Secure, Image based Private Key for Secret Message Cryptography

Ziad Alqadi
Professor
Al Balqa Applied University
Amman 11134, Jordan 15008

Yousif Eltous
Professor
Al Balqa Applied University
Amman 11134, Jordan 15008

Amjad Al Hindi
Professor
Al Balqa Applied University
Amman 11134, Jordan 15008

ABSTRACT
The protection of text messages, whether short or long, is a very important process, and therefore, in this research paper, a new method will be presented to encrypt and decrypt these messages. The proposed method will base on a color image which will kept in secret and used to generate the private key, thus we can guarantee the protection of the secret message from being hacked. The proposed method will be tested and implemented, the obtained results will be used to prove that the method provides good values for MSE and PSNR during the encryption and decryption phases. The proposed method performance parameters will be compared with DES and AES methods parameter to justify the performance enhancement achieved by the proposed method.

Keywords
Cryptography, encryption time, decryption time, MSE, PSNR, image_key

1. INTRODUCTION
Digital color image [9-15] as shown in figure 1 consists of a big number of pixels arranged in a three dimensional matrix (one 2D matrix for each color: 1 red, 2 green, 3 blue) [30-35], the pixel color will be obtained as a process of mixing the three colors [52-56] as shown in figure 2.

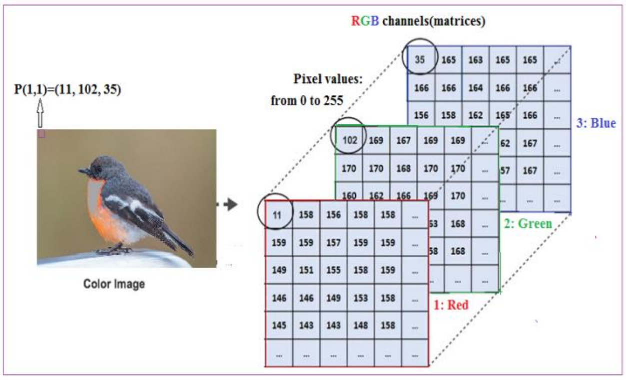

Figure 1: Digital color image structure

	Red	Green	Blue	Hexadecimal code
	0	0	0	#000000
	255	255	255	#FFFFFF
	255	0	0	#FF0000
	0	255	0	#00FF00
	0	0	255	#0000FF
	255	128	0	#FF8000
	255	255	0	#FFFF00
	128	128	128	#808080

Figure 2: Pixel colors

The digital color image has unique properties that will be employed in this research paper, the most important of which are the following [19-27]:

- ✓ Ease of obtaining a digital color image at no cost.
- ✓ Easy color digital image processing.
- ✓ A digital image is a great store of data.
- ✓ The pixel values in the image cover the ASCII characters.
- ✓ The size of the digital image can be adjusted to suit the specific application by implementing the process of resizing and figure 3 illustrates an example of image resizing [28-30].

a

33	187	223	40	103
238	131	26	47	172
40	165	167	118	134
254	37	218	113	103

48	118	85	182	43
21	170	159	126	89
152	37	116	101	207
211	23	141	218	149

52	157	54	82	130
93	150	134	126	114
136	19	31	235	80
217	83	236	33	199

b=imresize(a,[3,3])

33	223	103
40	167	134
254	218	103

48	85	43
152	116	207
211	141	149

52	54	130
136	31	80
217	236	199

Figure 3: Image resizing example

Depending on the characteristics of the above-mentioned image, the digital image can easily be employed to protect confidential data consisting of text messages or text files by implementing the encryption and decryption process of confidential data to protect it from the risk of penetration or the risk of its use by intruders [40-41].

Data cryptography is used to protect secret data by using private key (PK) and manipulating a set of operations to apply data encryption and data decryption as shown in figure 4 [44-51].

