Bulletin of Electrical Engineering and Informatics
Vol. 13, No. 3, June 2024, pp. 1788~1801
ISSN: 2302-9285, DOI: 10.11591/eei.v13i3.7140

Secure map-based crypto-stego technique based on mac address

Dima S. Kasasbeh[1], Bushra M. Al-Ja'afreh[1], Mohammed Anbar[1], Iznan H. Hasbullah[1], Mahmoud Al Khasawneh[2]
[1]National Advanced IPv6 Center (NAv6), University Sains Malaysia (USM), Penang, Malaysia
[2]School of Computing, Skyline University College, University City of Sharjah, Sharjah, United Arab Emirates

Article Info

Article history:

Received Jul 4, 2023
Revised Sep 28, 2023
Accepted Oct 12, 2023

Keywords:

Cryptography
Crypto-stego
Information hiding
Mac-address map locations
Map-based
Steganography

ABSTRACT

Steganography and cryptography are spy craft cousins, working differently to achieve the same target. Cryptography is perceptible and observable without understanding the real content, while steganography hides the content so that it is not perceptible or observable and without producing noticeable changes to the carrier image. The challenge is finding the right balance between security and retrievability of embedded data from embedding locations without increasing the required embedded information. This paper proposes a secure map-based steganography technique to enhance the message security level based on the sender and recipient mac addresses. The proposed technique uses rivest-shamir-adleman (RSA) to encrypt the message, then embeds the cipher message in the host image based on the sender and recipient media access control addresses (mac addresses) exclusive or operation "XOR" results without increasing the required embedded information for the embedding location map. The proposed technique is evaluated on various metrics, including peak signal-to-noise ratio (PSNR) and embedding capacity, and the results show that it provides a high level of security and robustness against attacks without an extra location map. The proposed technique can embed more data up to 196.608 KB in the same image with a PSNR higher than 50.58 dB.

Corresponding Author:

Mohammed Anbar
National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia (USM)
11800 Gelugor, Penang, Malaysia
Email: anbar@usm.my

1. INTRODUCTION

The internet and public communication networks provide great convenience in transferring large amounts of messages; their communication channels are used to deliver and exchange information. However, the openness of the internet and communication networks requires robust techniques to protect the transferred digital information from intrusion or destruction, copying or modification, and assurance that the data are protected from intruders and hackers and are correctly delivered to recipients. Individuals try to keep their messages safe by using more advanced steganography techniques than traditional cryptographic methods or by combining traditional cryptographic methods with steganography techniques [1]–[3]. Steganography makes use of the hidden message's appearance to enhance the performance of the communication channel, which allows important digital information to be hidden within a spoof carrier image in such a way that the modifications are imperceptible to some degree. Although it is commonly used to hide confidential digital information, it can also be used to perform other functions related to the communication channel and secretly broadcast digital information [1], [4], [5].

Digital images have been chosen as the suitable digital medium to hold the transferred secret information due to their widespread use in numerous internet applications. Moreover, digital images can be easily shared and stored without arousing suspicion, making them an ideal choice for covert communication. In addition, digital images offer a high level of steganography security, which makes it difficult for unauthorized individuals to detect the hidden information within the image. This makes digital images a popular choice for espionage and other covert operations [6], [7]. However, steganography attackers may use sophisticated techniques to detect hidden secret information statistically or visually, making it challenging to ensure the security of steganographic communication. To overcome this difficulty, steganography techniques are constantly changing to stay one step ahead of potential attackers, and researchers are constantly coming up with new ways to improve the security of steganographic communication and shield the stego image from attackers' analysis by keeping the stego image as close to the original as possible [8], [9].

Cryptography and steganography are two important techniques used to protect digital information and ensure secure communication over the internet and public communication networks. While cryptography involves encoding messages to prevent unauthorized access, steganography involves hiding messages within seemingly harmless messages to maintain secrecy. Both techniques are essential in ensuring digital information's confidentiality, integrity, and authenticity, especially in today's world where cyber threats are becoming increasingly sophisticated [7], [10]. Steganography and cryptography are cousins in the spy-craft family. Each works in a different way to achieve the same target; cryptography is perceptible and observable without understanding the real content, while steganography hides the content so that it is not perceptible or observable and without producing noticeable changes to the carrier media [4], [7], [11]. The main goal of both cryptography and steganography is security. Cryptography focuses on keeping the contents of the message secret, while steganography focuses on keeping the confidentiality and existence of the message secret so that unauthorized people don't know that digital information is hidden in the cover image. As a result, steganography has inherited various security characteristics from its ancestors [7], [11].

The crypto-stego technique is different from the stego-crypto technique in that it primarily focuses on using cryptography as the main method of securing messages, while steganography is used as an additional layer of protection. In crypto-stego, the message is first encrypted using cryptographic algorithms and then hidden within a carrier file using steganography techniques, making it even more difficult for unauthorized individuals to detect and decipher the hidden message [1], [12], [13]. In the stego-crypto technique, the message is first hidden within a carrier file using steganography techniques, and then the stego image is encrypted using cryptographic algorithms. This added layer of security ensures that even if the carrier file is intercepted, it would be extremely challenging for unauthorized individuals to access the hidden message. However, it is important to note that the encryption process may introduce some additional distortion to the stego image, which could potentially affect its quality or appearance [2], [5], [11].

Researchers in the literature have proposed various steganography techniques, including cryptographic-based, perception-based, least significant bit LSB-based, histogram-based, and feature extraction-based [1]–[3], [11], [12]. Each technique has its own strengths and weaknesses, and the choice of technique depends on the specific application requirements and constraints. Additionally, ongoing research is focused on developing new steganography techniques to improve hidden information's security and robustness. The limitations and drawbacks of these techniques include susceptibility to statistical attacks such as histogram analysis and a relatively small embedding capacity compared to other methods; thus, increasing embedding capacity reduces image quality and requires a location map that increases the amount of information to be embedded. In this paper, we propose a secure map-based crypto-stego technique to overcome these limitations and enhance the security of messages hidden in images without the need for a location map. The proposed technique encrypts the message using rivest-shamir-adleman (RSA) to provide an added layer of security to the message transmission process, ensuring that only authorized parties can access the encrypted message. The message is rendered unreadable and then embedded in a cover image using the proposed embedding mechanism based on the mac's exclusive or operation XOR operation result between the sender and recipient mac addresses as mapping locations.

The rest of this paper is structured as follows: in section 2, we describe the related work. We provide a detailed description of the proposed technique in section 3, followed by section 4 on experimental results. Some conclusions and future work are drawn in section 5.

