International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2021.34072

Volume 7, Issue 8
August - 2021

Subject Review: Information Hiding Using Chaotic Map

Zahraa Salah Dhaief[1], Raniah Ali Mustafa[2], & Amal Abdulbaqi Maryoosh[3]

[1-3]Department of Computer Science,

College of Education, Mustansiriyah University

Baghdad,

Iraq

ABSTRACT

It is vital to convert information into an unidentifiable form in order to protect your confidential information from intruders. As a result, intruders will be unable to obtain your original information. As a result, security is the most difficult component for all users who wish to share their confidential information. In recent years, because of the quick rise of the internet and quick communication technology, the security and confidentiality of sensitive information has become a top priority and worry.

Information concealment is the technique of communicating secret information in a suitable carrier, such as a picture, video, or voice. Various technologies for information concealment, such as encryption, steganography, hashing, and authentication, have been developed and are in use today to safeguard information from unauthorized access.

Steganography's principal purpose is to conceal the existence of secure information, making it difficult for an unauthorized person to discover it. Steganography is the art of concealing information sensitive information in any medium in order to send it through a communication network in a secure manner.

The main goal of this paper is to examine and describe strategies for hiding information within multimedia using chaotic maps, as well as to compare various methods.

Key Words: Information hiding, Steganography, Cryptography, Chaotic Map, Least significant bit (LSB).

1. INTRODUCTION

In today's world, most people utilize the internet on their computers, mobile phones, laptops, tablets, and other devices in their daily lives, for example, to conduct their job from anywhere and email it to a recipient. Occasionally, a person will use a communication network to communicate confidential information to another user. Because there are so many invaders willing to seize secret information in this information era, protecting our secret information is our first priority.

Cryptography, steganography, hashing, and other approaches for securing information are available. In cryptography, users can change their original data into an unreadable format, making it impossible for attackers to find it. Hash Functions employ a mathematical process to "encrypt" data in an irreversible way. Steganography is a science and an art of encrypting messages so that only the person who send and intended receiver are aware on their presence, the sort of security by obscurity [1].

In photographs, information can be buried in a variety of ways. Straight message insertion is possible, which simply encodes all of the data in the image. To incorporate the message solely in "noisy" parts of the image that won't get as much attention, more complicated encoding might be used. The message might also be strewn about the cover image at random. The following are the most common approaches for discovering information hidden in photographs [2]:

- Least significant bit (LSB) insertion
- Masking and filtering techniques
- Transformations

Any approach for concealing information must have specific properties:

1. Capacity: The maximum quantity of data that can be concealed behind a cover material. The quantity of information that can be hidden is limited by the fact that the hidden information should not totally alter the original message in order to prevent drawing inadvertent attention to it.

2. Security: Data should be secure, with only the intended user having access to it, thanks to the information concealing method. In other words, it refers to the inability of an unauthorized user to find hidden information. To safeguard the confidentiality and sensitivity of information being conveyed, this is critical.

3. Robustness: This relates to the maximum amount of data that can be concealed without causing harm or deleting the data that has been hidden.

4. Perceptibility: Data should be hidden in such a way that the disguised cover signal and the original cover data signal are indistinguishable to the naked eye [3].

Many various study domains, such as engineering, science, physics, mathematics, and biology, have contributed to the development of chaos theory since the 1970s. Chaos is a dynamical system whose initial circumstances are extremely important. A minor difference in the initial parameters will result in a significant difference in the final result. It's a semi-random nonlinear system with deterministic behaviour. In steganography, chaos can be put used to ensure a high level of protection because of its chaotic behaviour. The physical layer's security can benefit from chaos [4].

2. LITERATURE SURVEY

Various ways of information concealment have been developed in recent years, with many different types of covers and encryption algorithms being employed with them. The sensitivity of chaotic maps to initial conditions and control parameters is well recognized. Because of these characteristics, they can be used as building blocks for a variety of cryptography and steganographic approaches. Some of these researches are discussed in this section.

Jianhua Song and Qun Ding [5] to improve information security, a new concealing information mechanism according to the Tent chaotic map and LSB has been presented. Tent Chaos encryption is applied to the secret message first, and then there's LSB steganography is applied to the cover-encrypted image's message. When compared to the usual way of obscuring visual information, the outcomes of the simulation reveal the fact that methodology significantly enhanced imperceptibility and security, and obtained good results.

Mazhar Tayel et al. [6] the goal of this research is to present a new form of chaos steganography technique to conceal multimedia data, such as images, text, or sound. The suggested approach uses a chaos distribution structure to coordinate data in picture dimensions. Because the data is encoded in the pixels' least significant bits, it cannot be seen inside the image. The embedded data is segregated and reassembled using the chaos coordination's beginning state when the image is received. The algorithm is applied to three categories of information, the first of which is image information, the second of which is text data, and the third of which is information about a sound signal, using a Mat lab application. When steganalysis is done on the composed original image, the results demonstrate that the tested data is well hidden in the original images with a high level of security.

