International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No. # (Mon-20..)

http://dx.doi.org/10.12785/ijcds/XXXXXX

Image Steganography Technique based on Lorenz Chaotic System and Bloom Filter

Ahmad Salim[1], Khitam Abdulbasit Mohammed[2], Farah Maath Jasem[2] and Ali Makki Sagheer[2]

[1]*Middle Technical University, Baghdad, Iraq*
[2]*College of Computer Science and Information Technology, University of Anbar, Anbar, Iraq*

[1]*Received XX Mon. 20XX, Revised XX Mon. 20XX, Accepted XX Mon. 20XX, Published XX Mon. 20XX*

Abstract: Steganography is the study of invisible communication, which typically focuses on methods of concealing the existence of the communicated message. Steganography is now widely used as a means of protecting sensitive data. In addition, one of the most common methods of information hiding is the Least Significant Bit (LSB) technique. This technique is extremely vulnerable to statistical attacks which are still challenging. This article presents a new method by using Lorenz's chaotic system to generate a series of pseudo-random positions for embedding secret information within the cover image. Moreover, the Bloom filter is suggested to be used to prevent repetition and storage in the same pixel as well as data loss. The similarity metric results show how powerful and secure the proposed method is against both visual and analytical attacks, with a PSNR of 48.57% and a NPCR of 32.35%.

Keywords: Information security, Steganography, Image encryption, Chaotic system, Lorenz system, Bloom filter

1. INTRODUCTION

The protection and integrity of digital information are increasingly dependent on information security in today's Internet and technologically advanced world. Due to the widespread adoption of digital technologies, an ever-increasing volume of data is generated, transmitted, and stored. The possibility of cyberattacks and data breaches has also increased. Hence, Information security must protect numerous types of data, including personal, financial, confidential, and sensitive data such as healthcare data, biometrics, as well as trade secrets and intellectual property [1][2]. Information security includes a wide range of practices and measures, such as cryptography and steganography, to prevent unauthorized access, data theft, and data misuse.

Moreover, cryptography is a study of secure communication techniques, including encryption, which involves converting plaintext data into ciphertext to protect its confidentiality from unauthorized access or interception [3]. Steganography refers to the practice of concealing secret messages or data (stego-data) within another data (cover), such as images, audio files, or video, in a way that is undetectable to unauthorized parties [4]. Images are commonly used as a cover for hiding information because of the high level of redundancy, they are ubiquitous and could store large amounts of data. it is easily can be shared and transmitted. Unlike cryptography, which secures information by encoding it, steganography conceals information by embedding it within other seemingly innocuous data, making it invisible to anyone who is not looking for it [5][6]. It has been used in various applications, such as covert communication, digital watermarking, and copyright protection.

Besides, it has been implemented by using various techniques, such as spatial domain, transform domain or spread spectrum techniques. There are several weaknesses in using spread spectrum techniques in steganography such as: limited capacity, susceptibility to detection, computational complexity, and vulnerability to collusion attacks. Moreover, The Least Significant Bit (LSB) technique is commonly used in image steganography [7][8]. However, this technique has deficiencies in terms of robustness and resistance to statistical assaults. In addition, common drawbacks of transform domain techniques in image steganography include the potential for cover image distortion or information loss, as well as being prone to statistical analysis attacks.

Despite being deterministic, the outcomes of chaotic systems are highly unpredictable due to their sensitivity to initial conditions. Nonlinear dynamics characterize the behavior of chaotic systems, which can result in intricate patterns and structures. Chaotic systems have applications in various fields, including physics, biology, economics, and cryptography [9][10]. However, the design and analysis of chaotic systems require advanced mathematical techniques and computational simulations.

This study aims to develop a new method that utilizes chaotic systems to generate a series of pseudo random image positions. In these positions, sensitive data is concealed, making it difficult for attackers and intruders to access it even if they detect its presence.

The outline for this article is as follows: section 1 presents a comprehensive introduction to the technique of Steganography and its various applications. Section 2 presents the literature review. The procedure method of the Bloom filter and the chaotic Lorenz system will be presented in the third and fourth sections. The proposed system will be presented in section five and the sixth section will discuss the most results. In conclusion, the article's findings and implications are summarized in section seven.

