Journal of Theoretical and Applied Information Technology
30th November 2017. Vol.95. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION

[1, 3] MOHAMMED MAHDI HASHIM, [1, 2] MOHD SHAFRY MOHD RAHIM

[1] Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia

[2] UTM (IRDA) Digital Media Center, Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia

[3]Uruk University, Baghdad, Iraq

E-mail: [1]comp.mmh@gmail.com, [2]shafry@utm.my

ABSTRACT

Presently, the evolution massive of the internet gives more attention, play important role in the field of communication, and transfer messages. Nowadays, hiding sensitive or secret information inside trusted media such image without being noticed by the intruder is more needed because of the privacy cases, this method called steganography. In this paper, a method of hiding secret data in an image based on odd/even pixels distribution scheme and two parameters random function have introduced. The objective of this study is to increase the imperceptibility of proposed method with a high payload capacity of secret message. Two main process are used in the proposed method, which are embedding process and extracting process. Huffman coding technique is utilize to compress the secret message before embedding process. The security and capacity of the proposed method will increase after preparation secret message. The main objective of proposed scheme is to increase image quality (PSNR) in stego image. Two main things make the method effective: first, checking matching of secret bits with LSB and mapping to determine even and odd word during embedding, and second, segmenting the secret message to track and map every bit in stego image. Experimental results of the proposed method can achieve a high imperceptibility and robustness was emphasized.

Keywords: *Image Steganography, Least Significant Bit (LSB), Odd/Even pixel distribution, Peak Signal to Noise Ratio (PSNR), Information Security*

1. INTRODUCTION

Now days, the security factor of information is the most significant factors of information technology and communication. Cryptography was created as a technique for satisfy personal private information communication, and various methods proposed to encrypt and decrypt information to keep the message more secret. The spread of multimedia data in our electronic world detect a new way for communication using digital Steganography. Steganography, where the appearance of communication is hidden, differs from cryptography, in which communication is evident but the content of that communication is unclear.

Steganography is the art and science that deals with information 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]. 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][25]. There is a different between steganography and cryptography in the manner, so steganography hides the existence of data while cryptography scrambles the data to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

change it's the meaning and quality so that it looks meaningless to others.

the general requirements to obtain a better performance of hiding data and measures the strengths and weaknesses points in steganography techniques are (security, capacity ,Imperceptibility). First requirement is capacity, it refers to the maximum amount of secret message which can be embedded into cover image without retraction of the image quality. It is usually represented in terms of bits per pixel. Security is the second important requirement evaluation standard in steganography. Security in steganography should be resistance against the steganalysis attacks. The last requirement of steganography is imperceptibility. Imperceptibility means the image Transparency and quality. After hiding secret message into cover image, Transparency and quality will be degraded into stego-image as compared to cover-image. so the result of stego image should be appears as possible as like the original image . The Imperceptibility in the stego image can be measured by peak signal-to-noise ratio (PSNR). So higher the PSNR means a good image quality.

Steganography hides the data in a cover media such. Text, audio, image or video. Many various kinds in Steganography based on the type of cover media, such as image steganography, audio steganography, text steganography video steganography [3], [4]. In steganography the media carrier is called the cover object and the hidden information it called the payload capacity. The cover object depends on the amount of secret message that can be hidden, the imperceptibility of the message and its robustness. Image is one of most popular as a cover object because of its widely used in daily applications and high redundancy in representation. Hide secret message within cover image is called the stego-image. Image steganography techniques are classified into two major categories such as spatial domain and transform domain.

In order to make steganography method more effective three questions must be solved (security, capacity and imperceptibility). The most important question is the imperceptibility, which shows how difficult it is to determine and distinguish the existence of a hidden message, this is achieved by odd/even pixels distribution scheme. Other important question in steganography is security, which refers to a batter steganography system, resists the external attacks. Last question is capacity, which is the maximum information that can safely hide in a cover image with high image quality and undetectability (imperceptibility) of the data. These important questions are going to solve in proposed method.

