Available Online at www.ijcsmc.com/journal

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. 11, Issue. 3, March 2022, pg.138 – 151

Image Encryption using Variable Length Blocks and Variable Length PK

Mua'ad M. Abu-Faraj*; Ziad A. Alqadi**
*Department of Computer Information Technology, The University of Jordan, Aqaba 77110, Jordan
**Electrical Engineering Department, Albalqa Applied University, Amman 15008, Jordan

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i03.016

Abstract: The colored digital image is one of the most important and popular types of digital data for use in many vital applications, which requires the provision of safe methods to protect it from penetration operations and protect it from tampering and data thieves. In this research paper, a new method for protecting digital images of various types will be presented, which is characterized by ease of implementation and providing a high degree of security and protection for the digital image. A secret color image known only by the sender and receiver will be used as an image_ key, this image_key will be used to generate a private key to encrypt-decrypted any color image by applying image resizing. The private key will be variable, and will match the image block size. The image to be encrypted-decrypted will be divided into blocks, the block size will be variable and agree upon between the sender and receiver. The proposed method will be implemented, the obtained results will be analyzed to prove the efficiency, security level and quality parameters provided by the proposed method.

Keywords: Cryptography, PK, MSE, PSNR, throughput, cryptography time, image_key, reshaping, resizing.

Introduction

Colored digital images are one of the most common types of digital data circulated through various social media for several reasons, the most important of which are [48-52]:

- Ease of obtaining the digital image at no cost due to the availability of many means, media and equipment through which the image can be obtained [12-15].
- Ease of processing the colored digital image because it is represented by a three-dimensional matrix (the first dimension is red, the second is green, and the third is blue) (see figure 1), and this turns the image processing process into an easy process for matrix processing [16-20].

- The possibility of processing or using the matrix of each of the three colors separately and independently.
- The large size of the digital image, which can be employed for multiple processing operations, such as the process of hiding confidential data in the digital image [17-25].
- The possibility of forming one-dimensional arrays of variable lengths of the digital image, according to the user's request. Here, the digital image can be used to generate the private keys necessary for the encryption and decryption process of confidential data, including color digital images, this operation can be implemented by using image reshaping explained in the example shown in figure 2, the length of the private key can be determined by applying the image resizing operation explained by the examples shown in figures 3 and 4 [26-32].

