Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
ISSN: 2788-7421

Image Steganography Based on Chaotic Function and Randomize Function

Rusul Mansoor Al-Amri[1], Dalal N. Hamood[2], Alaa Kadhim Farhan[3]

[1]Computer Department/College of Science University AL-Nahrain, Baghdad, 10001, Iraq
[1]College of Nursing, University of Al-Ameed Karbala, PO No: 198 Iraq
[2]Computer Department/College of Science University AL-Nahrain, Baghdad, 10001, Iraq
[3]Department of Computer Sciences, University of Technology, Baghdad 10011, Iraq

*Corresponding Author: **Rusul Mansoor Al-Amri**

DOI: https://doi.org/10.52866/ ijcsm.2023.01.01.007
Received Sebtember 2022; Accepted December 2022; Available online January 2023

ABSTRACT: The exchange of data is not limited to personal text information or information about institutions and governments, but includes digital media transferred via the Internet including everything, whether texts, images or videos and audio, or animation. These media need high-security protection and high speed during its transmission from one site to another. In this study, a new method is suggested for hiding a gray-level image within a larger color image based on the proposed steganography map that merged chaotic function and randomize function. The size of the chaos and randomize functions is 16 bytes. Experimental results obtained a successful method based on mean squared error, signal-to-noise ratio, peak signal noise rate, embedding capacity, entropy, and histogram. This method can rapidly hide and extract ciphertext in and from the gray image. The original image and the stego image are difficult to distinguish because the correlation between them is very close to 1, indicating that attackers cannot easily differentiate these images with the naked eye. This condition can successfully hide information on the Internet.

Keywords: Randomize Function, Chaotic Function, Color Image, LSB Technique.

1. INTRODUCTION

Safeguarding private data transferred via networks is highly necessary. [1] [2]. These data include not only personal text information or information about institutions and the government, but also digital media via the Internet, such as everything, whether texts, images, videos or audio, and animation [3] [4]. These media need high-security protection and high speed during its transmission from one site to another [5]. The exchange of all media, whether digital or text, is highly susceptible to intrusive attacks, especially at the present time, where tools and methods that can violate privacy [6][7], data security, and safety are available. Therefore, researchers determine more complex hiding methods and discover how these algorithms suffer from easy access by attackers [8][9]. Some algorithms suffered from slowness during hiding. Thus, this research introduces a steganography method. The proposed method is better than the previous approach, where the steganography map depends mainly on merging two maps. Map1 consists of 16 numbers generated from chaotic functions, whereas map2 consists of 16 numbers generated from the randomized function that generates numbers between ranges 0 and 3. The final map is obtained after merging these maps. The final map shows gray images of different sizes, and resolutions are hidden in color images with large size. This proposed method was characterized by the fact that the method of concealment is difficult to break and has a high level of safety and protection. Related works are presented in Section 2. The required measurements are explained in Section 3. The proposed method is discussed in Section 4. Section 5 presents the results of the study, as well as the conclusions. Section 6 lists the references.

2. RELATED WORK

Arshiya S. Ansari, Mohammad S. Mohammadi, and Mohammad T. Parvez [10] proposed a masking method that is suitable for various image formats, particularly for the cover image. This method has many benefits, including the

*Corresponding author: sosoalhaji28@gmail.com

application of unified security to all image formats, the ability to select the cover images that are most appropriate for the length of the data and network bandwidth. The results of this method are very effective and efficient

Yasir Ahmed Hamza, Nada Elya Tewfiq, and Mohammed Qasim Ahmed [11], along with visual coding, suggested improving image masks. Images were captured with a size of 128x128. Binary images are encrypted by sharing (2 out of 2), from which two secret participations are generated during the entry process, and the cover image is divided into three layers (RGB) with a size of 512x512. The method starts by converting the first layer of blue color through the discrete Shearlet transform (DST), resulting in the first secret participation in the first layer (blue) converted on the image masks. The criteria are applied to the experimental results, and the first image's participation is extracted from the encrypted image using the blue layer's coefficients and XORed. The second secret participation is used to create the secret logo for the original image. Then, the results obtained were in accordance with the criteria's standards. This suggested approach was coded to compare with the research from our work (EISU (DST and SSH)).

Raheem Abdul Sahib Ogla [12] proposed a method of masking based on the spiral search machine, where they used the measures of the structural index to obtain the image quality, retrieved accuracy, and improved quality. The results showed that the use of evaluation criteria, mean squared error (MSE) and peak signal-to-noise ratio (PSNR), improved the image quality by approximately 87%. Our research was compared with the suggested approach, and the proposed method was labeled and compared (SBSTUSSMFHSVCI).

Srushti S Yadahalli, Shambhavi Rege, and Dr. Reena Sonkusare [13] relied on the implementation of masking on two methods, the first (LSB) and the second (DWT). The image to be transferred was explained, encoded, and decoded using these methods, and then analyzed using image parameters. This proposed method obtained highly efficient results after applying the criteria. This suggested approach was written to compare with our work (IAAOISU LSB and DWT).

Jiaohua Qin, Yuanjing Luo Xuyu Xiang, Yun Tan, and Huajun Huang [14] covered the main areas of coverless image steganography research, which comprises more than 50 significant contributions. The study includes the underlying structures, pre-processing, feature extraction, production of hash sequences, and mapping relationships. The potential for future study is also highlighted, along with an assessment of the current methodologies.

Muhammad Aminul Islam, Md. Al-Amin Khan Riad, and Tanmoy Sarkar Pias [15] utilized an image as the cover object, and text is used as a secret message. Images in 24-bit RGB color are utilized for coverage and hiding purposes. This approach transforms a secret image into a new image called share2 image using a new image named share1. People can typically readily obtain the secret message if they are aware of the extraction technique. Visual encryption adds an extra layer of protection by using a key that is created by somebody once. We guarantee secured image steganography by using the suggested technique.

S. Sravani and R. Raniith [16] focused on steganography utilizing the LSB method. The method entails cloaking a secret image under a cover image before sending it via the internet. Text, images, audio clips, and video files can be used with this technique. Here, steganography is designed to conceal the position of a region (for example, in the form of a map) inside a cover image and send the image over the internet. For its use in security-based applications, the performance of this approach has been examined using MSE and PSNR values.

3. Required measurement

Many measurements for testing the experimental results are used in this sturdy. These measurements are as follows:

1. **MSE** is the average square of the pixel-by-pixel difference between the original image and the stego image is known as the MSE. It provides a gauge of the inaccuracy of the data embedding method in the cover image [17][18] [19]:

$$MSE=(a*b)^{-1}\sum_{i=1}^{a}\sum_{j=1}^{b}[I(I,j)-S(i,j)]^{2}\ldots\ldots(1)$$

a, b = Dimensions of the image   I = Original Image   S = stego image

2. **PSNR** is another well-liked metric for determining how much embedding has warped the cover image. It is the ratio of a signal's greatest possible value to its distortion noise power (MSE). It is expressed in dB. A higher PSNR value denotes a higher-quality embedding [20][21]:

$$PSNR=10\log_{10}\left(MAX^{2}/MSE\right)\ldots\ldots\ldots\ldots(2)$$

For an eight-bit gray scale image, MAX = 255.