In this paper, an image steganography technique is proposed based on odd/even pixels distribution scheme and two parameters random function for hiding secret message with high level of security without compromising on the quality of the stego image and no lossless of secret message. Two main process are used in the proposed scheme, which are embedding process and extracting process. Huffman coding technique is utilize to compress the secret message before embedding process. The security and capacity of the proposed method will increase after preparation secret message. Increase PSNR of image with high security these are the aims of the proposed. Proposed scheme does not allow revealing secret data to pursuer or intruder. Two main things make the method effective: first, checking matching of secret bits with LSB and mapping to determine even and odd word during embedding, and second, segmenting the secret message to track and map every bit in stego image. In addition to maintaining the security and capacity of the proposed method, robustness was also emphasized.

The remainder of the paper is structured as follows sections: In section 2, introduced briefly description about the simple steganography method that are related to the proposed work. The proposed method describes in section 3. In Section 4, Experimental result is given in details. Finally, in section 5, the conclusion of this paper.

2- RELATED WORK.

In this section, authors are discussing one of the most popular and frequently substitution technique utilized in steganography method is the Least-Significant-Bit (LSB) that form the basis to the proposed method. The embedding process is hiding secret message bits in the LSB of randomly

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

selected pixels. The pixel selection is depends on stego key shared between sender and receiver [10]. This technique was easy to be implemented and able to increase security of the secret messages. One bit-plane method was implemented. The second step was using Huffman compression to be applied on the secret message. This method enhanced the capability of embedding secret message and the security performance.

New steganography system using noise for embedding was suggested in (2016) by Wu, et al. [9], Sanguinetti, et al. [24] using noise to provide good environment against statistical attack and to increase the security even with high capacity. Sedighi, et al. [11] proved that choosing hosting image in advance has an effect on security and capacity. Mohamed, M. and Mohamed, [12] proved that the capacity relies on the method used like LSB. Improving the embedding method based on edge area is still promising and worthwhile [13].

Al-Dmour et al. [8] have proposed a Boolean operation known as XOR in their proposed work. The XOR operation was an easy and so effective process especially to reduce the differences between the cover and stego-image. The proposed algorithm embedded the three bits of secret data in the selected adaptive edge of the cover image. However, the proposed algorithm would restrict the area of the secret data that could be embedded.

A novel approach has proposed by manjula et al [15], to enhance secure image steganography based on double encryption algorithms. First encrypted using AES algorithm and then public cryptography method ECC .Then to reduce the payload capacity, the LZW compressed algorithm has been implement. The night tour algorithm is proposed to improve LSB insertion. The result show that a good image quality and reduce the amount of distortion in stego image.

Secure Image steganography through The EMD (Exploiting Modification Direction) and spatial domain has done by Kuo et al. The proposed scheme has two main contribution make the system more effective. First is only n/2 pixels will be modified and the value is +1 or −1 when the group has n pixels. Secondly, the embedded capacity maintains at least 1 bpp when n is increasing. The cover image is divided into non-overlapping blocks by scanning each line of pixel from left to right and top to down manner to obtain optimal n-tuples to hide the secret message [29].

Jiang N et al. [16] introduced two LSB steganography algorithms based on NEQR for quantum images. Embedding the secret bits by replace with LSB of the pixels directly. Second algorithm is block of LSB that belong to one image block. The extracting algorithm can retrieve the secret data only depends on the stego key. Experimental results show a good image quality and capacity and the robustness can be adjusted depends on the needs of application.

Genetic Algorithm (GA) based on a tunable visual image quality was introduced by (Kanan, and Nazeri ,2014). Lossless data in special domain was used to optimize problems in steganography. Experimental results show high-embedded capacity with enhanced PSNR [17].

Muhammad. K et al. [20] proposed an imperceptible image steganographic technique based on PBSA and M -LSB for grayscale images. The secret data is manipulated by encrypted and shuffled using pattern based bits shuffling algorithm (PBSA) . The result of encrypted message is embedded by using M - LSB method , scattering secret message inside the image pixel , hence making its extraction relatively more difficult for attackers. Proposed method is evaluated by qualitative and quantitative analysis which supports the effectiveness of the proposed method.

A new symmetric key based on image steganography technique has introduced by Rajendran et al. the pixel position has been chosen randomly to hide secret bits. The main issue of proposed system is to selected pixel position randomly from cover image using chaotic map to increase the efficiency and security. Four different grayscale images are used for testing and prove the performance of proposed system [28].

