High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method

Rana Sami Hameed[1], Siti Salasiah Mokri[2]
Department of Electrical,
Electronic and Systems Engineering
Faculty of Engineering and Built Environment
Universiti Kebangsaan Malaysia
Selangor, Malaysia

Mustafa Sabah Taha[3]
Missan Oil Training Institute, Ministry of Oil, Iraq

Mustafa Muneeb Taher[4]
College of Computing Science & Information Technology
University Tenaga Nasional, Selangor, Malaysia

***Abstract*—Data security is becoming an important issue because of the vast use of the Internet and data transfer from one place to another. Security of these data is essential, especially when these data represent critical information. There are several techniques used to hide these data, such as encryption. Steganography can be utilised as an alternative to encryption because encryption is susceptible to data modification during transmission. Steganography is the hiding data on a cover multimedia such as images, audio, and video. The technique allows security for data transmission so unwanted third parties cannot notice the hidden data. The challenge of steganography is the trade-off between the hidden data's payload capacity and the system's imperceptibility and robustness. If the hidden data increases, the imperceptibility and the robustness will be decreased. This case is a big challenge in this digital world where social media, Internet, and data transfer are used hugely. Because of this, this paper proposes using a modified Least Significant Bit (LSB) method for the embedding process called Multi-Layer Least Significant Bit Exchange Method (MLLSBEM). This proposed algorithm uses the AES encryption method to encrypt the secret text and then uses Huffman coding to compress the encrypted message as pre-processing data. The proposed study seeks to strike a compromise between important issues, provide maximum payload capacity, and retain high security, imperceptibility, and reliability for secret communication Using image processing and steganography techniques. Simulation findings demonstrate that the suggested method is superior for existing PSNR, SSIM, NCC, and payload capacity investigations. The proposed method is immune to the histogram, chi-square, and HVS attacks.**

***Keywords*—Information hiding; steganography; cryptography; multi-layer security; high capacity component**

I. Introduction

Increasing the use of data transfer from one place to another, especially with the improvement of the Internet and online transferring tools, the concern of data privacy and security becomes an important issue [1]. Third-party attacking of data is a risk. This circumstance means that attackers can reach the sender's data in many ways leading to the possibility of malicious threats, eavesdropping, and other malicious activities [2]. Three common techniques are used in this field to ensure data security and privacy: steganography, cryptography, and the watermarking technique. These three techniques are used to ensure security in different ways [3]. In steganography, the required data, which can be called the secret data that is to be sent, is hidden within media data such as images, video, audio, and protocol. On the other hand, in cryptography, the required data to be sent is coded with a predefined code known by both the transmitter and the receiver while in watermarking, the secret data does not change, but it is carried on multimedia data, such as images, to be sent to the required receiver to ensure confidentiality [4]. Image steganography is a widely used technique because the secret data does not change as in cryptography and does not appear as in watermarking. Image steganography can hide the secret data in its original format within the image by using a stego-key at the transmitter. The same stego-key is used at the receiver to recover the hidden data from the stego-image, as shown in Fig. 1.

Image steganography system has become the most popular research area than the other types of systems because of the availability, ease to use by users, and the ability to hold a large amount of data, in addition to the difficulty of noticing the hidden data by the unwanted third party [5].

However, using image steganography nowadays, where a high volume of data exchange is required, becomes a challenge, in particular to the issue of the payload capacity. Besides this, the trade-off challenge between payload capacity, security, and visual image quality is also a critical issue. These criteria imply that when the hidden data increases, the security of the steganography technique will decline and vice versa. Accordingly, as the amount of hidden data increases, the imperceptibility will decrease as well [6].

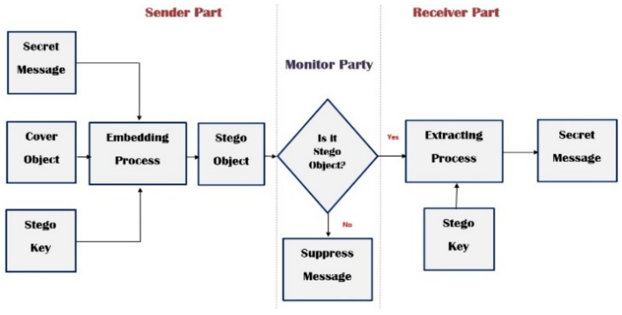


Fig. 1. The General Principle of the Image Steganography System.

Several methods and techniques have been used in the literature to overcome these challenges. The most straightforward and efficient method uses the Least Significant Bit (LSB) as an embedding technique, as in Gupta et al. [7] and Hameed et al. [8]. They propose LSB with some encryption techniques to ensure the system's security. Maurya & Gupta [9] suggested a method based on the adaptive LSB substitution steganography technique. In this method, the aim is to divide the image into two segments - non-sensitive and sensitive parts based on texture analysis. The majority of the bits in the non-sensitive area are used to hold secret messages and other bits in the sensitive area. The main advantages of this method are achieving both high payload capacity and imperceptibility.