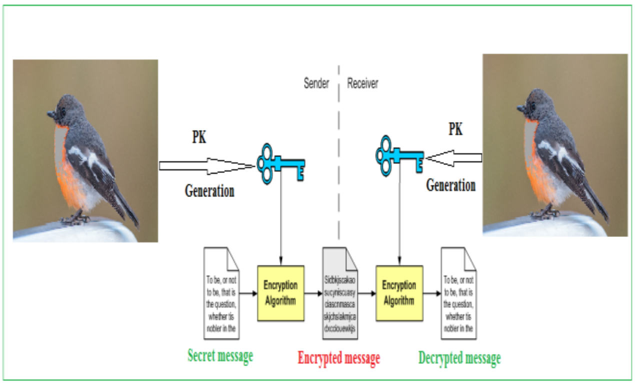

Figure 4: Data cryptography using digital color image

Digital color image can be easily used in the process of data cryptography to generate PK, here the selected color image can be kept in secret and it can be easily used to generate a secure private key, thus we can raise the security level of protecting secret messages and data files, and we can also get benefit of pixels' values which cover the character ASCII values [28-35].

- ✓ The data cryptography method is considered secure and efficient if it satisfies the following requirements:
- ✓ Provides a high efficiency by minimizing the encryption-decryption times.
- ✓ Provides good values of the quality parameters: peak signal to noise ratio (PSNR), and/or mean square error (MSE), these parameters can be calculated using equations 1 and 2[16-18].

$$MSE_z = \frac{1}{N}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[S(i,j)-R(i,j)]^2 \ , N = m*n \quad (1)$$

S and R are two images

Total MSE for color image

$$MSE_t = MSE_r + MSE_g + MSE_b$$

Calculate PSNR

$$PSNR = 10 * \log_{10}\frac{(MAX_I)^2}{MSE_t} \quad (2)$$

The data cryptography method must produce a destroyed encrypted image by minimizing PSNR and maximizing MSE in the encryption phase and full recovery of the original decrypted data by providing a zero MSE and infinite PSNR [18-22].

2. RELATED WORKS

Many methods are used for data cryptography [37-42], and many of these methods are based on DES (data encryption standard) and AES (advance encryption standard). These methods as shown in figures 5 and 6 use a private key with fixed length [1-8].

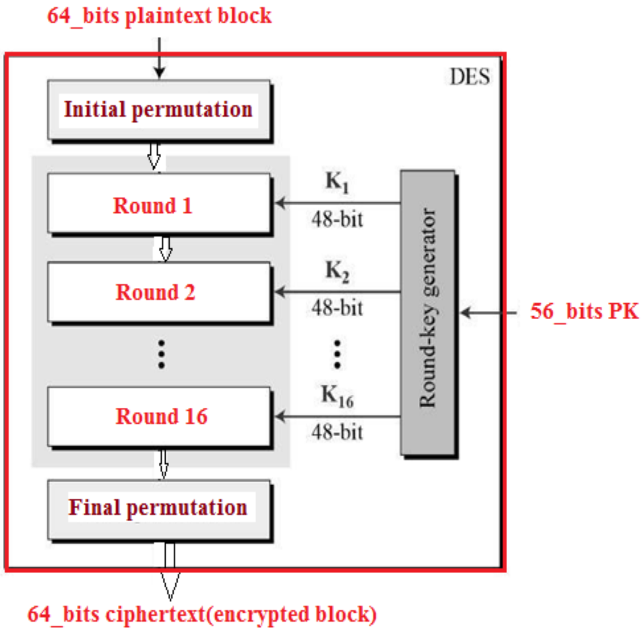

Figure 5: DES encryption

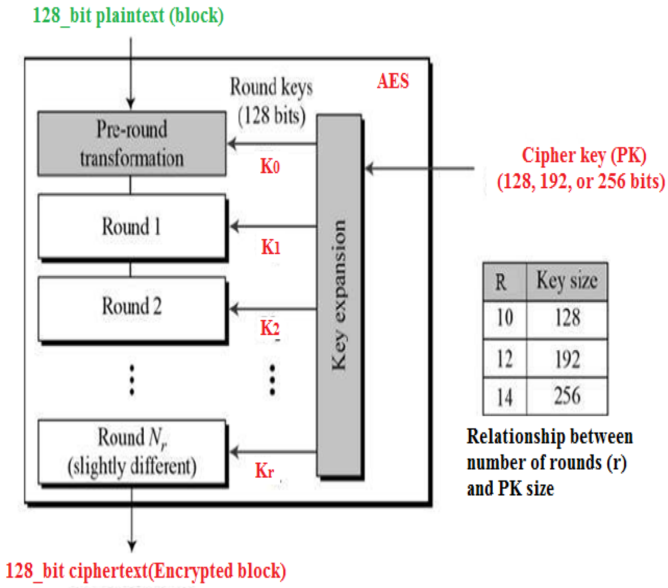

Figure 6: AES encryption

The DES_AES based methods of data cryptography are characterized by the following:

- The PK is has a small length, and sometimes it can be hacked.
- The data to be encrypted-decrypted must be divided into equal blocks with fixed length; this will negatively affect the cryptography process efficiency by increasing the encryption-decryption times.
- Sub keys calculations are required to generate the keys for various rounds of operation, this also requires an extra time which leads to slow the process of data cryptography.
- Many arithmetic and logic operation are required and they are repeated for various rounds.

DES_AES based methods give good values for the quality parameters, but they are not secure enough and not efficient, and to avoid these disadvantages we will introduce a new method which will raise the level of data security and enhance the efficiency of data cryptography keeping MSE and PSNR optimal [18-22].

3. MATERIALS AND METHODS

The proposed method uses digital color image as an image_key, it is chosen and agreed upon by the sender and receiver, kept secret, and used to generate the private key to carry out the encryption and decryption process of secret messages. To ensure the confidentiality process and to prevent any penetration, the image can be replaced from time to time and if the need arises. There are no special requirements for the image_key selection process, and the digital image selected to generate the key can be of any size.

The process of encryption phase can be implemented performing the following steps as shown in figure 7:

1) Get the secret digital color image.
2) Resize the image to 256x256 pixels image, here the rows and columns values are within the range 0 to 255 to cover the ASCII characters.
3) Select on channel from the resized image to be used as an image_key (we selected the red channel)

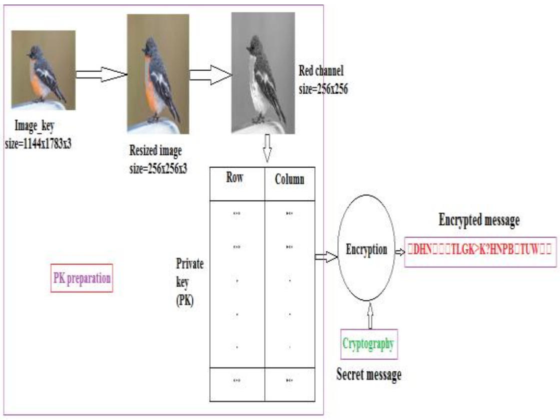

Figure 7: Encryption phase

4) PK creations: PK key used for encryption decryption is a two dimensional matrix (two columns matrix as shown in figure 7), each row contains the location of the ASCII character (row, column) in the image key. To insure that the image_key contains all the ASCII value the last column or row in the image_key can be replaced by the values 0 to 255. The private key can be generated by scanning the image_key to find the first appearance of each ASCII character value, and then the position of this value must be stored in the PK matrix.
5) For each character in the secret message, find the position in the PK and store 2 bytes of the decrypted message.

To decrease the efforts of computations and to decrease the encryption time steps 1 thru 4 can be implemented one time to generate the PK, this key can be saved and loaded when we need to encrypt any secret message, thus the encryption phase can be updated as shown in figure 8

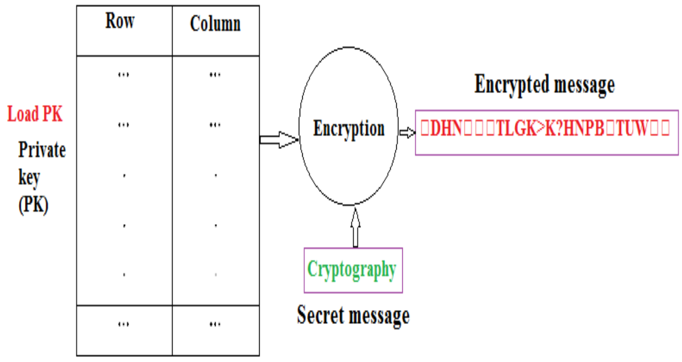

Figure 8: Improved encryption phase

Private Key preparation

The private key used to encrypt-decrypt secret messages is two columns matrix with 256 rows, each row contains the location of ASCII character in the image-key (resized to 256x256 pixels matrix)**,** and this key can be generated performing the following steps:

1) Get the color image_key.
2) Resize the image to an image with size 256x256x3.
3) Get on color channel (1: red for example).
4) Replace one row (or column) with the values 0 to 255 to insure that the image covers all the characters ASCII values (0 to 255).
5) For each character ASCII value find the first appearance of this value in the image, and add the location (row and column) to the PK.
6) Save the PK to be used in the encryption and decryption phases.

