Assiut Univ. J. of Mathematics and Computer Science Printed ISSN 1687-4897
48(2), pp.110-124 (2019)

AN IMPROVED LSB INVERSION IMAGE STEGANOGRAPHIC TECHNIQUE

Loay Mamdouh and Dalia Nashat

Department of Mathematics, Faculty of Science, Assiut University, Egypt

Received: 18/9/2019 **Accepted:**4/11/2019 **Available Online:**1/12/2019

Data hiding is a major mechanism used for secure data transmission in computer networks. One of the most important branches in data hiding is Steganography. Steganography techniques concerns with hiding the secret data within the cover image in order to avoid detection. Least Significant Bit (LSB) technique is used widely in steganographic images. The traditional LSB method replaces some LSB of the cover image with the secret data. In this paper, a new method based on LSB for image steganography is presented. The goal of the proposed method is to increase the embedding capacity and enhance the stego image quality. We invert LSBs of the cover image depending on the value of the secret data. The experimental results of this study indicate that our method achieves high capacity and good imperceptibility quality of the stego image.

Keywords: Information security, Image processing, Data hiding, Steganography, Image Steganography, LSB.

INTRODUCTION

In recent decades, the increasing progress in the evolution of the internet provides many benefits for transmission secret data over networks. One of the disadvantages of that evolution is that secret data becomes a candidate for unauthorized access during transmission over networks. Thus the issues of data security and confidentiality become the main topic in today's era. Many different techniques have been presented to protect data such as cryptography, steganography and watermarking [1, 2, 3]. Cryptography encrypts data into an unreadable form and the unauthorized user can see and decrypt the encrypted data if he has a key. Steganography differs from this, which concerns with hiding the existence of data, while watermarking concerns with preserving copyright

[1, 3, 4]. Steganography and watermarking are branches of data hiding [5].

Steganography is the art of hidden data in cover media such as text, audio, images, videos, and web, etc. to be difficult for any unauthorized user to know there is a data exist in the cover media [4, 6]. Image steganography in comparison with other forms of steganography is used widely due to a large amount of redundant data exists in the images that can be easily replaced to hide information in them. Also, it takes advantage of the limited power of the human visual system (HVS) into consideration [1, 7, 8, 9, 10, 11]. In image steganography, the cover image is the original image and the image that results from embedding secret data into the cover image called the stego image. The cover image should be similar to the stego image in which it is difficult for an eavesdropper to know the stego image.

The least significant bit (LSB) is the most popular method in steganographic images. Due to the advantages of LSB in steganographic image quality, this method used widely and continues to be improved up to date [3]. The main idea of LSB substitution method is altering directly some LSB of pixels in the cover image with secret bits. This method characterized by the ease and the simplicity of computation. But this method suffers from producing noticeable distortion in the stego image and this will attract the unauthorized user attention [1]. LSB inversion method inverts the LSB of the cover image based on the values of the secret data. The number of bits that modified in this method is less than that in the standard LSB method. Therefore enhances the quality of the stego image and raise the Peak Signal-to-Noise Ratio ($PSNR$) values. LSB inversion also decreases the chance of the hidden data to be detected [12].

There are many different steganographic methods for data hiding based on LSB like method in [13] which based on pairs matching. This approach focuses on pattern matching, so it is different from all the previous approaches. The secret bits are arranged in pairs to be secured and also the image pixel bits are arranged pairwise. The secret bits are compared with pixels bit pairs and replace the two LSBs with respective

matched pair number. If no pair is matched, then secret data pairs are embedded into the 0th pair of pixel bits. The results show that the proposed approach is more secure and achieves a good quality of stego image and carries high capacity of secret data.

The proposed technique in [14] used modulus -m arithmetic operation to embed secret data into a cover image and extract it. Also, one module is presented to test the host image. This method works in a spatial domain manner and pixels used the decimal value (0 – 255) to be represented. In future research, they intend to improve the method by doing grouping or multiple pixel embedding and extracting.

Method [15] introduced a new good system using Adding operation. The system Adding Binary value of secret text to the value of LSB pixel in a palette. This decreases the number of LSB that will be changed. Also, in the extraction of secret text, the system uses two keys to improve the power of embedding and the difficulty of breaking. The proposed system is easy in using and effective for security.

Marghny and Loay [1] proposed a data hiding scheme based on LSB technique. The scheme divides the cover image into two parts. In the first part, secret data are embedded using LSB substitution. Also, some bits have the secret data are inverted to improve the results. The second part used to indicate the bits inverted in the first part. The optimal LSBs method is applied after that to decrease the distortion and improve the imperceptibility of the stego image. The results indicate that the technique increases the capacity and stego image quality.