The challenge of using LSB is the payload capacity of the system. Nowadays, most researchers, according to the best of our knowledge, use Artificial Intelligence (AI) and Deep Learning (DL) algorithms to overcome the capacity challenge. The study by [10] proposed the General Adversarial Networks (GAN) as a form of DL algorithm. GAN employs game theory to train the generative model using an adversarial method based on two networks for generator and discriminator. The data is fed into the generator model, and the result is approximately equal to the input image. The discriminator networks determine the class of the created images. Using GAN in steganography allows for increasing the payload capacity of the system, but this approach increases the complexity of the developed steganography technique. This complexity arose from the training data requirement before applying steganography to train the model. To overcome this, Volkhonskiy et al. [11, 12] proposed a Steganographic GAN (SGAN) based on DCGAN to simplify the training process as in Shi et al. [13] and [14]. They propose four fractionally convolutional layers followed by a functional layer with Hyperbolic tangent activation with base WGAN. The proposed model is based on multi-layer steganography but also depends on eavesdropping on the generator. Simulation results show that using four layers increases the receiver's prediction complexity, so Yang et al. [15] and [16] use the SGAN with three layers process. They use pixel-wise segmentation. This use reduces the complexity of the process but increases the discriminator and generator losses.

The work in [17] uses fuzzy logic to make decisions based on local statistical, texture, and brightness information-based feature vectors. The fuzzy logic can be used instead of AI algorithms to reduce the decision complexity. Simulation results show that at higher embedding rates, the approach helps to eliminate stego-image distortions. The study by [18] explained another fuzzy-based technique in which, before the real embedding process, the cover pixel selection is based on fuzzy pixel classification, and the secret message is translated to a mode of fuzzy data.

Fuzzy logic can improve stenographic techniques in various ways, especially when there is vagueness in the image textures. It benefits the system by recognising appropriate visual patterns quickly and avoiding irreversible complexities. However, adding a fuzzy process to select the embedding process affects the system's capacity.

This paper proposed a Multi-Layer Least Significant Bit Exchange Method (MLLSBEM) algorithm as an effective hiding method to embed a high volume of security data into an image without affecting the security and imperceptibility of the system. Thus, several contributions of this paper can be summarised as the following:

- This paper proposes a hiding method based on multi-layer operations, which is Advanced Encryption System (AES) technique to enhance security. Furthermore, the paper uses Huffman coding to increase the payload capacity of the hidden data.
- The propose method is based on Linear Significant Bit Exchanging Method (LSBEM) that is a simple, secure, and efficient method used with image steganography based on the resulting image quality.
- The evaluation of the proposed multi-layer algorithm is performed on grey-scale and colour images to generalise its use and efficiency.

The remaining of this paper is structured as follows: the proposed algorithm description is discussed in Section II. The overall methodology and simulation parameters are mentioned in Section III. Simulation results and discussion based on performance metrics are presented in Section IV. Finally, the conclusion and some future work discussions are mentioned in Section V.

II. The Proposed Algorithm

This newly proposed technique aims to have a stego-image like the original image with high capacity hidden data. The aim is to satisfy the imperceptibility of maintaining a high PSNR value. The proposed MLLSBEM algorithm depends on two methods: designing a new LSBEM and using Implicit Key Generation (IKG). The proposed LSBEM technique's principle is to expand the LSB substitution method to exchange the secret message bits with the cover image's pixels using the shared IKG between the sender and receiver.

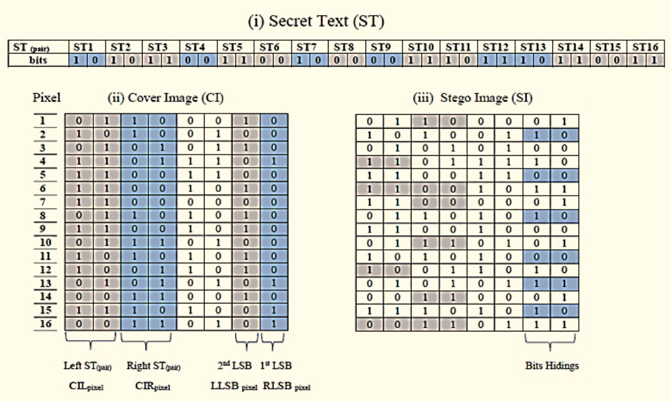
Algorithm 1: The proposed hiding algorithm

```
If STB1 = CIPLpixel,
        The BL of the pixel is set to ‘1'; otherwise, it is set to ‘0'.
If STB2 = CIPRpixel,
        The BR of the pixel is set to ‘1'; otherwise, it replaces it with a ‘0'.
If either BL or BR = 0,
        The next cover pixel's 2-LSBs are substituted with the previously unmatched secret bit pair (i.e., STB1 or STB2).
If BL and BR = 0,
The skipped mapped block. “there is no mapping”.
```

Algorithm 1 expresses the proposed algorithm to hide the secret payload in the carrier image. While Fig. 2 depicts the proposed scheme of the concealing process. As shown, the Secret Text Bits (STB) are initially grouped into two secret bit pairs, i.e. STB1 (1,0), STB2 (1,0), and STB3(1,1), as shown in Fig. 2(i). Similarly, all the cover image pixels bits are divided into pairs, as shown in Fig. 2(ii), with Left Pair called Cover Image Left Pixel (CIPLpixel) and the Right Pair called Cover

Image Right Pixel (CIPRpixel). CIPLpixel, pixel denotes the cover pixel's 7th and 8th Most Significant Bits (MSBs), while CIPRpixel denotes the 5th and 6th MSBs.

The pixel on the cover of the secret text bits pair would be mapped using CIPLpixel, and CIRpixel bits. Similarly, the 1st and 2nd LSBs of a cover pixel are represented by Right Bit (1LSBp) and Left Bit (2 LSBp), respectively, and are utilised as indicators for pixel pair mapping. In terms of indicator bits, 2LSBp, and 1LSBp, the pixel is closely related to CIPLpixel, and CIPRpixel, respectively, as shown in Fig. 2(iii).



ST (pair)	ST1		ST2		ST3		ST4		ST5		ST6		ST7		ST8		ST9		ST10		ST11		ST12		ST13		ST14		ST15		ST16	
bits	1	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	1	1

Pixel								
1	0	1	1	0	0	0	1	0
2	1	0	1	0	0	1	0	0
3	0	1	0	1	0	1	1	0
4	1	1	0	1	1	1	0	1
5	1	1	0	0	1	1	0	0
6	1	1	0	0	1	0	1	0
7	1	1	0	0	0	0	0	0
8	0	1	1	0	1	0	1	0
9	1	1	0	0	1	0	1	0
10	0	1	1	1	0	1	0	0
11	1	0	1	0	1	0	1	0
12	1	0	0	1	1	0	1	0
13	0	1	0	1	0	1	0	1
14	0	0	1	1	0	0	1	0
15	1	1	1	0	1	0	0	1
16	0	0	1	1	0	1	0	1

0	1	1	0	0	0	0	1
1	0	1	0	0	1	1	0
0	1	0	1	0	1	0	0
1	1	0	1	1	1	1	0
1	1	0	0	1	1	0	0
1	1	0	0	1	0	1	1
1	1	0	0	0	0	0	1
0	1	1	0	1	0	1	0
1	1	0	0	1	0	0	0
0	1	1	1	0	1	0	1
1	0	1	0	1	0	0	0
1	0	0	1	1	0	1	0
0	1	0	1	0	1	1	1
0	0	1	1	0	0	0	1
1	1	1	0	1	0	1	0
0	0	1	1	0	1	1	1

Fig. 2. The Full Scenario of the Proposed Embedding Process: (i) Secret Text Bits; (ii) Cover Image Pixels; (iii) Stego-image Pixels.

III. System Model and Methodology

Four phases describe the whole methodology of this paper, as shown in Fig. 3. These four phases are:

- Phase one: Data pre-processing. There are two stages in this phase which are (i) the secret message pre-processing and (ii) cover image preparation. In secret message processing, AES and Huffman coding are used while image normalisation is performed in the cover image preparation stage.
- Phase two: Embedding process. This phase also has two stages which are (i) LSB exchanging method and (ii) IKG, as described in Section II.
- Phase three: Evaluation process. This phase uses objectives and subjective evaluation metrics to test and evalaute the stego-image that includes the secret message. Some of the metrics used are Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), Structural Similarity Index Metric (SSIM), Mean Square Error (MSE), and payload capacity.
- Phase four: Extraction process. The objective of the extracting process is to extract the embedded data (secret bits) from the LSB pixels and simultaneously follow the procedure designed in the embedding process. Most of the information related to the extracting stage is made by the agreement between the sender and receiver parties.

The proposed methodology starts by applying data encryption using AES to convert the secret readable message to a non-readable message, raising the redundant characters, and then Huffman coding is used to reduce the size of the redundant character as much as possible. The proposed system perfectly deals with the USC-SIPI image database from the University of Southern California with different image sizes [15]. To work with this dataset, a preprocessng stage is needed to select the target pixel from the carrier image called "image normalisation process" before the embedding process. The proposed embedding algorithm (Stage 2), is applied. Then, the extraction process starts. The secret text bits are extracted by referring to the indicator bits (BLpixel or BRpixel) that the 2-LSBs substituted in each pixel. The extracting strategies are illustrated in Algorithm 2.

Algorithm 2. The proposed extracting algorithm.

```
First Action: If BL, the pixel is ‘1’ and BR, the pixel is ‘0’:
        Restore CILpixel as STB1, and
        Restore the 2-LSBs as STB2.
Second Action: If BL, the pixel is ‘0’ and BR, the pixel is ‘1’:
        Restore CIRpixel as STB2, and
        Restore the 2-LSBs as STB1.
Third Action: If both BLpixel, and BRpixel is ‘1’, then
        Restore STB1 from CILpixel bits, and
        Restore STB2 from the CIRpixel bits.
Fourth Action: If both BLpixel, and BRpixel are ‘0’, then
        No mapping indication.
```

Table I shows the simulation parameters used in this paper. The image size used is 512×512 with coloured and grey-scale images type. The payload capacities are 16384, 32768, and 49152 (16 kB, 32 kB and 49 kB). The PSNR threshold is 30 dB to consider imperceptibility.

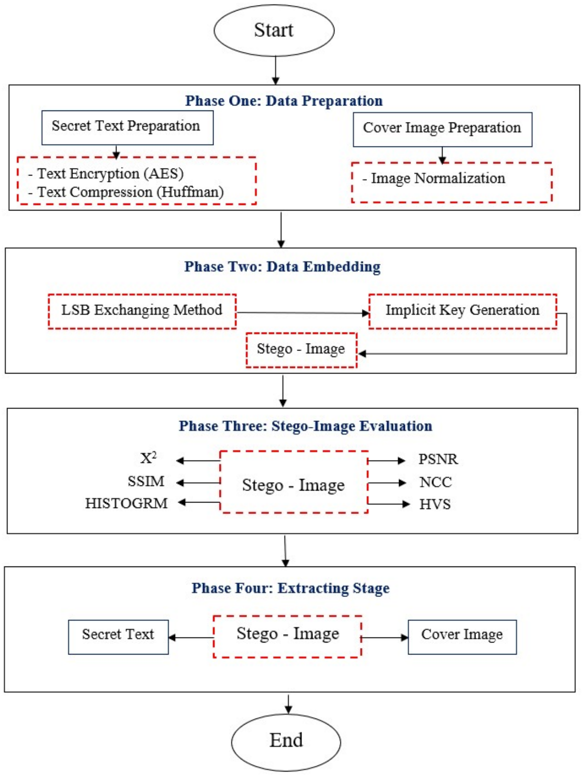


Fig. 3. The General Flowchart of the Proposed Methodology.

TABLE I. SIMULATION PARAMETERS

Simulation parameter	Values
Image size	512×512
Image format	TIFF format
Database used	USC-SIPI
Normalization	No
Payload capacity	16384, 32768, and 49152
PSNR threshold	30 dB
Coding	Huffman
Encryption	AES

IV. SIMULATION RESULTS AND DISCUSSION

In steganography, the imperceptibility and capacity of the proposed algorithm are the main concern in the simulation results. As known, there is a trade-off between capacity and imperceptibility of steganography. The proposed algorithm is evaluated based on the Embedding Capacity (EC) and three attacks system: the Human Visual System (HVS) attack, the Chi-square (χ^2)attack, and the Histogram attack. The comparison between the proposed algorithm with previously proposed methods in the literature is also presented.

The proposed algorithm uses colour and grey-scale images with different payload capacities which are 16 kB, 32 kB, and 49 kB. The 16384 bytes corresponded to 6.25%, meaning that every two pixels represented 16 bits; thus, 1/16 = 6.25% when 1 bit of two pixels was embedded. The 32768 bytes were equal to 12.5%, implying that every pixel corresponded to 8 bits, so 1/8 = 12.5% when 1 bit of one pixel was embedded. The 49152 bytes corresponded to 18.75%, signifying that every two pixels were assigned to 16 bits; accordingly, 3/16 = 18.75% when 1.5 bits of one pixel were embedded.

The PSNR threshold should be $\geqslant$ 30 dB in evaluating the imperceptibility to satisfy no HVS. In conventional image processing, the imperceptibility of the stego image is determined using the PSNR measures. By applying the PSNR measures, the fidelity of the stego image can be evaluated against the original carrier image. To ensure that the proposed system achieves the target aim, the proposed MLLSBEM is evaluated with two other embedding algorithms, the simple LSB and the embedding with pre-processing. Moreover, the proposed system is evaluated using various payload capacities: 16 kB, 32 kB, and 49 kB and three colour and grayscale images: Lena, Baboon, and Pepper. Table II presents the achievements of different embedding methods of grayscale images with 16 kB of payload capacities.

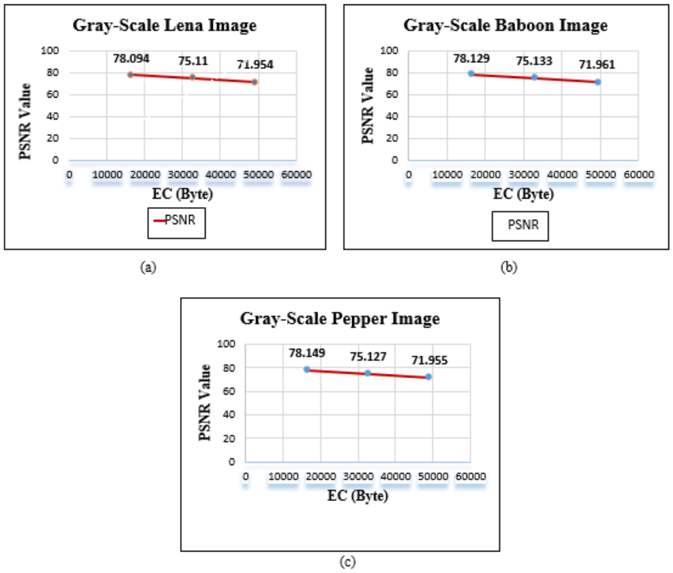
Simulation results in Table II show that the best PSNR comes from the proposed MLLSBEM because of the AES and Huffman coding compared to PSNR value of with pre-processing and simple LSB. Furthermore, the PSNR factor took the frequency of bits in the LSB of the cover image. The same conclusion comes from all the images via high PSNR value and low MSE. Fig. 4 shows the results of the proposed MLLSBEM using various payload capacities and various USC-SIPI dataset images Lina, Baboon and pepper images.

Coloured images are also used to evaluate their performance for the same payload capacities used in grey-scale images. Fig. 5 shows the PSNR values for the proposed algorithm when using coloured images. Simulation results show that the calculated PSNR values for the colour images are lower than the grey-scale images due to the representation of colour pixels with 24-bits for one pixel as opposed to only 8-bits for the grey scale. In addition, the Baboon image showed a higher PSNR value due to the different properties of this image, and also the nature of the image itself has more contrasts in the pixel value, thereby enabling the Baboon image to be more chaotic.

The proposed method used different evaluation metrics such as MSE, SSIM, and NCC to check the stego image before sending it to the authorised receiver to ensure that familiar attacks such as HVS, Chi-square and Histogram are unable to detect the secret message. Table III shows the various evaluation metrics with different amounts of embedding capacity for the standard grey-scale and coloured images.

TABLE II. THE DIFFERENT EMBEDDING METHODS OF GRAY-SCALE WITH 16 KB OF PAYLOAD CAPACITY

Image/ Dataset	PSNR evaluation metric		
	Simple LSB	*With Pre-processing*	*MLLSBEM (Proposed)*
Lena	65.225	71.332	78.094
Baboon	66.331	72.099	78.129
Pepper	64.997	71.009	78.1491



(a)

(b)

(c)

Fig. 4. The PSNR Values of Grey-scale Images with Various Payload Capacities. (a) Lena Image, (b) Baboon Image, (c) Pepper Image.

TABLE III. VARIOUS EVALUATION METRICS OF GRAY-SCALE AND COLORED IMAGES

Images	**Embedding Capacity**	**16384 Bytes**			**32768 Bytes**			**49152 Bytes**		
	Metrics	***MSE***	***SSIM***	***NCC***	***MSE***	***SSIM***	***NCC***	***MSE***	***SSIM***	***NCC***
Lena	Gray-Scale	0.0132	1	1	0.0144	0.998	0.976	0.0188	0.987	0.959
	Colored	0.0146	1	1	0.0146	0.998	0.987	0.0177	0.988	0.978
Baboon	Gray-Scale	0.0145	1	1	0.0149	0.999	0.997	0.0198	0.986	0.978
	Colored	0.0152	1	1	0.0159	0.999	0.997	0.0189	0.989	0.968
Pepper	Gray-Scale	0.0136	1	1	0.0175	0.998	0.998	0.0210	0.979	0.989
	Colored	0.0149	1	0.999	0.0169	0.997	0.989	0.0222	0.977	0.989

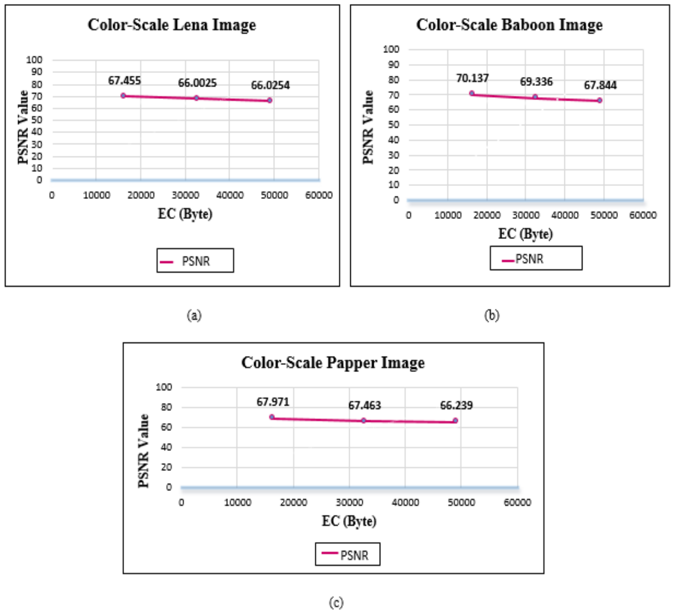


Fig. 5. The PSNR Values of Coloured Images with Various EC Values. (a) Lena Image, (b) Baboon Image, (c) Pepper Image.

A. Human Visual System Attacks Analysis

In image steganography, a system can detect edges that become blurred or unclear. Consequently, the LSB can detect the HVS attack, which is still ambiguous to human sight because it is trained to recognise the known things. This simulation aims to distinguish the presence or absence of the hidden data in the stego-image. Simulation results in Fig. 6 show that the eight-bit planes HVS attack can detect only the LSBs; the rest are ignored. The embedding in the bit planes 1 and 2 appears very clear where the vertical lines refer to the frequencies in their bits, implying that hidden information is embedded in these two-pixel. This type of detection is somewhat interactive between the system and humans because the system generates the pattern, and the human eyes detect it.

Fig. 7 depicts the comparison of the proposed MLLSBEM towards HVS attack as compared to the simple LSB and with pre-processing. Observations indicate that embedding simple LSB images is ineffective because the injection of the hidden bits directly, without processing or bit position selection, makes them immediately detectable by human eyes.

Due to preparation for the usage of picture normalisation, the pattern of the first bit-plane was improved for the pre-processing procedure. Using AES encryption and Huffman coding, the proposed MLLSBEM can generate a stego-image similar to the original cover image due to the arbitrary distribution of bits and the process of preserving the original image bit values by mapping the secret bits before embedding them.

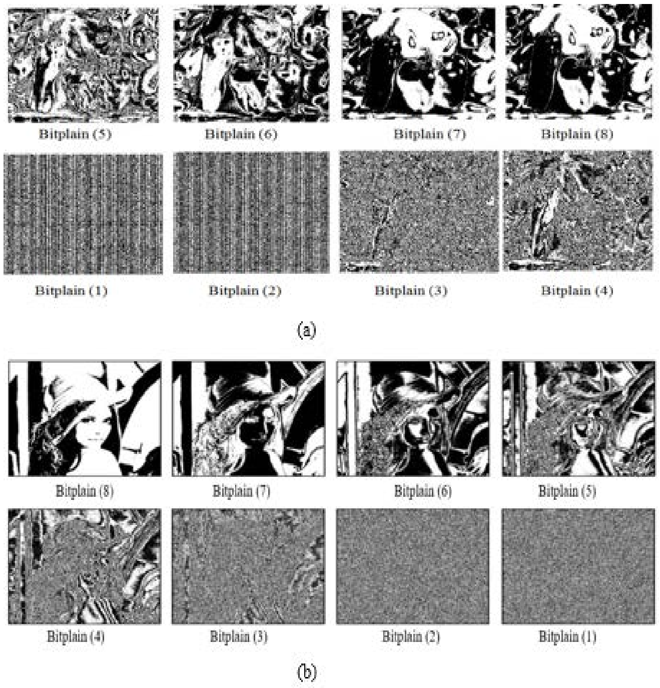


Fig. 6. The HVS Attacks with Various the Eight Bit-plains Layers. (a) Pepper Image, (b) Lena Image.

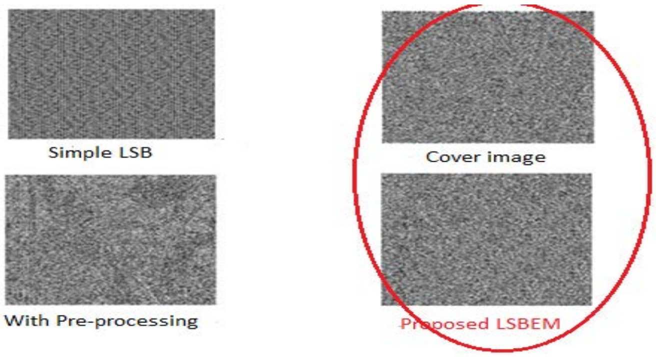


Fig. 7. The Figure shows Three Embedding Methods in Resistance against the HVS Attack on the Original Lena Image.

B. Chi-square Attack (X^2) Attack

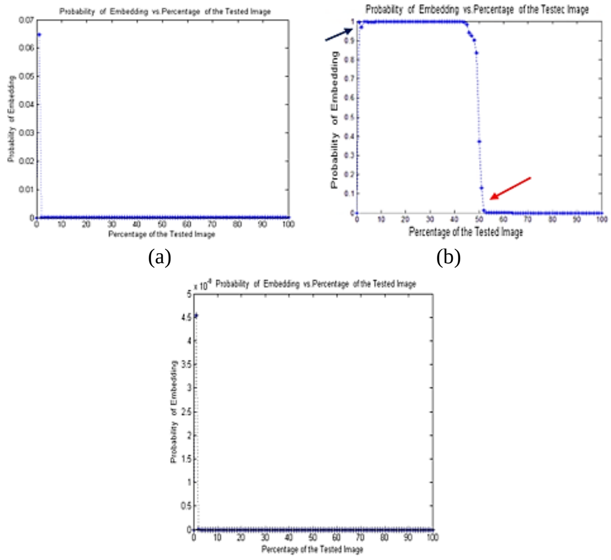
A special attack called Chi-square (χ2) is based on the statistical analysis of the Pairs of Values (PoVs) exchanged during the secret data embedding, which is also based on the probability distribution. The (χ2) attack can find the probability of embedding the secret bits inside the stego image where the normal image follows the usual behaviour.

Fig. 8(a) shows the χ2-test for the original pepper image. In the first 10%, the probability is 0.065 because when the function checks the pixels, most of the characters in the alphabet start with the same value as the frequent bits. Thus, the test detects this frequently and suggests these pixels as the embedded data. The absence of detection for embedding in the remaining images is normal, as the original images do not have any hidden data.

Fig. 8(b) shows the χ2-test for the simple LSB that detects fifty per cent of the image as concealed data with a probability of one. In Fig. 8(c), the proposed algorithm covers the entire image with a low probability, even better than the original image. This occurs because the statistical distributions of the values in the LSB are good. After all, the segments of the secret bits are chosen carefully.

C. Histogram Attack

The histogram analysis is applied to three types of images, as shown in Fig. 9. The analysis shows that the variance between the constructed histograms is comparatively low for all tested images when using the proposed MLLSBEM method. The distortions caused by the embedding process are not noticeable to the human eye when concealing an acceptable amount of secret bit. However, when we hide more secret bits (exceeding the embedding limit), the variance between the constructed histograms is high and noticeable to the human eye. Moreover, the PSNR value becomes low.



(a) (b)

(c)

Fig. 8. The χ2-test for Pepper Image. (a) The Original Image, (b) The Simple LSB, and (c) The Proposed MLLSBEM for 16 kB Pixels.

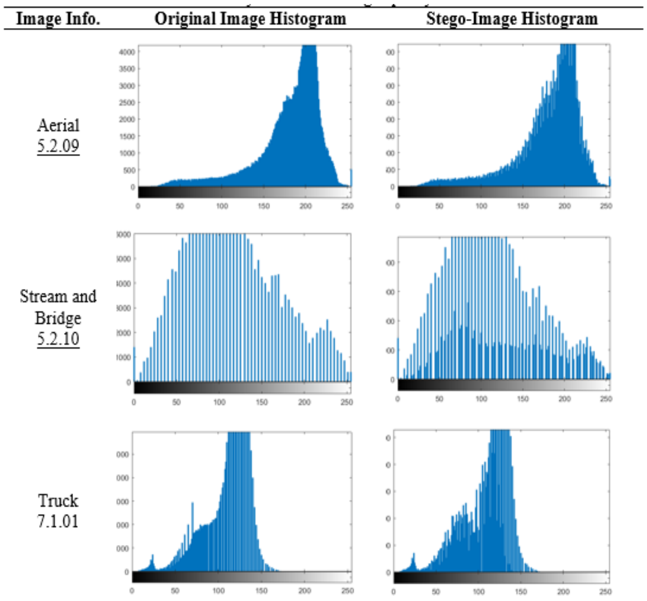


Fig. 9. Histogram Analysis of 16 kB Capacity of Grey-scale Image.

Fig. 10 shows the comparison between the stego images and the original image with different payload capacities. 18.75% embedding corresponds to 49 kB payload capacity.

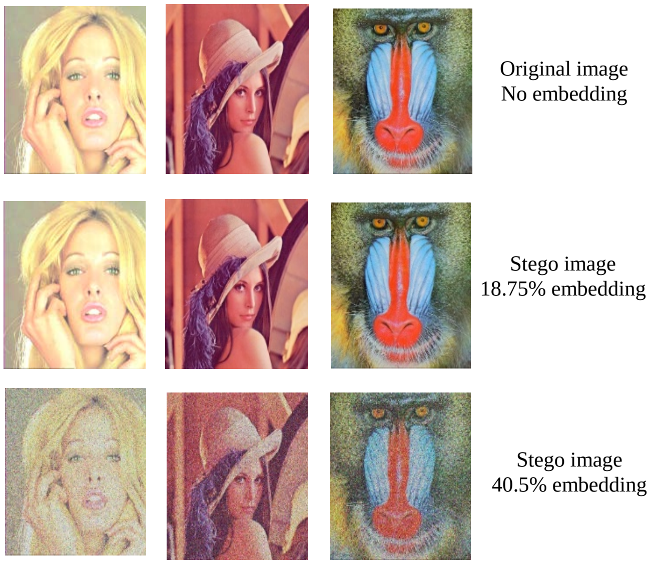


Fig. 10. The Stego and Original Images' Resemblance with Different Payload Capacity.

Table IV compares the proposed algorithm's results with the previously published methods. The evaluation results of the proposed method were found to be better than those reported in the literature. This evaluation indicates that the proposed algorithm used for the pre-processing and embedding stages in the proposed scheme improve the final results. The proposed method is excellent as compared to the previous studies in terms of PSNR, SSIM, NCC, MSE for different payload capacities. In addition, the proposed method is resistant towards the histogram, chi-square, and HVS attacks.

TABLE IV. THE EVALUATION RESULTS OF THE PROPOSED METHOD

Cover Image 512 X 512 Colour	**Lena**					**Baboon**					**Pepper**				
	Capacity (KB)	***PSNR***	***SSIM***	***NCC***	***MSE***	***Capacity (KB)***	***PSNR***	***SSIM***	***NCC***	***MSE***	***Capacity (KB)***	***PSNR***	***SSIM***	***NCC***	***MSE***
A. S. Ansari et al. 2017 [19]	34	59.19	-	-	1.93	34	59.21	-	-	1.90	34	58.95	-	-	2.02
S.A. Parah et al., 2018 [20]	16	55.80	-	0.99	-	-	-	-	-	-	16	52.88	-	0.99	-
R. Shanthakumari and S. Malliga, 2019 [21]	78	54.85	0.99	1	0.85	78	54.62	0.99	1	0.90	78	54.73	0.98	1	0.88
A.S. Ansari et al., 2020 [22]	35	66.67	-	-	-	35	69.45	-	-	-	35	67.16	-	-	-
L. Tang et al. 2021 [23]	80	65.7	0.99	-	-	56	66.9	1	-	-	80	65.4	0.99	-	-
Proposed Method	49	66.02	0.98	0.97	0.0177	49	67.84	0.98	0.96	0.018	49	66.23	0.97	0.98	0.02

V. CONCLUSION

We have presented a new image steganographic method using the MLLSBEM to hide the secret bits. The proposed algorithm uses pre-processing operations such as AES encryption and Huffman coding. The proposed embedding algorithm is based on the modified LSB exchanging method and IKG. Simulation results show that the proposed method is excellent as shown in the achievement of PSNR, SSIM, NCC, and payload capacity and is robust towards the histogram, chi-square, and HVS attacks. In the future, we plan to take into consideration an open challenge to achieve adaptable exchange between the cover image and secret bits. This work opens up several new avenues that are worth doing for the future. For instance, the security can be enhanced by mixing the frequency domain and spatial domain. This may achieve better results in terms of security and robustness. Also, the proposed method can be combined with the DWT and embedding may result in high coefficients based on the obtained findings. Many methods have already used high coefficients for the embedding. However, the use of LSBEM may yield better results in terms of security and imperceptibility. The most important gap in the steganography system is related to the capacity improvement of the secret message. The limitation of the secret message with PSNR makes the steganography difficult to improve. In such a scenario, it is better to handle the secret message before embedding and to make it dynamic with the embedding method. The concealed message's limitation (direct hiding) makes steganography difficult to improve. In this case, it's preferable to manipulate the secret message before embedding it by coding and compressing it, making the secret text pre-processing stage interactive with the embedding process.

