

A crypto-steganography scheme for IoT applications based on bit interchange and crypto-system

Suray Alsamarae¹, Ali Salem Ali²

¹Department of Computer Engineering, Faculty of Engineering, Al-Iraqia University, Baghdad, Iraq

²Department of Network Engineering, Faculty of Engineering, Al-Iraqia University, Baghdad, Iraq

Article Info

Article history:

Received Jun 2, 2022

Revised Aug 1, 2022

Accepted Sep 6, 2022

Keywords:

Cryptography

Hénon map

Hybrid cryptography

Internet of things

PSNR

Steganography

ABSTRACT

Image steganography and cryptography have been used widely due to the dramatic evolution of the internet of things (IoT) and the simplicity of capturing and transferring digital images. Pressing challenges in the context of a steganography system include security, imperceptibility, and capacity issues. In the existing schemes, fixing one issue has been indicated to affect the other and vice versa. Based on the above challenges, a new scheme has been proposed for the Crypt-steganography scheme. The proposed scheme consists of three main contributions. The first contribution is hybrid additive cryptography (HAC), which is related to encrypting secret messages before the embedding process to ensure security. The HAC depends on ElGamal elliptic curve cryptosystem (ECC) with cubic Bézier curve to achieve text confidentiality. The second contribution is a bit interchange method (BIGM), which is related to the embedding process and solves the image's imperceptibility. The third contribution is a new image partitioning method (IPM). The IPM contribution increases the randomization of selecting the embedding pixels. The IPM proposes a random pixel selection based on three iterations of the Hénon Map function used with IPM. Different parameters are used to evaluate the proposed scheme. Based on the findings, the proposed scheme gives evidence to overcome existing challenges.

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



Corresponding Author:

Suray Alsamarae

Department of Computer Engineering, College of Engineering, Al-Iraqia University

Baghdad, Iraq

Email: suraysaady80@gmail.com

1. INTRODUCTION

The internet of things (IoT) applications have recently grown fast because of data communication and user involvement in the continuously interconnected collaborative working devices [1]. The rapid development of IoT applications makes communication and transmission security issues more attractive. Therefore, it is necessary to implement effective security and confidentiality technology to transmit IoT [2]. Such security can be provided using security features such as information security techniques (steganography and encryption) with IoT systems [3]. Combining both techniques will ensure the secret data in the system [4], [5].

Based on the steganography scheme, the secret or private data can be hidden within different media, including the color or grayscale image. Generally, the steganography schemes are attained in the spatial and transform domains [3]. Two important concepts are involved in the steganography technique called stego and cover image [6], [7]. A stego image hosts the secret data with a certain quality, whereas the cover image is pure without containing the secret information. The steganography technique has been applied in the field of medical diagnoses [8], military and defense [9], [10], multimedia biometric data security [11], and cloud

computing [12]. On the next page, Figure 1 exposes the fundamental issues and difficulties concerning the performance of the existing steganography schemes related to the payload capacity, imperceptibility, and security [12], [13].

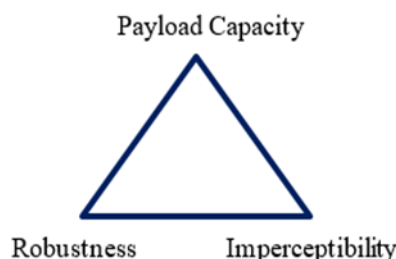


Figure 1. The fundamental issues related to the existing steganography systems

The second technique used to ensure the security of secret data is cryptography [14], [15]. Cryptography is one of the major important techniques and is widely used in our life, especially in information security [14], [16]. Cryptography is one of the mathematical methods that ensure the security of information communications. Cryptography contains algorithms and protocols used to improve security [17]. Therefore, cryptography applications are important to ensure secure communications between the sender and the recipient [16], [18].

The cryptography of the text increases the security of any steganography system or the security of the text itself [19]. The text represented as the media needs to be hidden or look for secure hosting media in the steganography [20]. Therefore, text encryption in steganography refers to the security of the text before embedding, protecting it from unauthorized detection or extraction by intruders or attackers. Therefore, this is the primary purpose of text encryption within the image steganography, thereby improving system security. As seen in Figure 1, the payload capacity of a steganography system is defined as the maximum size of the secret message that can be hidden into the image media [9], [18]. The imperceptibility of a steganography system signifies the carrier media quality that can be used for hiding the secret message following the algorithm embedment [21]. The security of a steganography system [11] Refers to its robustness against various statistical attacks such as the chi-square, human visual system (HVS), and histogram analysis (HA). In this perception, the present research intends to resolve various issues related to the existing steganography system and improve its robustness in terms of high security, high payload capacity, and imperceptibility.

It is essential to mention that several studies in image steganography and steganalysis focused on improving imperceptibility (embedding method). Based on this fact, the performance of the developed image steganography system was assessed in terms of the measures, including the peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) [12], [16], [22]. One of the prerequisites of any data embedment procedure is imperceptibility which hides the bits into the cover image so that it remains invisible to the eye or statistics [23]. The embedding procedure is inextricably linked to the hidden data payload volume and the steganography system's security. As a result, any reduction in embedded data to the cover image can result in minimal changes to the bits in the original image. This keeps the stego image looking very identical to the original [9], [11]. The PSNR is used to assess the image quality of a steganography method [24]. After embedding, the PSNR value is computed by comparing the original and stego pictures. If the PSNR value is greater than or equal to 30 dB, the data embedding process is deemed undetectable to the HVS [25]. If the value of SSIM is equal to 1, two images are considered similar in the case of SSIM. The photographs are considered noisy if they are not otherwise [9]. An enhancement of the PVD method called adaptive directional pixel value differencing (ADPVD) is proposed to hide secret information in RGB channels of images [21]. The enhancement algorithm used the directions within vertical, horizontal, and diagonal for each RGB channel to hide the information. Different evaluation criteria have been used to evaluate methods such as PSNR, mean square error (MSE), and HA.

Over the years, image steganography and steganalysis developers have focused on improving the PSNR value while evaluating the image steganography system [12], [22]. However, although various proposed solutions enhanced the PSNR, they could not keep the payload capacity at an acceptable level [23]. As a result, a correct embedding approach is still necessary to preserve the trade-off between stego image security and imperceptibility while also increasing the steganography system's durability. Few research has

attempted to improve PSNR values by lowering the MSE for the embedding procedure [26]. However, this comes at the expense of the stego image's imperceptibility and, as a result, the steganography system's robustness. As a result, there is a need to address this problem by developing a robust steganography approach that ensures the stego image's security, capacity, and imperceptibility.