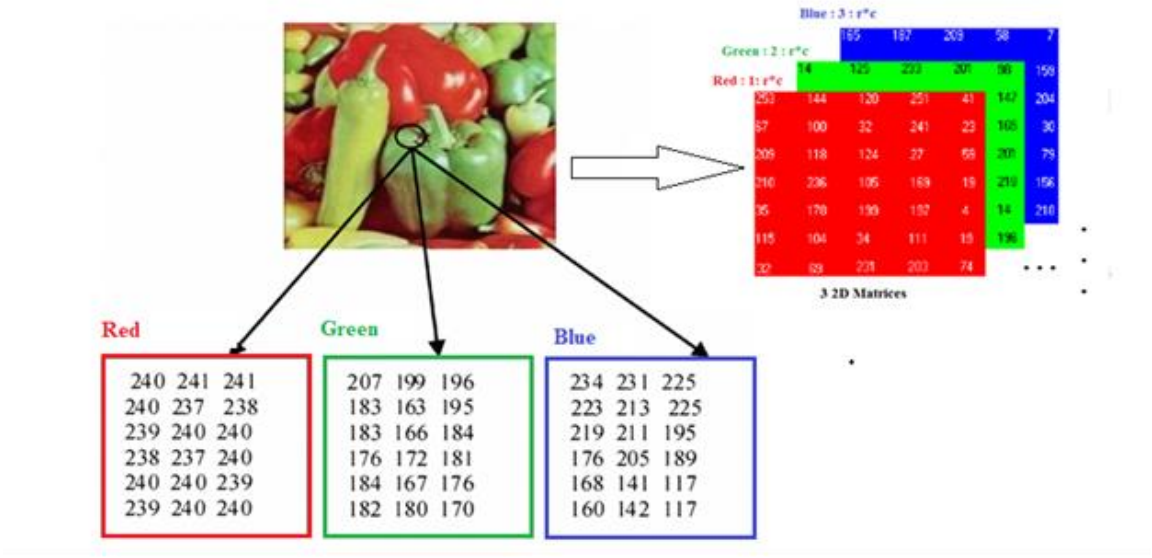

Figure 1: Color image representation

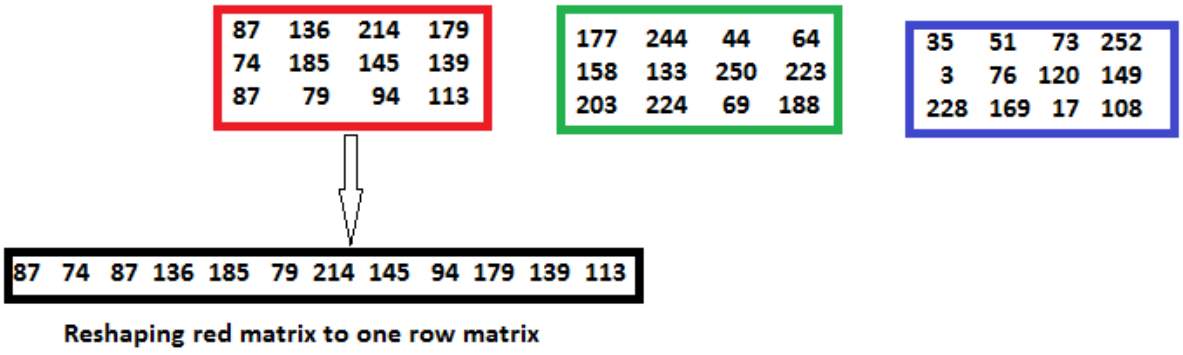

Figure 2: Image reshaping example

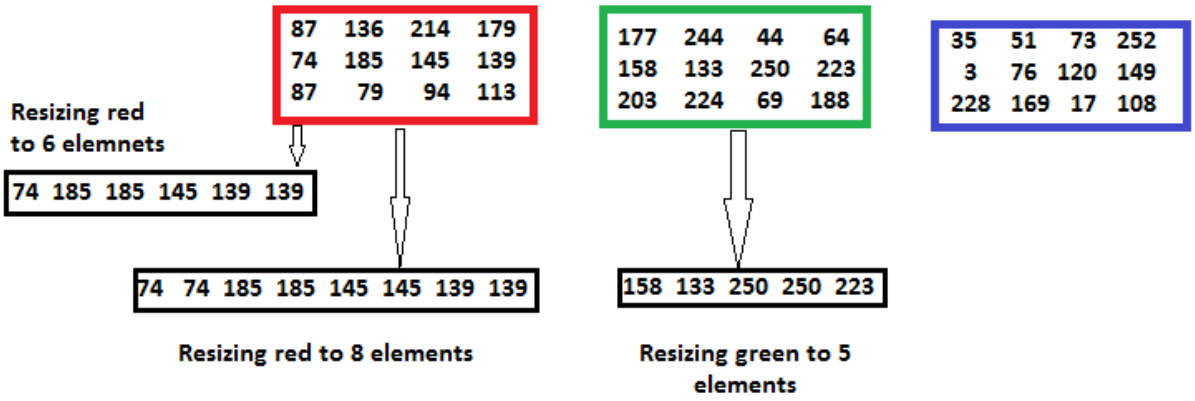

Figure 3: Image colors resizing

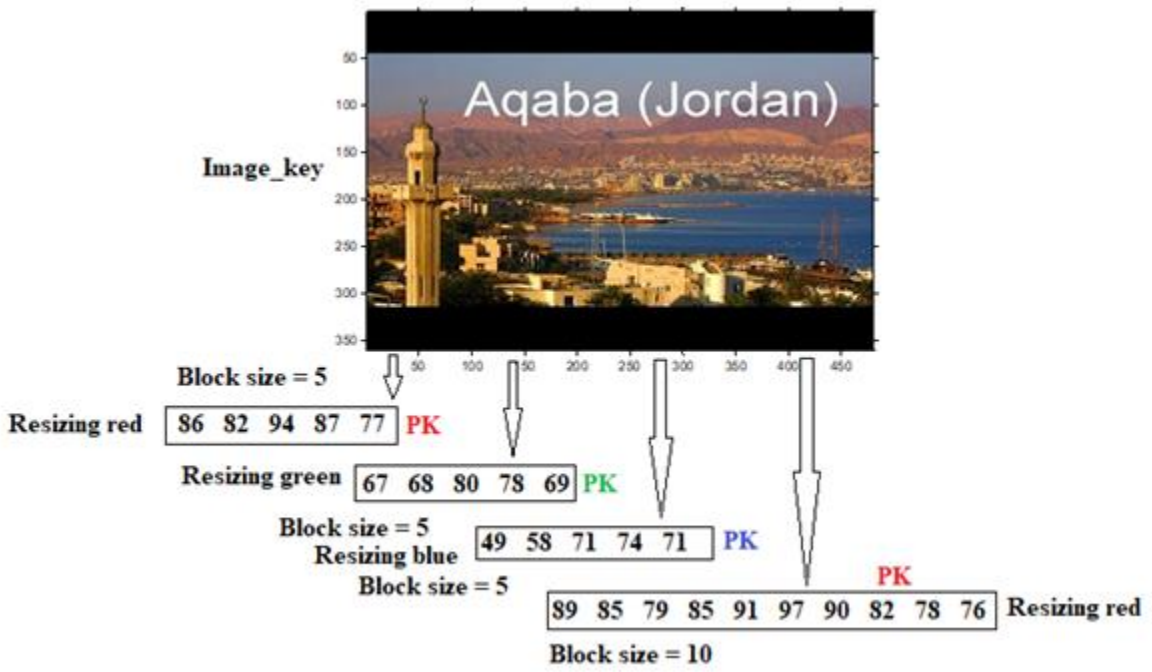

Figure 4: Various PKs extraction

The process of protecting a secret or private digital image, or a picture carrying confidential data, is a very important process in order to prevent intruders, or those who are not authorized to penetrate the image, understand it, or retrieve the data from it [33-40]. One of the most popular methods used to protect images is image cryptography. Data cryptography (as shown in figure 5) means encrypting the data before sending and decrypting the data after receiving to recover the original data [46-48].

