



Designing a Model for Hiding Images in RGB Cover Image Based Scrambling and Encryption Methods

Sheimaa A. Hadi*, Asraa Abdullah Hussein, Rafeef M. Al Baiyy

Department of Computer Science, University of Babylon, Babylon, Iraq

Corresponding Author Email: shaymaa.hadi@student.uobabylon.edu.iq

Copyright: ©2023 IIETA. This article is published by IIETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.130620>

ABSTRACT

Received: 24 September 2023

Revised: 28 November 2023

Accepted: 15 December 2023

Available online: 25 December 2023

Keywords:

steganography, gray image, encryption, scrambling, xor

In the digital world, one of the crucial issues is protecting information transmitted over a public network; therefore, encryption and steganography methods must be used to raise the level of data security. This paper invests scrambling and encryption techniques to protect data and compress it to reduce its size, thus increasing system performance. The system is built on protecting gray images after passing a set of steps. The first step denotes the scrambling stage that scatters the locations of gray images by adopting a logistic map method to make it difficult for intruders. The second step contains scattering the image again using the same method but with a different equation and then performing encryption based on the xor operation. The third step represents embedding the data and includes dividing the RGB cover image into three bands where each band is divided into (4×4) blocks, and the bits are stored in the location (2,2) from each band. It tested the system's efficiency by conducting experiments on a set of grayscale images and then using PSNR as a measurement function, where the result was 67.9705.

1. INTRODUCTION

The digital world with computer aid plays a vital role in exchanging information and facilitating many things in all areas of life, including banks, hospitals, companies, and trade [1, 2]. This information is subject to theft by unreliable people and hackers. Therefore, protecting and securing information has become the responsibility of all researchers who have enriched this field with much research using one data protection technique [3].

Encryption and concealment are among the most [4] important ways to protect information. Hiding is embedding information in various digital media such as text, image, video, and sound. In this way, the hidden information is not visible and is not noticed [5]. Encryption is the process of converting sensitive and important data into a chaotic, incomprehensible form and is used with concealment to increase the security level [6, 7].

The importance of protecting data from malicious violations by unauthorized parties appears in many areas such as preserving the information of people working in security, commercial and service companies also in the field of health care in terms of protecting medical records sent through public channels [1, 5].

2. RELATED WORK

The field of data protection and concealment is rich with researchers' products, this section reviews some of them. The researchers in the study of Ahmad and Abidi [8] used Deep

Learning as a way to hide data inside images. After that, to increase the level of security and confidentiality, the stego cover image was encrypted using Elliptic Curve Cryptography.

Invest the colors of the image and suggest a way [9] to combine MSB with LSB. The system uses a checker when replacing less important data with more important data. The proposed system has proven its efficiency in maintaining the quality of the steganography image through computing the histogram measurement between the cover image and the hidden image. To improve security and confidentiality, the researchers in the study of Durdu [10] suggest using two levels to conceal a color image inside another color image. The cover image is first resized by the system, and then LSB is applied to conceal the data. The output of the first level is sent to the second level, where it is concealed under the cover image. The suggested system [11] creates a conversion link between the sensitive information and the stego image by using an ISTNet steganography algorithm to create a stego image that is relatively similar to the original cover image.

Duan et al. [12] presented a new hiding method that uses deep learning with a high hiding capacity. The secret image is first converted using DCT and encrypted using Elliptic Curve Cryptography. A method called the SegNet has been adopted to improve the hiding capacity. The results of the system showed effective efficiency in assigning each pixel in the cover image so that the data hiding capacity reached 1.

Hamza et al. [13] proposed a new way to hide an encrypted binary logo image by generating two secret shares. The RGB cover image (512×512) is divided into three red, green, and blue bands during the data embedding process. Apply the Shearlet Transform (DST) to the blue band to get its

transactions. The first secret share is included in the blue band transactions and, when extracted, applies xor with the second secret share to generate the original binary logo image. The researcher in the study of Hamza [14] presented a method to hide logo images by adopting the ACM method and a matrix

of random bits generated by using BBS CSPRNG to encrypt the image to be hidden. The cover image is divided into blocks in the embedding process, and entropy is calculated for each block. The block with the highest entropy is selected for hiding using an LSB algorithm (Table 1).

