An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images

Majed O. Al-Dwairi
Department of Communication Technology Engineering, Faculty of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan
majeddw@bau.edu.jo

Amjad Y. Hendi
Department of Communication Technology Engineering, Faculty of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan
amjad_svyaz@yahoo.com

Ziad A. AlQadi
Computer & Network Engineering Department, Faculty of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan
natalia_maw@yahoo.com

***Abstract*—Digital color images are considered as the most widely used data. They are exchanged frequently on the internet and via email, so an efficient and highly secure method of color image encryption and decryption is needed. Different methods of encryption-decryption are used, but most of them suffer from low efficiency or low-security level or both. In this paper, an efficient and highly secure method of encryption-decryption will be proposed, tested, and implemented. The efficiency parameters will be calculated and compared with other methods' parameters to prove the efficiency of the proposed method.**

Keywords-encryption-decryption times; throughput; speedup; MSE; PSNR

I. INTRODUCTION

Digital images are one of the most widely used data types, and they are exchanged widely through e-mail and web browsing. A digital image may be confidential or contain highly confidential information [1]. In this case, it is necessary to encrypt it in order to make it difficult to identify or the information stored in it. The person authorized to view the image can decrypt it and return it to the original form without any errors. The digital image has a large size, so encoding it may take a lot of time, which leads us to build an effective method that reduces the encryption time as much as possible.

II. ENCRYPTION-DECRYPTION PARAMETERS

Regarding the effectiveness of the image encryption method, the following parameters must be taken into account:

- Encryption time: the time needed to process the encryption method in order to convert the original image to an encrypted image.
- Decryption time: the time needed to process the decryption method in order to convert the encrypted image to the original image. Encryption and decryption times must be as reduced as possible.
- Throughput: the number of bits encrypted or decrypted per time unit. It is equal to the image size in bits divided by the encryption or decryption time.
- Speedup: the proposed technique enhancement, which is equal with the proposed technique throughput divided by the throughput of another method.
- Block: the number of bytes to be encrypted/decrypted at the same moment.
- Key size: the number of values (elements) for a secret key, which must be equal with the block size.
- Hacking time: the time needed by an unauthorized person to guess the original image. This time must be as large as possible. This time depends on the length of the key used for encryption-decryption.
- Mean square error (MSE) and peak signal-to-noise ratio (PSNR): MSE is a measure of the quality of an estimator—it is always non-negative, and values closer to zero are better. But for measuring it between the original image and the encrypted one, the value must be very large. PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. For ideal encryption, the PSNR between the original image and the encrypted image must be very low, and between the original image and the decrypted one must be infinite (zero errors). These parameters can be calculated using the following formulas:

$$MSE = \sum_i^r \sum_j^c \sum_k^p \left(X(i,j,k) - Y(i,j,k)\right)^2 \quad (1)$$

$$d=max\{Xi,j,k,Yi,j,k\}, PSNR = 10log\left({d^2}/{MSE}\right) \quad (2)$$

where X and Y are color image matrices, r: rows, c: columns, p: number of colors.

III. RELATED WORK

Some authors take data encryption standard (DES) [2], or advanced encryption standard (AES) [3, 4] as bases for encryption-decryption, but most of these works suffer from high encryption-decryption time, which makes these methods inefficient. Author in [5] suggested a method of encryption-decryption by reshaping the 3D color matrix to a 2D matrix, squaring the matrix, generating a secret key with size equal to

Corresponding author: Majed O. Al-Dwairi

the image size, and applying matrix multiplication to get the decrypted image. This method provides a good throughput, but it is very difficult to remember the key, and thus the method requires storing and transferring the key. In [6] an efficient image encryption scheme using double logistic maps was proposed, in which the image matrix was confused from row and column. Confusion effect is carried out by the substitution stage and Chen's system is employed to diffuse the gray value distribution. In [7], a method of encryption-decryption was proposed, this method was based on matrix reordering and it has a medium throughput. In [8], a chaotic algorithm was presented applying encryption-decryption by using power and tangent functions instead of linear function. The process of encryption is one-time-one-password system and is more secure (but not enough) than the DES algorithm, also it has low efficient parameters with big encryption-decryption time and low throughput. In [9], an asymmetric image encryption-decryption method was proposed, this method is based on matrix transformation, but it has high encryption-decryption time and thus low throughput. In [10] a method based on Rubik's cube principle was proposed with a good security level, but low throughput. In [11] a method of encryption-decryption was presented, this method is based on using chaos-controlled poker shuffle operation, both variants of this method (A-I and A-II) have a poor throughput.

IV. PROPOSED METHOD

The proposed technique of color image encryption-decryption requires the following operations (Figure 1):

- Dividing the original image matrix into equal size blocks (in our testing experiment the block size was equal to 8 bytes).
- Selecting several secret keys (in our testing experiment we selected 4 keys).
- Key size must equal block size.
- Key value must in the range from 0 to 255.