An in-depth literature survey indicated that the studies on the trade-off between the steganography performance criteria are unbalanced [27]. Some researchers used a low payload capacity to increase PSNR and SSIM values. It has been observed that the use of the high payload capacity can affect the image quality, reducing the PSNR plus SSIM and vice versa. The PSNR is considered as low if it is less than equal to 45 dB. Conversely, the PSNR is acceptable if it is less than equal to 59 dB. Otherwise, PSNR is regarded as high [28]. The principle of image steganography methods is present in [29]. In this research, the crucial techniques based on image steganography are introduced in detail. Also, the authors present the primary evaluation criteria used to evaluate steganography. A quantum chaos map and mixing a Zaslavsky with the 3D Hanon map function are used to improve image steganography [30]. The proposed method depends on three phases, each with an algorithm. The proposed method consisted of steganography and encrypted data. The data confidentiality is ensured by combining cryptography and steganography to avoid potential spies and hackers [31]. The hidden message is embedded based on non-uniform systems by generating a random index vector (RIV) and the least significant bit (LSB) image pixels.

In an image steganography system, "security" is the vital characteristic that needs proper performance evaluation. Security refers to the "un-detectability" or "un-noticeability" of the steganography system [13]. Thus, any steganography method is considered to be secured if the secret data remains undetectable by the statistical analysis or removal after being detected by the attacker. Generally, the steganography methods may suffer from various types of steganalysis detection attacks wherein the intruders try to detect the existence or even to retrieve the secret data embedded in the stego image [13], [24]. To address this issue, a steganography system based on the Pixel Difference-based text encryption and random pixel section was proposed to protect the stego message during transmission [25]. Similarly, a bit-plane histogram-shifting-based embedding was proposed by [26]. However, these methods can be statistically analyzed, which facilitates the decoding of the secret text [24]. Consequently, existing steganography systems still suffer from several types of attacks and need further enhancement [13].

Different contributions have been mentioned in the proposed scheme to improve the image steganography system (ISS). The main contribution of this study is described: i) hybrid additive cryptography (HAC) is the first contribution. It describes the encryption method used to encrypt secret information before embedding. The proposed HAC is used to ensure the security of secret data; ii) the image partitioning method (IPM) is the second contribution of this study. This method used three iterations of the Hénon Map function to produce the high randomization of blocks and pixels in the cover image before embedding; and iii) the bit interchange method (BIGM) is the third contribution of the proposed scheme. The proposed BIGM makes the PSNR high as required, which reflects more space to embed the secret message and achieve high imperceptibility.

The paper's structure comprises four sections, including the introduction and literature review of the relevant studies of image steganography. The central aspect of the methodology of the proposed scheme is described in section 2. In the presented scheme, different methods and algorithms are proposed. These methods and algorithms are described in detail within section 3. The performance evaluation outcome of the developed image steganography scheme against different parameters and achieved in section 4. Finally, the conclusion of the paper with contributions is introduced in section 5.

2. METHOD

Different challenges in the context of a steganography system include security, imperceptibility, and capacity issues. Most researchers have highlighted the trade-offs between these issues. While, the trade-offs between payload and security have been neglected by researchers, as fixing one issue has been indicated to affect the other, and vice versa. Towards overcoming the aforementioned issues, a new scheme has been proposed for image steganography.

3. PROPOSED SCHEME

The proposed scheme is divided into three main contributions. The first contribution is HAC, which is related to the encryption of secret messages before the embedding process. The second contribution is the IPM, and the last contribution is a BIGM, which is related to the embedding process. The next subsections describe the contributions in detail. Figure 2 is mentioned the main steps of the proposed scheme.

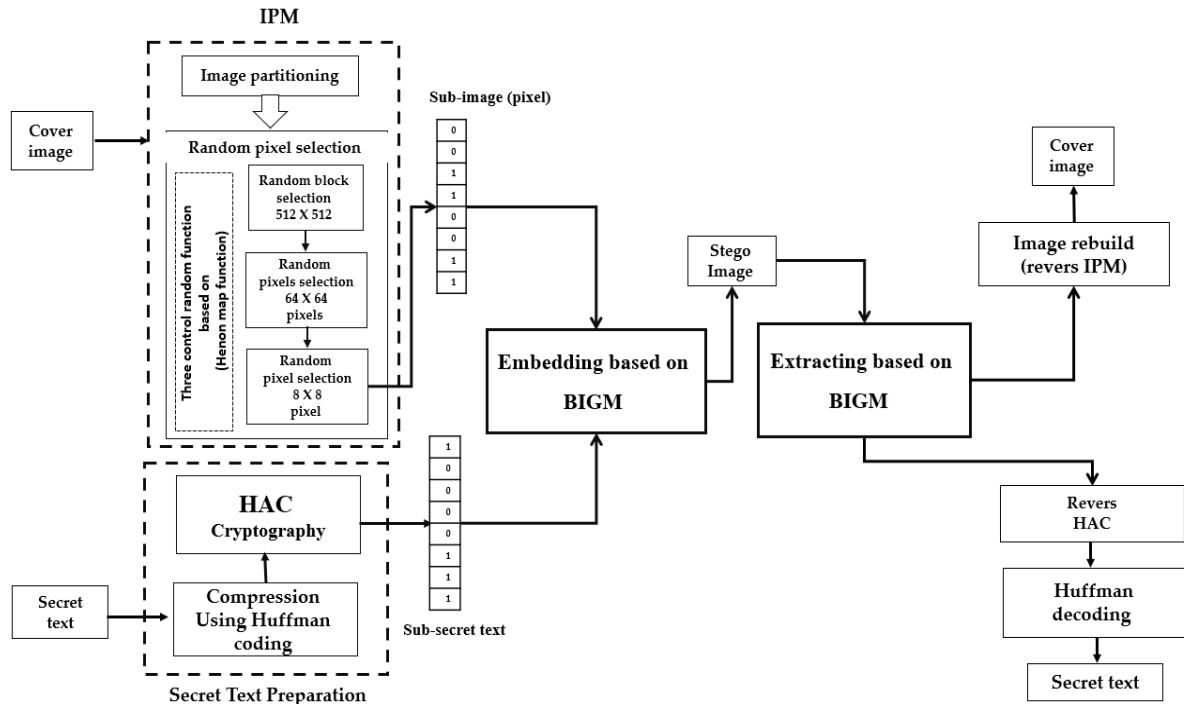


Figure 2. The structure of proposed scheme

3.1. Hybrid additive cryptography

This section discusses HAC based on ElGamal elliptic curve cryptosystem (ECC) with Cubic Bézier Curve to achieve text confidentiality. The confidentiality and security of the Text before embedding are necessary and needful. The proposed cryptography is used to enhance security level features via the novel hybrid cryptography approach that combines security concepts in Bézier curves techniques and the Elliptic curve EC points to produce a hybrid-key point (cypher key). The proposed HAC is shown in Figure 3.

