Increasing Damages in the Encrypted Color Image

Dr. Ziad A. Alqadi[1] and Hussein N. Hatamleh[2]

[1,2]Albalqa Applied University/Faculty of Engineering

Abstract— Color digital images are used in many important vital applications, and this digital image can be secret or it can be the carrier of highly confidential data that requires protection from the danger of tampering or intruders. Multiple methods are used to protect color digital images, the most important of which are encryption and decryption methods, and many of the methods used depend on standard methods.

Encryption methods based on standard algorithms are used to encrypt text messages and text files that are characterized by their small size, because these methods require a large time to implement the encryption and decryption process, which reduces their efficiency because the size of the digital image is often very large. In this paper, we will discuss a new method for encoding and decoding a digital image. This method will use a secret digital image as a key image that can be kept secretly without resorting to sending it, and it will be agreed upon between the sender and the receiver.

The image uses the key to generate a secret private key of the same size as the image to be encrypted to perform the necessary exclusions for encryption and decryption. In addition to the process of exclusion using the image key, the presented method implements the left-rotation operations for a specified number of digits (to be determined by the sender and in accordance with the receiver) in order to increase the degree of damage attached to the encrypted image to increase its distortion and make it completely incomprehensible.

The proposed method will be implemented using various images, and the practical results of this method will be compared with the results of the standard methods to show the extent to which the quality parameters (MSE, PSNR) and efficiency parameters (Encryption/decryption time, throughput) have been improved.

Keywords— Cryptography, image_key, XORing, nrd, rotate left, MSE, PSNR, throughput.

I. INTRODUCTION

The digital color image [12-17] is one of the most widely used types of data due to its use in various important and vital applications.

The digital image, despite its large size, is characterized by its ease of processing, since it is represented by a three-dimensional matrix, and as shown in the figure1 (one dimension for each color by allocating a two-dimensional matrix for each of the three colors: red, green and blue).[18-23]

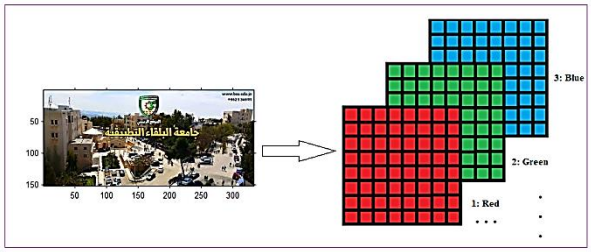

Figure 1: *Color image representation*

The digital image has a large size that depends on its accuracy. The image size is measured in bytes, the number of lines multiplied by the number of columns, multiplied by three, where each byte takes a value ranging from zero to 255, figure 2 shows the images used in this paper, while table 1 shows the basic information of these images [24-30]

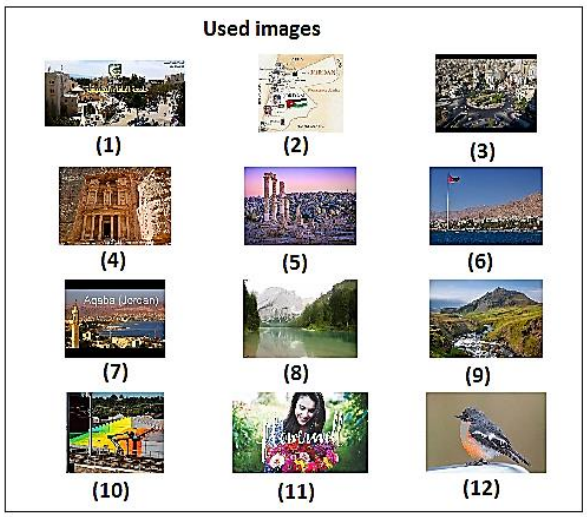

Figure 2: *Used color images*

Table 1: *Used 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

The digital image is characterized by the ease of processing because we are dealing with digital matrices, and a number of easy arithmetic and logical operations are implemented on the digital image, the most important of which are [31-36]:

- Image resizing: Increasing or decreasing the image size as shown in figure 3:

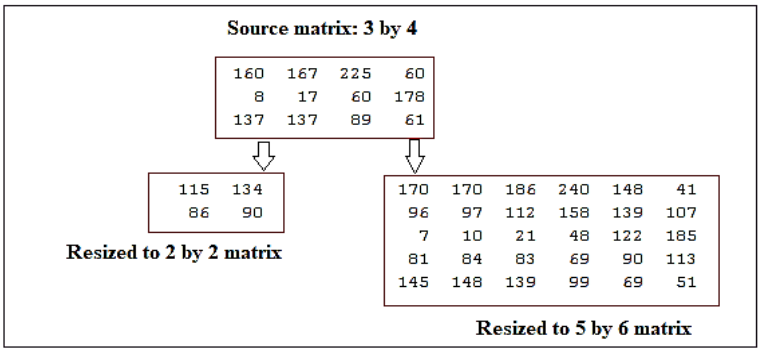

Figure 3: *Image resizing example*

- XORing: this operation is a pixel operation, the resulting image is a results of XORing each pixel in the first image with the associated pixel in the second image, the images must have the same dimension, and here we need image resizing if the images sizes are different as shown in the example illustrated in figure 4:

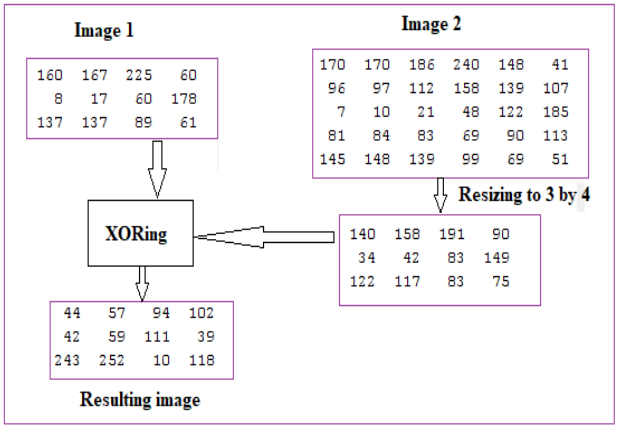

Figure 4: *Image XORing example*

- Pixel rotation left: This logical can be implemented using the binary value of the byte, the number of rotation digits can be determined to get the rotated left number, the same binary number can be retrieved by rotating the resulting binary number (8 – number of digits) times, figure 5 illustrate the rotating left operation, while table 2 shows how to use this operation in the encryption-decryption phases:

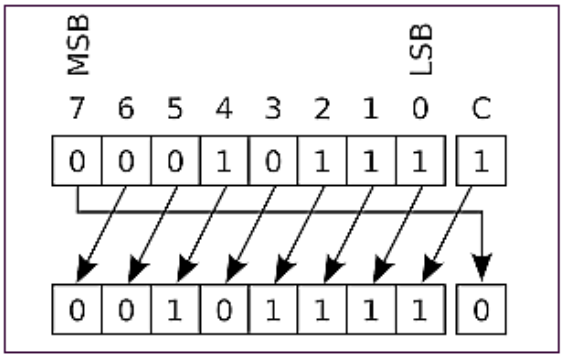

Figure 5: *Rotate left operation*

Table 2: Rotate left operation (a=193 decimal, 11000001 binary)

Encryption			Decryption		
Number of rotation digits	Binary	Decimal	Number of rotation digits	Binary	Decimal
1	10000011	131	7	11000001	193
2	00000111	7	6	11000001	193
3	00001110	14	5	11000001	193
4	00011100	28	4	11000001	193
5	00111000	56	3	11000001	193
6	01110000	112	2	11000001	193
7	11100000	224	1	11000001	193

Cryptography is one of the most important methods used to protect secret data (including color images) from being hacked, and it contains two phases: the encryption and decryption phases [37-44].

