VOL 3 (2019) NO 4

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Improving the Security of LSB Image Steganography

Jamil Al-Azzeh[#], Ziad Alqadi[#], Belal Ayyoub[#], Ahmad Sharadqh[#]

[#] *Computer Engineering Department, Al Balqa'a Applied university, Amman, Jordan*
E-mail: azzehjamil@gmail.com, natalia_maw@yahoo.com, belal_ayyoub@hotmail.com, ahmadsharadqh78@gmail.com

***Abstract*— Steganography is the technique of hiding secret data (message) within any media such as digital color image. In this paper we will merge steganography process with cryptography process in order to increase the security of the proposed method. The steganography process will based on LSB method, while the cryptography process will based on generating a huge private key and selecting a special function for encryption decryption. The proposed method will be implemented in order to calculate some performance parameters to prove the efficiency of the proposed method.**

***Keywords*— Steganography, LSB, encryption, decryption, private key, MSE, PSNR.**

I. Introduction

Steganography is the technique of hiding secret information (message) within any media such as digital color image [1-22. The objective of steganography is to hide a secret data within a covering image such a way that others cannot discern the presence of the hidden data.

Hiding secret data (message) into color image requires following elements as shown in figure (1):

- The covering color image that will hold the hidden secret message.
- The secret message may be plain text, cipher text or any type of data.

The stego function to be used to hide and unhide the message.

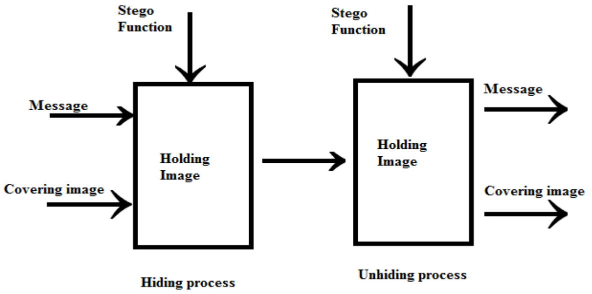

Fig.1 Process of steganography

One of the most popular methods used in steganography today is least significant bit (LSB) insertion. Here; the least significant bits of the covering color image are altered so that they form the embedded secret message as shown in table (1).

Table I
Hiding A (Binary Version= 01000001 Binary)

Pixel number					Remarks
	Pixel value (decimal)	Pixel value (binary)	Pixel value(binary)	Pixel value(decimal)	
1	200	11001000	11001000	200	No changes
2	155	10011011	10011011	155	No changes
3	170	10101010	10101010	170	No changes
4	95	01011111	01011110	94	Small changes
5	100	01100100	01100100	100	No changes
6	205	11001101	11001100	204	Small changes
7	120	01111000	01111000	120	No changes
8	180	10110100	10110101	181	Small changes

The advantages of LSB are its simplicity to hide the bits of the secret message directly into the LSB plane of covering color image and many techniques use these methods [3]. Applying the LSB method does not result in a human-perceptible difference because the changes between the covering and holding images are very small. Therefore, to the human eye, the resulting holding image will look identical to the covering image. This allows high perceptual transparency of LSB as shown in figures (2) and (3).

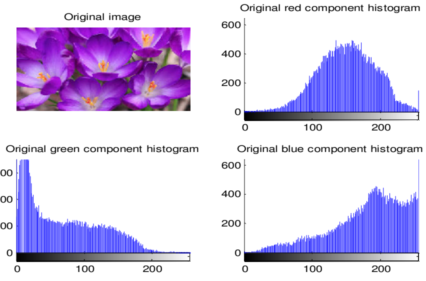

Fig 2 Original covering image

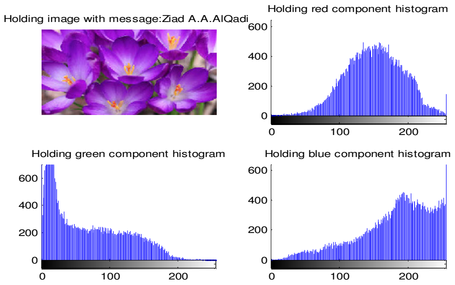

Fig. 3 Holding image

The disadvantages of LSB method is that the method is not secure, because it is very easy hack the secret message and extract it by any un- authorized person.

II. Material

Many authors provided various methods and techniques for data hiding based on LSB method of data hiding.