2. RELATED WORK

The mapping technique is a method for steganography within the spatial domain in which the embedding pixels are chosen based on some mathematical operation or mapping technique that depends on the pixel intensity value. Embedding is done by assigning every two or four bits of the secret message to each adjacent pixel, depending on some feature of that pixel. There are several existing steganography techniques based on mapping techniques like 3-D cat chaotic maps, 3-D Chebyshev maps, and 3-D logistic maps. The odd/even distribution used 3 LSB to embed one's value of the secret message in odd pixels and zeros in even pixels. The cover image is divided into blocks; the Henon map function randomly selects the destination pixel in each block and embeds the secret message into the image block. The least significant bit (LSB) technique replaces the least rightmost 3 bits of each image pixel with a 3-bit secret message. 3-LSB maximized embedding capacity about three times, but its effect was higher image distortion [14]. The steganography mechanism proposed in [15] conceals secret messages randomly into three-dimensions (3-D) color images of red, green, and blue (RGB image); the image embed pixels are selected based on a 3-D cat chaotic map.

A new steganography technique is suggested in [16] to improve information hiding efficiency and stego image visual quality. The secret message is randomly embedded into the RGB image using LSB substitution and secret map methods. 3D chaotic charts, Chebyshev maps, and 3D logistic maps are used to select embedding pixels in the cover image. 3D Chebyshev and 3D logistic maps are used to embed a secret message into the LSB of the cover image, which improves the stego image's visual quality with low distortion. Intermediate significant bit (ISB) changes the higher bit plane using LSB. It has high robustness and capacity, but lower image quality [16]. The model hides binary secret digital media in the 24-RGB image; the carrier image is converted to the YCbCr color model; then the XOR operation is applied between one pixel of secret digital media and one pixel from the YCbCr channel of the carrier image, and the XOR result is embedded in the LSB of the blue channel [17].

A new secret key mapping-based steganography schema for exchanging secret messages without effecting any change in the carrier media. The commonly used steganography testing image list is used by concatenating the image name with the secret message to generate a bit secret stream. A separate position file is produced consisting of the cover image pixel position if the LSB of the pixel matches the secret message bit stream. The separate position is encrypted using a symmetric secret key and transmitted along with the cover image. The reverse process is applied to generate the secret message: the pixel position is read from a separate position file, then the LSB of each pixel is combined to generate the secret message. The bit-by-bit matching technique produces time complexity with a low capacity [18]. In Table 1 shows the comparison between related mapping-based steganography techniques in [14]–[16], [18].

Table 1. Comparison between related mapping-based steganography techniques

Approach	Merits	Demerits	Performance criteria
Odd/even distribution with henon map function [14]	destination pixel selected using henon map function, simplicity, high imperceptibility	Lack of steganalysis attack evaluation	PSNR >66 dB EC=1 bpp (RGB) RAS: NA
3-D cat map [15]	Randomly embedding into RGB image using secure structure of chaotic map. high visual quality. Higher complexity encountered by the attackers	Limited payload	PSNR >54 dB MSE >0.2334 EC=1 bpp Entropy ~7 Contrast= Autocorrelation= Energy ~0.2 Homogeneity >0.8 RAS: histogram
Intermediate significant bit (ISB) and secret map techniques [16]	Strong resistance against statistical attacks, high embedding capacity without any distortion, improve security using secret keys	High sensitivity to its secret keys	PSNR ~45 dB EC=0.33 bpp (RGB) Entropy ~ identical Homogeneity ~ identical Contrast ~ identical Quality index~1 MSE ~2 RAS: histogram highlights slight changes
A new secret key mapping-based [18]	New perspective of exchanging secret data through steganography. separate position file store embedding pixel position. Robustness cover media does not change. enhanced security	Lack of steganalysis attack evaluation	PSNR infinity MSE=0 EC=1 bpp (RGB) RAS: NA

A variety of security techniques were developed to safeguard digital media content from illegal access. These security techniques, which involve both steganography and cryptography sciences, have served as a solid foundation for many studies in recent years. According to the study's requirements, several previous similar studies were included based on their methodology and compatibility with the proposed system's levels. Researchers have devised different security techniques that combine cryptography and steganography, to protect the shared multimedia elements and address the emerging problems in information security [19].

The DH method is based on adaptive block truncation coding (BTC) edge quantization (ABTC-EQ) using an optimal pixel adjustment process (OPAP). The DH method achieves high embedding capacity with low distortion. The cover grayscale image is divided into 4X4-sized blocks, and each block is compressed by ABTC-EQ to generate trios. 2LSB and LSB techniques are applied to embed 4 bits into the quantization values of trios. OPAP improves embedding capacity and reduces image distortion, while ABTC-EQ maintains image quality [20].

An improved canny edge detector (CED)-based technique is proposed to observe more edge pixels in the cover image. Further, using Huffman coding to transform secret messages into compressed form enhances security. Huffman tables are implemented to randomize the edge pixels, while Huffman encoding is applied to compress and protect secret messages. The coherent bit length is determined based on the sorting edge pixels to specify the secret message bitstream size. This method achieves high visual quality and embedding capacity. Huffman coding compresses the secret message to achieve a high payload and enhance security while embedding complex information that is not robust and vulnerable to a steganalysis attack [21].

The Huffman coding method is used to compress the secret message, and then the compressed message is embedded into the cover image using the odd/even distribution proposed method. The odd/even distribution used 3 LSB to embed one's value of the secret message in odd pixels, while zeros were in even pixels [14]. The cover image is divided into blocks; the henon map function randomly selects the destination pixel in each block and embeds the secret message into the image block. The LSB technique replaces the least rightmost 3 bits of each image pixel by a 3-bit secret message. 3-LSB maximized embedding capacity about 3 times, but its effect was higher image distortion. PVDMF is a steganography technique based on pixel value differencing (PVD) and modulus function (MF). PVDMF1 and PVDMF2 are two variants that use the difference between two consecutive pixels to embed a secret message. The embedded pixels are then readjusted to reduce stego image distortion. The proposed technique avoided FOBP and is resistant to the RS steganalysis analysis attack [22].