Table 1. Comparison between studies

Year	Reference No.	Details of Methods	Measures
2022	[8]	Deep Learning and Elliptic Curve Cryptography	PSNR=0.99 and 35 dB
2021	[9]	Combine (LSB and MSB) bits based on check MSB	PSNR=72.023, MSE=0.0040
2021	[10]	LSB with two layers of hiding	PSNR=1.2 dB, SSIM=0.0025
2021	[11]	Image Style Transfer (ISTNet)	Increases steganography capacity from 0.06 bpp to 8 bpp
2020	[12]	SegNet Deep Neural Network, Discrete cosine transform (DCT) Elliptic Curve Cryptography (ECC)	PSNR=40dB, SSIM=0.96
2022	[13]	Visual cryptography, Discrete Cosine Transform (DCT)	PSNR=54.15 SSIM=0.9999
2019	[14]	ACM and an array of random bits generated using BBS CSPRNG	The suggested method achieved the best quality for the stego-image

3. CONCEPTUAL FRAMEWORK

3.1 Chaotic map

A nonlinear mathematical function that provides a random string that is hard to predict is widely used in cryptography systems based on random to increase the system's robustness against attacks and thefts [15]. One of the most well-known chaotic maps is the logistic map, characterized by its simplicity and ability to show chaotic behavior when used in many dynamic systems under certain conditions and limitations. Therefore, it was adopted in this paper as a method for scattering image locations. A logistic map provides a one-dimensional random binary series using the following equation [16]:

$$y_{n+1} = \mu * y_n * (1 - Y_n) \quad (1)$$

where, μ represent a parameter between [0,4], y_{n+1} represent new chaotic set from (0,1), Y_n represent current set from (0,1).

3.2 Encryption

Encryption is securing information so that only authorized parties can read it. It is done by converting the original plain text message into cipher text using one of the encryption algorithms [17]. There are several types of encryption methods, mainly divided into symmetric essential encryption methods, where the same key is used for encryption and decryption, and the other type is called asymmetric encryption, in which different keys are used for encryption and decryption [18]. Xor was used as a method of encryption in order to increase the level of security and increase confidentiality.

3.3 Scrambling

Scrambling is a technique used to alter or rearrange data or information, making it easier to understand or interpret with a specific method or algorithm to reverse the process. Scrambling can be used for various purposes, such as protecting sensitive information, preventing unauthorized access to data, or ensuring the confidentiality of messages or communications [19, 20]. This paper used scattering twice

using the logistic map to add randomness and thus increase the efficiency and robustness of the proposed system.

4. PROPOSED METHOD

This paragraph explains the processes of hiding and retrieval at the sender and recipient, as shown in Figure 1.

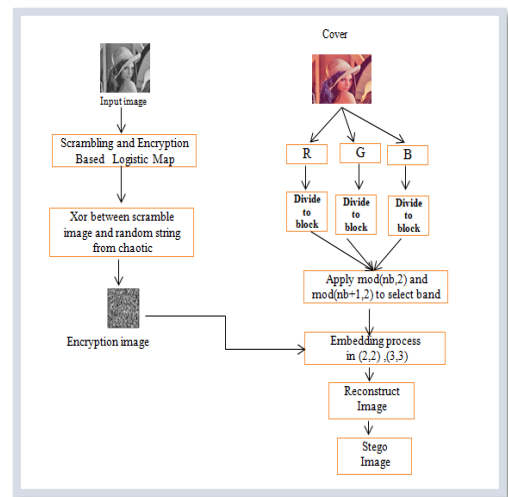


Figure 1. General diagram for proposed system

Sender side “steganography stage”.