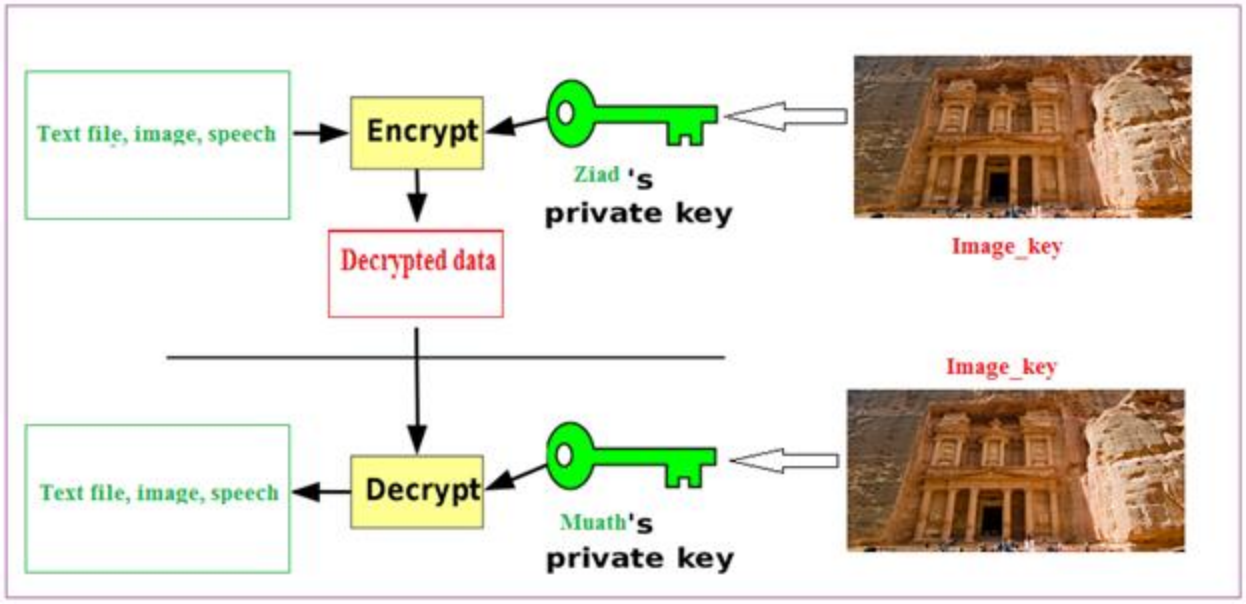

Figure 5: Data cryptography process

The effectiveness of the method to be used in the encryption and decryption process can be measured by the quality parameters, which are: mean square error (MSE) and peak signal to noise ratio (PSNR). The data encryption process must destroy the data completely so that it becomes incomprehensible and useless and therefore the MSE value must be very high and the PSNR value very low, the decryption process must recover the original data so the MSE between the encrypted data and original data must equal zero, while PSNR must equal infinite. MSE and PSNR between two sets of data S and R with length = N can be calculated using equations 1 and 2 [41-47].