Khodaei and Faez [16] presented a new technique based on LSB substitution and pixel value differencing (PVD) for greyscale images. The cover image is divided into some non-overlapping blocks, every block has three consecutive pixels. LSB substitution and optimal pixel adjustment process (OPAP) are used to embed secret bits in the central pixel. Results demonstrate that this technique embeds a large amount of secret data and have high visual quality of the stego images.

Authors in [3] introduced a simple and safe technique using XOR operation to hide data in LSB methods. The XOR operation is easy and

quick and with this operation, the hidden bits cannot be directly retrieved. The experimental results show that the quality of the stego image is excellent, the $PSNR$ values above 50 dB and the technique provides security to data with very simple operation.

The present research introduces a new scheme based on inverting LSB with an Optimal LSBs technique. We invert LSBs instead of replacing it with a secret message to enhance the stego image quality. The secret bits are arranged in pairs. Four LSBs of each pixel for embedding are used. Every 2 LSBs of the 4 LSBs used for embedding one pair. The LSBs are inverting according to the values of the secret bits in the pair. After inverting, apply the Optimal LSBs scheme to increase the stego image quality. Standard grayscale images are used to expert the performance of our method.

The paper is organized such that in Section 2, a brief description of the optimal LSB scheme is given. Section 3 explains the proposed method. In Section 4, the experimental results are discussed. The conclusion is introduced in Section 5.

THE OPTIMAL LSBs TECHNIQUE

The Optimal LSBs technique is one of the improved techniques based on the simple LSB method. It improves the quality of the stego image by using an Optimal Pixel Adjustment Process (OPAP). The main idea of the Optimal LSBs is choosing three candidates having the secret data in for the pixel and then comparing them to know the closest to the original pixel value. The closest one is the best candidate and called the optimal pixel. It is used to embed secret data [17, 18)]. The embedding algorithm steps are as follows [1, 17]:

- Assume u_i is the pixel values of the $i-$ th pixel in the cover image and r bit(s) is the secret bits.
- Embed r bit(s) in u_i using the LSB method. Then the stego pixel u_i' can be obtained.

- generate another two-pixel value u'_- and u'_+ by adjusting the (r + 1) – th bit as follows:

$$(u'_+, u'_-) = \begin{cases} u'_+ = u'_i + 2^r \\ u'_- = u'_i - 2^r \end{cases} \quad (1)$$

The embedded bits in u'_- and u'_+ are identical to u'_i because the last bits r they have are the same.

- The optimal candidate u''_i can be obtained as follows:

$$u''_i = \begin{cases} u'_i, if \left| u_i - u'_i \right| \leq \left| u_i - u'_- \right| \leq \left| u_i - u'_+ \right| \\ u'_+, if \left| u_i - u'_+ \right| \leq \left| u_i - u'_i \right| \leq \left| u_i - u'_- \right| \\ u'_-, if \left| u_i - u'_- \right| \leq \left| u_i - u'_i \right| \leq \left| u_i - u'_+ \right| \end{cases} \quad (2)$$

- Finally, alter the original pixel values u_i with all the optimal candidates u''_i .

In the following is an example demonstrates how the optimal LSBs method can reduce the distortion generated by the simple LSBs method. Let u_i = 21, r = 3 and the three secret bits are 000. After using the simple 3-LSBs method, the generated stego pixel is u'_i = 16. Adjust the 4-th bit of u'_i to generate the two-pixel values u'_+ = 24 and u'_- = 8. The three pixels u'_i = 16, u'_+ =24 and u'_- = 8 have the same last three bits. The closest to the original pixel value is u'_+= 24 and is called the optimal candidate. As we see the distortion produced in the stego image can be decreased by using the optimal LSBs method.

THE PROPOSED METHOD

The presented method is based on inverting LSB with an Optimal LSBs scheme. We invert the value of some LSB of each pixel in the

cover image instead of altering it with secret bits to improve the quality of the stego image. The secret bits are divided into pairs. Each pair will need 2 LSBs of the cover pixel for embedding. Each cover pixel will be used to embed two pairs, so we use 4 LSBs of each for embedding. According to the values of each pair, the value of LSBs will be inverted. We compare the values of the two bits for each pair. If they are matched and its values are 0, then don't invert any bits. If their values are 1, then invert the 2 LSBs. In the case of no matching, if the first bit is 0 and the second is 1, then invert first LSB. If the opposite, then invert the second LSB. After that, we apply the Optimal LSBs scheme to increase the imperceptibility. The algorithm of our presented method consists of two parts. The first is the embedding algorithm describes the steps for embedding secret data. The second is the extracting algorithm describes the steps for extracting secret data from the stego image. Now, we describe the image used in our method.

