

Design secure multi-level communication system based on duffing chaotic map and steganography

Aliaa Sadoon Abd, Ehab AbdulRazzaq Hussein

Department of Electrical Engineering, Faculty of Engineering, University of Babylon, Babylon, Iraq

Article Info

Article history:

Received May 16, 2021

Revised Nov 22, 2021

Accepted Nov 27, 2021

Keywords:

Chaotic maps

Encryption

Multilevel security

Steganography

ABSTRACT

Cryptography and steganography are among the most important sciences that have been properly used to keep confidential data from potential spies and hackers. They can be used separately or together. Encryption involves the basic principle of instantaneous conversion of valuable information into a specific form that unauthorized persons will not understand to decrypt it. While steganography is the science of embedding confidential data inside a cover, in a way that cannot be recognized or seen by the human eye. This paper presents a high-resolution chaotic approach applied to images that hide information. A more secure and reliable system is designed to properly include confidential data transmitted through transmission channels. This is done by working the use of encryption and steganography together. This work proposed a new method that achieves a very high level of hidden information based on non-uniform systems by generating a random index vector (RIV) for hidden data within least significant bit (LSB) image pixels. This method prevents the reduction of image quality. The simulation results also show that the peak signal to noise ratio (PSNR) is up to 74.87 dB and the mean square error (MSE) values is up to 0.0828, which sufficiently indicates the effectiveness of the proposed algorithm.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ehab AbdulRazzaq Hussein

Department of Electrical Engineering, Faculty of Engineering, University of Babylon

Babylon, Iraq

Email: dr.ehab@uobabylon.edu.iq

1. INTRODUCTION

Many people when they are sending secret data through various types of communication channels, the first possible thing that comes to their minds is "hacking" and "spies" and how they can protect their confidential information from these spies. To overcome this problem, steganography was used, which is one of the most important sciences that people use, to properly protect their data. This is achieved by hiding secret data or embedding it inside the cover (carrier). By following a method that cannot be done by people who do not have the right to do so. In other words, just (only the person who sends the data and the recipient is the only one who can disclose and know confidential data) [1], [2]. There is a lot of research into both techniques of steganography, and some of this research are briefly described. The research that presented methods of hiding the information in the image is as follows. Chaos science has become popular recently used in both steganography and cryptography. The previous research had least significant bit (LSB).

uggested a chaotic way to hide text in images. The method demonstrated how it was possible to hide a secret message in an image using the least significant bit entry method with chaos. Alam *et al.* [3] suggested a method for masking images through the use of edges and logistical maps as a random generator of secret keys for random least significant bit (LSB) replacement. Sabery and Yagobi [4] suggested using a simple

logistic map to hide classified photos in host photos. Embedding was performed in the logistic map to identify blocks of pixels.

Senthil *et al.* [5]. Suggested a way to display clutter-based adaptive image masking, which contained matrix coding and least significant bit matching (LSBM) merging efficiencies for data embedding. Anees *et al.* [6], design a method of hiding information in the spatial domain using chaotic maps to Resolve pixel positions. Neeta *et al.* [7] suggested using Henon random maps for masking images and to enhance traditional LSB technology. Liu and Xia [8], the authors propose a new chaotic map, called two-dimensional triangle function combination discrete chaotic map (2D-TFCDM), using discrete fractional calculus. Also, the Khao behaviors are discussed numerically. Next, diagrams of bifurcation and stage pictures are shown. Finally, the detached partial map is converted into an algorithm by producing the keys through the elliptic curve in a specified field. In this paper, both researchers Patro and Pointia suggested the use of 1D chaotic map in conjunction with a bit-level algorithm for image encryption [9]. The algorithm is two-stage, firstly the 1D linear chaotic maps used are used in a bit level propagation process and then they use the beta map for bit-level scrambling, rows, and columns. In this paper [10], Mandal and Das proposed a method for encoding and decoding color image using microcontroller. Two microcontrollers can be used for the driver and driven system that helps in transmitting and receiving data.