The encryption phase is required to destroy the original image completely and making it unuseful for any third person or party (see figure 6). This can be done by using a secret private key and manipulating a sequence of operations using the input image and the PK to generate an encrypted image. The decryption phase is required to recover the same source image identical to the original one without losing any piece of information [50-54]

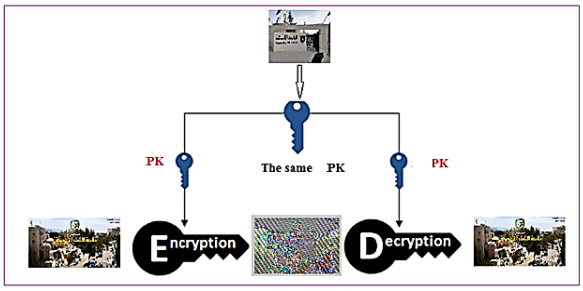

***Figure 6:** Image Cryptography*

The quality of the images can be measured by using mean square error (MSE) and/or peak signal to noise ratio (PSNR), these parameters can be calculated between two images using equations 1 and 2 [45-49].

The MSE represents the cumulative squared error between the denoised and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the

error, and hence the higher quality, and the higher the value of PSNR the higher the quality level, and here the effective filter used to reduce the salt and pepper noise must minimize the value of MSE and at the same time maximize the value of PSNR, and acceptable values for the PSNR are above 50 dB.

MSE of x channel

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

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

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

II. RELATED WORKS

Nowadays, multiple methods of secret data cryptography are used, and the majority of these methods are based on a standard DES (data encryption standard) such 3DES, AES and blowfish (BF) methods [1-5].

The above-mentioned standard methods are similar in the encryption and decryption mechanism. These methods, as indicated in table 3, have the following characteristics:

Table 3: Standard encryption methods features [1-11]

Method parameter	DES	3DES	AES	Blowfish
PK length(bit)	56(fixed)	112, 168(fixed)	128, 192, 256(fixed)	32-448(fixed)
Block size(bit)	64(fixed)	64(fixed)	128(fixed)	64(fixed)
Ability to deal with images	Difficult	Difficult	Difficult	Difficult
Encryption quality	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR

Decryption quality	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR
Efficiency	Slow	Slow	Slow	Moderate
Attack	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack
Structure	Feistel	Feistel	Substitution-Permutation	Feistel
Block cipher	Binary	Binary	Binary	Binary
Rounds	16(fixed)	48(fixed)	10,12,14(fixed)	16(fixed)
Flexibility to modification	no	yes	yes	yes
Simplicity	no	no	no	no
Security level	Adequate	Adequate	Excellent	Excellent
Throughput	Low	low	Low	Moderate

- The use of a single private key with a fixed length that does not change and in some cases can be hacked, and this is a problem that must be eliminated
- Dividing the secret data to be encrypted into blocks of fixed length and this length cannot be changed, and this can be expressed as one of the disadvantages of these methods.
- A fixed and unchangeable number of rounds are used.
- All other sub-private keys used in encryption are generated from the private key using specific arithmetic operations, and this in turn makes the degree of security and protection completely dependent on the private key.
- These methods provide excellent values of MSE and PSNR in both phases: encryption and decryption.
- These methods were designed to encrypt-decrypt secret short messages and confidential text files, using data with big size as color image will drop down the efficiency of data cryptography by requiring much encryption and decryption times.
- These methods require much rounds and this will negatively affect the efficiency. Each round contains a set of operations which will require extra time or execution.
- Generating and manipulating S-box will add an extra execution time, and thus speeding the process of cryptography.

For secret data with large sizes (such as color image) the number of generated blocks will be so big, thus will require extra time for data dividing before encryption and assembling after decryption.