The deoxyribonucleic acid (DNA) sequence is combined with hyperelliptic curve cryptography to produce a highly secured steganography technique [23]. The nucleotide to a binary transformation table is used to convert the carrier image into DNA sequences; the DNA triplet values of the carrier image and secret message are converted to binary representation; and an XOR logic operation is applied to generate the stego image. A multi-level secret data concealing technique that combines integrated visual cryptography and steganography The visual cryptographic technique is applied to generate the shares, and the halftoning method is used to reduce carrier image pixels before embedding encrypted shares using LSB [24]. Ahmed and Ahmed [25] improved secret message security and robustness by combining steganography with cryptography. The secret message has been encrypted using the one-time pad (OTP) symmetric encryption technique. LSB substitution is used to embed the encrypted message.

3. THE PROPOSED TECHNIQUE

In this paper, a secure map-based crypto-stego technique is proposed to guarantee a secure and efficient message transmission based on mac addresses (media access control addresses) between the sender and recipient for transmitting sensitive information without the risk of interception or tampering. The key strategy of our technique focuses on using the RSA encryption algorithm to encrypt the secret message before embedding it into a spoof cover image and transmitting it to the recipient without the need for extra transmission content for the embedding map location.

The proposed technique uses the mac addresses of the sender and recipient, which were previously shared between the two parties based on their communication agreement, to determine the embedding locations in the carrier image; in other words, the sender and recipient mac addresses are used in our proposed mapping location generation to generate the embedding locations. The proposed technique consists of three main stages: the crypto stage, the mapping generation stage, and the stego stage at the sender side, and the extraction stage at the recipient side. All these stages are illustrated in Figure 1.

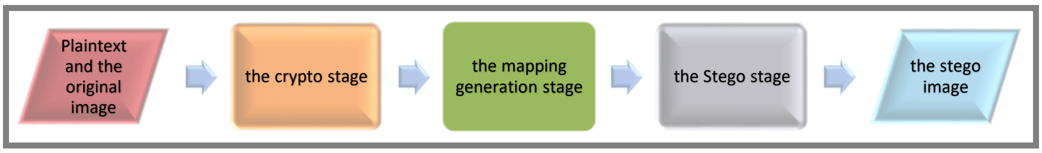


Figure 1. The proposed technique of three stages: the crypto stage, the mapping generation stage and the stego stage

As shown in Figure 1, the main inputs of our proposed technique are plaintext and the original carrier image. The plaintext is a secret message that the sender wants to transfer to the recipient through a public, unsecure network. This message is hidden in the carrier image after it is encrypted by the RSA algorithm using the generated embedding location map. The stego image is the main output, which is the carrier image with a secret message hidden in its pixels. The RSA algorithm ensures the security of the hidden message by encrypting it, making it difficult for unauthorized individuals to access or decipher. The embedding location map generated by our technique determines the specific pixels in the carrier image where the encrypted message will be concealed, ensuring seamless integration of the secret message into the image.

3.1. The crypto stage

First, the RSA algorithm encrypts the secret message, which converts it to an unreadable format "the cipher message". This ensures the confidentiality and security of the message being transmitted. Then, the cipher message is divided into two equal parts, MP1 and MP2 as illustrated in Figure 2.

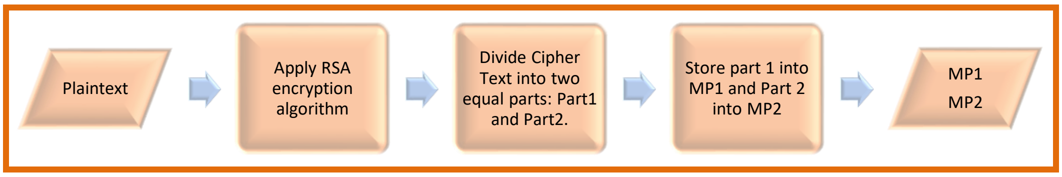


Figure 2. The crypto stage

To illustrate the proposed crypto stage the pseudocode of this algorithm as:

Algorithm 1. The crypto algorithm

Input: Plaintext. Output: MP1, Mp2.
Step 1: Read Plaintext. Step 2: Apply RIVEST-SHAMIR-ADLEMAN (RSA) encryption algorithm. Step 3: Divide Cipher Text into two equal parts: Part1 and Part2. Step 4: Store part 1 into MP1 and Part 2 into MP2

3.2. The mapping generation stage

The sender's and recipient's mac addresses are used to construct an embedding location map. A simple XOR operation is applied between both the recipient and sender mac addresses to generate 12 hexadecimal values from D0 to D11 that are used as embedding location maps. For instance, if the sender's mac address is CB: 2A:1F: AB: C5:E9 and the recipient's mac address is 2D:0A:6B: CE: F4:94, then the XOR operation result is E6:20:74:65:31:7D. Figure 3 illustrate the mac addresses of the sender and recipient XOR operation result with its 12 digits. Figure 4 shows the mapping generation stage.

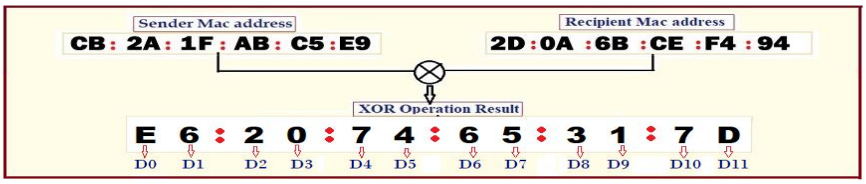


Figure 3. The mac addresses of the sender and recipient XOR operation result with its 12 digits

a. Let MP1_Set denotes the embedding set "either shadow or blank set" for the MP1 cipher part, and MP2_Set denotes the embedding set "either shadow or blank set" for the MP2 cipher part. MP1_Set and MP2_Set are determined based on the mac's XOR result as:
   - Let Sum=$\sum_{i=0}^{11} D_i$, denotes the summation of the mac's XOR result digits from zero to eleven.
   - If the Sum mod 2==0, then MP2_Set equal the blank set and MP1_Set equal the shadow. Otherwise, MP1_Set equals the black set and MP2_Set equals the shadow.

b. Let Shadow_Seq denote the sequence of embedding blocks for the shadow set Blank_Seq denote the sequence of embedding blocks for the blank set, shadow_seq and blank_seq are determined as follows:
   – Let $Avg1 = \frac{\sum_{i=0}^{5} D_i}{6}$ denotes the average of the first six digits of the mac's XOR result, and $Avg2 = \frac{\sum_{i=6}^{11} D_i}{6}$ denotes the average of the least six digits of the mac's XOR result.
   – The binary representation of Avg1 is used to determine the first block to embed the cipher message part "either MP1 or MP2" within the blank set using the following notation:
      a) Let blank set first block horizontal location BFB_H equal the first two digits of the binary representation of Avg1 from left to right, and the blank set first block vertical location BFB_V equal the least two digits of the binary representation of Avg1 from right to left. For example, if the Avg1 value in binary is 1010, the first blank block horizontal location BFB_H is 10, and the first blank block vertical location BFB_V is 01, the start embedding block [2, 1]. The second block is then embedded at [3, 1], [0, 2] respectively and so on; if needed, restart from block [0, 0] until the message part, either MP1 or MP2, has been embedded into the blank set.
      b) The same way is applied Avg2 to determine the set first block horizontal and vertical locations of the shadow set SFB_H, SFB_V.