The PK key can be easily changed when the needs arise; this can be done by simply replacing the selected image_key by another image and repeating again the PK preparation cycle. Table 1 and 2 show examples of a PKs using the images shown in figure 9.

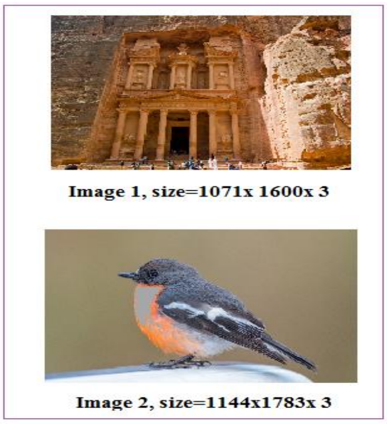

Figure 9: Image_keys

Table 1: Part of PK generated using Image_key 1

Matrix key index	Character	PK Contents		Encoded character	
		Row	**Column**	1st character	2nd character
66	A	**68**	**1**	67	0
67	B	**18**	**1**	17	0
68	C	**8**	**1**	7	0
69	D	**69**	**1**	68	0

70	E	**237**	**1**	236	0
71	F	**7**	**1**	6	0
72	G	**19**	**1**	18	0
73	H	**15**	**1**	14	0
74	I	**22**	**2**	21	1
75	J	**115**	**1**	114	0
76	K	**59**	**1**	58	0
77	L	**67**	**1**	66	0

Table 2: Part of PK generated using Image_key 2

Matrix key index	Character	PK contents		Encoded character	
		Row	**Column**	1st character	2nd character
66	A	**256**	**66**	255	65
67	B	**77**	**66**	76	65
68	C	**256**	**68**	255	67
69	D	**80**	**67**	79	66
70	E	**256**	**70**	255	69
71	F	**77**	**63**	76	62
72	G	**78**	**69**	77	68
73	H	**256**	**73**	255	72
74	I	**76**	**73**	75	72
75	J	**256**	**75**	255	74
76	K	**80**	**75**	79	74
77	L	77	64	76	63

The decryption phase can be implemented executing the following steps (as shown in figure 10)

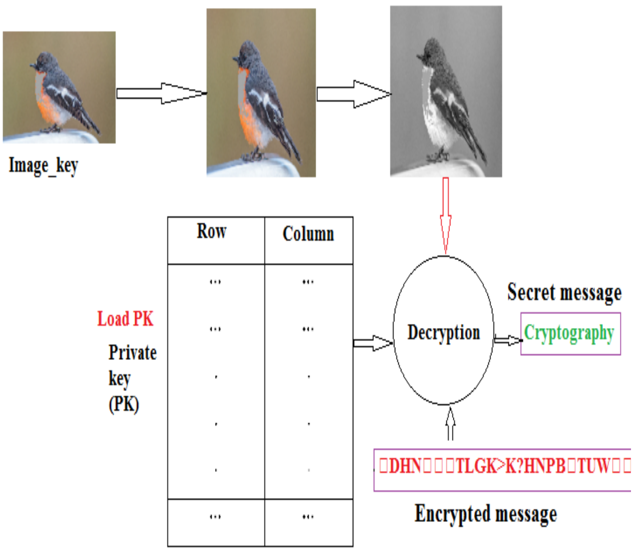

Figure 10: Decryption phase

1) Load the PK.
2) Get the color image and prepare the image_key.
3) Get the decrypted message.
4) For each two bytes of the decrypted message, use these bytes as a location in the image_key to get the ASCII value from the image_key.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

Quality analysis

Deferent short messages were taken and encrypted-decrypted using the proposed method, the image shown in figure 10 was taken as an image_key, for each message the quality parameters were calculated, table 3 shows the obtained results:

Table 3: MSE and PSNR calculations for short messages

Message size(byte)	Between source and encrypted messages		Between source and decrypted messages	
	MSE	PSNR	MSE	PSNR
10	1.4231e+004	15.2717	0	Infinite
50	1.5488e+004	14.4255	0	Infinite
100	1.6608e+004	13.7269	0	Infinite
200	1.5641e+004	14.3271	0	Infinite
400	1.5992e+004	14.1051	0	Infinite
500	1.6576e+004	13.7463	0	Infinite
600	1.6956e+004	13.5195	0	Infinite
700	1.5433e+004	14.4607	0	Infinite
800	1.6493e+004	13.7967	0	Infinite
900	1.7186e+004	13.3853	0	Infinite
1000	1.5951e+004	14.1306	0	Infinite

The same experiment was repeated for long messages; table 4 shows the obtained experimental results:

Table 3: MSE and PSNR calculations for short messages

Message size(K. byte)	Between source and encrypted messages		Between source and decrypted messages	
	MSE	PSNR	MSE	PSNR
10	1.6336e+004	13.8923	0	Infinite
50	1.6354e+004	13.8812	0	Infinite
100	1.6316e+004	13.9045	0	Infinite
200	1.6328e+004	13.8972	0	Infinite
400	1.6358e+004	13.8788	0	Infinite
500	1.6316e+004	13.9047	0	Infinite
600	1.6349e+004	13.8845	0	Infinite
700	1.6322e+004	13.9010	0	Infinite
800	1.6331e+004	13.8955	0	Infinite
900	1.6335e+004	13.8930	0	Infinite
1000	1.6337e+004	13.8914	0	Infinite

From the results shown in tables 3 and 4 we can see that the proposed method satisfies the cryptography quality issues for any message with any length, the proposed method destroyed the message after encryption by maximizing MSE and minimizing PSNR and recovers the original message after decryption by providing a zero MSE and infinite PSNR.

Performance analysis

For performance analysis the encryption-decryption times were calculated and compared with DES and AES times, tables 4 and 5 show the obtained results using short messages and long messages.

Table 4: Cryptography times using short messages

Message size(byte)	DES		AES		Proposed	
	EN_time (seconds)	DEC_time (seconds)	EN_time (seconds)	DEC_time (seconds)	EN_time (seconds)	DEC_time (seconds)
10	0.0001	0.0001	0.0001	0.0001	0.000001	0.000001
50	0.0004	0.0004	0.0003	0.0003	0.000001	0.000001
100	0.0008	0.0069	0.0005	0.0005	0.000001	0.000001
200	0.0019	0.0015	0.0011	0.0011	0.000001	0.000001
400	0.0034	0.0027	0.0025	0.0023	0.000001	0.000001
500	0.0041	0.0036	0.0029	0.0029	0.000001	0.000001
600	0.0051	0.0041	0.0034	0.0032	0.000001	0.000001
700	0.0058	0.0053	0.0039	0.0038	0.000001	0.000001
800	0.0067	0.0059	0.0044	0.0043	0.000001	0.000001
900	0.0073	0.0064	0.0049	0.0048	0.000001	0.000001
1000	0.0082	0.0071	0.0057	0.0056	0.000001	0.000001

Table 5: Cryptography times using long messages

Message size(K. byte)	DES		AES		Proposed	
	EN_time (seconds)	DEC_time (seconds)	EN_time (seconds)	DEC_time (seconds)	EN_time (seconds)	DEC_time (seconds)
10	0.0598	0.0519	0.0420	0.0398	0.001000	0.000001
50	0.2987	0.2592	0.2010	0.1966	0.006000	0.002000
100	0.5969	0.5182	0.4100	0.4029	0.010000	0.003000
200	1.1929	1.0357	0.8000	0.7857	0.020000	0.006000
400	2.3857	2.0714	1.6000	1.5714	0.040000	0.010000
500	2.9821	2.5893	2.0000	1.9643	0.050000	0.012000
600	3.5786	3.1071	2.4000	2.3571	0.061000	0.015000
700	4.1750	3.6250	2.8000	2.7500	0.071000	0.017000
800	4.7714	4.1429	3.2000	3.1429	0.079000	0.019000
900	5.3679	4.6607	3.6000	3.5357	0.088000	0.022000
1000	5.9643	5.1786	4.0000	3.9286	0.098000	0.025000

From table 5 we can see that the propose method enhanced the performance of the processes of message cryptography by rapidly reducing the encryption and decryption times, figures 11 and 12 show the achieved enhancement provided by the proposed method.