2. Literature Review

Steganography is the method of secretly encoding data in an unidentifiable form within a cover object. Identifying the locations where a secret data is concealed within images is a big challenge for researchers. Thus, numerous methods have been developed and suggested to overcome the common attacks on traditional methods of concealment. One of the techniques used in the field of information steganography is meta-heuristic algorithms. For instance, [11] proposed a steganography technique that used the Bee Colony Optimization (BCO) algorithm to optimize the embedding of secret information within an image. Moreover, the technique used Optical Pixel Adjustment to ensure the steganographic image's ability to remain visually similar to the original image. On another hand, [12] presented a steganography technique that used the Fractional Grey Wolf Optimization (FGWO) algorithm to identify interesting regions within a video frame for embedding secret information. As the efficiency of the method is quite important, the researcher used multi-objective cost function to ensure the steganographic video remains perceptually similar to the original video. Both studies proposed steganography methods that make use of optimization algorithms to covertly insert information into digital media without compromising its original visual quality. However, the proposed techniques have the drawback of requiring a significant amount of processing power and sufficient time to finish the optimization procedure.

Furthermore, deep learning is widely used to hide secret information within images [13][14]. [13] suggested a novel image steganography technique based on deep convolutional networks (DCNs). The proposed technique proves the ability to hide secret images into cover images by replacing the high-frequency components of the cover with those of the secret image. The proposed technique may not be effective for embedding large secret images into cover images due to limitations in the size of a high-frequency components that can be replaced. In [14] the authors proposed an image steganography method with deep learning-based edge detection to hide secret messages in digital images. The proposed technique consists of two stages: first, the image is preprocessed to extract its edges utilizing DCNs, and second, the secret message was embedded into the edges of the image using a binary code. However, the proposed technique is ineffective if the input image contains low-contrast edges.

Moreover, several scientific studies suggested using chaotic systems to hide confidential information within images. In [15], the authors proposed a steganographic method to improve the systems of chaotic range. The proposed technique aimed to enhance the security and robustness of steganography against various attacks, such as statistical analysis and visual detection. The proposed technique achieved a high embedding capacity and ensured low distortion of the cover image. The outcomes prove the proposed technique is suitable for various applications, including medical image transmission.

Many efforts have been made by researchers to construct an optimal solution. In [16], a new steganography technique that utilized chaos theory to embed secret data in digital images. The proposed algorithm applies the logistic map to generate a chaotic sequence which is used to select the embedding locations in the cover image. After encrypting the secret data using a symmetric key algorithm, it is then embedded into the cover image using a modified version of the Least Significant Bit (LSB) technique. Besides, the proposed algorithm included a recovery process that extracts the secret data from the cover by using the same chaotic sequence and symmetric key used in the embedding process. The authors evaluated the performance of the proposed algorithm by conducting experiments on various digital images and comparing it with several existing steganography techniques. The outcomes indicate high embedding capacity, good visual quality, and robustness against various attacks. Nevertheless, there is not enough attention paid to the computational complexity and the effect of embedding on image quality during the verification process. A method for hiding secret data within images using chaotic systems and polygonal shapes was suggested by [17]. The proposed method applied a unique procedure by dividing the cover image into small polygonal regions and then encrypting the secret data using a chaotic map. The encrypted data were entrenched into the rectangular region using a specific algorithm. The proposed method has been examined on several standard images and was compared with the existing steganographic methods. The outcomes prove that the suggested method achieved more image quality and security than the previous studies. However, using chaotic maps and polygonal shapes limits practical usage.

Finally, a study was proposed to protect users' sensitive data from being leaked to unauthorized parties while ensuring the efficient transmission of information within the IoT network [18]. The study presented the theoretical foundations of steganography and chaotic functions. Moreover, the study demonstrated the procedure for creating a secure and efficient communication protocol for the IoT. The proposed solution used a combination of chaos-based encryption and steganography to hide sensitive data in non-sensitive data, which is then transmitted through the IoT network.