III. THE PROPOSED METHOD

The proposed method required an image_key to generate the PK, this image is to be resized to match the size of the image to be encrypted, the image_key must be kept in secret, also it is required to get the number of bits used to perform the rotate left operation, this number can take the values within the range 1 to 7, when decryption the number of selected digits must be subtracted from 8 as shown in table 2.

The following algorithm describes the encryption phase of the proposed method:

Input:

Image to be encrypted, image_key, number of rotation digits (nrd);

Output:

Encrypted image

Process:

1- *Get: the image to be encrypted (a), image_key, nrd.*
2- *Resize the image_key to match the image (a).*
3- *For each byte in image (a) do the following:*
   a) *Convert the byte to binary.*
   b) *Rotate the byte nrd digits to the left.*
   c) *Convert the results to decimal.*
   d) *XOR the results by the associated byte from the image_key.*
4- *Save the encrypted image.*

The following algorithm describes the decryption phase of the proposed method:

Input:

Encrypted, image_key, number of rotation digits (nrd);

Output:

Decrypted image

Process:

1) *Get: the image to be decrypted (b), image_key, and nrd.*
2) *Resize the image_key to match the image (b).*
3) *For each byte in image (a) do the following:*
    a. *XOR the results by the associated byte from the image_key.*
    b. *Convert the byte to binary.*
    c. *Rotate the byte 8-nrd digits to the left.*
    d. *Convert the results to decimal.*
4) *Save the encrypted image.*

Figures 7 and 8 illustrate an examples o encryption-decryption phases:

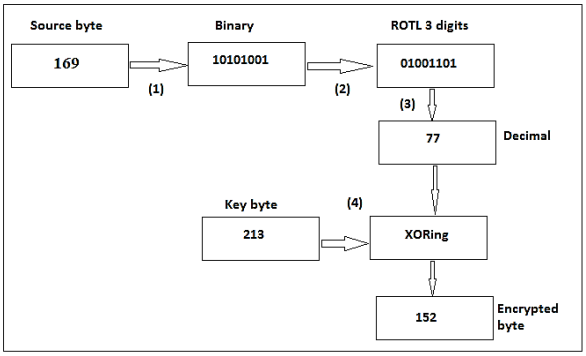

Figure 7: *Encryption example*

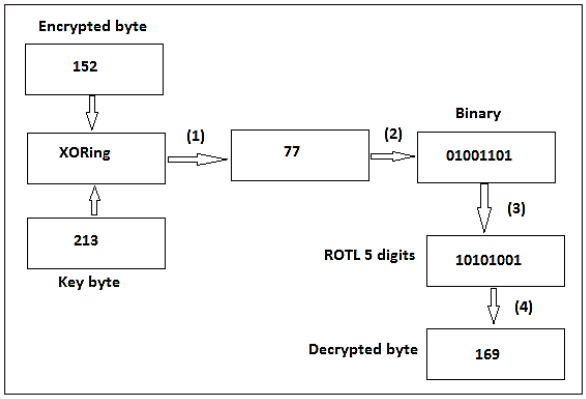

Figure 8: *Decryption example*

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

Images shown in figure 2 were implemented using the proposed method, image 12 was selected as an image_key, figures 9 and 10 show a sample outputs of the implemetation process (nrd=3 in the encryption phase and 5 in the decryption phase).

