IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 40, No. 1, February, 2023, pp. 235-240
Journal homepage: http://iieta.org/journals/ts

Efficient Method to Message-Image Cryptography Using Reordered Image-Key

Rashad J. Rasras[1*], Mutaz Rasmi Abu Sara[2], Ziad Alqadi[1]

[1] Department of Electrical Engineering, Al-Balqa' Applied University, Amman 11134, P.O. Box 15008, Jordan
[2] Faculty of Engineering and Information Technology, IT Department, Palestine Ahliya University, Bethlehem 1041, Palestine

Corresponding Author Email: rashad.rasras@bau.edu.jo

https://doi.org/10.18280/ts.400122

Received: 19 September 2022
Accepted: 30 January 2023

Keywords:
cryptography, flipping, image_key, MSE, PSNR, resizing

ABSTRACT

Color image may be secret or holding secret data, also secret messages may be so confidential. To protect these data, we have to use a simple and efficient method. In this research a method of data encryption-decryption will be presented. The suggested method will use a complicated PK to apply image encryption/decryption using XORing operation, the used image key will be reordered using a secret ordering sequence. Any modifications made to the PK during the decryption process will be regarded as a hacking attempt and result in corrupted decrypted data; hence, the encryption and decryption processes must employ the same secret information. The PK will provide an enormous key space that could resist any type of hacking attempts. The suggested method will be tested and the obtained results will be compared with those of DES and AES, the throughputs and speedup will be calculated. It will be shown how easily we can use encrypt decrypt color images with any size using a fix image key, and it will be shown how the suggested method maintain desirable values of MSE and PSNR parameters.

1. INTRODUCTION

The process of encrypting and decrypting data [1, 2] is an important process in order to protect confidential text messages or protect digital images from tampering with intruders by not enabling them to understand confidential data [3, 4].

Most encryption operations depend on the use of a private secret key [5-7], as this key is used in the process of executing some specific operations on the secret data to generate destructive and incomprehensible data [8, 9] as shown in the Figure 1. In order to generate data that is similar to the original secret data without ever losing any data or any part of it, the decryption process is carried out using the specified operations on the secret key and the encrypted data [10-12].

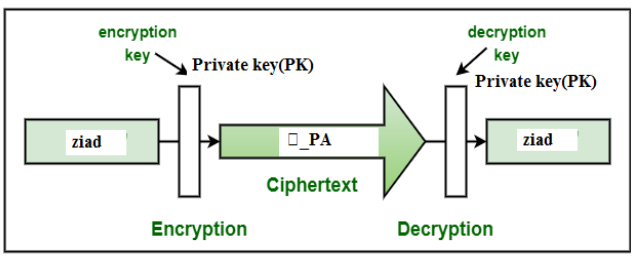

Figure 1. Encryption-decryption process

Confidential data is circulated, whether short messages, long messages or digital images that could be a personal nature or carry sensitive data through many different social media, which calls for preventing third parties from accessing and viewing this data [13-15].

The majority of the approaches used today to protect sensitive data are based on DES and AES standard methods. Although DES is fast to encrypt and decrypt data, it lacks security due to the short length of the used public key, which makes it susceptible to hacking by outside attackers. The U.S. government selected AES as its symmetric block cipher because it was designed to be easy to implement in hardware and software, as well as in limited environments, and to give strong protections against a variety of attack.

Jose et al. [16-18] introduced steganography methods of data hiding and extracting based on the least significant bit (LSB)] [17, 18]. The LSB technique was modified, and improved, to increase its level of protection [19]. LSB is an unsecure method of hiding secret messages, and the process of data hiding can be implemented by reserving 8 bytes of the holding image to store one character of the message. LSB requires the binary code of the character, and each bit of this code can be inserted in the least bit of the selected byte of the holding image. The benefits of using LSB-based approaches are low MSE and high PSNR [20], which make changes in the holding image difficult for the human eye to notice.

