Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 6, June 2020, pg.156 – 164

Securing LSB2 Message Steganography

Dr. Saleh A. Khawatreh[1]; Dr. Jihad Nader[2]; Dr. Mohammad S. Khrisat[3]; Prof. Yousif Eltous[4]; Prof. Ziad Alqadi[5]
Al-Ahliyya Amman University[1], Albalqa Applied University [2, 3, 4, 5], Faculty of Engineering Technology, Jordan, Amman

Abstract: Securing the confidential secret and personal messages is a vital and important task. In this paper we will show how to increase the security of LSB2 method of data steganography to protect the message imbedded in digital color image. An encryption phase will be added to the hiding process, this encryption will be based on dividing the holding image into blocks and reordering the blocks to get the encrypted image, the reordering sequence here will be kept as a PK to decrypt the encrypted image.
Keywords: Steganography, encryption, blocking factor, reordering table, PK, MSE, PSNR.

Introduction

Social media has spread recently, as it is now widely used in the circulation of various messages [1], [2], [3], [4]. Some of the messages in circulation are confidential or may be of a personal nature [49], [50], which requires their protection [51], [52], [53] and preventing intruders from reading [23[, [24], [25] or understanding them by hiding or encrypting them [46], [47], [48].
The digital color image is considered one of the most important types of digital data used to carry and hide private messages [5], [6], [7], for several reasons, the most important of which are: easy access to the image, ease of image processing, and the possession of a large size image that can hide short and long messages without affecting the digital image.
The digital color image is a three-dimensional matrix [1], [2] in which the first dimension is devoted to represent the red color [11], [12], [13]; the second dimension represents the green color, while the third dimension represents the blue color. Digital images are usually characterized by high resolution [14], [15], which means that the matrix is large and contains a huge number of pixels, which enables us to hide large text messages [16], [17].
To find out how clear the image is, we can use the histogram as shown in figure 1, where one trend is assigned to each color [18], [19]. Histogram [20] , [21], [22]is a one column matrix of 256 elements, each element value points to the repetition of color (0 to 255), the tree histograms can be added together to give use the image total histogram as shown in figure 2.

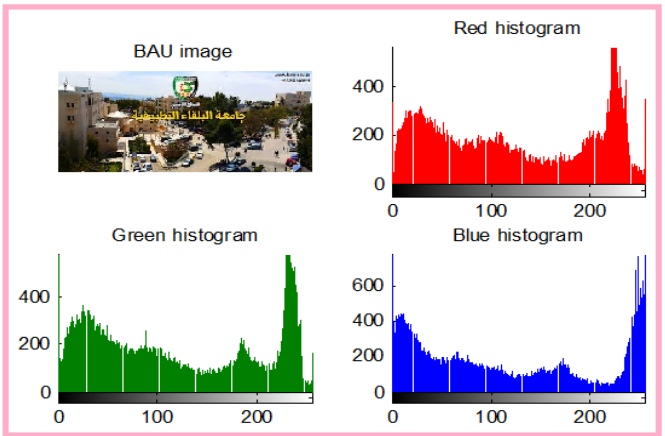

Figure 1: Color image and associated histograms

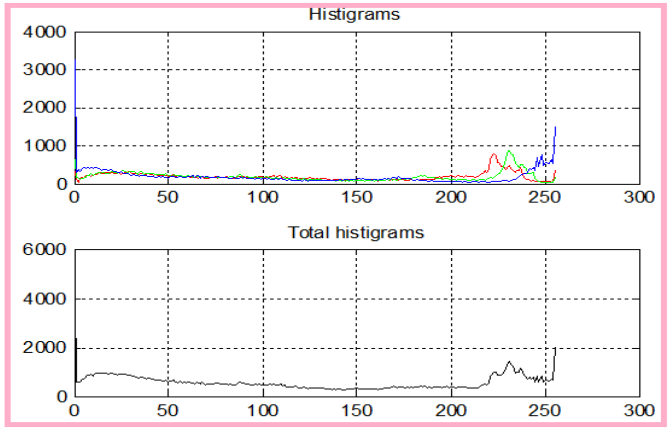

Figure 2: Image total histogram

Steganography and cryptography

Steganography is the art of hiding secret message in another holding or covering data, mainly color image [46], [47], [48]. The method of concealment shall be characterized by the following:

- Ease of implementation.
- The ability to fulfil messages of different sizes (short messages and long messages).
- That the concealment process does not significantly affect the image so that the observation result does not take place with the galaxy eye to prevent intruders from trying to process the image that carries the message [40], [41], [46].
- The method of concealment shall be safe [14], [15].