Step1: Read the cover RGB image and image to be protected

Step2: Scrambling

2.1 Scatter the secret image using a logistic map by generating a random string whose values are between (0-255) and of the same length as the image to be protected with parameters (initial values=0.1, size=4096, r=3.8).

2.2 arrange the generated random string and keep its positions as well.

2.3 scatter the gray image by rearranging its pixels depending on the index values retrieved from the random string arrangement.

Step3: Encryption

3.1 Before starting the encryption process, the secret image is again in order to increase security by adopting another

method of scattering the values based on the following equation:

$$Y = \text{mod}(k, m) + 1 \quad (2)$$

where, k from equation $k = (\text{key} * L)$;

Key: prime number;

L: a counter starting from 1 to the length of the block;

m: index of value original random string generated using the logistic map.

3.2 An xor has been made between the scattered image generated in step 2 and the scattered random series currently generated.

3.3 Reshape it into an image (64×64).

Step4: Embedding

4.1 Dividing the cover RGB image into three bands (R, G, and B), then splitting each band into non-overlapping blocks of size (4×4).

4.2 In the embedding process, the secret data bits are distributed as follows: Test each band of the three bands for the hiding process according to the following equation:

$$\text{Mod}(nb, 3) \quad (3)$$

where, nb represents no. of block.

- a. If the remainder is 0, the block is selected from Band R.
- b. If 1, the block is selected from band G.
- c. If two, the block is selected from band B and stored in the site (2,2) in the LSB method.

In the same cycle, the equation is applied to the following block number according to the equation:

$$Bb = \text{mod}(nb + 1, 3) \quad (4)$$

It is hidden according to the result. If it is zero, it selects the first band and so on, and it is stored on the site (3, 3).

In other words, in one cycle, two bits are stored in the locations (2, 2) and (3, 3) according to the result of the above equations. Receiver side “Extraction stage”.

At this stage, the recipient divides the hidden image into three bands (R, G, B), each into blocks (4×4). From the R band array, choose the pixel (2,2) to retrieve the first bit of the secret data where the G band retrieves the second and third bit from the B band, respectively, to get the string of secret data. After obtaining the entire secret string, the decoding xor method is made between the string decompression and the generated random string using a logistic map method described previously in step 3. The last step is to retrieve the original string before scattering and then reshape it into an image.

5. RESULT

This part reviews the results of the proposed system building using a set of grayscale secret images with a dimension of 64×64 within an RGB cover image of 512×512 (Figure 2).

5.1 Evaluate the encryption method

Before presenting the results, reviewing the most important criteria used in evaluating the proposed coding method is necessary.

A coding method was applied, and general metrics were adopted to evaluate the strength of the proposed coding

method. It uses the degree of correlation between two adjacent pixels in an image or the degree of relationship between them. It is called correlation, a statistical measure of safety calculated based on the following Eq. (5).

$$CC = \frac{\sum_K \sum_L (I_{mn} - \bar{I}) * (Q_{mn} - \bar{Q})}{\sqrt{\sum_m \sum_n (I_{mn} - \bar{I})^2 * (Q_{mn} - \bar{Q})^2}} \quad (5)$$



Figure 2. Grayscale secret images and cover image

In addition, the average unified variable intensity and the pixel rate of change number were used. UACI stands for average intensity differences between the plane and encoded images. In contrast, NPCR represents the percentage of pixel numbers between the plane and encoded images. These are computed depending on the following equations. The results of encoding are shown in the Table 2.

$$NPCR = \frac{B(i,j)}{m * n} \quad (6)$$

$$B(i,j) = \begin{cases} 0 & \text{if } Orj_{img(i,j)} = decr_{img} \\ 1 & \text{Otherwise} \end{cases} \quad (7)$$

$$UACI = \frac{1}{m * n} \left[\sum_{i,j} \frac{B(i,j) - \bar{B}(i,j)}{L - 1} \right] \quad (8)$$