Seyyedi, et al. [21]. Introduced an image steganography based on wavelet transform and RC4 algorithm. The Cover image in proposed method is partitioned into 64 blocks of (8 × 8) with

Journal of Theoretical and Applied Information Technology
30th November 2017. Vol.95. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

applied wavelet transform. Secret message in this method encrypted before embedding by using RC4 algorithm to increase the security of the system. Stego image here is difficult to detect by HVS attack.

According to Roy research, the input is a carrier image and secret message and the output is stego-image. The scheme process was started with converting the secret message into binary code and then calculating its size. In this algorithm image is partitioned into non-overlapping blocks and Find smooth and textured areas inside the block using the individual entropies. Variable embedding rate data hiding scheme is ensured both smooth and textured areas in the cover image and this can be optimally used with high embedding efficiency. The method is shown optimally results in terms of stego- image fidelity and statistical imperceptibility [30].

Different carrier of image steganography used to encrypt the secret data proposed by Sneha Bansod and Gunjan Bhure (2014). The secure data is hidden using some JPEG or BMP images, which may be more helpful in this case and to keep the data safe. The LSB modification is used to embed the secret data [31].

Thakur et al. have carried out a novel security method based on image Steganography with cryptograph to hide secret image. The idea of the presented method is to encrypt the secret image using the proposed encryption scheme at first and then hides the encrypted image by Steganography scheme. The algorithm consists of two main sections. The first is to proposed encryption technique to encrypt the confidential image based on symmetric key concept. The second uses Steganography technique to hide the encrypted image using randomization techniques and LSB insertion [33].

Hence, more researcher efforts are still required to obtain image steganography techniques that provide an imperceptibility, capacity and high security against intruder. This study suggests an efficient and batter imperceptibility algorithm based on odd/even pixels distribution scheme and two parameters random function. The results showed this algorithm was much secure with a good imperceptibility invisibility.

3- PROPOSED TECHNIQUE.

The proposed method used the spatial domain of the cover image based on odd/even pixels distribution scheme and two parameters random function for hiding a large amount of data with higher security thereby generating a stego image. The main in this paper is to develop and design a method that will provide a higher level of security to the secret message without compromising on the quality of the stego image. Figure 1. Show the entire proposed scheme.

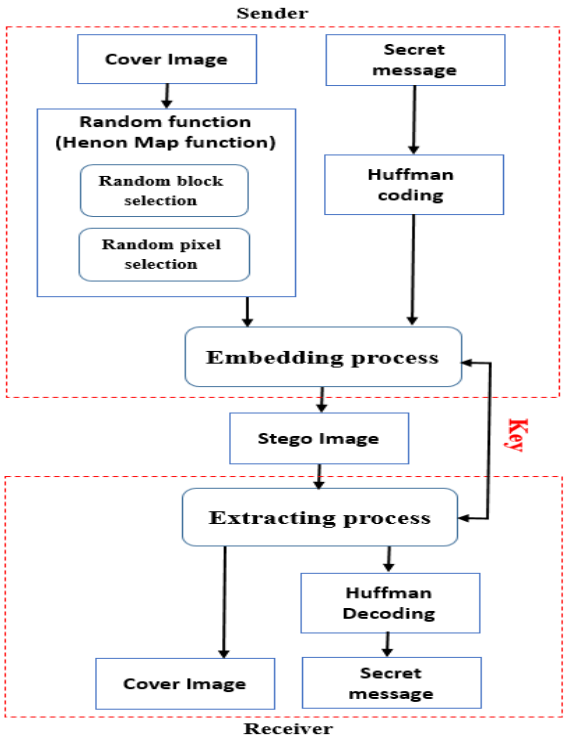

Figure 1: Block diagram of proposed scheme.

The proposed method contains two phases:

3.1- Embedding process.

In our proposed method, two processes in side embedding stage (block selection and embedding data) run simultaneously for inserting or hiding text message into an image. As initial stage we divide, the cover image into 8×8 blocks each with 64×64 pixels. The process of selection will be occur randomly under Henon map function for blocks and then pixels, as shown in Figure 2. Henon map function is used to achieve objective of the security random function.

Journal of Theoretical and Applied Information Technology
30th November 2017. Vol.95. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

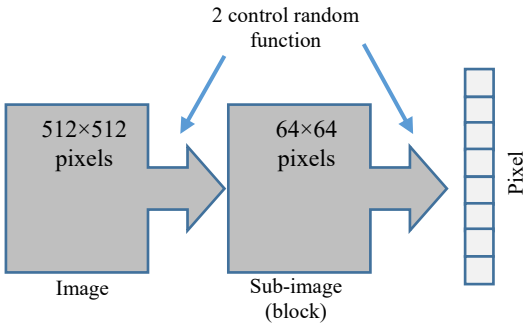

Figure 2: Get pixel from image with method.

Embedded the secret message in the LSB according to the odd/even distribution method is the second objective of our proposed method to keep the quality of the image same of original. It means the pixel that end with 1 in LSB that's mean pixel value is odd or else it's even value. Embedding in this case will insert the ones value of secret message to odd pixels and zeros of secret message to even pixels. Standard embedding illustrate in Figure 3.

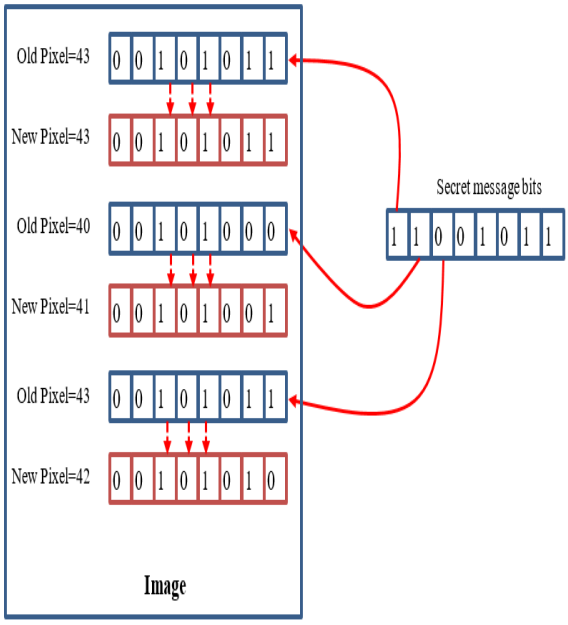

Figure 3: Standard Embedding secret bits to image pixels.

Means embedding 1 value from secret bits to 1 value of pixel made it no change as shown in Figure 2, then the pixel stay the same without change in other hand embedding 1 of secret bit value to 0 of LSB pixel value made change in pixel value replace by one, also when embed 0 value to 1 value the pixel replace by 0 as in the third case of example. Therefore, the imperceptibility of our method will increase.

3.1.1 Embedding Algorithm.

Input: Original image of size N×N, secret message.

Output: Stego Image.

1. Read and convert secret message into binary
2. Perform the Huffman coding on secret message.
3. Calculate the size of the message (no. of character or byte).
4. Let L=length of secret message in bits.
5. Select a cover image (512 x 512).
6. Generate random number by using Henon map function.
7. Select one block of 64 blocks each of (8x8) by using number generator.
8. Used second parameter of Henon map to select the destination pixel.
9. Create M vector and arrange it according to Odd/Even.
10. Mark the LSB of each pixel.
11. Then make loop from I=1: N.
12. Get message bit (0 or 1).
13. If secret message is 0 and pixel is even, do nothing
14. If secret message = 0 and pixel is odd, replace by 0 the value of the LSB layer.
15. If secret message is 1 and pixel is even, replace by 1 the value of the LSB layer
16. If message bit is 1 and pixel is odd, do nothing.
17. I= I+1
18. Return Stego Image.
19. END.

3.2 - Extracting Process.

Extracting process aim to get the data from LSB pixels at the same time should follow the procedure designed and build in embedding process. Extracting process located in the other part (receiver) which includes procedure agreed by the two parties using stego key to guide the process. The procedure of extracting is like the embedding

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

process but in reverse, that's mean that collect the components of the LSBs of the pixels and determine the pixel if it's odd or even. Means, Even pixel value contain 0 in LSB position due to binary impact value, and 1 in LSB of odd pixel value. Most of variable information reflected by image and block partitioning, in additional to fragment of secret message. Such of this information called public information, while private information considered as the method followed by embedding process. For the two process, embedding and extracting achieved two main objectives security and imperceptibility as shown in Figure 4.

