsüne hem de gömü verisine bağlı olduğu için, bu değerlerdeki küçük değişiklikler şifre çözme işleminde büyük değişikliklere yol açacağı için gizli veri hakkında da en ufak bir bilgi vermeyecektir [33]. Sistemin bu durumda başlangıç değerlerine yüksek hassasiyet gösterdiği söylenebilecektir. Önerilen yöntemde maksimum 4 bit düzlemdeki bitlerde değişiklik yapma imkânı olduğu için gömme kapasitesi yüksek ve örtü görüntüsünün maksimum yarısı kadar olacaktır ayrıca, kaotik haritayla şifreleme işlemi gerçekleştirildiğinde gizli verilerin güvenliği de sağlanmış olacaktır. Maksimum gömme kapasite kullanılmadan en az anlamlı 4 bite düşük kapasite veriler gizlendiğinde ise örtü görüntüsünde yüksek algılanamazlık sağlanacaktır. Gömülecek verinin kapasitesine göre algoritmaların başarıları farklılık gösterecektir. Düşük kapasiteye sahip verinin gömüldüğü şemalarda [17-19] yüksek algılanamazlık değerleri elde edildiği görülürken, yüksek kapasite ile ön plana çıkan çalışmaların [31,32] sonuçlarına bakıldığında önerilen yöntemin sonuçlarının daha başarılı olduğu görülmüştür.

Makalenin geri kalan kısmı şu şekilde devam edecektir; 3. bölümde, ön bilgi verildikten sonra önerilen yöntem anlatılacaktır. 4. bölümde, yöntemin sonuçları ve performans ölçütleri detaylı bir şekilde incelenecektir. 5. bölümde, önerilen yöntemin literatürdeki bazı yöntemlerden üstün olduğu gösterilip sonlandırılacaktır.

3. ÖN HAZIRLIKLAR VE ÖNERİLEN YÖNTEM (PRELIMINARIES AND PROPOSED METHOD)

Makalenin bu bölümünde, öncelikle ön bilgi verilecek ve ardından önerilen yöntem anlatılacaktır.

3.1. Ön Hazırlıklar (Preliminaries)

Bu alt bölümde makale için gerekli bazı ön bilgiler uygulamalarla birlikte verilecektir.

3.1.1. Lojistik harita (Logistic map)

Kaotik sistemler gelişi güzel ilerleyip tahmin edilemez davranış gösterirler. Başlangıç şartlarına bağımlıdırlar. Çok yakın iki noktadan başlayan sistemlerin izleyeceği yol tamamen birbirinden farklıdır [34]. Bu özelliğinden dolayı burada 1B lojistik harita rastgele sayı üretmek için kullanılacaktır. Bir lojistik harita, Denklem (1) ile ifade edilir.

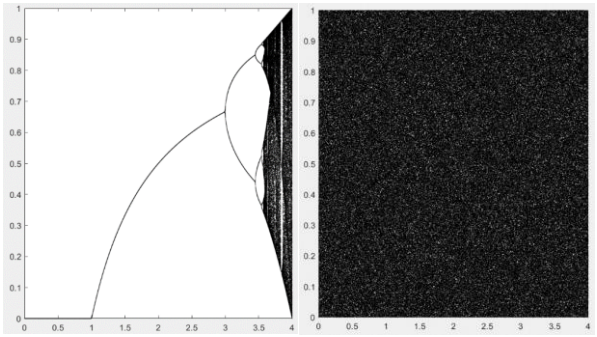
$$x_{n+1} = u * x_n * (1 - x_n) \quad (1)$$

x_0, (0-1) arasında kaotik haritanın başlangıç değeri olarak seçildiğinde, lojistik harita kontrol parametresi olan u'nun [3,57-4] değerleri arasında sistemin kaotik duruma geçtiğini, dağılımın düzensizleştiğini Şekil 3 (a)'daki lojistik haritanın çatallanma diyagramında görebilmekteyiz.

Lojistik harita 2^k ile çarpılarak genişletilebilir. Çatallanma diyagramındaki düzensizliği (0-4) arasında genişletmek için k en az 9 olması gerekmektedir. Burada lojistik harita örnek örtü görüntüsündeki toplam piksel sayısı olan 2^{16} ile çarpılıp Denklem (2)'deki gibi tekrar düzenlenmiştir [1].

$$x_{n+1} = mod(u * x_n * (1 - x_n) * 2^{16}, 1) \quad (2)$$

Şekil 3 (b)'de genişletilmiş lojistik haritanın çatallanma diyagramı görülmektedir. Lojistik haritanın kontrol parametresi olan u değeri 0'dan itibaren sistem düzensiz dağılım göstermektedir.



(a) **(b)**

Şekil 3. Çatallanma diyagramları (a) Logistik harita (b) Geliştirilmiş lojistik harita (The bifurcation diagrams (a) Logistic map (b) Improved logistic map

3.1.2. LSB steganografi ve BPCS (LSB steganography ve BPCS)

LSB yöntemi uzamsal alan görüntü steganografisinde kullanılan, görüntü pikselinin en küçük bitini doğrudan değiştirerek gömme işlemini yapan en basit tekniklerden birisidir [19,23,35,36]. LSB algoritmasının işlem adımlarını şu şekilde örneklendirebiliriz;

Adım 1: Örtü görüntüsü pikselleri bir matris olarak okunur,

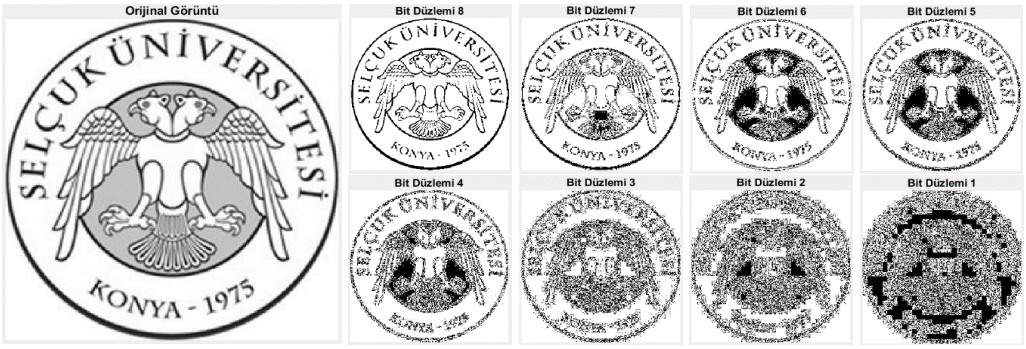
Adım 2: Örtü görüntüsünde verinin gömüleceği piksel binary forma dönüştürülür. Örneğin değeri "153" olan bir pikselin binary değeri "10011001" dir,

Adım 3: Gizlenecek veri binary forma dönüştürülür. Örneğin gizlenecek veri "b" harfi ise, binary değeri "01100010" dır,

Adım 4: Verinin gömüleceği piksel ile gizlenecek verinin binary değerleri XOR işlemine tabi tutulur. 10011001 x 01100010, XOR işleminin sonucunda elde edilen "11111011" binary değeri üzerinde işlem yapılan pikselin yeni değeri olacaktır.