Suppose the gray image I consist of n Pixels $I = \{P_1, \dots, P_n\}$. Every pixel consists of 8-bits:

$$P_i = \{b_1, \dots, b_8\}, b_j \in \{1,0\}. \quad (3)$$

The size of the image N estimated as:

$$N = H\ x\ W. \quad (4)$$

Where H, W is the image height and width respectively. Assume M be the secret bits with length n:

$$M = \{m_1, m_2, \dots, m_n\}, where\ m_i \in \{1,0\}. \quad (5)$$

The maximum embedding capacity h in the image I can be estimated in terms of bits as:

$$1 \leq h \leq (N\ x\ 8). \quad (6)$$

The Embedding Algorithm:

The inputs for embedding are a grayscale image as a cover image and a series of pseudo-random data as a secret data. The output is the stego image. Now the steps for embedding as follows:

- Convert the secret data into the binary system and then divide it into pairs.
- Compare the two bits of the pair.
- In the case of they are matching:
  - If their values are 0, then don't invert any LSBs.
  - If their values are 1, then invert the 1st and 2nd LSBs of the pixel.
- In the case of they are not matching:
  - If the first bit is 0 and the second is 1, then invert the 1st LSB only.
  - If the first bit is 1 and the second is 0, then invert the 2nd LSB only.
- Repeat steps 2, 3 and 4 for the next pair with using the 3rd and 4th LSBs of the pixel.
- Apply the optimal LSBs method to the obtained pixel.
- Repeat the previous steps from step 2 until embedding all the secret data.
- In the end, the stego image will be obtained and send to the receiver.

The Extracting Algorithm:

The inputs for extracting are the original and stego images. The original image is required to know the inverted bits in each pixel of the stego image to retrieve the secret data. The output is the secret data. Now the steps for extracting as follows:

- Compare the 1st and 2nd LSBs of the first pixel in the original image with the corresponding in the stego image to determine the inverted bits.

- According to the inverted bits, decide which case is applied and then retrieve the secret data.
- Repeat the previous steps for the 3rd and 4th LSBs of the first pixel.
- Repeat the previous steps for all pixels.
- By this, the secret data is retrieved.

EXPERIMENTAL RESULTS

To measure the efficiency of the proposed technique, several experiments have experimented. The seven standard grayscale images ”Lena”, ”Baboon”, ”Pepper”, ”Barbara”, ”Elaine”, ”Cameraman” and ”Tiffany” each with the size 512 X 512 are used as cover images and three of them are shown in figure1. The secret data are a series of pseudo-random data. We used Matlab 2017 to execute the experiments. The evaluation of the performance of the presented method is measured from two major points of view: the visual quality of stego image and the embedding capacity. The estimation of the stego image quality is evaluated by using the peak signal-to-noise ratio ($PSNR$). $PSNR$ is the most popular measurements and used widely to evaluate the performance of the steganographic method. It evaluated the similarity between the original and stego images. The value of $PSNR$ increasing when the original and stego images are similar. $PSNR$ is expressed as a logarithmic decibel scale and can be defined as [1, 19, 20, 21]:

$$PSNR = 10.\log_{10}\frac{255^2}{MSE}\ (dB) \qquad (7)$$

Where MSE is the Mean Square Error between the cover and stego images and estimated as:

$$MSE = \frac{1}{W\ x\ H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(I_{ij} - I'_{ij}\right)^2 \qquad (8)$$

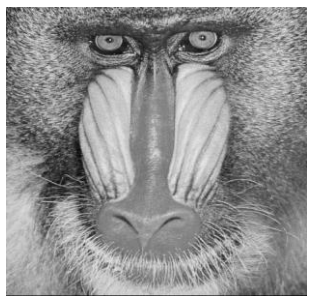
Where H and W are the height and width for a cover image respectively and I_{ij} and I'_{ij} are the pixel values of the cover and stego images respectively.