Sivakumar and Venkatesan [21] suggested matrix reordering based method of color image encryption - decryption with an average throughput. The security level and efficiency parameters of this method were increased, but a large amount of memory space was needed for the private secret key due to its size and complexity. Gao et al. [22] suggested method of image encryption on the base of a chaotic algorithm using the power and tangent functions rather than linear functions. In this method One-time-one-password encryption is used, which is more secure than the DES algorithm (although not secure enough). Additionally, it includes inefficient parameters that lead to slow encryption-decryption process and low performance. Asymmetric color image encryption-decryption was realized using a matrix transformation; however, the throughput was low due to the

long encryption-decryption processes [23]. A method of image encryption method based on matrix decompositions is suggested, where the order and rank of the deconstructed components serve as unique key parameters [24]. Wang and Zhang [25] suggested a chaos-controlled poker shuffle operation based method of color image encryption-decryption. The drawback of both versions of this method was its poor throughput.

Accordingly, any method can be adopted, provided that the following requirements are met:

- ✓ In order to give a high level of data confidentiality and protection the suggested technique must employ secret key that is hard for hackers to penetrate [26].
- ✓ The quality factors values must be acceptable. MSE and PSNR are factors that are used to evaluate the quality of suggested method (see Eqns. (1) and (2)). If the data was destructed then the calculated value of MSE for the original and encrypted data must be very high, whereas PSNR should be very low (see Table 1). Calculated value of MSE for original and decrypted data should equal zero, whereas PSNR must be infinite [27, 28].
- ✓ The suggested method must be effective by reducing encryption decryption times and increasing method throughput. (bytes manipulated in second) [29-31].
- ✓ The suggested method should be easy to implement.

MSE between S and R, n: message length

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

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

Table 1. Quality factors

	Original		Encrypted		Decrypted	
	MSE	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**
Original	-	-	High	Low	Zero	Infinite
Encrypted	High	Low	-	-	High	Low
Decrypted	Zero	Infinite	High	Low	-	-

Digital color image is huge incubator of data, it represents a set of three bytes, where each of byte carries the information about the red, green and blue colors (RGB), producing a total of 24 bits per pixel in the source imager. So the image may be represented by 3 dimensions for red, green, and blue as illustrated in Figure 2.

The color image may be easily employed as PK, this key is simple to manipulate. The key preprocessing in this research will focus on image flipping and image resizing, these operations are explained in the Figures 3, 4, and 5.

In our proposed method we will use the reordering sequence, this sequence contains 3 parameters with values 1 or 2, 1 means that the color matrix flipped row-wise down, 2 means the color matrix is flipped column wise left to right (for example the sequence 1 2 2 means: red color is flipped row-wise, green color is flipped column wise, blue color is flipped column wise, Figure 6 shows how a color image is reordered using the sequence.

