Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption

Mohammed Mahdi Hashim\textsuperscript{1,4}, Ali Abdulwahhab Abdulrazzaq\textsuperscript{2}, Mohd Shafry Mohd Rahim\textsuperscript{1,3}, Mustafa Sabah Taha\textsuperscript{2,5}, Hiyam Nadhim Khalid\textsuperscript{6}, Sameer abdulsattar lafty\textsuperscript{1}

\textsuperscript{1}School of Computing, Facility of Engineering, University Technology Malaysia, Johor Bahru, Malaysia
\textsuperscript{2}Technical Instructors Training Institute, Middle Technical University, Baghdad, Iraq
\textsuperscript{3}UTM (IRDA) Digital Media Center, Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia
\textsuperscript{4}Faculty of Engineering, Uruk University, Baghdad, Iraq
\textsuperscript{5}Basrah Oil Training Institute, Ministry of Oil, Iraq
\textsuperscript{6}Faculty of Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM, Bangi, Selangor, Malaysia
E-mail: comp.mmh@gmail.com (Mohammed Mahdi Hashim)

Abstract. Recently, steganography has played an important part in the field of communication, especially in image steganography. The major points of image steganography are the image quality (imperceptibility) of the stego image and the security of the system towards stopping the recoverability of the secret data. A new steganography scheme based on two control random parameters and multi-level encryption can address the security challenge while the $P_{\text{Even}}/P_{\text{Odd}}$ classification can ensure the imperceptibility of the stego image. The objectives of study to increase the security and PSNR of the image by using the Huffman coding technique to compress the secret data prior to embedding; this will also ensure an increase in the payload capacity. The proposed scheme takes effect after encrypting and compressing the secret data. It is deployed when matching the secret bits with the LSB during embedding to determine 0 ($P_{\text{Even}}$) and 1 ($P_{\text{Odd}}$) while classifying the secret message to track and map each bit in the stego image. The results showed the embedding of the secret message based on $P_{\text{Even}}/P_{\text{Odd}}$ with two control random parameters and multi-level encryption to improve the steganography.

Keywords: Information hiding, multi-level encryption, Image steganography, Security, Image quality.

1. Introduction

Network revolution has made digital communication easy and has resulted in a remarkable increase in the number of active digital communication users. Meanwhile, it comes with security challenges with respect to data transmission over a public network. In order to secure data, two major processes (digital watermarking and steganography) have been used. Digital watermarking is an early technique
created for secure personal information transmission, and various methods have been proposed in this field to ensure the privacy of messages. Steganography refers to the science converting a message into a form that ensures a complete undetectability of any hidden piece of information in the carrier. Steganography ensures that a secret information is kept undetectable by the human visual system (HVS) [1]. The word ‘steganography’ is derived from the two Greek words ‘steganos’ (which means covered, concealed, or protected) and ‘graphein’ (which means write) [2]. Steganography differed from cryptography in the sense that it is mainly used to conceal the existence of secret information while cryptography is used to scramble a data in order to alter its meaning and quality to unauthorized users [3].

Steganography is another science and art of covert communication in a manner of complete silence of hiding information into where secret data is hidden in media carriers, so that secret information will be undetectable by human visual system (HVS), also will not be discovered [1][26]. The word of steganography comes from Greek, steganos means ‘covered’, protected or concealed ‘ and graphein means ‘write’ and that is refer to data hiding or secret writing [2][37]. Steganography is different from cryptography in the style, steganography is used to conceal the existence of secret data whilst cryptography is scrambled the data to change it’s the meaning and quality of cover where it looks meaningless to others [3].

To achieve a better steganographic performance, there are certain properties that are used to access the strengths and drawbacks of the employed steganographic techniques. Such properties include the security, imperceptibility, and capacity of the technique. The capacity of a steganographic technique implies the amount of embeddable secret data in the cover object without causing many distortions on the image quality. The capacity of a steganographic technique is generally represented in bit per pixel (bpp) [4]. Another important property of a steganographic technique is its security. A secure steganography technique must be resistant to steganalysis attacks. The final property of a steganographic technique is imperceptibility which implies the transparency and quality of the image. After concealing the secret data into the cover image, the quality and transparency will degrade into stego-images compared to the cover image. Hence, the stego image usually has almost the same quality as the original image. The PSNR is used to determine the imperceptibility of the stego image, where a higher PSNR indicates a good image quality [5][27].

With steganography, the data is concealed in a carrier such as a video, text, or audio [5]. Several steganography methods exist based on the type of carrier media, including (image, video, text, and audio) steganography [6,7]. The carrier media in steganography is referred to as the cover object while the hidden information is referred to as the payload capacity. The cover object used depends on the volume of secret data to be embedded, while the imperceptibility of the secret message depends on the systems’ robustness. Image is the commonest carrier media due to its wide usage in daily applications, as well as its high rate of redundancy. The stego image is the secret data which is hidden in a cover image. There are two major categories of image steganographic techniques - spatial domain and transform domain [8] [25].

To enhance the effectiveness of a steganography method, its security, capacity, and imperceptibility-related issues must be addressed. Among these areas of concern, the imperceptibility of the system is weighty as it relates to how difficult it is to differentiate the existence/absence of a secret message. The imperceptibility of the system can only be achieved through an odd/even pixels distribution format. Another area of concern is the security which relates to the ability of a steganography system to withstand external attacks. Finally, is the issue of capacity which relates to the maximum volume of information that can be safely embedded in a cover image without much distortions and a high level of data undetectability. The proposed method will address these areas of concern in the existing steganography systems [46,47].

This paper suggests an improvement on the steganography system based on the P.Even/P.Odd pixels scheme. The scheme employs a multi-level encryption system and 2 control random parameters for embedding secret texts with a high level of security and with neither a compromise on the stego images’ quality nor a secret message loss. There are three processes in the proposed system which includes a multi-level encryption scheme, an embedding scheme, and a retrieval/extraction scheme. Prior to the embedding scheme, the MLE is first used to encrypt the secret text before using the
Huffman coding algorithm to compress it to ensure an increase in the security and capacity respectively. In this paper, the major aim of the proposed scheme is to increase the PSNR of the image and ensure a high image security. With the proposed system, it is impossible to reveal the secret data to an intruder. The proposed scheme takes effect after encrypting and compressing the secret data. It is deployed when matching the secret bits with the LSB during embedding to determine 0 (P_Even) and 1 (P_Odd) while classifying the secret message to track and map each bit in the stego image. Additionally, the robustness of the system was also emphasized.

The rest of the study is constructed as follow sections: A state of the arts which related to image steganography is discussed in section 2 while the proposed scheme is described in section 3. In Section 4, the empirical result is given in more details. The last section of study is the conclusion.

2. State of the Art

A review of the existing literature shows that the LSB substitution scheme is the simplest and most common method for embedding secret text within the image. In the LSB substitution method, the secret text is first transformed to binary system (Bs) and used to substitute the LSB bits of the cover object (image). Regarding the gray-scale images whose pixels have just one value in the range of 0 to 255 and the bit deepness of 8 bits, there is no conversion of the secret data bits into binary bits as they are used directly to replace the LSB of the cover object (image). For the color images with 3 paths (RGB) and the bit deepness of 24 bits, the cover object (image) is first partitioned into 3 channels before using each channel for embedding the secret message. In the end, the three paths are combined to achieve the stego image. Being that a special form of the LSB substitution scheme is used in the proposed method in this work, it is therefore mathematically expressed with enough detail to enhance it a better understanding of the basic concept in section 3. The basic concept of the LSB-based steganography is further elucidated utilizing a simple instance: Assume B to be a grayscale image which consists of 8 pixels \(B=B_1, B_2, B_3, \ldots B_8\) and with the next values for their decimal and associated binary substitutions as given in table 1:

| Decimal No. | \(B_1\) | \(B_2\) | \(B_3\) | \(B_4\) | \(B_5\) | \(B_6\) | \(B_8\) |
|------------|---------|---------|---------|---------|---------|---------|---------|
| Binary No. | 0111011 | 1000110 | 0110000 | 1000000 | 0010100 | 1000101 | 0111011 |
| Secret letter = | A |

| Decimal No. | \(Z_1\) | \(Z_2\) | \(Z_3\) | \(Z_4\) | \(Z_5\) | \(Z_6\) | \(Z_8\) |
|------------|---------|---------|---------|---------|---------|---------|---------|
| Binary No. | 0111011 | 1000110 | 0110000 | 1000000 | 0010100 | 1000101 | 0111011 |
| Secret letter = | A |

Let X be the secret text, such that X= ‘A’ with the binary form X= 01000001. To embed X inside a given cover image B, the LSB of the pixels \(B=B_1, B_2, B_3, \ldots B_8\) are replaced with the bits of X (01000001) and the resulting pixel after the embedment is represented as \(Z=Z_1, Z_2, Z_3, \ldots, Z_8\) with their decimal and associated binary values as given in table 2.
The LSB in the pixels \([Z = Z_1, Z_2, Z_3, \ldots, Z_8]\) are the altered pixels which are the outcome of the embedding process. The embedding capacity can be increased by using more than 1 LSB but this will reduce a imperceptibility of the stego image and make it easily detectable by the HVS.

The embedding scheme is used to conceal the bits of a secret text into the LSB of randomly selected pixels. The pixel is selected based on the stego key that the sender shared with the recipient [9]. This technique can be easily implemented and can ensure the security of the hidden information.