2. IMAGE STEGANOGRAPHY

The image steganography is the most used method for concealment bit inside the LSB cover image. In this method, it is necessary to use a lossless compression method because this method uses bits per pixel. If the lossless compression method is not used, the information hidden in the image may be lost during the compression process [11], [12]. If a 24-bit color image is used, then you can use for each of the colors (red, blue, yellow) and therefore save 3 bits per pixel. Therefore, more data can be hidden. In general, for image steganography, any of the formats, portable network graphics, (PNG) and joint photographic experts' group (JPEG). Can be used to hide the secret message [13]. One of the most important methods used in concealment is the LSB. The idea of this technique is interesting. The smallest bits in each image can be considered random noise, so changing them does not change the appearance of the image. This idea can be considered as the basis of this method, in short, the message bits are replaced before embedding, resulting in the bits being distributed evenly. Some algorithms change the visited LSB pixels in a random walk. Others change the pixels in certain areas of the image, increasing or decreasing the pixel value instead of changing the last bit [14]. Another fundamental category of steganography technique is defiantly the most developed transform domain technique in which a used number of efficient algorithms have been merely proposed transform domain methods hide messages in significant areas of the cover image which merely makes them more robust to possible attacks [15]. The use of redundancy in the field of discrete cosine transforms (DCT), which is used in JPEG compression, is most of the work of this group. Of course, there are other algorithms that use other conversion domains, such as the frequency domain. Embedding in the DCT domain [16] is done simply by changing the DCT coefficients, for example by changing the minimum bit value of each coefficient. One of the limitations of embedding in the DCT domain is that many coefficients are 64 to zero, and a change in many values from zero to non-zero will affect the compression rate [17]. Hence, using DCT there are fewer bits than LSB for hiding and embedding. The embedding capacity also depends on the type of image used for DCT embedding. This is because the number of non-zero DCT coefficients may vary depending on the image texture.

3. CHAOTIC MAPS

Chaos accurately represents a long-term periodic behavior in a deterministic system that typically permits significant sensitivity to any slight change in initial values or necessary parameters. Chaos is gratefully considered one of the potential behaviors positively associated with the continuous growth of a nonlinear physical system. It ordinarily occurs for certain considerable values of system parameters [18]. There are two types of chaotic systems, the 1st type is chaotic flows are known as continues systems, and can be represented with differential equations, there are many types of chaotic flow such as Lorenz, Rossler and Chan systems [19]. While the 2nd types of chaos are chaotic maps are referring to that with difference equations. Also, chaotic maps have many types such as logistic, Henon, Doffing and Duffing maps [20], [21]. In this paper are used Duffing map also known as "Holmes map" is apart from chaotic maps and discrete time dynamical systems. It is an example of a dynamic system that typically exhibits chaotic behavior [22], [23]. The used Duffing map naturally considers a minor point (X_n, Y_n) in the user plane and maps it to a new point given by (1).

$$\begin{aligned} X_{n+1} &= Y_n \\ y_{n+1} &= -bX_n + aY_n + Y_n^3. \end{aligned} \quad (1)$$

There are two specific parameters a and b , $a = 2.75$ and $b = 0.2$ to typically produce chaotic behavior. The trajectory and orbit are two practical terms used to properly designate the successful development of these non-static systems. The trajectory naturally regards the track efficiently performed by the flow-through time and the number of points which a map moved over the iteration. The time-domain will be represented by a strange attractor in the phase space. While the strange attractor accurately represents the prime-time series of the chaotic system, Figure 1(a) sufficiently illustrates the prime-time series of the chaotic system and the changing aspects (dynamics) of the strange attractor, as shown in Figure 1(b).

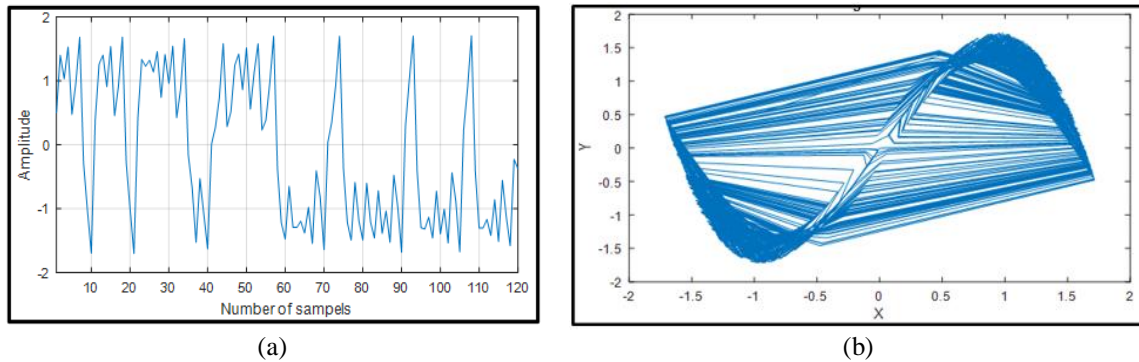


Figure 1. Duffing map algorithm, (a) Time series for chaotic duffing map and (b) strange attractor for duffing map

The sensitivity of Duffing map from any varies small change in any parameters of initial values make the new trajectory after some generated samples as shown in Figure 2, where values of blue line are $X(1) = -1$, $Y(1) = 0.5$, $a = 2.75$ & $b = 0.15$ and the same values but slight change in the red line. Figure 2 illustrates that make a new trajectory because this sensitivity. All the initial values and parameters will be used as a key from to an encryption system.

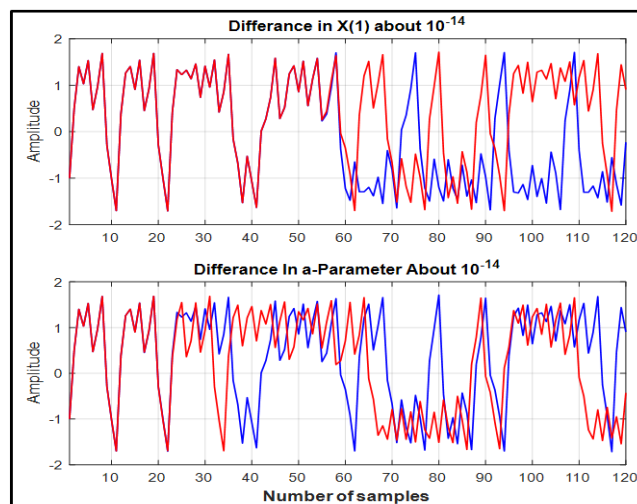


Figure 2. Duffing map sensitivity from initial conditions and parameters

4. METHODOLOGY OF PROPOSED ALGORITHM

The process of hiding data is not enough to immunity of data against from attack because just to know that the eavesdropper image sent information can be retrieved in a simple manner. In order to obtain a very high level of hidden information, we propose a new method based on chaotic systems by generating random index vector (RIV) for the hidden data inside the LSB of the image pixels. In order to generate RIV, the three conditions must be met:

1. The length of RIV generated should be equal to the length of data to be hidden.
 2. The values of RIV must be true values and the range of RIV began from 1 to multiply the dimensions of image (r*c*d).
 3. Not to duplicate any index from RIV.
- After the generated the RIV with these specifications, they are used to hide the data inside the LSB of image pixels.

Proposed chaotic steganography algorithm. The following algorithm is used to produce RIV based on chaotic Duffing map.

1. Load the cover picture and the secret message.
2. Converting the cover picture with dimensions (r*c*d) to one vector.
Where: r: No. of rows, c: No. of column, d: Dimensions of pixel.
3. Converting the secret message to binary data.
4. Generating chaotic random numbers (CRN) and multiplied by a large number like (10¹²).

$$CRN = round(X * 10^{12}) \tag{2}$$

5. Obtained the random index to embed binary data by using the equation:
6. $New\ Index = mod[CRN, (r * c * d)]$.
7. Repeating the process from step 4 and check if the new index is used before, and must be changed otherwise. It completes the repeating process entail reach to the total length of binary message.
8. Embedding each bit form binary message in the LSB of the cover picture, vector based on a random chaotic index.
9. Finally reconstructed the Stego-image with the original dimension. Reconstructed the Stego-image with the original dimension.