ACKNOWLEDGMENT

The authors would like to acknowledge Universiti Kebangsaan Malaysia and the Ministry of Education, Malaysia (MOE) for the Research University Grant with code: GUP-2019-023 to support this project.

REFERENCES

[1] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana, and S. K. Pani, "SSII: secured and high-quality steganography using intelligent hybrid optimisation algorithms for IoT," *IEEE Access*, vol. 9, pp. 87563-87578, 2021.

[2] Taha, Mustafa Sabah, et al. "High payload image steganography scheme with minimum distortion based on distinction grade value method." *Multimedia Tools and Applications* (2022): 1-34.

[3] X. Duan *et al.*, "High-capacity image steganography based on improved FC-DenseNet," *IEEE Access,* vol. 8, pp. 170174-170182, 2020.

[4] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *Journal of Systems Engineering and Electronics,* vol. 29, no. 3, pp. 639-649, 2018.

[5] Hadad, Abbas Abd-Alhussein, et al. "A Robust Color Image Watermarking Scheme Based on Discrete Wavelet Transform Domain and Discrete Slantlet Transform Technique." *Journal homepage: http://iieta. org/journals/isi* 27.2 (2022): 313-319.

[6] Y. Ren, T. Liu, L. Zhai, and L. Wang, "Hiding Data in Colors: Secure and Lossless Deep Image Steganography via Conditional Invertible Neural Networks," *arXiv preprint arXiv:2201.07444*, 2022.

[7] A. Gupta, H. Shukla, and M. Gupta, "A Secure Image Steganography using X86 Assembly LSB," *NEU Journal for Artificial Intelligence and Internet of Things*, vol. 1, no. 1, pp. 38-47, 2022.

[8] M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, "An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques," *IEEE Access*, vol. 7, pp. 185189-185204, 2019.

[9] I. Maurya, and S. K. Gupta. "Secure image steganography through pre-processing." *In Soft Computing: Theories and Applications*, pp. 133-145. Springer, Singapore, 2019.

[10] S. Venkatesh, V. Sivakumar, A. K. Vagheesan, S. Sakthivelan, K. J. Kumar, and K. K. Nagarajan. "GANash -- A GAN approach to steganography." arXiv preprint arXiv:2110.13650, 2021.

[11] D. Volkhonskiy, B. Borisenko, and E. Burnaev. "Generative adversarial networks for image steganography". *Open Review*, 2016.

[12] D. Volkhonskiy, I. Nazarov, and E. Burnaev. "Steganographicgenerative adversarial networks." *In Twelfth International Conference on Machine Vision (ICMV 2019),* vol. 11433, pp. 114333M. International Society for Optics and Photonics, 2020.

[13] H. Shi, X. Zhang, S. Wang, G. Fu, and J. Tang. "Synchronised detection and recovery of steganographic messages with ad-versarial learning." *In International Conference on Computational Science*, pages 31–43. Springer, 2019.

[14] H. Shi, J. Dong, W. Wang, Y. Qian, and Xiaoyu Zhang. “Ssgan: secure steganography based on generative adversarial networks.” *In Pacific Rim Conference on Multimedia*, pages 534–544. Springer, 2017.

[15] J. Yang, K. Liu, X. Kang, E. K. Wong, and Y. QingShi. “Spatial image steganography based on generative adversarial network.” *arXiv preprint*, arXiv:1804.07939, 2018.

[16] J. Yang, D. Ruan, J. Huang, X. Kang, and Y. QingShi. “An embedding cost learning framework using gan.” *IEEE Transactions on Information Forensics and Security*, 15:839–851, 2019.

[17] H. Dadgostar, and F. Afsari. “Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB.” *Journal of Information Security and Applications*, 30: 94–104, 2016.

[18] M. Islam, A. Roy, and R. Laskar. “Neural network based robust image watermarking technique in LWT domain.” *Journal of Intelligent & Fuzzy Systems*, 34(3): 1691–1700, 2018.

[19] A.S. Ansari, M.S. Mohammadi, and M.T. Parvez. “JPEG Image Steganography based on Coefficients Selection and Partition.” *International Journal of Image, Graphics and Signal Processing*, 9(6), 14, 2017.

[20] S.A. Parah, J.A. Sheikh, J.A. Akhoon, N. A. Loan, and G.M. Bhat, “ Information hiding in edges: A high capacity information hiding technique using hybrid edge detection.” *Multimedia Tools and Applications.* 77(1): 185–207, 2018.

[21] R. Shanthakumari, and S. Malliga. “Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment.” *Sadhana - Academy Proceedings in Engineering Sciences*, 44(5), 2019.

[22] A.S. Ansari, M.S. Mohammadi, and M.T. Parvez. 2020. “A multiple-format steganography algorithm for color images.” *IEEE Access*, 8: 83926–83939S, 2020.

[23] L. Tang, D. Wu, H. Wang, M. Chen, and J. Xie. “An adaptive fuzzy inference approach for color image steganography.” *Soft Computing*, 25(16): 10987–11004, 2021.