Many methods were introduced for message steganography [45], [48], [49], and the most widely used methods are based on least significant bit (LSB) method such as LSB2 method.
LSB method of message hiding reserves 8 bytes from the covering image to hold one message character, thus the capacity of this method is equal to the image size divided by 8. LSB2 method of steganography reserves 4 bytes from the covering image to hold one character from the message, thus the capacity of LSB2 method equal the image size divided by 4, figure 3 shows how LSB and LSB2 act with the bits to hold the message characters.

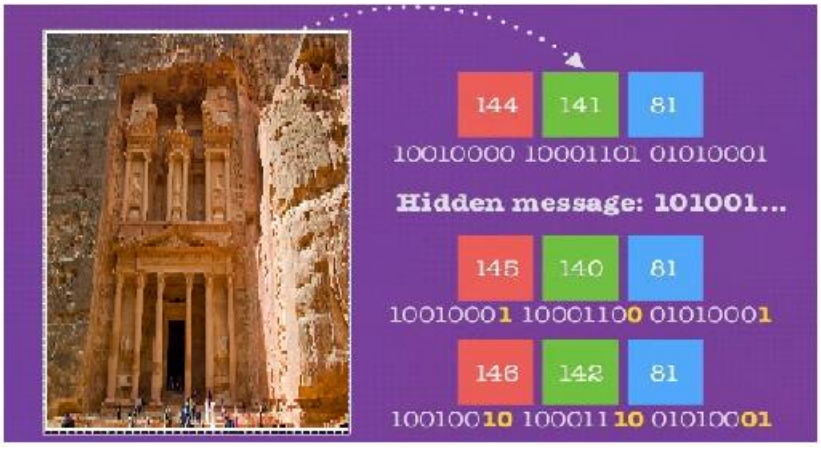

Figure 3: LSB and LSB2 operation

Here in this paper we will use LSB2 method of data hiding because it has a higher capacity as shown in table 1:

Table 1: Capacities of LSB and LSB2

Image number	Size(byte)	Maximum message length(byte) using LSB	Maximum message length(byte) using LSB2
1	150849	18856	37712
2	77976	9747	19494
3	518400	64800	129600
4	5140800	642600	1285200
5	4326210	540776	1081552
6	122265	15283	30566
7	151353	18919	37838
8	1890000	236250	472500
9	6119256	764907	1529814
10	151875	18984	37968

LSB2 method has in noticeable effect [23], [24] on the holding image and the changes on the holding byte range from -3 to 3 as shown in table 2:

Table 2: Changes of the holding byte using LSB2 method

Original LSB2 bits	Holding LSB2 bits	Remark
00	00	No change
00	01	Add 1
00	10	Add 2
00	11	Add 3
01	00	Subtract 1
01	01	No change
01	10	Add 1
01	11	Add 2
10	00	Subtract 2
10	01	Subtract 1
10	10	No change
10	11	Add 1
11	00	Subtract 3
11	01	Subtract 2
11	10	Subtract 1
11	11	No change

LSB2 method provides the following advantages:

- ✓ High capacity.
- ✓ Easy to implement.

- ✓ Minor changes in the holding image, LSB2 provides a high value for peak-to-signal-noise ratio (PSNR), and low vale for mean square error (MSE) between the original and the holding images, thus the changes in the image cannot be noticed by a human eyes .

The disadvantage of LSB2 method is that it easy can be hacked (not secure), and to overcome this disadvantage we have to encrypt the holding image [11], [12], [13].

Encryption is the destruction of data [8], [9], [10] that becomes incomprehensible, and here many methods were introduced for encryption, and in our paper we will focus on blocking and reordering method of data encryption [25-45].

Encryption method must provide the following:

- ✓ Low value of PSNR between the original image and the encrypted one [31], [32].
- ✓ High value of MSE between the original image and the encrypted one [33], [34].
- ✓ High level of security by using a private key, which can not be hacked [35], [36].