3. **Entropy** A measure of the degree of uncertainty surrounding a group of variables is called joint entropy [22][23][24]:

$$H(S)=-\sum_{i=1}^{n}P(X)\log_{b}P(X_i)\ldots\ldots(3)$$

H (X) = amount of randomness for a variable (X), $\sum_{i=1}^{n}$ = sum of the variable's possible values
P(X) = probability of event X, *b* = the chosen log base.

2- **Embedded capacity** (EC) is used to embed and calculate the highest number of safe bits that can be hidden in the image that is measured in units of bits per pixel (bpp) [25][26].

$$\mathbf{EC = N/(H*W)\ bPP \ \ldots\ldots\ldots\ldots\ldots (4)}$$

EC = Embedded capacity, N = highest number of safe bits, H = Height of image,

W = Width of image, bpp = bit per pixel

2- **Histogram** is used to enhance contrast in photographs, and equalization is a computer image processing technique. It achieves this condition by successfully extending the intensity range of the image and effectively spreading out the most common intensity levels [27].

6. **Investigation and correlation.** The variance refers to how the pixel values are spread in the images, where the variance is calculated for the original image and the stego image**,** whereas correlation coefficients are used to measure the strength of the relationship between two variables [28][29][30].

4. METHOD PROCESS

In this proposed method, the practical scheme is clarified in general, especially in hiding the gray-level image within the large color image of the displayed model by selecting an indiscriminate gray image with certain characteristics that have been converted into a Binary Code and it is hidden according to a proposed map inside another color image that has been indiscriminately selected with certain characteristics and specifications, as shown in Figure (1). In this study, a method or map to steganography was proposed based on the merger between map 1 which represents those generated by chaotic function, and map 2 based on randomize function. Chaotic function (map 1) consists of 16 characters generated by the chaotic logistic function, and randomize function (map 2) consists of 16 characters generated by randomizing function. Each number is divided by 3, and the remainder is obtained because hiding is limited by three bits only. After the two maps are created, they are combined. Thus, the final map is formed, which is 32-character long, as shown in Figure (2). The main steps of the proposed method are illustrated as follows:

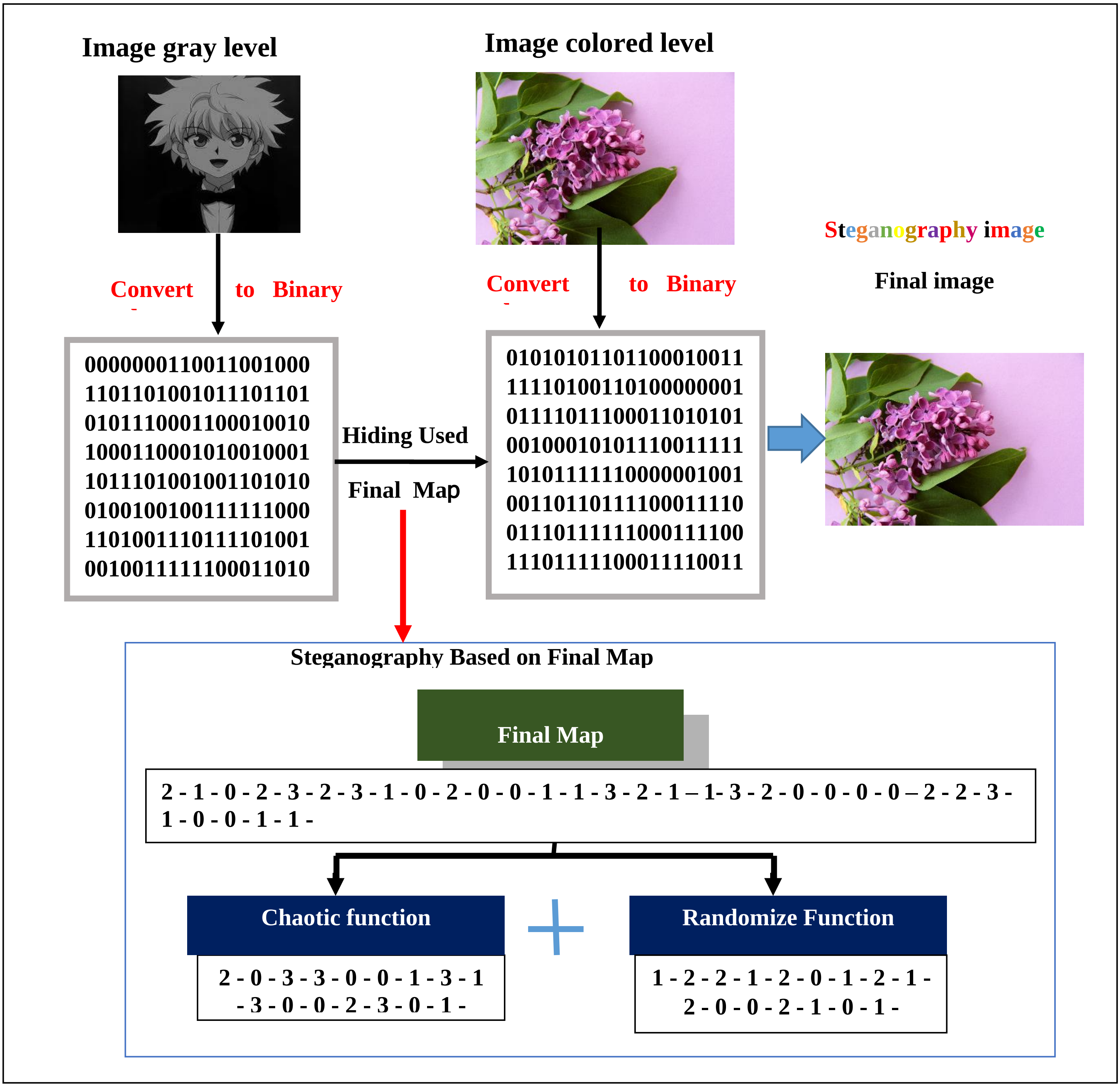

FIGURE 1:- Block Diagram of Steganography Gray Image Level in Color Image Level

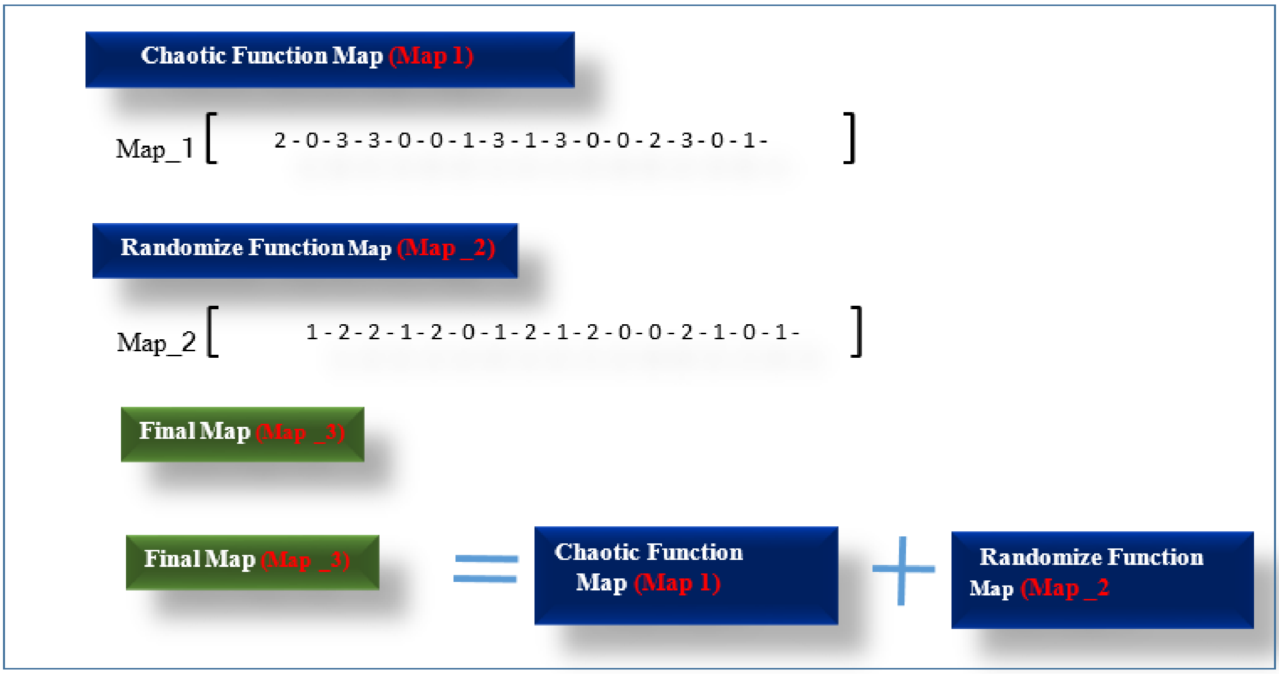

FIGURE 2. **Hiding (Final) Map**

2- Preparing the final map that consists two parts, as shown in Figure (3).

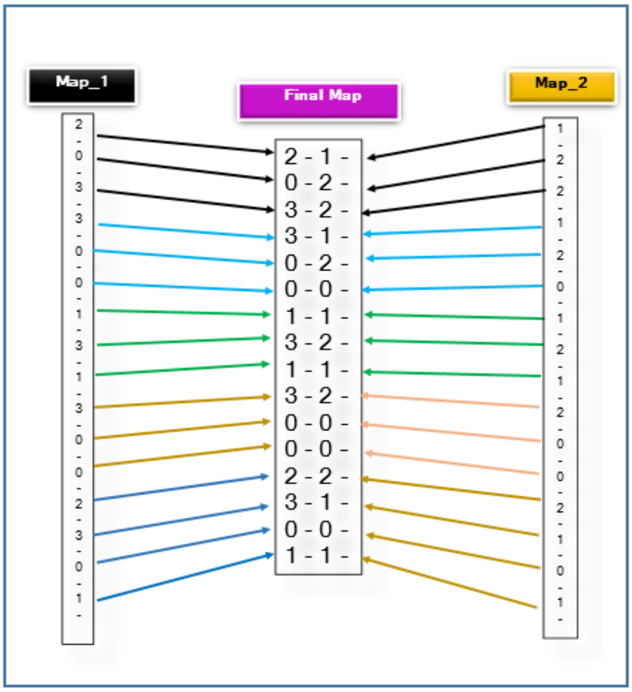

FIGURE 3. **Preparing the Final Map**

Final Map = [2 - 1 - 0 - 2 - 3 - 2 - 3 - 1 - 0 - 2 - 0 - 0 - 1 - 1 - 3 - 2 - 1 – 1- 3 - 2 - 0 - 0 - 0 - 0 – 2 - 2 - 3 - 1 - 0 - 0 - 1 - 1 -]

2. Preparing the gray-level image that converts the gray image to binary code, as shown in Figure (4).

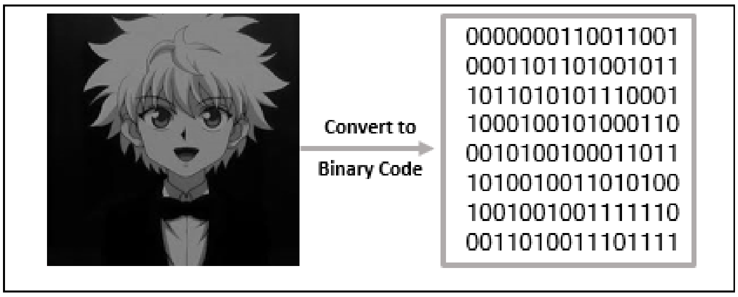

FIGURE 4. **Converting the first gray-level image to binary code**

3. Preparing the cover image (colored_ image) that is divided into three channels (Red, Green, and Blue), as shown in Figure (5).

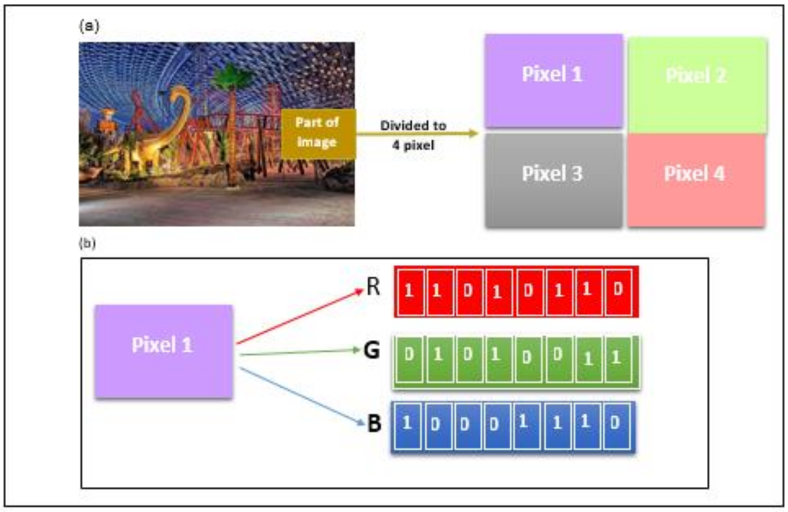

FIGURE 5. **Converting the cover image (colored_ image) into three channels. (a) Colored image divided into pixels, (b) pixel divided into bits.**

Figure (6) illustrates the hiding process when the bits are stored based on the final map by repeating the map until all the storage are as follows: When the number is 1 in the final map, we store one bit of the gray-level image in the color image, regardless of the channel stuck in the pixel. If the channel is red, then one bit will be saved in the red channel; if the channel is green, then one bit will be stored in the green channel; if the channel is blue, then one bit will be stored in the blue channel.

