IMAGE STEGANOGRAPHY TECHNIQUE USING SWAPPING METHOD AND TEXT MANIPULATION

HAJIR SAIED FARHAT ALMSHAWIT
AZANA HAFIZAH MOHD

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor Malaysia.

hajer.saied2007@gmail.com, azana@ukm.edu.my

ABSTRACT

Nowadays, developments in the world of digital communication and technology play a vital role in our life. Therefore, systems of information security have become a key role in transmission of confidential data. Steganography technique is considered an effective method to hide confidential information. The big challenge in steganography systems is data security and ability to hide the maximum amount of secret data as possible. Therefore, the issue needs to be addressed. This issue can be solved by maintaining the high value of PSNR (Peak Signal to Noise Ratio) in order to increase the resistance against detection attacks. Therefore, this research proposes an enhanced image steganographic method which made by using swapping method and text manipulation. The enablement of the proposed method shows the improvement of capacity building and security to overcome the problems. The proposed method involves four stages to achieve the objectives of this study which begins with the preparation stage for images and secret text and ends with evaluation stage. Where the proposed study has used standard images from database (USP-SIPI). Through this method, a better result of PSNR and MSE is achieved, 63.95 and 0.026 respectively. The effective of proposed method has been demonstrated by comparing the results of this study with the results of previous methods.

Keyword: Peak Signal to Noise Ratio , Mean Square Error.

I. INTRODUCTION

In the technology and internet era, the rapid development in the world of communication plays an important role in our lives. The systems of information security have a key role in the transmission of confidential data. Information security is classified into two categories: information hiding and information encryption. The goal of both is the same, which is securing data but their approaches are different. Both goals have been advanced by researchers. Information encryption is a

technique to convert secret data into unreadable form. However, this method can be noticeable by intruders. Hence, it is necessary to provide imperceptible communication without anyone noticing the connection. This is why the technique of hiding information is needed (Kadhim et al. 2019).

The technique of information hiding contains two subdisciplines which are watermarking and steganography, and both are used to conceal secret data and are similar, but both depend on different objectives. The main objective of steganography is to hide the presence of communication and the protection of confidential data. In contrast, the main objective of watermarking is to protect the integrity of confidential data without hiding the presence of communication (Hussain et al. 2018).

Recently, steganography technique has played an important role in a wide range of applications such as enhancing mobile banking reliability, transporting of confidential military information, the reliability of online voting, and other intelligence organizations, and concealing communication between two parties. The design of steganography is more effective than other information hiding techniques since it keeps the consistency of data form. Thus, there is no question about the existence of secret information (Rizal Isnanto et al. 2018). The strength of steganography technique relies on many factors which are as follows: the power of confidential information to keep the concealed information using strong algorithms, sufficient space to assign confidential information, the algorithm should strongly deliver messages safely from the sender to the receiver without losing any data during data compression and provide good resistant against attackers. In addition, the protection of passphrase and algorithms used should remain secret, because if the attackers cannot detect the presence of hidden data, they cannot extract the hidden data as the algorithm used has not been exposed (Yari & Zargari 2017).

Steganography is the science or art that hides secret messages inside a cover medium from unauthorized personnel or devices, and the cover media can be text, image, audio, video, or protocol where each one has advantages and disadvantages. Also, the secret message can be text, image, or any data. According to several studies (Rajput & Chavan 2017). the best cover medium for embedding secret data is the image since the image has two features: it is the most common medium and the image has a high frequency of redundant information and ability to hide the secret data without visible impacts (Rajput & Chavan 2017). This study has highlighted images as cover media and secret data as plain text.

Different methods have been proposed in the image steganography approach based on applications and the stages used in the embedding process. Each method had some limitations and strength.

In recent years, the number of cybercriminals has increased. This issue has always been a main subject of attention for security experts around the world. On other hand, the amount of data used has increased daily. As a result, the main challenge in the image steganography technique is concealing secret information with the following requirements: high security, high payload capacity, good robustness, and minimum imperceptibility. All these requirements are very important in the era of technology (Kadhim et al. 2019; Arroyo et al. 2020).

Therefore, this study will fill the study gap by focusing on the image steganography IRFC among public university staff in pre-implementation phase of the Campus ERP project in Malaysia.

This paper consists of five (5) sections. Section I discuss the background of image steganography technique. Section II presents a comprehensive digital image steganography medium and a comprehensive taxonomy of steganography methods. It also reviews the literature on the image steganography methods relevant to this study discuss Section III elucidates the methodology used in the study. Section IV presents the findings of the work and discussion. Lastly, section V concludes the paper with a summary of the findings and recommended future work.