The proposed method

The proposed method for secret message hiding will be implemented as follows:

Hiding process:

This phase can be implemented as shown in figure 4 applying the following tasks:

1) Message hiding:
   In this task we shall select the message and the covering image, and then we have to apply LSB2 method to generate the holding image.
2) The holding image must be encrypted using blocking and reordering method: here we have to select the number of blocks (blocking factor); then we have to divide the holding image into equal blocks (as shown in table 3: here blocking factor equal 11), at the end we have to reorder the blocks to get the encrypted image (here the sequence of the reordering will be used as a PK).

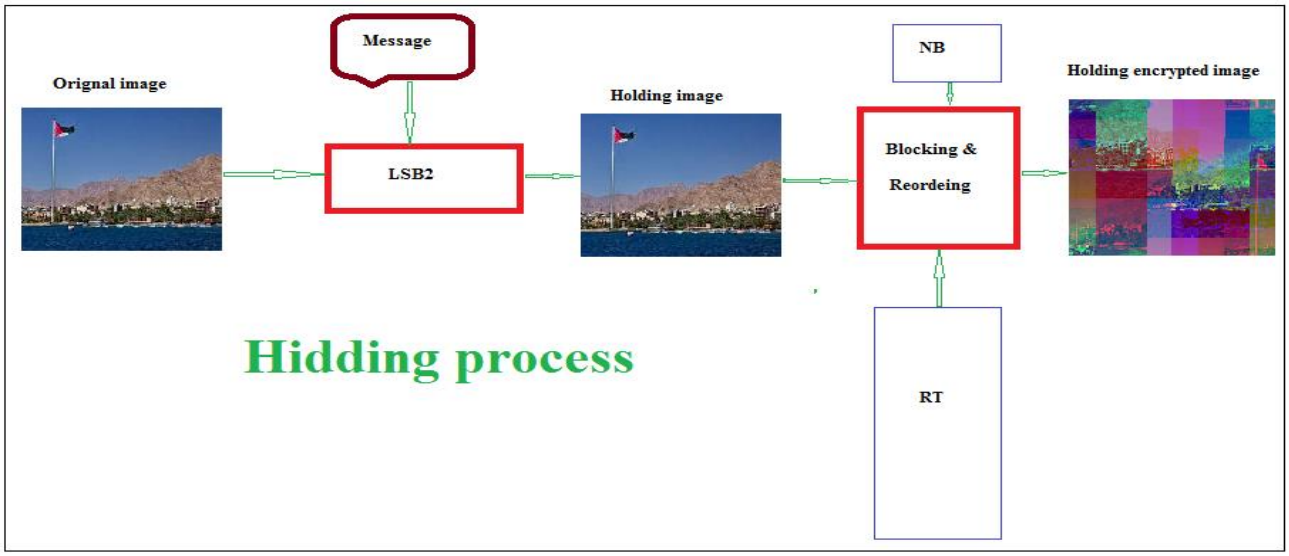

Figure 4: Hiding diagram

Table 3: Reordering table for image 5

Block number	Size	Order(PK)
1	393291	7
2	393291	11
3	393291	9
4	393291	12
5	393291	6
6	393291	2
7	393291	4
8	393291	8
9	393291	3
10	393291	1
11	393291	5
12	9	10

Extracting process:

The extraction process as shown in figure 5 will be implemented applying the following tasks:

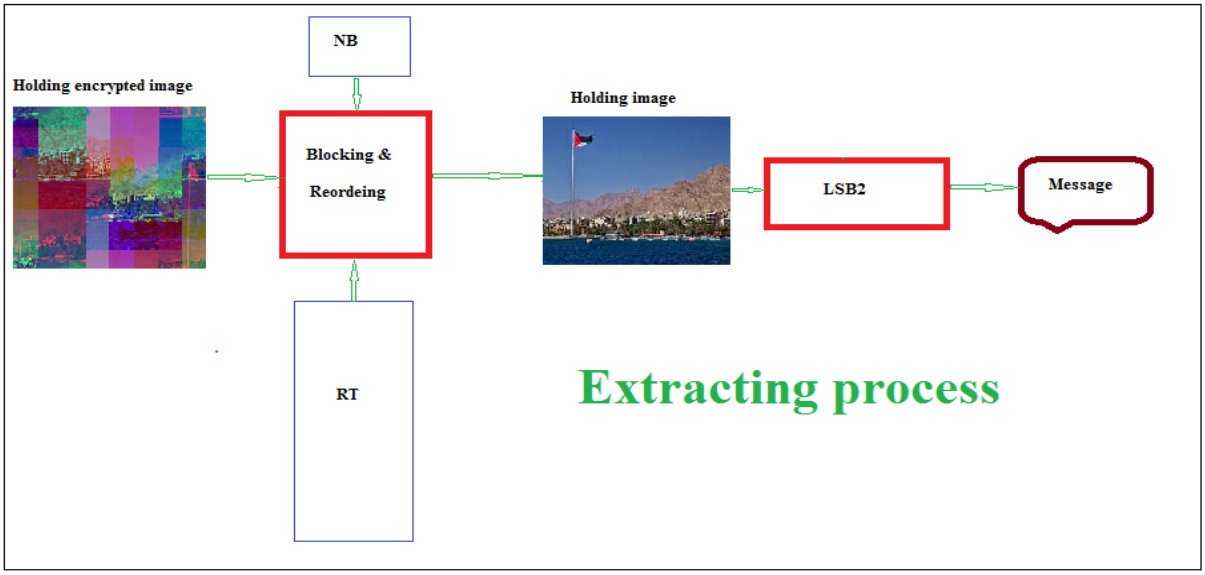

Figure 5: Message extracting diagram

- Decryption
  Here we must have the PK (see table 4), this key can be used to reorder the image to get the decrypted image

Table 4: PK

Order(PK)
7
11
9
12
6
2
4
8
3
1
5
10

- Apply LSB2 to extract the message from the decrypted image.

Implementation and experimental results

The proposed method was implemented using the images shown in table 1, figures 6, 7 and 8 shows the obtained outputs of using image 2 and the message " 'May God protect Jordan and the Jordanians' with length=41:

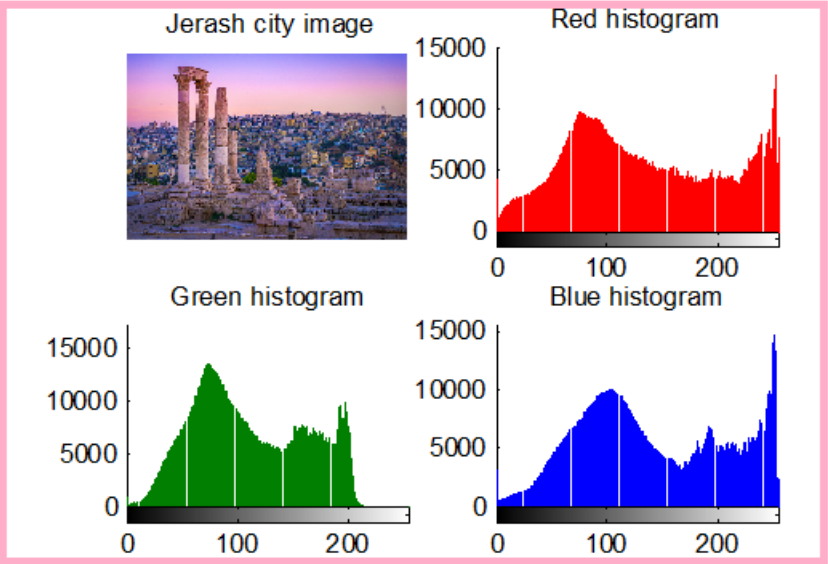

Figure 6: Covering image (example)