$$MSE_{SR} = \frac{1}{N}\sum_{j=0}^{n-1}[S(j) - R(j)]^2 \ , N = n \qquad (1)$$

$$PSNR_{SR} = 10 * \log_{10} \frac{(MAX_i)^2}{MSE_{SR}} \qquad (2)$$

Related works

Many methods are used in data cryptography, many of them are based on standard methods of data cryptography, such as DES, 3DES, AES, and blowfish (BF), these methods can be characterized as follows [1-4]:

- They use fixed block size, the data to be encrypted must be divided into equal sizes blocks, the block size is fixed and cannot be changed.
- These methods are efficient in encrypting-decrypting messages and text files with small sizes, and they become inefficient when dealing with images with huge size.

- They use fixed length PK, this PK sometimes can be hacked, the length of PK cannot be changed, and it is used to generate other key needed for data encryption and decryption.
- These methods provide good value for MSE and PSNR [5, 6].
- The structure of each algorithm is based on Feistel functions by applying a sequence of logical and arithmetic operations.
- The process of encryption/decryption is to be divided into a fixed number of rounds, the round then will be used to encrypt/decrypt each of the data blocks.
- For data with huge sizes these methods are not efficient and they require big time to maintain the process of encryption/decryption, thus the methods throughput (bytes encrypted/decrypted per second) will be low.
- Mainly these methods are hardly to program, the algorithms cannot be modified [7-11].

Most of the above mention characteristics are considered to be disadvantages which must be eliminated by any proposed method of data cryptography.

The proposed method

The proposed method depends on the use of a color image that is agreed upon by the sender and receiver and is kept secret. This image is used to generate the private key, as shown in the figure 6

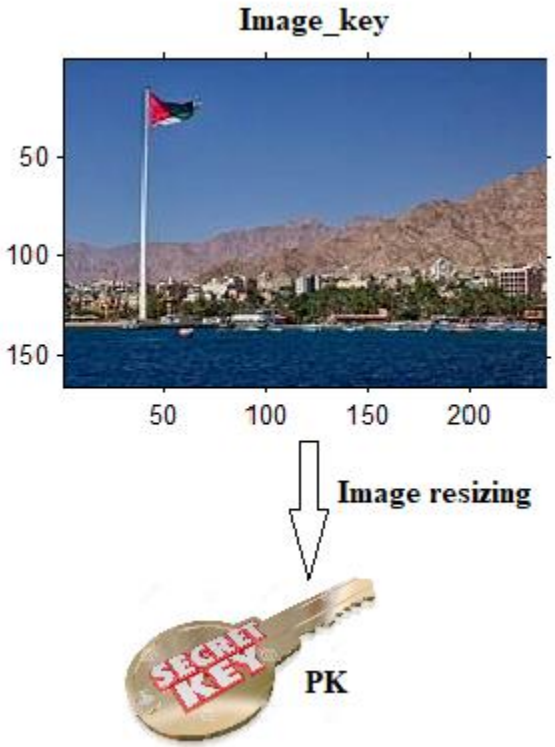

Figure 6: PK generation

The process of hacking the key image is a very difficult or impossible process for the following reasons:

- The large image size, which makes the process of guessing the image is difficult.
- Images are kept secretly and are not sent via various means of communication.
- Use one of the three color arrays to generate the private key and this must be specified by the sender in agreement with the receiver.
- The possibility of changing the image easily without affecting the proposed method and at any appropriate moment.
- The size of the block in the image to be encrypted is also secret.
- The size and contents of the private key depend on the key image and on the block size.

Below is the proposed algorithm of image encryption phase:

Inputs:

Image to be encrypted (A), Image_key (K), Block size (BS), Color channel (CC) to be used to generate PK.

Outputs:

Encrypted image (E)

Process:

1. *Get the inputs*
2. *Retrieve the size of A*
3. *Reshape A to one row matrix (RA).*
4. *Divide RA into equal blocks using BS.*
5. *Resize CC to BS to generate PK.*
6. *XOR each block with PK.*
7. *Reshape RA back to 3D matrix to get E.*

The decryption algorithm is as follows:

Inputs:

Encrypted (E), Image_key (K), Block size (BS), Color channel (CC) to be used to generate PK.

Outputs:

Decrypted image (D)

Process:

1. *Get the inputs*
2. *Retrieve the size of E*
3. *Reshape E to one row matrix (RE).*
4. *Divide RE into equal blocks using BS.*
5. *Resize CC to BS to generate PK.*
6. *XOR each block with PK.*
7. *Reshape RE back to 3D matrix to get D.*

Implementation and experimental results

The proposed method was implemented using mat lab, the programs were executed using I5 processor with 2,4 MHz and 8 G byte RAM, several various images were used in the implementation process, figure 7 shows the selected used images, where table 1 shows the basic information of these images.