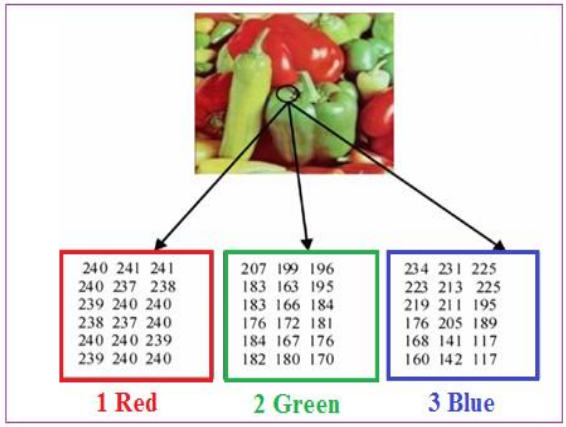

Figure 2. Color image representation

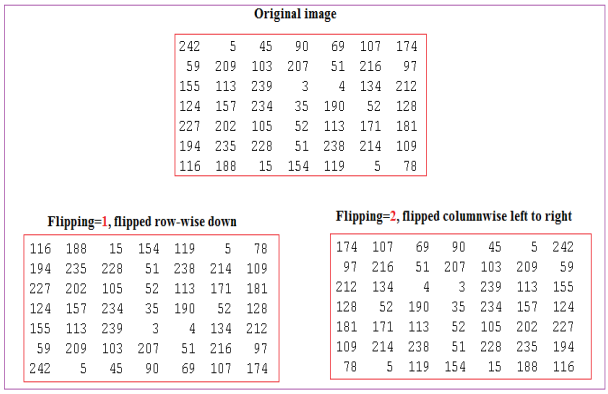

Figure 3. Image flipping

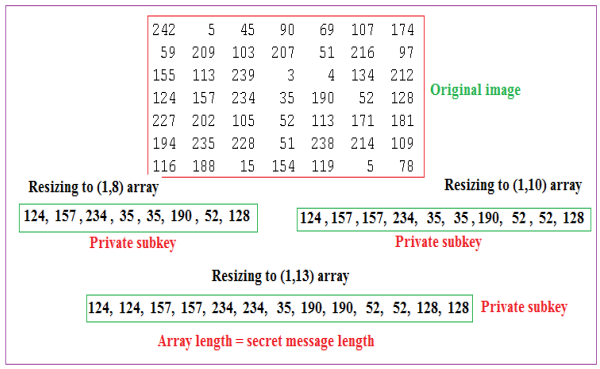

Figure 4. Image resizing to meet the message length

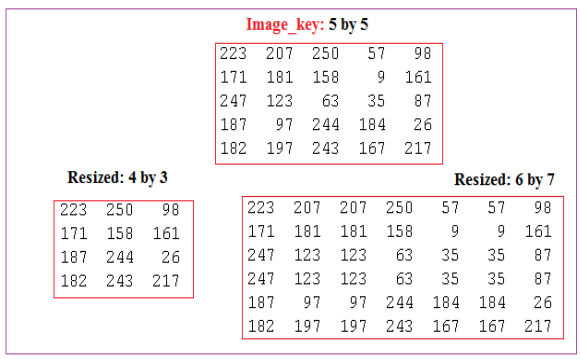

Figure 5. Image resizing to meet another message size

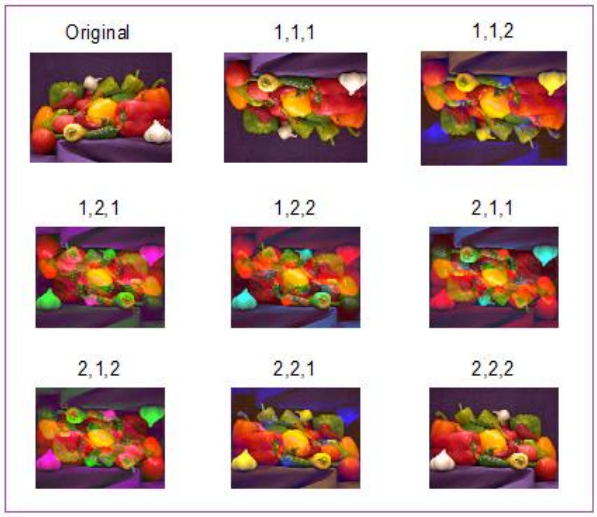

Figure 6. Using reordering sequence

2. THE NEW SUGGESTED METHOD

The new suggested method provides a special PK which includes the image-key (which must be kept confidential and without transmission) and the reordering sequence, By using this PK we can apply encryption process as shown in Figure 7, and decryption process as shown in Figure 8:

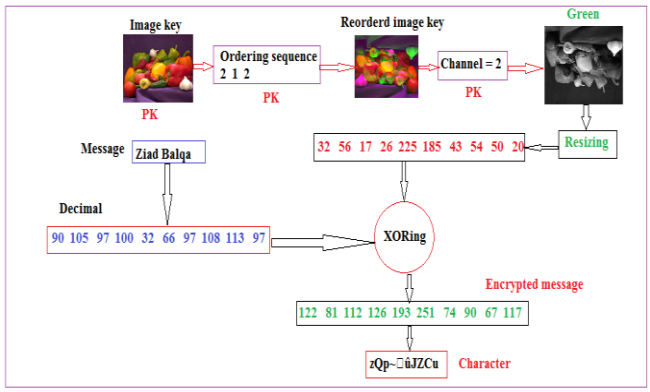

Figure 7. Proposed encryption phase

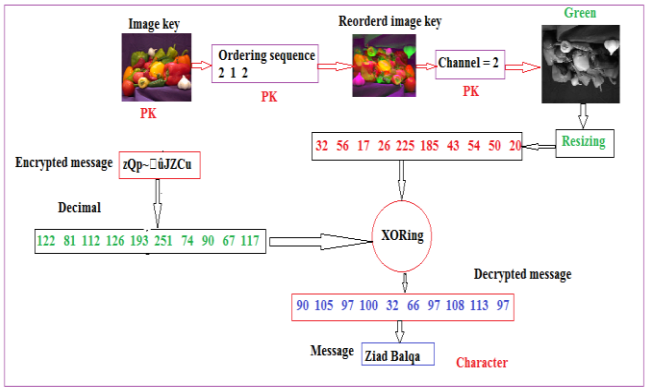

Figure 8. Proposed decryption phase (example)