Melad j. Saeed [7] this study describes a new color picture steganography method according to steganography in chaos and encrypted text in the DCT domain, in which DCT is utilized to transfer from the spatial domain to the frequency domain of the original image (cover image). The chaotic function was employed in two steps in this technique: first, for encryption of the secret message, and then, in order to embed in the DCT cover image. This innovative technicality gets good outcomes by forthright crucial steganography characteristic like as imperceptibility;

DOI: 10.31695/IJASRE.2021.34072

it is further enhanced by having a mean square error of less than one (MSE), By using variable length codes to secure the secret message characters and inserting the hidden message in one level of encryption, the peak signal to noise ratio (PSNR) and normalized correlation (NC) were enhanced using variable length codes to secure the secret message characters and putting a hidden message at a single the level of encryption image in color merely increased the security.

Ratnakirti Roy et al. [8] propose an image steganography with adaptive edges approach that combines both features to embed data using matrix encoding and LSBM while using a chaotic mapping scheme in order to provide improved the payload's security. Any image steganography system must have high imperceptibility and fidelity, and efforts have been made to make certain that suggested technicality fits these requirements.

In this research, D. Battikh et al. [9] suggest a chaos-based upgrade of the AE-LSB and the EA-LSBMR, two spatial steganographic algorithms, with the goal of analyzing their performance. The first is a pixel value difference-based adaptive LSB (Least Significant Bit) steganographic approach, which has a great capacity for embedding and produces invisible stego pictures. The second approach is to uses a strategy that adapts to the edge to choose an embedding zone based on the size of the hidden message and the distinction between two uninteresting pixels on the front cover. Both methods have a lower level of protection contra assaults attempting to reclaim confidential information. To address this flaw, they propose that these approaches' message security be improved. The improvement entails using an efficient chaotic system to select where the pixels in the cover image are secret message's bits will be hidden placed in a faux chaotic fashion. In this method, against message recovery the inserted message becomes secure. attempts and is uniformly distributed across the entire image. Experiments indicate that the algorithms' security improves.

Sujarani Rajendran and Manivannan Doraipandian [10] offer a new symmetric key based picture concealing technique in this study. Using a one-dimensional logistic map, pseudo random keys are created, and these keys are in use to choose the pixel position of the image on the cover at random to keep the hidden secret image. The selection of pixel position in the cover image is the most important security feature of the projected approach. The suggested technique Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) measurements are used to compare the results, and the outcomes reveal that the suggested scheme provides an effective level of security.

This work by Hassan Elkamchouchi et al. [11] looks into numerous different schemes for disguising in the form of a colourful cover image, a grayscale image the spatial domain. First, we investigate whether two-dimensional (Baker's map) or one-dimensional (Tent map) chaotic maps should be used to determine the pixels containing the secret message bits should be inserted. Because the human eye isn't particularly sensibility to small changes in this color spectrum, the embedding procedure affects the cover's red color channel picture for the previously pixels chosen. Following that, two LSB embedding techniques are investigated: a pixel with one bit and a pixel with two bits. Because the peak signal-to-noise ratio (PSNR) is high, while the mean squared error (MSE) is low for the several options tested, the preliminary findings suggest that eavesdroppers will have little reason to suspect the presence of a hidden message within the conveyed image. When using two-dimensional maps and/or the LSB technique with one bit per pixel, however, the time required for the embedding process is clearly impacted.

By combining two 2-D chaotic maps, new LSBs spatial domain approach was suggested Aya H. S. Abdelgader et al. [12]. The proposed method encrypts the secret message with a mixed chaotic map and hides the data with LSB.

In this paper, Ola N. Kadhim and Zahir M. Hussain [13] present two strategies for image steganography in the spatial domain. In steganography, several methods use chaos theory to monitor the addresses of scrambled bits. The very first is method uses the well-known LSB technique, while the second uses a new approach that looks for parts of the secret message and the cover image are identical. To extract the jumbled addresses bits, in the chaotic map, a modified logistic map is utilized to construct integer chaotic series. For the purpose of testing and evaluating the proposed approaches' new levels of security, the PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Square Error), and histogram analysis, and correlation analysis are employed. The proposed methods outperform existing systems, according to the findings.