5.2 Evaluate the proposed system

The quality of the stego-image and the embedding capability are the two characteristics we consider for evaluation. The quantity of secret bits embedded in the cover image is a gauge for capacity. Various metrics, including PSNR, can be used to evaluate the stego-quality images. The average pixel difference between the cover image and the stego image is measured using PSNR. The quality of the stego image is inversely proportional to the PSNR value. The mean square error (MSE) indicates the squared error between the stego and cover images. The PSNR and MSE are Computes as follows:

$$PSNR = 10 \log_{10} \frac{(2^p - 1)^2}{MSE} \quad (9)$$

$$MSE = \frac{1}{K * L} \sum_{i=1}^k \sum_{j=1}^L (I_{k*m} - \bar{I}_{k*m})^2 \quad (10)$$

Table 2. Result of encryption









Secret Images	Encrypted Image (64*64)	Correlation Coefficient Values	NPCR Values	UAC Values
		0.0302	99.6094	33.4543
		0.0093	99.6582	34.7906
		0.0208	99.5361	33.5169
		0.0190	99.6582	36.3352

Table 2 and Figure 3 note that the correlation coefficients (CC) are extremely low, indicating that the original image and its encrypted counterpart are entirely unrelated, which suggests that image encryption is highly effective and offers higher security. The two highest values for (NPCR) and (UACI) indicate 99.6094 and 36.3352, respectively, while the two lowest values for (NPCR) and (UACI) are 99.5361 and 33.4543, respectively, for the images tested in the encryption system, as shown in Table 2, which indicates that the proposed system is robust against differential attacks.

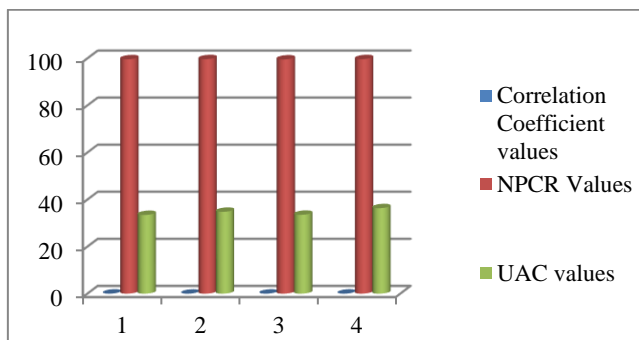


Figure 3. The result of encryption measures

6. CONCLUSION

The charge of development in the world of technology and the Internet is the fear of information theft and manipulation by unauthorized persons. Therefore, work continues despite scientists and researchers developing methods and techniques for protecting information and providing this field with a lot of research and systems. This paper proposes a system to hide gray images in RGB cover images, starting by scattering the image using the logistic map method and then encoding-based xor with a second scatter in the same way. The next step is the

embedding process by distributing bits successively on the image bands after they are divided into blocks (4×4). From the results shown in the tables above, it can be noted that the proposed encryption method gives high values after matching the original image with the encrypted one, as the correlation coefficients are very small, represented by the highest value of 0.0302, and this indicates the efficiency of the proposed method.

