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.1 – 9

Secure Secret Message Steganography (SSMS)

Prof. Yousif Eltous[1]; Dr. Majed Omar Dwairi[2]; Dr. Mohammad S. Khrisat[3]; Dr. Saleh A. Khawatreh[4]; Prof. Ziad Alqadi[5]
Albalqa Applied University[1, 2, 3, 5]
Al-Ahliyya Amman University[4]

Abstract: Secret message are distinguished by their personal nature or by containing confidential information, which makes it imperative for us to hide this data and prevent unauthorized entities or intrusive people from viewing or understanding it. In this research paper a new SSMS method of data steganography will be proposed, tested and implemented. It will be shown that SSMS method will keep the parameters of LSB method without changes especially MSE and PSNR values. SSMS method will add a high level of security to protect the hidden message; this will be done by using a special PMT as a private key.
Keywords: RGB color image, steganography, PMT, hiding time, extraction time, MSE, PSNR, throughput.

Introduction

Many of the messages circulating through different social media are distinguished by their personal nature or by containing confidential information, which makes it imperative for us to hide this data and prevent unauthorized entities or intrusive people from viewing or understanding it [22], [27]. And to implement the concealment process, it is necessary to search for a medium that carries confidential data so that this medium is large and that a concealment process does not result in a message from affecting the pregnant media and that the change is not noticed by the naked eye [29]. The color digital image [1], [2], [3], [4] is considered one of the best circles used to hide secret messages due to their availability and large size (see figure 1) [5], [6], [7].
RGB color model as shown in figure 2 based on adaptive primary colors: red, green and blue. Colors can be viewed spatially by using the RGB cube shown in figure 2 [8], [9], [12].

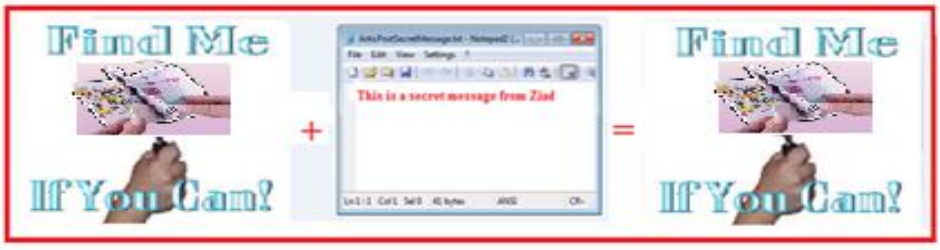

Figure 1: Using color image as a holding image

Red- specifies the intensity of red as integer between 0 and 255, 0 specifies the absence of the red color, while 255 specifies fully saturation with red color [13], [14], [15].
Green- specifies the intensity of green as integer between 0 and 255, 0 specifies the absence of the green color, while 255 specifies fully saturation with green color [16], [17], [18].
Blue- specifies the intensity of blue as integer between 0 and 255, 0 specifies the absence of the blue color, while 255 specifies fully saturation with blue color [19], [20], [21].

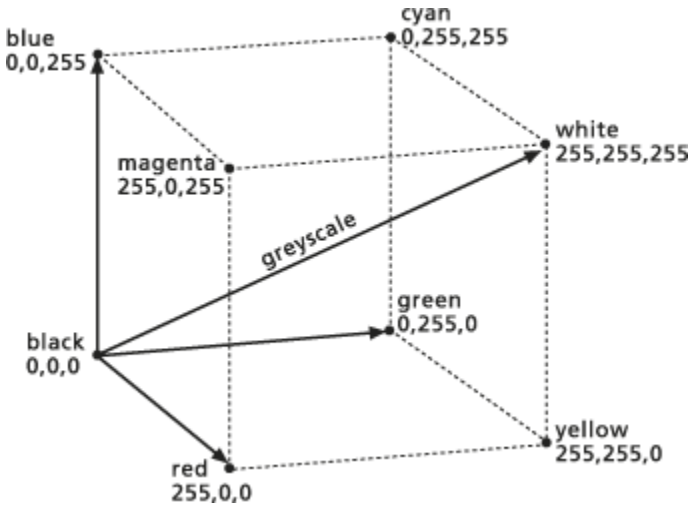

Figure 2: RGB cube colors

The digital color image is the most excellent medium that can be used to hide the secret message because of its large size and its contain a huge number of colors that can be used to carry the parts of the secret message [23].

Data steganography

The process of concealing data (steganography) differs from the encryption process [22], [23]m [24] in that the concealment process does not lead to distorting the data carrying the message, but the carrier appears very close to the original media and cannot be observed with the eye, which prevents the intruders' suspicion from attention to the matter [25], [26], [27].

There are many methods for hiding data, but the simplest is the least significant bit (LSB) method [10], [11], [29]. This method is considered effective for the speed of its implementation and the possibility of hiding messages in a large size without significantly affecting the carrier [[34], [35], [36]. In this case, the size of the hidden message can reach the size of the image divided by 8. In this method, 8 bytes of the image are assigned to carry one symbol from the secret message so that the lower bit is used to carry the relevant bit from the message as shown in figure 3.

Figure 3: LSB implementation

The advantages of LSB method are as follows:

- The ability to hide large, medium and short messages.
- The hidden message does not affect the image so that the carrier image appears in perfect conformity with the original image without noticing any change in the naked eye, here LSB methods provides a high value of peak-to-signal-noise ratio (PSNR) and low value of mean square error (MSE) between the original and the holding images [28], [31], [32], [33].
- High speed in implementation because it did not need a high time to hide the message.

The high value of PSNR and low value of MSE can be achieved by minimizing the changes in the image colors, theses changes can not be noticed abd ranges from -1 to + 1 in the holding byte as shown in table 1:

Table 1: Effects of LSB hiding

Image LSB bit	Message bit	Remark
0	0	No change
0	1	Add 1
1	0	Subtract 1
1	1	No change

Figiure 4 shows the results of adding 1 to the red colors, subtracting one from the green colors, here the PSNR was equal 115.0466 and MSE was equal 0.6556 (exellent values).

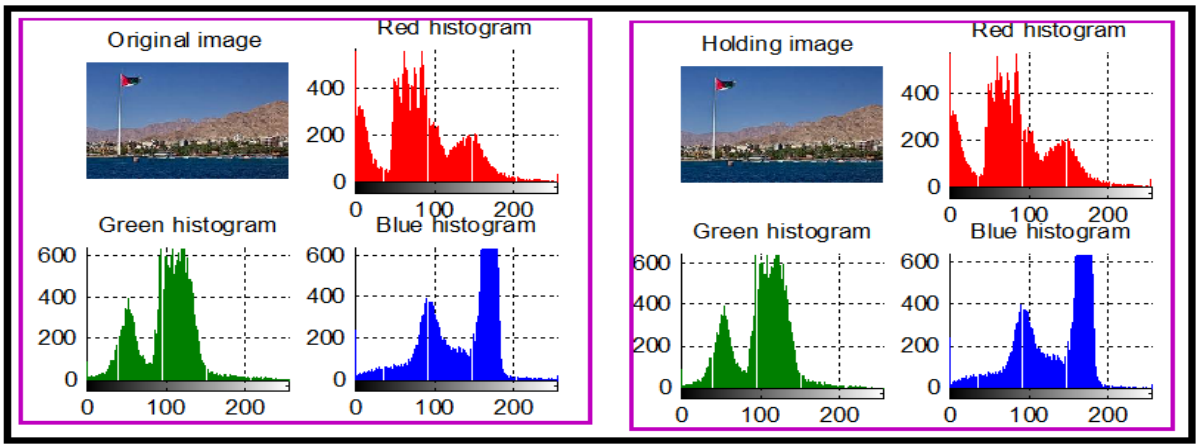

Figure 4: Example of LSB implementation

One of the major disadvantages of LSB method is the low level of protection and security that enables intruders to penetrate the message and know its contents, which requires a change in this method to increase the level of safety and protection.

Color image reordering

Image reordering is used to to add safety and protection conditions to LSB method of data hiding. The process of reshaping the color image and mixing colors depends on the use of a special schedule that is used as a secret key and is called a partition map table (PMT). Here we have to reshape the color image 3D matrix into one row matrix, then we have to create PMT table to devide the row image matrix into various partitions. For each partition we have to define the size and location, these patitions must be mixed and un updated PMT must be saved to be used as key to extract the message. Table 2 shows the PMT example used to devide a color image, while table 3 shows the updated PMT (UPMT) used to reorder the image and to extract the hidden message.

Table 2: PMT example

Partition number	Size	Location
1	1000	1
2	13000	1001
3	50000	14001
4	10000	64001
5	5000	74001
6	6000	79001
7	6000	85001
8	Depends on the image size	91001

Table 3: UPMT

Partition number	Size	Location	Order
1	1000	1	8
2	13000	1001	4
3	50000	14001	1
4	10000	64001	7
5	5000	74001	6
6	6000	79001	5
7	6000	85001	3
8	Depends on the image size	91001	2

Figure 5 shows the original and reorder images using PMT

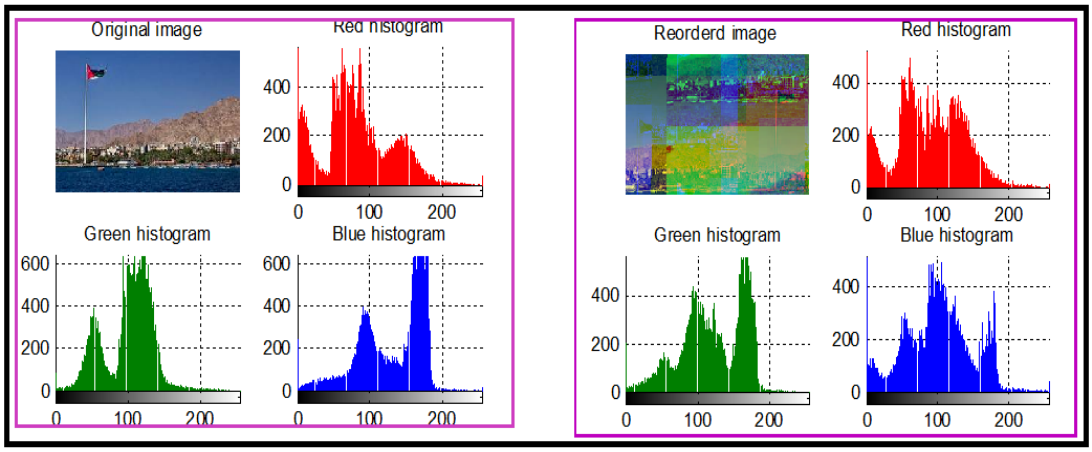

Figure 5: Image reordering using PMT (example)

The proposed SSMS method of data steganography

SSMS method of data steganogrphy for hiding phase can be implemented applying the followinng steps as shown in figure 6:

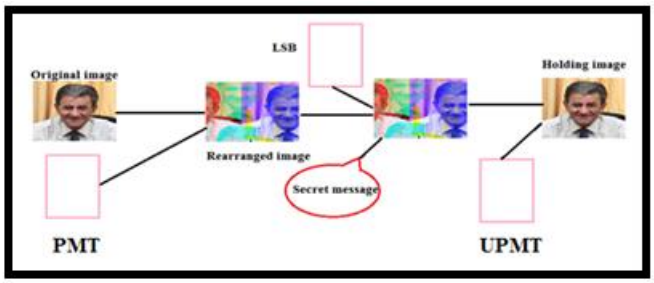

Figure 6: SSMS hiding phase

1) Get the original image.
2) Get the message.
3) Reshape the color image 3D matrix into one row matrix.
4) Generate PMT.
5) Reorder the row matrix according PMT.
6) Rearrange the row matrix and update PMT to create UPMT.
7) Apply LSB method of data hiding for each character in the message.
8) Use UPMT to get the original image.
9) Reshape the row matrix to get the holding image 3D matrix.

The extraction phase can be implemented as shown in figure 7 applying the following steps:

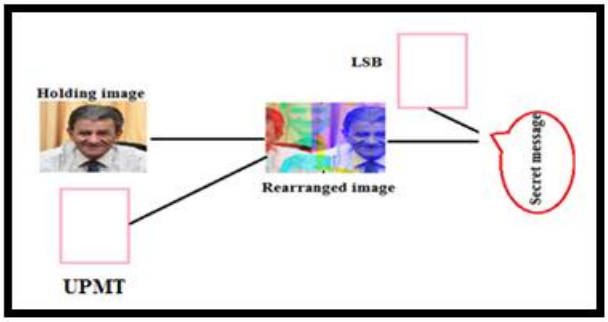

Figure 7: Extraction phase

1) Get the holding image.
2) Reshape the color image 3D matrix into one row matrix.
3) Get U PMT.
4) Reorder the row matrix according UPMT.
5) Rearrange the row matrix using UPMT.
6) Apply LSB method of data hiding to extract message characters.

Implementation and experimental results

Several images were selected, and several messages were defined, these images and messages were used in the proposed SSMS method, table 4 shows the extracted wrong message "Ziad AlQadi" from a holding image without using reordering phase:

Table 4: Receiving wrong messages from a holding image without reordering

Image number	Image size(byte)	Extracted Message
1	150849	C-*#
2	177976	□
3	518400	- 3DNOPNNMNP
4	5140800	&-'#,9SmF0
5	4326210	@'+@FEC;$
6	122265	YZ[\]_klmopp
7	518400	RG/?xŠ
8	150975	¯°°
9	150975	9-JuŠŠ
10	151353	#
11	1890000	th[PPO=/1?LS
12	6119256	
13	150876	××
14	150738	(c[lz?-
15	151875	FB=965887543

Figure 8 shows an example hiding the mentioned message:

Figure 8: Message hiding results example

The following massage 'Amman is the capital city of Jordan' was selected (length=37), SSMS method was implemented using the images listed in table 4, and table 5 shows the results of hiding phase, tables 5 and 6 show the obtained experimental results:

Table 5: Hiding results (message length=35)

Image number	Rearranging time(second)	LSB hiding time(second)	Rearranging time(second)	Total hiding time(second)	MSE	PSNR
1	0.001000	0.0470	0.001000	0.0490	0.0045	164.9037
2	0.001200	0.0550	0.001200	0.0574	0.0098	157.0681
3	0.003000	0.0580	0.003000	0.0640	0.00047068	187.4386
4	0.025000	0.2140	0.025000	0.2640	0.00016768	197.7599
5	0.025000	0.1910	0.025000	0.2410	0.00016758	197.7656
6	0.001000	0.0580	0.001000	0.0600	0.0052	163.3501
7	0.003000	0.0630	0.003000	0.0690	0.00047068	187.4386
8	0.001000	0.0550	0.001000	0.0570	0.0026	170.4125
9	0.001000	0.0500	0.001000	0.0520	0.0045	164.8973
10	0.001000	0.0500	0.001000	0.0520	0.0051	163.6221
11	0.010000	0.2650	0.010000	0.2850	0.00030212	191.8723
12	0.031000	0.2590	0.031000	0.3210	0.00012959	200.3365
13	0.001000	0.0500	0.001000	0.0520	0.0051	163.5646
14	0.001000	0.0490	0.001000	0.0510	0.0052	163.3379
15	0.001000	0.0500	0.001000	0.0520	0.0051	163.6565
Average	**0.0071**	**0.1009**	**0.0071**	**0.1151**	**0.0033**	**175.8283**
	Throughput (character per second			**35/0.1151=304.0834**		

Table 6: Extraction results (Message length=35)

Image number	Rearranging time(second)	LSB extracting time(second)	Total hiding time(second)
1	0.001000	0.0370	0.0380
2	0.001200	0.0380	0.0392
3	0.003000	0.0450	0.0480
4	0.025000	0.0730	0.0980
5	0.025000	0.0770	0.1020
6	0.001000	0.0430	0.0440
7	0.003000	0.0430	0.0460
8	0.001000	0.0450	0.0460
9	0.001000	0.0470	0.0480

10	0.001000	0.0370	0.0380
11	0.010000	0.0540	0.0640
12	0.031000	0.0890	0.1200
13	0.001000	0.0440	0.0450
14	0.001000	0.0410	0.0420
15	0.001000	0.0440	0.0450
Average	**0.0071**	**0.0505**	**0.0575**
Throughput		**608.6957**	

From the obtained results shown in tables 5 and 6 we can see the following facts:

- ✓ SSMS provides a high efficiency by having significant high throughput in hiding and extraction phases.
- ✓ SSMS provides a high value of PSNR and low value of MSE between the original image and the holding one; this means that the process of massage hiding will be un noticeable.
- ✓ SSMS remains having a good parameters even if increase the message length as shown in tables 7 and 8.

Table 7: Hiding results (message length=107)

Image number	Rearranging time(second)	LSB hiding time(second)	Rearranging time(second)	Total hiding time(second)	MSE	PSNR
1	0.001000	0.0500	0.001000	0.0520	0.0142	153.3613
2	0.001200	0.0580	0.001200	0.0604	0.0308	145.6429
3	0.003000	0.0670	0.003000	0.0730	0.0014	176.3980
4	0.025000	0.2300	0.025000	0.2800	0.00048708	187.0960
5	0.025000	0.2100	0.025000	0.2600	0.00048356	187.1685
6	0.001000	0.0590	0.001000	0.0610	0.0153	152.6011
7	0.003000	0.0650	0.003000	0.0710	0.0014	176.3980
8	0.001000	0.0590	0.001000	0.0610	0.0075	159.7654
9	0.001000	0.0590	0.001000	0.0610	0.0144	153.2215
10	0.001000	0.0520	0.001000	0.0540	0.0151	152.7841
11	0.010000	0.1300	0.010000	0.1500	0.00098836	180.0199
12	0.031000	0.2780	0.031000	0.3400	0.00040119	189.0360
13	0.001000	0.0650	0.001000	0.0670	0.0156	152.4117
14	0.001000	0.0590	0.001000	0.0610	0.0156	152.4068
15	0.0071	0.0580	0.0071	0.0722	0.0157	152.3555
Average	**0.0075**	**0.0999**	**0.0075**	**0.1149**	**0.0100**	164.7111
Throughput (character per second				**107/0.1050=931.2446**		

Table 8: Extraction results (Message length=107)

Image number	Rearranging time(second)	LSB extracting time(second)	Total hiding time(second)
1	0.001000	0.0370	0.0380
2	0.001200	0.0450	0.0462
3	0.003000	0.0490	0.0520
4	0.025000	0.0830	0.1080
5	0.025000	0.0760	0.1010
6	0.001000	0.0420	0.0430
7	0.003000	0.0470	0.0500
8	0.001000	0.0430	0.0440
9	0.001000	0.0460	0.0470
10	0.001000	0.0490	0.0500
11	0.010000	0.0760	0.0860

12	0.031000	0.0890	0.1200
13	0.001000	0.0560	0.0570
14	0.001000	0.0470	0.0480
15	0.001000	0.0450	0.0521
Average	**0.0071**	**0.0553**	**0.0628**
Throughput		**1703.8**	

Conclusion

SSMS method of data steganography was proposed, tested and implemented, It was shown that the proposed SSMS method does not negatively affect the value of LSB method parameters such as MSE and PSNR, and it keeps these parameters as they were for LSB method of data steganography. The proposed SSMS method protects secret messages by providing a high level of security using PMT as a private key. PMT is very difficult to hack and it may change from time to time.

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] 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.
[35] 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 13, pp. 76-90, 2019.
[36] 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.