II. LITERATURE REVIEW

A. INFORMATION HIDING

In the modern era, the use of digital communication plays a vital role in our lives. High protection for data is provided to security systems by effective methods. Security system is classified into two categories: Data Cryptography and Information Hiding (Kadhim et al. 2019). The goal of both is similar, which is to secure data from unauthorized persons, but their approaches are different Some researchers have classified security systems as shown in Figure 1 (Kadhim et al. 2019).

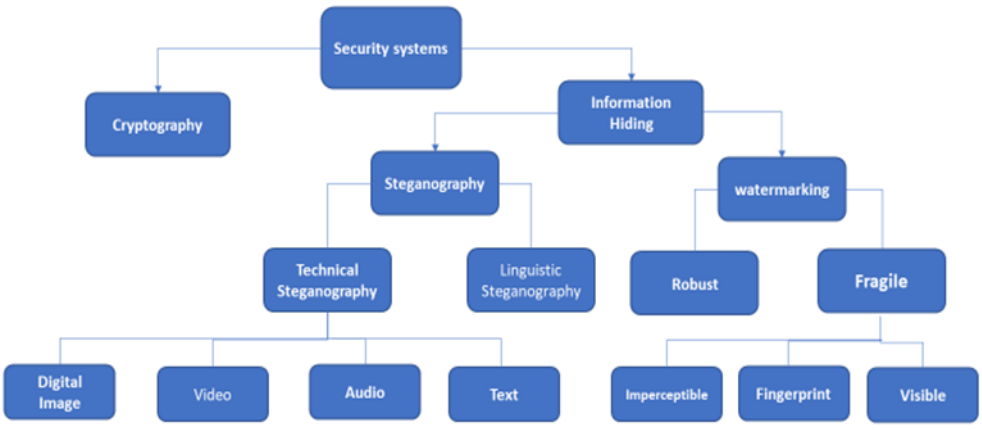


Figure 1 Classification of security systems

The various techniques available for security systems across the world are digital watermarking, cryptography, and steganography, all of which provide data protection for secret communications. Digital watermarking is an information hiding technique that protects intellectual property of the rightful owner from illegal copying (Laishram & Tuithung 2018). Cryptography is another information hiding technique that aims to convert secret data into encrypted data "unreadable form" during transmission by using different methodologies. There are two ways to perform this technique. The first way has Symmetric key Cryptography which involves only one key for both sides (encryption &decryption). In contrast, another way has multiple keys, whereas a public key uses encryption purpose, and private keys use decryption purpose by authorized systems or personals. (Laishram & Tuithung 2018; Kadhim et al. 2019).

Steganography is another method of information hiding technique that aims to convert secret data into encrypted data without changing the format of the data. It is more effective than the cryptography technique because it is difficult to notice the hidden data by unauthorized systems or personnel. The difference between the Cryptography and steganography techniques is that the Cryptography technique is considered as broken if the unauthorized party can access original information, while steganography technique is considered as broken if the unauthorized party can discover the existence of secret information (Kadhim et al. 2019). The design of steganography is more effective than cryptography, because it keeps to the consistency of data form and thus it does not attract doubts about the existence of hidden information (Rizal Isnanto et al. 2018).

Recently, several studies have focused on image steganography technique. It is the most common because of the ease of using images in multimedia connections through social media applications such as Facebook, WhatsApp, and various low-priced devices such as IP cameras and smart phones. As a result, users can simply hide confidential information inside the digital images (Hussain et al. 2018).

Generally, there are many types of steganography techniques. Users can conceal secret data through different communication carriers known as "the cover object", which may include data or digital files such as image, text, audio, protocol, video, and Deoxyribonucleic acid (DNA)(Hussain et al. 2018).

B. DIGITAL IMAGE STEGANOGRAPHY

This study selected a digital image as a cover medium. Recently, a digital image has been usually used as a carrier to conceal information as secret messages are hidden by using pixel intensities in the

cover of image. Commonly, the size of the image ranges from 8 bits – 24 bits as big image size leads to larger hidden information. As a result, large images need compression process and some techniques like masking, LSB insertion and filtering to evade detection from attackers.