Wu, et al. [10] suggested a novel noise-based steganography system for secret data embedding. The system depends on noise to confer security against statistical attacks and to increase embedding capacity. Sedighi, et al. [11] demonstrated the effect of choosing the cover image in advance on the capacity and security of steganography systems. Mohamed and Mohamed [9] opined that the capacity of a steganography system depends on the method used. The studies on the improvement of the embedding method based on the image edge area are still preliminary but promising [10].

An imperceptible image steganographic method which is based on the PBSA and M -LSB has been proposed by Muhammad et al. [33] for grayscale images. Here, the secret data is altered through encrypted and then, shuffled using a pattern-based bit shuffling algorithm (PBSA). Later, the M - LSB method is deployed to embed the encrypted message by scattering the secret message inside the image pixel. This makes the extraction of the hidden message more difficult for the attackers. The proposed scheme in this work is evaluated qualitatively and quantitatively to verify its effectiveness.

Khamy et al. have proposed a new steganography technique to minimize and solve the distortion on the stego -image. The proposed scheme uses two LSB steganography algorithms based on NEQR. The cover image is divided into blocks and each block hides one secret message bit. In the first LSB algorithm, the secret message bit is embedded by directly replacing the LSB bits of the cover image with the secret message bits, and then, the second LSB algorithm is a block LSB which embeds a secret message bit into a number of pixels that belong to one image block [16].

A secure image steganographic method which is based on the SKA-LSB substitution method with a multi-level of cryptography has been proposed by Khan et al. [15]. Here, the stego key is first encrypted using a two-level encryption algorithm (TLEA). Then, the secret data is encrypted with the multi-level encryption algorithm (MLEA) and before embedding into an image via an adaptive LSB substitution method with the aid of a stego key [15].

A three-phase intelligent method for color images has also been proposed for the improvement of the embedding payload and visual imperceptibility [28]. Prior to the embedding step in this method, a learning system (LS) is first applied, while the remaining the phases are applied post the embedding process. The number of embeddable secret bits inside the pixels is determined using an ANN and an adaptive GA. From the results, the proposed system successfully embedded a larger payload of up to 12 bpp with achieved a good visual quality.

A novel secure steganography method was put forward by [29] which was based on edge detection and Huffman Encoding. Coherent bit length was also adopted to embed different bits of secret data according to the values of the edge pixels values.

Singh et al [39] proposed a spatial domain-based color image steganography technique which is dependent on the hash function and edge detection technique. In this method, the canny edge is first applied on the color image to detect the edges before using the hash function algorithm to embed the secret text into the image. Different image formats such as -jpg, jpeg, bmp, tiff, etc can be used in the proposed scheme.

The review conducted so far showed that several techniques have been proposed and used for securing the privacy of secret information during transmission, with more focus on the payload, security, image quality, and computational complexity. Evidently, the existing techniques are either computationally complex or too naive. The less computationally complex methods cost-effective but cannot ensure a better security, image quality, and a higher payload. These drawbacks restrict their usage in top-secret communication systems. Contrarily, the more complicated methods can ensure a higher payload, security, and a better visual quality but they are computationally costly.
3. Proposition and Methodology

The suggested scheme and its main parts are discussed in detailed within this section. The pictorial details are aimed at presenting the novelty of the system to the readers in a clearer manner. The proposed framework is developed for application on the grayscale image based on multi-levels encryption and steganography. The proposed framework (unlike the other steganographic frameworks which have failed to achieve a suitable level of image quality and payload in a cost-effective way) can ensure a balance between payload, imperceptibility, computational complexity (CC) and robust (security) in a cost-effective way. The framework is ideal for application in the secure transmission of different secret bits, such as the transmission of electronic patient records (EPR) to the health care centers, private communication which demands privacy, as well as sharing of top-secret sensitive communication between intelligence units. Figure 1 depicts a schematic representation of the suggested scheme in this study.

Figure 1. The entire diagram illustrating the proposed scheme.

There are four main sub-algorithms in the proposed framework: 1) an MLE for the encryption of the secret text prior to the embedding process. The MLE was developed based on the inspiration derived from [40] on the need to increase the security of secret information by introducing several barriers to invaders during the retrieval of secret information. Aziz et al. [41] suggested the use of the AES algorithm to encrypt secret information along with an encrypted secret key prior to the embedding process as used by [42]. Meanwhile, the AES algorithm was proven to be computationally costly and hence, cannot be applicable in real-time security applications [43, 44]. 2) Using the Huffman coding technique to compress the secret text prior to embedding, this will also ensure an increase in the payload capacity. 3) Thied algorithm is the text embedding framework which adaptively conceals the encrypted secret data in the carrier to produce the stego images that will be transmitted to the related units or users. 4) The final algorithm is the retrieval/extraction algorithm which retrieves the intended information from the stego image at the receivers’ end for onward usage. Section 3 provides a brief overview of these algorithms.

3.1. Multi-level encryption (MLE)

To complicate the attempted retrieval of the secret data from the stego image more difficult for the attacker, the MLE was utilized to encode the secret text before embedding. The MLE is relatively good performance when compared to the RSA, AES, and others encryption schemes, and this is why it
was selected for this study [12]. There are 3 processes in the MLE, including an XOR operation, the division of the secret message bits into blocks, and the shuffling of the secret bits based on a secret key. The MLE concept can be better understood with a simple illustration: Assume ST to be a secret text (ST=“Z”) with its binary version (ST= 01011010). Then, apply the first operation in the MLE (XOR operation), i.e., ST = (S⊕11111111) = (01011010⊕11111111) = (10100101). Proceed with the second MLE operation which is the division of the secret bits into 4 blocks. This division is mainly performed for several reasons, including confusing an attacker when trying to find the actual pattern deployed. The concept followed here is as follows: Block 1 (M1) contains all the 8th and 4th bit of each byte of the secret message bits; Block 2 (M2) contains all the 7th and 3rd bits; Block 3 (M3) contains all the 6th and 2nd bits; and Block 4 (M4) contains the 5th and 1st bit, as presented in the table below.

| Block | Selected Bits | All Bytes |
|-------|---------------|-----------|
| B1    | 8th, 4th      | In all bytes of message |
| B2    | 7th, 3rd      | In all bytes of message |
| B3    | 6th, 2nd      | In all bytes of message |
| B4    | 5th, 1st      | In all bytes of message |

Now, concatenate on the four secret text blocks, i.e., STB = [B1, B2, B3, B4]; dividing MS = (10100101) into four blocks results in B1 = (10), B2 = (01), B3 = (10)2, and B4 = (01); hence, STB = (10011001). The third step will be performing the secret key based on shuffling. Behold key = "24521786" as shown in Figure 2. Shuffle the bits of STB = (10011001) and store the result bits in the variable MM. The procedure is showed in figure 2:

![Figure 2. A standard i.e. of secret pattern utilized in bits shuffling](image-url)

Shuffle the bits of STB= (10011001) and store the resultant bits into a variable MM. This procedure works as follows.

| Steps | Algorithm of Shuffle the Bits |
|-------|------------------------------|
| a.    | Take the i-th digit from the secret key |
| b.    | Separate the secret bit at the i-th digit position from STB |
| c.    | Concatenate the separated bit with MM and increment the value of i. |
| d.    | Repeat step (a) to (c) until all bits of SMB are shuffled. |

Then, perform this process on the STB bits, the 1st digit in the secret key is 3, hence, the 3rd bit from STB will stored in MM. The next digit of the secret key is 4, meaning that the 4th bit of STB is concatenated with MM. This process is continued for the remaining STB bits and the resultant bits achieved are MM= (01101010).

3.2 Huffman coding

One of the most famous data compression techniques is the Huffman Coding. It considers one kind of prefix code. Huffman coding was proposed by David A. Huffman in 1952 based on redundant letters in the text [45]. Huffman coding is used for lossless data compression. In the proposed method in this study, the Huffman coding algorithm was used to compress the secret information before the embedding scheme. The data compression step adopted in this study is very useful compared to the other techniques.
3.3. Embedding Algorithm

The EA is used to conceal the compressed secret data inside the LSB part of the carrier using a secret key. The embedding stage consists of 2 processes which are block selection and data embedding. These two processes run simultaneously to insert or hide the secret text into the carrier. Initially, the cover image was divided into 8×8 blocks of 64×64 pixels each. The selection process was done randomly under a Henon map function for the blocks and then, the pixels (Figure 3). The Henon function is applied to ensure the security of the system. The secret message is embedded in the LSB in accordance to the $P_{Even}$/$P_{Odd}$ classification scheme. The second objective of the proposed scheme is to ensure a minimal distortion of the embedded image and keep it as close as possible to the quality of the original image. This implies that the pixel that end with 1 in the LSB must have a pixel value of 0 or else 1.

Figure 3. Illustrating the random selection pixels in proposed scheme.

The embedding process, in this case, will insert the 1 to the $P_{Odd}$ pixels and the 0 to the $P_{Even}$ pixels. Figure 4 shows the standard embedding process.

Figure 4. Illustrative example of proposed embedding algorithm (EA).

The embedding of the 1 value of the secret bits to the 1 value of pixel ensures no alteration in the image quality, as shown in Figure 4. However, the embedding of the 1 value of the secret bit to the 0 value of the LSB pixel can alter the pixel value (replaced 0 by 1); also, when 0 value is embedded to 1 value, the pixel value is replaced by 0, as represented in the third example. So, there is an increase in the imperceptibility of the proposed method. The major steps of the embedding mechanism are illustrated in the EA.
**Embedding Algorithm**

Input: Cvr_Img (Cover Image), ST (Secret text).
Output: S (Stego Image).

Begin
1. Read and convert ST into binary.
2. Apply the MLE on from step 2
3. Using Huffman coding with the result of step 2.
4. Calculate the size of ST.
5. Choose Cvr_Img (512 X 512).
6. Divide Cvr_Img into 64 blocks.
7. Select random no. using Henon Map Function.
8. Select one block of 64 via use Henon map function.
9. Used the second parameter of Henon Map to select the destination pixel.
10. Generate H vector and arrange it accordingly to \( P_{Even}/P_{Odd} \).
11. Allusion to the LSB of each pixel.
12. loop from P=1: N.
13. Obtained message bit (0 or 1).
14. If ST is 0 and pixel is \( P_{Even} \), do nothing
15. If ST = 0 and pixel is \( P_{Odd} \), replace via 0 the value of LSB position.
16. If ST is 1 and pixel is \( P_{Even} \), replace via 1 the value of LSB location.
17. If ST is 1 and pixel is \( P_{Odd} \), do nothing.
18. P = P +1
19. Return S.

**Extracting Algorithm**

The extracting process is aimed at retrieving the data from the LSB pixels and at the same time follow the designed procedure for the embedding phase. The extracting process is performed by the recipient of the secret message using a stego key shared with the sender. The extracting process is a reverse of the embedding process, meaning that the LSB components of the pixels are collected to determine if the pixels are \( P_{Even} \) or \( P_{Odd} \). The \( P_{Even} \) pixel has a value of 0 in the LSB position because of the binary impact value, while the \( P_{Odd} \) pixel has a value of 1. Most of the variable information are reflected by the image and block partitioning in addition to the fractions of the secret message. Such information is referred to as public information, but it is considered as a private information if accompanied by an embedding process. The embedding and extracting processes are aimed at achieving two major objectives of security and imperceptibility (Figure 5).

![Figure 5. Two contributions within proposed scheme.](image-url)
4. Result and Discussion
In this study, a technique for the embedding of secret texts into cover images with a higher level of security was proposed. The performance of the proposed scheme was evaluated using several tests with respect to its stego-image accuracy, resistance to steg analysis, embedding efficiency, and runtime performance. The simulation part of the scheme was performed on a MATLAB 10 platform running on Windows 10. Eight standard color images of 512 x 512 pixels were used as the carrier to generate the stego-image. During the experiments, the image quality (PSNR) and embedding efficiency of the proposed method was benchmarked against different methods.

The stego images’ quality was measured by the peak signal to noise ratio (PSNR), a common performance determinant for image steganographic techniques [14]. The PSNR is calculated by first determining the mean square error (MSE) using Eq. 1:

\[
MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2
\]

The MSE is a measure of the average squared difference between the original (I) and stego images (S). N x N represents the row and column sizes of the cover image. Then, the PSNR value is determined using Eq. 2; a higher PSNR value is ideal as it suggests a superiority of the signal to that of noise.

\[
PSNR = 10 \log_{10} \left( \frac{MAX^2}{MSE} \right)
\]

where MAX represents the maximum possible value of the image pixel. The results of the evaluation showed a PSNR value of >66 times better than that of the HVS threshold between the cover and stego images. Thus, the proposed algorithm was observed to achieve less embedding-related visual distortion. The embedding capacity as earlier defined is the maximum amount of embeddable secret data in a carrier expressed as the number of bits to be hide into a carrier. The embedding capacity efficiency (ECE) is calculated using Eq. 3:

\[
ECE = \frac{\text{The number of message bits}}{\text{The number of cover image pixels}} \text{ (bit /pixel)}
\]

The ECE is evaluated via a percentage of a secret bits embedded in all the pixels of the carrier. To benchmark the outcome of this work with the existing literature, the proposed scheme was evaluated using 4 images as presented in Table 3, while Table 4 presented the outcome of the evaluations.

| Table 3. Benchmark image dataset. |
|----------------------------------|
| lena1                             |
| pepper2                           |
| baboon3                           |
| cameraman4                        |
The results that are obtained from these empirical are recorded briefly in Table 4, Table 5 and Table 6. The text message has been utilized as secret message.

Table 4. Comparison between a proposed scheme and conferences papers based on PSNR parameter.

| Ref          | Evaluation Parameters | Lena | Baboon | Pappers | Cameraman |
|--------------|-----------------------|------|--------|---------|-----------|
| Color mapping [12] | ST (Bits)             | 131072 | N/A    | 131072 | N/A       |
|              | PSNR (dB)             | 61.97  | N/A    | 60.97  | N/A       |
| FPGA [13]    | ST (Bits)             | 14856  | 14856  | N/A    | N/A       |
|              | PSNR (dB)             | 54.14  | 54.14  | N/A    | N/A       |
| PRT [22]     | ST (Bits)             | 4432   | 8768   | 4296   | N/A       |
|              | PSNR (dB)             | 61.30  | 60.08  | 61.37  | N/A       |
| Logistic map [23] | PSNR (dB)           | 233016 | N/A    | 233016 | N/A       |
| Ref [35]     | ST (Bits)             | 131072 | 131072 | N/A    | N/A       |
|              | PSNR (dB)             | 51.17  | 51.17  | 51.19  | N/A       |
| Ref [36]     | ST (Bits)             | 16000  | 16000  | N/A    | 16000     |
|              | PSNR (dB)             | 62.14  | 62.01  | N/A    | 62.40     |
| Proposed Scheme | PSNR (dB)         | 66.62  | 67.68  | 67.22  | 65.84     |

Table 5. Comparison between a proposed scheme and important studies based on PSNR parameter.

| Ref          | Evaluation Parameters | Lena | Baboon | Pappers | Cameraman |
|--------------|-----------------------|------|--------|---------|-----------|
| CISSKA [15]  | Capacity (Bits)       | 64000 | 64000  | N/A    | N/A       |
|              | PSNR (dB)             | 55.89 | 47.87  | N/A    | N/A       |
| NEQR [16]    | Capacity (Bits)       | 262144 | 262144 | 262144 | 262144   |
|              | PSNR (dB)             | 50.84 | 50.37  | 50.62  | 51.61     |
| Predictive edge [17] | Capacity (Bits)   | N/A  | 30000  | 38657  | N/A       |
|              | PSNR (dB)             | N/A   | 53.02  | 50.29  | N/A       |
| HOLM [18]    | Capacity (Bits)       | 262100 | 262100 | 262100 | N/A       |
|              | PSNR (dB)             | 40.5267 | 39.2301 | 40.5133 | N/A       |
| FPGA [19]    | Capacity (Bits)       | 262144 | 262144 | 262144 | N/A       |
|              | PSNR (dB)             | 55.48  | 55.54  | 55.18  | N/A       |
| ABC [20]     | Capacity (Bits)       | 131072 | 131072 | 131072 | N/A       |
|              | PSNR (dB)             | 56.39  | 56.39  | 57.37  | N/A       |
| Flipping [21] | Capacity (Bits)      | 262144 | 262144 | 262144 | N/A       |
|              | PSNR (dB)             | 51.27  | 51.28  | 51.28  | N/A       |
| Ref [24]     | Capacity (Bits)       | 150000 | 56000  | 105000 | N/A       |
|              | PSNR (dB)             | 49.60  | 49.80  | 49.20  | N/A       |
| Ref [28]     | Capacity (Bits)       | 150000 | 56000  | 150000 | N/A       |
|              | PSNR (dB)             | 52.30  | 52     | 52     | N/A       |
| 2k correction [29] | Capacity (Bits)  | 38427  | 108074 | 35946  | N/A       |
|              | PSNR (dB)             | 63.48  | 58.37  | 63.23  | N/A       |
| Bit Flipping [38] | Capacity (Bits) | 262144 | 262144 | 262144 | N/A       |
|              | PSNR (dB)             | 48.27  | 47.33  | 46.34  | N/A       |
| Ref [39]     | Capacity (Bits)       | 34296  | 34296  | 34296  | 34296     |
|              | PSNR (dB)             | 39.63  | 41.58  | 38.65  | 41.60     |
| Proposed Scheme | Capacity (Bits)  | 262144 | 262144 | 262144 | 262144     |
|              | PSNR (dB)             | 66.62  | 67.68  | 67.22  | 65.84     |
To compare the performance of the proposed scheme with other methods, the achieved PSNR values are graphically represented in figure 6 and figure 7.

![Figure 6. Comparison of PSNR](image)

![Figure 7. Comparison of PSNR](image)

The experimental results in terms of the PSNR and a payload capacity of 1 (i.e. 1 bit per pixel for the proposed method, are shown in Table 4 [30-34]. The PSNR value of the proposed scheme was higher compared to the other works since it manipulated the LSB of each pixel value to conceal a secret text.

| Carrier Image | cyclic Code Ref [30] | KT algorithm Ref [31] | Ref [32] | Ref [33] | Ref [34] | Proposed scheme |
|---------------|-----------------------|-----------------------|----------|----------|----------|-----------------|
| Lena carrier  | 56.01                 | 55.91                 | 59.008   | 51.13    | 65.09    | 66.62          |
| Pappers carrier | 55.88         | 55.85                 | 58.881   | N/A      | N/A      | 67.68          |
| Baboon carrier | N/A              | 55.933                | 58.938   | 51.15    | N/A      | 65.84          |

However, a major limitation of the proposed scheme relates to its capacity; a higher capacity would degrade the quality of the image. The other limitation of the method is that only 4 datasets were tested with the method.

Based on the empirical results, the proposed method achieved a lower rate of image distortion (imperceptibility) and a better embedding capacity compared to the benchmarking schemes. Thus, it could be concluded that the proposed scheme performed better than the benchmarking schemes in terms of embedding capacity and imperceptibility. Some of the weaknesses of the proposed scheme will be considered for improvement in the future works.
5. Conclusions and Recommendations

In this paper, an improved steganography system which utilizes LSB pixel values based on $P_{\text{Even}}/P_{\text{Odd}}$ was proposed in the spatial domain. The system was proposed to maintain the security of secret texts based on two control random parameters and multi-level encryption. To increase the payload capacity of the system, the secret data was first compressed using Huffman coding scheme. The secret text was manipulated prior to the embedding phase to increase embedding capacity and security of the system. The major objective of the proposed system is to achieve stego images with a higher PSNR to ensure resistance to any form of attack. The system ensures that the secrecy of the secret data is intact and inaccessible to an intruder. The proposed scheme takes effect after encrypting and compressing the secret data. It is deployed when matching the secret bits with the LSB during embedding to determine 0 ($P_{\text{Even}}$) and 1 ($P_{\text{Odd}}$) while classifying the secret message to track and map each bit in the stego image. The results showed that the proposed work achieved an improved steganography.

References

[1] Provos N and Honeyman P 2003 Hide and seek: An introduction to steganography IEEE security & privacy 99 32-44.
[2] Al-Mualla M and Al-Ahmad H 2008 Information hiding: steganography and watermarking. Proceedings of the IEEE.
[3] Bhuvanaya R, Vijayalakshmi K, Uma S and Suresh A 2018 Secret data sharing using steganography and image processing.
[4] Nayak D K and Bhagyati C 2013 A threshold-LSB based information hiding scheme using digital images In Computer and Communication Technology (ICCCT) 4th International Conference on (pp. 269-272) IEEE.
[5] Hashim M, Rahim M, Shafry M and Alwan A A 2018 A review and open issues of multifarious image steganography techniques in spatial domain Journal of Theoretical & Applied Information Technology 96.
[6] Bhattacharyya D, Kim T H and Dutta P 2012 A method of data hiding in audio signal Journal of the Chinese Institute of Engineers 35 523-528.
[7] Dumitrescu S, Wu X and Memon N 2002 On steganalysis of random LSB embedding in continuous-tone images In Image Processing International Conference on (Vol. 3, pp. 641-644) IEE.
[8] Agilandeeswari L, Brindha K, Sunny S and Muralibabu K 2013 A novel architecture for information hiding using HMAC-MD5 International Journal of Engineering & Technology 2 134.
[9] Ali A H, Mokhtar M R and George L E 2017 Enhancing the hiding capacity of audio steganography based on block mapping Journal of Theoretical & Applied Information Technology 95.
[10] Wu B, Chang M P, Shastri B J, Ma P Y, and Prucnal P R 2016 Dispersion deployment and compensation for optical steganography based on noise IEEE Photonics Technology Letters 28 421-424.
[11] Sedighi V, Cogranne R and Fridrich J 2016 Content-adaptive steganography by minimizing statistical detectability IEEE Transactions on Information Forensics and Security 11 221-234.
[12] Al-Omari Z Y and Al-Taani A T 2017 Secure LSB steganography for colored images using character-color mapping. In Information and Communication Systems (ICICS), 8th International Conference on (pp. 104-110) IEEE.
[13] AlWatyan A, Mater W, Almutairi O, Almutairi M, Al-Noori A and Abed S E 2017 Security approach for LSB steganography-based FPGA implementation In Modeling, Simulation, and Applied Optimization (ICMSAO), 2017 7th International Conference on (pp. 1-5) IEEE.
[14] Bansod S, and Bhure G 2014 Data encryption by image steganography Int. J. Inform. Comput. Technol. Int. Res. Publ. House 4 453-458.
[15] Muhammad K, Ahmad J, Rehman N U, Jan Z and Sajjad M 2017 CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method Multimedia Tools and Applications 76 8597-8626.

[16] Jiang N, Zhao N and Wang L 2016 LSB based quantum image steganography algorithm International Journal of Theoretical Physics 55 107-123.

[17] Chakraborty S, Jalal A S and Bhatnagar C 2017 LSB based on blind predictive edge adaptive image steganography Multimedia Tools and Applications 76 7973-7987.

[18] Huang H and Zhou Z 2016 An Image Steganography Algorithm based on the Quantitative Features of Higher Order Local Model International Journal of Security and Its Applications 10 83-92.

[19] Elshazly E A, Safey A and El-Kordy O Z M 2016 FPGA Implementation of Robust Image Steganography Technique based on Least Significant Bit (LSB) in Spatial Domain International Journal of Computer Application 146.

[20] Banharnsakun A 2018 Artificial bee colony approach for enhancing LSB based image steganography Multimedia Tools and Applications 1-14.

[21] Kumar R and Chand S 2016 A reversible data hiding scheme using bit flipping strategy Journal of Discrete Mathematical Sciences and Cryptography 19 331-345.