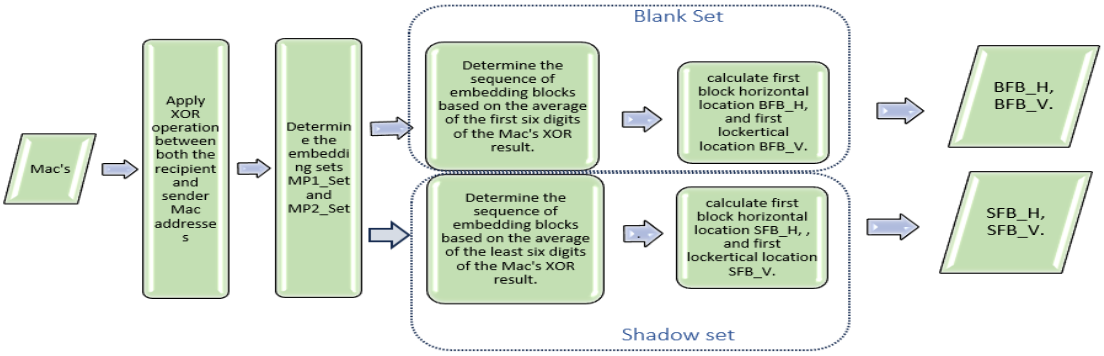


Figure 4. The mapping generation stage

3.3. The stego stage

In the stego stage, a map-based embedding mechanism is proposed to offer an effective and innovative solution for secure communication by hiding the encrypted message's existence in a spoof carrier image using mac's XOR result without an extra map location. Since unauthorized users cannot find the hidden message, it also offers a high level of security. The MP1 and MP2 bitstreams are embedded into the carrier image based on embedding block sequences and 2LSB. This process is reversible, allowing for the extraction of the embedded bitstreams without any loss of information or quality degradation in the cover image as illustrated in Figure 5. To illustrate the proposed stego stage the pseudocode of this algorithm as Algorithm 2.

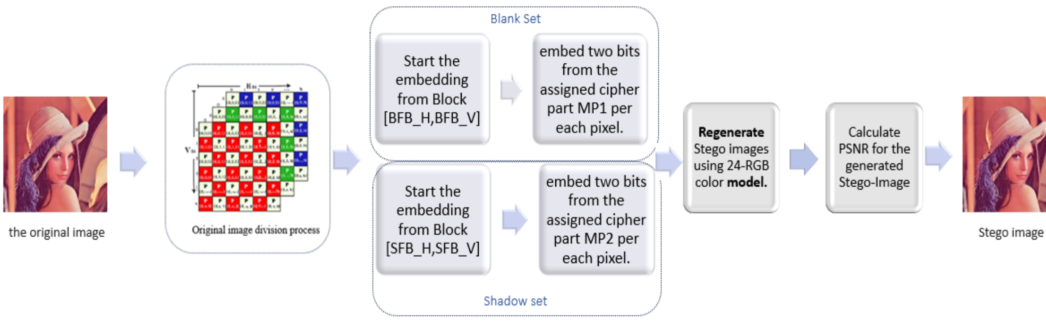


Figure 5. The stego stage

Algorithm 2. The stego algorithm

```
Input: MP1, MP2, MP1_Set, MP2_Set, BFB_H, BFB_V, SFB_H, SFB_V, and Original Image.
Output: Stego-Image.
Divide the Original image of size V × H into sixteen non-overlapping blocks of size V/16
× H/16.
For each color channel //start with the green color channel then blue finally red
IF MP1_Set == Blank set
        Start from Block[BFB_H,BFB_V] until cover all blocks
              For row =0 to V/16 Step1
                     If row%2==0?column=0: column =1
                     For column to H/16 Step 2
                            Take 2-bit from MP1 embed it into pixel [row, column]
       Start from Block[SFB_H,SFB_V] until cover all blocks
              For row =0 to V/16 Step1
                     If row%2==0?column=1: column =0
                     For column to H/16 Step 2
                            Take 2-bit from MP2 embed it into pixel [row, column]
ELSE
       Start from Block[BFB_H,BFB_V] until cover all blocks
              For row =0 to V/16 Step1
                     If row%2==0?column=0: column =1
                     For column to H/16 Step 2
                            Take 2-bit from MP2 embed it into pixel [row, column]
       Start from Block[SFB_H,SFB_V] until cover all blocks
              For row =0 to V/16 Step1
                     If row%2==0?column=1: column =0
                     For a column to H/16 Step 2
                            Take 2-bit from MP1 embed it into pixel [row, column]
Regenerate Stego images using 24-RGB color model.
Calculate PSNR for the generated Stego-Image
```

3.4. Extraction stage

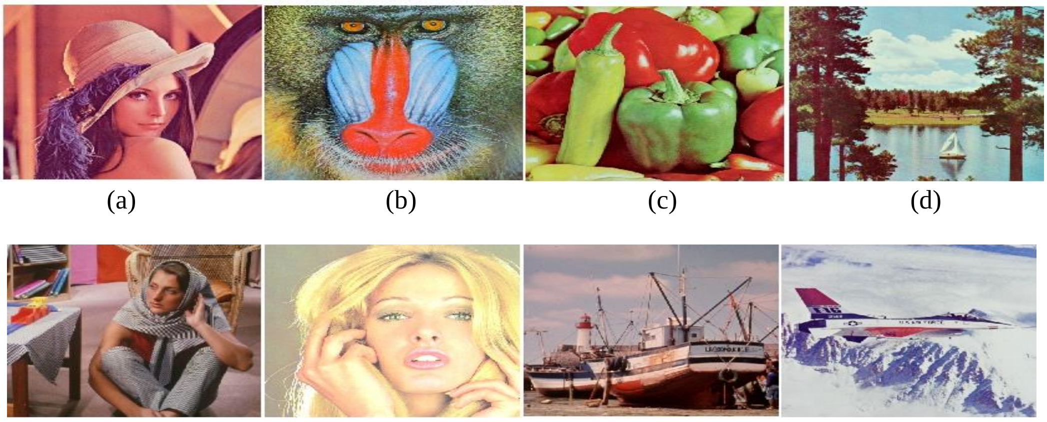
The extraction stage involves retrieving the hidden cipher message parts MP1 and MP2 from the carrier image. This is done by first identifying the location of the embedded cipher message parts and the block sequence, which is determined based on the mac's XOR result, as illustrated in the proposed embedding technique. The 2LSB technique is then used to extract the message from each block pixel by pixel, and the extracted message is reconstructed to obtain the original hidden message "cipher massage". The extraction process must be performed carefully to avoid any loss or corruption of the hidden cipher message. Overall, the embedding and extraction stages ensure secure and reliable transmission. Finally, the cipher message must be decrypted to generate the original message.