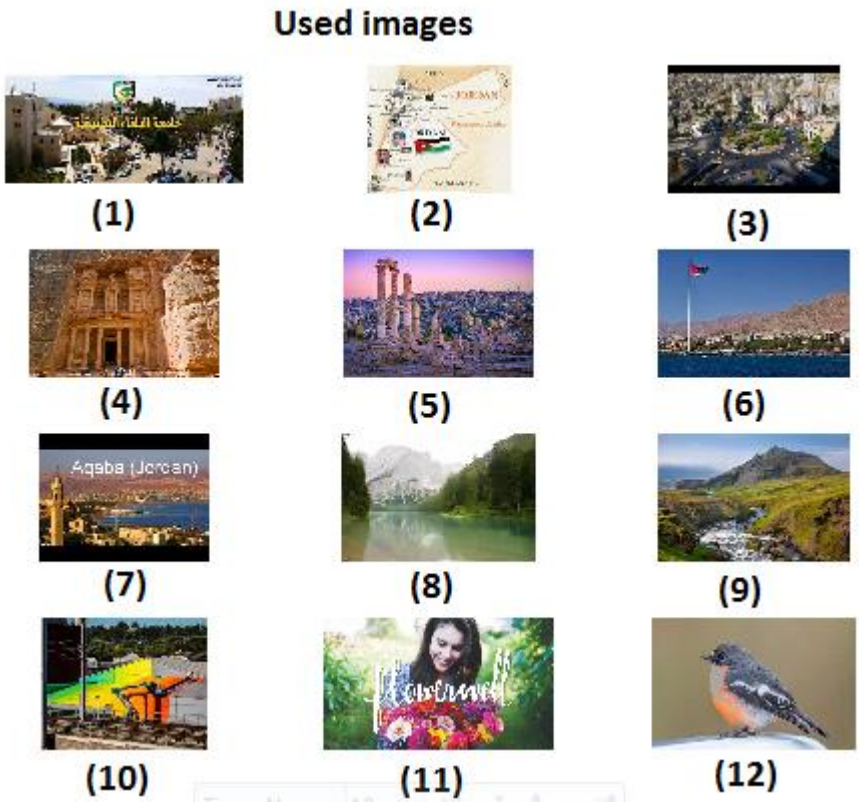

Figure 7: Selected used color images

Table 1: Selected used color images basic information

Image number	Dimension	Size(byte)
1	151 333 3	150849
2	152 171 3	77976
3	360 480 3	518400
4	1071 1600 3	5140800
5	981 1470 3	4326210
6	165 247 3	122265
7	360 480 3	518400
8	183 275 3	150975
9	183 275 3	150975
10	201 251 3	151353
11	600 1050 3	1890000
12	1144 1783 3	6119256

Image 1 was selected as an image to be encrypted, the block size was set to 20 bytes, then each of the other images was selected as an image_key, the results of implementation are shown in table 2, figure 8 shows a sample output:

Table 2: Results of encrypting-decrypting image 1 using BS=20 byte

Image_key number	MSE	PSNR	Encryption time(second)	Throughput(K byte per second)
1	1.1305e+004	17.4956	0.048580	3.0324
2	2.7783e+004	8.5034	0.046919	3.1397
3	4.0831e+003	27.6791	0.049558	2.9725
4	1.4707e+004	14.8646	0.065264	2.2572
5	1.2301e+004	16.6512	0.061683	2.3882
6	4.2726e+003	27.2256	0.049061	3.0027
7	4.5463e+003	26.6046	0.049586	2.9709
8	1.2770e+004	16.2768	0.048616	3.0301
9	6.9311e+003	22.3875	0.047843	3.0791
10	9.0258e+003	19.7468	0.047197	3.1212
11	1.3327e+004	15.8501	0.056798	2.5936
12	1.7109e+004	13.3514	0.067085	2.1959
Average			**0.0532**	**2815.3**