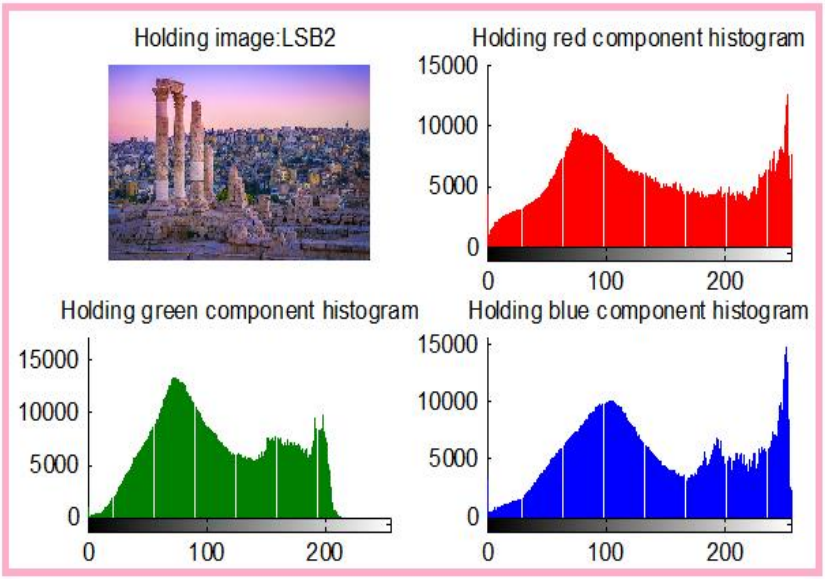

Figure 7: Holding image (example)

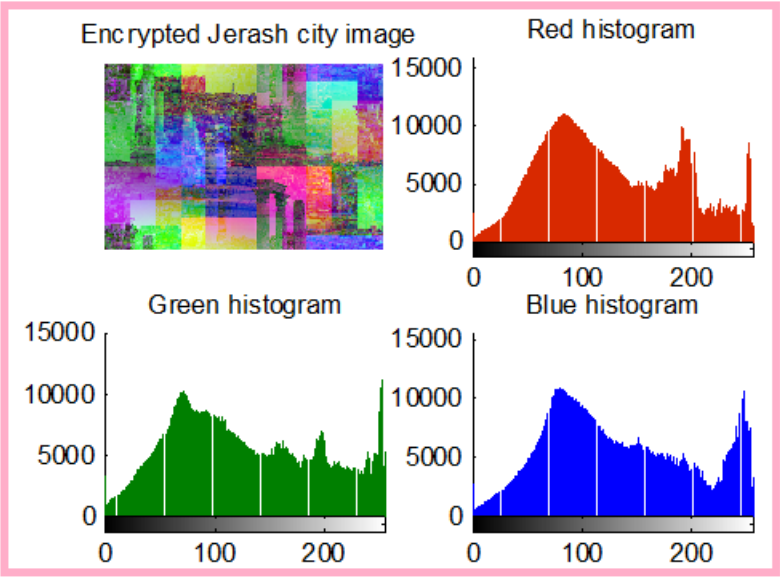

Figure 8: Encrypted holding image (example)

LSB2 method was applied using the smallest image in size, table 5 shows the experimental results, while table 6 shows the experimental results using bigger image.

Table 5: using the smallest image (image 2)

Message length	MSE	PSNR	Hiding time(second)
41	0.0062	161.6874	0.00001
82	0.0107	156.2165	0.0001
164	0.0205	149.6892	0.0020
328	0.0411	142.7390	0.0040
656	0.0810	135.9584	0.0060
1312	0.1631	128.9575	0.0120
2624	0.3243	122.0860	0.0250
5248	0.6503	115.1290	0.0730
Average	**0.1622**	**139.0579**	**0.0153**

Table 6: using the biggest image (image 9)

Message length	MSE	PSNR	Hiding time(second)
41	0.000055072	208.8940	0.0030
82	0.00011554	201.4845	0.0030
164	0.00024055	194.1510	0.0050
328	0.00050022	186.8298	0.0060
656	0.0010	179.7846	0.0080
1312	0.0020	173.1017	0.0140
2624	0.0040	165.9906	0.0270
5248	0.0081	158.9733	0.0530
Average	**0.0020**	**183.6512**	**0.0149**

From tables 5 and 6 we can see that using bigger images will enhance the parameter PSNR and MSE for LSB2.

The encryption phase must reduce the value of PSNR and increase the value of MSE; this was proved by the experimental results shown in table 7:

Table 7: Encryption result

Use message :'May God protect Jordan and the Jordanians' with length=41

Image number	Block size	MSE	PSNR	Encryption time
1	13713	13984	15.3689	0.000100
2	7088	4352.1	27.0410	0.000010
3	47127	8114.9	20.8107	0.0020
4	467345	8887.4	19.9014	0.0260
5	393291	8389.6	20.4777	0.0220
6	11115	5198.4	25.2642	0.0010
7	13759	9584.8	19.1460	0.000010
8	171818	11909	16.9744	0.0090
9	556296	3206.4	30.0962	0.0310
10	13806	15797	14.1496	0.0010
Average		**8942.4**	**20.9230**	**0.0092**

From table 7 we can see the following:

- Low PSNR value.
- High MSE value.
- The encryption process add significant small value to the hiding time (0.009 seconds in average);
- The same blocking factor and PK may be used for deferent images.