Adım 5: Bir önceki adımda elde edilen binary formun decimal karşılığı olan "251" ilgili pikselin yeni değeri olarak yazılır ve gizli veri içeren stego görüntü oluşturulur. Sonuçta "153" olan pikselin değeri "251" olarak değiştirilmiş ve "b" harfi gizlenmiş olacaktır. Örtü görüntüsündeki ve stego görüntüsündeki ilgili piksel tekrar XOR işlemine tabi tutulursa gizli veri okunabilecektir.

Görüntülerdeki piksel değerleri binary değerlerle temsil edildiğinde, tüm piksellerin her bir biti bir binary görüntü oluşturacaktır. Her bir binary görüntü bit düzlemi olarak bilinir. Şekil 4'te gri tonlu bir görüntü ve bu görüntünün bit düzlem görüntüleri görülmektedir. Görüntüdeki tüm piksellerin en az anlamlı bitleri (LSBs), en az anlamlı bit düzlem görüntüsünü (bit düzlemi 1) oluştururken, tüm piksellerin en çok anlamlı bitleri (MSBs), en çok anlamlı bit düzlem görüntüsünü (bit düzlemi 8) oluşturur.



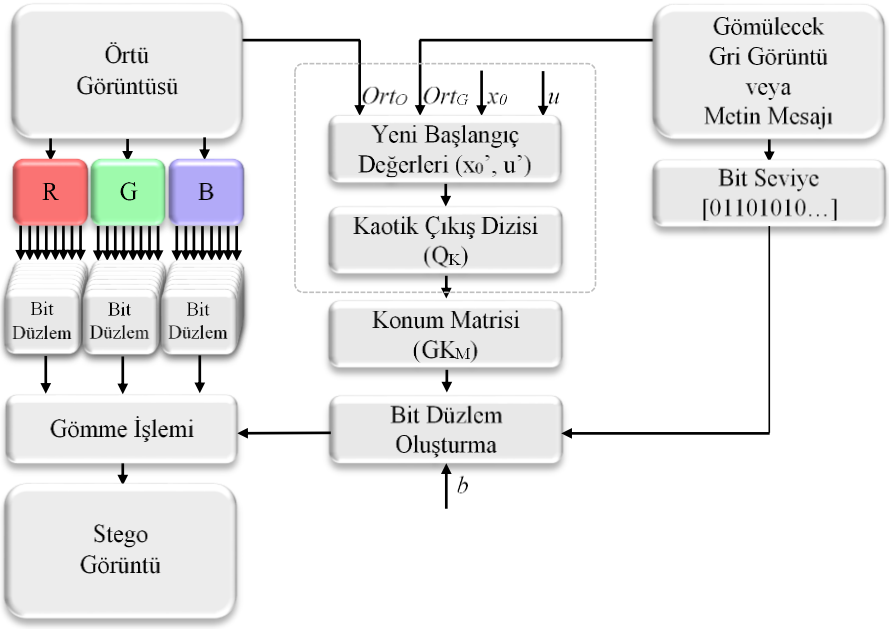
Şekil 4. (a) Orijinal gri görüntü (b) Görüntünün bit düzlemleri ((a) Original gray-level image (b) Bit-planes of the gray-level image)

LSB tekniğinde veriler 4 LSB bite gizlenirken, gömme kapasitesi artırabilmek için geliştirilen BPCS steganografi tekniği ile en az anlamlı bit düzleminden, en çok anlamlı bit düzlemine kadar tüm düzlemlerin piksel bloklarında veri gizlenebilmektedir. BPCS steganografisinde görüntü "bilgilendirici bölge" ve "gürültülü bölge" olarak ikiye ayrılır ve gizli veriler görüntü kalitesini bozmadan görüntünün gürültü bloklarında saklanabilir [26,37].

Şekil 4 (b)'deki bit düzlemi görüntülerinden de görülebileceği gibi, MSB bit düzlemleri görüntü hakkında büyük bilgi verirken, LSB bit düzlemleri görüntü hakkında bilgi vermeyecek ve karşımıza rastgele gürültü olarak çıkacaktır. Yani 4 MSB bit düzleminden oluşan görüntü, orijinal görüntü hakkında yeterli bilgiyi sunarken, 4 LSB bit düzleminin görüntüden atılması ya da değiştirilmesi orijinal görüntü üzerine çok etki etmeyecektir. Şekil 5'te bit düzlemlerden tekrar elde edilen görüntüler gösterilmiştir. Bu görüntülere bakarak 4 LSB bit düzlemleri veri gizlemek ve şifrelemek için idealdir diyebiliriz.

Önerilen yöntemde renkli örtü görüntüsüne gizlenmek istenen gri resim veya metnin, program esnasında seçilecek en fazla 4 LSB bit düzlemine kaotik haritayla üretilen diziye göre rastgele dağıtılması ile stego görüntü oluşturulacaktır. Bir sonraki bölümde önerilen yöntem detaylı incelenecektir.

Şekil 5. (a) 8 Bit Düzlem Görüntü (b) 8+7 Bit Düzlem Görüntü (c) 8+7+6 Bit Düzlem Görüntü (d) 8+7+6+5 Bit Düzlem Görüntü ((a) 8 Bit plane of the image (b) 8+7 Bit planes of the image (c) 8+7+6 Bit planes of the image (d) 8+7+6+5 Bit planes of the image)



Şekil 6. Önerilen yöntemin blok diyagramı (The block diagram of the proposed method)

3.2. Önerilen Yöntem (Proposed Method)

Önerilen yöntemde bilgi gizleme işlemi bir renkli görüntünün RGB kanallarında bit düzlemlerine gömülerek gerçekleştirilecektir. Bu yöntemin blok diyagramı Şekil 6'da görülmektedir. Gizlenmek istenen gri seviye görüntü veya metin dizisinin bitleri renkli örtü görüntüsünün seçilen bit düzlemlerine, geliştirilen 1B lojistik harita ile üretilen değerler kullanılarak rastgele konumlarda XOR işlemiyle gizlenecektir. Gizli bilgiyi geri getirme işleminde lojistik haritanın ürettiği değerler tekrar kullanılarak, gömme adımlarının ters yönde işletilmesi gerekmektedir.

Önerilen yöntemde gizli bilgiyi gömme işlemi için yürütülen algoritma adımları şu şekildedir.

Adım 1: Örtü görüntüsünü bit düzlemlere ayırma

Renkli örtü görüntüsünün RGB renk düzeyleri bit düzlemlerine ayrılır. Sadece en fazla 4 LSB bit düzleminde değişiklik yapılacağı için, algoritmanın başlangıcında bilginin gizleneceği bit düzlem sayısı (b) seçilir. Örneğin, 256x256 piksel boyutlarına sahip bir renkli örtü görüntüsünde bilgi gizlemek için maksimum 4 bit düzlem seçilirse, 786432 bit kullanılabilir olacaktır.

Adım 2: Gizlenecek veriyi uygun forma getirme

Önerilen yöntemde hem görüntü hem de metin mesajlarını renkli görüntü üzerine gizleme imkânı sunulmuştur. Metin mesajı gizlerken her bir karakter 8bitlik binary forma dönüştürüldükten sonra mesajın tamamını içeren bir bit dizisi elde edilmelidir. Gri seviyeli görüntülerde ise görüntü önce tek boyutlu matrise dönüştürüldükten sonra bit dizisi haline getirilmelidir.

Adım 3: Kaotik harita başlangıç değerlerini hesaplama

Kaotik haritanın başlangıç değerleri, örtü görüntüsünün ve gizlenmek istenen verinin ortalama değerleri kullanılarak tekrar hesaplanır. Bu şekilde kaotik sistemin hem örtü görüntüsüne hem de gizlenmek istenen bilgiye bağlı olması sağlanır.

$$Ort_O = \sum_{k=1}^{c} \sum_{i=1}^{M} \sum_{j=1}^{N} P_{ij}/(M * N * c) \quad (3)$$

$$Ort_G = \sum_{i=1}^{L} D_i/(L) \quad (4)$$

Denklem (3), örtü görüntünün ve eğer gizlenmek istenen bilgi bir görüntü ise bu görüntünün ortalama piksel değerini hesaplamak için kullanılacak denklemlerdir. Denklem (4), gizlenmek istenen bilgi metin mesajı ise metin mesajının ortalama değerini hesaplamak için kullanılan denklemdir. Burada M, görüntünün bir satırında bulunan piksel sayısı N, görüntünün bir sütununda bulunan piksel sayısı, P_{ij} ilgili pikseldeki gri seviye renk değeri, c ise renk kanal sayısıdır. L, tek boyutlu matrisin uzunluğudur, D_i tek boyutlu matristeki ilgili değerdir.

$$x_0' = x_0 * Ort_O - floor(x_0 * Ort_O) \quad (5)$$

$$u' = 4 * (u * Ort_G - floor(u * Ort_G)) \quad (6)$$

Denklem (5) ve (6), ortalama değerlere göre kaotik haritanın başlangıç değerlerini tekrar hesaplamak için kullanılır [1]. Burada x_0', 0-1 arasında, u', 0-4 arasında değer olacaktır.

Adım 5: Kaotik çıktı dizisini elde etme

Önceki adımda hesaplanan x_0' ve u' başlangıç değerleri Denklem (2)'de geliştirilen 1B kaotik haritaya uygulanıp Q_K kaotik çıktı dizisi elde edilir. Kaotik çıktı dizisinin boyutu başlangıçta seçilen bit düzlem görüntüsü (b) sayısına bağlı olarak değişebilecektir. Denklem (7) ile hesaplanır [1].

$$s = M * N * c * b \tag{7}$$

Adım 6: Gizleme konum matrisini elde etme

Hesaplanan Q_K kaotik çıktı dizisi, küçükten büyüğe sıralanarak $K=\{k_1, k_2, \ldots k_s\}$ konum matrisi elde edilir. Elde edilen sıralı matristen Denklem (8), (9) ve (10) kullanılarak, gizleme konum matrisi $GK_M=\{gk_{m1}, gk_{m2}, \ldots gk_{ms}\}$ hesaplanır [1].

$$K_c(i) = mod(floor(K(i)/(M * N)), c) + 1 \tag{8}$$

$$K_M(i) = mod(K(i), N) + 1 \tag{9}$$

$$K_N(i) = mod\big(floor\big(\big(K(i)\big)/M\big), N\big) + 1 \tag{10}$$

Burada $gk_{mi}=\{K_M(i), K_N(i), K_c(i)\}$'dir. $K_c(i)$, gizleme yapılacak bit düzlem konumu, $K_M(i)$, satır konumu ve $K_N(i)$, sütun konumudur.

Adım 7: Stego görüntünün oluşturulması

Gizlenecek bilgi dizisindeki bitler üretilen kaotik haritaya göre bit düzlemlerdeki satır ve sütunlara XOR işlemiyle gömülür ve stego görüntü elde edilmiş olur. Bilgi gizleme adımlarının tersi izlenerek görüntüdeki gizli bilgiye ulaşmak mümkündür. Burada lojistik kaotik haritanın başlangıç değerleri (x_0, u), bu değerleri tekrar elde etmek için gerekli olan örtü görüntüsünün ve gizli bilginin ortalama değerleri (Ort_O, Ort_G), kaotik harita genişletme katsayısı (k), gizlenecek bilginin uzunluğu (L) ve işlem yapılacak olan bit düzlem sayısı (b) gizli anahtarlardır. Gizli veriye ulaşmak için bu anahtarlara sahip olmak gerekir.

Gizli bilginin kaotik haritayla rastgele konumlara gömülmesi görüntünün, bit düzlemleri incelendiğinde orijinalinde olduğu gibi gürültü şeklinde görünmesini sağlayacaktır. Görüntü üzerinde büyük etkisi olan 4 MSB bit düzleminde değişiklik yapılmaması ise bilgi gizlenmiş stego görüntünün, örtü görüntüsünde gözle görülür büyük farkların olmasını engelleyecektir. Anahtarlardaki en ufak bir değişiklik kaotik sistemin özelliğinden kaynaklı olarak çıkışta büyük değişikliklere neden olacak ve gizlenmiş bilgiye dair sonuç elde edilemeyecektir [33].

4. DENEYSEL SONUÇLAR VE PERFORMANS ÖLÇÜTLERİ (EXPERIMENTAL RESULTS AND PERFORMANCE METRICS)

Bu makalede önerilen algoritma MATLAB yazılımı ile test edilmiştir. Deneysel sonuçlarda 256x256 boyutunda renkli Lena örtü görüntüsü üzerine farklı boyutlarda gri seviye görüntüler ve farklı uzunlukta metin mesajları gizlenmiştir. Önerilen yöntemin etkinliği farklı ölçülerdeki örtü görüntüsünde de değerlendirilebilir.

4.1. İstatistiksel Ölçütler (Statistical Metrics)

Stego görüntüler istatistiksel olarak değerlendirilmek için aşağıdaki yöntemlerle test edildi. Rastsallık ölçeği olarak Denklem (11)'deki bilgi entropisi kullanılmıştır. Stego görüntü ile örtü görüntüsü arasındaki benzerliği test etmek için Denklem (12) ile korelasyon hesabı yapılmıştır. GLCM (Gray-Level Co-occurrence Matrix – Gri-Seviye Eş Oluşum Matrisi) köşegenindeki eleman dağılımlarının yakınlığını ölçmek için Denklem (13)'teki homojenlik formülü kullanılmıştır. GLCM köşegenindeki elemanların karelerin toplamı Denklem (14)'teki enerji formülü ile hesaplanmıştır. Stego görüntülerdeki tüm pikseller için bir piksel ile komşuları arasındaki yoğunluk kontrastının ölçmek için Denklem (15)'teki kontrast formülü kullanılmıştır. Bu ölçütlerden elde edilen sonuçlar Çizelge 1'de gösterilmektedir.

$$I(R) = \sum_{i=0}^{F-1} P(R = i) x \log_2 P(R = i) \tag{11}$$

$$Kor = \sum_{ij}^{MN} (i - v_i) x (j - v_j) x P_{ij} / (\sigma_i x \sigma_j) \tag{12}$$

$$H = \sum_{ij}^{MN} P_{ij} / (1 - |i - j|) \tag{13}$$

$$E = \sum_{ij}^{MN} P_{ij}^2 \tag{14}$$

$$Kon = \sum_{ij}^{MN} |i - j|^2 x P_{ij} \tag{15}$$

Bu sonuçlardan da görüleceği üzere sadece entropi ölçümlerinde çok küçük değişiklikler olmuştur. Örtü görüntüsüne gizli veri olarak görüntünün gömülmesi, metin gömülmesine göre biraz daha büyük entropi değerleri çıkarmıştır, diğer analiz ölçümleri ise tutarlıdır. 1 bit düzlemde ya da 4 bit düzlemde değişiklik yapılması bu sonuçlarda değişikliğe neden olmamıştır. Sonuçlar saldırganların istatistiksel saldırıları kullanamayacaklarını göstermektedir.

4.2. Sapma Niceleme Ölçütleri (Deviation Quantification Metrics)

Örtü görüntüsü ve stego görüntü arasındaki bozulma, Denklem (16)'daki MSE ve Denklem (17)'deki PSNR değerleri ile değerlendirildi.

$$MSE = \sum_{ij}^{MN} (CP_{ij} - SP_{ij})^2 / (MxN) \tag{16}$$

$$PSNR = 10xlg(255^2 / MSE)(dB) \tag{17}$$

PSNR değerinin 35dB'den büyük olması durumunda, örtü görüntüsü ile stego görüntünün arasındaki farkı söylemek zordur. PSNR değerinin ne kadar büyükse, stego görüntüde bozulma o kadar küçük olacaktır ve bilgilerin saldırganlar tarafından bulunma olasılığı azalacaktır.

Çeşitli boyutlardaki gizli verilerle ölçülen MSE ve PSNR değerleri Çizelge 2'de gösterilmektedir. Deneysel sonuçlardan görülebileceği gibi, çeşitli boyutlardaki metin ve görüntü verilerini örtü görüntüsüne eklediğimizde PSNR değeri 35dB'den büyük olmuştur, bu sonuçlarla saldırganların gömülü gizli verileri görsel olarak bulması zordur.

Çizelge 1. İstatistiksel ölçütlerin sonuçları (The results of statistical metrics)

İstatistiksel Analiz		Örtü Görüntüsü R	Örtü Görüntüsü G	Örtü Görüntüsü B	Bit Düzlem	Gizli Veri Görsel/Metin	Stego Görüntüsü R	Stego Görüntüsü G	Stego Görüntüsü B
Entropy	Lena	7.22864	7.54978	6.96750	1	150x150	7.23076	7.55072	6.96781
						22500byte	7.23084	7.55090	6.96773
					2	150x150	7.23482	7.55332	6.98000
						22500byte	7.23341	7.55222	6.96988
					3	150x150	7.24479	7.55856	6.97475
						22500byte	7.23965	7.55668	6.97306
					4	150x150	7.26371	7.57229	6.99044
						22500byte	7.25385	7.56567	6.98412
Korelasyon	Lena	0.93011	0.93163	0.86993	1	150x150	0.93011	0.93163	0.86993
						22500byte	0.93011	0.93163	0.86993
					2	150x150	0.93011	0.93163	0.86993
						22500byte	0.93011	0.93163	0.86993
					3	150x150	0.93011	0.93163	0.86993
						22500byte	0.93011	0.93163	0.86993
					4	150x150	0.93011	0.93163	0.86993
						22500byte	0.93011	0.93163	0.86993
Homojenlik	Lena	0.88354	0.87769	0.88855	1	150x150	0.88354	0.87769	0.88855
						22500byte	0.88354	0.87769	0.88855
					2	150x150	0.88354	0.87769	0.88855
						22500byte	0.88354	0.87769	0.88855
					3	150x150	0.88354	0.87769	0.88855
						22500byte	0.88354	0.87769	0.88855
					4	150x150	0.88354	0.87769	0.88855
						22500byte	0.88354	0.87769	0.88855
Kontrast	Lena	0.33033	0.36677	0.29951	1	150x150	0.33033	0.36677	0.29951
						22500byte	0.33033	0.36677	0.29951
					2	150x150	0.33033	0.36677	0.29951
						22500byte	0.33033	0.36677	0.29951
					3	150x150	0.33033	0.36677	0.29951
						22500byte	0.33033	0.36677	0.29951
					4	150x150	0.33033	0.36677	0.29951
						22500byte	0.33033	0.36677	0.29951
Enerji	Lena	0.15673	0.10307	0.18235	1	150x150	0.15673	0.10307	0.18235
						22500byte	0.15673	0.10307	0.18235
					2	150x150	0.15673	0.10307	0.18235
						22500byte	0.15673	0.10307	0.18235
					3	150x150	0.15673	0.10307	0.18235
						22500byte	0.15673	0.10307	0.18235
					4	150x150	0.15673	0.10307	0.18235
						22500byte	0.15673	0.10307	0.18235