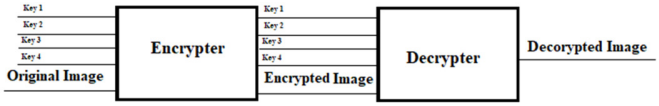


Fig. 1. Proposed encryptor-decryptor

The encryption phase can be implemented applying the following steps:

- Get the original color image matrix.
- Reshape the color image matrix from 3D to 1D.
- Divide the 1D matrix into equal blocks with size equal to 8 bytes.
- Define 4 private keys with 8 elements each.
- Each data matrix block must be submitted to exclusive-OR operation with key1, key2, key3, and key4 consecutively.
- The obtained blocks are the encrypted blocks.

The decryption phase can be implemented applying the following steps:

- Get the encrypted color image matrix.
- Reshape the color image matrix from 3D to 1D.
- Divide the 1D matrix into equal blocks with size equal to 8 bytes.
- Use the defined 4 private keys with 8 elements each.
- Each data block be submitted to exclusive-OR with key4, key3, key 2, and key1 consecutively.
- The obtained blocks are the decrypted blocks which must be reshaped back to get the decrypted image.

The proposed algorithm provides a high level of security, the number of combinations to guess the four keys is very high and equal to $256^8 \times 256^8 \times 256^8 \times 256^8 = 256^{32}$ making the hacking process very difficult. Figure 2 shows an example of the keys, while Figures 3-5 show the original, encrypted and decrypted images obtained by applying the proposed method. From Figures 4 and 5 we can see that the original and decrypted images are the same.

55	166	13	58	170	79	78	184
243	33	17	32	42	232	35	157
69	56	182	140	240	84	180	241
148	224	191	97	185	42	244	50

Fig. 2. Keys example

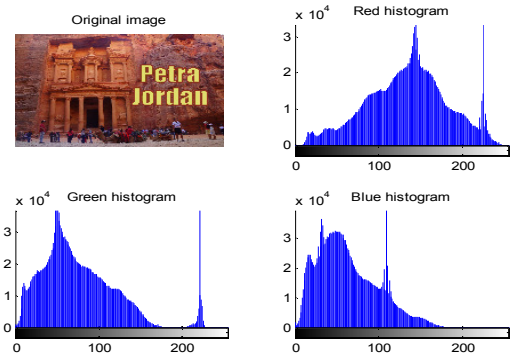


Fig. 3. Original image and histograms

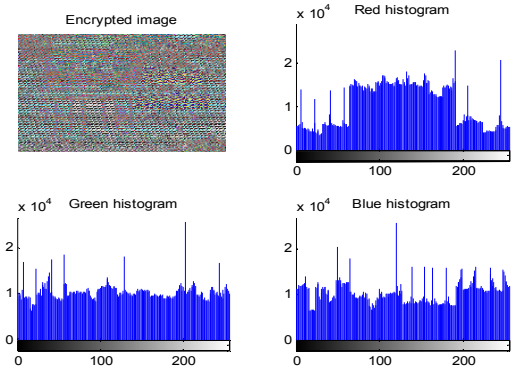


Fig. 4. Encrypted image and histograms

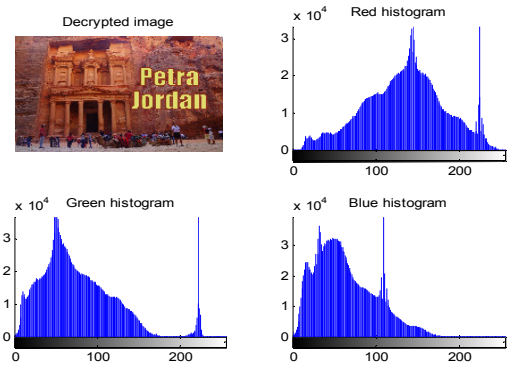


Fig. 5. Decrypted image and histograms

V. RESULTS AND DISCUSSION

The proposed method can be used to encrypt-decrypt color images of any type or size. Several images were treated by the proposed technique, and Table I shows the results of the implementation. From Table I we can conclude the following:

- Calculated encryption/decryption times are significantly small and grow linearly (as shown in Figure 6) when the image size grows.
- The proposed technique is accurate by keeping the decrypted image the same with the original image (zero MSE and infinite PSNR).
- The proposed technique distorts the encrypted image by maximizing MSE and minimizing PSNR between the original image and the encrypted one.
- The throughput of the proposed technique is always between 28 and 29 MBits per second, which is considered a high-performance index.