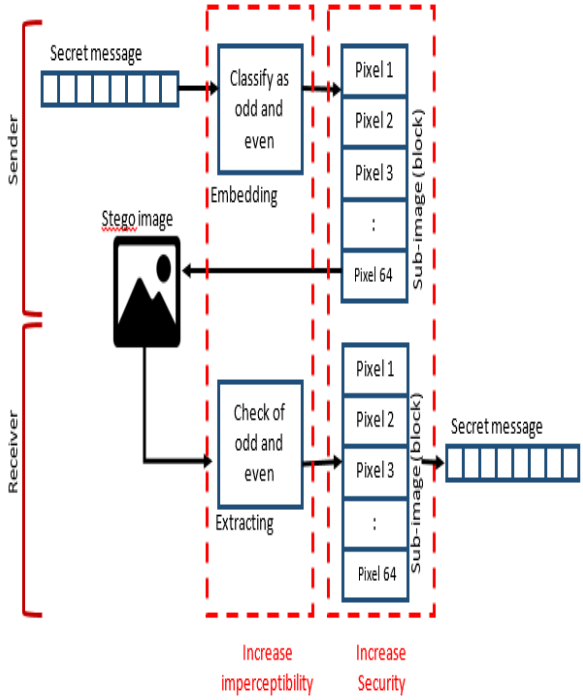

Figure 4: Two main objectives within embedding and extracting process.

4- EXPERIMENTAL RESULT.

In this section. Some experiments are carried out to prove the performance of the proposed scheme. Every data hiding Method that is designed to enhance the quality of the cover image as well as the payload capacity of secret data that can be hidden. Images that have hidden data will be subject to alteration and distortion [32].

The proposed method was tested for stego-image accuracy, impedance against steganalysis, additional to efficiency of embedding and runtime performance. The proposed scheme has been simulated using the MATLAB 10 program on Windows 10. Four standard images of size 512 x 512 color image are used as the cover-image to create the stego-image. In the experiments, the proposed method is compared with [16], GA [17], [18], NEQR [19] PBSA [20] and [21] in image quality (PSNR) and embedding efficiency.

The quality and performance of stego image is evaluated using PSNR peak signal to noise ratio. PSNR is used to measurements performance of steganography [23] [26]. To calculate PSNR, first MSE (Mean Square Error) is calculated using equation (1):

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

MSE is the average squared difference between original image (I) and stego image (S). NxN are the size of row and column of cover image. Thereafter PSNR value is calculated using equation (3). A higher value of PSNR is better because of the superiority of the signal to that of the noise [22].

$$PSNR = 10.log_{10}\left(\frac{MAX_1^2}{MSE}\right) \quad (2)$$

Where MAX is the maximum possible pixel value of the image. Another performance measurement is the embedding payload efficiency (capacity). The experimental results of this algorithm shows that the PSNR between both the cover and stego image is more than 66 that is better the threshold for human visible system (HVS). Thus, it is evident that the proposed algorithm make much less visual distortion because of embedding. Embedding payload is the amount of secret data can be hidden within the cover media, which can expressed as number of bits, which shows the max message size can inserted

Journal of Theoretical and Applied Information Technology
30th November 2017. Vol.95. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

into a cover image [27]. The embedding capacity efficiency is calculated using equation (4):

$$\text{Embedding capacity} = \frac{\text{The number of message bits}}{\text{The number of cover image pixels}} \text{ (bit /pixel)} \quad (3)$$

The embedding capacity efficiency is evaluated by the percentage of the embedded secret bits in the whole pixels of the cover image.

To benchmark the observation of this study with already existing literature, the proposed method has been tested using four images according to table 1.

Table 1: Images are used from dataset to benchmark.

Lena	Pepper
	
Baboon	**Cameraman**
	

The results that are obtained from these experiments are recorded and can be summarized in Table 2, Table 3 and Table 4.