The encryption process could be implemented by performing the following steps (an example is shown in Figure 7):

Step 1: Select the image_key.
Implantation of this step using mat lab operation is:

$$\boldsymbol{a = imread('peppers.png');}$$

Step 2: Select the reordering sequence.
Implantation of this step using mat lab operation is:

$$\boldsymbol{k1 = 2; k2 = 1; k3 = 2;}$$

Step3: Reorder the image_key using the selected sequence.
Implantation of this step using mat lab operation is:

$$\boldsymbol{b(:,:,1) = flipdim(a(:,:,1), k1);}$$
$$\boldsymbol{b(:,:,2) = flipdim(a(:,:,2), k2);}$$
$$\boldsymbol{b(:,:,3) = flipdim(a(:,:,3), k3);}$$
$$\boldsymbol{k = b(:,:,2);}$$

Step 4: Get the data to be encrypted (message or color image).
Implantation of this step using mat lab operation is:

$$\boldsymbol{mes = 'Data\ cryptography'}$$
$$\boldsymbol{mes1 = unit8(mes);}$$
$$\boldsymbol{L = length(mes);}$$

Step 5: Resize the reordered image_key to meet the data size.
Implantation of this step using mat lab operation is:

$$\boldsymbol{key = imresize(k, [1, L]);}$$

Step 6: Get the encrypted data by apply XORing using the data and the resized key.
Implantation of this step using mat lab operation is:

$$\boldsymbol{encm = bitxor(key, mes1);}$$
$$\boldsymbol{mesen = char(encm)}$$

In Figure 7, shown an example of implementation encryption process.

The decryption process may apply in similar sequence by performing the following steps (an example is shown in Figure 8):

Step 1: Get the image_key.
Step 2: Get the reordering sequence.
Step3: Reorder the image_key using the selected sequence.
Step 4: Get the encrypted data (message or color image).
Step 5: Resize the reordered image_key to meet the data size.
Step 6: Get the decrypted data by apply XORing using the encrypted data and the resized key.

In Figure 8, shown an example of implementation decryption phase.

3. IMPLEMENTATION AND EXPERIMENTAL RESULTS

To study the practical result of suggested method, messages of various lengths were processed by developed software programs. Table 2 shows the output values of MSE, PSNR, and encryption time for messages of different length.

As seen in Table 2, the suggested method provides a good result when message encryption decryption processes, the result of the quality parameters is as recommended and the encryption time is significant small and for short and long messages. Figure 9 shows the curve that relates the encryption (decryption) time and the message length, while Figure 10 shows an example of output images.

Table 2. Messages cryptography results

Message length character)	MSE	PSNR	Encryption decryption) time (second)
100	4.6739e+003	26.3278	0.044000
200	4.4804e+003	26.6721	0.045000
400	4.8404e+003	25.9777	0.045200
800	5.5147e+003	24.6735	0.046000
1600	4.8409e+003	25.9767	0.046300
3200	5.1740e+003	25.3113	0.047000
6400	5.0713e+003	25.5117	0.047700
10000	4.9826e+003	25.6882	0.048000
20000	5.0304e+003	25.5927	0.048400
50000	5.0717e+003	25.5109	0.049000
100000	5.0254e+003	25.6026	0.051000

