A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages

Rashad J. Rasras
Department of Computer Engineering
Al-Balqa' Applied University
Amman, Jordan
rashad.rasras@bau.edu.jo

Ziad A. AlQadi
Department of Computer Engineering
Al-Balqa' Applied University
Amman, Jordan
natalia_maw@yahoo.com

Mutaz Rasmi Abu Sara
Department of Computer Science
Taibah University
Al-Medina, Saudi Arabia
mabusara@taibahu.edu.sa

***Abstract*—Steganography and cryptography are very important techniques used in data security to hide and secure secret messages in transmitted data. This paper will introduce, implement and test a novel methodology which can be used as a secure and highly efficient method of data hiding and data extracting. Some efficiency parameters will be experimentally obtained and compared with other existing methods parameters to prove the efficiency of the proposed methodology.**

Keywords-steganography; decryption time; MSE; cryptography; encryption time; speedup; PSNR

I. INTRODUCTION

Steganography is the process of hiding secret messages in such a way that no one except the sender and the intended recipient can see them. The process of hiding data is used in many important applications in order to maintain confidentiality of important data, prevent unauthorized persons from identifying or understanding the confidential message, or add mark or a tag to the digital image to be used in order to identify the digital image ownership. Cryptography is the process of changing data so that they are not readable. Unauthorized parties might see there are data communicated but can't understand them. Digital color images can be used as a media to carry the secret massage, because of their size, and because they are commonly presented by 3 2D matrices (one for the red color, one for the green color and the last one for the blue color) [1, 2]. The process of hiding a secret message can be realized by applying the following phases [3]:

A. Steganography

- Select the original covering color image.
- Select the secret message.
- Use an available method of data hiding to insert the message into the image.

B. Cryptography

Here we have to perform the following tasks:

- Get the holding color image.
- Use one of the available methods to encrypt the image and get the encrypted image.

Corresponding author: R. J. Rasras

C. Message Extraction

The process of getting the secret message (extracting the message) can be done by applying the cryptography and then the steganography based on the methods used in the hiding phase. The selected methods for data hiding-extraction and data encryption-decryption must be secure and efficient by achieving the following: minimizing hiding-extraction time, minimizing encryption-decryption time, maximizing the process throughput by increasing the number of bytes to be treated per second, and excluding any loss of information during the entire process.

II. RELATED WORK

Many steganography methods are based on the least significant bit (LSB) method of data hiding and extracting [4-6]. Some improvements were added to enhance the security level of LSB method in [7-9]. LSB is an unsecure method of hiding secret messages, and the process of data hiding can be implemented by reserving 8 bytes of the holding image to store one character of the message. LSB requires the binary version of the character, and each bit of this version can be inserted in the least bit of the selected byte of the holding image. The advantages of the LSB based methods are the low values of mean square error (MSE), and the high values of peak signal to noise ratio (PSNR) [10], which make difficult for the human eye to notice the changes in the holding image.

Authors in [11] proposed a method of color image encryption-decryption based on matrix reordering and with a medium throughput. Authors in [12] suggested a method of encryption-decryption in digital color images by applying matrix multiplication. This method gave good efficiency parameters and high security level but the size of the private secret key used for encryption-decryption was very big and complicated and required big memory size to be stored. Authors in [13] suggested a method of image encryption-decryption based on a chaotic algorithm using the power and tangent functions instead of linear functions. The process of encryption is one-time-one-password system and is more secure (but not enough) than the DES algorithm. Also, it has low efficient parameters with big encryption-decryption time and low throughput. In [14], an asymmetric color image encryption-decryption method was introduced based on matrix

transformation but it had high encryption-decryption time and thus low throughput. In [15] a method of color image encryption-decryption was proposed based on Rubik's cube principle, with good security level but with low throughput. In [16] a method of color image encryption-decryption was presented based on using chaos-controlled poker shuffle operation. Both variants of this method had poor throughput.

III. THE PROPOSED METHODOLOGY

A. Image Hiding

Hiding a secret message in a covering color image can be implemented by applying the following phases:

1) Inserting the Message Into the Image

Here we have to perform the following steps:

- Select the covering color image.
- Get the secret message.
- Define the starting position in the image and the message length (row, column, length). This position can be used as a first secret private key (key1).
- Insert the characters of the secret message, by reserving one byte of the image to one character of the message.
- Save the holding image and key1.

2) Holding Image Encryption

Here we have to perform the following steps:

- Get the holding color image.
- Reshape the 3D color matrix to 2D matrix.
- Divide the 2D matrix into equal sizes blocks (in our paper block size=4×4 matrix).
- Select a 4×4 matrix with values in the range 0 to 255 to be used as secret private key (key2).
- Apply XOR operations (each block with key2) to get the encrypted 2D matrix.
- Reshape the 2D matrix to 3D color matrix to get the encrypted color image.
- Save the encrypted color image and key2.

B. Message Extraction

Extracting the secret message from the holding encrypted image can be implemented by applying the following phases:

1) Color Image Decryption.

Here we have to perform the following steps:

- Get the encrypted color image.
- Reshape the 3D color matrix to 2D matrix.
- Divide the 2D matrix into 4×4 blocks.
- Get key2.
- XOR each block with key2 to get the decrypted 2D matrix.
- Reshape the 2D matrix to 3D matrix to get the decrypted color image.

2) Extracting the Secret Message

Here we have to perform the following steps:

- Get key1.
- Use key1 to extract the characters from the image.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed methodology was implemented and various images of different sizes and types were used. To show the efficiency enhancement the proposed methodology was implemented in two phases, inserting and extracting the secret message in the image. The following message "ZIAD ALQADI" with length=11 characters was inserted-extracted by using selected position at first, and then by using the LSB method. Figure 1 shows the original color image, while Figure 2 shows the holding image.

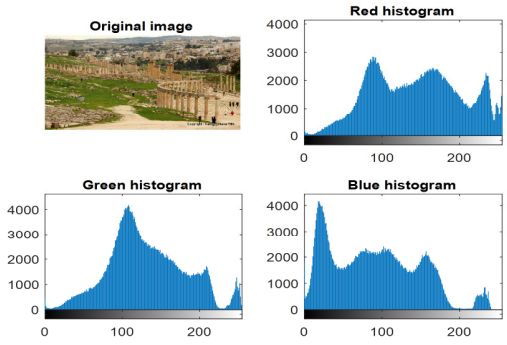

Fig. 1. Original color image with histograms.

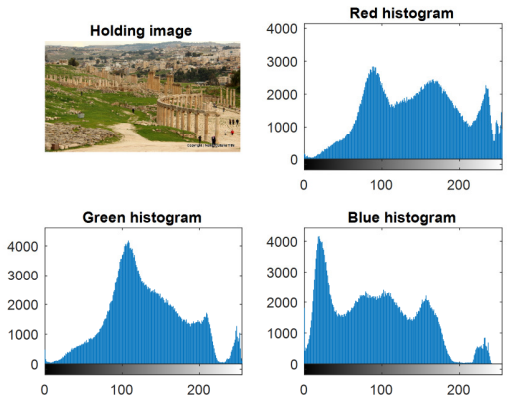

Fig. 2. Holding image with histograms.

Message insertion was implemented several times. The results of implementation are shown in Table I, while Table II shows the results obtained with the use of the LSB method. Table III shows a summary comparison between the results of the two methods.

TABLE I. RESULTS OF POSITION METHOD: MESSAGE LENGTH=11

Image No.	Size (byte)	Hiding time (s)	Extracting time(s)	Throughput (bytes per sec)	PSNR	MSE
1	270948	0.0028	0.0028	4.4850e+07	144.1719	0.0356
2	151875	0.0029	0.0029	5.1967e+07	118.1217	0.4821
3	49152	0.0027	0.0027	1.8039e+07	101.5034	2.5004
4	1125600	0.0028	0.0028	2.6035e+08	151.1818	0.0177
5	540000	0.0035	0.0035	1.5337e+08	129.3189	0.1573
6	3396069	0.0053	0.0053	6.3618e+08	143.2701	0.0390
7	2359296	0.0052	0.0052	4.5703e+08	140.0368	0.0539
8	928800	0.0040	0.0040	2.3078e+08	155.3087	0.0117
9	432000	0.0031	0.0031	1.3759e+08	138.6389	0.0620
10	151353	0.0027	0.0027	5.5868e+07	135.3198	0.0863
Avg.	940510	0.0035	0.0035	204602400	135.6872	0.3446

TABLE II. RESULTS OF LSB METHOD:MESSAGE LENGTH=11

Image No.	Size (byte)	Hiding time (s)	Extracting time(s)	Throughput (bytes per sec)	PSNR	MSE
1	270948	0.2325	0.0033	1.1653e+06	202.9637	9.9650e-05
2	151875	0.1474	0.0548	1.0305e+06	197.1750	1.7778e-04
3	49152	0.0441	0.0027	1.1133e+06	185.7361	5.4932e-04
4	1125600	0.9244	0.0049	1.2177e+06	217.2052	2.3987e-05
5	540000	0.4473	0.0037	1.2072e+06	209.8601	5.0000e-05
6	3396069	2.7665	0.0096	1.2275e+06	228.2482	7.9504e-06
7	2359296	1.8971	0.0076	1.2436e+06	224.6056	1.1444e-05
8	928800	0.7984	0.0045	1.1634e+06	215.2834	2.9070e-05
9	432000	0.3542	0.0036	1.2195e+06	207.6287	6.2500e-05
10	151353	0.1309	0.0029	1.1565e+06	197.1406	1.7839e-04
Avg.	940510	0.7743	0.0098	1174450	208.5847	1.1901e-04

TABLE III. RESULTS COMPARISON

Method	Size (byte)	Hiding time(s)	Extracting time(s)	Throughput (bytes per sec)	PSNR	MSE
Selected position (1)	940510	0.0035	0.0035	204602400	135.6872	0.3446
LSB (2)	940510	0.7743	0.0098	1174450	208.5847	1.1901e-04
Speed up of (1)		0.7743/0.0035=221.2286	0.0098/0.0035=2.8000			

From Table III we can see that the performance of the proposed selected position method is better than the performance of the LSB method (including encryption and decryption times and throughput) and that the SNR and MSE values for LSB method are better than those of the proposed selected position method. These parameters are not considerable because the second stage is encryption of the holding image, so MSE and PSNR are to be ignored.

Fig. 3. Holding color image and histograms

The second phase of secret message hiding-extracting was encryption-decryption. The output of the first phase was taken and implemented several times using the same images and applying encryption-decryption by dividing the image matrix into equal blocks (sized 4×4) and the results show a high value of MSE (low value of PSNR) between the holding image and the decrypted one, which is a good indicator. Figures 3-5 show some outputs of the implementation.

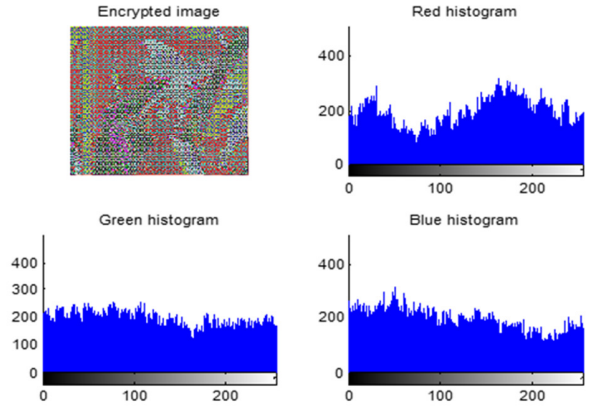

Fig. 4. Encrypted color image and histograms

Table IV shows the values of the efficiency parameters obtained during the process of implementation. In Table V we see a result comparison of the proposed and other existing methods.