TABLE I. CALCULATED PARAMETERS

Image number	Size (Mbits)	Encryption time (s)	Decryption time (s)	Throughput (Mbps)
1	2.0672	0.0710	0.0710	29.1151
2	1.1587	0.0410	0.0410	28.2613
3	0.3750	0.0130	0.0130	28.8462
4	8.5876	0.2940	0.2940	29.2097
5	4.1199	0.1410	0.1410	29.2190
6	25.9100	0.8930	0.8930	29.0145
7	18	0.628000	0.628000	28.6624
8	7.0862	0.2470	0.2470	28.6890
9	3.2959	0.1150	0.1150	28.6600
10	1.1547	0.0390	0.0390	29.6085

To prove the correctness of the proposed technique, MSE and PSNR were calculated (Table II). The proposed technique was compared with other existing techniques and the results of the comparison are shown in Table III. From these results we can see that the proposed technique enhanced efficiency by minimizing encryption-decryption times, and maximizing throughput which speeds up the proposed technique. Note that increasing the block size will increase the technique efficiency by decreasing the encryption-decryption time and increasing the throughput.

TABLE II. MSE AND PSNR CALCULATIONS

Image number	Comparing encrypted image with original		Comparing decrypted image with original	
	MSE	PSNR	MSE	PSNR
1	1.6997e+004	13.4173	0	Infinite
2	7.8742e+003	21.1118	0	Infinite
3	6.0695e+003	23.7150	0	Infinite
4	7.7992e+003	21.2075	0	Infinite
5	1.1871e+004	17.0068	0	Infinite
6	1.4770e+004	14.8217	0	Infinite
7	1.3579e+004	15.6623	0	Infinite
8	1.3214e+004	15.9352	0	Infinite
9	1.0662e+004	18.0805	0	Infinite
10	1.2664e+004	16.3601	0	Infinite

TABLE III. COMPARISON RESULTS

Method	Encryption time (s)	Decryption time (s)	Throughput (Mbits)	Speedup of the proposed method	Order
Proposed	0.0513	0.0513	29.2398	1	1
[4]	0.06469	0.062727	23.1876	1.2610	2
[6]	0.23	0.23	6.5217	4.4835	4
[7]	0.5	0.5	3	9.7466	6
[8]	0.4	0.4	3.7500	7.7973	5
[9]	0.12	0.12	12.5000	2.3392	3
[10] v. A-I	0.56	0.56	2.6786	10.9161	7
[10] v. A-II	1.01	1.01	1.4852	19.6874	8

Image size=256×256×3×8=1572864bit=1.5000Mbits

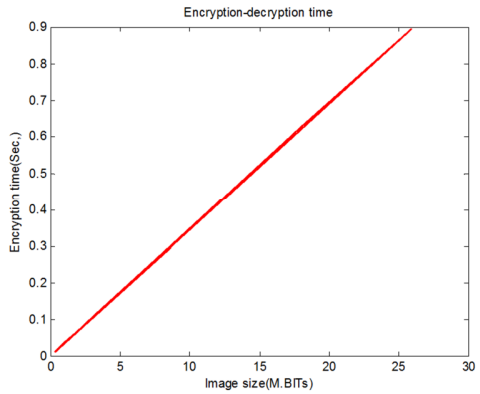


Fig. 6. Relationship between image size and encryption time

The proposed technique was implemented using the previous images with a block size equal to 16 pixels and with one 16 element key, the results of the implementation are shown in Tables IV-V.

TABLE IV. PARAMETERS FOR BLOCK SIZE =16, ONE KEY

Image number	Size (Mbits)	Encryption time (s)	Decryption time (s)	Throughput (Mbps)
1	2.0672	0.0290	0.0290	71.2817
2	1.1587	0.0170	0.0170	68.1597
3	0.3750	0.0050	0.0050	75.0000
4	8.5876	0.1250	0.1250	68.7012
5	4.1199	0.0560	0.0560	73.5692
6	25.9100	0.3670	0.3670	70.5993
7	18	0.2540	0.2540	70.8661
8	7.0862	0.1010	0.1010	70.1602
9	3.2959	0.0470	0.0470	70.1255
10	1.1547	0.0160	0.0160	72.1707

Here the technique efficiency was rapidly increased but with some negative effects by increasing the PSNR between the original and the encrypted image, which means that the encrypted image moves toward the original image. However, this level of PSNR is still acceptable. Table VI shows the efficiency speedup of increased block size.