2- When the number is 2 in the map, two bits of the gray-level image are stored in the color image, regardless of the channel stuck in the pixel.

2- 3- When the number is 3 in the map, three bits of the gray-level image are stored in the color image, regardless the channel stuck in the pixel. When the number is zero in the final map, no bit is stored in the channel and the passage to the next channel.

We must consider the size of the cover image, which must be twice the size of the gray-level image, and its resolution must be high.

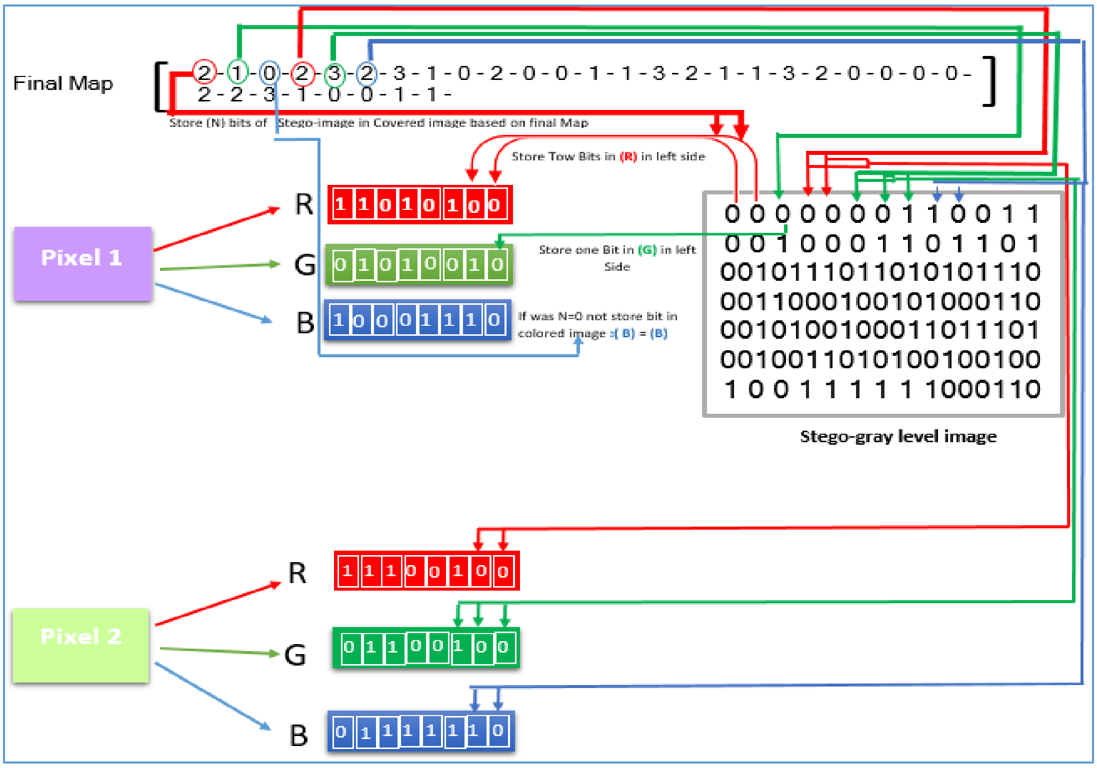

FIGURE 6. Gray image hidden into color image

The following algorithm explains the steps of the hiding process, see algorithm (1).

Input: img1 , img2 , Map.

Output : stego image

Processes:

Begin

Step 1: Set org-img = Null;

Step 2: For i=img1.hight D0

Step 3: For j=img1.width D0

Step 3.1: Get pixel (i,j);

Step 3.2: Org-img = org-img + pixel;

End for

End for

// Convert image from 2-D
//array to 1-D array

Step 4: For i=0 to img2.high D0

Step 5: For j=0 to img2 width D0

Step 5.1: Mix (img2.R , org-img [i] , Map [i]);

End for

End for

// Mix function Divide the number of //bits from the original image //according to the map and place it in //the second image in the red //pixel

Step 6: Final image = img2;

End

After the hiding process, the gray image is embedded in the color image, and the stego image over the network is sent from the sender to the recipient. The recipient extracts the gray image from the colored image through the extracting process. The proposed method must be available to the user to extract the gray image according to the proposed final map explained in Figure (3). The extracting process is explained in Figure (7).

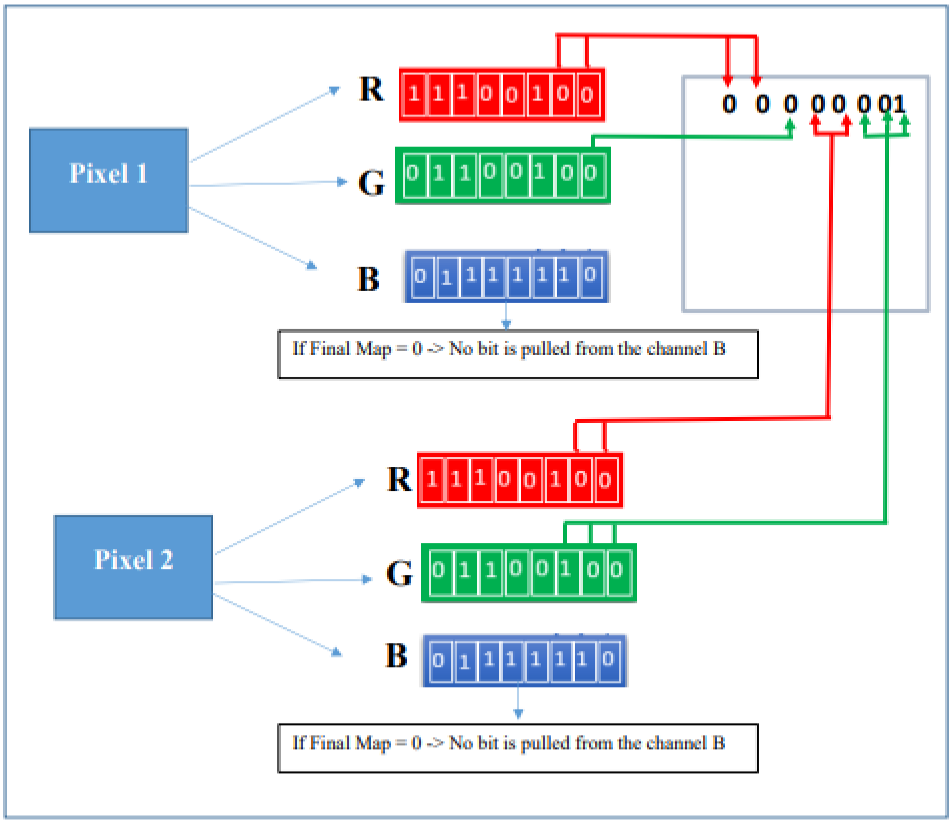

FIGURE 7. **Extraction process of stego image 1 according to the final map**

In the extracting process, the method of pulling the bits of the gray image from the colored image is repeated until it is a complete image according to the final map, as shown in Figure (8).

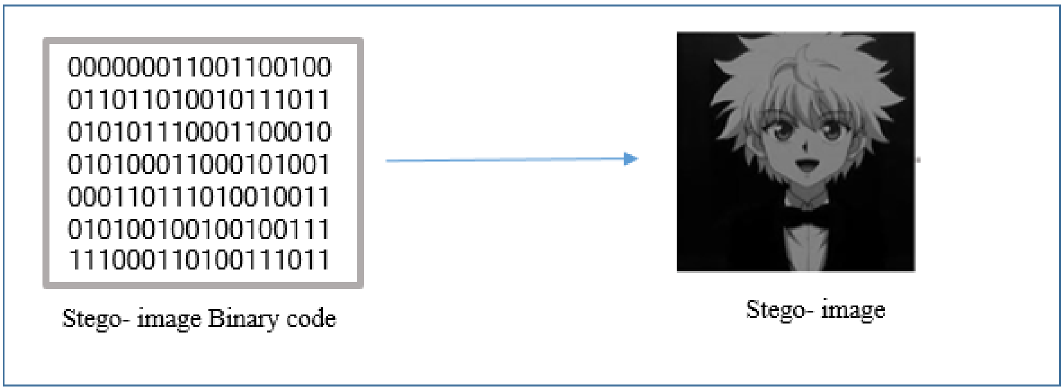

FIGURE 8: **Conversion of stego-image 1 to binary code**

Table 1 shows the properties of some gray-level images to be hidden and the color images that form the cover image.

Table 1. Properties of some gray-level image and colored–level image

NO.	Gray image	gray-level image size	Dimensions	Color image	Colored image size	Dimensions
1		8.2 KB	42 x 72		28.1 KB	362 x 253
2		90.5 KB	267 x 337		1.3 MB	5184 x 3456
3		19.1 KB	301 x 293		44.2 KB	608 x 431
4		57.1 KB	449 x 389		9.9 MB	6914 x 4463
5		21 KB	284 x 440		64.9 KB	841 x 614
6		23.3 KB	296 x 202		243.2 KB	900 x 599
7		25.9 KB	288 x 395		2.5 MB	3840 x 2560
8		13.1 KB	252 x 179		1.4 MB	3840 x 2560
9		94.2 KB	318 x 242		341 KB	1200 x 800
10		36.6 KB	409 x 290		315.8 KB	1600 x 1066

5. EXPERIMENTAL RESULT AND DISCUSSION

Each steganography method, whether a special steganography method for hiding text in an image or an image in an image or any other type of masking, must apply many evaluation criteria and to obtain successful results. The proposed method is used to hide a gray image inside a large colored cover image, where the characteristics of different gray images, such as type, accuracy, size, and selection, were obtained, and several images were selected with different properties that are large and with high accuracy. The proposed method consists of two stages; the hiding stage contains three steps, as shown in Figure (7).

2- After creating the final map, the gray-level used for hiding is selected.
2. The colored image that is used to embed the image's gray level is selcted.
3. Stego method is applied on the image and saved on the device.

The second stage is the extracting stage, which involves three steps.
1. After returning the final map, the stego image used to extract the gray-level is selected.
2. The gray-level image is extracted.
3. The gray-level image without any distortions or damage is extracted.