Table 2: Comparison of the quality of the Stego-Image for proposed method and other methods.

Image / Method	Lena	Baboon	Papers	Camera man
Ref [16]	51.09	51.37	-	-
GA Ref [17]	47.03	47.02	47.03	
Ref [18]	39.63	41.58	38.65	-
NEQR Ref [19]	50.84	50.37	50.62	51.61
Proposed method	66.63	65.85	67.69	67.23

Table 2 list the PSNR comparison of proposed technique with other proposed method. For comparison text message has used as secret message. In order to have a comparison between the proposed algorithm and others methods, a graphical representation of the PSNR values is shown in Figure 5. It is clear that the PSNR for the proposed algorithm achieves a higher visual quality compared others methods.

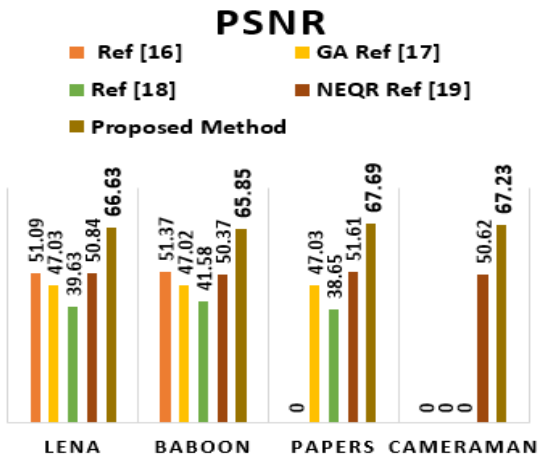

Figure 5: Comparison of PSNR

Table3: Experimental results based on PSNR with embedding capacity=1.

Image / Method	Lena	Baboon	Average
PBSA Ref [20]	51.13	51.15	51.14
Ref [21]	65.09	-	65.09
Proposed method	66.63	65.85	66.24

Table 3 shows the experimental results based on PSNR with embedding capacity =1 i.e. 1 bit per pixel for the proposed method, PBSA [20] and [21]. The image used "Lena" and "Baboon" gray scale images with size 512*512 to show the experimental result. It is observed that, the proposed method obtain higher PSNR value compared to PBSA [20] and [21] since the proposed method manipulate least significant bit of every pixel to hide the secret message.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

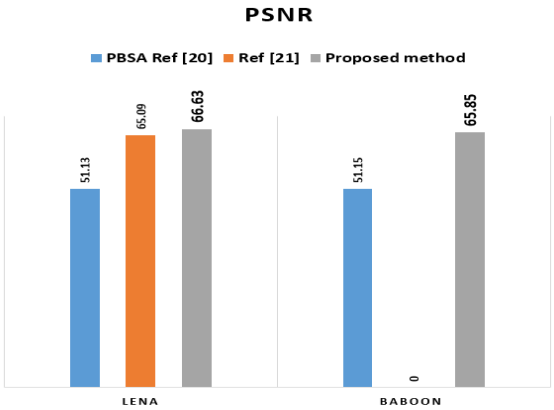

Figure 6: Comparison of PSNR for proposed method and other methods.

A graphical representation of PSNR values is shown in Figure 6. The proposed method is provides a higher PSNR than PBSA [20] and [21]. Experimental result demonstrated that the proposed algorithm has achieved better imperceptibility result with high embedded capacity than other technique.

Table4: Comparison of the capacity for the proposed scheme and other methods.

Method	Capacity in Byte
Ref [16]	**17125**
GA Ref [17]	**16384**
Ref [18]	**4287**
NEQR Ref [19]	**32000**
Proposed method	**32768**

Table 4 list the embedding capacity comparison of proposed technique with other proposed methods. In order to have a comparison between the proposed algorithm and others methods, a graphical representation of the embedding capacity values is shown in Figure 7.

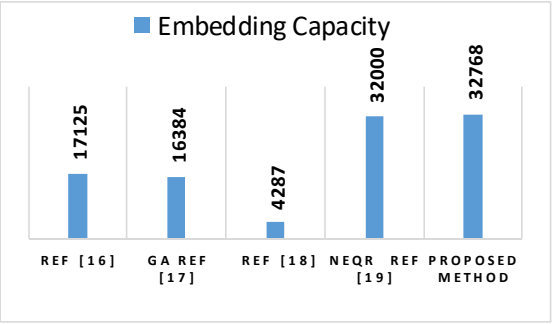

Figure 7. Comparison of the capacity.