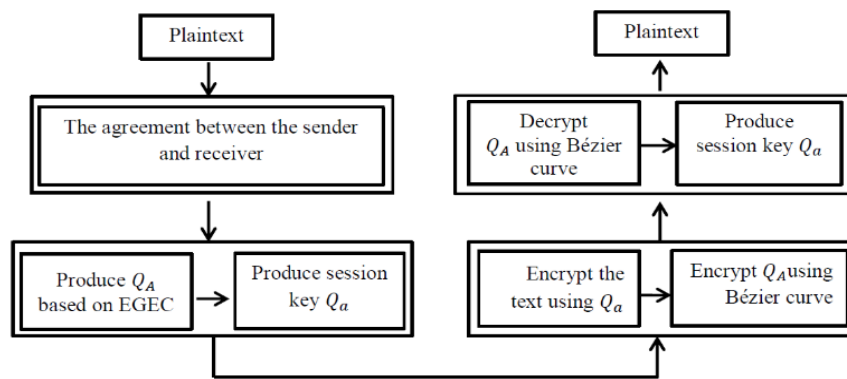


Figure 3. Illustration diagram of the proposed methods

3.1.1. Agreement between sender and receiver

The framework agreement is done between the sender and the receiver. The authentication is used to emphasize the receiver part, and the data was sent from a recognized sender part and did not modify in between by an unauthorized person. In this stage, a new method is proposed to generate a session key from the master key using Bézier curves equations and fitting the curve on the master key. The procedure is achieved by monitoring points between the receiver and sender sides. Algorithm 1 describes the agreement procedure:

Algorithm 1

1. The Elliptic-curve (EC) produce through finite field (FF) $E(Ep)$.
2. Base point $B \in E(Ep)$.
In a secret way, control the secret point for Bézier:
 $BP_1 = (x_1, y_1), BP_2 = (x_2, y_2), BP_3 = (x_3, y_3)$ and
 $t = (t_1, t_2) \in [0,1]$ and the compute t by: $= (t_1, t_2) \in [0,1] \text{ Mod } p$.
3. Secretly on a base point P that related E , ($P \in E(Ep)$).

3.1.2. Key produce phase

This phase describes the creation of the cryptography keys, the Master Key (Q_A) and Session-Key (Q_a). The Q_A is the major key that used to produce the Q_a , while the Q_a is the key which uses to encrypt a text.

a. Master key production (Q_A)

The major process for master key (Q_A) within this work is to produce the Q_a . This work introduces a new algorithm to produce the Q_A by utilizing the ElGamal Elliptic Curve algorithm (EEC). The result is a point that represents the master key between sender and receiver.

b. Session key production (Q_a)

In this phase, a new algorithm to produce the Q_a using the Q_A is introduced. The master key Q_A will convert into binary bits (Bin) then convert it to decimal (De). Finally, multiply De with the Q_A and the result point is represented as Q_a . The key generation process is explained in detail within algorithm 2:

Algorithm 2

1. Receiver chosen random integer d as secret point.
2. Compute the Public-Key Q_B using the d integer:
 $dB = Q_B$ and keep d as a secret integer.
3. Chosen random integer e by sender as a secret pint.
4. Compute the master key Q_A by using e and Q_B
 $eQ_B = Q_A = (x_4, y_4)$.
5. Convert the Q_A to Bin and to De, compute $n = \text{De Mod } p$.
6. Compute the session key Q_a by using n and Q_A :
 $nQ_A = Q_a$.

3.1.3. Encryption stage

Securing secret information is the most important issue in text encryption. In the proposed method, the encryption stage consists of two parts:

a. Encrypt the secret text process

After building the master key from the recipient's public key in this algorithm, a new technique was added in this part by converting the Q_A into binary bits and then into decimal to generate the session key to increase the security and robustness of the algorithm. This technique is used as the authentication between the sender and receiver. This change will make the encryption process more secure than the existing algorithms process.

b. Encrypt the master key process

The Q_A must transfer with the ciphertext to a receiver part. Therefore, the algorithm 3 must be encrypt the Q_A before sending it. The cubic Bézier curve and agreed on control points (Bézier points) between the sender and receiver are used for encrypting the cipher key with the ciphertext. The flowchart of the proposed encryption idea is shown in Figure 4. Algorithm 3 is explained in detail the proposed encryption process:

Algorithm 3

1. Select the secret text.
2. Convert all the characters of text to ASCII value.
3. Use point P to compute $m_i P = M, i = 1, 2, 3, \dots$
4. Encrypt the message point M using Q_a by: $C = M + Q_a$, C is ciphertext.
5. Encrypt the $Q_A = (x_4, y_4)$ using secret control points of Bézier:
 $BP_1 = (x_1, y_1), BP_2 = (x_2, y_2), BP_3 = (x_3, y_3)$ and
 $t = (t_1, t_2) \in [0,1]$ and the compute t by: $= (t_1, t_2) \in [0,1] \text{ Mod } p$, via:
 $K_1 = x_1(1-t_1)^3 + 3x_2(1-t_1)^2t_1 + 3x_3(1-t_1)t_1^2 + t_4t_1^3 \text{ Mod } p$
 $K_2 = y_1(1-t_2)^3 + 3y_2(1-t_2)^2t_2 + 3y_3(1-t_2)t_2^2 + y_4t_2^3 \text{ Mod } p$
 $K = (K_1, K_2)$ is cipher key.
6. Send $\{C, K\}$ to receiver side.
7. End

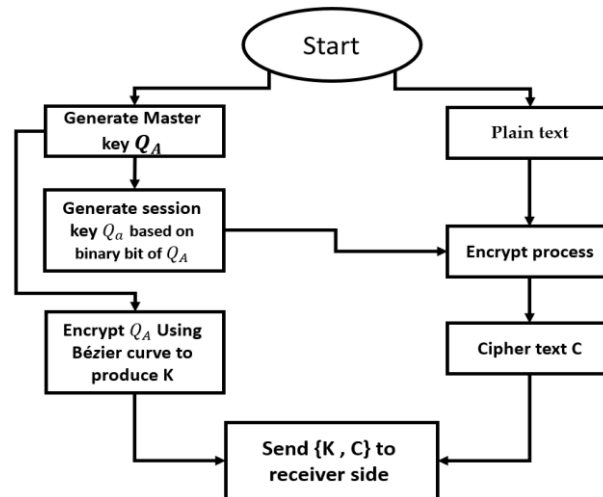


Figure 4. Encryption process with proposed scheme

3.1.4. Decryption process

The aim of the decryption stage is to retrieve the original text during the reverse processes of the encryption algorithm (algorithm 3). On the receiver side, the ciphertext and cipher key are used in the decryption process (algorithm 4). Firstly, algorithm 4 is used the secret control points (Bézier points). The Bézier points are used to decrypt the cipher key and then find the session key. Secondly, the session key is used to decrypt the ciphertext. The proposed decryption method is explained in detail in algorithm 4:

Algorithm 4

- 1- Receive $\{C, K\}$ from sender side.
- 2- Find the Q_A via decrypt $K = (K_1, K_2)$ using
 $BP_1 = (x_1, y_1), BP_2 = (x_2, y_2), BP_3 = (x_3, y_3)$ and $t = (t_1, t_2) \in [0,1] \text{ Mod } p$
 $x_4 = [k_1 - x_1(1-t_1)^3 + 3x_2(1-t_1)^2t_1 + 3x_3(1-t_1)t_1^2]. (t_1^3)^{-1} \text{ Mod } p$
 $y_4 = [k_2 - y_2(1-t_2)^3 + 3y_2(1-t_2)^2t_2 + 3y_3(1-t_2)t_2^2]. (t_2^3)^{-1} \text{ Mod } p$
 $Q_A = (x_4, y_4)$ the master key.
- 3- Convert the Q_A to Bin and then to De, finally, compute $n = De \text{ Mod } p$
- 4- Compute the Q_a by using n and Q_A :
 $nQ_A = Q_a$.
- 5- Decrypt the ciphertext C using the Q_a via:
 $M = C - Q_a$.
- 6- Using secret point P to solve DLP for $M = m_i P$.
- 7- Convert the value of m_i into ASCII characters
- 8- Obtained the text
- 9- End

Proposed encryption example

1. The Agreement Process Between Alice and Bob

- Publicly: Alice and Bob agree on an elliptic curve E over F_{967} ($E(F_{967})$) and $B = (887, 292) \in E$, where $\#E = 919$
 $E: y^2 = x^3 + 78x + 96 \text{ mod } 967$, where $a = 78, b = 96$ and $p = 967$ satisfy the condition $4a^3 + 27b^2 \text{ mod } p : [4(78^3) + 27(96^2)] \text{ mod } 967 = 300 \neq 0$.
- Secretly: Alice and Bob agree on Bezier point $BP_1 = (215, 115)$,
 $BP_2 = (160, 140), BP_3 = (100, 75)$ and $t = (0.86, 0.75) \in [0,1] \text{ mod } 967$, and they compute:
 $t = (0.86, 0.75) \in [0,1] \text{ mod } 967$
 $t = (86 * 100^{-1}, 75 * 100^{-1}) \text{ mod } 967$
 $t = (86 * 938, 75 * 938) \text{ mod } 967$
 $t = (407, 726)$.
- Secretly: Alice and Bob agree on another base point on E , let $P = (678, 801)$.

2. Key Generation Process

- Bob chooses a random integer $d = 612$ as a private key, and then computes the public key:
 $Q_B = dB = 612(887, 292) = (937, 739)$, and keep d secret
- Alice chooses a random integer $e = 521$ as a secret key, and uses Bob's public key to compute the master key:
 $Q_A = eQ_B = 521(937, 739) = (330, 235)$.
- Alice converts the master key $Q_A = (330, 235)$ to binary bits:
 $B_A = 10100101011101011$, and then converts it to decimal
 $Dec. = 84715$, and computes $n = Dec. \text{ mod } p$
 $n = 84715 \text{ mod } 967 = 856$
- Calculate the session key Q_a by: $Q_a = nQ_A = 586(330, 235)$
 $Q_a = (208, 534)$.

3. Encryption process (Alice)

- Chooses a text: "*elgamal*".
- Converts each characters into ASCII values:
 $e: m_1 = 101, l: m_2 = 108, g: m_3 = 103, a: m_4 = 97,$
 $m: m_5 = 109, a: m_6 = 97, l: m_7 = 108.$
- Uses the secret point $P = (678,801)$ to compute
 $m_1P = 101(678,801) = (838,836) = M.$
- Encrypts the master M and based on session key Q_a by compute:
 $C = M + Q_a = (838,836) + (208,388) = (331724).$
- Encrypts the master $Q_a = (175,388)$ using $BP_1 = (225,366)$
 $, BP_2 = (450,530), BP_3 = (100,75)$ and $t = (407,726)$ by:
 $k_1 = x_1(1 - t_1)^3 + 3x_2(1 - t_1)^2t_1 + 3x_3(1 - t_1)t_1^2$
 $+ x_4t_1^3 \text{ mod } p$
 $215(1 - 407)^3 + 3(160)(1 - 407)^2(407)$
 $+ 3(100)(1 - 407)(407^2)$
 $+ (330)(407^3) \text{ mod } 967$
 $= 120394754485 \text{ mod } 967 = 530.$
 $K = (633,530)$ is ciphered session key.
- Sends $\{C, K\}$ to Bop.

4. Decryption Process (Bop)

- Receives $\{C, K\}$ to Bop
- Decrypts $K = (633,530)$ using $BP_1 = (2015,115),$
 $BP_2 = (160,140), BP_3 = (100,75)$ and $t = (407,726)$ by
 compute and find the master key:
 $x_4 = [k_1 - x_1(1 - t_1)^3 - 3x_2(1 - t_1)^2t_1$
 $- 3x_3(1 - t_1)t_1^2](t_1^3)^{-1} \text{ mod } p$
 $[633 - 215(1 - 407)^3 - 3(160)(1 - 407)^2(407)$
 $- 3(100)(1 - 407)(407^2)]. (407^3)^{-1} \text{ mod } 967$
 $= (2362222313)(319) \text{ mod } 967 = 330.$

To be continued 

3.2. Huffman coding

In compression theory in computer science, Huffman coding (HC) is a compression algorithm that reduces data such as text data. The algorithm exploits the letters' hesitation (weight) and the text file's length or text stream. In HC, the text stream lengths are important and necessary with the algorithm for lossless data compression. The suitable fragmentation for the text stream length makes the system more reliable and robust [27]. The main goal of the HC algorithm is to reduce the size of the text before embedding it in the image. The main process of the Huffman algorithm depends on reducing frequent letters and giving them priority codes or short paths in a Huffman tree. Khan *et al.* [13] illustrate strategies for reducing text frequency (redundancy) through HC.

3.3. Image partitioning method

A new partitioning method is used in this study to improve the security of image steganography. This method is called the IPM. This method partitions an image into three phases to secure the final embedding pixel using a randomization procedure. There are various advantages of using a randomization algorithm, as follows: i) simplicity for solving various problems; ii) highly efficient; iii) easy implementation; iv) optimum output is produced with a very high probability of achieving randomization goal.