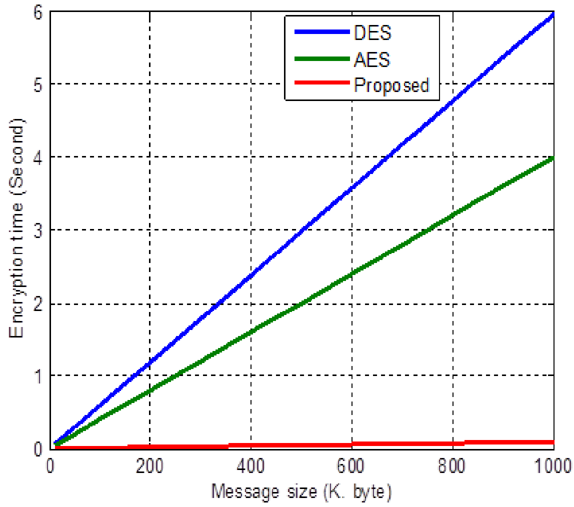

Figure 11: Encryption times comparison

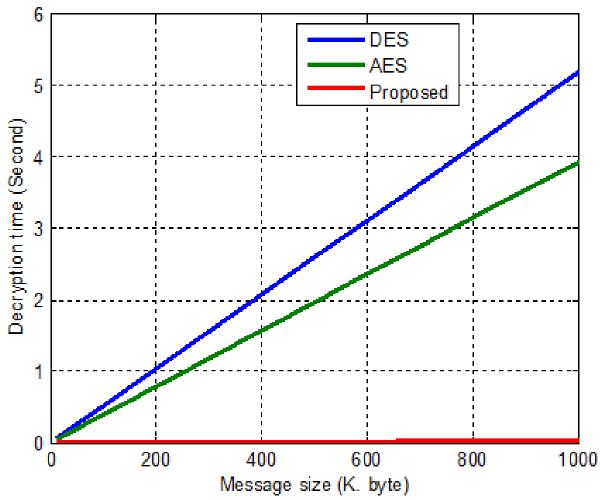

Figure 11: Decryption times comparison

5. CONCLUSION

A simple and easy to implement method of message cryptography was proposed and implemented. The proposed method used an image_key to generate a private key necessary for cryptography; using secret image_key will enhance the level of security and will protect the secret message from being hacked.

The proposed method can be used to encrypt_decrypt any message with any length and regardless the message length the method gave excellent value for MSE and PSNR during the encryption and decryption phases. The proposed method increased the efficiency of data cryptography by rapidly decreasing encryption and decryption times as they was compared with DES and AES times.

6. REFERENCES

[1] E. Fujisaki and T. Okamoto, Secure Integration of Asymmetric and Symmetric Encryption Schemes, *J Cryptol*, vol. 26, pp. 80-101, 2013.

[2] K. Kurosawa and T. Takagi, "Some RSA-Based Encryption Schemes with Tight Security Reduction" in Advances in Cryptology - ASIACRYPT 2003. ASIACRYPT 2003. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, vol. 2894, 2003.

[3] Musbah J. Aqel, Ziad A. Alqadi, Ibraheim M. El Emary**,** Analysis of Stream Cipher Security Algorithm**,** Journal of Information and Computing Science Vol. 2, No. 4, 2007, pp. 288-298.

[4] Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, 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, 2019.

[5] Dr. Hatim Zaini Prof. Ziad Alqadi, SIMPLE, EFFICIENT AND HIGHLY SECURE METHOD FOR TEXT FILES CRYPTOGRAPHY, World Journal of Engineering Research and Technology, vol. 7, issue 6, 2021.

[6] Dr. Mohammad S. Khrisat Prof. Ziad Alqadi, ANALYSIS OF TEXT FILES ENCRYPTION-DECRYPTION METHODS, IJETRM, vol. 5, issue 3, pp. 48-54, 2021.