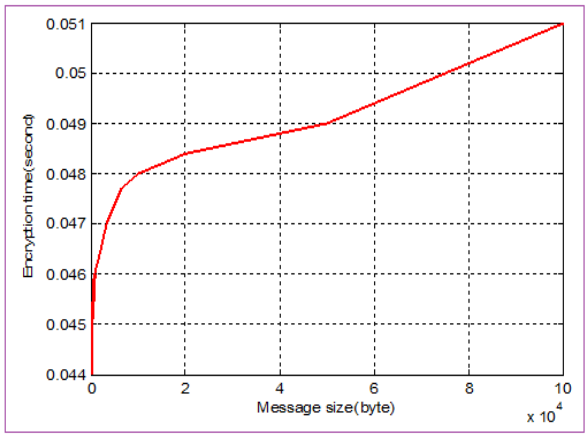

Figure 9. Relation between encryption time and message length

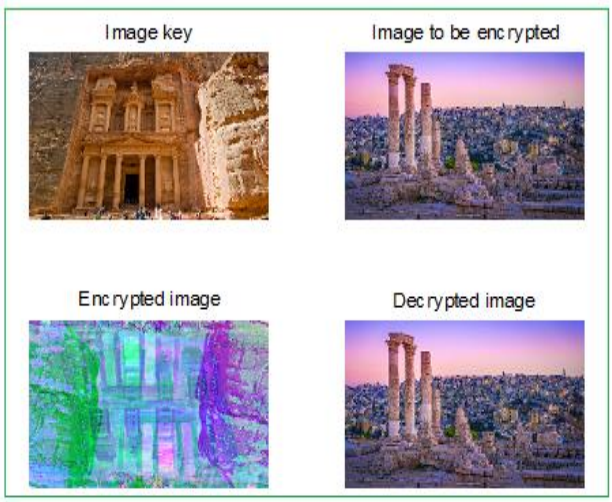

Figure 10. Output images (example of image encryption/decryption)

The results of comparisons between the suggested method and standard method DES and AES are shown in Table 3:

As seen in Table 3, the suggested method is more productive by increasing the method throughput due to decreasing the encryption time. In comparison to DES and AES methods, our method has good speed up as noticed in Figure 11 and Table 4 (the method maintain the quality parameters values acceptable in encryption and decryption processes, see Table 6).

Table 3. Comparisons results

Message size	DES	AES	Suggested
20527	2	4	0.043000
36002	4	6	0.044000
45911	5	8	0.044300
59852	7	11	0.045300
69545	9	13	0.045400
137325	17	26	0.047000
158959	20	30	0.047900
166364	21	31	0.048300
191383	24	36	0.050700
232398	30	44	0.051000
Average time	14	21	0.0467
Bytes/sec	7987.9	5325.2	2394600

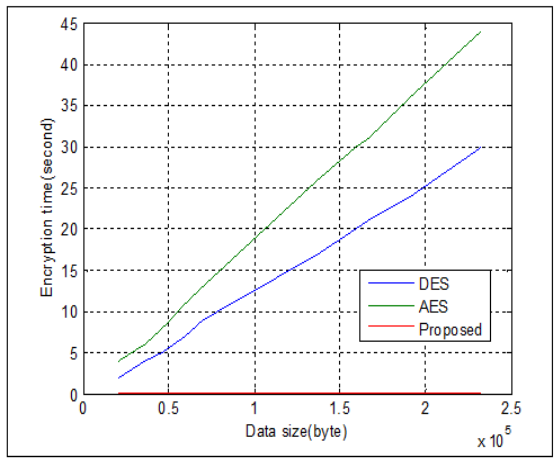

Figure 11. Encryption time comparisons

Table 4. Method speed up

Speedup 1 with 2=time 2/time 1	DES	AES	Suggested
DES	1	1.5000	0.0033
AES	0.6667	1	0.0022
Proposed	299.7859	449.6788	1

Table 5. Differences between the three methods

Feature	DES	AES	Suggested
Data block size	64	64	Text size
PK length	56	128, 192, or 256	Image key size+ ordering sequence+ color number
Principle	Feistel Cipher	substitution and permutation	Image selecting, reordering, resizing
Rounds	14	16	No rounds
Operation	Expansion Permutation, Xor, S-box, P-box, Xor and Swap	Sub bytes, Shift rows, Mix columns, Add round keys	Reordering, resizing, XORing
Security	Low	High	Very high
Speed	slow	slow	Very fast
Image encryption Simplicity	Difficult Not simple	Difficult Not simple	Very easy Very simple

Table 6. Image key size=1071x1600x3=5140800 byte

Image to be encrypted size (byte)	MSE	PSNR	Encryption (decryption) time (second)
150849	5.9042e+003	23.9911	0.062000
77976	5.8934e+003	24.0093	0.060000
518400	4.6121e+004	10.3318	0.064000
4326210	6.8828e+005	3.3519	0.096000
122265	6.1142e+003	23.6415	0.061000
151353	6.5574e+003	22.9418	0.062400
150975	6.8631e+003	22.4861	0.062100
1890000	2.0286e+005	5.7359	0.076000
6119256	9.8454e+005	2.8464	0.109000
Average=1.5008e+006			0.0725
Throughput	1.5008e+006/0.0725=2.0701e+007 byte per second		

From the output results we can summarize the differences between the three methods as shown in Table 5.