Conclusion

A method of improving the security of LSB2 method of secret message steganography was introduced.
The obtained experimental results showed that the proposed method satisfies the requirements of data encryption by decreasing the value of PSNR and decreasing the value of MSE. The method is secure because it uses a PK which is very difficult to guess and hack.

References

[1] Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.
[2] 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, vol. 153, issue 2, pp. 31-34, 2016.
[3] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.
[4] Mohammed Ashraf Al Zudool, Saleh Khawatreh, Ziad A. Alqadi, Efficient Methods used to Extract Color Image Features, IJCSMC, vol. 6, issue 12, pp. 7-14, 2017.
[5] Akram A. Moustafa and Ziad A. Alqadi, Reconstructed Color Image Segmentation, Proceedings of the World Congress on Engineering and Computer Science, WCECS 2009, vol. II, 2009.
[6] 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, vol. 96, issue 13, pp. 4081-4091, 2018.
[7] Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.
[8] Dr Rushdi S Abu Zneit, Dr Ziad AlQadi, Dr Mohammad Abu Zalata, A Methodology to Create a Fingerprint for RGB Color Image, IJCSMC, vol. 6, issue 1, pp. 205-212. 2017.
[9] RA Zneit, Ziad Alqadi, Dr Mohammad Abu Zalata, Procedural analysis of RGB color image objects, IJCSMC, vol. 6, issue 1, pp. 197-204, 2017.
[10] Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, vol. 9, issue 6, pp. 4942-4945, 2019.
[11] Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. AlQadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering, Technology & Applied Science Research, vol. 9, issue 1, pp. 3681-3684, 2019.
[12] Dr. Amjad Hindi, Dr. Ghazi M. Qaryouti, Prof. Yousif Eltous, Prof. Mohammad Abuzalata, Prof. Ziad Alqadi, Color Image Compression using Linear Prediction Coding, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 13 – 20, 2020.
[13] Ziad Alqadi, Mohammad Abuzalata, Yousf Eltous, Ghazi M Qaryouti, Analysis of fingerprint minutiae to form fingerprint identifier, International Journal on Informatics Visualization, vol. 4, issue 1, pp. 10-15, 2020.
[14] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TO CREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.
[15] Prof. Ziad Alqadi, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Dr. Mohammad S. Khrisat, Features Analysis of RGB Color Image based on Wavelet Packet Information, IJCSMC, vol. 9, issue 3, pp. 149 – 156, 2020.
[16] Ziad Alqadi Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, VALUABLE WAVELET PACKET INFORMATION TO ANALYZE COLOR IMAGES FEATURES, International Journal of Current Advanced Research, vol. 9, issue 2, pp. 2319-6505, 2020.
[17] Amjad Hindi, Majed Omar Dwairi, Ziad Alqadi, Analysis of Digital Signals using Wavelet Packet Tree, IJCSMC, vol. 9, issue 2, pp. 96-103, 2020.