[7] Prof. Ziad Alqadi, EFFICIENT AND HIGHLY SECURE METHOD OF MESSAGE ENCRYPTION, IJETRM, vol. 5, issue 2, pp. 58-64, 2021.

[8] Dr. Jihad Nader; Dr. Mohammad S. Khrisat; Prof. Ziad Alqadi, A Survey of RGB Color Image Encryption Methods, IJCSMC, Vol. 9, Issue. 6, pp.106 –113, 2020.

[9] 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.

[10] 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.

[11] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A Alqadi, Mohammad Khalil Abuzalata, creating a Color Map be used to Convert a Gray Image to Color Image, International Journal of Computer Applications, vol. 153, issue 2, pp. 31-34, 2016.

[12] Qazem Jaber Ziad Alqadi, Jamil azza, Statistical analysis of methods used to enhance color image histogram, XX International scientific and technical conference, 2017.

[13] Bassam Subaih Ziad Alqadi, Hamdan Mazen, A Methodology to Analyze Objects in Digital Image using Mat lab, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 21-28, 2016.

[14] Mazen A. Hamdan Bassam Subaih, Prof. Ziad A. Alqadi, Extracting Isolated Words from an Image of Text, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 29-36, 2016.

[15] 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.

[16] Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.

[17] Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.

[18] 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, 2020.

[19] Ziad Alqadi, M Essayed Hussein, Window Averaging Method to Create a Feature Victor for RGB Color Image, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, pp. 60-66, 2017.

[20] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.

[21] Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.

[22] Yousf Eltous Ziad A. Al Qadi, Ghazi M. Qaryouti, Mohammad Abuzalata, ANALYSIS OF DIGITAL SIGNAL FEATURES EXTRACTION BASED ON KMEANS CLUSTERING, International Journal of Engineering Technology Research & Management, vol. 4, issue 1, pp. 66-75, 2020.

[23] Ziad A Alqadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[24] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.

[25] Ziad Alqadi, Majid Oriana, Husham Almujafet, Salah Al-Saleh, Hind Al Husband, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 8, pp. 30-48, 2019.

[26] Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.

[27] Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqh, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8, issue 5, pp. 2780-2787, 2018.

[28] Jihad Nader Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.

[29] 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. 76-90, 2019.

[30] 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.

[31] Musbah Aqel Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences, vol. 6, issue 1, pp. 45-52, 2009.

[32] Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.

[33] Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7, issue 3, pp. 104-107, 2018.

[34] Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, 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, 2019.

[35] Majed O Al-Dwairi, A Hindi, 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.

[36] Amjad Y Hindi, 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.

[37] Ziad A Alqadi, Accurate Method for RGB Image Encryption, International Journal of Computer Science and Mobile Computing, vol. 9, issue 1, pp. 12-21,2020.

[38] Ziad Alqadi, 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.

[39] Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, JOIV: International Journal on Informatics Visualization, vol. 3, issue 3, pp. 262-265, 2019.

[40] 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.

[41] 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.

[42] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein, A Comparison BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, International Journal of Computer Science & Information Technology (IJCSIT), vol. 8, issue 5, pp. 125-131, 2016.

[43] PROF. ZIAD A. ALQADI, A SIMPLE METHOD TO ENCRYPT-DECRYPT SPEECH SIGNAL, International Journal of Engineering Technology Research & Management, vol. 5, issue 2, pp. 44-52, 2021.

[44] Ziad Alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2. Issue 4, pp. 288-298, 2007.

[45] Rashad J Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 14-26, 2019.

[46] Musbah Aqel, Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, vol. 6, issue 1, pp. 45-52, 2009.

[47] 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.

[48] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.

[49] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, uggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.

[50] Akram A Moustafa, Ziad A Alqadi, A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image, Journal of Computer Science, vol. 5, issue 5, pp. 355-362, 2009.

[51] Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, International Journal of Computer Science and Mobile Computing, vol. 8, issue 6, pp. 106-123, 2019.

[52] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.

[53] 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.

[54] ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.

[55] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.

[56] Ziad Alqadi, A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image, Journal of Computer Science, vol. 5, issue 5, pp. 355-362, 2209.