In summary, the proposed techniques for selecting hiding positions for secret information within images suffer from several weaknesses, including the reliance on features within the images that can be detected and thus reduce the amount of data that can be concealed. Additionally, the use of complex techniques for selecting positions and hiding data can result in system resource wastage. Furthermore, the potential conflicts that may arise in selected hiding locations are not taken into consideration. The analysis of various steganographic techniques shown in Table 1. Considering all of the aforementioned points, these factors motivate us to propose a new method in an attempt to improve the process of concealing secret data within digital images.

3. Lorenz Chaotic System

Numerous schemes for image encryption based on chaotic mapping have been proposed recently. Chaotic systems have garnered significant attention in various fields, including database security, the Internet, transactions, and banking Due to their high sensitivity to initial conditions and parameters. Cryptography provides robust encryption capabilities, which has increased interest in chaotic schemes. Thus, a chaotic cryptographic system is impervious to statistical attacks. Even though this field has achieved good accomplishments, unfortunately, existing encryption/decryption algorithms still face limitations that restrict their applicability to real systems. Consequently, in 1963, American scientist Lorenz made a significant discovery while studying the weather, introducing a system known as the Lorenz system (LS) [19][20]. The three dimensions of the LS are shown in Equations (1, 2, and 3), which is considered a dynamic equation [21].

$$\frac{dx}{dt} = a(y - x) \tag{1}$$

$$\frac{dy}{dt} = cx - xz - y \tag{2}$$

$$\frac{dz}{dt} = xy - bz \tag{3}$$

a, b, and c represent the parameters of the LS, where $a = 10$, $b = 2.66$, and $c \geq 24.75$ are considered the optimal values for these parameters. Figure (1) showcases the chaotic attractors produced by the LS [21]. The figure illustrates a noticeable distinction among the three variables (x, y, and z), indicating their non-periodic nature and unpredictability. Furthermore, the system's dynamic trajectory manifests as a three-dimensional double-helix structure [22][23].

The LS possesses several features that render it advantageous for cryptographic purposes. The following aspects are particularly crucial: the equations' six parameters (x, y, z, a, b, and c) can expand the key space, increasing the key's predictability difficulty. Additionally, the system's multidimensionality adds complexity to its dynamics [24].

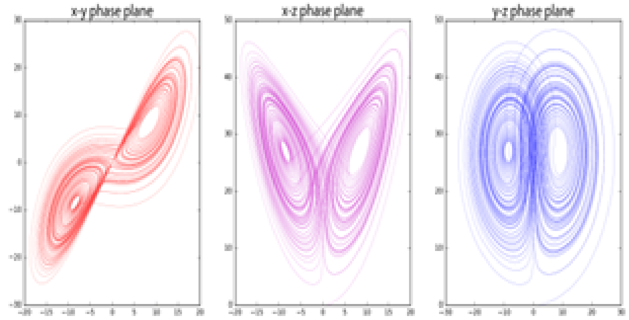

Figure 1. Lorenz system chaotic attractors.

Chaotic systems offer certain desirable properties such as sensitivity to initial conditions, unpredictability, and potential for high entropy. Chaotic sequences may exhibit better statistical properties and increased resistance against certain attacks. Therefore, chaotic systems are considered more advantageous for cryptography and secure communication compared to other systems for generating random sequences, such as Pseudo-Random Generators (PRGs) [25].

4. Bloom Filter

The Bloom Filter (BF) is an intelligent data structure utilized across various domains to optimize memory consumption and improve search efficiency through membership filtering. Bloom Filter is now widely used and popular in a variety of applications such as security, big data, cloud computing, and Networking. This filter checks whether an item is probably already stored, which is helpful for quickly identifying potential duplicates during storage. There are five main categories for the BF: Standard BF, counting BF, fingerprint-based BF, hierarchical BF, and multidimensional BF [26][27].

This paper focuses on Standard Bloom Filter (SBF). SBF utilizes k hash functions to map an element to k positions. The efficiency of the filter depends on the value of k [26]. The SBF [28] is created using an array of m elements, each of which is a single bit, and k hash functions. The initial step involves setting all positions of the SBF to zero.