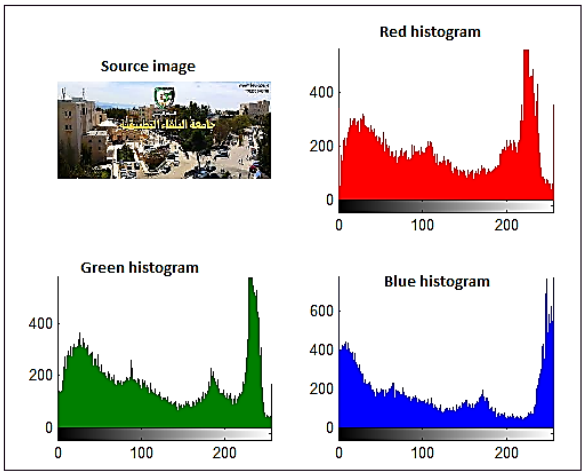

Figure 9: *Source image*

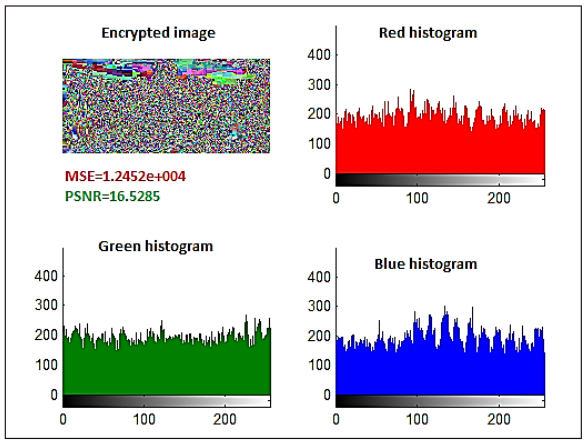

Figure 10: *Decrypted image*

Figure 11 shows how the damage of the image was increased using the proposed method.

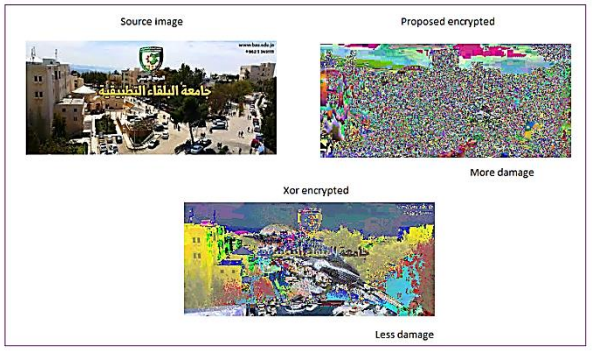

Figure 11: *More image damaging using the proposed method*

The MSE and PSNR values between the source and encrypted images were calculated, table 4 shows the obtained results.

Table 4: *MSE and PSNR results*

Image number	MSE	PSNR
1	11392	17.4187
2	17979	12.8555

3	12287	16.6624
4	95718	19.1595
5	92666	19.4835
6	85898	20.2419
7	13536	15.6941
8	10855	17.9014
9	95820	19.1488
10	11869	17.0082
11	11861	17.0154
12	73535	21.7960

Different values of nrd were used and the obtained values for MSE and PSNR were acceptable for each selected nrd, this is shown in table 5.

Table 5: *PSNR values or different nrd values*

Image	**Rotation digits(encryption: decryption)**						
	1:7	2:6	3:5	4:4	5:3	6:2	7:1
1	15.5476	15.6174	17.4187	16.5285	16.3884	16.5149	16.4511
2	14.6972	13.2535	12.8555	15.4900	15.0289	14.8645	15.0917
3	16.0085	16.8512	16.6624	16.6592	16.8552	17.0525	17.1776
9	20.5262	19.2685	19.1488	19.1648	19.3116	19.2760	18.7113
10	16.8392	16.7052	17.0082	17.0220	16.8612	17.1492	17.3721

The encryption (decryption) time was calculated, table 6 shows the obtained results for time calculations:

Table 6: *Times calculation results*

Image number	**Encryption(decryption) time (second)**	**Throughput (byte per second)**
1	14.876000	10140
2	7.727000	10091
3	52.119000	9946
4	510.657000	10067
5	433.311000	9984
6	12.373000	9882
7	51.550000	10056
8	14.920000	10119
9	14.946000	10101
10	15.035000	10067
11	187.718000	10068
12	607.463000	10073
Average	160.2246	10050

From table 6 we can see that the proposed method is effecient and provides a good throughput with the averag equal 10050 byte per second, increasing the image size will increase the encryption(decryption) time and there is a linear relationship between the image size and the encryption time as shown in figure 12