However, proposed method has limitations in term of capacity, so increase the capacity will degradation image quality (imperceptibility) and other limitation in proposed method, four dataset only have been tested within this method.

From the above empirical results, we can see the distortion rate (imperceptibility) of image and hiding capacity comparison with others. Therefore, the proposed method is reduced the distortion on the cover image with high hiding capacity. We have considers some disadvantage (weakness) and tried to overcome some problem and still some improvement needed with future work.

5- Conclusion

In this paper, an imperceptible image steganographic technique based on odd/even pixel distribution scheme is proposed using spatial domain, with maintaining the security of secret data embedded that is generated by Henon maps function. Huffman coding technique is used to compress the secret message before embedding. Manipulating secret message before embedding help to increase the security and capacity of the scheme. Aim of the proposed system is to increase PSNR of the image so that it can stop front of any type of attack, and at the same time increase the payload capacity of the secret message. Proposed system does not allow revealing secret data to pursuer or intruder. Two main things make the system effective: first, checking matching of secret bits with LSB and mapping to determine even and odd word during embedding, and second, segmenting the secret message to track and map every bit in stego image. In addition to maintaining the security and capacity of the proposed system with high visual quality of stego images by compare with other methods, robustness was also emphasized.

ACKNOWLEDGEMENTS

Mohammed is grateful to the ministry of higher education and scientific research of Iraq and Uruk University for the study leave and University Technology Malaysia for technical assistance.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[1] Sellars, Duncan. "An introduction to steganography." *Student Papers* (1999).

[2] Al-Mualla,Mohammed and Hussain Al-Ahmad. "Information hiding: steganography and watermarking." Proceedings of the IEEE (2008).

[3] Bhattacharyya, Debnath, Tai-hoon Kim, and Poulami Dutta. "A method of data hiding in audio signal." Journal of the Chinese Institute of Engineers 35.5 (2012): 523-528.

[4] Dumitrescu, Sorina, Xiaolin Wu, and Nasir Memon. "On steganalysis of random LSB embedding in continuous-tone images." *Image Processing. 2002. Proceedings. 2002 International Conference on*. Vol. 3. IEEE, 2002.

[5] Subhedar, Mansi S., and Vijay H. Mankar. "Current status and key issues in image steganography: A survey." Computer science review 13 (2014): 95-113.

[6] Huffman, David A. "A method for the construction of minimum-redundancy codes." Proceedings of the IRE 40.9 (1952): 1098-1101.

[7] Mathur, Mridul Kumar, Seema Loonker, and Dheeraj Saxena. "Lossless Huffman coding technique for image compression and reconstruction using binary trees." *International Journal of Computer Technology and Applications* 3.1 (2012).

[8] Al-Dmour, Hayat, and Ahmed Al-Ani. "A steganography embedding method based on edge identification and XOR coding." *Expert systems with Applications* 46 (2016): 293-306.

[9] Wu, Ben,et al."Dispersion Deployment and Compensation for Optical Steganography Based on Noise." *IEEE Photonics Technology Letters* 28.4 (2016): 421-424.

[10] ALI, AHMED HUSSAIN, MOHD ROSMADI MOKHTAR, and LOAY EDWAR GEORGE. "ENHANCING THE HIDING CAPACITY OF AUDIO STEGANOGRAPHY BASED ON BLOCK MAPPING." Journal of Theoretical & Applied Information Technology 95.7 (2017):166

[11] Sedighi, Vahid, Rémi Cogranne, and Jessica Fridrich. "Content-adaptive steganography by minimizing statistical detectability." *IEEE* Transactions on Information Forensics and Security 11.2 (2016): 221-234

[12] Mohamed, Marghny H.,and Loay M. Mohamed. "High Capacity Image Steganography Technique based on LSB Substitution Method." Applied Mathematics & Information Sciences 10.1 (2016): 259.