5. Methodology of the Proposed Technique

The basis of this approach is to hide the encrypted data in arbitrary locations in the cover image. This is to overcome the major drawback of the traditional LSB technique where the data is embedded in some sort of sequence which makes it vulnerable to steganalysis and less secure. For this purpose, the Lorenz Chaotic System has been used to produce a pseudo-random sequence. The output of this system is a three-axis vector. Two axes (X, Y)

TABLE I. ANALYSIS OF VARIOUS STEGANOGRAPHIC TECHNIQUES

Technique	Expediency	Impairments
Metaheuristic Algorithms (BCO) and (FGWO)	Maintain the quality of the cover image	Requiring a significant amount of processing power and time
Deep learning algorithms	Well resistant to statistical attacks	Many lost positions in the cover image
Chaotic systems	High embedding capacity	collision and secret data loss

were used to point at the pixel where the encrypted data will be stored and the third axis (Z) is the encrypted data. The LS exhibits chaotic behavior, implying that it is highly sensitive to its initial conditions. Notably, the system of equations is entirely deterministic, meaning that if the initial conditions were precisely the same, the outcome would be identical. Chaotic behavior arises from even the slightest differences in the starting state, resulting in a completely different final state. As such, the system is both unpredictable and deterministic. The initial state of (X, Y, and Z) serves as the key to restoring the secret image.

The LS comprises three nonlinear differential equations that depict the development of three variables: X, Y, and Z. These variables represent the state of the system at any given time. These states might repeat during the cycle. Since the (X, Y) values given from the chaotic system represent the position in which the encrypted data will be hidden, a Bloom filter is applied to make sure that the system doesn't use the same value twice. This is to prevent overwriting and hence losing data during the hiding phase. Figure (2) illustrates the phases of the proposed technique.

In the beginning, the proposed system uses the initial values (a, b, and c) along with the given (X, Y, and Z: namely the key) to generate the chaotic sequence. The below-modified equations (4, 5, and 6 respectively) demonstrate how the chaotic sequence (Dx, Dy, and Dz) is generated. The generated sequence splits into two parts: a location to store the encrypted data in the cover image (Dx, Dy), and a key (Dz) that goes to the Enc phase (as in figure 2). The values of Dx and Dy are modulus of n and m (that's rows and columns of the cover image) while Dz is a modulus of 256 (that's equivalent to one byte). During the encryption phase, the system takes the pixel from the secret image and divides it into its three channels (RGB), then performs a XOR operation with corresponding (Dz) from the current iteration. The result encrypted byte of data then goes into a Huffman coding phase to be reduced into 6 bits. After the Enc phase, a Bloom filter is applied to ensure the given location (Dx, Dy) has not been used in the previous iterations. The final phase is the LSB where the system embeds the given 6-bit encrypted data into the location (Dx, Dy) in the cover image. Each 2 bits go into a channel in the current pixel of the cover image. Figure (3) shows the steps of the process flow in the proposed method.

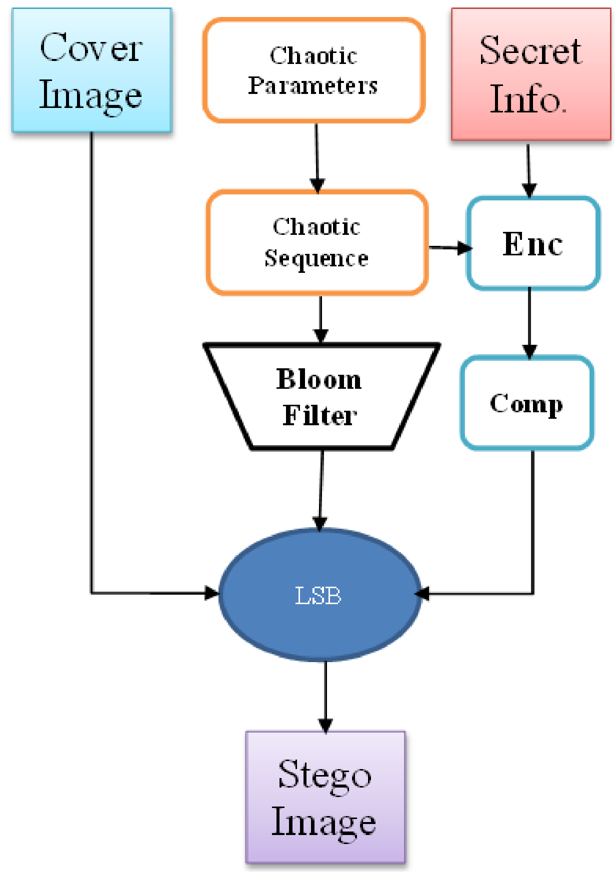

Figure 2. Proposed Steganographic Technique.

$$Dx_i = |a \cdot (Y_{i-1} - X_{i-1})| \cdot i \bmod n \quad (4)$$

$$Dy_i = |cX_{i-1} - X_i Z_{i-1} - Y_{i-1}| \cdot i \bmod m \quad (5)$$

$$Dz_i = (|X_i Y_i - b * Z_(i-1)| * i) mod 256 \quad (6)$$

Where n represents the rows' number and m represents the columns' number in the cover image, in addition to that i is a counter in terms of the number of pixels (n*m).

6. Results and Discussion

Chaotic systems play a vital role in steganography, which is the practice of hiding information within other data. Chaotic systems provide a way to generate a seem-

Input:
Secret Image
Cover Image
Lorenz Parameters
Output:
Stego Image
Begin:

Step1:	R, G and B = Decompose secret image to RGB
Step2:	Foreach (R, G and B = Ch) repeat steps (3 to 7)
Step3:	Generate Lorenz sequences (X, Y and Z) from Lorenz equations based on Lorenz parameters (2, 3, and 4).
Step4:	Encrypted Ch = Ch ⊕ Z
Step5:	Compressed Ch= apply Huffman to encrypted Ch
Step6:	If X, Y is used before (Bloom filter), Go to Step3
Step7:	Stego image= embed Encrypted Ch into (X, Y) location in Cover Image using LSB
Step8:	Return (Stego image)

End

Figure 3. Algorithm of the Proposed Technique.

ingly random pattern that can be used to encrypt and hide information within an image or other media file. The unpredictable nature of chaotic systems makes it difficult for unauthorized users to detect hidden information.

This section provides an overview of the main experimental outcomes that were achieved through the utilization of the suggested technique, which were subsequently compared to alternative methods employed for the same purpose. The proposed approach's effectiveness and efficiency were evaluated by measuring several similarity and randomness metrics, such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Normalized Protein Catabolic Rate (NPCR), Unified Average Change Intensity (UACI), entropy, and correlation. For experimentation purposes, the method was implemented and coded in the C# language, utilizing a computer equipped with a core i7 processor and 16 GB RAM. A Lina image measuring 512x512 was utilized as the cover photo, and other images measuring 128*128 were used as secret images that were concealed using the proposed method.

The values of the key used as parameters in the Lorenz system are X=0.51, Y=2.91, Z=1.32, a=10, b=2.6, and c=28.97. The hiding process in this work depends on the previous values, as the values of (a, b, and c) are fixed, as they are the optimal values to get chaotic, while the values of (X, Y, and Z) are the real key values, and any simple change to these values changes the series of hiding completely because the Lorenz chaotic system is very sensitive to the initial state and sensitive to any change in its values.

The proposed steganographic technique must pass the visual attack, which aims to reveal hidden data through visual inspection. It is clear by looking at Figure 4 that there is a great match between the cover and the stego images (tiff images), and this confirms that there is great difficulty in discovering that there is hidden information in the image through the naked eye. Moreover, the results in Table 2, especially the quality metrics (PCNR and MSE), which measure the image visual quality, show that the suggested technology is very good, as the PCNR percentage exceeded more than 40%, and this confirms that the suggested technique is well resistant to visual attacks. These indicators measure the percentage of the difference between the cover and stego image, where the lower the MSE percentage, means more similarity between the two images, while PSNR does the opposite.