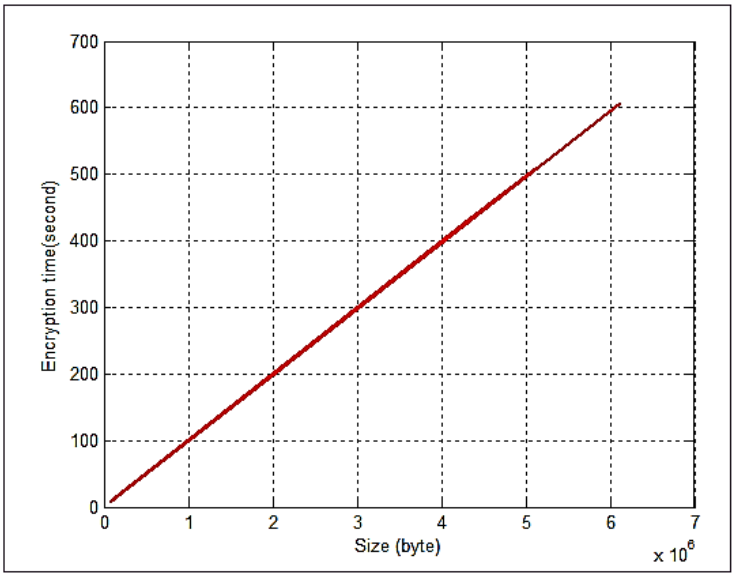

Figure 12: *Relationship between encryption time and image size.*

The used images were encrypted –decrypted using the standard methods of data cryptography, table 7 shows a comparison between the results of the proposed method and the obtained results of standard methods of data cryptography.

Table 7: *Results comparisons*

Image number	Encryption time (second)	DES	3DES	AES	BF
1	14.876000	19.4729	56.6	28.4	16.4557
2	7.727000	10.0658	29.3	14.7	8.5062
3	52.119000	66.9197	194.7	97.4	56.5507
4	510.657000	663.6202	1930.5	966.3	560.7942
5	433.311000	558.4656	1624.6	813.2	471.9330
6	12.373000	15.7831	45.9	0.0230	13.3375
7	51.550000	66.9197	194.7	97.4	56.5507
8	14.920000	19.4892	56.7	28.4	16.4694
9	14.946000	19.4892	56.7	28.4	16.4694
10	15.035000	19.5380	56.8	28.4	16.5106
11	187.718000	243.9780	709.7	355.3	206.1743
12	607.463000	789.9280	2297.9	1150.2	667.5309
Average	160.2246	207.8058	604.5083	300.6769	175.6069

From table 7 we can see that the proposed method provides a highest efficiency by reducing the required time for encryption (decryption) as shown in figure 13, also the proposed method has a good speedup comparing with other methods as show in table 8.

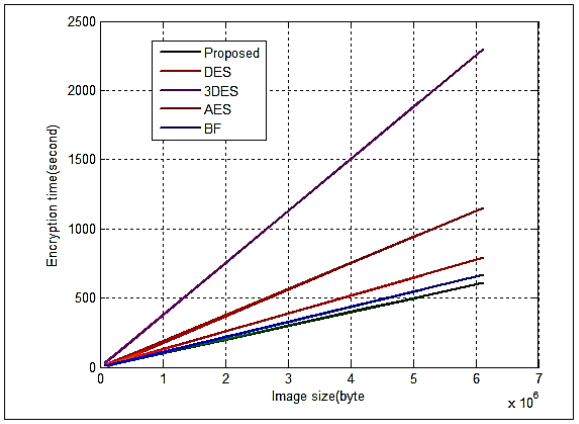

Figure 13: *Encryption times comparisons*

Table 8: *Speedup calculation*

	Proposed	DES	3DES	AES	PF
Proposed	1.0000	1.2970	3.7729	1.8766	1.0960
DES	0.7710	1.0000	2.9090	1.4469	0.8451
3DES	0.2650	0.3438	1.0000	0.4974	0.2905
AES	0.5329	0.6911	2.0105	1.0000	0.5840
BF	0.9124	1.1834	3.4424	1.7122	1.0000