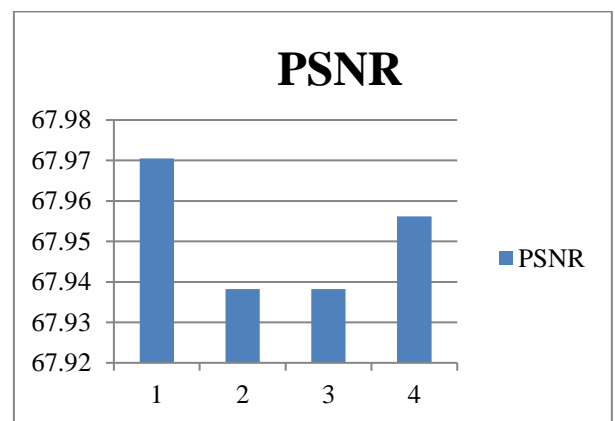


Figure 4. The PSNR in a set of experiences

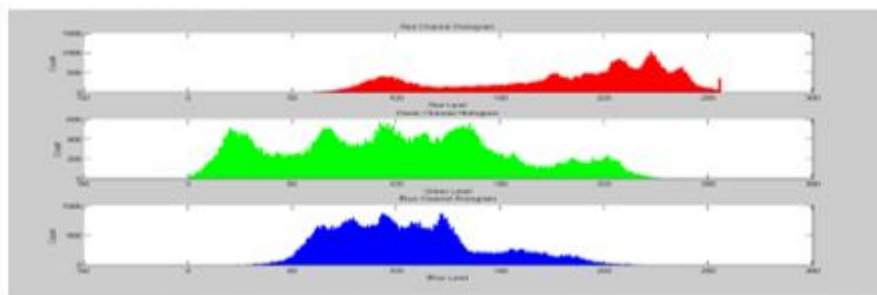
In addition, the masking system presented in this paper achieved perfect results by not noticing any distortion in the overlay image, and this is clear from the value of the PSNR (Figure 4); the lowest value for the tested images is 67.9382 (Table 3 and Figure 5).

Future works:

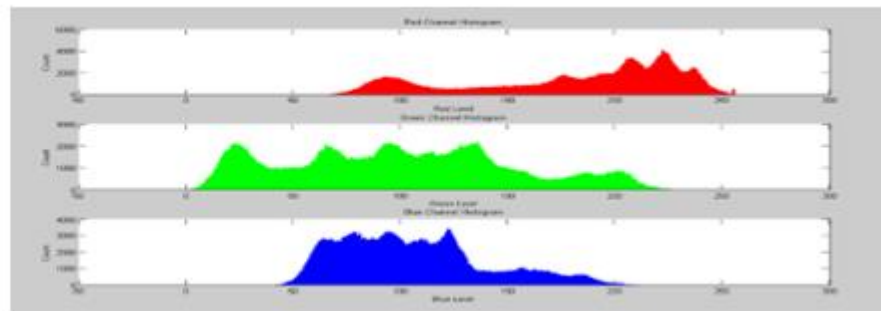
- 1- Developing the proposed method to apply it to color images and hide them within a video.
- 2- Developing the method to be applied to other types of media.
- 3- Adding some improvements to the proposed method for use in protecting medical images.

Table 3. Result of proposed system

Cover Image	Secret Images	PSNR	MSE
		67.9705	0.0104
		67.9382	0.0104
		67.9382	0.0105
		67.9562	0.0104



(a)



(b)

Figure 5. (a) The original cover image and RGB histogram, (b) The stego image and RGB histogram

REFERENCE

[1] Naser, M.A., Al-alak, S.M.K., Hussein, A.M., Jawad, M.J. (2022). Steganography and cryptography techniques based secure data transferring through public network channel. *Baghdad Science Journal*, 19(6): 1362-1368. <https://doi.org/10.21123/bsj.2022.6142>

[2] Yahya, A. (2019). *Steganography Techniques for Digital Images*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-78597-4>

[3] Kaur, A., Kaur, R. (2019). RGB based images steganography for hiding single and multiple data for security. *International Journal of Research in Electronics and Computer Engineering*, 7(4): 130-136.