Based on these advantages, the proposed IPM has used a random approach with the proposed scheme. The IPM has two phases; the first is responsible for image partitioning, and the second is responsible for random pixel selection based on Hénon map function (HMF). Both phases work together to achieve the security level of the proposed work. Three phases in image partitioning will be performed. The image is partitioned into an 8×8 block (comprising 64 blocks) as an initial partitioning. The second partitioning selects a block out of the 64 blocks and further partitions it into a block of 64×64 pixels (4096 pixels). The final partitioning selects a sub-pixel from the 4096 pixels and partitions it into a block of 8×8 pixels (64 pixels). Figure 5 illustrates the image partitioning of the proposed method.

To achieve enhanced security in a proposed work, three control random parameter function based on the Henon map function have been used. In most studies, researchers have commonly implemented a single parameter to choose the number, whereby an initial condition for this function (single) is 10^{15} , while the probability of finding the number is 2^{50} . On the other hand, the Henon map function increases the complexity in the attempts of finding the number by 10^{30} , which is a rough equivalent of 2^{100} . This is sufficient to secure the secret text within an image. The HMF is an idea about dynamic function (DF) with a chaotic behaviour. The Henon map has two initial parameters: ($a=1.4$) and ($b=0.3$) which serve a chose behaviour for the chaotic function. The HMF depends primarily on a and b parameters and can be illustrated as a coordinate point (X_n, Y_n) on a plane. These points will be used in this function as (1).

Continued here:

$$y_4 = [k_2 - y_1(1 - t_2)^3 - 3y_2(1 - t_2)^2t_2$$

$$- 3y_3(1 - t_2)t_2^2](t_2^3)^{-1} \text{ mod } p$$

$$[530 - 115(1 - 726)^3 - 3(140)(1 - 726)^2(726)$$

$$- 3(75)(1 - 726)(726^2)]. (726^3)^{-1} \text{ mod } 967$$

$$= (-30470317595)(74) \text{ mod } 967 = 235.$$

$Q_A = (330,235)$ is the master Key.

- Converts the master key $Q_A = (330,235)$ to binary bits:
 $Q_A = 10100101011101011,$ and then converts it to decimal
 $Dec. = 84715,$ and computes $n = Dec. \text{ mod } p$
 $n = 84715 \text{ mod } 976 = 586.$
- Calculate the session key Q_a by: $nQ_a = 586(330,235)$
 $Q_a = (208,534).$
- Decrypts the ciphertext $C = (331,724)$ to find the message M
 by
 Compute: $M = C - Q_a$
 $= (331,724) - (208,534)$
 $= (331,724) + (208,534 \text{ mod } 967)$
 $= (331,724) + (208,433)$
 $= (838,836).$
- Uses the secret point $P = (678,801)$ to solve DLP for $M =$
 m_1P
- $(838,836) = m_1(678,801)$
- $P = (678,801), 2P = (540,950), 3P = (690,221),$
- $4P = (216,77), 5P = (400,497), \dots, 101P = (838,836) =$
 $M.$
- then, $m_1 = 101 \rightarrow$ character e.
 By the same way, for each remaining characters

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad (1)$$

The main objective of using three steps (for block and pixel) with a random map is to increase the security of the embedded process in an image. To achieve a random pixel distribution, pixel matching with secret data value is needed.

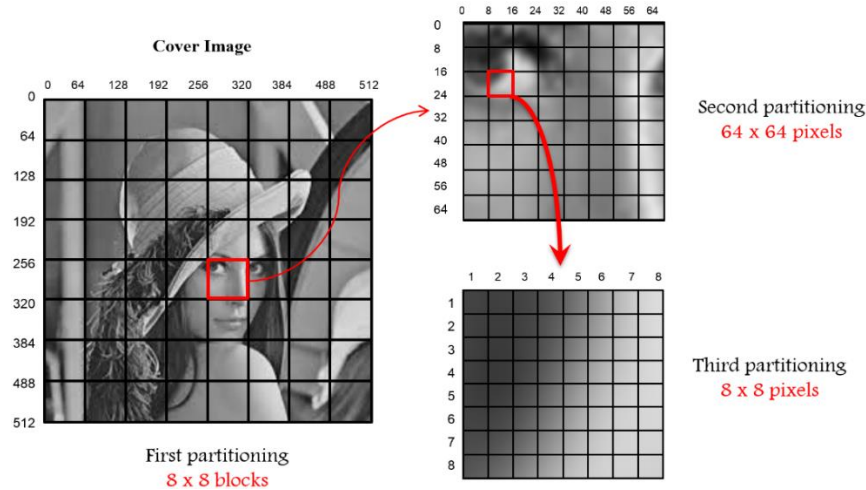


Figure 5. Image partitioning based on the proposed IPM

3.4. Embedding process based on Bit interchange method

Proposed BIGM aims to keep the stego image with secret data like the original image. After selecting the pixels using IPM, the embedding process is ready. Before the embedding process, the secret data is divided into 64 bits. At this stage, the 64 bits (the last stage of IPM) will replace with 64 bits (from the secret data). Before replacing (embedding process), check the match between the bits in the original image and the bits in the secret data. The secret data is exchanged and embedded if the number of matching bits is less than the number of non-matching bits. Otherwise, directly embed the secret bits. Figure 6 shows red bits represent non-matching bits, and green bits represent match bits.

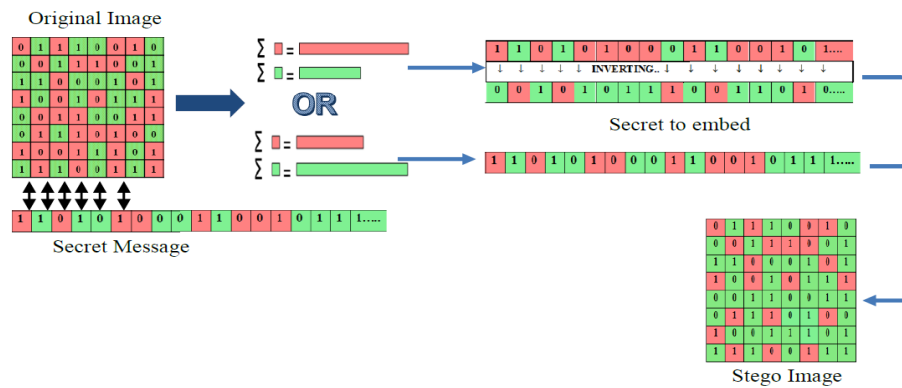


Figure 6. The main procedure of BIGM

The pixels for each cycle checked the LSBs and compared them with the corresponding bit in the secret data. The BIGM procedure is considered when between cover image LSBs and secret bits conform. This procedure condition is stored in the stego key to retrieve the information later on from the receiver. Stego key is built through the embedding method and consists of a lot of sequence information about the embedding process. The other side inverted this procedure to extract the secret message. The payload capacity of the secret message is estimated for bitplane (1) using: $(512 \times 512) / 8 = 32768$ bits. Irrespective of the inversion of the secret during embedding, all embedding occurs in bitplane (1), as illustrated in Figure 7.