Our method can be easily applied for encryption and decryption of secret color images, keeping the method efficient and keeping the quality parameters as recommended as shown in Table 6.

4. CONCLUSION

A method of data encryption and decryption was presented, and implemented for images and text messages. The new suggested method is very secure it employs image_key and reordering sequence as a private key, the key is so complicated that is difficult to hack. The experimental results showed that the suggested method is very easy and highly efficient and it has a reasonable speed up comparing with DES and AES method. The suggested technique satisfies all of the requirements for image quality by preserving appropriate MSE and PSNR values. The obtained experimental result values of MSE and PSNR showed that the encysted images or messages were totally destroyed and the decrypted images or messages were the same as originals, which satisfied the quality requirements of data encryption and decryption. The speed analysis of the obtained results showed that the new suggested method was highly efficient by increasing the throughput of data cryptography and it provided the speed up in comparison to other standard methods DES and AES.

REFERENCES

[1] Nadeem, A., Javed, M.Y. (2005). A performance comparison of data encryption algorithms. In 2005 international Conference on Information and Communication Technologies, pp. 84-89. https://doi.org/10.1109/ICICT.2005.1598556

[2] [Wikipedia-BC] "Block Cipher", http://en.wikipedia.org/wiki/Block_cipher, accessed on 27 July 2007.

[3] Aqel, M.J., Alqadi, Z.A., El Emary, I.M. (2007). Analysis of stream cipher security algorithm. Journal of Information and Computing Science, 2(4): 288-298.

[4] Nader, J., Khrisat, M.S., Alqadi, Z. (2020). A survey of RGB color image encryption methods. International Journal of Computer Science and Mobile Computing, 9(6): 106-113.

[5] Rasras, R.J., Alqadi, Z., Sara, M.R.A., Zahran, B. (2019). Developing new multilevel security algorithm for data encryption-decryption (MLS_ED). International Journal of Advanced Trends in Computer Science and Engineering, 8(6): 3228-3235. http://dx.doi.org/10.30534/ijatcse/2019/90862019

[6] Al-Dwairi, M.O., Hendi, A., AlQadi, Z. (2019). An efficient and highly secure technique to encrypt-decrypt color images. Engineering, Technology & Applied Science Research, 9(3): 4165-4168. http://dx.doi.org/10.48084/etasr.2525

[7] Hendi, A.Y., Dwairi, M.O., Al-Qadi, Z.A., Soliman, M.S. (2019). A novel simple and highly secure method for data encryption-decryption. International Journal of Communication Networks and Information Security, 11(1): 232-238.

[8] Al-Dwairi, M.O., Alqadi, Z.A., Abujazar, A.A., Zneit, R.A. (2010). Optimized true-color image processing. World Applied Sciences Journal, 8(10): 1175-1182.

[9] Moustafa, A.A., Alqadi, Z.A. (2009). Color image reconstruction using a new R'G'I model. Journal of Computer Science, 5(4): 250-254. https://doi.org/10.3844/jcssp.2009.250.254

[10] Barakat, M., Zaini, H., Alqadi, Z. (2021). Text file Encryption_Decryption using key quotient and remainder. International Journal of Engineering Technology Research & Management, 5(4): 9-21.

[11] AlQadi, Z., Hussein, M.E. (2017). Window averaging method to create a feature victor for RGB color image. International Journal of Computer Science and Mobile Computing, 6(2): 60-66.

