BİLGİSAYAR BİLİMLERİ
VE
TEKNOLOJİLERİ DERGİSİ
JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGIES
http://dergipark.org.tr/tr/pub/bibted

Araştırma Makalesi

# An Efficient Steganography Method Based on Chaotic Functions and XOR Operation for Data Hiding

**Selman Yakut**[*1]

*[1]Inonu University, Faculty of Engineering, Software Engineering Department, Malatya, Türkiye*

**Keywords:**
Steganography
Chaotic functions
Logistic Map
Tent Map

## ABSTRACT

The advancing technology and digitalizing world have increased the importance of secure data transmission. Steganography, a technique that ensures secure data communication, is a critical component of data security. Derived from the term meaning "hidden writing" in Turkish, steganography is based on the principle of embedding the data to be hidden into a carrier medium. While historically applied using primitive methods, steganography has transitioned to the use of modern techniques and methods in today's digitalized era. In this study, a steganography method based on chaotic functions and the XOR operation is proposed. The proposed method consists of two stages. In the first stage, data embedding, the data to be hidden is first converted into binary format. This binary data is then subjected to an XOR operation with a tent map sequence. The resulting final data is embedded into a grayscale image by determining its embedding positions using a logistic map. In the second stage, data extraction, the embedded message is retrieved using the logistic map, and the extracted message is XORed with the tent map to recover the original data. The effectiveness of the proposed method was evaluated using commonly employed metrics such as PSNR, MSE, and SSIM on images in the literature. The results demonstrate that the proposed method offers a robust structure against steganalysis techniques while ensuring critical security parameters.

# Veri Gizlemede Kaotik fonksiyonlar ve XOR İşlemi Tabanlı Etkili bir Steganografi Yöntemi

**Anahtar Kelimeler:**
Steganografi
Kaotik fonksiyonlar
Logistic harita
Tent harita

## ÖZ

Gelişen teknoloji ve dijitalleşen dünya, güvenli veri iletiminin önemini artırmaktadır. Steganografi, verilerin güvenli bir şekilde iletilmesini ele alan ve veri güvenliğinin kritik bir parçasını oluşturan bir tekniktir. Türkçe'de "gizli yazı" anlamına gelen steganografi, gizlenmek istenen verinin taşıyıcı bir veri aracılığıyla aktarılması esasına dayanır. Tarihsel olarak ilkel yöntemlerle uygulanan steganografi, dijitalleşen dünya ile birlikte modern tekniklerin ve yöntemlerin kullanımına geçiş yapmıştır. Bu çalışmada, kaotik fonksiyonlar ve XOR işlemi tabanlı bir steganografi yöntemi önerilmektedir. Önerilen yöntem iki aşamadan oluşmaktadır. Birinci aşama olan veri gömme işleminde, gizlenecek veri önce ikilik formata dönüştürülür. Ardından bu veri, tent map dizisi ile XOR işlemine tabi tutulur. Bu işlem sonucunda elde edilen nihai veri, logistic map kullanılarak gri seviye bir görüntünün gömüleme pozisyonları belirlenerek yerleştirilir. İkinci aşama olan veri çıkarma işleminde, logistic map yardımıyla gömülü mesaj çıkarılır ve çıkarılan bu mesaj tent map ile XOR işlemine tabi tutularak orijinal veri elde edilir. Önerilen yöntemin etkinliği, literatürdeki görüntüler üzerinde gerçekleştirilen PSNR, MSE ve SSIM gibi metriklerle test edilmiştir. Sonuçlar, yöntemin steganaliz tekniklerine karşı dayanıklı bir yapı sunduğunu ve güvenlik parametrelerini sağladığını göstermiştir.

[*]**Corresponding Author**

[*](selman.yakut@inonu.edu.tr) ORCID ID 0000-0002-0649-1993

**e-ISSN: 2717-8579**

**Geliş Tarihi: 29/11/2024; Kabul Tarihi: 28/12/2024**

## 1. INTRODUCTION

Data security is a fundamental requirement in the advancing technological and digital world. Numerous algorithms, security systems, protocols, and similar approaches have been proposed to ensure data security. One of the critical components of data security is steganography, which translates to "hidden writing." Steganography involves embedding any message that needs to be transmitted into a carrier medium in a way that prevents it from being detected (Kipper, 2019). While historically performed using primitive methods, steganography now requires modern techniques and approaches due to technological advancements. The ever-growing volume of data and its transmission in today's digital era further emphasizes its importance.

In the literature, various steganography methods have been proposed depending on factors such as the type of carrier data and the method used (Kipper, 2019). The carrier medium and the type of transmitted message can include various formats such as video, images, text, or audio signals (Cheddad, Condell, Curran, & Mc Kevitt, 2010). Additionally, the techniques used may differ based on whether the data is manipulated in the spatial domain or frequency domain (Karakış, Gürkahraman, Çiğdem, Öztoprak, & Topaktaş, 2021). The Least Significant Bit (LSB) algorithm is widely used in various data types, particularly images and videos (Akyüz, 2021). To enhance the security of steganography algorithms and approaches, additional operations and functions are employed alongside LSB bits. One such function is chaotic functions, which exhibit chaotic properties based on specific parameters (Yakut, Tuncer, & Ozer, 2019). These functions are utilized in various fields to address complex problems (Özbay, 2023). In the literature, chaotic functions are applied in diverse ways to develop steganography methods. By employing chaotic functions, the selection of LSB bits for embedding data can lead to effective and secure steganography methods.

In this study, a new steganography method is proposed for secure data transmission. The proposed method combines chaotic functions and the XOR operation to provide a complex and secure steganographic structure. Initially, the data to be embedded is encrypted by XORing it with a chaotic sequence generated using the tent map. The encrypted data is then embedded into the LSB bits of pixels at specified positions in a grayscale image, with these positions determined using the logistic map. The proposed method ensures two levels of security by utilizing chaotic functions for both the encryption process and the determination of embedding positions in the grayscale image. Furthermore, tests conducted using analysis tools such as PSNR, SSIM, and MSE demonstrate the effectiveness of the proposed approach. Additionally, the random outputs and efficiency of the chaotic functions used further validate the effectiveness of the proposed method.

This study is organized as follows: Section 2 presents the related literature. Section 3 describes the proposed approach. Section 4 provides the experimental results of the proposed approach. Finally, Section 5 concludes the study.

## 2. LITERATURE REVIEW

In the literature, numerous approaches to steganography have been proposed based on parameters such as the type of carrier data, the data to be transmitted, and the methods employed. Among these, the use of images as carriers for transmitting secret messages is one of the most commonly utilized steganographic mediums. For such transmissions, one of the earliest and simplest approaches involves embedding data into the least significant bits (LSBs) of the carrier medium. Additionally, the use of frequency domain transformations for data embedding is also prevalent (Kipper, 2019). To determine the embedding positions and ensure the security of transmitted data, various approaches have been explored in the literature. Among these, chaotic functions are widely employed. Chaotic functions are frequently used in areas such as data hiding and encryption to enhance data security (Akyüz, 2021). Their properties of randomness and unpredictability make them highly effective in increasing security in steganographic applications. The use of chaotic functions in data hiding is well-documented in the literature.

Khalil et al. proposed a novel data hiding algorithm utilizing 1D and 2D chaotic maps combined with LSB techniques for concealing various types of data (images, text, audio) within cover images of different dimensions, achieving successful test results (Khalil, Sarhan, & Alshewimy, 2024). Pak et al. introduced an improved one-dimensional chaotic map, demonstrating superior performance compared to existing models, and aimed to enhance the robustness of the LSB steganography algorithm against attacks using this model (Pak et al., 2020). Tiwari et al. implemented data hiding in images by employing two chaotic systems: the first determined the pixel positions for data embedding, while the second set the initial conditions for the first chaotic system (Kumar Tiwari, Rajpoot, K. Shukla, & Karthikeyan, 2015). Nasr et al. combined chaotic Henon, Baker, and Arnold maps with audio steganography to propose a secure data hiding method for image encryption (Nasr et al., 2024).

Ghosh et al. combined a chaotic 2D classical map and a linear feedback shift register, demonstrating that this approach effectively enhances encryption security and plays a vital role in ensuring data privacy and security in medical image steganography within healthcare networks (Ghosh, Saha, Pal, & Jha, 2024). Alzubi et al.

introduced a novel image hiding formula based on a chaotic map system employing Tent map, Singer map, and Logistic map for pixel- and bit-level scrambling, which can be used in sensitive fields such as military and healthcare (Alzubi, Alzubi, Suseendran, & Akila, 2019). Kumar and Hussaini proposed an effective method combining an artificial neural network and a cyclic chaos algorithm to select the best cover image, enhancing visual quality, hiding capacity, and security (Kumar & Hussaini, 2021).

López Torres et al. proposed a crypto-steganography algorithm combining chaos, DNA coding, and edge-based techniques, achieving high similarity and low error between the original and stego images (López Torres, Alvarado-Nieto, Amaya-Barrera, & Parra, 2024). Durafe and Patidar presented a novel and effective color image steganography model, combining DNA-hyperchaotic encryption and DWT-SVD embedding techniques using unique fractal cover images, which can be applied across various fields (Durafe & Patidar, 2024). Karakış et al. demonstrated a method for medical image steganography that conceals data in non-tumor pixels using discrete wavelet transform and k-means clustering-based segmentation, preserving image fidelity while securely storing large patient data (Karakış et al., 2021).

Ranjithkumar et al. utilized chaotic maps to propose a video steganography method with three-layered security, embedding data into the spatial domain of cover video frames to ensure confidentiality (Ranjithkumar, Ganeshkumar, & Senthamilarasu, 2021). Nagarajegowda and Krishnan introduced an efficient video steganography method embedding audio or image-based secret data into a cover video, using a hybrid algorithm combining 2D-Henon and 3D-Logistic maps for encryption (Nagarajegowda & Krishnan, 2024).

Madhu et al. combined a dynamic 8-bit XOR algorithm with the AES encryption algorithm to securely store hidden data in images, achieving effective results (Madhu, Vasuhi, & Samydurai, 2024). Balkesen and Koçer proposed an approach that embeds AES-encrypted data into random bit positions of the cover image (Balkesen & Koçer, 2020).

The literature highlights the widespread use of XOR operations and chaotic functions in steganographic approaches. Their combined application facilitates the development of effective and secure data embedding techniques. Chaotic functions, known for their ability to generate unpredictable sequences, offer robust solutions in steganography. Additionally, XORing data with chaotic functions before embedding can provide dual-layer security.

## 3. PROPOSED METHOD

In this study, a steganography method utilizing Logistic Map and Tent Map chaotic functions in combination with the XOR operation is proposed for secure data transmission. The proposed method consists of two main components: embedding the secret message into the carrier data and extracting the embedded message from the carrier data. The chaotic functions, which form the core of the proposed method, are introduced first, followed by a detailed discussion of the data embedding and extraction processes.

### 3.1. Chaotic Functions

Chaotic functions, due to their sensitivity to initial conditions and their capacity to generate randomness, are widely used in security-critical applications such as encryption, steganography, and random number generation (Yakut et al., 2019; Yakut, Tuncer, & Özer, 2020). Although these functions have simple mathematical equations, they exhibit chaotic behavior under specific parameter values. For these parameter values, chaotic functions produce unpredictable and non-deterministic sequences.

These functions are highly sensitive to initial conditions in their chaotic parameter ranges. In other words, a small change in the initial value can lead to significant differences in the system's subsequent behavior. This sensitivity makes them highly suitable for applications such as random number generation and encryption, where unpredictability and randomness are essential.

### 3.1.1. Logistic Map

The logistic map generates the next value x( n+1) based on the previous value $x(n)$ using the following equation:

$$x(n+1) = r * x(n) * \left(1 - x(n)\right) \tag{1}$$

Here, $xn$: Represents the state at the n-th iteration, taking values between 0 and 1. $r$: A control parameter, typically chosen between 0 and 4, which determines the behavior of the logistic map.

The value of the control parameter $r$ dictates whether the logistic map exhibits chaotic behavior. For instance, values of $r$≥3.57 tend to trigger chaotic dynamics.

### 3.1.2. Tent Map

The Tent Map is a mathematical example of a chaotic dynamical system commonly used in applications requiring randomness or chaos. It generates a chaotic sequence by iteratively updating a value within a specific range (e.g., [0,1]).

The Tent Map produces new values through iterations based on an initial value and a control parameter.

Mathematically, the Tent Map is defined by an $x$ value and a parameter $\mu$ as follows:

$$x(n+1) = \begin{cases} \mu * x(n), & x(n) < 0.5 \\ \mu * (1 - x(n)), & other \end{cases} \tag{2}$$

Here, $xn$: Represents the value at each iteration. $\mu$: A control parameter (typically set to 2.0) that influences the chaotic behavior of the system. Adjusting the value of $\mu$ directly affects the chaotic dynamics of the Tent Map.

### 3.2. Embedding Function

In the proposed method, the final state of the data to be embedded and its embedding positions are determined using chaotic functions and the XOR operation. The pseudocode for the embedding function is provided in Algorithm 1. Initially, the message to be hidden is converted into a byte array in UTF-8 format. It is then encrypted using the chaotic sequence generated by the Tent Map function through an XOR operation. This encryption enhances the security of the message and allows decryption during the extraction process using the same Tent Map sequence. Subsequently, the encrypted bytes are split into bits and embedded into random bit positions specified by the Logistic Map sequence. The Logistic Map determines the exact locations within the image where each bit will be embedded, enabling the message to be concealed by altering the specified bit positions in the image. This process ensures that the data is hidden within the image with no noticeable changes to its visual appearance.

**Algorithm 1.** Embedding function pseudocode

```
- Embeding Function
  Input: image_path, message (secret message)
  Output: Image with embedded message (stego_image)

  - Convert the message to a byte array
  - Open the image at image_path, and load into array
  - Generate chaotic sequences:
    - length = size of message in bytes * 8
    - logistic_seq = call logistic map function
    - tent_seq = call tent map function
  - Encrypt the message with XOR
  - Convert encrypted bytes to bits
  - Embed each bit of encrypted message in positions
defined by Logistic map:
    - Create flat_img_data
    - Loop for i = 0 to length of encrypted_bits:
      - pos = i mod flat_img_data length
      - bit_pos = logistic_seq[i]
      - Clear bit at bit_pos in flat_img_data[pos] and
replace it with encrypted_bits[i]
  - Reshape flat_img_data to original image shape and
return stego_image
```

### 3.3. Extracting Function

The algorithm for extracting the hidden message in the proposed method is provided in Algorithm 2. During the extraction process, the values of the chaotic functions are recalculated. These values are then used to determine the bit positions. Using the same chaotic sequences and positions, the embedded bits are read from the image, and the original byte sequence is reconstructed. The extracted bit sequence is then decrypted by applying the XOR operation with the Tent Map sequence, recovering the original message. In this method, chaotic sequences not only ensure randomness during the embedding process but also act as keys for XOR encryption, enhancing security. By leveraging the randomness properties of chaotic systems, the message is securely encrypted and inconspicuously embedded within an image.

**Algorithm 2.** Extracting function pseudocode

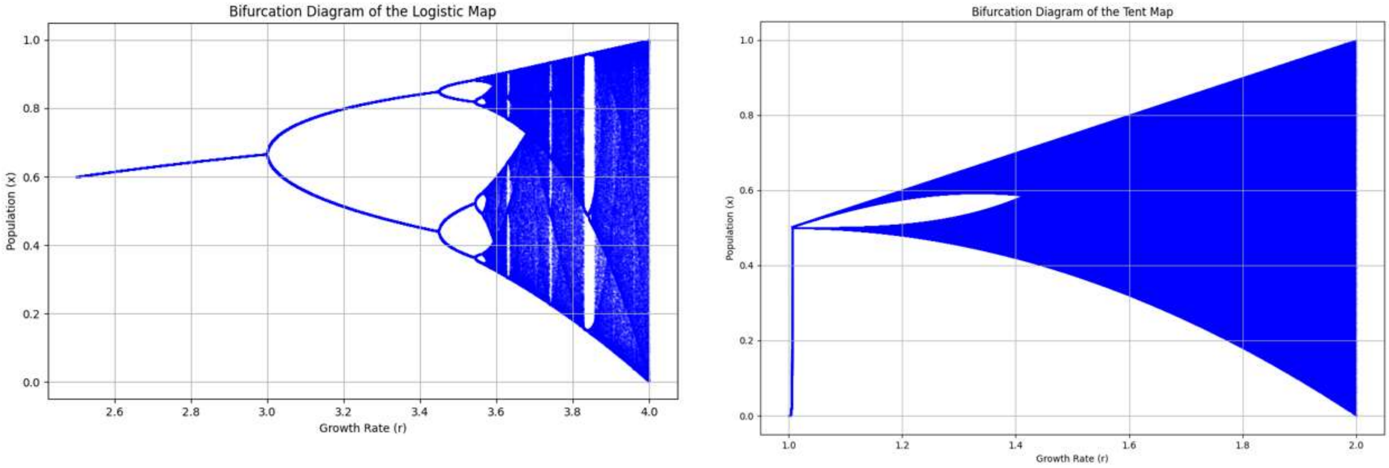
```
- Extracting Function
  Input: Image with embedded message (stego_image)
  Output: Message (secret message)

- Load the stego image, and load into array
  - Generate chaotic sequences:
    - bit_length = message_length * 8
    - logistic_seq = call logistic map function
    - tent_seq = call tent map function
  - Extract encrypted bits from specified positions:
    - Create flat_img_data (flattened image data)
    - Initialize an empty extracted_bits array
    - Loop for i = 0 to bit_length:
      - pos = i mod flat_img_data length
      - bit_pos = logistic_seq[i]
      - Extract bit at bit_pos in flat_img_data[pos] and add
it to extracted_bits[i]
  - Convert extracted_bits back to bytes
  - Decrypt the extracted data with XOR
  - Convert byte array to a UTF-8 string and return
return UTF-8 string (secret message)
```

## 4. EXPERIMENTAL RESULS

Various parameters were used to assess the security and effectiveness of the proposed approach. These parameters primarily include robustness and imperceptibility. Robustness refers to the system's ability to retrieve the embedded data even when subjected to various attacks. Additionally, since chaotic functions are employed in the proposed approach, the randomness of these functions was also evaluated. Furthermore, the combined use of XOR encryption and chaotic bit selection provides a dual-layer security mechanism. XOR is a simple yet powerful operation commonly used in encryption and steganography due to its bit-level functionality, reversibility, and masking capabilities. Its ability to recover the original data when applied twice with the same key offers a significant advantage in security applications. Thus, the proposed method ensures both data confidentiality and security. To demonstrate the effectiveness of the method, the message embedded in grayscale images was: "In this study, a steganography approach based on chaotic functions and the XOR method was proposed."

The chaotic functions used in the proposed approach, namely the Logistic Map and Tent Map, enhance the security of data embedding by leveraging their randomness properties. Chaotic functions such as the Logistic Map and Tent Map are widely utilized in data hiding and encryption to ensure data security. The unpredictability and randomness properties of chaotic maps are essential for enhancing security in steganographic applications. In the proposed approach, chaotic functions form the core of data masking and embedding processes. These functions were selected because of their simplicity and effectiveness. Parameter values were carefully chosen to ensure the chaotic behavior of the maps, as these maps exhibit extreme sensitivity to initial conditions within their chaotic parameter ranges.

In bifurcation diagrams, it can be observed that as the control parameter values of the Logistic and Tent Maps increase, their dynamic behaviors evolve. For both maps, the system remains stable at lower parameter values, with the population converging to a single fixed point. In the Logistic Map, as the parameter value increases, the system transitions to periodic oscillations, resulting in bifurcations that produce 2, 4, 8, and so on, periodic cycles. When the parameter exceeds 3.57, the system becomes entirely chaotic. Similarly, in the Tent Map, the system converges to a fixed point within the range of 0–1, exhibits periodic behavior within the range of 1–2, and demonstrates chaotic behavior for parameter values greater than 2.



(a) (b)

**Figure 1.** (a) Bifurcation diagram of the Logistic Map, (b) Bifurcation diagram of the Tent Map

### 4.1. Imperceptibility Anaysis

Imperceptibility refers to the inability to detect changes in the carrier image after data embedding. While these changes may sometimes be visually noticeable, they are often evaluated using various steganalysis methods. To measure the difference between the carrier image and the stego image containing the embedded data, the PSNR (Peak Signal-to-Noise Ratio) metric was used. PSNR quantifies pixel-level differences between two images and compares them against noise levels. A high PSNR value indicates that the embedded data is imperceptible. PSNR provides a numerical representation of the similarity between the original image and a distorted or reconstructed image. It is generally accepted that a PSNR value above 30 dB signifies imperceptibility of the embedded data. The relevant equation is provided in Equation (3). In the equation, $R$ denotes the maximum pixel value in the image.

$$PSNR = 10.\log_{10}(\frac{R^2}{MSE}) \tag{3}$$

MSE (Mean Squared Error) represents the average squared difference between corresponding pixels of two images. It is calculated as the mean of the squared differences between the pixel values of the original image and the reconstructed (or distorted) image. The formula for MSE is provided in Equation (4).

In the equation: $m$, $n$: Represent the dimensions of the image (height and width). $I(i, j)$: Denotes the pixel value at $(i, j)$ in the original image. $K(i, j)$: Denotes the pixel value at $(i, j)$ in the reconstructed (or distorted) image.

$$MSE = \frac{1}{m.n}\sum_{i=1}^{m}\sum_{j=1}^{n}(I(i,j) - K(i,j))^2 \tag{4}$$

SSIM (Structural Similarity Index) is widely used to evaluate the performance of image processing techniques such as compression, image restoration, noise reduction, and others. The operations for calculating SSIM are provided in Equation (5).

In the equation: $I(i, j)$: Represents the intensity of the pixel at $(i, j)$ in the original (carrier) image. $I'(i, j)$: Represents the intensity of the pixel at $(i, j)$ in the stego image (containing the hidden message). $M, N$: Denote the dimensions of the image, where $M$ is the number of rows and $N$ is the number of columns.

$$\text{SNR} = 10.\log_{10}\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M} I(i,j)^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(I(i,j) - I(i,j))^2}\right) \tag{5}$$

The SPSNR, MSE, and SSIM test results for the proposed approach are presented in Table 1. The obtained results indicate that the differences between the two images are minimal, demonstrating that the steganography process has a negligible impact on both visual quality and structural similarity. These parameters serve as indicators of the effectiveness of the proposed method.

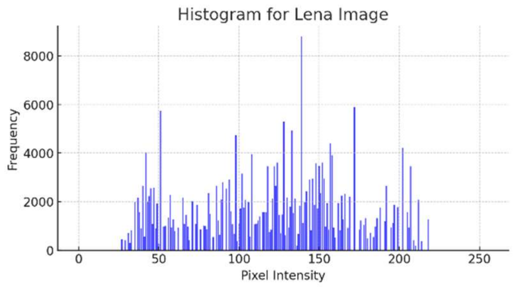
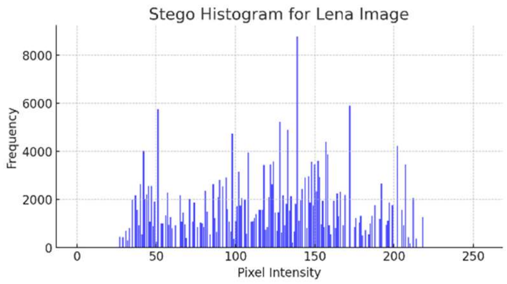
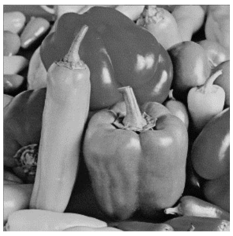
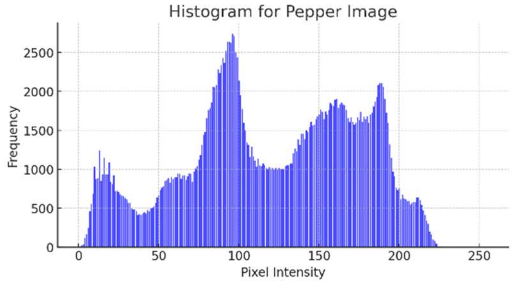
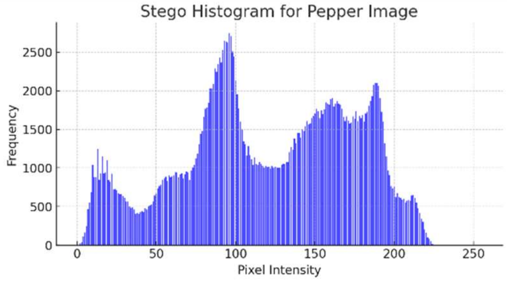
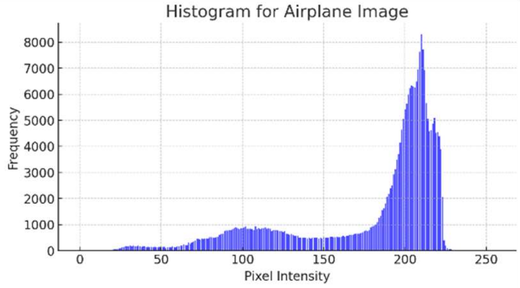
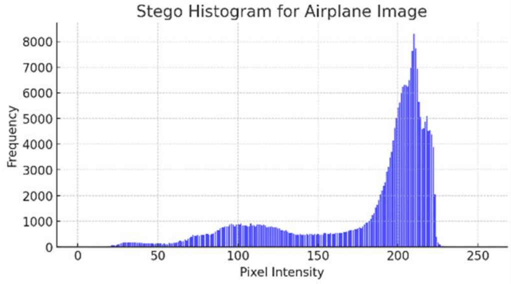
**Table 1.** SPSNR, SSIM, and MSE test results of the proposed method

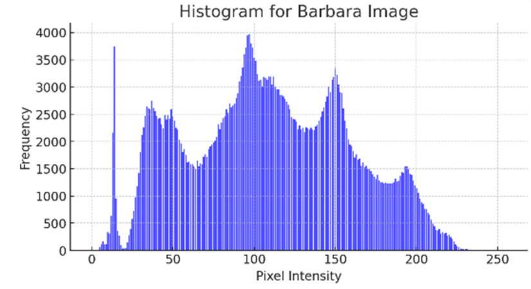
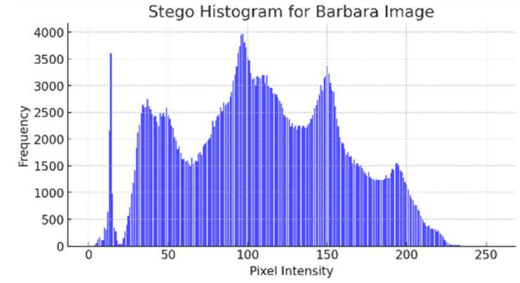
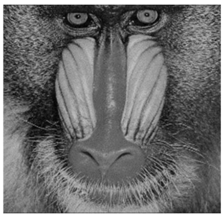
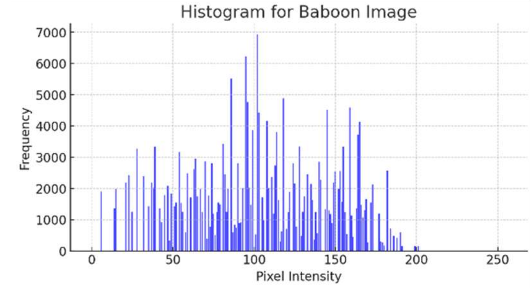
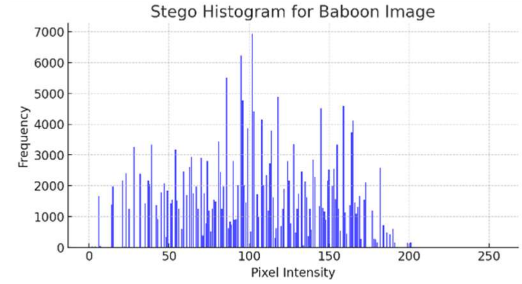
| | MSE | SSIM | PSNR |
|---|---|---|---|
| Lena | 0.0085 | 0.9979 | 68.86 dB |
| Paper | 0.010967 | 0.9990 | 67.73 dB |
| Airplane | 0.0084 | 0.9984 | 68.88 dB |
| Barbara | 0.0067 | 0.9994 | 69.88 dB |
| Baboon | 0.0096 | 0.9992 | 68.33 dB |

## 4.2. Histogram Analysis

Histogram analysis is a fundamental tool for evaluating the security and imperceptibility of steganography. Histograms assess the impact of the embedding process on visual quality and reveal differences between the original image and the stego image. The histogram results for the proposed method are presented in Table 2. In the proposed approach, histogram analysis examines changes in pixel intensity distributions when the message is embedded into the image (stego image). The similarity of the histograms indicates that the steganography process is imperceptible. Since there are no significant changes in the histogram, the embedding process remains undetectable.

**Table 2.** Histogram analysis results of the proposed method for commonly used ımages in the literature

| Orijinal resim | The histogram value of the original image | The histogram value of the stego image |
|---|---|---|
| Lena |  |  |
|  Paper |  |  |
| Airplane |  |  |

| | | |
|---|---|---|
| <br>**Barbara** |  |  |
| <br>**Baboon** |  |  |

## 5. CONCLUSION

In this study, an effective data hiding algorithm was proposed by combining chaotic functions and XOR operations. In the proposed approach, the Logistic Map was used to determine the pixels where data would be embedded, while the Tent Map was employed to generate data for encrypting the original message. The original data was encrypted by XORing it with the output of the Tent Map chaotic function. By combining two chaotic functions with XOR operations, the algorithm provides a dual-layered security mechanism, preventing the extraction and decryption of the embedded data. The proposed algorithm was tested using commonly used images from the literature, with results evaluated through PSNR, MSE, and SSIM metrics. Additionally, the histogram analysis results for the same images were presented. The test results demonstrate the success of the proposed method on these images. Moreover, the randomness tests for the chaotic functions indicate that the algorithm prevents predictability. The tests conducted on grayscale images and the successful application results further validate the effectiveness of the proposed algorithm.

In future work, the proposed method is intended to be adapted for video steganography. The performance of the chaotic functions enables the algorithm to be applied to such data. Additionally, the application of the proposed method to data in the frequency domain could provide effective solutions for these approaches as well.

## REFERENCES

Akyüz, D. (2021). Yeni Kaotik Video Steganografi Metodu. İstanbul Ticaret Üniversitesi.

Alzubi, J. A., Alzubi, O. A., Suseendran, G., & Akila, D. (2019). +A Novel chaotic map encryption methodology for image cryptography and secret communication with steganography. International Journal of Recent Technology and Engineering, 8(1C2), 1122–1128.

Balkesen, C., & Koçer, H. E. (2020). Şifrelenmiş Verileri Rast Gele Piksel Yaklaşımı ile Bir Görüntüye Gömme. European Journal of Science and Technology, (September), 123–130. https://doi.org/10.31590/ejosat.802191

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. https://doi.org/10.1016/j.sigpro.2009.08.010

Durafe, A., & Patidar, V. (2024). Image Steganography Using Fractal Cover and Combined Chaos-DNA Based Encryption. Annals of Data Science, 11(3), 855–885. https://doi.org/10.1007/s40745-022-00457-x

Ghosh, S., Saha, A., Pal, T., & Jha, A. K. (2024). A comparative analysis of chaos theory based medical image steganography to enhance data security. Procedia Computer Science, 235, 1024–1033. https://doi.org/10.1016/j.procs.2024.04.097

Karakış, R., Gürkahraman, K., Çiğdem, B., Öztoprak, I., & Topaktaş, A. S. (2021). Bölütlenen beyin bölgelerinin tıbbi görüntü steganografi için değerlendirilmesi. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 36(4), 2301–2314. https://doi.org/10.17341/gazimmfd.753989

Khalil, N., Sarhan, A., & Alshewimy, M. A. M. (2024). A secure image steganography based on LSB technique and 2D chaotic maps. Computers and Electrical Engineering, 119(PB), 109566. https://doi.org/10.1016/j.compeleceng.2024.109566

Kipper, G. (2019). Investigator's Guide to Steganography. New York.

Kumar, M., & Hussaini, T. (2021). A Neural Network Based Image Steganography Method using Cyclic Chaos and Integer Wavelet Transform. 2021 Asian Conference on Innovation in Technology, ASIANCON 2021, 1–6. https://doi.org/10.1109/ASIANCON51346.2021.9544831

KumarTiwari, A., Rajpoot, A., K. Shukla, K., & Karthikeyan, S. (2015). A Robust Method for Image Steganography based on Chaos Theory. International Journal of Computer Applications, 113(4), 35–41. https://doi.org/10.5120/19817-1637

López Torres, E. A., Alvarado-Nieto, D., Amaya-Barrera, I., & Parra, C. A. S. (2024). Crypto-steganographic model using chaos and coding based in deoxyribonucleic acid. International Journal of Electrical and Computer Engineering, 14(4), 4239–4247. https://doi.org/10.11591/ijece.v14i4.pp4239-4247

Madhu, D., Vasuhi, S., & Samydurai, A. (2024). Dynamic 8-bit XOR algorithm with AES crypto algorithm for image steganography. Signal, Image and Video Processing, 18(Suppl 1), 429–445. https://doi.org/10.1007/s11760-024-03165-6

Nagarajegowda, S., & Krishnan, K. (2024). An adaptive approach for multi-media steganography using improved chaotic map and discrete cosine transform. Signal, Image and Video Processing, 18(10), 6695–6711. https://doi.org/10.1007/s11760-024-03345-4

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. https://doi.org/10.1038/s41598-024-70940-3

Özbay, F. A. (2023). A modified seahorse optimization algorithm based on chaotic maps for solving global optimization and engineering problems. Engineering Science and Technology, an International Journal, 41, 101408. https://doi.org/10.1016/j.jestch.2023.101408

Pak, C., Kim, J., An, K., Kim, C., Kim, K., & Pak, C. (2020). A novel color image LSB steganography using improved 1D chaotic map. Multimedia Tools and Applications, 79(1–2), 1409–1425. https://doi.org/10.1007/s11042-019-08103-0

Ranjithkumar, R., Ganeshkumar, D., & Senthamilarasu, S. (2021). Efficient and secure data hiding in video sequence with three layer security: an approach using chaos. Multimedia Tools and Applications, 80(9), 13865–13878. https://doi.org/10.1007/s11042-020-10324-7

Yakut, S., Tuncer, T., & Ozer, A. B. (2019). Secure and efficient hybrid random number generator based on sponge constructionsfor cryptographic applications. Elektronika Ir Elektrotechnika, 25(4), 40–46. https://doi.org/10.5755/j01.eie.25.4.23969

Yakut, S., Tuncer, T., & Özer, A. B. (2020). A New Secure and Efficient Approach for TRNG and Its Post-Processing Algorithms. Journal of Circuits, Systems and Computers, 29(15). https://doi.org/10.1142/S0218126620502448