UACI and NPCR were used to evaluate the performance of the proposed image steganography method which hides secret information within digital images. UACI takes contrast and brightness factors into account when comparing two images, and the higher value of the metric shows that the adjustment introduced less optical distortion, and this is evident in the results in the second table. Conversely, the high NPCR value indicates that the information steganography method presents significant visual differences between the original image and the modified image, and this is evident from the results that the proposed method gave a lower distortion rate compared to other methods.

The main weakness of LSB is the ease of discovering hidden data with images through statistical attacks, but the high similarity rate between the original image and the image after hiding confirms the difficulty of discovering secret information. Additionally, the process of concealment in a pseudo-random order using the chaotic Lorenz system makes security with the proposed technique on two levels, because it is impossible to view the confidential information even if its existence is discovered in the image.

Figure 4. The Cover and Stego Images.

Table 3 illustrates the results of the suggested technique in terms of entropy and correlation. It turns out that the entropy value of the stego image is very close to the original image, meaning that the pixel values that have been changed are few, and thus confirms that the suggested method is

TABLE II. THE RESULTS OF THE SIMILARITY METRICS

Methods	PSNR %	MSE %	NPCR %	UACI %
Our method	48.57	28.54	32.35	1.76
Traditional LSB	41.56	49.32	90.26	0.05
Method [29]	47.71	-	-	-
Method [30]	43.61	-	-	-

resistant to analytical and statistical attacks. In addition, the high correlation value between the image resulting from the proposed technique and the cover image supports the idea that the two images are very similar.

Figure 5 shows the histograms of the images in the previous figure before and after hiding. The figure shows the differences between the graphs are very small which confirms the success and effectiveness of the suggested algorithm in terms of visual and statistical attacks. Consequently, the results show a significant correlation between the cover and the image after hiding, in addition this confirms that the proposed technique is effective in facing analytical and visual attacks. Finally, the results provide competitive results compared to the traditional methods and the methods proposed by researchers in the same field, as they showed clear superiority during testing and experiment.

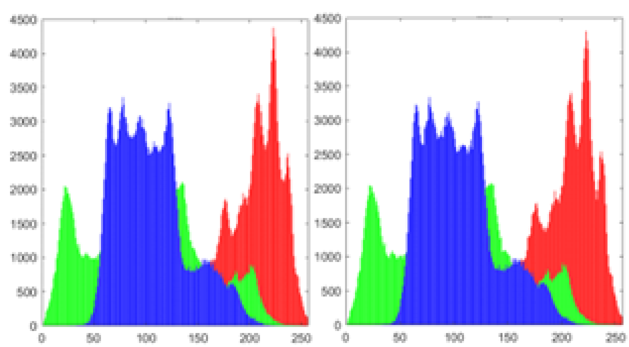

Figure 5. Histogram of the Cover and Stego Images.

Finally, in terms of capacity, the proposed technique provides the possibility to utilize every pixel in the cover image, thus achieving the maximum utilization of hiding locations. Table 4 illustrates the average embedding time rate of the proposed method compared to other techniques. The values indicate that the proposed method takes slightly more time than the classical LSB approach due to the utilization of a chaotic system for generating embedding locations instead of sequential embedding. However, overall, the embedding time using the proposed technique remains competitive compared to other methods.

7. Conclusions and Future Work

A digital image steganography technique has been proposed based on the chaotic LS and Bloom filter. The chaotic system was used to generate a series of semi-randomly arranged positions to hide secret information, while the BF was used to avoid hiding in the same location more than once and thus losing data. The entropy values showed that the hiding process did not cause a significant and clear change to the cover image. Furthermore, the outcomes of the similarity metrics showed that the suggested method is well resistant to analytical and visual attacks. Finally, it is clear from all the above and compared to other methods that the proposed technique is efficient and competitive.

References

[1] A. Salim, A. M. Sagheer, and L. Yaseen, "Design and implementation of a secure mobile banking system based on elliptic curve integrated encryption schema," in *International Conference on Applied Computing to Support Industry: Innovation and Technology*. Springer, 2019, pp. 424–438.