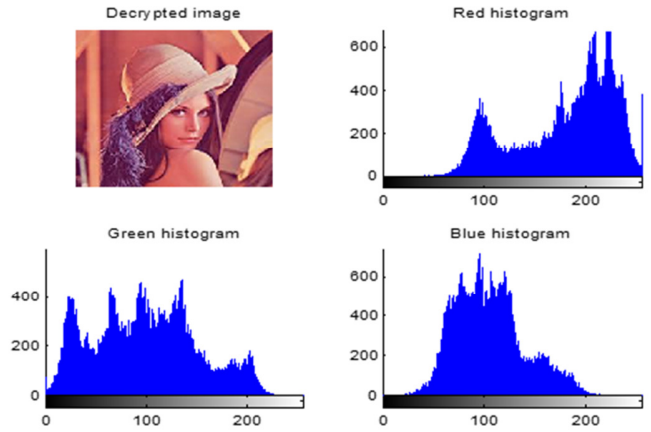

Fig. 5. Decrypted color image and histograms

TABLE IV. EFFICIENCY PARAMETERS OF THE PROPOSED METHOD

Img.	Size (bytes)	Encryption time (s)	Decryption time (s)	Throughput (Bps)
1	270948	0.0380	0.0380	7.1302e+006
2	151875	0.0230	0.0230	6.6033e+006
3	49152	0.0070	0.0070	7.0217e+006
4	1125600	0.1620	0.1620	6.9481e+006
5	540000	0.0780	0.0780	6.9231e+006
6	3396069	0.4950	0.4950	6.8607e+006
7	2359296	0.3470	0.3470	6.7991e+006
8	928800	0.1560	0.1560	5.9538e+006
9	432000	0.0610	0.0610	7.0820e+006
10	151353	0.0210	0.0210	7.2073e+006
Avg.	940510	0.1388	0.1388	6852930

TABLE V. COMPARISON WITH OTHER METHODS

Method	Encryption time(s)	Decryption time(s)	Total time	Speedup of the proposed method
Proposed	0.0245	0.0245	0.0490	1.0000
[11]	0.0682	0.0662	0.1344	2.7429
[12]	0.2335	0.2335	0.4670	9.5306
[13]	0.5035	0.5035	1.0070	20.5510
[14]	0.4035	0.4035	0.8070	16.4694
[15]	0.1235	0.1235	0.2470	5.0408
[16] A-I	0.5635	0.5635	1.1270	23.0000
[16] A-II	1.01	1.01	2.0200	41.2245

From Table V we can see that the proposed methodology gives a good improvement in the efficiency parameter values.

V. CONCLUSIONS

A methodology of secret message steganography was proposed, tested and implemented. The proposed methodology was based on selecting a position in the color image to start hiding the secret message and matrix blocking to encrypt-decrypt the holding color image. The proposed methodology increased the security level by using 2 private keys, and enhanced the efficiency comparing with other existing methods.

REFERENCES

[1] A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using A New R'G'I Model", Journal of Computer Science, Vol. 5, No. 4, pp. 250-254, 2009

[2] K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi, H Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014

[3] 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, Vol. 96. No. 13, pp. 4081-4091, 2018

[4] M. Jose, "Hiding Image in Image Using LSB Insertion Method with ImprovedSecurity and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014

[5] R. M. Patel, D. J. Shah, "Conceal gram :Digital image in image using LSB insertion method", International Journal of Electronics and Communication Engineering & Technology, Vol. 4, No. 1, pp. 230-2035, 2013

[6] N. Akhtar, P. Johri, S. Khan, "Enhancing the security and quality ofLSB based image steganography", 5th International Conference on Computational Intelligence and Communication Networks, Mathura, India, Seprember 27-29, 2013

[7] M. Juneja, P. S. Sandhu, "An improved LSB based Steganography with enhanced Security and Embedding/Extraction", 3rd International Conference on Intelligent Computational Systems, Hong Kong China, January 26-27, 2013

[8] J. Nadir, Z. Alqadi, A. Abu Ein, "Classification of Matrix Multiplication, Methods Used to Encrypt-decrypt Color Image", International Journal of Computer and Information Technology, Vol. 5, No. 5, pp. 459-464, 2016

[9] R. C. Gonzalez, R. Elwood, Digital Image Processing, Addison-Wesley, New York, 1992

[10] J. N. Abdel-Jalil, "Performance analysis of color image encryption/decryption techniques", International Journal of Advanced Computer Technology, Vol. 5, No. 4, pp. 13-17, 2016

[11] T. Sivakumar, R. Venkatesan, "A Novel Image Encryption Approach using Matrix Reordering", WSEAS Transactions on Computers, Vol. 12, No. 11, pp. 407-418, 2013

[12] H. Gao, Y. Zhang, S. Liang, D. Li, "A New Chaotic Algorithm for Image Encryption", Chaos, Solitons & Fractals, Vol. 29, No. 2, pp. 393-399, 2006

[13] G. Chen, Y. Mao, C. K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", Chaos, Solitons and Fractals, Vol. 21, No. 3, pp.749-761, 2004

[14] K. Loukhaoukha, J. Y. Chouinard, A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, Vol. 2012, ArticleID 173931, 2011

[15] X. Wang, J. Zhang, "An Image Scrambling Encryption using Chaos-controlled Poker Shuffle Operation", IEEE International Symposium on Biometrics and Security Technologies, Islamabad, Pakistan, April 23-24, 2008