TABLE V. MSE AND PSNR FOR BLOCK SIZE =16 AND ONE KEY

Image number	Comparing encrypted image with original		Comparing decrypted image with original	
	MSE	PSNR	MSE	PSNR
1	9.1362e+003	19.6253	0	Infinite
2	7.4460e+003	21.6710	0	Infinite
3	7.3327e+003	21.8243	0	Infinite
4	7.5590e+003	21.5203	0	Infinite
5	8.6746e+003	20.1437	0	Infinite
6	8.5122e+003	20.3327	0	Infinite
7	8.7733e+003	20.0305	0	Infinite
8	8.1958e+003	20.7116	0	Infinite
9	7.7113e+003	21.3209	0	Infinite
10	7.3976e+003	21.7362	0	Infinite

TABLE VI. SPEEDUP WITH INCREASED BLOCK SIZE

Image number	Throughput (Mbps)		Speed up of (2)
	Block size=8 Number of keys=4 (1)	Block size=16 Number of keys=1 (2)	
1	29.1151	71.2817	2.4483
2	28.2613	68.1597	2.4118
3	28.8462	75.0000	2.6000
4	29.2097	68.7012	2.3520
5	29.2190	73.5692	2.5179
6	29.0145	70.5993	2.4332
7	28.6624	70.8661	2.4724
8	28.6890	70.1602	2.4455
9	28.6600	70.1255	2.4468
10	29.6085	72.1707	2.4375

VI. CONCLUSIONS

An efficient and highly secure technique for color image encryption-decryption was proposed. The proposed technique was implemented and tested, and the experimental results showed the following conclusions:

- The proposed technique is very efficient by increasing the throughput and decreasing encryption-decryption times.
- The proposed technique is 100% accurate by achieving zero MSE and infinite PSNR between the original image and the decrypted one.

REFERENCES

[1] M. J. Aqel, Z. AlQadi, A. A. Abdullah, "RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication", International Journal of Engineering and Technology, Vol. 7, No. 3.13, pp. 104-107, 2018

[2] J. Thakur, N. Kumar, "DES, AES, and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol. 1, No. 2, pp. 6-12, 2011

[3] S. A. M. Rizvi, S. Z. Hussain, N. Wadhwa, "A Comparative Study of Two Symmetric Encryption Algorithms across Different Platforms", International Conference on Security and Management, World Academy of Science, Las Vegas, USA, July 18-21, 2011

[4] S. Wang, Y. Zheng, Z. Gao, "A New Image Scrambling Method through Folding Transform", IEEE International Conference on Computer Application and System Modeling, Taiyuan, China, October 22-24, 2010

[5] J. N. Abdel-Jalil, "Performance analysis of color image encryption\decryption techniques", International Journal of Advanced Computer Technology, Vol. 5, No. 4, pp. 13-17, 2016

[6] G. Ye, "An Efficient Image Encryption Scheme based on Logistic maps", International Journal of Pure and Applied Mathematics, Vol. 55, No. 1, pp. 37-47, 2009

[7] T. Sivakumar, R. Venkatesan, "A Novel Image Encryption Approach using Matrix Reordering", WSEAS Transactions on Computers, Vol. 12, No. 11, pp. 407-418, 2013

[8] H. Gao, Y. Zhang, S. Liang, D. Li, "A New Chaotic Algorithm for Image Encryption", Chaos, Solitons & Fractals, Vol. 29, No. 2, pp. 393-399, 2006

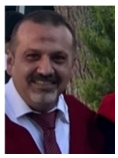
[9] G. Chen, Y. Mao, C. K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", Chaos, Solitons & Fractals, Vol. 21, No. 3, pp. 749–761, 2004

[10] K. Loukhaoukha, J. Y. Chouinard, A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, Vol. 2012, Article ID 173931, pp. pp. 1-13, 2012

[11] X. Wang, J. Zhang, "An Image Scrambling Encryption using Chaos-controlled Poker Shuffle Operation", IEEE International Symposium on Biometrics and Security Technologies, Islamabad, Pakistan, April 23-24, 2008

AUTHORS PROFILE

Majed O. Al-Dwairi, PhD in Communication Systems. He was born in 1968 in Jordan. He received his Diploma Degree in 1994 and his PhD degree from Ukraine state Academy in 1998 in the field of Multichannel Communication. An associate professor in the Department of Communication Engineering Technology, Faculty of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan. His research interests include optical communication networks, digital communications, signal and image processing, Antenna design, and microstrip patch antennas.



Amjad Y. Hendi, PhD in Radio and TV Systems. He received his Diploma Degree in 1994 and PhD Degree from the Ukraine state Academy in 1998 in the field of Radio & TV systems. His research interests include digital communications, signal and image processing, antenna design, optimization techniques in antenna design, and antenna measurement techniques and microstrip patch antennas.

Ziad A. AlQadi, PhD in Computer Engineering. He was born in 1955 in Jordan. He received his Diploma Degree in 1980 and PhD Degree from Ukraine in 1986 in the field of Computer Engineering. Currently he is a Professor at the Computer Engineering Department, Faculty of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan.