High Level Secure Messages Based On Steganography And Cryptography

S.Jagadeesan[1], C.Mani[2], R.Navin Kumar[3], S.Prabhakaran[4]
Assistant Professor[1,3], Associate Professor[2], Department of CSE, Nandha Engineering College, Erode,
Assistant Professor[4], Department of EEE, Nandha Engineering College, Erode,.

Abstract *— Steganography and cryptography are very important techniques utilized in information security to cover and secure secret messages in transmitted information. This paper can introduce, implement and take a look at a unique methodology which may be used as a secure and extremely economical method {of information|of knowledge|} activity as well as data extracting. Some potency parameters are going to be through an experiment obtained and compared with alternative existing ways parameters to prove the potency of the planned methodology.*

Keywords - *steganography; cryptography time; MSE; cyptography; cryptography time; speedup; PSNR*

I. INTRODUCTION

Steganography is that the method of concealing secret messages in such some way that nobody except the sender and therefore the supposed recipient will see them. the method of concealing knowledge is employed in several vital applications so as to maintain confidentiality of vital knowledge, forestall unauthorized persons from distinguishing or understanding the confidential message, or add mark or a tag to the digital image to be utilized in order to spot the digital image possession. Cryptography is that the method of adjusting knowledge so they're not legible. Unauthorized parties would possibly see there area unit knowledge communicated however can't perceive them. Digital color pictures are often used as a media to hold the key massage, attributable to their size, and since they're usually given by three second matrices (one for the red color, one for the inexperienced color and therefore the last one for the blue color) [1, 2]. the method of concealing a secret message are often complete by applying the subsequent 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.

C. Message Extraction

The process of obtaining the key message (extracting the message) will be done by applying the cryptography and so the steganography supported the strategies utilized in the activity part. the chosen strategies for information hiding-extraction and information encryption-decryption should be secure and economical by achieving the following: minimizing hiding-extraction time, minimizing encryption-decryption time, maximising the method turnout by increasing the quantity of bytes to be treated per second, and excluding any loss of knowledge throughout the complete method.

II. RELATED WORK

Many steganography ways area unit supported the smallest amount important bit (LSB) technique of knowledge concealment and extracting [4- 6]. Some enhancements were intercalary to boost the safety level of LSB technique in [7-9]. LSB is associate degree unsecure technique of concealment secret messages, and therefore the method of knowledge concealment are often enforced by reserving eight bytes of the holding image to store one character of the message. LSB needs the binary version of the character, and every little bit of} this version are often inserted within the least bit of the chosen computer memory unit of the holding image. the benefits of the LSB based mostly ways area unit the low values of mean sq. error (MSE), and therefore the high values of peak signal to noise magnitude relation (PSNR) [10], that build troublesome for the human eye to note the changes within the holding image. Authors in [11] projected a way of color image encryption-decryption supported matrix rearrangement and with a medium output. Authors in [12] prompt a way of encryption-decryption in digital color pictures by applying matrix operation. This technique gave sensible potency parameters and high security level however the scale of the non-public secret key used for encryption-decryption was terribly massive and complex and needed massive memory size to be keep. Authors in [13] prompt a way of image encryption- decoding

supported a chaotic algorithmic rule victimization the ability and tangent functions rather than linear functions. the method of encoding is one-time-one-password system and is safer (but not enough) than the DES algorithmic rule. Also, it's low economical parameters with massive encryption-decryption time and low output. In [14], associate degree uneven color image encryption-decryption technique was introduced supported matrix

transformation however it had high encryption-decryption time and so low output. In a way of color image encryption-decryption was projected supported Rubik's cube principle, with sensible security level however with low output. In a way of color image encryption-decryption was bestowed supported victimization chaos-controlled poker shuffle operation. each variants of this technique had poor output

III.THE PROPOSED METHODOLOGY

A. Image concealment

Hiding a secret message during a covering color image are often enforced by applying the subsequent phases:

1) Inserting the Message Into the Image

Here we've got to perform the subsequent steps:

• Select the covering color image.

• Get the key message.

• Define the beginning position within the image and therefore the message length (row, column, length). This position are often used as a primary secret non-public key (key1).

• Insert the characters of the key message, by reserving one computer memory unit of the image to 1 character of the message.

• Save the holding image and key1.

2) Holding Image secret writing

Here we've got to perform the subsequent steps:

• Get the holding color image.

• Reshape the 3D color matrix to 2nd matrix.

• Divide the 2nd matrix into equal sizes blocks (in our paper block size=4×4 matrix).

• Select a 4×4 matrix with values within the vary zero to 255 to be used as secret non-public key (key2).

• Apply XOR operations (each block with key2) to urge the encrypted 2nd matrix.

• Reshape the 2nd matrix to 3D color matrix to urge the encrypted color image.

• Save the encrypted color image and key2.

B. Message Extraction

Extracting the key message from the holding encrypted image are often enforced by applying the subsequent phases:

1) Color Image cryptography.

Here we've got to perform the subsequent steps:

• Get the encrypted color image.

• Reshape the 3D color matrix to 2nd matrix.

• Divide the 2nd matrix into 4×4 blocks.

• Get key2.

color image.

2) Extracting the key Message

Here we've got to perform the subsequent steps:

• Get key1.