5. MEASURING OF IMAGE QUALITY

The primary goal of using Steganography is Hiding confidential data inside the cover file (audio, photo, and video). in a way that is not possible. It can be identified with the naked human eyes or exposed and manipulated by spies. As a result, the distortion that occurs in the cover file begins with a slight distortion and then to severe. Measuring and evaluating parameters require criteria. Several parameters and criteria is used to measure the acceptability of this distortion and its effect. These parameters and criteria are used for evaluating the system. The parameters used in this work are listed:

- Mean squared error (MSE)
- Peak signal to noise ratio (PSNR)
- Structural similarity index (SSIM)

These tests are applied to the image file, where a comparison is made between the original image and the image after hiding, and this is done using MATLAB, it implements and analyzes this design.

5.1. Mean squared error (MSE)

The mean squared errors (MSE) between two images are $Pic1$ (m,n) and $Pic2$ (m,n) is can be calculated from (3) [24], [25].

$$MSE = \frac{1}{m*n} \sum_{i=1}^{m*n} \sum_{j=1}^n (Pic1(i,j)_i - Pic2(i,j)_i)^2 \tag{3}$$

In the (3) $Pic1_i$ is original image, $Pic1_j$ Is Stego-image, m and n are the number of rows and columns in an input image, respectively (Dimension of image matrix).

5.2. Peak signal to noise ratio (PSNR)

It is an expression of the ratio between the signal and the power of the noise, is measured in decibels (dB) and it is a good measure for comparing restoration results for the same image. PSNR will help to avoid this problem by scaling the MSE according to the given image. As shown in (4) [25], [26].

$$PSNR(dB) = 10 \log_{10} \left[\frac{255^2}{MSE} \right]. \tag{4}$$

5.3. Structural similarity index (SSIM)

It is employed for measuring the similarity between two images as in the method for predicting the perceived quality of the image. The equation of the Structural Similarity Index can be viewed in (5) [23]. Where

μ_x, μ_y represent the local means, σ_x, σ_y represent the standard deviations while σ_{xy} represent the cross-covariance.

$$SSIM(\%) = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \times 100\% \tag{5}$$

6. SIMULATION RESULTS AND DISCUSSION

The primary goal of using Steganography is Hiding confidential data inside the cover file (audio, photo, and video). In a way that is not possible. It can be identified with the naked human eyes or exposed and manipulated by spies. As a result, the distortion that occurs in the cover file begins with a slight distortion and then to severe. A simulation model based on block diagram given in Figure 1, has been designed using MATLAB. The parameters used in the simulation were as follows ($X(1) = -1, Y(1) = 0.5, a = 2.75$ & $b = 0.15$).

6.1. Result of steganography

In this research, the principle of steganography was applied to an image that represents an information cover as shown in Figure 3 it size (41.3 KB), (512 * 341 pixels). Another image was used to represent the message as shown in Figure 3, it's size about (8) times less than the size of the cover. The simulation results are presented as follows: The amount of effect of the cover with hidden information, image effect (message) after retrieving it, secure in Chaotic map and Cryptanalysis.

In this method, show that the embedding technology adopted in this research has very little effect on the quality of the original image, after including the data in it, so that the difference in quality between the original image and Stego-image cannot be noticed, so that it can be neglected in which the Least Significant Bits of the cover is used to hidden the bit of information inside it. After the data are properly included in the cover image. Figure 4 shows the great similarity between the cover image and the Stego-image, which means that the embedded information is not easily seen or sensed by the hacker.

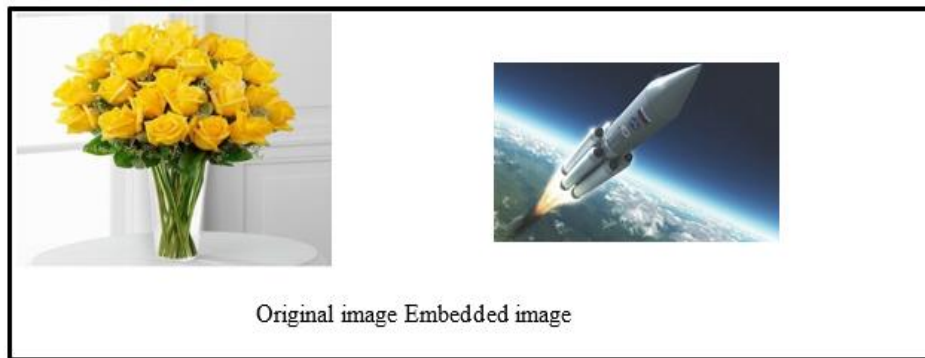


Figure 3. Original image and embedded image

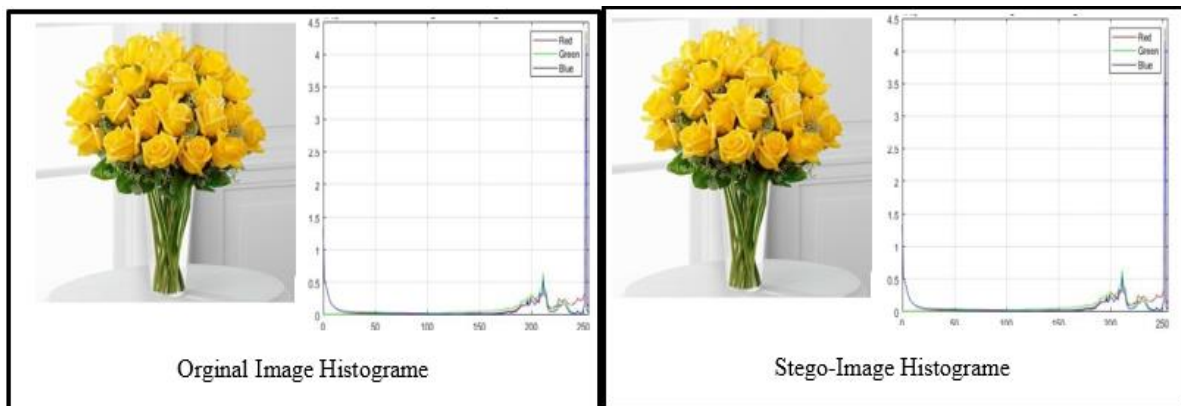


Figure 4. The similarity between the origin image and Stego-image

Figure 4 shows the original image and the Stego-image, also the histogram. The original image is not affected after the carrying, the information ensures that there is no distortion in image quality. Obtaining the cover without distortion is one of the most important reasons for evaluating the performance of the proposed program. And Table 1 shows parameters measuring image quality between the Stego-image and the cover image.

In the proposed method, notice that the information sent reaches the person concerned without any loss in it. Figure 5 shows the information before sending and after receiving and the similarities between them. Also the histogram does not change after receiving the information. This proves the effectiveness of the proposed system in preserving information from being lost or distorted.

Table 1. Parameters measuring of image quality

Parameters measuring of image quality	SSIM%	MSE	PSNR (dB)
Value	99.997%	0.083	74.87

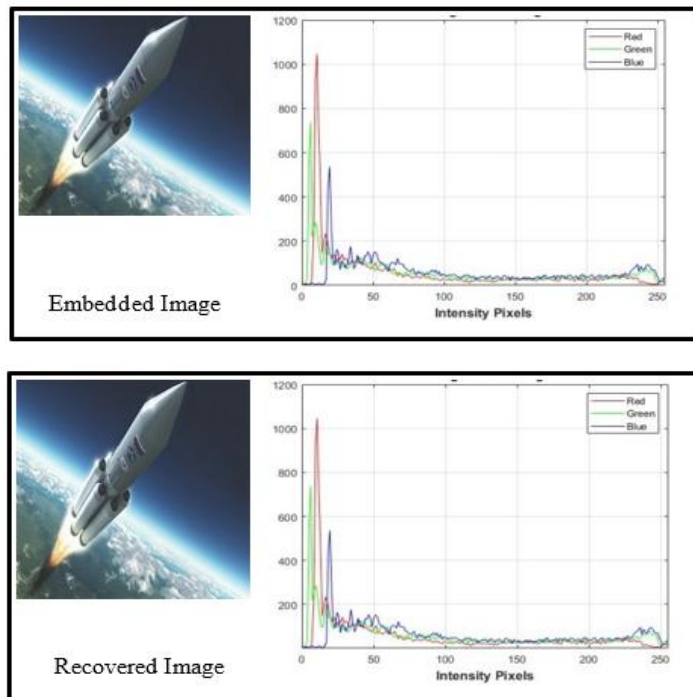


Figure 5. Shows the information before sending and after receiving

After measuring the efficiency of the proposed method in pictures. Table 2 shows the system efficiency through the values of (PSN, MSE, structural similarity index (SSIM)) between the data before sending and after receiving. Table 2 shows the measurements made between the message before hidden and after it was received, the extent to which the information sent was preserved and reached the intended person without any loss or change.

Table 2. Parameters measuring message quality

Parameters measuring of image quality	SSIM%	MSE	PSNR (dB)
Value	100%	0	Infinity

6.2. Result for security based on chaotic

Another security level was also used, represented by using Duffing map and controlling it through the parameters and the initial values (x, y, a, b). The sensitivity of Duffing map from any varies small change in any parameters of initial values make the result variable and receive wrong information. Figure 6 shows the operation without any change in the parameter values, where the values of $X(1) = -1, Y(1) = 0.5, a = 2.75$ & $b = 0.15$.

However, when adding a change to the value of 0.000001 to one of the variables, it leads to a deviation from the path of receiving the correct information, and thus the hacker is not able to retrieve the information even when its presence is sensed. Figure 7 shows the received message, where values of parameters as $(X(I) = -1, Y(I) = 0.5 + 0.000001, a = 2.75 \text{ \& } b = 0.15)$.

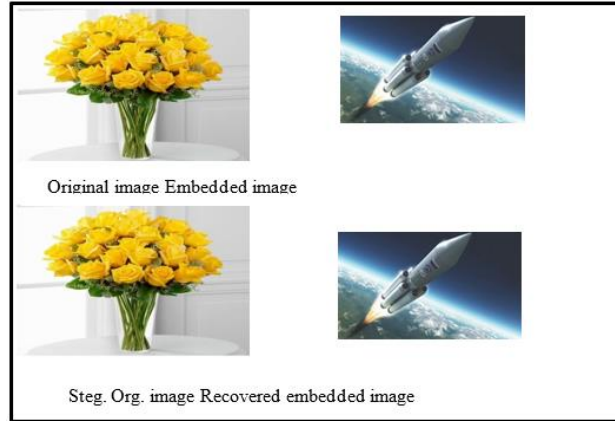


Figure 6. Shows the operation without any change in the parameter values



Figure 7. Received message when change in parameter

Parameter values that determine the efficiency of the system (SSIM, MSE, and PSNR) change in certain proportions. In the last case at $Y(I) = 0.5 + 0.000001$ and Table 3 shows each parameter value that measures the quality of the image. The histogram of the recovered secret image will be completely different from that sent image. The reason is due to a very small change which occurred in the values of the parameters used, which act as secret keys known to the sender and the recipient only. Figure 8 shows this case when the change in the parameter about 0.000001.

Table 3. Parameters measuring of image quality when a change in parameter

Parameters measuring of image quality	SSIM%	MSE	PSNR (dB)
Value	25%	0.95	48.53

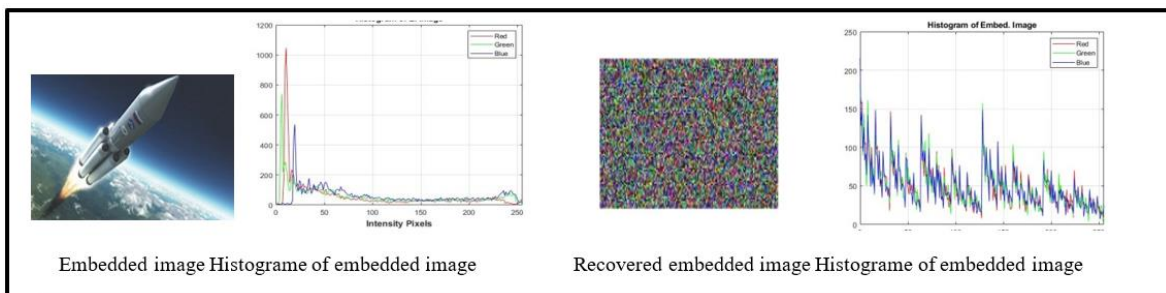


Figure 8. Histogram of receiving messages when change in parameter

7. CONCLUSION

There are different ways to withhold secret data. An efficient algorithm for performing steganography was properly presented in this work. The proposed method represents a high-resolution chaotic approach to be applied to the information hiding images. In which, a more secure and reliable system is properly designed to include the secret data sent over transmission channels. This is achieved by working with the encryption and steganography system together. The highest PSNR and lowest MSE value were obtained objectively compared to other effective methods that use both encryption and steganography together. In summary, the obtained results of the proposed method show that a robust algorithm can be created. The used methods sufficiently developed in this research can be much more robust alongside a deep learning algorithm that can be addressed in future research.




REFERENCES

- [1] W. Easttom, "Steganography," in *Modern Cryptography*, pp. 337-356, December 2020, doi: 10.1007/978-3-030-63115-4_16.
- [2] E. A. Hussein, M. K. Khashan, and A. K. Jawad, "A High Security and Noise Immunity of Speech Based on Double Chaotic Masking," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 4270-4278, August 2020, doi: 10.11591/ijece.v10i4.
- [3] S. Alam, V. Kumar, W. A. Siddiqui, and M. Ahmad, "Key Dependent Image Steganography Using Edge Detection," in *2014 Fourth International Conference on Advanced Computing & Communication Technologies*, Feb. 2014, pp. 85-88, doi: 10.1109/ACCT.2014.72.
- [4] K. M. Sabery and M. Yaghoobi, "A Simple and Robust Approach for Image Hiding Using Chaotic Logistic Map," in *2008 International Conference on Advanced Computer Theory and Engineering*, Dec. 2008, pp. 623-627, doi: 10.1109/ICACTE.2008.178.
- [5] K. Senthil, K. Prasanthi, and R. K. Rajaram, "A Modern Avatar of Julius Ceasar and Vigenere Cipher," *International Conference on Computational Intelligence and Computing Research*, pp. 1-3, Dec. 2013, doi: 10.1109/ICCC.2013.6724170.
- [6] A. Anees, A. M. Siddiqui, J. Ahmed, and I. Hussain, "A Technique for Digital Steganography Using Chaotic Maps," *Nonlinear Dynamics*, pp. 807-816, Mar. 2014, doi: 10.1007/s11071-013-1105-3.
- [7] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of LSB steganography and its evaluation for various bits," in *2006 1st international conference on digital information management*, Dec. 2006, pp. 173-178. IEEE, doi: 10.1109/ICDIM.2006.369349.
- [8] Z. Liu and T. Xia, "Novel Two Dimensional Fractional-Order Discrete Chaotic Map and Its Application to Image Encryption," *Appl. Comput. Info.*, vol. 14, no. 2, pp. 177-185, July 2018, doi: 10.1016/j.aci.2017.07.002.
- [9] K. A. K. Patro and B. Acharya, "A simple, Secure, and Time-Efficient Bit-Plane Operated Bitlevel Image Encryption Scheme Using 1-D Chaotic Maps," *Innovations in soft computing and information technology*, Springer, Singapore, pp. 261-278, January 2019, doi: 10.1007/978-981-13-3185-5_23.
- [10] M. K. Mandal and A. K. Das, "Chaos-Based Colour Image Encryption Using Microcontroller ATMEGA 32. Nanoelectronics," *Circuits and Communication Systems*, Springer, Singapore, pp. 281-287, August 2019, doi: 10.1007/978-981-13-0776-8_26.
- [11] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010, doi: 10.1016/j.sigpro.2009.08.010.
- [12] V. Hajduk, M. Broda, O. Kováč, and D. Levický, "Image steganography with using QR code and cryptography," in *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*, pp. 350-353, April 2016, IEEE, doi: 10.1109/RADIOELEK.2016.7477370.
- [13] S. Pramanik, R. Ghosh, D. Pandey, D. Samanta, S. Dutta, and S. Dutta, "Techniques of Steganography and Cryptography in Digital Transformation," in *Emerging Challenges, Solutions, and Best Practices for Digital Enterprise Transformation*, pp. 24-44. IGI Global, 2021, doi: 10.4018/978-1-7998-8587-0.ch002.
- [14] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Secured and Robust Information Hiding Scheme," *Paper presented at the Malaysian Technical Universities Conference on Engineering and Technology (MUCET2012)*, Kangar, Perlis, Malaysia, vol. 53, no. 7, 2012, pp. 463-471, doi: 10.1016/j.proeng.2013.02.060.
- [15] Q. Ding and J. Pan, "The Research of Optimization Parameter Based on Lorenz Chaotic Masking Secure Communication," *First International Conference on Pervasive Computing, Signal Processing and Applications*, 2010, pp. 1136-1139, doi: 10.1109/PCSPA.2010.280.
- [16] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, no. 3, pp. 727-752, 2010, doi: 10.1016/j.sigpro.2009.08.010.
- [17] M. Cattani, I. L. Caldas, S. L. de Souza, and K. C. Iarosz, "Deterministic Chaos Theory: Basic Concepts," *Rev. Bras Ensino Fis.*, vol. 39, no. 1, 2017, doi: 10.1590/1806-9126-RBEF-2016-0185.
- [18] B. Jovic, "Chaotic Signals and Their Use in Secure Communications," in *Synchronization Techniques for Chaotic Communication Systems*, pp. 31-47, 2011, doi: 10.1007/978-3-642-21849-1_2.
- [19] A. Kanso and H. S. Own, "Steganographic algorithm based on a chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 8, pp. 3287-3302, 2012, doi: 10.1016/j.cnsns.2011.12.012.
- [20] J. Feng, "Chaos controls of a duffing system with impacts," *AIP Advances*, vol. 8, no. 4, pp. 045303, 2018, doi: 10.1063/1.5021965.
- [21] X. Wang, J. Zhao, and H. Liu, "A new image encryption algorithm based on chaos," *Optics Communications*, vol. 285, no. 5, pp. 562-566, 2012, doi: 10.1016/j.optcom.2011.10.098.
- [22] R. Wang, J. Deng, and Z. Jing, "Chaos control in duffing system," *Chaos, Solitons & Fractals*, vol. 27, no. 1, pp. 249-257, 2006, doi: 10.1016/j.chaos.2005.03.038.
- [23] R. J. Anderson and F. A. Petitcolas, "On the limits of steganography," *IEEE Journal on selected areas in communications*, vol. 16, no. 4, pp. 474-481, doi: 10.1109/49.668971.
- [24] T. Bedwal and M. Kumar, "An enhanced and secure image steganographic technique using RGB-box mapping," in *Confluence 2013: The Next Generation Information Technology Summit (4th International Conference)*, Jun. 2014, pp. 385-393, doi: 10.1049/cp.2013.2347.