DOI: 10.31695/IJASRE.2021.34072

Yasser Mohammad Al-Sharo [14] the primary goal of this research is to improve data security on the internet transfers by combining two approaches: picture steganography to disguise data transport in image media, as well as a chaotic map is used to reroute the transfer data's format from the start. The combination of both of these approaches is useful in securing data in a variety of formats, including text, audio, and image. JAVA programming was used to prototype the proposed method, and the produced programming was used to test a total of 20 images and text messages of useable sizes on the data set (plain data). The simulation was carried out on a local server to evaluate Performance in terms of security is based on two criteria: simple data transfer distance and data size. On the simulation test, many attacks are attempted utilizing well-known attacking strategies such as analyzing the quality of stego pictures. The findings of the experiment demonstrate that roughly 85% of the attacking efforts miss the stego pictures. 95% of attempts fail to remap significant portions of the chaotic data. The findings suggest that the planned security measures are effective solutions for securing online data transfers are of very high quality. The study's contribution is the successful combination of steganography and chaotic map techniques to ensure a great degree of security in data transfer over the internet.

Zahraa Salah Dhaief et al. [15] present a status of dual stenographic approach in this study. Dual Steganography is a security method that combines steganography and cryptography. This technique has the benefit of offering excellent security while requiring little time. This study presents a dual steganography technique that provides an extra layer of protection. In two phases, the proposed algorithm embeds secret text messages in the cover image. A chaotic map cipher approach for encrypting text and an LSB (Least Significant Bit) image steganography technique for hiding encrypted text in an image are included in the two phases. An RGB image hides the text holding encrypted data.

In this research, Aya Jaradat et al. [16] offer a steganography algorithm based on Chaos theory and particle swarm optimization, with the goal of locating the optimal pixel placements in the cover image to hide the secret data while keeping the stego-quality image's. The host and secret pictures are separated into sections to increase embedding capacity, with each block storing a sufficient quantity of secret bits. The suggested system surpasses current methods in terms of PSNR and SSIM picture quality measures, according to experimental results.

In this paper, A. A. Karawia [17] proposes a medical picture steganographic technique based on least significant bit modification and chaotic map. The fundamental issue is that most present approaches do not adequately safeguard the choice of pixels for embedding within the host image. To choose the positions of these pixels at random, the author employed a piecewise smooth chaotic map in two dimensions. On the contrary, no bits in the confidential medical image are lost during transmission. To do so, a one- dimensional piecewise chaotic map is employed in order to encrypt the confidential medical image (Tent map). The steganographic algorithm is then employed to conceal the bits of the encrypted secret medical image. Before the embedding procedure, the each embedded pixel's bits are randomly jumbled. The stego image is then generated. The peak signal-to-noise ratio, mean square error, histogram test, picture quality measure, and relative entropy test are used to analyze the host and stego images. When compared to the host image, the stego image produces satisfactory results. The chi-square assault test is also carried out, and the stego picture is found to be resistant. The proposed technique can help with medical image transmission across communication media.

3. COMPARATIVE ANALYSIS OF THE SCHEMES

In this section, we will compare past information hiding approaches based on the chaotic map that was utilized to hide information, as well as the PSNR and MSE values. The comparisons between earlier systems are shown in Table 1.

DOI: 10.31695/IJASRE.2021.34072

Table1.1. An examination of the schemes in comparison

Ref.	Information hiding technique	Hidden data	Cover type	PSNR			MSE		
[5]	LSB and Tent chaotic map	Text	image	55.789			NA		
[6]	The least significant bit and chaos theory	image, text, sound	Gray image	image	text	sound	image	text	sound
				57.6872	58.7404	58.3189	7.3150	5.7401	6.3252
[7]	For color images, chaotic steganography and encrypting text in the DCT domain	Text	color image	63.1627			0.0315		
[8]	An edge adaptive image steganography system that uses a chaotic mapping approach and combines the benefits of matrix encoding and LSBM to embed data.	Image	Image	71.94			NA		
[9]	The AE-LSB and the EA-LSBMR are two spatial steganographic algorithms that have been enhanced by chaos.	Image	Image	60.03			NA		
[10]	A new image concealing approach based on symmetric keys.	Image	Image	35.70			18.36		
[11]	With the spatial domain, hiding a grayscale image in a colourful cover image	Gray scale image	Colored image	44.678			NA		
[12]	A new LSBs spatial domain technique based on combining two 2-D chaotic maps has been developed.	Image	Image	53.8			NA		
[13]	In the spatial domain, image steganography.	Text, image	Gray-scale Image	Text	Image		Text	Image	
				56.1089	54.3719		0.1593	0.2376	
[14]	Images steganography is used to hide transfer data in image media, and a chaotic map is used to remap the transfer data's original format.	Text	Gray Image, color image	Gray Image	color image		NA		
				< 30	> 40				

4. CONCLUSIONS

In this research, we examine information hiding approaches based on the utilization of a chaotic map with various methodologies across time (2011-2021). Due to advancements in the world of information technology, steganography has become a pressing issue at this moment. Many criteria, such as the quantity of the data to be contained, security needs, and the environment in which the data is conveyed, can be used to figure out what the optimum data-hiding approach is. Data steganography and encryption methods can be combined for increased security. According to the findings of this study, all of these ways are beneficial to the data steganography process. Each scheme is unique in its approach, which makes it suitable for a variety of implementations. Most recently proposed data concealing methods have increased the level of security by providing many security approaches, such as data hiding and encryption. Each technology has its own set of benefits and drawbacks, which is why new technologies were introduced.