Typically, the image steganography technique is evaluated by the following main objectives which are described as follows: (1) capacity of embedding secret data, which means how maximum the payload can be accomplished, (2) visual image quality, which means, how perceptibly similar are the stego-image and its cover image, and (3) security. How can stego-image protect its self from the various attacks? Thus, the perfect of image steganography is that it must achieve the above objectives concurrently. However, the approaches of image steganography which have high payload suffer from distortion in the stego image. In contrast, image steganographic approaches which have minimum distortion suffer from low payload. Therefore, the main challenge in an image steganography technique is how to achieve these objectives of highly security, highly payload, and minimum imperceptibility simultaneously (Hussain et al. 2018; Al-Husainy & Uliyan 2019).

- Classification of Image Steganography Methods

  There are various methods that have been proposed in an image steganography technique. This relies on the nature of cover image, the retrieval processes, the nature of embedding processes, and the adaptive steganography. These methods are classified by Kadhim et al. (2019) as illustrated in Figure 2.

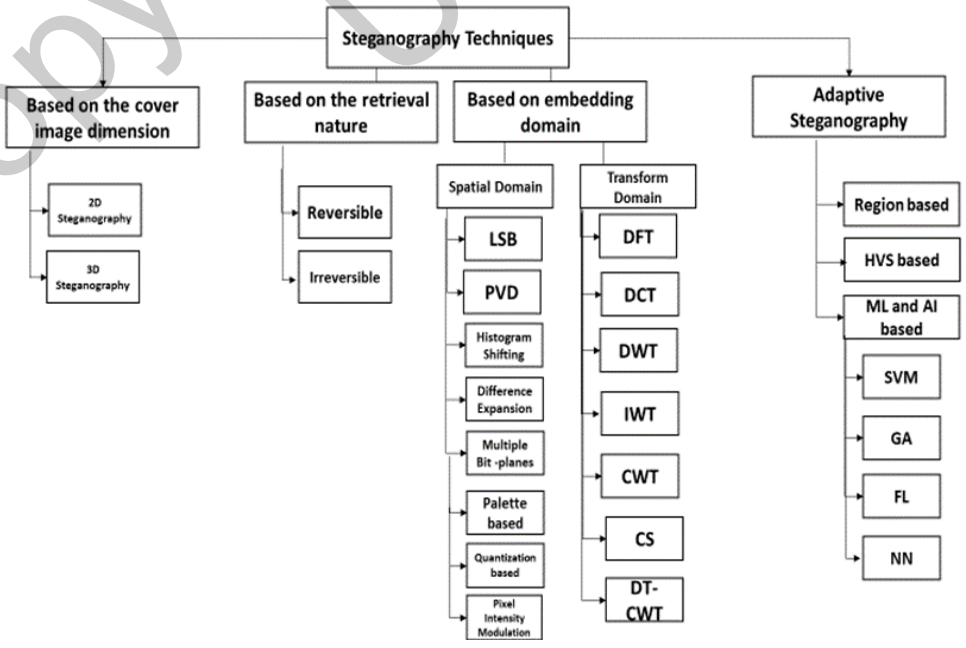


Figure 2 Taxonomy of image steganography methods

This study selected the “spatial domain embedding technique” which is called a “substitution technique”. It is more common than a transform domain technique due to the ease of extraction and the embedding process, but it has less robustness. This technique is a collection of simple methods that generate a secret channel in the parts of the cover image where there occurs a little change that cannot be detected by Human Visual Systems (Kaur & Rani 2016).

- Classification of Steganalysis Techniques

Steganalysis technique is also known as “The steganography detection techniques”. It is the science or art of detecting the secret messages embedded in the steganography technique. Steganalysis is designed to analyze and extract the secret messages during the embedding processes. Steganalysis and steganography techniques are countermeasures of each other. The difference between them is that the actual target of steganography technique is hiding secret data and defeating any detection attacks in the embedding process, while the target of steganalysis technique is extracting secret data from the stego image and detecting the existence of secret data by attackers (Yari & Zargari 2018; Hussain et al. 2018). Steganalysis techniques are usually classified into categories described by Hussain et al. (2018) as follows:

1. Visual Steganalysis Technique

It is one of the most substantial requirements of any steganography technique. Some visual relics are invisible due to the limitation of Human Visual System (HVS). There are various visual quality measures which are useful in evaluating the visual quality of stego image such as PSNR, SSIM, and MSE.

2. Statistical Steganalysis Technique

It uses the structural features of image files to detect unusual characteristics that are caused using steganography techniques. These methods can easily expose the presence of secret data and evaluate its size. There are several kinds of statistical methods such as bit plane analysis, Chi-square analysis, histogram analysis, and RS analysis.