The proposed method added an enhancement to the standard methods of data cryptography as shown in table 9:

Table 9: *Enhancements provided by the proposed method*

Method parameter	DES	3DES	AES	Blowfish	Proposed
PK length(bit)	56(fixed)	112, 168(fixed)	128, 192, 256(fixed)	32-448(fixed)	Variable
Block size(bit)	64(fixed)	64(fixed)	128(fixed)	64(fixed)	Variable
Ability to deal with images	Difficult	Difficult	Difficult	Difficult	Easy

Encryption quality	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR
Decryption quality	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR
Efficiency	Slow	Slow	Slow	Moderate	High
Attack	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack	Very difficult
Structure	Feistel	Feistel	Substitution-Permutation	Feistel	Simple logical operations
Block cipher	Binary	Binary	Binary	Binary	Decimal and binary
Rounds	16(fixed)	48(fixed)	10,12,14(fixed)	16(fixed)	1 round
Flexibility to modification	no	yes	yes	yes	Yes
Simplicity	no	no	no	no	Yes
Security level	Adequate	Adequate	Excellent	Excellent	Excellent
Throughput	Low	low	Low	Moderate	High

V. CONCLUSION

A new and easy-to-implement method has been introduced to encrypt and decrypt color digital images in order to provide the necessary protection for digital images and prevent the penetration of these images.
The ease of implementation lies in the simplicity of the operations used, which were limited to logical rotations and exclusions. The proposed method provides a very high degree of protection for digital images, through the use of another digital image that is used as a private key that is kept secretly by the sender and receiver, which is used to carry out the exclusion process. In addition, the number of left rotation digits is also confidential. Referring to the practical results that were obtained after implementing the proposed method on a set of color images, we found that the use of this method leads to an increase in the percentage of destruction and distortion in the encrypted image, while maintaining excellent values for both MSE and PSNR.

The encryption and decoding time of the proposed method was calculated and the results were compared with the results of the standard methods. It was found that the proposed method increases the efficiency of the encryption and decryption process by reducing the time of encryption and decryption. The proposed method has achieved a remarkable speedup value. The proposed method is flexible due to the ease of replacing the key image and the ease of changing the number of left-rotation digits.

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] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 648-656, 2021.

[47] Ziad Alqadi Mua'ad Abu-Faraj , Khaled Aldebei, DEEP MACHINE LEARNING TO ENHANCE ANN PERFORMANCE: FINGERPRINT CLASSIFIER CASE STUDY, JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, vol. 56, issue 6, pp. 686-694, 2021.

[48] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 451-458, 2021.

[49] Mua'ad M. Abu-Faraj Prof. Ziad Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, International Journal of Computer Science and Network Security, vol. 20, issue 11, pp. 53-60, 2021.

[50] 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.

[51] 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.

[52] Ziad A Alqadi, Mohamad Tariq Barakat, A Case Study to Improve the Quality of Median Filter, International Journal of Computer Science and Mobile Computing, vol. 10, issue 11, pp. 19 – 28, 2021.

[53] Dr. Hatim Ghazi Zaini Prof. Ziad Alqadi, High Salt and Pepper Noise Ratio Reduction, International Journal of Computer Science and Mobile Computing, vol. 10, issue 9, pp. 88 – 97, 2021.

[54] Prof. Mohamad K. Abu Zalata, Hussein N. Hatamleh, Prof. Ziad A. Alqadi, Detailed Study of Low Density Salt and Pepper Noise Removal from Digital Color Images, IJCSMC, Vol. 11, Issue. 2, PP. 56 – 67, February 2022.