4. EVALUATION AND EXPERIMENTAL RESULTS

The effectiveness of the proposed technique is assessed empirically or visually. The carrier image properties and characteristics from a visual quality and image histograms are analyzed using the grayscale images for visual assessment. The main variable that is typically measured in empirical studies of steganography techniques is the stego image visual quality achieved on a specific set of testing images. To achieve the objectives, this section focuses on an empirical performance evaluation of the suggested technique using grayscale images. On the carrier images contained within the grayscale images, qualitative and quantitative analyses were carried out to assess the effectiveness of the proposed technique and show its applicability.

4.1. Benchmark

The first version of the USC-SIPI image database was made available in 1977 to aid research in machine vision, image analysis, and image processing. The main characteristics of the test images are used to divide the USC-SIPI database into volumes. The image sizes in each volume range from 256×256 to 1024×1024 pixels. The RGB color image, which has 24 bits per pixel. Lena, Baboon, Pepper, Lake, Barbara, Tiffany, Boats, and Airplane were used as the cover images. These standardized 512×512 RGB images from the USC-SIPI image database are frequently used in steganography techniques literature. These testing images are shown in Figure 6. Figure 6(a): the standardized 512×512 Lena image; Figure 6(b): the standardized 512×512 Baboon image; Figure 6(c): the standardized 512×512 Pepper image; Figure 6(d): the standardized 512×512 Lake image; Figure 6(e): the standardized 512×512 Barbara image; Figure 6(f): the standardized 512×512 Tiffany image; Figure 6(g): the standardized 512×512 Boats image; and Figure 6(h): the standardized 512×512 Airplane image.



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 6. The original 512×512 testing images: (a) Lena, (b) Baboon, (c) Pepper, (d) Lake, (e) Barbara, (f) Tiffany, (g) Boats, and (h) Airplane

4.2. Evaluation matrices

Evaluation and analysis of the performance of the steganography technique depends on the embedding capacity (payloads size) and stego image visual quality peak signal-to-noise ratio (PSNR) related variables. Stego image distortion shouldn't impair human vision, and the amount of payload that can be embedded is crucial. The size of message that can be incorporated into each algorithm is thoroughly tested. PSNR, bits per pixel (which indicates the number of embedded bits in each pixel) and mean-square error (MSE) (which represents the difference between the original image and the stego image) are common evaluation matrices for steganography techniques and measurement tools that are frequently used in image quality assessment.

The pure payload, which chooses how many pixels to use during the embedding process, serves as a gauge for the embedding capacity. PSNR evaluates the visual quality of the image. The PSNR gauges how closely the stego image resembles the original image. The term "pure payload" refers to the largest amount of bitstream sequences that can be concealed within a carrier image with a 512×512 8-bit pixel size. Higher visual quality and better performance are both correlated with higher PSNR values. To determine the PSNR value using (1):

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{1}$$

where the difference between the original image I and the stego image I' is represented by MSE. To determine the MSE using (2):

$$MSE = \left(\frac{1}{M\times N}\right)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(I(x,y)-\grave{I}(x,y))^2 \tag{2}$$

where M×N is the dimension of the cover image measured by pixels; I(x,y) is the pixel value of the cover image; and I'(x,y) is the pixel value of the stego image.

The embedding bitstream sequence determines the PSNR value, which is calculated using the average PSNR, the 1's bits PSNR, and the 0's bits PSNR. After embedding a stream of 1's bits, the PSNR for 1's bits and the PSNR for 0's bits were calculated. By averaging the PSNR of 100 randomly chosen embeddings of the bitstream of 0s and 1s, the average PSNR was calculated.

The performance metrics were the embedding capacity in a bit and the stego image visual quality (PSNR). The embedding capacity is measured by the pure payload and the embedding rate. The pure payload denotes to the actual size of the embedded secret message in bits, while the embedding rate denotes to the maximum size of the secret message in bits that can be embedded into the cover image of size 512×512. The embedding rate can be calculated using (3):

$$Embedding\ Rate = \frac{Maximum\ Hidding\ Capacity}{Cover\ Image\ Size * Bits\ per\ pixel} \times 100\% \tag{3}$$

4.3. Experimental results

The performance of the proposed technique was investigated, analyzed, and evaluated through experiments using C#.NET 2022. Several experiments were conducted to evaluate the performance of the proposed steganography technique. The relationship between the embedding rate and the proposed steganography technique's performance was studied; increasing the embedding rate increases the hiding capacity while decreasing the stego image quality. Moreover, a comparison between the proposed algorithm and other related embedding methods is presented. The experimental result generated from applying 2LSB on nine 24 RGB color images of size 512×512 is illustrated in Table 2.

Table 2. Experimental results generated from applying 2LSB on nine 24 RGB image

	1's bits 100% ER	1's bits 50% ER	Average PSNR 100% ER
Lena	43.53	46.55	46.32
Lake	43.36	46.37	46.62
Baboon	43.46	46.46	46.15
Barbara	43.36	46.73	47.23
Airplane	44.27	41.35	39.63
Peppers	43.36	46.39	45.71
Boats	43.47	46.49	45.36
Tiffany	31.35	42.35	42.07
Average	42.02	45.33625	44.88625

The experimental results show that increasing the embedding rate increase embedding capacity and decrease PSNR value. Distributed the secret message within the carrier image enhances steganography robustness. Several tests embed a sequence of 1'-bits with a size of 196.608 KB using the 2LSB for each color channel separately and for all channels together. Table 3 shows the experimental results generated from applying 2LSB to each color channel.

Table 3. Experimental results generated from applying 2LSB on RGB channels of 24 RGB image

	1st channel	2nd channel	3rd channel	ALL channel
Lena	50.21	51.11	52.17	51.14
Lake	50.09	51.07	51.92	51.08
Baboon	49.13	50.87	51.13	50.16
Barbara	48.23	50.17	50.61	50.23
Airplane	47.10	49.11	50.09	49.89
Peppers	50.05	51.87	51.89	51.09
Boats	50.06	51.95	52.12	51.42
Tiffany	49.08	50.18	50.38	49.68
Average	49.73	50.79	51.28	50.58

The experimental results show that, on average, 2-LSB method using Lena image outperforms in terms of PSNR value for each color channel spirited and all color channels. There is a tradeoff between the actual payload and the achieved PSNR. Increasing the actual payload value requires increasing the number of embedding regions, the number of divisions subblocks, or both, which decreases the PSNR value. Moreover, the payload at a fixed number of embedding regions and division subblocks should be lower than the maximum capacity. On the other hand, increasing the embedding capacity using different number of blocks leads to decrease PSNR value depending on the bit sequence in the secret message. Figure 7 shows this relationship between the embedding capacity and the PSNR using the Lena image. A comparison between the proposed steganography technique and existing state-of-the-art techniques in terms of embedding capacity and stego image quality is presented in Table 4.

As shown in Table 4, the proposed technique outperforms the other algorithms in terms of embedding capacity while maintaining a high PSNR level. Although technique outperforms the proposed technique in term of PSNR, it has the lowest embedding capacity. For example, odd/even distribution with henon map function [14] embeds 32,768 KB on average with a PSNR of 56.68 dB, while the proposed technique can embed more data up to 196.608 KB in the same image with PSNR higher than 50.58 dB. The outcomes show that the proposed technique outperforms the existing methods in terms of embedding capacity with a good PSNR value. The results shown in Table 4 make it abundantly clear that the proposed technique outperformed the existing ones in terms of embedding capacity and PSNR. Although the proposed data embedding technique seeks to significantly alter the carrier image content, it is noted that the stego image's visual quality is still acceptable and undetectable to the human eye.

Finally, to evaluate the proposed algorithm against steganalysis attacks, several experiments regarding the histogram and the human visual system (HVS) attack are constructed. These experiments aim to assess the effectiveness of the proposed technique against steganalysis attacks. The experiments involve comparing the original image with a stego image to evaluate the proposed technique. In addition, compare the histogram of the stego image with the original image histogram. shows the original carrier images, Lena, Baboon, Pepper, and Airplane with their histograms, along with the corresponding stego images with their histograms as shown in Figure 8 (in Appendix). Figure 8(a): the standardized 512x512 Lena image histograms, along with the corresponding stego images with their histograms; Figure 8(b): the standardized 512x512 Baboon image histograms, along with the corresponding stego images with their histograms; Figure 8(c): the standardized 512x512 Pepper image histograms, along with the corresponding stego images with their histograms; and Figure 8(d): the standardized 512x512 Airplane image histograms, along with the corresponding stego images with their histograms.

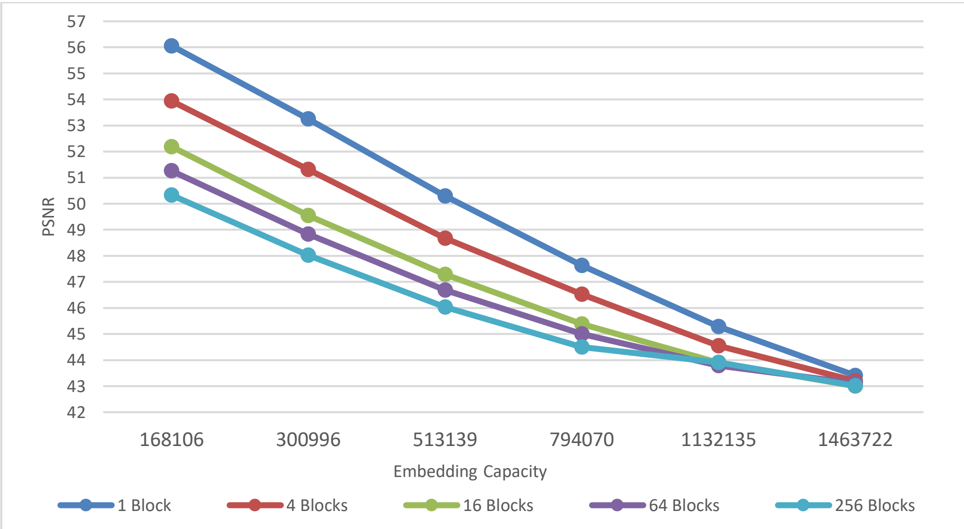


Figure 7. The effect of increasing payload on the PSNR for different number of blocks using Lena RGB image

Table 4. Comparison of PSNR values and embedding capacity values with others related works

Method	PSNR (dB)	Capacity (KB)
Odd/even distribution with henon map function [14]	56.68	32,768
3-D cat map [15]	48.98	196.608
The proposed technique in [16]	44.42	196.608
The proposed technique in [17]	54.7	524,288
Our proposed technique	50.58	196.608

4.4. Discussion

Increasing the number of embedding locations increases the maximum capacity for each color component while decreasing the PSNR value. Likewise, increasing the number of embedding locations within the same block leads to increasing the maximum capacity for each color component while decreasing the PSNR. In other words, there is always a tradeoff between the embedding capacity and the stego image's visual quality. The proposed technique focuses on improving both capacity and visual quality. The proposed technique can determine the best number of blocks and embedding locations that maximize the embedding capacity while achieving the highest image visual quality without the need for extra information for the location map. Only a few dominant RGB colors are used in the images of Lena, Tiffany, and Airplane to create a similar hue value and fluid color transitions. The totally RGB dominant hues in the Pepper image are more prominent than those with higher dispersion because of how bright the image's content is. For instance, the image of Lena has red and orange tones, the image of Tiffany has yellow tones with high brightness, and the image of the Airplane has a light color with high brightness. Baboon, Pepper, and Barbara are fully colored images that exhibit realistic RGB colors and hues and are very similar to natural images. The aim of embedding data with low distortion based on human eyes' perceptual sensitivity to the green color is in direct conflict with the abundance of green color in Baboon and Pepper images. This is because green light is the color that human eyes are most sensitive to, so when trying to embed the data, a carrier image that is greener will cause higher levels of data distortion.