• Use key1 to extract the characters from the image.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The projected methodology was enforced and varied pictures of various sizes and kinds were used. to point out the potency sweetening the projected methodology was enforced in 2 phases, inserting and extracting the key message within the image. the subsequent message "ZIAD ALQADI" with length=11 characters was inserted-extracted by victimization hand-picked position initially, then by victimization the LSB technique. Figure one shows the first color image, whereas Figure two shows the holding image

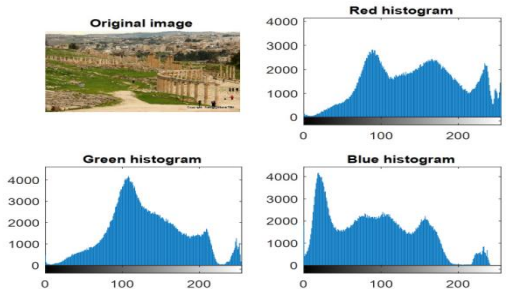

Fig. 1. Original color image with histograms.

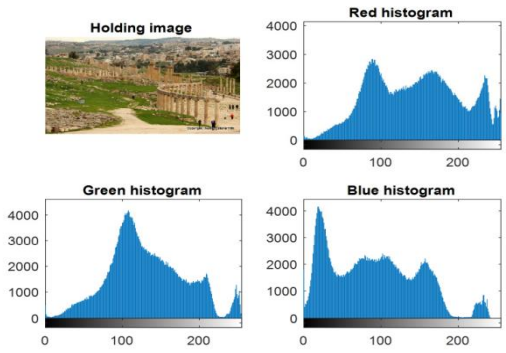

Fig. 2. Holding image with histograms.

Message insertion was enforced many times. The results of implementation ar shown in Table I, whereas Table II shows the results obtained with the employment of the LSB technique. Table III shows a outline comparison between the results of the 2 ways.

ABLE 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 projected elect position methodology is healthier than the performance of the LSB methodology (including secret writing and secret writing times and throughput) which the SNR and MSE values for LSB methodology area unit higher than those of the projected elect position methodology.

These parameters are not considerable because the second stage is encryption of the holding image, so MSE and PSNR are to be ignored.

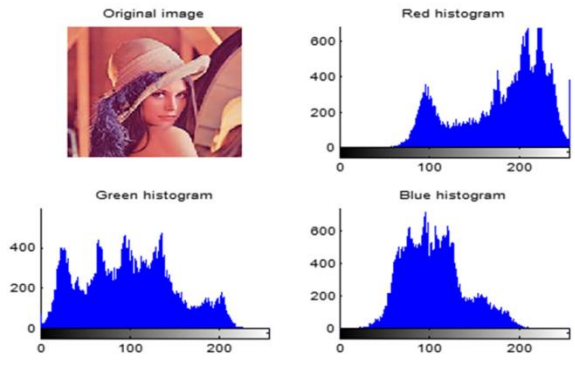

Fig. 3. Holding color image and histograms

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.

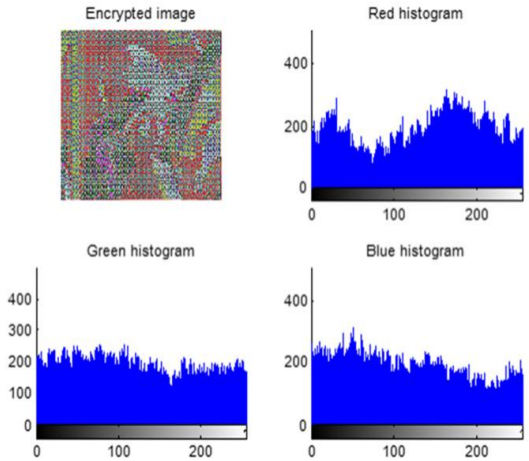

Fig. 4.Encrypted color image and histograms

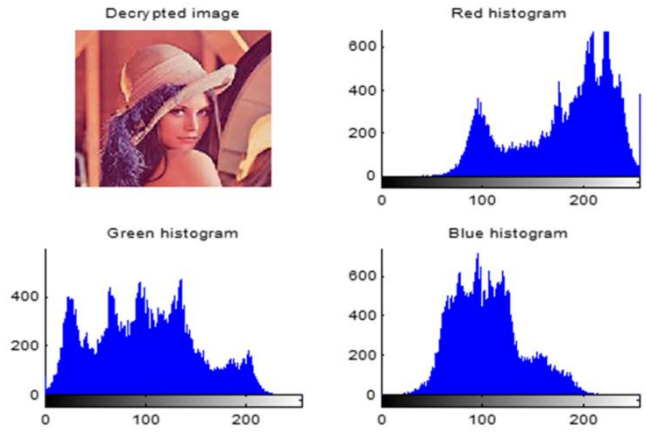

Fig. 5.Decrypted color image and histograms

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 O THER 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

The idea 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] S.Jagadeesan, "*Steganography Using Genetic Algorithm Along with Visual Cryptography for Mobile Environment Applications*", CIIT Journal of Wireless Communications, Vol.7, No-9,pp-0974-9756,2015.

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

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

[9] 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

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

[11] 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

[12] 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

[13] 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

[14] 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

[15] T.Satish Vijay Rajeev, Gousiya Begum, "*Threshold Cryptosystem Mining of Association Rules using Horizontal Distributed Database*", SSRG-International Journal of Computer Science and Engineering(SSRG-IJCSE) Volume 3 Issue 3 2017.