[2] A. Ahmad, A. Ullah, C. Feng, M. Khan, S. Ashraf, M. Adnan, S. Nazir, and H. U. Khan, "Towards an improved energy efficient and end-to-end secure protocol for iot healthcare applications," *Security and Communication Networks*, vol. 2020, pp. 1–10, 2020.

[3] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[4] B. Q. A. Ali, H. I. Shahadi, M. S. Kod, and H. R. Farhan, "Covert voip communication based on audio steganography," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 821–830, 2022.

[5] R. Anderson, "Information hiding: First international workshop cambridge, uk, may 30–june 1, 1996 proceedings," in *International Workshop on Information Hiding 1*. Springer, 1996.

[6] K.-H. Jung, "Steganography based on interpolation and edge detection techniques," in *Cryptographic and Information Security Approaches for Images and Videos*. CRC Press, 2018, pp. 597–626.

[7] S.-H. Liu, T.-H. Chen, H.-X. Yao, and W. Gao, "A variable depth lsb data hiding technique in images," in *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 04EX826)*, vol. 7. IEEE, 2004, pp. 3990–3994.

[8] S. A. S. Almola, N. H. Qasim, and H. A. A. Alasadi, "Robust method for embedding an image inside cover image based on least significant bit steganography," *Informatica*, vol. 46, no. 9, 2023.

[9] L. Kocarev and S. Lian, *Chaos-based cryptography: Theory, algorithms and applications*. Springer Science & Business Media, 2011, vol. 354.

[10] S. Banerjee and J. Kurths, "Chaos and cryptography: a new dimension in secure communications," pp. 1441–1445, 2014.

[11] I. A. Saleh and A. Al-Omary, "Apply bee colony optimization for

TABLE III. THE ENTROPY AND CORRELATION BETWEEN IMAGES

Methods	R	G	B	Correlation %
Original	7.23	7.63	6.98	-
Hidden by our method	7.26	7.62	6.95	0.99%
Hidden by traditional LSB	4.95	5.29	4.66	0.91%
Method [31]	6.23	5.46	4.68	-

TABLE IV. AVERAGE EMBBADING TIME

Methods	Average Time (second)
Classical LSB	0.81
Method [32]	18.22
Proposed method	13.52

image steganography with optical pixel adjustment," *International Journal of Computing and Digital Systems*, vol. 5, no. 05, 2016.

[12] M. Suresh and I. S. Sam, "Optimized interesting region identification for video steganography using fractional grey wolf optimization along with multi-objective cost function," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 6, pp. 3489–3496, 2022.

[13] P. Wu, Y. Yang, and X. Li, "Image-into-image steganography using deep convolutional network," in *Advances in Multimedia Information Processing–PCM 2018: 19th Pacific-Rim Conference on Multimedia, Hefei, China, September 21-22, 2018, Proceedings, Part II 19*. Springer, 2018, pp. 792–802.

[14] B. Ray, S. Mukhopadhyay, S. Hossain, S. K. Ghosal, and R. Sarkar, "Image steganography using deep learning based edge detection," *Multimedia Tools and Applications*, vol. 80, no. 24, pp. 33 475–33 503, 2021.

[15] S. S. Jamal, S. Farwa, A. H. Alkhaldi, M. Aslam, and M. A. Gondal, "A robust steganographic technique based on improved chaotic-range systems," *Chinese Journal of Physics*, vol. 61, pp. 301–309, 2019.

[16] M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1898–1907, 2014.

[17] D. Dey, S. Pattanayak, and S. Samanta, "Chaotic based image steganography using polygonal method," in *Nonlinear Dynamics and Applications: Proceedings of the ICNDA 2022*. Springer, 2022, pp. 575–586.

[18] H. E. Rostam, H. Motameni, and R. Enayatifar, "Privacy-preserving in the internet of things based on steganography and chaotic functions," *Optik*, vol. 258, p. 168864, 2022.

[19] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, pp. 2395–2405, 2019.

[20] T. Li, W. Yan, and Z. Chi, "A new image encryption algorithm based on optimized lorenz chaotic system," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 13, p. e5902, 2022.