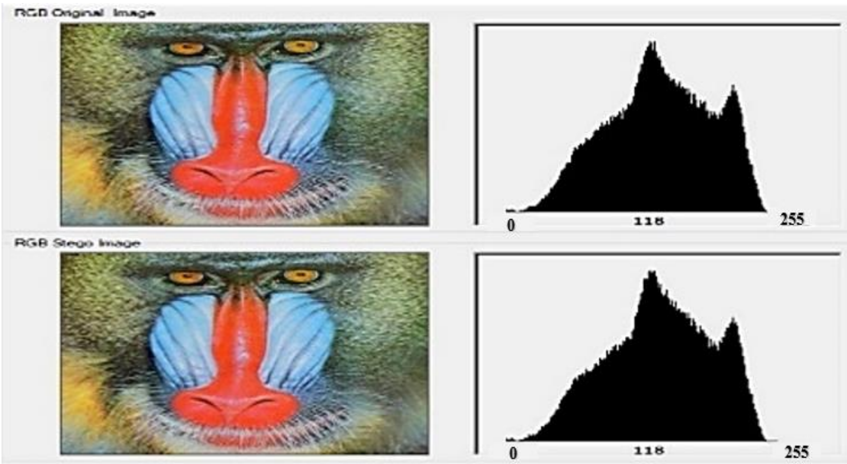
5. CONCLUSION

In this paper, a secure map-based crypto-stego technique is proposed to offer an effective solution for enhancing the security of messages hidden in images and improve embedding security and robustness. By utilizing the RSA encryption and the proposed unique embedding mechanism based on mac addresses, the technique ensures that only authorized parties can access the encrypted message. This approach eliminates the need for a location map, making it a more practical and efficient solution for secure message transmission.

In the future, the potential security threats that may arise from using this technique should also be investigated to ensure its effectiveness against various attacks. the concept of data embedding based on mac addresses will be extended to other applications to enhance their security. Overall, the proposed technique offers a promising solution for secure and efficient message transmission and can be further developed and applied in various domains.

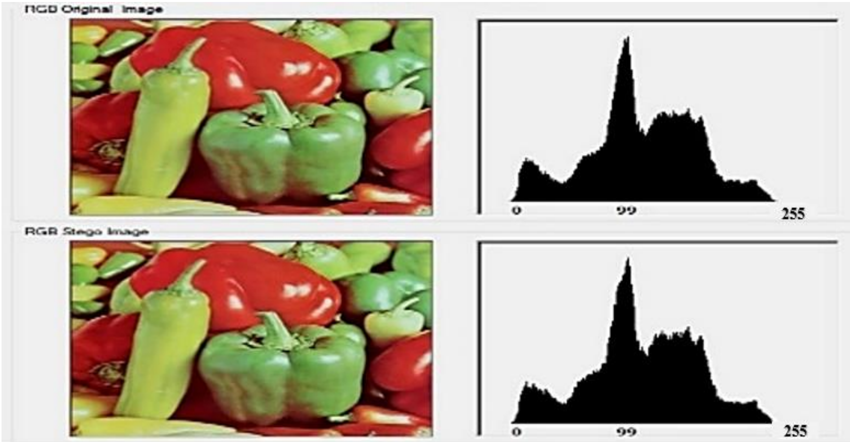
APPENDIX

(a)

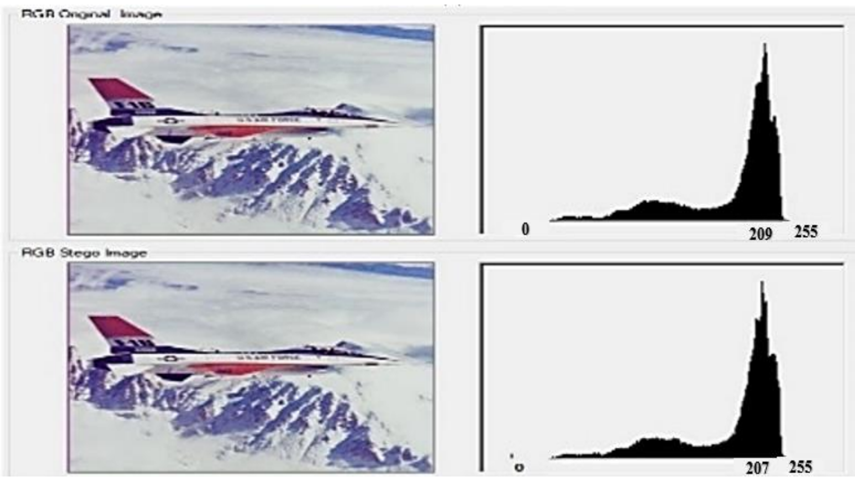


(b)

Figure 8. The original carrier images with their histograms, along with the corresponding stego images with their histograms; (a) Lena and (b) Baboon



(c)



(d)

Figure 8. The original carrier images with their histograms, along with the corresponding stego images with their histograms; (c) Pepper and (d) Airplane *(continue)*

ACKNOWLEDGEMENTS

This research is funded by University Sains Malaysia (USM) via external grant (number 304/PNAV/650958/U154).

REFERENCES

[1] C. Kim, C. N. Yang, J. Baek, and L. Leng, "Survey on data hiding based on block truncation coding," *Applied Sciences (Switzerland)*, vol. 11, no. 19, p. 9209, Oct. 2021, doi: 10.3390/app11199209.

[2] Q. Feng, L. Leng, C. C. Chang, J. H. Horng, and M. Wu, "Reversible Data Hiding in Encrypted Images with Extended Parametric Binary Tree Labeling," *Applied Sciences (Switzerland)*, vol. 13, no. 4, p. 2458, Feb. 2023, doi: 10.3390/app13042458.

[3] D. Kasasbeh, M. Anbar, G. Issa, B. A. Alabsi, and S. D. A. Rihan, "Adaptive 3D Reversible Data Hiding Technique Based on the Cumulative Peak Bins in the Histogram of Directional Prediction Error," *Electronics (Switzerland)*, vol. 12, no. 15, p. 3245, Jul. 2023, doi: 10.3390/electronics12153245.

[4] K. J. Giri, S. A. Parah, R. Bashir, and K. Muhammad, "Multimedia Security, Algorithm Development, Analysis and Applications," in *Singapore: Springer Singapore, 2021*, K. J. Giri, S. A. Parah, R. Bashir, and K. Muhammad, Eds., in Algorithms for Intelligent Systems. Singapore: Springer Singapore, 2021, doi: 10.1007/978-981-15-8711-5.

[5] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.

[6] D. Chadwick and B. Preneel, "Communications and multimedia security," *IFIP Advances in Information and Communication Technology*, vol. 175, 2005, doi: 10.1007/11382324.