The secret data is inverted and embedded when the majority does not correspond to the matching bits. Otherwise, the secret data is inserted directly into the cover image. The most important procedure is to mark all the pixels into the block map called the BIGM block. Figure 8 shows the details of this procedure. Simplistically, in BIGM, the embedding follows a certain condition: the matching between bits of secret data and bits in the LSB image if many should be embedded directly or else inverting then embed.

It is important to check the LSB of the pixel because all the information related to inspection is also stored in the BIGM block. Tracking the pixel is impossible without a BIGM block. Therefore, mapping and storing the procedure is necessary. During the checking of matching pixels, it is necessary to keep the mess of the bit distribution as much as possible so that the HVS attack can be avoided.

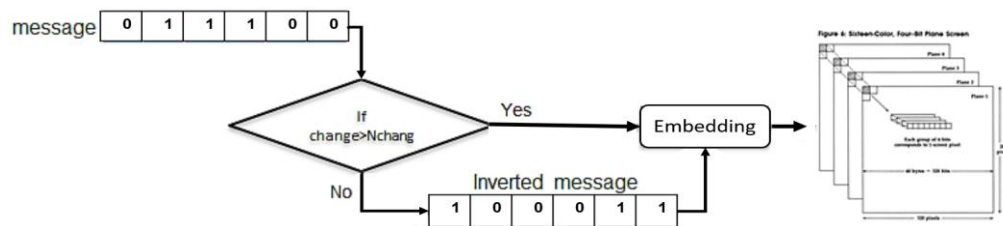


Figure 7. The BIGM procedure in proposed scheme

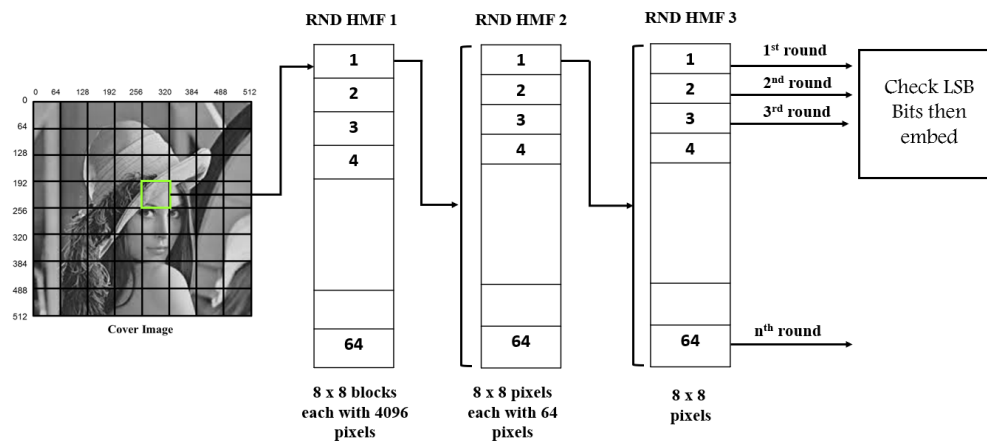


Figure 8. The procedure of IPM method with checking LSB before embedding

4. RESULTS AND DISCUSSION

The approaches for evaluating the stego image can be objective or subjective. The objective evaluation methods use mathematical criteria and a variety of other criteria, such as ground truth or prior information from statistical concerns, to determine the discrepancies between the stego picture and the cover image. On the other hand, subjective evaluation approaches rely on human observation and judgment rather than any reference standards. The outcomes will be described in detail.

4.1. Evaluation criteria

Various types of steganalysis (stego analysis) methods have been proposed to test stego image performance prior to sending it out to receivers. Leading methods to simulate attacks on steganography performance in the literature include chi-square, HVS attack, MSE, PSNR, HA, and SSIM.

MSE

$$MSE = \frac{1}{M*N} \sum_{i=1}^M \sum_{j=1}^N (a(i,j) - b(i,j))^2 \tag{2}$$

PSNR

$$PSNR = 10 \log_{10} \frac{I_{max}^2}{MSE} \tag{3}$$

SSIM

$$SSIM = \frac{(2P_0 Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_0^2 Q_S^2 + C_1)(\sigma_0^2 + \sigma_S^2 + C_2)} \tag{4}$$

In MSE and PSNR, the three embeddings include simple LSB, PVD, and proposed method, as shown in Table 1. When the result of the proposed system is compared against the performance of existing methods in data hiding, a distinguishable performance difference is noted, as shown in Table 2. Table 3 compares the findings obtained using the SSIM and MSE to those obtained using existing state-of-the-art approaches. The proposed method's evaluation findings were found to be superior to those published in the literature. The cover image is viewed as the stego image in the image histogram, and this is the major goal of the image steganography histogram, as illustrated in Figures 9 for color and grayscale images, respectively. The cover image is viewed as the stego image in the image histogram, and this is the major goal of the image steganography histogram, as illustrated in Figures 9 for color and grayscale images, respectively.

Table 1. Different result related to MSE and PSNR with different techniques with proposed work

Payload (bytes)	Embedding percent (%)	MSE (LSB)	MSE (PVD)	MSE (proposed work)	PSNR (LSB)	PSNR (PVD)	PSNR (proposed work)
16384	6.25	0.3328	0.2123	0.1012	62.2	71.32	78.09
32768	12.5	0.6453	0.5023	0.2011	61.22	67.63	73.25
49152	18.75	0.9332	0.8323	0.6011	55.76	63.16	68.94
65536	25	1.3228	0.9881	0.8021	50.82	55.91	61.41

Table 2. PSNR benchmarking at 16384 bytes of capacity payload data

Reference	Payload capacity (bytes)	Lena	Papper
[32]	16384	64.54	64.72
[26]	16384	72.09	71.32
[25]	16384	68.34	68.26
[24]	16384	71.27	71.27
Proposed work	16384	73.09	73.15

Table 3. Results of the suggested scheme vs the state of the art in SSIM and MSE

Reference	Dataset/Image size	EP (%)	SSIM	MSE
[30]	USC-SIPI 512×512	6.25	0.996	0.0127
[32]	USC-SIPI 512×512	6.25	0.957	0.0240
[26]	USC-SIPI 512×512	6.25	0.968	0.0236
[25]	USC-SIPI 512×512	6.25	0.981	0.0122
Proposed study	USC-SIPI 512×512	6.25	1	0.0101