[12] Ayyoub, B.Z.B., Nader, J., Al-Qadi, Z., Zahran, B. (2019). Suggested method to create color image features victor. Journal of Engineering and Applied Sciences, 14(1): 2203-2207. http://dx.doi.org/10.36478/jeasci.2019.2203.2207

[13] Al Azzeh, J., Alhatamleh, H., Alqadi, Z.A., Abuzalata, M.K. (2016). Creating a color map to be used to convert a gray image to color image. International Journal of Computer Applications, 153(2): 31-34. https://doi.org/10.5120/ijca2016911975

[14] Abu-Ein, A., Alqadi, Z.A., Nader, J. (2016). A technique of hiding secrete text in wave file. International Journal of Computer Applications, 9(2): 96-103. https://doi.org/10.5120/ijca2016911732

[15] Priya, D. (2002). Performance Comparison: Security Design Choices. Microsoft Developer Network. http://www.sciepub.com/reference/116125.

[16] Jose, M. (2014). Hiding image in image using LSB insertion method with improved security and quality. International Journal of Science and Research, 3(9): 2281-2284.

[17] Patel, R.M., Shah, D.J. (2013). Conceal gram: Digital

image in image using LSB insertion method. International Journal of Electronics and Communication Engineering & Technology, 4(1): 230-2035.
[18] Akhtar, N., Johri, P., Khan, S. (2013). Enhancing the security and quality of LSB based image steganography. In 2013 5th International Conference and Computational Intelligence and Communication Networks, pp. 385-390. https://doi.org/10.1109/CICN.2013.85
[19] Juneja, M., Sandhu, P.S. (2013). An improved LSB based steganography with enhanced security and embedding/extraction. In 3rd International Conference on Intelligent Computational Systems, Hong Kong China, pp. 29-34.
[20] Nadir, J., Alqadi, Z., Ein, A.A. (2016). Classification of matrix multiplication methods used to encrypt-decrypt color image. International Journal of Computer and Information Technology, 5(5): 459-464.
[21] Sivakumar, T., Venkatesan, R. (2013). A novel image encryption approach using matrix reordering. WSEAS Transactions on Computers, 12(11): 407-418.
[22] Gao, H., Zhang, Y., Liang, S., Li, D. (2006). A new chaotic algorithm for image encryption. Chaos, Solitons & Fractals, 29(2): 393-399. https://doi.org/10.1016/j.chaos.2005.08.110
[23] Chen, G., Mao, Y., Chui, C.K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3): 749-761. https://doi.org/10.1016/j.chaos.2003.12.022
[24] Khalane, V., Suralkar, S., Bhadade, U. (2020). Image encryption based on matrix factorization. International Journal of Safety and Security Engineering, 10(5): 655-661. https://doi.org/10.18280/ijsse.100510
[25] Wang, X., Zhang, J. (2008). An image scrambling encryption using chaos-controlled Poker shuffle operation. In 2008 International Symposium on Biometrics and Security Technologies, pp. 1-6. https://doi.org/10.1109/ISBAST.2008.4547639
[26] Al-Dwairi, M.O., Hendi, A.Y., Soliman, M.S., Alqadi, Z.A. (2019). A new method for voice signal features creation. International Journal of Electrical and Computer Engineering, 9(5): 4077. http://dx.doi.org/10.11591/ijece.v9i5.pp4077-4091
[27] Nadir, J., Ein, A.A., Alqadi, Z. (2016). A technique to encrypt-decrypt stereo wave file. International Journal of Computer and Information Technology, 5(5): 465-470.
[28] Hindi, A., Dwairi, M.O., Alqadi, Z. (2020). Analysis of digital signals using wavelet packet tree. International Journal of Computer Science and Mobile Computing, 9(2): 96-103.
[29] Al-Dwairi, M.O., Hendi, A., AlQadi, Z. (2019). An efficient and highly secure technique to encrypt-decrypt color images. Engineering, Technology & Applied Science Research, 9(3): 4165-4168. http://dx.doi.org/10.48084/etasr.2525
[30] Zahran, B., Alqadi, Z., Nader, J., Ein, A.A. (2016). A comparison between parallel and segmentation methods used for image encryption-decryption. International Journal of Computer Science & Information Technology (IJCSIT) Volume, 8(5): 127-133. https://doi.org/10.5121/ijcsit.2016.8509
[31] Dwairi, M.O., Alqadi, Z., Khrisat, M.S., Hindi, A., Khawatreh, S.A. (2020). Digital color image encryption-decryption using segmentation and reordering. International Journal of Latest Research in Engineering and Technology (IJLRET), 6(5): 6-12.