ACKNOWLEDGMENT

The authors wish to express his gratitude to Mustansiriyah University (www.uomustansiriyah.edu.iq) in Baghdad, Iraq, for its assistance with this project.

DOI: 10.31695/IJASRE.2021.34072

REFERENCES

[1] Komal Pate, Sumit Utareja, Hitesh Gupta, "A Survey of Information Hiding Techniques", International Journal of Emerging Technology and Advanced Engineering, January 2013, Volume 3, Issue 1.

[2] Sabu M Thampi, "Information Hiding Techniques: A Tutorial Review".

[3] Richa Gupta1, Sunny Gupta2, Anuradha Singha, " Importance and Techniques of Information Hiding: A Review", International Journal of Computer Trends and Technology (IJCTT), Mar 2014, volume 9 number 5.

[4] Peipei Liu, Zhongliang Zhu, Hongxia Wang Tianyun Yan, "A Novel Image Steganography Using Chaotic Map and Visual Model".

[5] Jianhua Song, Qun Ding, "An information hiding method based on LSB and tent chaotic map," Proc. SPIE 8009, Third International Conference on Digital Image Processing (ICDIP 2011), 800920 (8 July 2011).

[6] Mazhar Tayel, Hamed Shawky, Alaa El-Din Sayed Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data", ICACT2012, Feb. 19-22, 2012.

[7] MELAD J. SAEED, "A NEW TECHNIQUE BASED ON CHAOTIC STEGANOGRAPHY AND ENCRYPTION TEXT IN DCT DOMAIN FOR COLOR IMAGE", Journal of Engineering Science and Technology, 2013, Vol. 8, No. 5, pages 508 – 520.

[8] Ratnakirti Roy, Anirban Sarkar, Suvamoy Changder, "Chaos based Edge Adaptive Image Steganography", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.

[9] D. Battikh, S. El Assad, B. Bakhache, O. Deforges, M. Khalil, "Chaos-based Spatial Steganography System for Images" , International Journal of Chaotic Computing (IJCC), Volume 3, Issue 1, June 2014/2015.

[10] Sujarani Rajendran, Manivannan Doraipandian, "Chaotic Map Based Random Image Steganography Using LSB Technique", International Journal of Network Security, July 2017, Vol.19, No.4, PP.593-598.

[11] Hassan Elkamchouchi , Wessam M. Salama , Yasmine Abouelseoud, "Data Hiding in a Digital Cover Image Using Chaotic Maps and LSB Technique", Proceedings of ICCES 2017 12th International Conference on Computer Engineering and Systems.

[12] Aya H. S. Abdelgader , Raneem A. Aboughalia , Osama A. S. Alkishriwo, " Combined Image Encryption and Steganography Algorithm in the Spatial Domain", First Conference for Engineering Sciences and Technology (CEST-2018) 25-27 September 2018 / Libya.

[13] Ola N. Kadhim and Zahir M. Hussain, "Information Hiding using Chaotic-Address Steganography", Journal of Computer Science 2018, 14 (9): pages 1247-1266.

[14] Yasser Mohammad Al-Sharo, "Images Steganography Approach Supporting Chaotic Map Technique for the Security of Online Transfer", International Journal of Advanced Computer Science and Applications (IJACSA), 2019, Vol. 10, No. 4.

[15] Zahraa Salah Dhaief, Raniah Ali Mustafa and Amal Abdulbaqi Maryoosh, " Hiding Encrypted Text in Image using Least Significant Bit image Steganography Technique", International Journal of Engineering Research and Advanced Technology (IJERAT), 8 August -2020, Volume.6, Issue.

[16] Aya Jaradat, Eyad Taqieddin, and Moad Mowafi, "A High-Capacity Image Steganography Method Using Chaotic Particle Swarm Optimization" , Hindawi Security and Communication Networks, Volume 2021, Article ID 6679284, 11 pages.

[17] A. A. Karawia, "Medical image steganographic algorithm via modified LSB method and chaotic map", The Institution of Engineering and Technology, Article in IET Image Processing · May 2021.

C author: zehraa_84@uomustansiriyah.edu.iq

DOI: 10.31695/IJASRE.2021.34072