[7] N. J. Daras and M. T. Rassias, "Computation, cryptography, and network security," in *Computation, Cryptography, and Network Security*, N. J. Daras and M. T. Rassias, Eds., Cham: Springer International Publishing, 2015, pp. 1–756, doi: 10.1007/978-3-319-18275-9.

[8] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13–14, no. C, pp. 95–113, Nov. 2014, doi: 10.1016/j.cosrev.2014.09.001.

[9] K. Patil, R. Gupta, and G. Singh, “Digital Image Steganalysis Schemes for Breaking Steganography,” *International Conference on Advances in Communication and Computing Technologies*, 2012, pp. 11-15.
[10] 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 Computing Electronics and Control)*, vol. 17, no. 5, pp. 2400–2409, Oct. 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.
[11] S. Ghoul, R. Sulaiman, and Z. Shukur, “A Review on Security Techniques in Image Steganography,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, pp. 361–385, 2023, doi: 10.14569/IJACSA.2023.0140640.
[12] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, “Hiding data using efficient combination of RSA cryptography, and compression steganography techniques,” *IEEE Access*, vol. 9, pp. 31805–31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
[13] M. Y. Mowafi, F. A. Al-Omari, and D. S. Kasasbeh, “Data hiding in color images using huffman coding and histogram modification,” *International Journal on Communications Antenna and Propagation*, vol. 9, no. 1, pp. 68–73, Feb. 2019, doi: 10.15866/irecap.v9i1.15668.
[14] M. M. Hashim and M. S. Mohd Rahim, “Image steganography based on odd/even pixels distribution scheme and two parameters random function,” *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 22, pp. 5977–5986, 2017.
[15] S. M. Hameed, Z. H. Ali, G. K. AL-Khafaji, and S. Ahmed, “Chaos-based Color Image Steganography Method Using 3 D Cat Map,” *Iraqi Journal of Science*, vol. 62, no. 9, pp. 3220–3227, Sep. 2021, doi: 10.24996/ijs.2021.62.9.34.
[16] A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, “Image steganography using least significant bit and secret map techniques,” *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 935–946, Feb. 2020, doi: 10.11591/ijece.v10i1.pp935-946.
[17] Z. A. Alwan, H. M. Farhan, and S. Q. Mahdi, “Color image steganography in YCbCr space,” *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 202–209, Feb. 2020, doi: 10.11591/ijece.v10i1.pp202-209.
[18] G. Umamaheswari and C. P. Sumathi, “A New Information Hiding Technique Matching Secret Message And Cover Image Binary Value,” *International Journal of Computer Science and Information Security*, vol. 15, no. 1, pp. 321–326, 2017.
[19] J. R. Vacca, “Computer and Information Security Handbook,” *Computer and Information Security Handbook*, pp. 1–1237, 2017, doi: 10.1016/B978-0-12-803843-7.15012-4.
[20] C. Kim, C. N. Yang, and L. Leng, “High-capacity data hiding for abtc-eq based compressed image,” *Electronics (Switzerland)*, vol. 9, no. 4, p. 644, Apr. 2020, doi: 10.3390/electronics9040644.
[21] S. Sun, “A novel edge based image steganography with 2k correction and Huffman encoding,” *Information Processing Letters*, vol. 116, no. 2, pp. 93–99, Feb. 2016, doi: 10.1016/j.ipl.2015.09.016.
[22] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed, and K. H. Jung, “A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement,” *Signal Processing: Image Communication*, vol. 50, pp. 44–57, Feb. 2017, doi: 10.1016/j.image.2016.10.005.
[23] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, “An Improved Level of Security for DNA Steganography Using Hyperelliptic Curve Cryptography,” *Wireless Personal Communications*, vol. 89, no. 4, pp. 1221–1242, Aug. 2016, doi: 10.1007/s11277-016-3313-x.
[24] S. S. Patil and P. S. Goud, “Enhanced Multi Level Secret Data Hiding,” in *In: An International Conference*, 2016, pp. 846–850.
[25] A. Ahmed and A. Ahmed, “A Secure Image Steganography using LSB and Double XOR Operations,” *International Journal of Computer Science and Network Security*, vol. 20, no. 5, p. 139, 2020.

BIOGRAPHIES OF AUTHORS

Dima S. Kasasbeh received the B.Sc. and M.Sc. degrees in Computer Engineering from Jordan University of Science and Technology, Jordan. in 2008 and 2014, respectively, and Ph.D. degree in Cyber security from National Advanced IPv6 Centre (NAv6), University Sains Malaysia. Her research interest includes data compression, image processing, information hiding, steganography, and cyber security. She can be contacted at email: Eng.dimakasasbeh@student.usm.my.

Bushra M. Al-Ja’afreh obtained a B.Sc. degree in Computer Information Systems from Jordan University of Science and Technology (JUST) in 2009 and M.Sc. degree in Computer Science from JUST too. She is currently pursuing a Ph.D. degree at the National Advanced IPv6 Centre (NAv6), University Sains Malaysia. Her research interests include cyber security, mutual authentication, signcryption, steganography, cloud computing, elliptic curve cryptography, and networks. She can be contacted at email: bushraaljaafreh@student.usm.my.

Mohammed Anbar obtained his Ph.D. in Advanced Internet Security and Monitoring from University Sains Malaysia (USM). He is currently a senior lecturer at National Advanced IPv6 Centre (NAv6), University Sains Malaysia. His current research interests include malware detection, web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, internet of things (IoT), and IPv6 security. He can be contacted at email: anbar@usm.my.

Iznan H. Hasbullah received the B.Sc. degree in Electrical Engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing the M.Sc. degree in Advanced Network Security. He worked as a software developer, the research and development consultant, a CTO, and a network security auditor prior to joining the National Advanced IPv6 Centre (NAv6), in 2010, as a research officer. His research interests include unified communication, network security, network protocols, and next generation networks. He can be contacted at email: iznan@usm.my.

Mahmoud Al Khasawneh received the B.Sc. degree in (Computer Science) Yarmouk University, Jordan 2003, Master (Computer Science) University Teknologi Malaysia (UTM), Malaysia 2013. Ph.D. (Computer Science) University Teknologi Malaysia (UTM), Malaysia 2018. He is currently Assistant Professor at School of Computing, Skyline University College, University City of Sharjah. His research interests include big data, artificial intelligence, security, image encryption, wireless networks, blockchain and internet of things. He can be contacted at email: mahmoud.alkhasawaneh@skylineuniversity.ac.ae.