Çizelge 2. Sapma niceleme ölçütlerin sonuçları (The results of deviation quantification metrics)

Sapma Niceleme Ölçütleri	Bit Düzlem	Gizli Veri Görsel	Stego Görüntüsü PSNR	Stego Görüntüsü MSE	Gizli Veri Metin	Stego Görüntüsü PSNR	Stego Görüntüsü MSE
Lena	1	75x100	54.4359	0.23415	7500byte	56.7213	0.13834
		80x250	51.1192	0.50253	20000byte	52.0467	0.40589
		150x150	49.745	0.6897	22500byte	51.949	0.4151
	2	75x100	50.451	0.58611	7500byte	52.776	0.34315
		80x250	47.1289	1.2595	20000byte	48.0586	1.0168
		150x150	45.773	1.7211	22500byte	47.984	1.0344
	3	75x100	45.9967	1.6346	7500byte	48.2873	0.96461
		80x250	42.6487	3.5336	20000byte	43.6272	2.8207
		150x150	41.291	4.8306	22500byte	43.506	2.9005
	4	75x100	41.1858	4.9488	7500byte	43.491	2.9106
		80x250	37.8531	10.6602	20000byte	38.7813	8.6089
		150x150	36.503	14.5472	22500byte	38.657	8.8585

4.3. Görüntü Kalitesinin Değerlendirilmesi (Evaluation Of Image Quality)

Stego görüntü ve örtü görüntüsü arasındaki benzerliği ve stego görüntünün kalitesini Denklem (18)'deki görüntü doğruluğu ve Denklem (19)'daki kalite indeksi parametreleri ile değerlendirebiliriz.

$$GD = 1 - \sum_{ij}^{MN}(CP_{ij} - SP_{ij})^2 / \sum_{ij}^{MN}(CP_{ij}\ x\ SP_{ij}) \quad (18)$$

$$KI = 4\ x\ \sigma_{CS}\ x\ \overline{CP}\ x\ \overline{CS}\ /\left((\sigma_c^2 + \sigma_s^2)\ x\ [\overline{CP}^2 + \overline{CS}^2]\right) \quad (19)$$

$$\overline{CP} = \sum_{ij}^{MN} CP_{ij}/(M\ x\ N)\ ,\ \overline{CS} = \sum_{ij}^{MN} SP_{ij}/(M\ x\ N)$$

$$\sigma_c^2 = \sum_{ij}^{MN}\left(CP_{ij} - \overline{CP}\right)^2/(M\ x\ N - 1)$$

$$\sigma_s^2 = \sum_{ij}^{MN}(SP_{ij} - \overline{SP})^2/(M\ x\ N - 1)$$

$$\sigma_{CS} = \sum_{ij}^{MN}\left(CP_{ij} - \overline{CP}\right)x\left(SP_{ij} - \overline{SP}\right)/(M\ x\ N - 1)$$

Bu iki ölçüt sonuçlarının 1'e yakın çıkması karşılaştırılan stego görüntüsü ve örtü görüntüsünün birbirine yakın olduğu anlamına gelecektir. Sonuçlar 1'e ne kadar yakınsa görüntüler o kadar benzerdir diyebiliriz. Çizelge 3'teki görüntü kalitesi sonuçlarına baktığımızda önerilen yöntemin üstün kalitede bir stego görüntüsü sağlayabileceği görülmektedir.

Çizelge 3. Görüntü kalitesi ölçütlerinin sonuçları (The results of image quality metrics)

Kalite Ölçütleri	Bit Düzlem	Gizli Veri Görsel	Stego Görüntüsü		Gizli Veri Metin	Stego Görüntüsü	
			Kalite İndeksi	Görüntü Doğruluğu		Kalite İndeksi	Görüntü Doğruluğu
Lena	1	75x100	0.99996	0.99999	7500byte	0.99998	0.99999
		80x250	0.99992	0.99997	20000byte	0.99994	0.99998
		150x150	0.99989	0.99996	22500byte	0.99994	0.99998
	2	75x100	0.99991	0.99997	7500byte	0.99995	0.99998
		80x250	0.99981	0.99993	20000byte	0.99984	0.99995
		150x150	0.99974	0.99991	22500byte	0.99984	0.99994
	3	75x100	0.99975	0.99991	7500byte	0.99985	0.99995
		80x250	0.99946	0.99981	20000byte	0.99957	0.99985
		150x150	0.99926	0.99974	22500byte	0.99955	0.99984
	4	75x100	0.99924	0.99973	7500byte	0.99955	0.99984
		80x250	0.99836	0.99943	20000byte	0.99868	0.99954
		150x150	0.99777	0.99922	22500byte	0.99864	0.99952

4.4. Görüntü Histogramı (Image Histogram)

Stego görüntünün histogramı örtü görüntüsünün histogramı ile benzer olduğunda, istatistiksel saldırılara karşı sağlamlığı söylenebilir. Şekil 7, örtü görüntüsü ve görüntü ve metin gömülerek oluşan stego görüntülerin histogramları gösterilmektedir. Bu histogramlardaki benzerlik önerilen algoritmanın istatistiksel saldırılara karşı sağlam olduğunu göstermektedir.

4.5. Anahtar Hassasiyeti (Key Sensivity)

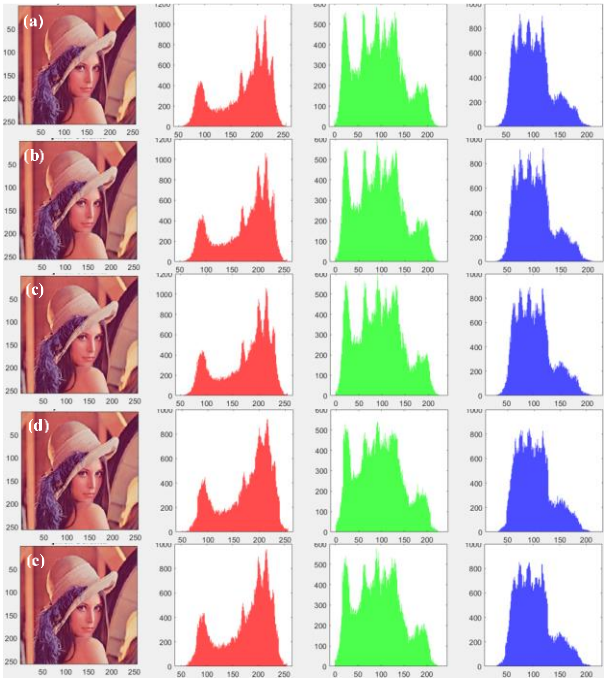
Algoritmaların gücünü belirlemeye yarayan kriterlerden bir tanesi anahtar duyarlılığı yani anahtarlardaki ufak değişikliklerde algoritmanın verdiği cevaptır. Önerilen yöntemde kullanılan gizli anahtarlardan ($x_0, u, Ort_O, Ort_G, k, L, b$) daha önceki bölümde bahsedilmişti. Bu anahtarlarda bazı ufak değişikliklerle gizli verileri çıkarmak için yapılan deneylerin sonuçları Şekil 8'de gösterilmektedir.