The second measurement embedding capacity is the amount of data bits that can be embedded within the cover media and expressed as a number of bits per pixel (bpp). Increasing the value of the capacity means increasing the amount of data bits carried over cover media [1, 19]. The capacity is evaluated as [1, 22]:

$$Capacity = \frac{Total\ number\ of\ bits\ embedded\ into\ image}{Total\ number\ of\ pixels}\ (bits/pixels) \qquad (9)$$

Table 1. shows the results of the presented method in terms of embedding capacity (in bits) and $PSNR$ values. The results indicate that our method achieves large embedding capacity and high $PSNR$ values. The average $PSNR$ value is greater than 35 and this means that the original image is similar to the stego image. This similarity makes the distinction between them is difficult for the human eye.

(a) Lena



(b) Baboon

(c) Peppers

Figure 1. Three cover images with size 512 X 512.

Figure .2 shows three of the stego images obtained by our method. From figures 1 and 2 we can notice that the cover and stego images are similar. This means that the stego images have high quality and the distortion is imperceptible for the human eyes.

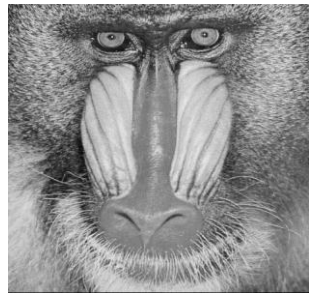
Table 1. Experimental Results

Cover Images	**The Proposed Method**	
	Capacity	**PSNR**
Lena	1048576	35.7741
Baboon	1048576	35.7784
Peppers	1048576	35.7815
Cameraman	1048576	35.7838
Barbara	1048576	35.7779
Elaine	1048576	35.7806
Tiffany	1048576	35.8148

Table 2. indicates a comparison between the proposed method and Marghny and Loay [1] method in terms of $PSNR$ and capacity. The comparison shows that at the same capacity approximately, the $PSNR$ values of the proposed method are higher than that in [1] method. The capacity of our method differs slightly from [1] method by one bit. This because we used a grayscale image of size 512 X 512 and used 4 LSBs of

each pixel for embedding two pairs of secret bits. Then the capacity can be evaluated as: 512 X 512 X 4 = 1048576 bits.

(a) Lena



(b) Baboon

(c) Peppers

Figure 2. Three stego images at capacity= 1048576 bits.

Table 2. Comparison between the proposed method and Marghny and Loay [1] method.

Cover Images	**Marghny and Loay [1] method**		**The Proposed Method**	
	Capacity	**PSNR**	**Capacity**	**PSNR**
Lena	1048575	34.84	1048576	35.7741
Baboon	1048575	34.83	1048576	35.7784
Peppers	1048575	34.83	1048576	35.7815
Cameraman	1048575	34.88	1048576	35.7838
Barbara	1048575	34.82	1048576	35.7779
Elaine	1048575	34.86	1048576	35.7806

Another comparison of our results with the results in [16] method in terms of $PSNR$ and embedding capacity in table 3. From the comparison, we can see that our method have higher $PSNR$ values at different capacity. This means that our method has better performance for any capacity. Also, here our proposed method capacity is differing slightly from [16] method and the reason for this is mentioned before in the previous comparison.

Table 3. Comparisons of the results between the proposed method and Khodaei and Faez [16] method.

Cover Images	**M. Khodaei and K. Faez [16] method**		**The Proposed Method**	
	Capacity	**PSNR**	**Capacity**	**PSNR**
Lena	967524	32.77	967524	36.1245
Baboon	988371	31.93	988372	36.0374
Peppers	965803	32.83	965804	36.1384
Barbara	997958	31.34	997960	35.9955
Tiffany	966169	32.93	966172	36.1637

CONCLUSION

This study presents a new steganographic image scheme based on inverting LSB with an Optimal LSBs technique. Inverting LSB instead of replacing it with secret bits decrease the distribution and thus improves

the stego image quality. Secret bits are divided into pairs. 4 LSBs of each cover pixel are used to embed two pairs. LSBs are inverted according to the value of each pair. Results demonstrate that the proposed method increases the amount of embedding capacity and achieves high $PSNR$ values.

REFERENCES

[1] Mohamed, M. H., & Mohamed, L. M. High capacity image steganography technique based on LSB substitution method. *Applied Mathematics & Information Sciences*, *10*(1), 259-266, (2016).

[2] Lee, Y. P., Lee, J. C., Chen, W. K., Chang, K. C., Su, J., & Chang, C. P. High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Information Sciences*, 191, 214-225, 2012.

[3] Astuti, Y. P., Rachmawanto, E. H., & Sari, C. A. Simple and secure image steganography using LSB and triple XOR operation on MSB. In *2018 International Conference on Information and Communications Technology (ICOIACT)*. 191-195, IEEE, 2018.