- [25] S. Rajendran and M. Doraipandian, "Chaotic map based random image steganography using lsb technique," *Int. J. Netw. Secur.*, vol. 19, no. 4 pp. 593-598, 2017, doi: 10.6633/IJNS.201707.19(4).12).
- [26] S. D. Ahmadi and H. Sajedi, "Image steganography with artificial immune system," *Artificial Intelligence and Robotics (IRANOPEN)*, pp. 45-50. IEEE, 2017, doi: 10.1109/RIOS.2017.7956442.

BIOGRAPHIES OF AUTHORS



Aliaa Sadoon Abd    Electrical Engineer was born in Karbala on 1995. She obtained his BCs degree (2017) in Electrical Engineering at the Faculty of Engineering, University of Babylon. Currently she is studying for a master's degree in Electrical Engineering at the Faculty of Engineering, University of Babylon. Her main interest is communication systems, digital signal processing, and security. She can be contacted at email: alia.burhan@student.uobabylon.edu.iq.



Ehab AbdulRazzaq Hussein, PhD. MSc.    Electrical Engineering was born in Babylon on January 1, 1976. He obtained his BSc degree (1997) in Electrical Engineering at the Faculty of Engineering, University of Babylon and MSc degree (2000), in electrical engineering at the Department of Electrical Engineering, University of Technology and his PhD degree (2007) from the Department of Electrical Engineering at the Faculty of Engineering, University of Basrah, Currently he works as professor at the Electrical Department at the Faculty of Engineering, University of Babylon. His main interest is signal processing, security, information transition, sensors and control system analysis. ResearchGate Profile: <https://www.researchgate.net/profile/Ehab-Hussein>. He can be contacted at email: dr.ehab@uobabylon.edu.iq.