In [4] the authors proposed a survey on recent achievement of LSB based image steganography and discussed the enhancements done to improve current LSB based steganographic methods. They also proposed two new steganographic techniques. In [5] a new secret data hiding technique was proposed which was based on LSB method with different progression. Experimental results showed that the proposed method is fast and highly efficient as compared to traditional LSB method. In [6] a new method was proposed in which multiple RGB images are embedded into single RGB image using DWT. Proposed system has high embedding capacity and security with minimal changes in stego image. In [7] a very latest approach of binary image steganography was proposed. This technique reduces the distortion on the textures. The proposed method also provides a measurement scheme. The authors concluded that their method has high statistical security with high data hiding capacity. In [8] a new approach based on heuristic genetic algorithm was proposed, which optimally find the appropriate locations in cover image to hide data. Simulation results showed that their method is more efficient than traditional LSB based method. In [9] a new improved version of LSB method was presented, which preserved the histogram and thus prevented the histogram analysis-based attacks. This method also eliminates the embedding of extra bits thus leads to high stego image quality.

In [10] Authors proposed Huffman coding based novel steganographic technique of LSB substitution. This work mainly focuses on high security and embedding capacity and acceptable level of visual quality of stego image. Experimental results demonstrate that proposed scheme has peak signal to noise ratio (PSNR) of 30 dB to 31 dB.

In [11] New steganographic method was proposed and implemented based on bit inversion. Experimental results represented that PSNR value of stego image is improved using this method.

In [12] a comparative analysis of secrete message hiding methods was proposed and it was mentioned that the analyzed methods: Optimum Pixel Adjustment Procedure [13], Inverted Pattern Approach [14], P Method Using Relative Entropy [14], and Pixel Value Differencing (PVD) [15] reduces the distortion caused by the LSB substitution methods.

III. Method / Algorithm

The proposed method can be implemented applying the following phases:

Phase 1: Generating private key.

Here the private key is used for color image encryption-decryption; it can be generated by performing the following steps:

1) Apply the following formula to generate the private key:

$$key = uint8(255 * rand(5000, 5000, 3))$$

This key is very huge and complicated in order to maximize the hacking time and makes it impossible for hacking.

2) Save the private key

Phase 2: Hiding secret message

This phase can be implemented applying the following steps:

1) Get the original covering image.
2) Retrieve the image size (Rows, columns, colors).
3) Apply LSB method to insert the message into the covering image.
4) Load the private key.
5) Extract the used-key from the private key applying the following formula:

$$Usedkey = key(1 : rows, 1 : columns, 1 : colors)$$

6) Encrypt the holding image using a selected stego-function(XORing the holding image with the used-key):

$$Encryptedcolorimage = Holdingcolorimage \oplus Usedkey$$

7) Save the encrypted image.

Phase 3: Extracting the secret message

This phase can be implemented applying the following steps:

1) Get the encrypted holding image.
2) Retrieve the image size (Rows, columns, colors).
3) Load the private key.
4) Extract the used-key from the private key applying the following formula:

$$Usedkey = key(1 : rows, 1 : columns, 1 : colors)$$

5) Decrypt the holding encrypted image using the stego-function:

$$Decryptedcolorimage = Encryptedcolorimage \oplus Usedkey$$

6) Apply LSB method to extract the message into the decrypted holding image.

IV. Result

The proposed method was implemented by using the covering image and a secret message 'Ziad A.A.AlQadi' and the results of implementation are shown in figures (4) through (7):