Deneysel sonuçlar, önerilen algoritmanın gizli anahtarlarındaki değişikliklere karşı çok hassas olduğunu, bu da saldırganların, anahtar değerlerini tam bilmeden gizli verileri çıkarmasının imkânsız olduğunu göstermektedir.

4.6. Ki-Kare Testi (Chi-Square Test)

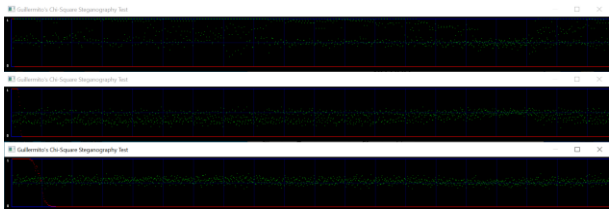
Önerilen algoritma ile gizli veriler örtü görüntüsünün en düşük bit düzlemlerine gömüldüğü için bu işlemden sonra en düşük bit düzlemi değişecektir. Burada, beklenen frekans ile gözlenen frekans arasında anlamlı bir fark olup olmadığını anlamak için istatistiksel bir ölçü olan Ki-kare testi uygulanır [38]. Ki-kare testi, 1999 yılında Westfeld ve Pfitzmann tarafından önerilen istatistiksel bir analiz yöntemidir [39]. Bu testi gerçekleştirmek için açık kaynak kodlu bir program olan Guillermito yazılımını kullandık [40]. Sonuçlar Şekil 9'da gösterilmiştir.

Şekilde kırmızı çizgi Ki-kare testinin sonucunu göstermektedir. Kırmızı çizgi '1' yakınsa, örtü görüntüsünde gizli bilgilerin olma olasılığının yüksek olduğu, '0' yakınsa, örtü görüntüsünde gizli bilgi varlığına dair bir bilgi olmadığı anlamına gelir. Yeşil eğri, görüntüdeki en düşük bitlerin ortalama değerini temsil eder. Bu test sonucu ile saldırganların önerilen yöntemle elde edilen stego görüntüsünden gömülü gizli verileri bulamayacağı sonucuna ulaşabiliriz.



Şekil 7. Histogram sonuçları (a) Orijinal örtü görüntüsü (b) 1 bit düzlemde 150x150 görüntü gizlenmiş stego görüntüsü (c) 1 bit düzlemde 22500byte metin gizlenmiş stego görüntüsü (d) 4 bit düzlemde 150x150 görüntü gizlenmiş stego görüntüsü (e) 4 bit düzlemde 22500byte metin gizlenmiş stego görüntüsü (The histogram results (a) Original cover image (b) Stego image with 150x150 of image hidden in 1 bit plane (c) Stego image with 22500bytes of text hidden in 1 bit plane (d) Stego image with 150x150 of image hidden in 4 bit plane (e) Stego image with 22500bytes of text hidden in 4 bit plane)

Şekil 8. Anahtarlardaki küçük değişiklikler için çıkarma sonuçları (a) x_0=0.155802408854157 ve x_0=0.155802408854158 (b) u=3.417600000000221 ve u=3.417600000000222 (c) k=16 ve k=16.00000000000001 (d) Ort_O=124.0779012044271 ve Ort_O=124.0779012044272 (Extraction results for the minor changes in keys (a) x_0=0.155802408854157 and x_0=0.155802408854158 (b) u=3.417600000000221 and u=3.417600000000222 (c) k=16 and k=16.00000000000001 (d) Ort_O=124.0779012044271 and Ort_O=124.0779012044272)



Şekil 9. Ki-Kare test sonuçları (a) Örtü görüntüsü (b) 150x150 görüntü gizlenmiş stego görüntü (c) 22500byte metin gizlenmiş stego görüntü (Chi-square test results (a) cover image (b) 150x150 image hidden stego image (c) 22500byte text hidden stego image)

5. SONUÇ (CONCLUSION)

Önerilen yöntemin literatürdeki güncel yöntemlerle karşılaştırılması Çizelge 4'te verilmiştir. Karşılaştırmada örtü görüntüsü olarak Lena renkli görüntüsüne LSB steganografi yöntemiyle veri gizleyen çalışmalar seçilmiştir. Bu çalışmalarda gömü verisi olarak farklı boyutta görüntü ve metin verisi kullanıldığı görülmektedir. Sonuçlardan da anlaşılabileceği gibi stego görüntülerin kalitesi gömü verisi olarak kullanılacak veri türüne ve boyutuna göre değişmektedir. Önerdiğimiz yöntem, elde ettiği başarılı sonuçlarla bu çalışmalarla birlikte literatürdeki yerini alabilir.

Bu çalışmada, renkli örtü görüntüsü içerisine, görüntü ve metin mesajları gizlemek için bir yöntem önerildi. Bu yöntemde kapasite olarak büyük verilerin gizlenmesine imkân veren LSB steganografisi üzerine çalışıldı. Renkli örtü görüntüsü renk kanallarına ayrıldıktan sonra, her renk kanalı bit düzlem görüntüleri olarak değerlendirildi. İşlem yapılacak bit düzlem sayısı algoritmanın başında, algoritmayı kullanan kişiye bırakıldı ve en fazla 4 bit düzlem görüntüsünde değişiklik yapılmasına izin verildi. Gizlenecek verilerin bit düzlemlere sıralı bir şekilde gömülüp, bit düzlem incelenmesinde saldırganların gizli bilgiye direk ulaşmasını engellemek için, geliştirilen kaotik lojistik harita ile gömü verisinin seçilen bit düzlemlerin rastgele konumlarına gizlenme işlemi

gerçekleştirildi. Bu sayede gizli verilerin en az anlamlı bit düzlemlerinde görüntü olarak görünmesi engellenip, gürültü olarak görünmesi sağlandı. Ayrıca, kaotik lojistik haritanın başlangıç değerlerinin hem örtü görüntüsüne hem de gizlenecek veriye bağlı olması, saldırganların kaotik başlangıç için bu bilgilere sahip olmadan gizli veriler hakkında düzgün sonuçlar elde edememesi sağladı. Algoritmanın gizli anahtarlara duyarlılığı testlerle gösterildi, anahtarlardaki en ufak bir değişiklikte gizli bilgi hakkında çıkarım yapamayacak kadar büyük sonuçların elde edildiği gösterildi. Gömü verisi olarak metin ve görüntü bilgilerinin kullanılması sonucu elde edilen stego görüntüsünün kalite sonuçları ve diğer test sonuçları karşılaştırmalı olarak gösterildi. Test sonuçlarına tekrar bakıldığında önerilen algoritmanın renkli örtü görüntüsüne bilgi gizleme işleminde kullanılabileceği uygun görülmektedir. Sonraki çalışmalar için renkli gömü görüntüsünün, renkli örtü görüntüsüne, görüntünün oluşmasına büyük etki sunan 4 MSB bit düzleminin kaotik olarak şifrelenerek gizlenmesi öneri olarak verilebilir.