[18] Amjad Y. Hindi, Majed O. Dwairi, Ziad A. AlQadi, Creating Human Speech Identifier using WPT, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 117 – 123, 2020.
[19] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Efficiency analysis of color image features extraction methods, International Journal of Software & Hardware Research in Engineering, vol. 8, issue 2, pp. 58-65, 2020.
[20] Ziad A. AlQadi Amjad Y. Hindi, Majed O. Dwairi, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.
[21] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.
[22] Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.
[23] Ziad Alqad, Prof. Yousf Eltous Dr. Ghazi M. Qaryouti, Prof. Mohammad Abuzalata, Analysis of Digital Signal Features Extraction Based on LBP Operator, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 1, pp. 1-7, 2020.
[24] Ziad A. AlQadi, A Highly Secure and Accurate Method for RGB Image Encryption, IJCSMC, vol. 9, issue 2, pp. 12-21, 2020.
[25] Belal Zahran Rashad J. Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, pp. 3228-3235, 2020.
[26] Ziad Alqad, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.
[27] Majed O Al-Dwairi, A Hendi, Z AlQadi, An efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.
[28] Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, A novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp. 232-238, 2019.
[29] Ziad Alqadi, Ahmad Sharadqh, Naseem Asad, Ismail Shayeb, Jamil Al-Azzeh, Belal Ayyoub, A highly secure method of secret message encoding, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 3, pp. 82-87, 2019.
[30] Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, IJCSMC, Vol. 8, Issue 6, pp. 106 –123, 2019.
[31] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, IJCSMC, vol. 8, issue 3, pp. 14-26, 2019.
[32] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh, A Novel Based On Image Blocking Method To Encrypt-Decrypt Color, International Journal on Informatics Visualization, vol. 3, issue 1, pp. 86-93, 2019.
[33] Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION, VOL 3 (2019) NO 3, pp. 262-265.
[34] S. Wang, Y. Zheng, Z. Gao, "A New Image Scrambling Method through Folding Transform", IEEE International Conference on Computer Application and System Modeling, Taiyuan, China, October 22-24, 2010.
[35] 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.
[36] G. Ye, "An Efficient Image Encryption Scheme based on Logistic maps", International Journal of Pure and Applied Mathematics, Vol. 55, No. 1, pp. 37-47, 2009.
[37] T. Sivakumar, R. Venkatesan, "A Novel Image Encryption Approach using Matrix Reordering", WSEAS Transactions on Computers, Vol. 12, No. 11, pp. 407-418, 2013.
[38] H. Gao, Y. Zhang, S. Liang, D. Li, "A New Logistic maps for Image Encryption", Chaos- Solutions & Fractals, Vol. 29, No. 2, pp. 393- 399, 2006.
[39] G. Chen, Y. Mao, C. K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", Chaos, Solutions & Fractals, Vol. 21, No. 3, pp. 749–761, 2004.
[40] 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, Article ID 173931, pp. pp. 1-13, 2012.
[41] 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.
[42] Prof. Ziad Alqad i Prof. Yousif Eltous, Dr. Majed Omar Dwairi, Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, Secure Secret Message Steganography (SSMS), International Journal of Computer Science and Mobile Computing, vol. 9, issue 6, pp. 1-9, 2020.
[43] Dr. Saleh A. Khawatreh Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Digital color image encryption-decryption using segmentation and reordering, International Journal of Latest Research in Engineering and Technology (IJLRET), vol. 6, issue 5, pp. 6-12, 2020.
[44] Prof. Ziad Alqadi Prof. Yousif Eltous, Dr. Akram Moustafa Hamarchi, Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, Color Image Encryption-Decryption using RANDOM Noise and PMT, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 5, pp. 1-7, 2020.
[45] Prof. Ziad Alqadi Prof. Yousif Eltous, Dr. Akram Moustafa Hamarchi, Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, SPEECH SIGNAL ENCRYPTION-DECRYPTION USING NOISE SIGNAL AND PMT, International Journal of Engineering Technology Research & Management, vol. 4, issue 5, pp. 49-59, 2020.
[46] Prof. Ziad Alqadi Dr. Saleh A. Khawatreh, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, A Novel Method to Encrypt-Decrypt Digital Speech Signal (EDDSS), International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 4, pp. 117-123, 2020.
[47] Prof. Ziad Alqadi Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, Dr. Majed Omar Dwairi, Dr. Amjad Hindi, Prof. Yousif Eltous, Analysis of Color Image Noising Process, International Journal of Computer Science and Mobile Computing, vol. 9, issue 6, pp. 65 – 72, 2020.
[48] Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Improving the security of LSB image steganography, JOIV: International Journal on Informatics Visualization, vol. 3, issue 4, pp. 384-387, 2019.
[49] Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Rushdi Abu Zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3, pp. 748-754, 2019.
[50] Ahmad Sharadqh Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 306 – 319, 2019.
[51] J Al-Azzeh M Abuzalata, Ziad Alqadi, Modified Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing, vol. 8, issue 2, pp. 93-103, 2019.
[52] Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. AlQadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering, Technology & Applied Science Research, vol. 9, issue 1, pp. 3681-3684, 2019.
[53] 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, vol. 8, issue 3, pp.18, 2019.