[22] Burie J C, Ogier J M and Loc C V 2017 A spatial domain steganography for grayscale documents using pattern recognition techniques In Document Analysis and Recognition (ICDAR), 2017 14th IAPR International Conference on (Vol. 9, pp. 21-26) IEEE.

[23] Ulker M and Arslan B 2018 A novel secure model: Image steganography with logistic map and secret key In Digital Forensic and Security (ISDFS), 2018 6th International Symposium on (pp. 1-5) IEEE.

[24] Ou B, Li X, Zhao Y and Ni R 2015 Efficient color image reversible data hiding based on channel-dependent payload partition and adaptive embedding Signal Processing 108 642-657.

[25] Hong, W 2012 Adaptive reversible data hiding method based on error energy control and histogram shifting Optics Communications 285 101-108.

[26] Li X, Li J, Li B and Yang B 2013 High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion Signal processing 93 198-205.

[27] Li J, Li X and Yang B 2013 Reversible data hiding scheme for color image based on prediction-error expansion and cross-channel correlation Signal Processing 93 2748-2758.

[28] El-Emam N N and Al-Diabat M 2015 A novel algorithm for colour image steganography using a new intelligent technique based on three phases Applied Soft Computing 37 830-846.

[29] Sun S 2016 A novel edge-based image steganography with 2k correction and Huffman encoding. Information Processing Letters 116 93-99.

[30] Rodrigues A and Bhise A 2017 Reversible image steganography using cyclic codes and dynamic cover pixel selection In Wireless Communications, Signal Processing and Networking (WiSPNET), 2017 International Conference on (pp. 509-513) IEEE.

[31] Astuti Y P, De Rosal Ignatius Moses Setiadi E, Rachmawanto H and Sari C A Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB.

[32] Gulappagol L and ShivaKumar K B 2017 Secured data transmission using knight and LSB technique In Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), 2017 International Conference on (pp. 253-259) IEEE.

[33] Seyyedi S A, Sadau V and Ivanov N 2016 A Secure Steganography Method Based on Integer Lifting Wavelet Transform IJ Network Security 18 124-132.

[34] Burie J C, Ogier J M, and Loc C V 2017 A spatial domain steganography for grayscale documents using pattern recognition techniques In Document Analysis and Recognition (ICDAR), 2017 14th IAPR International Conference on (Vol. 9, pp. 21-26) IEEE.

[35] Oravec J and Turán J 2017 Substitution steganography with security improved by chaotic image encryption In Informatics, 2017 IEEE 14th International Scientific Conference on (pp. 284-288) IEEE.
[36] Maji G, Mandal S, Sen S and Debnath N C 2018 Dual image based LSB steganography In Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), 2018 2nd International Conference on (pp. 61-66) IEEE.

[37] Sharma V K, Srivastava D K and Mathur P 2018 Efficient image steganography using graph signal processing IET Image Processing 12 1065-1071.

[38] Sahu A K, Swain G and Babu E S 2018 Digital Image Steganography Using Bit Flipping Cybernetics and Information Technologies 12 69-80.

[39] Singh S and Datar A 2015 Improved hash-based approach for secure color image steganography using canny edge detection method International Journal of Computer Science and Network Security (IJCNS) 15 92.

[40] El-Emam N N 2015 New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization Computers & Security 55 21-45.

[41] Aziz M, Tayarani-N M H and Afsar M 2015 A cycling chaos-based cryptic-free algorithm for image steganography Nonlinear Dynamics 80 1271-1290.

[42] Nguyen T D, Arch-Int S and Arch-Int N 2016 An adaptive multi bit-plane image steganography using block data-hiding Multimedia Tools and Applications 75 8319-8345.

[43] Jinomeiq L, Baoduui W and Xinmei W 2007 One AES S-box to increase complexity and its cryptanalysis Journal of Systems Engineering and Electronics 18 427-433.

[44] Liu Q, Li P Y, Zhang M C, Sui Y X and Yang H J 2015 A novel image encryption algorithm based on chaos maps with Markov properties Communications in Nonlinear Science and Numerical Simulation 20 506-515.

[45] Huffman D A 1952 A method for the construction of minimum-redundancy codes Proceedings of the IRE 40 1098-1101.

[46] Mahdi Hashim M O H A M M E D, RAHIM M and Shafry M 2017 Image steganography based on odd/even pixels distribution scheme and two parameters random function Journal of Theoretical & Applied Information Technology 95 22.

[47] Domain W T I S 2018 A review and open issues of diverse text watermarking techniques in spatial domain Journal of Theoretical and Applied Information Technology 96.

Acknowledgments
This work is a part of wide research supported by the University Technology Malaysia (UTM), Johor Bahru, Malaysia. The authors would like to thank the reviewers for their insightful comments and helpful suggestions for a better research.