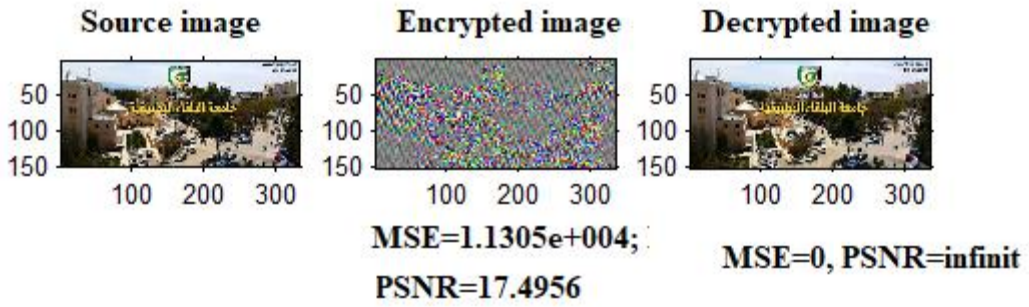

Figure 8: Sample output of encrypting-decrypting image 1

From table 2 we can see that the quality parameters MSE and PSNR have an acceptable values and the proposed method provides a good throughput by minimizing the encryption-decryption time.

Image 1 was selected as an image_key, other images were encrypted using the selected image_key with a block size equal 20 bytes, figure 9 shows a sample output, while table 3 shows the obtained results:

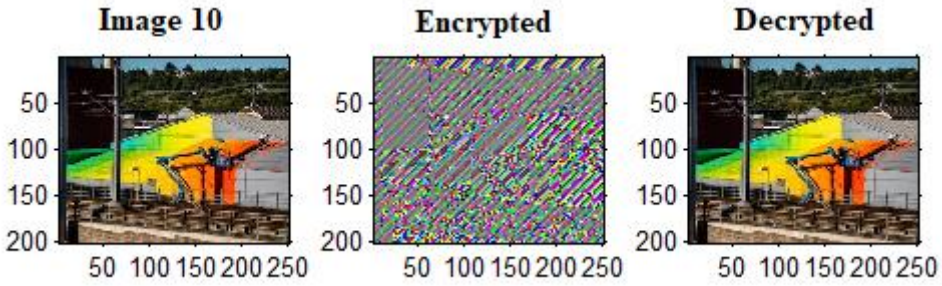

Figure 9: Encrypting-decrypting image 10

Table 3: Images encryption results

Image to encrypt	MSE	PSNR	Encryption time(second)
1	1.1305e+004	17.4956	0.048210
2	1.1718e+004	17.1366	0.040097
3	1.1202e+004	17.5871	0.083969
4	1.0659e+004	18.0838	0.537757
5	1.0632e+004	18.1088	0.455827
6	1.0742e+004	18.0060	0.047533
7	1.2560e+004	16.4423	0.083894
8	1.1352e+004	17.4538	0.047487
9	1.0590e+004	18.1486	0.047679
10	1.1466e+004	17.3537	0.048575
11	1.0738e+004	18.0095	0.226486
12	1.1547e+004	17.2839	0.624856

From table 3 we can see that the proposed method keeps excellent values for MSE and PSNR for all images with various size and the encryption time was very low, this time will slowly increase when the image size increases as shown in figure 10.

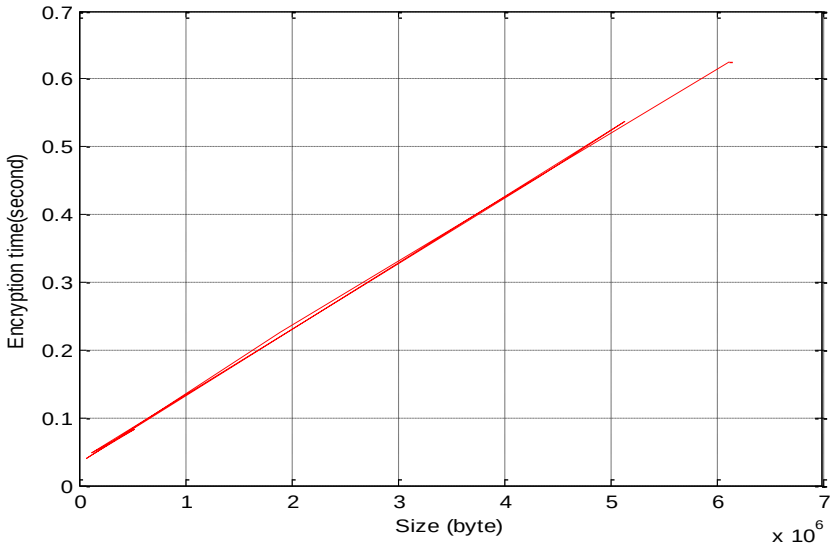

Figure 10: Relationship between image size and encryption time

Image 1 was selected as an image to be encrypted, Image 6 was selected as an image_key, various block sizes were used, table 4 shows the obtained experimental result:

Table 4: Encrypting image 1 using various block size

Block size(byte)	Encryption time(second)	Throughput(byte per second)	Throughput(K byte per second)	Throughput(M byte per second)
10	0.062098	2429200	2372.3	2.3167
20	0.047381	3183700	3109.1	3.0362
30	0.043287	3484900	3403.2	3.3234
40	0.040594	3716000	3628.9	3.5438
50	0.039570	3812200	3722.9	3.6356
60	0.037838	3986700	3893.3	3.8021
70	0.037373	4036300	3941.7	3.8493
80	0.036759	4103700	4007.5	3.9136
90	0.035974	4193300	4095.0	3.9990
100	0.035262	4277900	4177.6	4.0797
Average	0.0416	3722390	3635.2	3.5499

From table 4 we can see that using block with bigger size will decrease the encryption time and thus increase the method throughput as shown in figures 11 and 12.

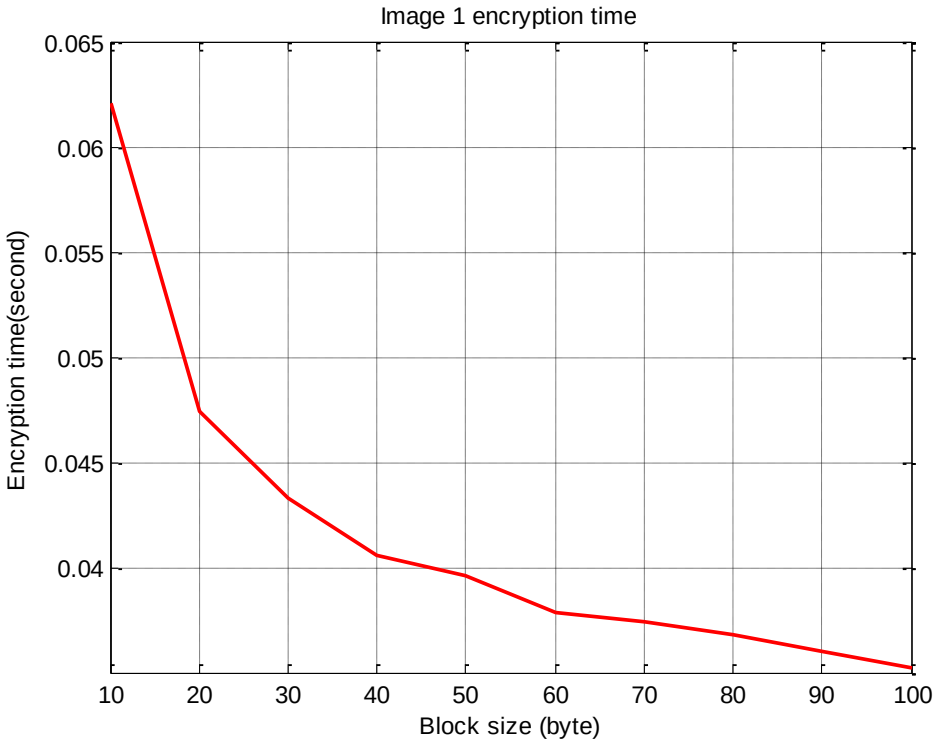

Figure 11: Relationship between block size and encryption time

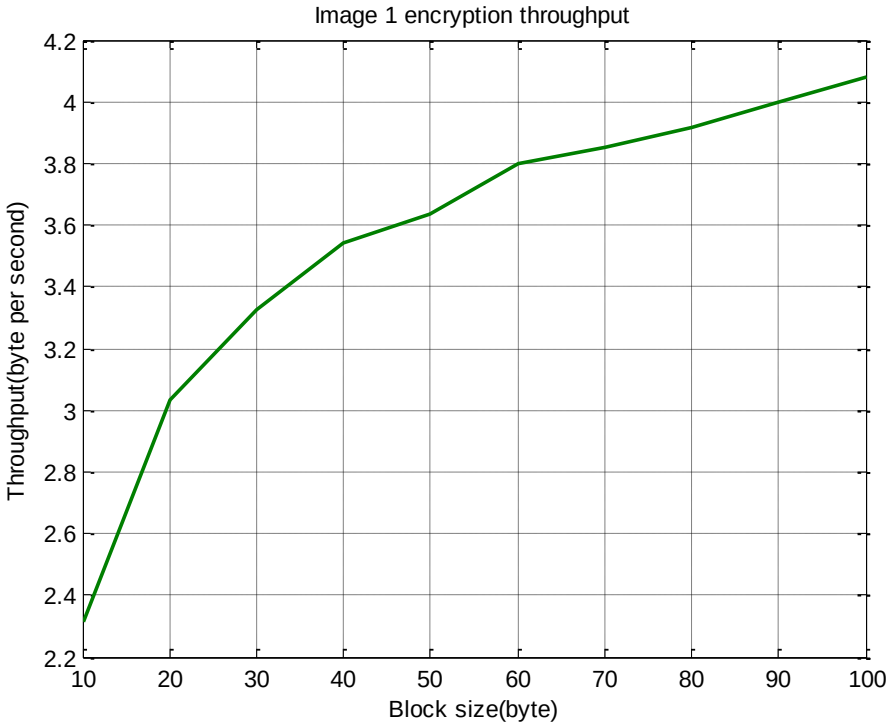

Figure 12 Relationship between block size and throughput

Some images were encrypted-decrypted using the standard methods of data cryptography, the average throughputs were calculated for each of these methods, table 5 shows the final results compared with the average throughput of the proposed method.

TABLE 5: Efficiency comparisons

Method	Average throughput(TP)	Speedup of the proposed method
DES	1356.3	2.6802
3DES	1179.7	3.0815
AES	1465.4	2.4807
BF	2453.7	1.4815
Proposed	3635.2	1.0000
Speedup of the proposed method=TP o the proposed method/TP of other method		

From table 5 we can see that the proposed method has a significant speed up, thus te proposed method will decrease the encryption-decryption time.

Conclusion

A simple and easy to implement method of data cryptography was introduced, tested and implemented. The proposed method provided a high level of security and protection from hacking, this was achieved by using a secret image as an image key, this image must be kept in secret and it can be replaced any time. One channel of the image_key must be used to generate PK. The PK contents depends on the selected image block size, and it changes when the block size changes.

The proposed method gave excellent value for MSE and PSNR during the encryption and decryption phase, the degree of image destruction after the encryption phase was very high and 100 % recovery of the original image was achieved after implementing the decryption phase.

The proposed method provides a high efficiency by reducing the encryption-decryption time and maximizing the throughput, the proposed method has a significant high speedup comparing with the standard method of data cryptography.

References

[1]. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

[2]. W. Stallings, Cryptography and Network Security, 4th Edition, Pearson Prentice Hall, 2006.

[3]. Singh S Preet, Mani Raman, "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.

[4]. Singh Gurjeevan, Kumar Ashwani, Sandha K.S. "A Study of New Trends in Blowfish Algorithm" International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.

[5]. Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[6]. Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

[7]. Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.

[8]. Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206.

[9]. Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[10]. Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[11]. Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis", IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.