[13] Mungmode, Sachin, R. R. Sedamkar, and Niranjan Kulkarni. "An Enhanced Edge Adaptive Steganography Approach using Threshold Value for Region Selection." arXiv preprint arXiv:1601.02076 (2016).

[15] Manjula, Y., and K. B. Shivakumar. "Enhanced secure image steganography using double encryption algorithms." Computing for Sustainable Global Development *(INDIACom)*, 2016 3rd International Conference on. IEEE, 2016.

[16] Mishra, Minati, Ashanta Ranjan Routray, and Sunit Kumar. "High Security Image Steganography with Modified Arnold cat map." arXiv preprint arXiv:1408.3838 (2014).

[17] Laha, Sumit, and Rinita Roy. "An improved image steganography scheme with high visual image quality." Computing, Communication and Security (ICCCS), 2015 International Conference *on*. IEEE, 2015.

[18] Singh, Saurabh, and Ashutosh Datar. "Improved hash based approach for secure color image steganography using canny edge detection method." International Journal of Computer Science and Network Security (IJCSNS) 15.7 (2015): 92.

[19] Jiang, Nan, Na Zhao, and Luo Wang. "LSB based quantum image steganography algorithm." International Journal of Theoretical Physics 55.1 (2016): 107-123.

[20] Muhammad, Khan, et al. "A new image steganographic technique using pattern based bits shuffling and magic LSB for grayscale images." arXiv preprint arXiv*:1601.01386* (2016).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[21] Seyyedi, Seyyed Amin, Vasili Sadau, and Nick Ivanov. "A Secure Steganography Method Based on Integer Lifting Wavelet Transform." IJ Network Security 18.1 (2016).

[22] SALMAN, AFAN GALIH. "STEGANOGRAPHY USING PIXEL VALUE DIFFERENCING SPIRAL." Journal of Theoretical & Applied Information Technology 75.1 (2015).

[23] Manimurugan, S., and Saad Al-Mutairi. "A NOVEL SECRET IMAGE HIDING TECHNIQUE FOR SECURE TRANSMISSION." Journal of Theoretical & Applied Information Technology 95.1 (2017):166

[24] Sanguinetti, Bruno, et al. "Perfectly secure steganography: hiding information in the quantum noise of a photograph." Physical Review A 93.1(2016): 012336.

[25] KADHEM, SUHAD M., MOHAMMED ALI, and W. DHURGHAM. "PROPOSED HYBRID METHOD TO HIDE INFORMATION IN ARABIC TEXT." Journal of Theoretical & Applied Information Technology 95.7 (2017).

[26] Sharifara, Ali, Mohd Shafry Mohd Rahim, and Morteza Bashardoost. "A novel approach to enhance robustness in digital image watermarking using multiple bit-planes of intermediate significant bits." *Informatics and* Creative Multimedia (ICICM), 2013 International Conference on .IEEE , 3013.

[27] Bashardoost, Morteza, et al. "A Novel Approach to Enhance the Security of the LSB Image Steganography."" *Research Journal of Applied Sciences, Engineering and Technology* 7.19 (2014): 3957-3963.

[28] Rajendran, Sujarani, and Manivannan Doraipandian. "Chaotic Map Based Random Image Steganography Using LSB Technique." *IJ Network Security* 19.4 (2017): 593-598.

[29] Kuo, Wen-Chung, Chun-Cheng Wang, and Hong-Ching Hou. "Signed digit data hiding scheme." *Information Processing Letters* 116.2 (2016): 183-191.

[30] Roy, Ratnakirti, and Suvamoy Changder. "Image steganography with block entropy based segmentation and variable rate embedding." *Business and Information Management (ICBIM), 2014 2nd International Conference on*. IEEE, 2014.

[31] Bansod, Sneha, and Gunjan Bhure. "Data encryption by image steganography." *Int. J. Inform. Comput. Technol. Int. Res. Publ. House* 4 (2014): 453-458.

[32] Nayak DK, Bhagvati C. A threshold-LSB based information hiding scheme using digital images. In: 4th InternationalConference on Computer and Communication Technology; 20{22 September 2013; Allahabad, India. New York, NY, USA: IEEE. pp. 269-272.