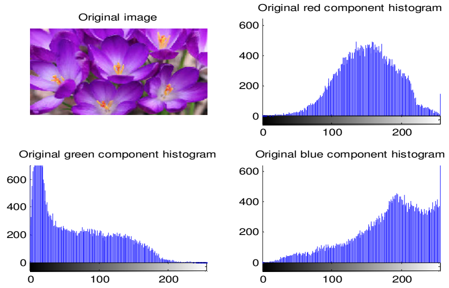

Fig 4 Original covering image

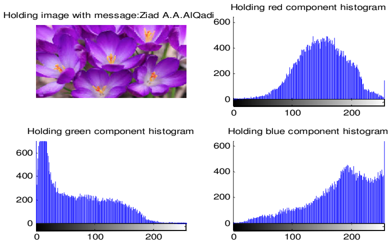

Fig 5. Holding image

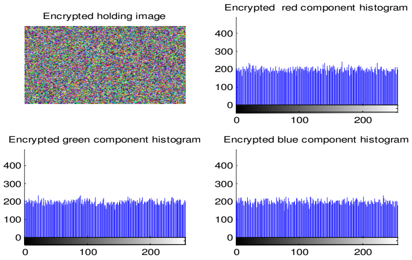

Fig 6. Encrypted holding image

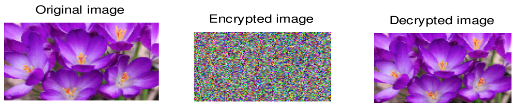

Fig 7. Original, encrypted and decrypted images

The proposed method was implemented several time using various images with a fixed message, table (2) shows the calculated performance parameters of this experiment:
We can see from table (2) that required total hiding times and total extraction times are very small and they range from 0.2620 to 0.3400 seconds depending on the covering image size.

Another experiment was implemented using various in size messages by fixing the covering image with size equal 983x1300x3 pixels, the results of this experiment are shown in table (3).

TABLE II
METHOD PERFORMANCE BY HIDING MESSAGE WITH SIZE=50 CHARACTERS

Image number	Image size	Maximum message length which can be inserted	Message insertion time (seconds)	Encryption time (seconds)	Total hiding time	Decryption time	Extraction time	Total extraction time
1	177x 284x3	18851	0.009	0.267	0.276	0.282	0.000001	0.282
2	222x 228x3	18981	0.011	0.262	0.273	0.267	0.001	0.268
3	186x271x3	18902	0.009	0.263	0.272	0.267	0.0001	0.2671
4	196x258x3	18963	0.009	0.263	0.272	0.271	0.0001	0.271
5	177x284x3	18851	0.009	0.267	0.276	0.282	0.000001	0.282
6	225x225x3	18984	0.009	0.263	0.272	0.269	0.001	0.27
7	168x300x3	18900	0.022	0.269	0.291	0.273	0.001	0.274
8	983x1300x3	479210	0.069	0.271	0.34	0.285	0.006	0.291
9	800x800x3	240000	0.037	0.268	0.305	0.289	0.004	0.293
10	750x1372x3	385875	0.057	0.269	0.326	0.275	0.004	0.279

TABLE III
METHOD PERFORMANCE BY HIDING VARIOUS MESSAGES IN IMAGE WITH SIZE=983X1300X3

Message size	Message insertion time (seconds)	Encryption time (seconds)	Total hiding time	Decryption time	Extraction time	Total extraction time
10	0.069	0.27	0.339	0.27	0.005	0.275
100	0.069	0.27	0.339	0.27	0.006	0.276
200	0.069	0.27	0.339	0.27	0.006	0.276
400	0.069	0.27	0.339	0.27	0.006	0.276
800	0.069	0.27	0.339	0.27	0.007	0.277
1600	0.073	0.27	0.343	0.27	0.008	0.278
3200	0.074	0.27	0.344	0.27	0.011	0.281
6400	0.075	0.27	0.345	0.27	0.016	0.286
12800	0.084	0.27	0.354	0.27	0.025	0.295
25600	0.098	0.27	0.368	0.27	0.045	0.315

Figure (8) shows the relationship between the hiding, extractions times and the message size.

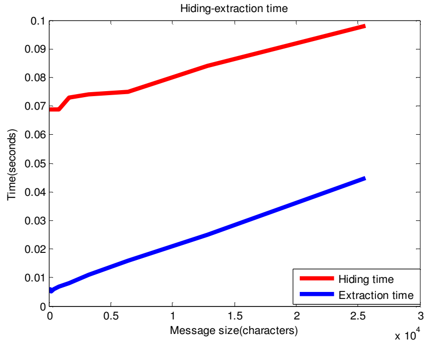

Fig 8. Hiding and extraction times

The covering original image was compared with decrypted one and they are much closed as shown in figure (9), the mean square error (MSE) [12] between them was calculated and it was equal 0.0187 which very small and acceptable, also PSNR [12] was calculated and it was equal 150.6190 which is very high and acceptable.

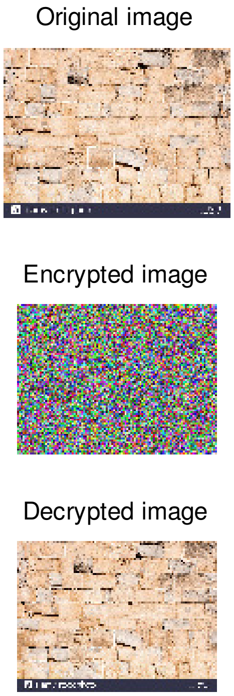

Fig 9. Used images.