3. Nonstructural Steganalysis Technique

In this method, the steganalyzer is used to model the cover image and evaluate the distortion between stego- image and cover file to expose the embedding secret information. The set of universal features of steganography is a set of specified features. Generally, there are several ways

in this area, and the most popular are “SPAM” Subtractive Pixel Adjacency and “SRM” Spatial Rich Model which are considered the best possibility of steganalysis or “SVM” Support Vector Machine.

C. RELATED WORKS

The main target of developing methods for hiding confidential information when transferred over open networks is to increase security, robustness, capacity of image steganography and providing strong resistance against intruders. This study focuses on spatial domain technique only. In recent years, several spatial domain methods have been used by researchers in this area which are briefly discussed in this section.

Table 1 Summary of relaed works

Title & Author	Method	Contributions	Type of images
“Image Steganography Based on Complemented Message and Inverted bit LSB Substitution”, Bhardwaj & Sharma 2016	Used inverted bit LSB method substitution and complemented message.	Provided 3 layers of security and obtained high value of PSNR and low value of MSE	Greyscale images
“3-Level Security Based Spread Spectrum Image Steganography with Enhanced Peak Signal to Noise Ratio” ,Yadav & Dutta 2017	Used cryptography techniques “RLE & RSA algorithms” and steganography technique “LSB method”	Provided 3 levels of security	Color images
“A Novel Approach for Image Steganography based on LSB Technique”, Rajput & Chavan 2017	Used LSB method with angular transformation concept	Increased the robustness and resistance against attackers	Color images
“Digital Image Steganography Using LSB Substitution, PVD, and EMD”, Pradhan et al. 2018	Used LSB Substitution method, EMD and PVD.	Improved the hiding capacity and PSNR.	Color images.
“New Steganography System Based on Huffman Coding and Fibonacci Decomposition”, Abu-Almash 2018	Used Huffman coding and Fibonacci Decomposition	Increased the robustness and capacity of steganography system.	Greyscale images
“Secure and hidden text using AES	Used cryptography by “AES algorithm” and	Provided security levels.	Color images

cryptography and LSB steganography", Hattim & Taha 2019	steganography by LSB method.		
"A novel steganography technique using grayscale image segmentation ***",Mangla et al.*** 2019	Used Least Significant Bits method with grayscale image segmentation.	Provided more robustness and security.	Greyscale images
"Image Steganography Based on LSB Matching and Image Enlargement", Al-Aidroos & Bahamish 2019.	Used LSB matching method and principle of an image enlargement.	Provided high embedding capacity and high quality of images.	Greyscale images
"Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography", Yahaya & Ajibola 2019	Used cryptography" AES" algorithm and steganography "LSB" method.	Produced double layers of protection and high quality of stego image.	Color images.
"A secret- key image steganography technique using random chain codes", Al-Husainy & Uliyan 2019	Used LSB method and random chain codes.	Achieved three characteristics: capacity, robustness, undetectability	Color images.
"Improved payload capacity in LSB image steganography uses dilated hybrid edge detection", Setiadi 2019	Used 3 most significant bits (MSB) method for pixels of a cover image and used dilated hybrid edge detection.	Improved the quality of imperceptibility, and increased the message embedding capacity.	Greyscale images.
"Steganography Technique with Huffman Code", Sethi & Patel 2019	Used Huffman coding &LSB method &	Provided multi-level security.	Grey-scale images
"An image steganography approach based on k-least significant bits (k-LSB)", Elharrouss et al. 2020	Used k-LSB method	Provided minimum distortion, cost, and loss of data.	Color images.
"An Efficient Least Significant Bit Image "Steganography with Secret Writing and Compression Techniques", Arroyo et al. 2020	Used LSB for steganography, Huffman coding for compression technique and Vigenere cipher for cryptography.	Improved the security of information hiding by introducing multiple layers of security.	Greyscale images.
"A new image steganography method with optimum pixel	Used similarities of the pixels based on LSB method.	Increased hiding capacity.	MRI & OT images, "medical

similarity for data hiding in medical images", Karakus & Avci 2020			images".
"Universal stego post-processing for enhancing image steganography", (Chen et al. 2020)	Used post-processing method on the embedding units of stego image directly.	Improved the security of most current steganography techniques for JPEG domains and spatial domains methods.	Grey-scale images.
"LSB-based Bit Flipping Methods for Color Image Steganography" Astuti et al. 2020	Used LSB based on bit flipping method	Provided maximum capacity and increased imperceptibility.	Color images.
"An effective and secure digital image steganography scheme using two random function and chaotic map", Abdulwahed 2020	Used new stego key adaptive LSB method.	Enhanced security, robustness, and capacity.	Grey-scales Images.
"Image Steganography and Steganalysis Based on Least Significant Bit (LSB)method", Rachael et al. 2020	Used LSB method.	Concealed secret message and extracted it without losing data.	Color images.
"Hide text depending on the three channels of pixels in color images using the modified LSB algorithm", Neamah et al. 2020	Used modified LSB algorithm.	Increased the quality of stego image.	Color images.