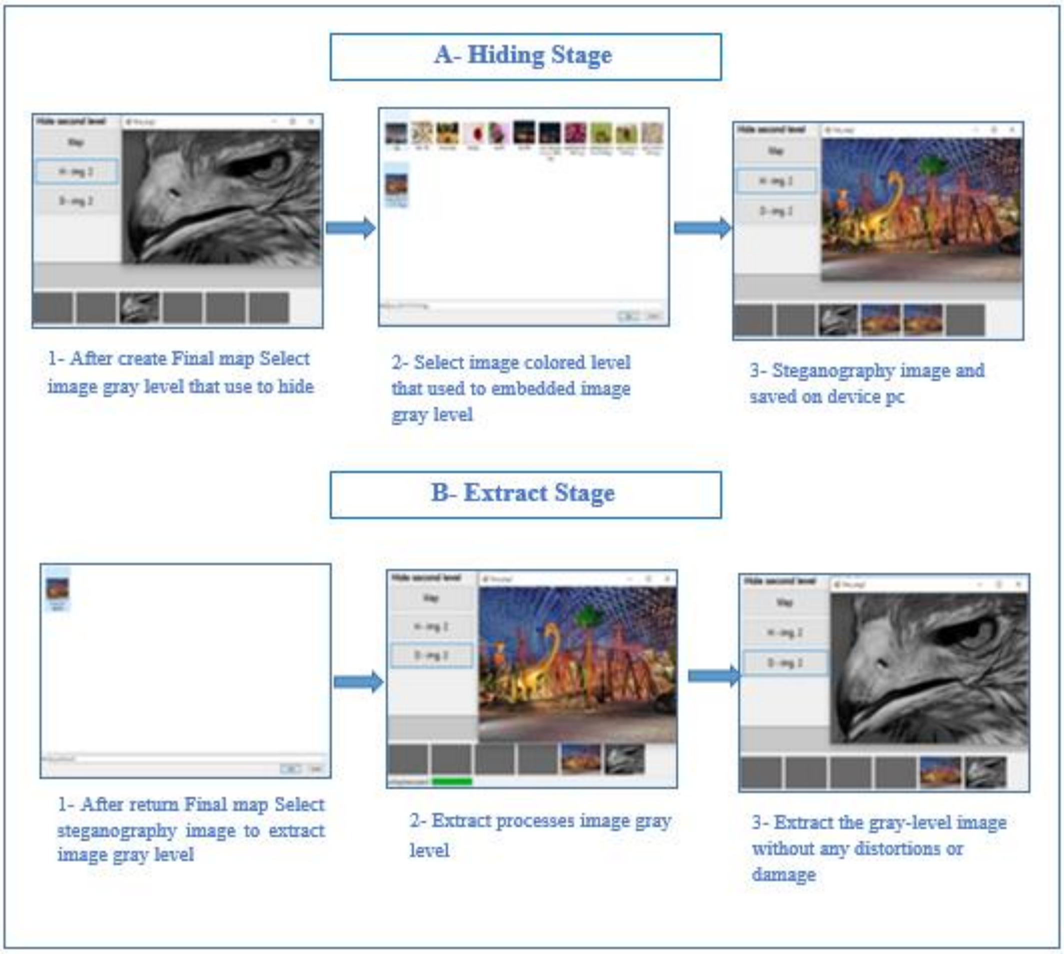

FIGURE 9. **Stage A- Hiding Stage B- Extraction Stage**

The hiding stage has been proven successful; the image was hidden without any distortions or errors according to the proposed map. After masking, the hidden image is sent to the recipient, which receives the hidden image. The image is clear and natural and used to extract the gray image without any errors or distortions. The recipient must own the entire software map to decompile the proposed hidden maps. The extraction stage included extracting the gray-level image from the color image. The image was extracted accurately and without any distortion, as shown in the implementation image. Several criteria were applied to test the efficiency of the proposed method, namely, MSE, SNR, and PSNR, and the results were good. Entropy and emended capacitance were also tested, achieving excellent results. The histogram was calculated for the hidden image, and the results of correlation and variance indicated excellent results, as shown in Table (2).

Table 2. Steganography coefficients: MSE, SNR, PSNR, EC, and entropy.

NO.	Gray image	Color image	MSE (bpp)	PSNR (bpp)	SNR (bpp)	Entropy (bit)	EC (bpp)
1			245.0050183	23.71247504	13.86163222	4.990729761	0.049476076
2			3962.948205	12.15061965	3.544547411	4.661142694	0.001207419
3			1389.64563	16.70176295	1.14212543	4.579923009	0.003419221
4			695.8653759	19.70555133	9.28271602	5.169705421	0.000120296
5			5088.780863	11.06466611	6.549719344	4.144281021	0.041897898
6			5263.623324	10.91795558	1.066308314	5.376563492	0.03181599
7			3592.963453	12.57627561	5.586926641	5.234295189	0.002005208
8			3313.969489	12.92731855	6.617512855	5.207284138	0.003072917
9			2544.742526	14.07436513	3.882916227	5.447184738	0.008933333
10			5305.744422	10.88334035	1.483882843	5.190162417	0.003227017

In the proposed method, MSE, PSNR, and SNR were measured on 10 images with different characteristics that were selected to hide the gray image within the color image, resulting in a hidden image. A certain number of bits will be stored. The characteristics of the image exhibit a great role, but we notice, from the table, that some of the applied results were good and some were relatively acceptable. The lower value of MSE indicates better image quality, according to the MSE equation.

$$MSE=(a*b)^{-1} \sum_{i=1}^{a} \sum_{j=1}^{b} [I[I(i,j)-S(i,j)]]^2 \; ……….(1)$$

The PSNR value is inversely proportional to that of MSE, as shown in the equation.

$$PSNR = 10 \log_{10} \left(MAX^2 / MSE \right) \;\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Figure 10 explains the relationship between MSE and PSNR, indicating an inverse proportion. When the percentage of MSE is low, the PSNR result is high; thus, the quality of the image is excellent.

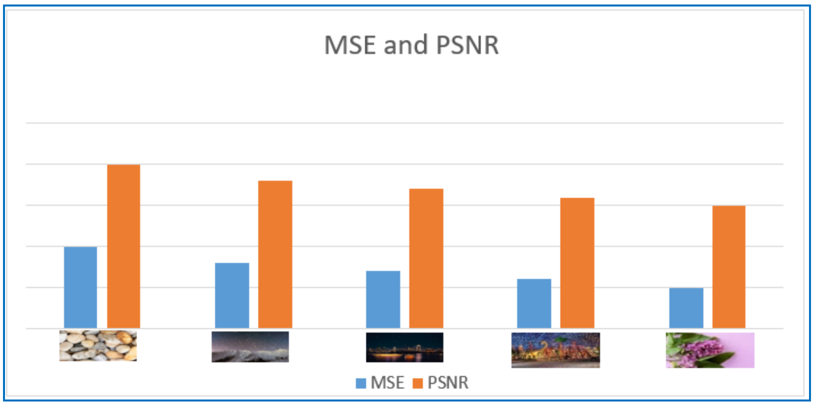

FIGURE 10. Relationship between MSE and PNSR Criteria

Table (2) shows that the entropy result is the level of randomness between the original image and the steganography image, calculated by the following equation:

$$H(S) = -\sum_{i=1}^{n} P(X) \log_b P(X_i) \;\ldots\ldots\ldots\ldots\ldots (3)$$

In this method, the image is hidden, and the results were excellent, as the randomness ranged between (5.447184738) and (4.144281021). The higher entropy value indicates more difficulty to predict and obtain the quality of the image.

EC is used in equation (4).

$$EC = N/(H*W) \; bPP \;\ldots\ldots\ldots\ldots\ldots (4)$$

The EC value ranges between the original image and stego image, and the highest value (0.049476076) and lowest value (0.000120296) were confirmed excellent, given the characteristics of the photos. Figure (11) explains the curve of the ratios of the entropy and EC of the 10 tested images.

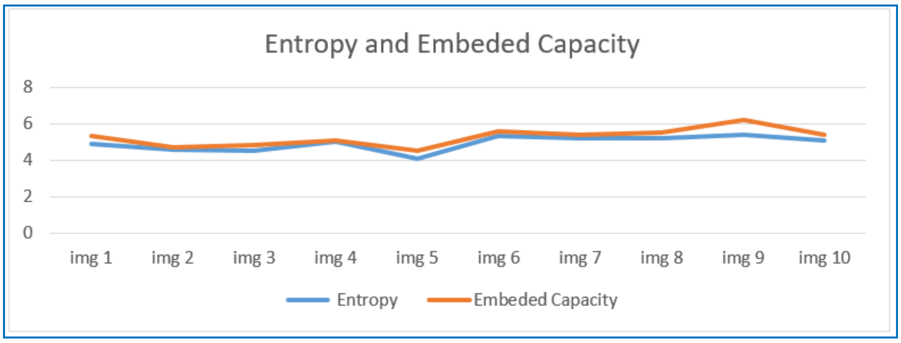

FIGURE 11. Curve of the entropy and EC ratios of the 10 tested images

Histogram

Figure (12) shows the histogram of the large colored image that hides the small image that was measured and plotted, and the results were excellent.