[21] Z. Wu, P. Pan, C. Sun, and B. Zhao, "Plaintext-related dynamic key chaotic image encryption algorithm," *Entropy*, vol. 23, no. 9, p. 1159, 2021.

[22] I. Grigorenko and E. Grigorenko, "Chaotic dynamics of the fractional lorenz system," *Physical review letters*, vol. 91, no. 3, p. 034101, 2003.

[23] D. A. Q. Shakir, A. Salim, S. Q. Abd Al-Rahman, and A. M. Sagheer, "Image encryption using lorenz chaotic system," *Journal of Techniques*, vol. 5, no. 1, pp. 122–128, 2023.

[24] J. Ahmad, F. Masood, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel secure occupancy monitoring scheme based on multi-chaos mapping," *Symmetry*, vol. 12, no. 3, p. 350, 2020.

[25] B. Khadem, A. Madadi, and K. Bakhtiyari, "Time/memory/data trade-off attack on a chaotic pseudo-random generator: A case study of gmjk," *Journal of Computational and Theoretical Nanoscience*, vol. 15, no. 11-12, pp. 3174–3179, 2018.

[26] R. Patgiri, S. Nayak, and S. K. Borgohain, "rdbf: A r-dimensional bloom filter for massive scale membership query," *Journal of Network and Computer Applications*, vol. 136, pp. 100–113, 2019.

[27] V. Bansal and S. Garg, "A cancelable biometric identification scheme based on bloom filter and format-preserving encryption," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5810–5821, 2022.

[28] M. Al-Hisnawi and M. Ahmadi, "Deep packet inspection using quotient filter," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2217–2220, 2016.

[29] S. Krishnagopal, S. Pratap, and B. Prakash, "Image encryption and steganography using chaotic maps with a double key protection," in *Proceedings of Fourth International Conference on Soft Computing for Problem Solving: SocProS 2014, Volume 2*. Springer, 2015, pp. 67–78.

[30] S. A. Al-Taweel, M. H. Al-Hada, and A. M. Nasser, "Image in image steganography technique based on arnold transform and lsb algorithms," *International Journal of Computer Applications*, vol. 181, no. 10, pp. 32–39, 2018.

[31] R. Moieni, S. Ibrahim, and L. Roohi, "A high capacity image steganography method using lorenz chaotic map," *ACIT*, 2013.

[32] A. Delmi, S. Suryadi, and Y. Satria, "Digital image steganography by using edge adaptive based chaos cryptography," in *Journal of Physics: Conference Series*, vol. 1442, no. 1. IOP Publishing, 2020, p. 012041.

Ahmad Salim is a Lecturer in Middle Technical University. He received his B.Sc. in Computer Science (2011) and M.Sc. in Computer Science (2018) from the University of Anbar, Iraq. He is interested in the following fields; Biometric, Information Security, Data Mining, Image Processing and Artificial Intelligence. He has published many papers in different scientific journals.

Khitam Abdulbasit is an assistant lecturer at the University of Anbar, known for her expertise in the field of computer science. She received her BSC in computer science in 2009 and later pursued her MSC in computer science, which she received in 2014. Khitam's research interests include various fields such as biometrics, data warehouse and data mining, data security, and AI.

Farah Maath Jasem was born in Iraq-Anbar in 1986. She received her B.Sc. of Artificial Intelligence in Computer Science Department at the University of Technology (2008) Iraq, M.Sc. in Data Security from the University of Anbar (2019)- Iraq. she is interested and publish several papers in Cryptology, Information Security, Image Processing, and intelligent system.

Ali Makki Sagheer was born in Iraq-Basrah 1979. He got on B.Sc. of Information System in Computer Science Department at the University of Technology (2001)-Iraq, M.Sc. in Data Security from the University of Technology (2004)-Iraq and Ph.D. in Computer Science from the University of Technology (2007)-Iraq. He is interested in Cybersecurity, Cryptology, Information and Network Security, Number Theory, Coding Systems, Multimedia Compression, Image Processing, Artificial Intelligence and Machine Learning. He published more than 95 papers in different scientific journals and conferences. Finally, he had obtained the Professor scientific degree in Cybersecurity since 18 Jul 2015.