[4] Kothari, L., Thakkar, R., & Khara, S. (2017, July). Data hiding on web using combination of Steganography and Cryptography. In *2017 International Conference on Computer, Communications and Electronics (Comptelix)*. 448-452, IEEE, 2017.

[5] Ardiansyah, G., Sari, C. A., & Rachmawanto, E. H. Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm. In *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*. IEEE, 2017, 249-254.

[6] Arun, C., & Murugan, S. Design of image steganography using LSB XOR substitution method. In *2017 International Conference on Communication and Signal Processing (ICCSP)*. 0674-0677. IEEE, 2017.

[7] Al-Husainy, M. A. F. A new image steganography based on decimal-digits representation. *Computer and Information Science*, *4*(6), 38, 2011.

[8] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), 727-752, 2010.

[9] Amanpreet, K., Renu, D., & Geeta, S. A new Image Steganography Based on First Component Alteration Technique: *International of Computer Science and Information Security*, 2009.

[10] Gutub, A., Al-Qahtani, A., & Tabakh, A. (2009, May). Triple-A: Secure RGB image steganography based on randomization. In *2009 IEEE/ACS International Conference on Computer Systems and Applications*. 400-403, IEEE, 2009.

[11] Bhattacharyya, D., Roy, A., Roy, P., & Kim, T. H. Receiver compatible data hiding in color image. *International Journal of Advanced Science and Technology*, *6*(1), 15-24, 2009.

[12] Majeed, M. A., & Sulaiman, R. AN IMPROVED LSB IMAGE STEGANOGRAPHY TECHNIQUE USING BIT-INVERSE IN 24 BIT COLOUR IMAGE. *Journal of Theoretical & Applied Information Technology*, *80*(2), 2015.

[13] Shehzad, D., & Dag, T. A novel image steganography technique based on similarity of bits pairs. In *2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC)*. 99-104, IEEE, 2017.

[14] Jaafar, S., Manaf, A. A., & Zeki, A. M. Steganography technique using modulus arithmetic. In *2007 9th International Symposium on Signal Processing and Its Applications*. 1-4, IEEE, 2007.

[15] Al-Farraji, O. I. I. Steganography By Use Binary Operations.

[16] Khodaei, M., & Faez, K. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. *IET Image processing*, *6*(6), 677-686, 2012.

[17] Wu, N. I., & Hwang, M. S. Data hiding: current status and key issues. *IJ Network Security*, *4*(1), 1-9, 2007.

[18] Chan, C. K., & Cheng, L. M. Hiding data in images by simple LSB substitution. *Pattern recognition*, *37*(3), 469-474, 2004.

[19] Chang, C. C., Chou, Y. C., & Kieu, T. D. Information hiding in dual images with reversibility. In *2009 Third International Conference on Multimedia and Ubiquitous Engineering*. 145-152, IEEE, 2009.

[20] GM. Kamau, S. Kimani, and W. Mwangi, An enhanced Least Significant Bit Steganographic Method for Information Hiding. *Journal of Information Engineering and Applications*, 2(9), 1-11, 2012.

[21] Nayak, D. K., & Bhagvati, C. A threshold-LSB based information hiding scheme using digital images. In *2013 4th International Conference on Computer and Communication Technology (ICCCT)*. 269-272, IEEE, 2013.

[22] Jain, Y. K., & Ahirwal, R. R. A novel image steganography method with adaptive number of least significant bits modification based on private stego-keys. *International Journal of Computer Science and Security*, *4*(1), 40-49, 2010.

الملخص العربي

التطور السريع والمستمر فى تكنولوجيا المعلومات ادي الى زيادة الاهتمام بحماية البيانات والمعلومات اثناء انتقالها عبر وسائل الاتصال. وعلم اخفاء المعلومات (Steganography) هو احدي الطرق المستخدمة لاخفاء البيانات داخل محتوي اخر بحيث يظهران ككيان واحد وبالتالي يتم نقل البيانات والمعلومات بطريقة سرية وامنه. وتعتبر طريقة البت الاقل اهمية ((Least Significant Bit (LSB من اسهل واكثر الطرق انتشارا لاخفاء البيانات. وفى هذا البحث تم تقديم طريقة باستخدام البت الاقل اهمية حيث يتم اخفاء المعلومات داخل الصور، ويتم تقييم هذه الطريقة باستخدام مقياسيين وهم كمية البيانات التي يتم اخفائها وكفاءة الصورة الناتجة بعد اخفاء البيانات داخلها. وقد اثبتت التجارب كفاءة الطريقة المقترحة.