Çizelge 4. Önceki yöntemlerle performans karşılaştırması (Performance comparison with the preceding methods)

Yöntem	Gizli Veri	Stego Görüntüsü			
		PSNR	MSE	Kalite İndeksi	Görüntü Doğruluğu
Önerilen Yöntem	150x150	49.745	0.6897	0.99989	0.99996
	22500byte	51.949	0.4151	0.99994	0.99998
Kalita vd. (2019) [31]	73695byte	42.2601	11.9138	0.9995	0.9989
Ogras (2019) [41]	100*100	58.626	-	0.998817	0.99965
Pak vd. (2020) [1]	128*192	42.0159	4.0878	0.999149	0.999792
Nazari & Ahmadi (2020) [32]	63752byte	49.6482	0.1172	0.9698	0.9999
Gangurde & Tiwari (2020) [42]	480byte	45.86564	1.68467	-	-
Jayakokela & Avila (2021) [43]	156byte	51.1469	0.4993	-	-
Karawia (2021) [44]	256*256	50.8091	0.5397	1	1
Tang vd. (2021) [45]	128*192	54.2324	0.2454	-	-
Mahdi & Maisa'a (2021) [46]	208byte	72.242	0.0038	-	-
Chowdhuri vd. (2021) [47]	52664byte	41.3335	-	0.9979	0.9918

ETİK STANDARTLARIN BEYANI (DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal özel bir izin gerektirmediğini beyan ederler.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

Hidayet ÇELİK: Deneyleri yapmış ve sonuçlarını analiz etmiştir. Makalenin yazım işlemini gerçekleştirmiştir.

Nurettin DOĞAN: Makalede kullanılacak yöntemleri belirlemiş ve makalede kullanılan algoritmayı kurmuştur.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur.

KAYNAKLAR (REFERENCES)

[1] Pak, C., Kim, J., An, K., Kim, C., Kim, K. & Pak, C., "A Novel Color Image LSB Steganography Using Improved 1D Chaotic Map.", ***Multimedia Tools And Applications,*** 79(1), 1409–1425, (2020).

[2] Beşkirli, A., Özdemir, D. & Beşkirli, M., "Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme." ***European Journal Of Science And Technology, (Special Issue),*** 284-291, (2019).

[3] Zaidan, B. B., Zaidan, A. A., & Mwafak, H., "New Comprehensive Study to Assess Comparatively the QKD, XKMS, KDM in the PKI encryption algorithms." ***Int. J. Comput. Sci. Eng,*** *1*(3), 263-268, (2009).

[4] Sharif, A., Mollaeefar, M., & Nazari, M. "A Novel Method For Digital Image Steganography Based On A New Three-Dimensional Chaotic Map." ***Multimedia Tools And Applications***, 76(6), 7849-7867, (2017).

[5] Westfeld, A., & Pfitzmann, A., "Attacks On Steganographic Systems." ***International Workshop On Information Hiding*** Springer, Berlin, Heidelberg, 61-76, (1999).

[6] Subhedar, M. S., & Mankar, V. H. "Current Status And Key Issues In Image Steganography: A survey." ***Computer Science Review***, 13, 95-113, (2014).

[7] Valandar, M. Y., Ayubi, P., & Barani, M. J. "A New Transform Domain Steganography Based On Modified Logistic Chaotic Map For Color Images." ***Journal Of Information Security And Applications***, 34, 142-151, (2017).

[8] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. "Image Steganography In Spatial Domain: A survey." ***Signal Processing: Image Communication***, 65, 46-66, (2018).

[9] Bilal, M., Imtiaz, S., Abdul, W., Ghouzali, S., & Asif, S. "Chaos Based Zero-Steganography Algorithm." ***Multimedia Tools And Applications***, 72(2), 1073-1092, (2014).

[10] Anees, A., Siddiqui, A. M., Ahmed, J., & Hussain, I. "A Technique For Digital Steganography Using Chaotic Maps." ***Nonlinear Dynamics***, 75(4), 807-816, (2014).

[11] Ghebleh, M., & Kanso, A. "A Robust Chaotic Algorithm For Digital Image Steganography." ***Communications in Nonlinear Science and Numerical Simulation***, 19(6), 1898-1907, (2014).

[12] Bansal, R., Nagpal, C. K., & Gupta, S. "An Efficient Hybrid Security Mechanism Based On Chaos And Improved BPCS." ***Multimedia Tools and Applications***, 77(6), 6799-6835, (2018).

[13] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. "Digital Image Steganography: Survey And Analysis Of Current Methods." ***Signal Processing***, 90(3), 727-752, (2010).

[14] Wang, Y., Tang, M., & Wang, Z. "High-Capacity Adaptive Steganography Based On LSB And Hamming Code." ***Optik***, 213, 164685, (2020).

[15] Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. "An Image Steganography Approach Based On K-Least Significant Bits (k-LSB)." ***In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*** 131-135, (2020).

[16] Rachael, O., Misra, S., Ahuja, R., Adewumi, A., Ayeni, F., & Mmaskeliunas, R. "Image Steganography And Steganalysis Based On Least Significant Bit (LSB)." ***In Proceedings of ICETIT 2019 Springer, Cham.,*** 1100-1111, (2020).

[17] Shehzad, D., & Dağ, T. "LSB Image Steganography Based On Blocks Matrix Determinant Method." ***KSII Transactions On Internet And Information Systems***, 13(7),3778-3793 (2019).

[18] Ali, U. A. M. E., Sohrawordi, M., & Uddin, M. P. "A Robust And Secured Image Steganography Using LSB And Random Bit Substitution." ***American Journal Of Engineering Research (AJER)***, 8(2), 39-44. (2019).