[4] Neamah, R.M., Abed, J.A., Abbood, E.A. (2020). Hide text depending on the three channels of pixels in color images using the modified LSB algorithm. *International Journal of Electrical and Computer Engineering*, 10(1): 809-815. <http://doi.org/10.11591/ijece.v10i1.pp809-815>

[5] Thahab, A.T. (2019). A secure image steganography

- based on burrows-wheeler transform and dynamic bit embedding. *International Journal of Electrical and Computer Engineering (IJECE)*, 9(1): 460-467. <http://doi.org/10.11591/ijece.v9i1.pp460-467>
- [6] Taouil, Y., Ameer, E.B. (2018). Steganographic scheme based on message-cover matching. *International Journal of Electrical and Computer Engineering (IJECE)*, 8(5): 3594-3603. <http://doi.org/10.11591/ijece.v8i5.pp3594-3603>
- [7] Shukur, W.A., Jabbar, K.K. (2018). Information hiding using LSB technique based on developed PSO algorithm. *International Journal of Electrical and Computer Engineering (IJECE)*, 8(2): 1156-1168. <http://doi.org/10.11591/ijece.v8i2.pp1156-1168>
- [8] Ahmad, S., Abidi, M.R. (2022). RGB based secure share creation in steganography with ECC and DNN. *Applications of Artificial Intelligence and Machine Learning*, Springer, Singapore, 237-250. https://doi.org/10.1007/978-981-19-4831-2_20
- [9] Mahdi, S.A., Maisa'a, A.K. (2021). An improved method for combine (LSB and MSB) based on color image RGB. *Engineering and Technology Journal*, 39(1): 231-242. <https://doi.org/10.30684/etj.v39i1B.1574>
- [10] Durdu, A. (2021). Nested two-layer RGB based reversible image steganography method. *Information Technology and Control*, 50(2): 264-283. <https://doi.org/10.5755/j01.itc.50.2.27461>
- [11] Bi, X.L., Yang, X.Y., Wang, C., Liu, J. (2021). High-capacity image steganography algorithm based on image style transfer. *Security and Communication Networks*, 2021: 4179340. <https://doi.org/10.1155/2021/4179340>
- [12] Duan, X., Guo, D., Liu, N., Li, B., Gou, M., Qin, C. (2020). A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access*, 8: 25777-25788. <https://doi.org/10.1109/ACCESS.2020.2971528>
- [13] Hamza, Y.A., Tewfiq, N.E., Ahmed, M.Q. (2022). An enhanced approach of image steganography using discrete Shearlet transform and secret Sharin sharing. *Baghdad Science Journal*, 19(1): 197-207. <https://doi.org/10.21123/bsj.2022.19.1.0197>
- [14] Hamza, Y.A. (2019). Highly secure image steganography approach using Arnold's Cat map and maximum image entropy. In *ICICT '19: Proceedings of the International Conference on Information and Communication Technology*, Baghdad, Iraq, pp. 134-138. <https://doi.org/10.1145/3321289.3321323>
- [15] Hadi, S.A., Ali, S.A., Jawad, M.J. (2022). A non-blind image watermarking method for -0652 copyright protection. *Journal for Babylon for Pure and Applied Sciences*, 30(2): 34-67.
- [16] Yu, C.Y., Li, X.W., Chen, X.N., Li, J.Z. (2019). An adaptive and secure holographic image watermarking scheme. *Entropy*, 21(5): 460. <http://doi.org/10.3390/e21050460>
- [17] Mangi, H.T., Ali, S.A., Jawad, M.J. (2023). Encrypting of text based on chaotic map. *Journal for Babylon for Pure and Applied Sciences*, 31(1): 25-39.
- [18] Menon, U., Menon, A.R., Hudlikar, A. (2020). A novel chaotic system for text encryption optimized with genetic algorithm. *International Journal of Advanced Computer Science and Applications*, 11(10): 34-40.
- [19] Taha, M.S., Mohd Rahim, M.S., Lafta, S.A., Hashim, M.M., Alzuabidi, H.M. (2019). Combination of steganography and cryptography: A short survey. *IOP Conference Series: Materials Science and Engineering*, 518: 052003. <https://doi.org/10.1088/1757-899X/518/5/052003>
- [20] Qu, Z.G., Cheng, Z.W., Wang, X.J. (2019). Matrix coding-based quantum image steganography algorithm. *IEEE Access*, 7: 35684-35698. <https://doi.org/10.1109/ACCESS.2019.2894295>