III. RESEARCH OBJECTIVES AND RESEARCH QUESTIONS

The main objective of this research is improving the image steganography method for concealment of secret data "plain text" inside a cover image while maintaining high capacity, good robustness, and good security. The objectives of this study are as follow:

1 To identify the capacity of embedded secret bits in order to preserve the visual quality of image.

2 To integrate the security of the proposed method using text encryption and compression method.

3 To assess the performance of the proposed method and compare the gain resolution with previous solutions.

The research gaps can be clearly seen through the following three questions:

1 How to enhance the payload capacity of the embedded secret data of the proposed method?

2 How to enhance the security of the proposed method while keeping the imperceptibility of stego image?

3 How to enhance the robustness of the proposed method while maintaining the visual quality of the produced image?

IV. METHODOLOGY AND PROPOSED FRAMEWORK

The proposed method includes four main stages to implement the image steganography technique, which are the preprocessing stage, the embedding stage, the extracting stage, and the evaluation stage. This proposed scheme starts with the pre-processing stage which includes text and image preparation before embedding the stage, and ends with the evaluation stage through measuring the popular metrics such as Peak Single Noise Ratio (PSNR) as well as Mean Square error (MSE) where PSNR evaluates the quality of stego image through analysis of MSE between the stego- image and the cover image.

This study has shown three contributions to enhance the proposed image of the steganography technique. The first one is to increase the hiding capacity of the cover image through using compression algorithm, which is the Huffman coding algorithm at the preprocessing stage, where it is used to fragment and compress confidential information before the embedding process. The second contribution is to increase the security of the proposed method by using the encryption algorithm which is the Encryption Advance Standard algorithm which is used to encrypt secret text during the pre-processing stage. The last contribution is to enhance the robustness of the proposed method by using Fibonacci decomposition algorithm which used to transfer the pixel value of the cover image from 8 bits to 12 bits and by using map of pixel and block randomization.

PROPOSED FRAMEWORK

The aim of this framework is to enhance the image steganography technique to hide confidential information in color images.tiff (RGB), as the selected images from USP- SIPI database which is used as a cover image. The size of the specific images is 512×512 pixels (24 bit/pixel). The framework of the proposed method is illustrated in Figure 3