[12]. Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Ahmad Sharadqh, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, Vol. 8, Issue. 8, August 2019, pg.50 – 62.

[13]. 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, 2018.

[14]. Akram A. Moustafa and 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 5 (5): 355-362, 2009.

[15]. 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.

[16]. 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.

[17]. 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.

[18]. Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952, 2010.

[19]. Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009.

[20]. 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.

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

[22]. 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.

[23]. Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.

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

[25]. 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.

[26]. H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A alqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology (I.RE.I.T.) Vol. 1, N. 6 ISSN 2281-2911.

[27]. 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, No 5, October 2016.

[28]. Z.A. Alqadi, A. Abu-Jazar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.

[29]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh: A Novel Based On Image Blocking Method to Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization, 2019.

[30]. 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 15th July 2018.

[31]. Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.

[32]. 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 (0975 – 8887). Volume 153 – No2, November 2016.

[33]. Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 76-90.

[34]. Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103.

[35]. Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.

[36]. Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019.

[37]. 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, March- 2019, pg. 14-26.

[38]. 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, (2019)

[39]. B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh, "A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 10, 2018.

[40]. 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(JATIT), Vol.96. No 13, 2018.pp: 4081-4091.

[41]. J. AL-AZZEH, B. ZAHRAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.

[42]. Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.

[43]. Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.

[44]. Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences, vol. 48, issue 12, pp. 177-182, 2022.

[45]. Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.

[46]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022, doi.org/10.3390/sym14040664.

[47]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022, doi.org/10.18280/ts.390117.

[48]. M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6, pp. 685-694, 2021, doi:10.35741/issn.0258-2724.56.6.61.

[49]. M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[50]. M. Abu-Faraj, and Z. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no. 12, pp. 648-656, 2021, doi: 10.22937/IJCSNS.2021.21.12.89.

[51]. M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61.

[52]. M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8.