From the obtained results we can raise the following facts:

- Color and gray images can be used for steganography.
- The used-key is as an image in size, this will enhance the method security.
- We can use any image, with different types and size.
- We can hide/extract huge messages without damaging the covering image.
- The performance of the proposed method is acceptable.

V. Conclusions

A simple, secure and highly efficient method of data steganography was proposed, tested and implemented.

The obtained results showed that encrypting-decrypting the holding image increases the method security without losing the method efficiency and without damaging the holding image by concentrating our mind on the advantages of LSB method of steganography and the advantages of the proposed data encryption-decryption methodology.

References

[1] Moh'd Zoghoul. Hussein Hatamleh,ZiadAlqadi, , Muhammed Mesleh, Belal Ayyoub, Jamil Al-azzeh, A comparative analysis of Huffman and LZW methods of color image compression-decompression: International Journal of Engineering Science Invention, 2019, Volume 8, Issue 04.

[2] Jamil Al-Azzeh, Bilal Zahran , Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh, A Novel Based on Image Blocking Method toEncrypt-Decrypt Color; INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION 2019, Volume 3 Issue 1.

[3] Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, Journal of Computer Science and Information Technology,2019, , Volume 8 Issue 3.

[4] Ziad Alqadi; Bilal Zahran; Qazem Jaber; Belal Ayyoub; Jamil Al-Azzeh,Enhancing the Capacity of LSB Method by Introducing LSB2Z Method; International Journal of Computer Science and Mobile Computing,2019, Volume 8 Issue 3.

[5] Ahmad Sharadqh, Belal Ayyoub, Ziad Alqadi, Jamil Al-azzeh; Experimental investigation of method used to remove salt and pepper noise from digital color image, International Journal of Research in Advanced Engineering and Technology,2019. Volume 5 Issue 1.

[6] Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Qazem Jaber,Modified, Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing,2019, Volume 8 Issue 2.

[7] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata, Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving, International Journal of Computer Science and Mobile Computing,2019, Volume 8 Issue 2.

[8] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Ahmad Sharadqh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing,2019, Volume 8 Issue 3.

[9] Jamil AL-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology 15th July 2018.

[10] Jamil AL-Azzeh, Bilal Zahran and Ziad Alqadi: Salt and Pepper Noise: Effects and Removal, International Journal on Informatics Visualization July 2018, Volume 2 Issue 4.

[11] Bilal Zahran, Jamil Al-Azzeh , Ziad Alqadi, Mohd-Ashraf Al Zoghoul : A Modified LBP Method To Extract Features From Color Images : Journal of Theoretical and Applied Information Technology May 2018,Volume 96, Issue 10.

[12] Mazen Abuzaher, Jamil AL-Azzeh, JPEG Based Compression Algorithm, International Journal of Engineering and Applied Sciences ,2017, Volume 4, Issue 4,

[13] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata , Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications , November 2016 ,Volume 153, Issue 2.

[14] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub and M. Mesleh," Creating Color Image Signature Based On Laplacian Equation , International Journal on Informatics Visualization, 2019,Volume 3, Issue 2.

[15] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub and M. Mesleh," A Novel Based On Image Blocking Method To Encrypt-Decrypt Color", International Journal on Informatics Visualization, Vol 3, No 1. 2019.

[16] J. AL-AZZEH, B. ZAHRAN, Z. ALQADI, B. AYYOUB, M. ABU-ZAHER,A novel Zero-error Method to Create a Secret Tag for an Image, Journal of Theoretical and Applied Information Technology(JATIT), Volume 96, Issue 13, 2018.pp: 4081-4091.

[17] Jihad Nader, Ziad Alqadi, Bilal Zahran, Analysis of Color Image Filtering Methods, International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.

[18] Ziad Alqadi, Bilal Zahran, Jihad Nader, Estimation and Tuning of FIR Lowpass Digital Filter Parameters, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, 2017, pp:18-23.

[19] B. Zahran , Z. Alqadi , J. Nader and A. Abu Ein, A Comparison between Parallel and Segmentation Methods Used for Image Encryption-Decryption, International Journal of Computer Science & Information Technology (IJCSIT) Volume 8, Issue 5, 2016.

[20] Belal Aub, Saleh Khawatreh, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications,2018 , Volume 179, Issue 9.

[21] Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, Suggested Method to Create Color Image Features Victor. Journal of Engineering and Applied Sciences, 2019, Volume 14, Issue 7.