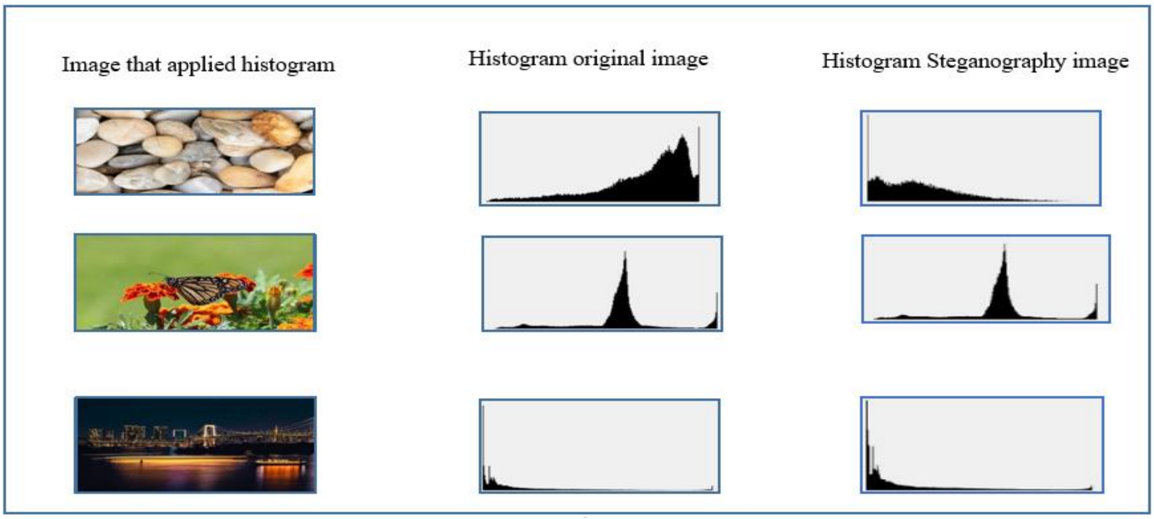

FIGURE 12. **Histogram of the original image and stego image**

The investigation variance and the correlation between the original image and the steganography image are calculated, as shown in Figure (13).

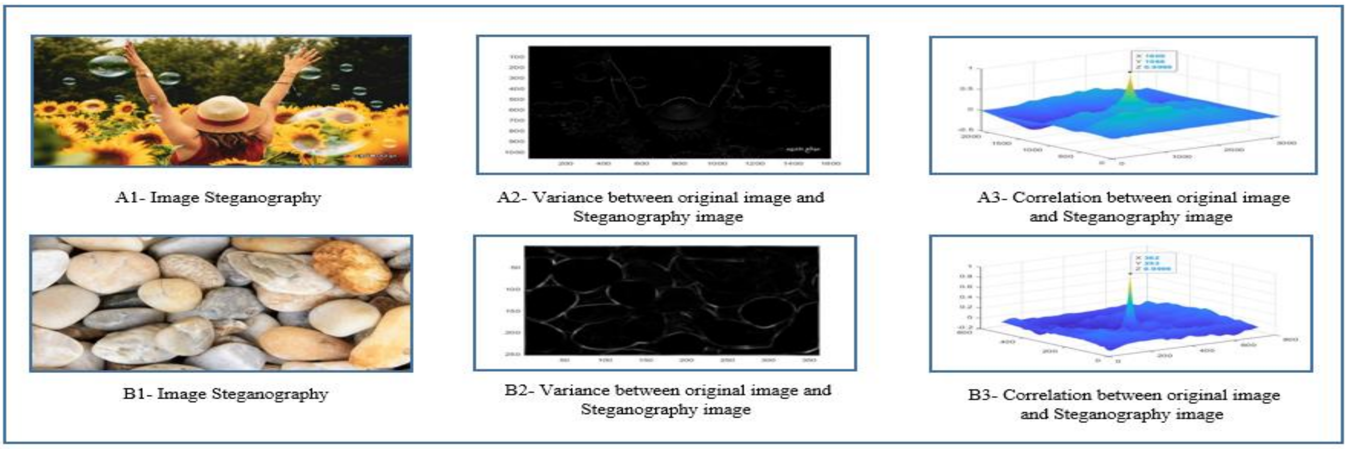

FIGURE 13. **Investigation and the correlation**

Table 3 shows that the correlation results were perfect and excellent, with high matching and lack of distinction between the original image and the stego image. When the result of the correlation is closer to 1, the result is perfect and excellent. The variance ratio is also excellent. The test criteria indicate the method is very successful in terms of concealment.

Table 3. Investigation Variance and Correlation

	A1- Image Steganography	B1- Image Steganography
Investigation Variance	516.2784	3.30571
Correlation	0.9999	0.9999

Table 4. Comparison evaluation criteria between the proposed method and other methods

Evaluation Criteria	MSE	PSNR	SNR	Entropy	EC	Variance	Correlation	Properties of each method
Propose method	1389.6	23.712	13.861	4.1442	0.00012	3.30571	0.9999	(5184 x 3456)
(EISU(DSTand SSH))	0.2501	54.15	-----------	----------	262144	-------	-------	(512x512)
(SBSTUSSMFHSVCI)	0.449	56.456	50.118	---------	195416	--------	-----------	(512x512)
(IAAOISU LSB and DWT)	2.4179	44.2964					0.9944	---------

Table 4 shows a comparison between the proposed method and several methods used in masking. Each method adopted several evaluation criteria to test its quality. The proposed method has been proven to be characterized by strong protection and speed of performance compared with other methods.

6. CONCLUSION

This research proposed a steganography technique for highly accurate concealment of gray-level images of various sizes and resolutions within huge colorful images of various sizes. The approach has strong protection power because the basis for generating values is random and the suggested masking maps are formed from chaotic and randomized functions. The values are generated from the chaotic and randomized function in the range of 0 and 3. This condition enables the approach to be used on the Internet, online, and live broadcasts because it protects data and transmission as long as the application of the results of the standard is excellent, the original image matches the hidden image up to 0.999, and it cannot be observed with the naked eye. The proposed approach can successful hide information on the Internet.

ACKNOWLEDGEMENTS

The authors would like to thank Al-Nahrain University, the University of Technology, University of Al-Ameed Karbala, and the Iraqi Ministry of Education for their support in the conduct of the work published in this paper.

CONFLICT OF INTEREST:

Author declear no conflict of interest

6. REFERENCES

[1] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, And Ahmed Bouridane, "Image Steganography: A Review Of The Recent Advances", Ieee Access, Received December 27, 2020, Accepted January 7, 2021, Date Of Publication January 25, 2021, Date Of Current Version February 10, 2021. Doi 10.1109/Access.2021.3053998.

[2] Dalal N. Hmood, Khamael A. Khudhia, Mohammed S. Altaei, "A Proposed Steganographic Method for Embedded Image In Audio File," International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (2): 2012.

[3] Shivam Ilasariya, MCT's Rajiv Gandhi Institute of Technology, Mumbai, India, Parth Patel, Vatsal Patel, and Swapnil Gharat, "Image Steganography Using Blowfish Algorithm and Transmission via Apache Kafka", IEEE, 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Date Added to IEEE Xplore: 25 February 2022, Tirunelveli, India, DOI: 10.1109/ICSSIT53264.2022.9716292.

[4] Juhi Singh and Mukesh Singla, "A Novel Method of high-Capacity Steganography Technique in Double Precision Images", IEEE,2021 International Conference on Computational Performance Evaluation (ComPE),12 April 2022, Shillong, India, DOI: 10.1109/ComPE53109.2021.9751905.

[5] Mehdi Sharifzadeh, Mohammed Aloraini, and Dan Schonfeld, "Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography". 2019 IEEE ACCESS. DOI 10.1109/TIFS.2019.2929441.

[6] Baqer A Hakim, Ahmed Dheyaa Radhi, and Fuqdan AL-Ibraheemi," An innovative and robust technique for human identification and authentication based on a secure clinical signals transmission", Int. J. Nonlinear Anal. Appl. 13 (2022) No. 1, 603-613 ISSN: 2008-6822 (electronic) ,doi.org/10.22075/ijnaa.2022.5542.

[7] S. Sravani and R. Ranjith, "Image Steganography for Confidential Data Communication", IEEE, 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT),03 November 2021, Kharagpur, India, DOI: 10.1109/ICCCNT51525.2021.9579814.

[8] Azhaar Akram Abdallah and Alaa Kadhim Farhan, ”A Proposed Image Encryption Algorithm Based on Multi ChaoticSystem, ” Iraqi Journal of Science, 2022, Vol. 63, No. 1, pp: 324-337DOI: 10.24996/ijs.2022.63.1.31.

[9] Arnold Gabriel Benedict, "Improved File Security System Using Multiple Image Steganography" Publisher: IEEE, Date Added to IEEE Xplore: 29 August 2019, INSPEC Accession Number: 18958412, DOI: 10.1109/IconDSC.2019.8816946.

[10] Arshiya S. Ansari, Mohammad S. Mohammadi, and Mohammad Tanvir Parvez, "A Multiple-Format Steganography Algorithm for Color Images" Publisher: IEEE, Date of Publication: 29 April 2020, DOI: 10.1109/ACCESS.2020.2991130.

[11] Yasir Ahmed Hamza, Nada Elya Tewfiq and Mohammed Qasim Ahmed, "An Enhanced Approach of Image Steganographic Using Discrete Shearlet Transform and Secret Sharing", Baghdad Science Journal P-ISSN: 2078-8665 Published Online First: July 2021 2022, 19(1): 197-207 E-ISSN: 2411-798, DOI: http://dx.doi.org/10.21123/bsj.2022.19.1.0197.

[12] Raheem Abdul Sahib Ogla "Symmetric- Based Steganography Technique Using Spiral-Searching Method for HSV Color Images", Baghdad Science Journal Vol.16(4) 2019, DOI: http://dx.doi.org/10.21123/bsj.2019.16.4.0948.

[13] Srushti S Yadahalli, Shambhavi Rege, and Dr. Reena Sonkusare, "Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques", Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020), IEEE Conference Record # 48766; IEEE Xplore ISBN: 978-1-7281-5371-1.

[14] Jiaohua Qin, Yuanjing uo, Xuyu Xiag, Yun Tan,andd Huajun Huang, "overless Image Steganography: A Survey", IEEE Access,25 November 2019, DOI 1 0.1109/ACCESS.2019.2955452.

[15] Muhammad Aminul Islam, Md. Al-Amin Khan Riad, and Tanmoy Sarkar Pias, "Enhancing Security of Image Steganography Using Visual Cryptography", 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), IEEE,05-07 January 2021, DOI: 10.1109/ICREST51555.2021.9331225.

[16] S. Sravani and R. Raniith, "Ima Steganography for Confidential Data Communication",202 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE,03 November 2021, DOI: 10.1109/ICCCNT51525.2021.9579814.

[17] Rupali Bhardwaj and Vaishali Sharmab, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution," 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India.

[18] Umme Sara1, Morium Akter, and Mohammad Shorif Uddin, "Image Quality Assessment through FSIM, SSIM, MSE, and PSNR—A Comparative Study", Journal of Computer and Communications Vol.07 No.03(2019), Article ID:90911,11 pages 10.4236/jcc.2019.73002.

[19] De Rosal Igantius Moses Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography", Multimedia Tools and Applications, Published: 03 November 2020.

[20] Tom Carter, "An introduction to information theory and entropy", Complex Systems Summer School, September 3, 2014.

[21] A. K. Farhan, N. M. G. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder," Entropy, vol. 21, no. 10, p. 958, 2019, DOI: 10.3390/e21100958.

[22] Azhaar Akram Abdallah and Alaa Kadhim Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System", Iraqi Journal of Science, 2022, Vol. 63, No. 1, pp: 324-337, DOI: 10.24996/ijs.2022.63.1.31.

[23]Mohammed Mahdi Hashim and Mohd Shafry Mohd Rahim,” Image Steganography Based On Odd/Even Pixels Distribution Scheme and Two Parameters Random Function”. Journal of Theoretical and Applied Information Technology, 30th November 2017. Vol.95. No 22.

[24] Hiba Abdel-Nabi and Ali Al-Haj, "Frequency domain-bas data hiding for encrypted medical images", Intelligent Data Security Solutions for e-Health Applications, 2020,https://doi.org/10.1016/B978-0-12-819511-6.00002-9.

[25] Serdar Solak, "High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms", Publisher: IEEE, 10 September 2020, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2020.3023197.

[26]Ammar Mohammed Ali And Alaa Kadhim Farhan ”Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document, ” in IEEE Access, vol. 8, pp. 27448-27458, 2020, DOI: 10.1109/ACCESS.2020.2971779.

[27] Upendra KumarAcharya and SandeepKumar, "Genetic algorithm based adaptive histogram equalization (GAAHE) technique for medical image enhancement", Optik, Volume 230, March 2021, 166273,doi.org/10.1016/j.ijleo.2021.166273.

[28]Kaiser A. Reshak, Ban N. Dhannoon, and Zainab N. Sultani,” Explicit feedback-based movie recommendation system: A survey," AIP Conference Proceedings 2290, 040009 (2020), doi.org/10.1063/5.0027433.

[29] Ali H. Alwan and Ali. H. Kashmar , "FCNN Model for Diagnosis and Analysis of Symmetric KeyCryptosystem",November 2022,Iraqi Journal for Computer Science and Mathematics,DOI: https://doi.org/10.52866/ijcsm.2023.01.01.006.
[30] Shams N. Abdul-wahab, Mostafa Abdulghafoor Mohammed, & Omar A. Hammood. (2021). Theoretical Background of steganography. Mesopotamian Journal of CyberSecurity, 2021, 22–32. https://doi.org/10.58496/MJCS/2021/005