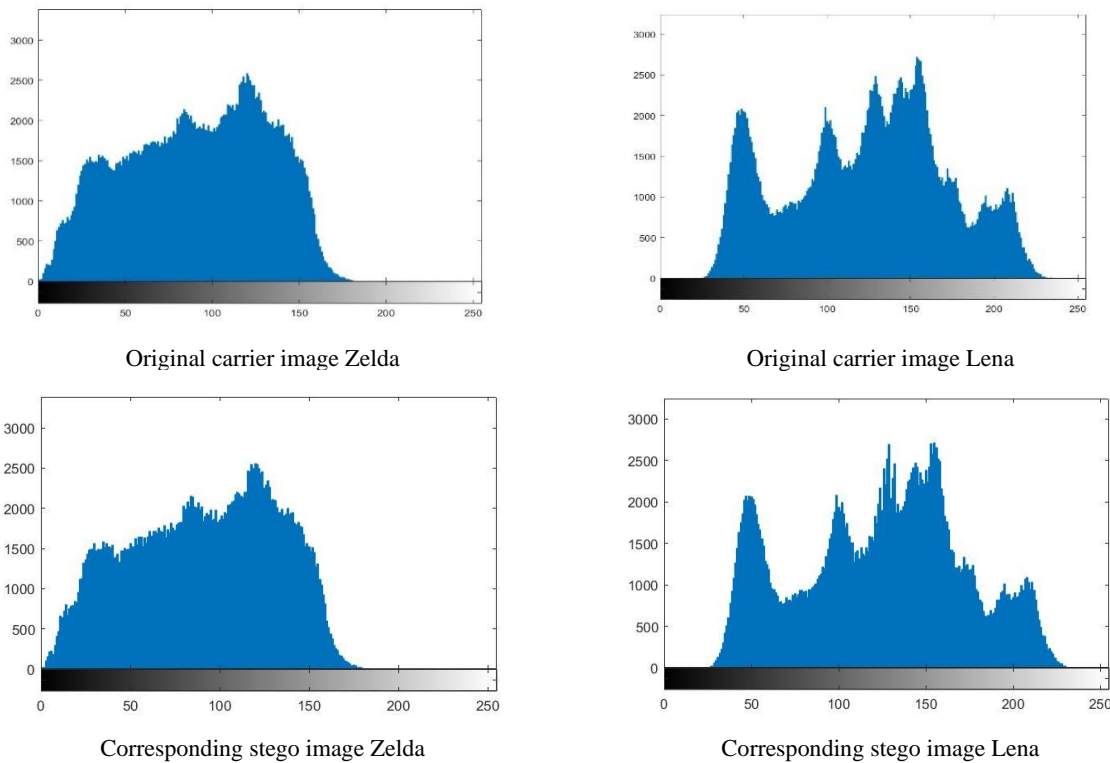


Figure 9. Histograms of the original carrier images and the corresponding stego images

5. CONCLUSION

The main objective of the proposed research is to improve and highlight the security of the image steganography system with maintaining the PSNR value. In this study, a high payload capacity of the secret message is used during hide within the image. The current study has many valuable contributions which are like IPM, HAC, and BIGM. These contributions achieved the objectives of image steganography, such as security, and produced a high value of imperceptibility. The results achieved in this study indicate that the proposed system is efficient in terms of security and capacity. Based on findings, the high result obtained in terms of PSNR, SSIM, and MSE when compared with important existing schemes. In addition, the plan for the exploration towards improving and continuing this research has been emphasized in the future. In short, the newly designed steganography scheme owing to its outperforming attributes, could improve the security, robustness, capacity, imperceptibility, and immunity against unknown and known attacks.

ACKNOWLEDGEMENTS

The authors would express great gratitude to the Computer Engineering Department at AL Iraqia University, Ministry of Higher Education and Scientific Research Iraq-Baghdad, for all support while writing this paper.




REFERENCES

- [1] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," *Mob. Networks Appl.*, no. March, 2022, doi: 10.1007/s11036-022-01937-3.
- [2] I. Almomani, A. Alkhayer, and W. El-Shafai, "A Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices," *Sensors*, vol. 22, no. 6, pp. 1–20, 2022, doi: 10.3390/s22062281.
- [3] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A Novel Image Steganography Method for Industrial Internet of Things Security," *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7743–7751, Nov. 2021, doi: 10.1109/TII.2021.3053595.
- [4] M. M. HASHIM, "High Secure Software Watermarking Based on White Space Scheme and Chaotic Logistic Map," *Trends Sci.*, vol. 18, no. 20, 2021.
- [5] M. K. Abed, M. M. Kareem, R. K. Ibrahim, M. M. Hashim, S. Kurnaz, and A. H. Ali, "Secure Medical Image Steganography Method Based on Pixels Variance Value and Eight Neighbors," in *2021 International Conference on Advanced Computer Applications, ACA 2021*, 2021, pp. 199–205, doi: 10.1109/ACA52198.2021.9626807.
- [6] Z. Wang, G. Feng, Z. Qian, and X. Zhang, "JPEG Steganography With Content Similarity Evaluation," *IEEE Trans. Cybern.*, pp. 1–12, 2022, doi: 10.1109/tyb.2022.3155732.
- [7] O. M. Osman, M. E. A. Kanona, M. K. Hassan, A. A. E. Elkhair, and K. S. Mohamed, "Hybrid multistage framework for data manipulation by combining cryptography and steganography," *Bull. Electr. Eng. Informatics*, vol. 11, no. 1, pp. 327–335, 2022, doi: 10.11591/eei.v11i1.3451.
- [8] A. A. A. Hadad, H. N. Khalid, Z. S. Naser, and M. S. Taha, "A Robust Color Image Watermarking Scheme Based on Discrete Wavelet Transform Domain and Discrete Slantlet Transform Technique," *Ing. des Syst. d'Information*, vol. 27, no. 2, pp. 313–319, 2022, doi: 10.18280/isi.270215.
- [9] P. Parmar and D. Sanghani, "Enhancing the Security of Confidential Data Using Video Steganography," in *Cybernetics, Cognition and Machine Learning Applications*, Springer, 2021, pp. 203–210.
- [10] M. M. Kareem, S. A. S. Lafta, H. F. Hashim, R. K. Al-Azzawi, and A. H. Ali, "Analyzing the BER and optical fiber length performances in OFDM RoF links," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 23, no. 3, pp. 1501–1509, 2021, doi: 10.11591/ijeecs.v23.i3.pp1501-1509.
- [11] K. Karampidis, E. Linardos, and E. Kavallieratou, "StegoPass – Utilization of Steganography to Produce a Novel Unbreakable Biometric Based Password Authentication Scheme," in *Computational Intelligence in Security for Information Systems Conference*, 2022, pp. 146–155, doi: 10.1007/978-3-030-87872-6_15.
- [12] K. D. Abel, S. Misra, A. Agrawal, R. Maskeliunas, and R. Damasevicius, "Data Security Using Cryptography and Steganography Technique on the Cloud," in *Lecture Notes in Electrical Engineering*, vol. 834, Springer, 2022, pp. 475–481.
- [13] S. Khan *et al.*, "A modulo function-based robust asymmetric variable data hiding using DCT," *Symmetry (Basel)*, vol. 12, no. 10, pp. 1–23, Oct. 2020, doi: 10.3390/sym12101659.
- [14] M. S. Taha, M. H. Mahdi, H. N. Khalid, A. H. Mohd Aman, and Z. S. Attarbashi, "A Steganography Embedding Method Based on Psingle/ Pdoubleand Huffman Coding," *2021 3rd Int. Cyber Resil. Conf. CRC 2021*, Jan. 2021, doi: 10.1109/CRC50527.2021.9392522.
- [15] F. H. MohammedSediq Al-Kadei, "Two-level hiding an encrypted image," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, pp. 961–969, 2020, doi: 10.11591/ijeecs.v18.i2.pp961-969.
- [16] R. Din and A. J. Qasim, "Steganography analysis techniques applied to audio and image files," *Bull. Electr. Eng. Informatics*, vol. 8, no. 4, pp. 1297–1302, 2019, doi: 10.11591/eei.v8i4.1626.
- [17] S. T. Mustafa, M. S. M. Rahim, F. Y. H. Ahmed, M. M. Hashim, and A. Zainal, "Hiding financial data in bank card image using contrast level value and text encryption for worthiness a robust steganography method," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 7 Special Issue, pp. 2783–2801, 2020, [Online]. Available: <https://www.researchgate.net/publication/341669833>.
- [18] F. Q. A. Alyousuf and R. Din, "Analysis review on feature-based and word-rule based techniques in text steganography," *Bull. Electr. Eng. Informatics*, vol. 9, no. 2, pp. 764–770, 2020, doi: 10.11591/eei.v9i2.2069.
- [19] K. A. -Majidi *et al.*, "MLCM: An efficient image encryption technique for IoT application based on multi-layer chaotic maps," *Int. J. Nonlinear Anal. Appl.*, vol. 0, pp. 2008–6822, Jun. 2022, doi: 10.22075/IJNAA.2022.6571.
- [20] M. M. Hashim, N. K. Ajeel, H. J. Alhamdane, A. H. Herez, M. S. Taha, and A. H. Ali, "Based on Competitive Marketing: A New Framework mechanism in Social Media," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 881, no. 1, 2020, doi: 10.1088/1757-899X/881/1/012121.
- [21] M. Abdel Hameed, S. Aly, and M. Hassaballah, "An efficient data hiding method based on adaptive directional pixel value