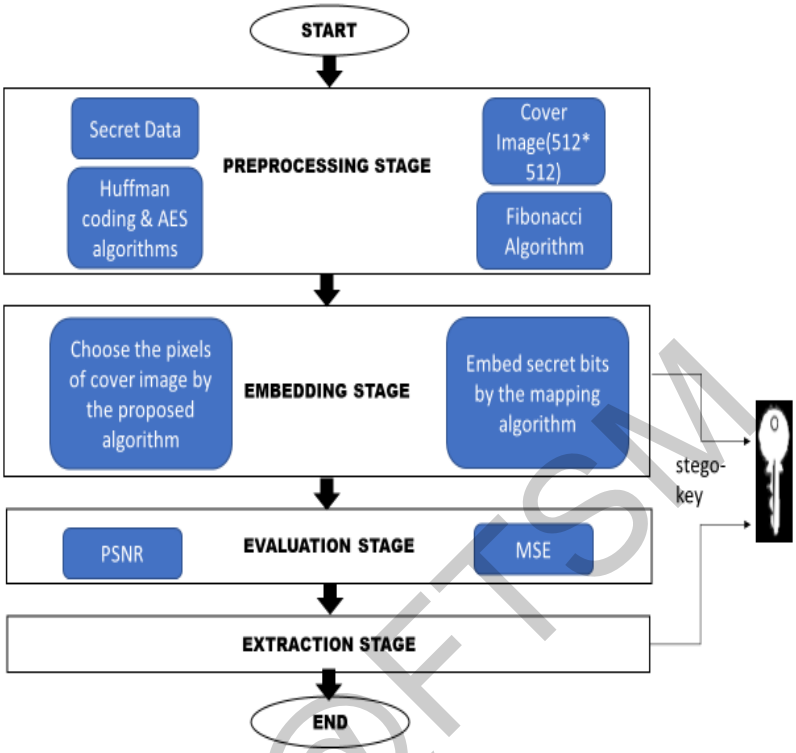


Figure 3 Framework of the proposed method

There are four stages for any steganography method. The most significant stage is the embedding stage, which represents the algorithm's power (Abu-Almash 2018). This proposed method, the embedding stage, depends on the swapping approach for concealing secret data inside color images. The mechanism of the proposed method is like the Least Significant Bits method (LSB) in which the Fibonacci decomposition algorithm is used during the embedding process. It targets the least significant bits that are located at the far right of the binary value. However, the key difference behind the Fibonacci algorithm lies on the use of specific table for the actual embedding process rather than using XOR or XNOR gates by LSB. As a result, a stego-image seems like the original image and it has high quality, where hackers and intruders cannot discover the existence of secret information.

V. RESULTS & DISCUSSION

After the embedding process, some invisible artifacts have occurred on the cover image by the steganography technique used where these artifacts may be unnoticeable to the human vision system. Therefore, some standard measuring methods are used to estimate the visual change levels for deciding whether the steganography technique is visual transparency. There are various visual quality metrices used to evaluate the quality of the steganography method. Generally, the most popular metrices are the PSNR and MSE which are used to measure the quality of the stego-image after the

embedding process (Hussain et al. 2018). The embedded secret data cause changes in the pixel values of the cover image. These changes need to be analyzed because it impacts the imperceptibility of the stego image "output". PSNR is used to evaluate the quality of the stego image by analyzing the value of MSE between the cover image of the "original image" and the stego image. The formula used to calculate the PSNR is as

$$PSNR = 10 \log 10\left(\frac{255^2}{MSE}\right) \quad \text{…(Error! No text of specified style in document..1)}$$

where MSE means the differences between the original image and the produced image. The general formula for MSE is as follows:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad \text{…(Error! No text of specified style in document..2)}$$

where "m" and" n" refer to the size of the image and I (i,j) and K(i,j) refer to the pixel value of the stego image and the cover image. PSNR is assessed in decibel (dB). This section introduces discussion on the experimental results of the suggested method and assess the performance of the suggested method through using the quality metrices. In addition, comparison is made between the gained solutions with the previous solutions. Table 2 introduces the results of the existing techniques and Table 3 introduces the results of this proposed method.

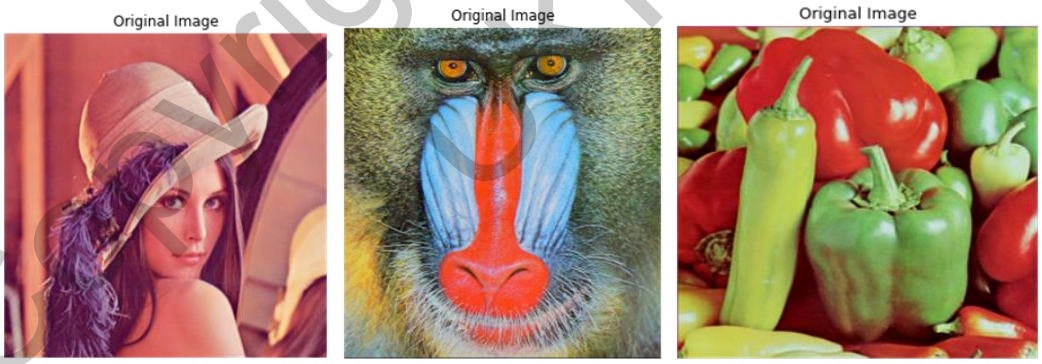
Table 2 Results of the existhing methods

The existing methods	PSNR (db)			Secret text or Capacity (bits)	Type of image and its size
	Lena	Pepper	Baboon		
(Neamah et al. 2020)	53.65	39.99	40.89	24,250	Color images, 512*512
(Abdulwahed 2020)	61.10	61.22	61.20	393,216	Grayscale images,512*512
(Prasad & Pal 2017)	31.01	30.10	31.01	2,219,715	Color images,512*512

Table 3 Results of the proposed method

Color Images size (512*512)	Capacity 34,400 (bits)		Capacity 413,600 (bits)		Capacity 1,992,000000(bits)	
	PSNR	MSE	PSNR	MSE	PSNR	MSE
Lena	63.643	0.028	62.519	0.036	60.182	0.062
Pepper	63.951	0.026	62.813	0.034	60.356	0.059
Baboon	63.664	0.027	62.519	0.036	60.214	0.061

The results of the experiment showed that the proposed method achieves a high concealment capability with high value of PSNR "63.95". By examining the images in Figure 4, human eyes are not able to notice the difference between the stego and the original images. The results highlighted in Table 3 have shown that the predicted calculations for the PSNR and MSE measurements of the three (512*512) images with different volumes of secret text are based on the proposed method. Obviously, the values of PSNR achieved by this proposed method are higher when compared to the values of PSNR of the previous methods. In addition, the experiment reveals the significant improvement in the MSE values of the proposed method. The lower MSE as well as the higher PSNR calculations prove that the proposed method has added double security levels by using the encryption and Fibonacci decomposition methods. It has also added a high payload capacity for data embedding by using the compression algorithm.



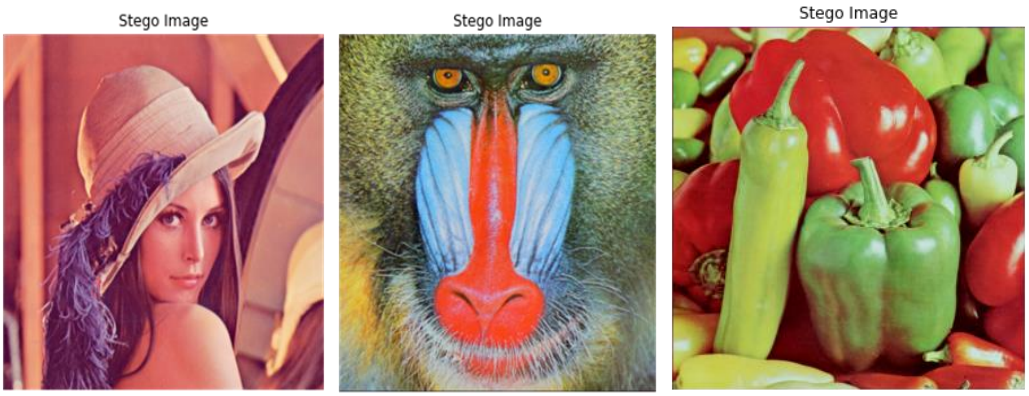


Figure 4 Original images and stego images

As a result of utilizing a combination of Huffman coding, Advanced Encryption Standard algorithm, and Fibonacci decomposition with enhanced embedding methods, the proposed technique of this study has shown better concealment algorithms compared to other previous studies such as the one presented by Neamah et al. (2020) and Prasad & Pal (2017). They have achieved low PSNR values for stego image with low embedding capacity of secret text with the largest volume of confidential data used ranging between 24,250 bits - 2,219,715 bits. Although, the volume of secret data used is small, their PSNR level is less than the levels obtained by this proposed method due to the combination of three techniques mentioned above. Huffman coding has increased the embedding capacity, but the Advanced Encryption Standard algorithm has improved the security of the secret data. Finally, the proposed method has introduced an additional obstacle for any future intruders.

In this study, the secret data has been concealed inside a color image, where the embedding capacity was “51.7 KB” and the value of PSNR was “62.81”. Although, the data embedding within grayscale images is simpler if compared to color images, the results obtained by this proposed technique achieved a higher PSNR value than the previous results highlighted by (Abdulwahed 2020) who concealed the secret data inside grayscale images, where his embedding capacity and PSNR values were , “49.152 KB” and “61.22” respectively . Finally, the secret extracted text used in the experiment of this study has been examined to ensure it is free from any linguistic mistakes where the results have demonstrated that the text file does not suffer from any linguistic mistakes.

VI. CONCLUSION

The main goal of this study is enhancing the proposed image steganography method through increasing the payload capacity, security, robustness, and imperceptibility of the image. The results have shown the efficiency of the proposed method. The other important contribution is the increase in the security of the secret text using the encryption technique and the use of different embedding algorithms based on the choice of the pixels of the cover image by the suggested algorithm. The results of PSNR and MSE have demonstrated that the visual quality of the stego image has been achieved, which refers to the low differences between the original image and the produced image. . One of these directions is that security can be improved by combining steganography techniques with other techniques such as cryptography; this may accomplish better results in the aspects of robustness and security. The other direction is the limitation of embedding capacity needs to handle the secret data before the embedding process by a special technique interactive with embedding methods.

For any future direction it is necessary to examine recent embedding techniques especially that are based on deep neural network architectures. These techniques have the ability to produce much more sophisticated embedding. Hence, embedding text within images through these sophisticated embedding would considerably enhance the security behind the steganography.

ACKNOWLEDGEMENT

The authors would like to thanks, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia by giving the authors an opportunity to conduct this research.