[19] Bhuiyan, T., Sarower, A. H., Karim, R., & Hassan, M.. An Image Steganography Algorithm Using LSB Replacement Through XOR Substitution***. In 2019 International Conference on Information and Communications Technology (ICOIACT*** **) *IEEE***, 44-49, (2019)

[20] Kusuma, E. J., Sari, C. A., Rachmawanto, E. H., & Moses Setiadi, D. R. I. "A Combination Of Inverted LSB, RSA, And Arnold Transformation To Get Secure And Imperceptible Image Steganography." ***Journal Of ICT Research & Applications***, 12(2), (2018).

[21] Zhou, R. G., Luo, J., Liu, X., Zhu, C., Wei, L., & Zhang, X. "A Novel Quantum İmage Steganography Scheme Based On LSB." ***International Journal Of Theoretical Physics***, 57(6), 1848-1863, (2018).

[22] Nguyen, T. D., Arch-Int, S., & Arch-Int, N. "An Adaptive Multi Bit-Plane Image Steganography Using Block Data-Hiding." ***Multimedia Tools And Applications***, 75(14), 8319-8345, (2016).

[23] Zhou, X., Gong, W., Fu, W., & Jin, L. "An Improved Method For LSB Based Color Image Steganography Combined With Cryptography." ***In 2016 IEEE/ACIS 15th International Conference On Computer And Information Science (ICIS), IEEE***, 1-4, (2016).

[24] Patel, N., & Meena, S. "LSB Based Image Steganography Using Dynamic Key Cryptography." ***In 2016 International Conference On Emerging Trends In Communication Technologies (ETCT), IEEE***, 1-5, (2016).

[25] Singh, A., & Singh, H. "An Improved LSB Based Image Steganography Technique For RGB Images. ***In 2015 IEEE International Conference On Electrical, Computer And Communication Technologies (ICECCT), IEEE***, 1-4, (2015).

[26] Sun, S. "A New Information Hiding Method Based On Improved BPCS Steganography." ***Advances In Multimedia***, vol. 2015, Article ID 698492, 7 pages (2015).

[27] Kumar, B. R., Suresh, K., Basheer, S. K., & Kumar, M. R. K. "Enhanced Approach To Steganography Using Bit Planes". ***International Journal Of Computer Science And Information Technologies***, 3(6), 5472-5475, (2012).

[28] Bansod, S. P., Mane, V. M., & Ragha, R. "Modified BPCS Steganography Using Hybrid Cryptography For Improving Data Embedding Capacity***." In 2012 International Conference On Communication, Information & Computing Technology (ICCICT), IEEE***, 1-6, (2012).

[29] Daneshkhah, A., Aghaeinia, H., & Seyedi, S. H. "A More Secure Steganography Method In Spatial Domain." ***In 2011 Second International Conference On Intelligent Systems, Modelling And Simulation, IEEE***, 189-194, (2011).

[30] Bui, C. N., Lee, H. Y., Joo, J. C., & Lee, H. K. "Secure Bit-Plane Based Steganography For Secret Communication." ***IEICE Transactions On Information And Systems***, 93(1), 79-86, (2010).

[31] Kalita, M., Tuithung, T., & Majumder, S., "A New Steganography Method Using Integer Wavelet Transform And Least Significant Bit Substitution." ***The Comput J***, 62, 1639–55, (2019).

[32] Nazari, M., & Ahmadi, I.D., "A Novel Chaotic Steganography Method With Three Approaches For Color And Grayscale Images Based On FIS And DCT With Flexible Capacity.", ***Multimedia Tools Appl***, 79,13693–724, (2020).

[33] Doğan, N. & Çelik, H., "Tarama Modeli Kullanan Karma Bir Görüntü Şifreleme Yöntemi". ***Politeknik Dergisi,*** 1-1, (2021).

[34] Özkaynak, F., & Özer, A. B. "Lojistik Harita ile Rasgele Sayı Üretilmesi ve İstatistiki Yöntemlerle Sınanması." (2006).

[35] Jumaa, N. K. "Hiding Of Random Permutated Encrypted Text Using Lsb Steganography With Random Pixels Generator." ***International Journal Of Computer Applications***, 113(13), (2015).

[36] Astuti, E. Z., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., & Sarker, M. K.. "LSB-Based Bit Flipping Methods For Color Image Steganography." ***In Journal of Physics: Conference Series IOP Publishing*** vol. 1501, no. 1, p. 012019, (2020)

[37] Khairnar, P. P., & Khan, V. U. "Steganography Using BPCS Technology." ***International Journal Of Engineering And Science***, 3(2), 8-16, (2013).

[38] Aziz, M., Tayarani-N, M. H., & Afsar, M., "A Cycling Chaos-Based Cryptic-Free Algorithm For Image Steganography." ***Nonlinear Dynamics***, 80(3), 1271-1290, (2015).

[39] Westfeld, A., Pfitzmann, A., "Attacks On Steganographic Systems", ***International workshop on information hiding. IH1999***, 61–76, (1999).

[40] El Loco, G., "Steganography: A Few Tools to Discover Hidden Data", 2004. http://www.guillermito2.net/stegano/tools/index.html [Erişim: Haziran, 2021]

[41] Ogras H, "An Efcient Steganography Technique For Images Using Chaotic Bitstream." ***Int J Comput Netw Inf Secur*** 11:21–27, (2019).

[42] Gangurde, S., & Tiwari, K., "LSB Steganography Using Pixel Locator Sequence with AES.", ***arXiv e-prints, arXiv-2012.,*** (2020).

[43] Jayakokela, S., & Avila, J. "Steganography based Information Hiding and Transmission via SC-FDMA Transceiver.", ***In 2021 5th International Conference On Intelligent Computing And Control Systems (ICICCS) IEEE***., 33-37, (2021).

[44] Karawia, A.A, "Medical Image Steganographic Algorithm Via Modified LSB Method And Chaotic Map.", ***IET Image Processing***. (2021).

[45] Tang, L., Wu, D., Wang, H., Chen, M., & Xie, J. "An Adaptive Fuzzy Inference Approach For Color Image Steganography.", ***Soft Computing,*** 1-18, (2021).

[46] Mahdi, S. A., & Maisa'a, A. K., "An Improved Method for Combine (LSB and MSB) Based on Color Image RGB.", ***Engineering and Technology Journal***, 39(1B), 231-242, (2021).

[47] Chowdhuri, P., Jana, B., & Giri, D. "Secured Steganographic Scheme For Highly Compressed Color Image Using Weighted Matrix Through DCT." ***International Journal Of Computers And Applications***, 43(1), 38-49, (2021).