- differencing (ADPVD),” *Multimed. Tools Appl.*, vol. 77, no. 12, pp. 14705–14723, 2018, doi: 10.1007/s11042-017-5056-4.
- [22] M. Du, T. Luo, H. Xu, Y. Song, C. Wang, and L. Li, “Robust HDR video watermarking method based on the HVS model and T-QR,” *Multimed. Tools Appl.*, pp. 1–21, 2022, doi: 10.1007/s11042-022-13145-y.
- [23] D. R. I. M. Setiadi, “PSNR vs SSIM: imperceptibility quality assessment for image steganography,” *Multimed. Tools Appl.*, vol. 80, no. 6, pp. 8423–8444, 2021, doi: 10.1007/s11042-020-10035-z.
- [24] M. M. Hashim, A. A. Mahmood, and M. Q. Mohammed, “A pixel contrast based medical image steganography to ensure and secure patient data,” *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. Special Issue, pp. 1885–1904, 2021, doi: 10.22075/ijnaa.2021.5939.
- [25] C. A. Sari, G. Ardiansyah, D. R. I. Moses Setiadi, and E. H. Rachmawanto, “An improved security and message capacity using AES and Huffman coding on image steganography,” *Telkomnika (Telecommunication Comput. Electron. Control.)*, vol. 17, no. 5, pp. 2400–2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.
- [26] I. J. Kadhim, P. Premaratne, and P. J. Vial, “High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform,” *Cogn. Syst. Res.*, vol. 60, pp. 20–32, 2020, doi: 10.1016/j.cogsys.2019.11.002.
- [27] A. Nag, J. P. Singh, S. Biswas, D. Sarkar, and P. P. Sarkar, “A Huffman code based image steganography technique,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014, vol. 8321, pp. 257–265, doi: 10.1007/978-3-319-04126-1_22.
- [28] A. K. Sahu, G. Swain, M. Sahu, and J. Hemalatha, “Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP,” *J. Inf. Secur. Appl.*, vol. 58, p. 102808, 2021, doi: 10.1016/j.jisa.2021.102808.
- [29] M. Hassaballah, *Digital media steganography: principles, algorithms, and advances*. Academic Press, 2020.
- [30] A. H. Khaleel *et al.*, “Secure image hiding in speech signal by steganography-mining and encryption,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1412–1419, 2019, doi: 10.11591/ijeecs.v16.i3.pp1416-1423.
- [31] S. Pramanik, R. P. Singh, and R. Ghosh, “A new encrypted method in image steganography,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, no. 3, pp. 1412–1419, 2019, doi: 10.11591/ijeecs.v13.i3.pp1412-1419.
- [32] H. F. Hashim, M. M. Kareem, W. K. Al-Azzawi, and A. H. Ali, “Improving the performance of photovoltaic module during partial shading using ANN,” *Int. J. Power Electron. Drive Syst.*, vol. 12, no. 4, pp. 2435–2442, 2021, doi: 10.11591/ijpeds.v12.i4.pp2435-2442.

BIOGRAPHIES OF AUTHORS



Suray Alsamarae    is a lecturer in the Computer Engineering Department, College of Engineering, Al-Iraqia University, Iraq- Baghdad. He received a BSc degree in Computer Science from Al Mamoun University College, Iraq-Baghdad in 2006. He received a Master's degree in Computer Science from Southern Illinois University, the U.S.A in 2018. Currently, he His research interests include computer security, network and security, cloud security, and blockchain technology. He can be contacted at email: suraysaady80@gmail.com, suray.alsamarae@aliraqia.edu.iq.



Ali Salem Ali    received a BSc degree in Computer Science from Al-Mamoun University College, Iraq- Baghdad in 2004. He received a Master's degree in Computer Science from National Technical University Kharkov Polytechnic Institute, Ukraine-Kharkov in 2008. And the Ph.D. degree from Kharkov National University of Radio Electronic Currently, he is a lecturer in the Network Engineering Department, College of Engineering, Al-Iraqia University, Iraq-Baghdad. His research interests include computer security, network and security, cloud security, network management, and computer technology. He can be contacted at email: alialbander2004@gmail.com.