REFERENCE

Abdulwahed, M. N. 2020. An effective and secure digital image steganography scheme using two random function and chaotic map. *Journal of Theoretical and Applied Information Technology* 98(1): 78–91.

Abu-Almash, F. S. 2018. New Steganography System Based on Huffman Coding and Fibonacci Decomposition. *Ibn AL- Haitham Journal For Pure and Applied Science* 31(1): 13. doi:10.30526/31.1.1831

Al-Aidroos, N. M. & Bahamish, H. A. 2019. Image Steganography Based on LSB Matching and Image Enlargement. *2019 1st International Conference of Intelligent Computing and Engineering: Toward Intelligent Solutions for Developing and Empowering our Societies, ICOICE 2019* 1–6. doi:10.1109/ICOICE48418.2019.9035172

Al-Husainy, M. A. F. & Uliyan, D. M. 2019. A secret-key image steganography technique using random chain codes. *International Journal of Technology* 10(4): 731–740. doi:10.14716/ijtech.v10i4.653

Arroyo, J. C. T., Espadero, J. A., Ganas, M. A., Ardeña, R. F., Vilchez, R. N. & Delima, A. J. P. 2020. An efficient least significant bit image steganography with secret writing and compression techniques. *International Journal of Advanced Trends in Computer Science and Engineering* 9(3): 3280–3286. doi:10.30534/ijatcse/2020/124932020

Astuti, E. Z., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A. & Sarker, M. K. 2020. LSB-based Bit Flipping Methods for Color Image Steganography. *Journal of Physics: Conference Series* 1501(1). doi:10.1088/1742-6596/1501/1/012019

Bhardwaj, R. & Sharma, V. 2016. Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution. *Procedia Computer Science* 93(September): 832–838. doi:10.1016/j.procs.2016.07.245

Chen, B., Luo, W., Zheng, P. & Huang, J. 2020. Universal stego post-processing for enhancing image steganography. *Contents lists available at ScienceDirect Journal of Information Security and Applications journal homepage: www.elsevier.com/locate/jisa* 55. doi:/10.1016/j.jisa.2020.102664

Elharrouss, O., Almaadeed, N. & Al-Maadeed, S. 2020. An image steganography approach based on k-least significant bits (k-LSB). *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020* 131–135. doi:10.1109/ICIoT48696.2020.9089566

Hattim, M. & Taha, Z. 2019. Secure and hidden text using aes cryptography and lsb steganography.

Journal of Engineering Science and Technology 14(3): 1434–1450.

Karakus, S. & Avci, E. 2020. A new image steganography method with optimum pixel similarity for data hiding in medical images. *Medical Hypotheses* 139(March): 109691. doi:10.1016/j.mehy.2020.109691

Mangla, F. U., Nokhaiz, S., Ramzan, M. & Lali, I. U. 2019. A novel steganography technique using grayscale image segmentation 6(5): 84–91.

Neamah, R. M., Abed, J. A. & Abbood, E. A. 2020. Hide text depending on the three channels of pixels in color images using the modified LSB algorithm. *International Journal of Electrical and Computer Engineering* 10(1): 809–815. doi:10.11591/ijece.v10i1.pp809-815

Prasad, S. & Pal, A. K. 2017. An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society Open Science* 4(4). doi:10.1098/rsos.161066

Rachael, O., Misra, S., Ahuja, R., Adewumi, A., Ayeni, F. & Mmaskeliunas, R. 2020. Image Steganography and Steganalysis Based on Least Significant Bit (LSB). *Lecture Notes in Electrical Engineering* 605(September): 1100–1111. doi:10.1007/978-3-030-30577-2_97

Rajput, G. G. & Chavan, R. 2017. A novel approach for image steganography based on LSB technique. *ACM International Conference Proceeding Series* Part F1302: 167–170. doi:10.1145/3093241.3093247

Sethi, N. & Patel, P. 2019. Steganography Technique with Huffman Code. *International Journal of Recent Technology and Engineering* 8(2S4): 867–870. doi:10.35940/ijrte.b1173.0782s419

Setiadi, D. R. I. M. 2019. Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. *Journal of King Saud University - Computer and Information Sciences* (2019). doi:10.1016/j.jksuci.2019.12.007

Yadav, P. & Dutta, M. 2017. 3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio. *2017 4th International Conference on Image Information Processing, ICIIP 2017* 2018-Janua: 122–126. doi:10.1109/ICIIP.2017.8313696

Yahaya, M. M. & Ajibola, A. 2019. Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 5(6): 317–322. doi:10.32628/cseit195659