iJETRM
International Journal of Engineering Technology Research & Management

COLOR IMAGE ENCRYPTION-DECRYPTION USING SMT

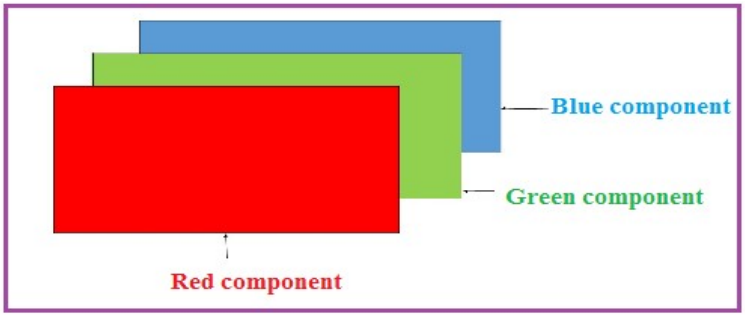
Dr. Mohammad S. Khrisat
Dr. Saleh A. Khawatreh
Dr. Majed Omar Dwairi
Dr. Amjad Hindi
Prof. Ziad Alqadi
Albalqa Applied University, Faculty of engineering technology, Al-Ahliyya Amman University
mkhrisat@bau.edu.jo
skhawatreh@ammanu.edu.jo
majeddw@gmail.com
amjadhindi@bau.edu.jo
natalia_maw@yahoo.com

ABSTRACT
Digital color image is very famous and important data type; it is used in many important vital applications such as banking systems, protection and security systems, so image protection is required. In this research paper we will introduce a simplified method of color image encryption-decryption which is based on using SMT and PK; the method will be tested and implemented using various color images. The issues of security, efficiency and accuracy will be discussed; the obtained experimental results will be analyzed in order to raise some judgments.

KEYWORDS:
Color image, encryption, SMT, PK, decryption, encryption time, efficiency measures, speedup, throughput, MSE, PSNR.

INTRODUCTION

The digital image [1],[2],[3],[4]is one of the most important types of digital data circulating between people and between different institutions, because it is used in many important and vital applications such as banking applications, military and medical applications and many others [5],[6], [7]. The digital image sometimes contains confidential information, or the image may be of a personal nature, which requires preventing unaffected entities and people from understanding it or spying on it, and this in turn leads us to search for a safe and effective way to encode the digital image by creating a destroyed encrypted image. The unauthorized person cannot understand it with the naked eye or even restore it using programmatic methods [8], [9], [10].
The digital image represents the three-dimensional matrix, the first dimension is devoted to represent the red color, and the second dimension is to represent the green color, while the third dimension represents the blue color [11],[12],[13], as shown in Figure 1.



iJETRM
International Journal of Engineering Technology Research & Management

Figure 1: Color image components

The true color of the pixel is formed by mixing the three colors [14], [15], [16], [17], as shown in the figure 2, and the image can be dealt with by retrieving the two-dimensional matrix for each color, and the image can also be reshaped with any dimensions we see suitable for the image processing process. Figure 3 shows an example of a digital image and for each of the three colors [18], [19], [20].

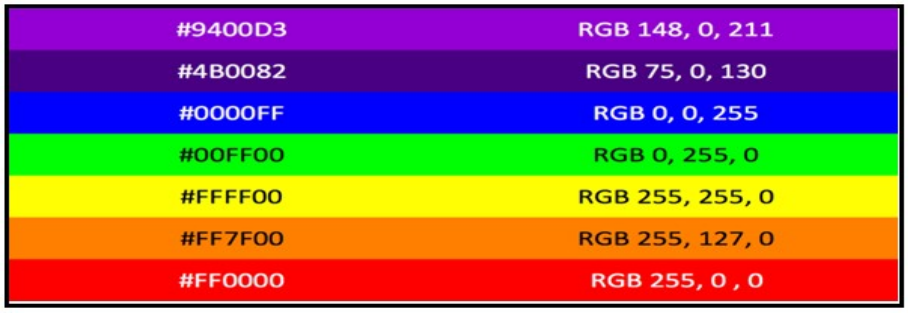


Figure 2: Mixing the color for a color pixel

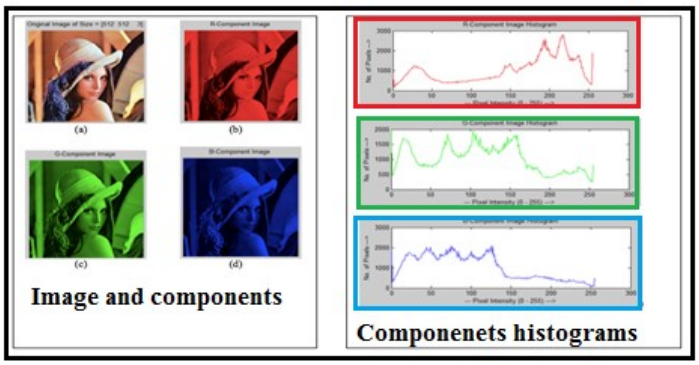
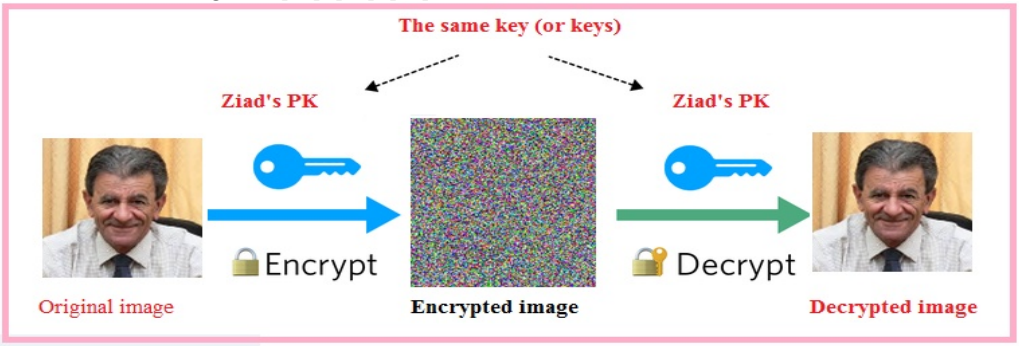


Figure 3: Color image components and there histograms

The process of encrypting the digital image is defined as the process of destroying the original image so that an incomprehensible and distorted image is produced and this process is usually done using a special private key that is known by the sender and receiver and by using this key and some special operations the encrypted image is generated as shown In figure 4 [21], [22]. [23].



iJETRM
International Journal of Engineering Technology Research & Management

Figure 4: Encryption-decryption process.

The process of decrypting the digital image is defined as the process of returning the image to its original, so that it is completely identical to the original image, using the same key and special and specific operations [24], 25], [26].

Related works

The efficiency of the encrypting and decrypting method is measured by various factors, the most important of which are [36], [37]:

- The extent of distortion of the original image, and in this case, the value of the mean square error (MSE) between the original and encrypted images must be very high (or the value of peak-signal-to-noise ratio (PSNR) t should be very low value)[30], [31].
- Not to lose any part of the original image information, in this case the value of the mean square error (MSE) between the original and decrypted images must be closed to zero (or the value of peak-signal-to-noise ratio (PSNR) t should be closed to infinite) [27], [28], [29].
- High speed by reducing encrypting time and decrypting time.
- High level of security and protection with hard-to-hack keys [41].
- Ease of implementation.

There are now several methods available that range in how well they encode a digital image, some of these methods were based on image blocking and XORING the created blocks by a private key [31], [32], [33], [35], [41], in [34], and others were based on matrix multiplication of the original image and a special generated private key matrix [30]. In [37] the authors used matrix reordering principle, while in [39] the encryption was based on based on 3D Chaotic Cat Maps. In [40] the authors introduced a method based on Rubik's Cube principle; these methods will be implemented to make comparisons with the proposed here method.

The proposed method

The proposed method as shown in figure 5 uses two private keys:

- Private key (PK), it is a huge 3D matrix which can cover any digital color image, it will be during the encryption-decryption processes adopted to the image size, this key must be generated once and saved by the sender and the receiver, it also can be updated any time. This key contains the values from 0 to 255 and it is very difficult to hack it.
- SMT (segment map table)(this structure was taken from the operating system and here thanks to segmentation memory management), this table will be created for any image and it contains the following fields as shown in table 1, this table must be used as a second secret key and it will be generated from the initial SMT shown in table 2:

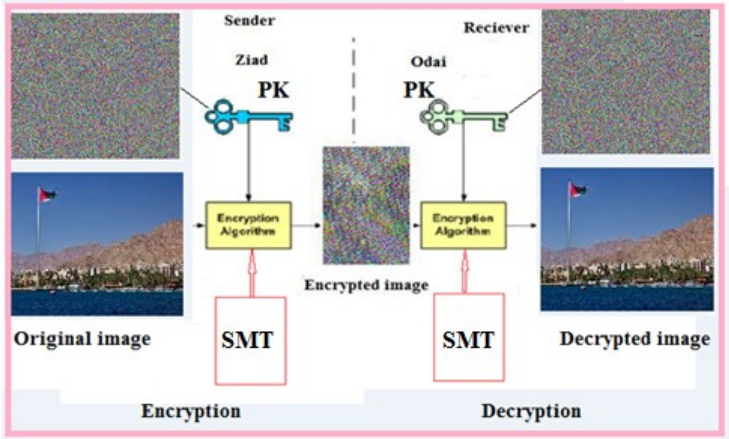


Figure 5: Proposed method

iJETRM
International Journal of Engineering Technology Research & Management

Table 1: Secret SMT (example)

Segment number	Size	Location
3	27500	1
5	92875	27501
1	2000	120376
4	24000	122376
2	5500	146375

Table 2: Initial SMT (example)

Segment number	Size	Location
1	2000	1
2	5500	2001
3	27500	7501
4	24000	35001
5	92875	59001

The process of encryption can be implemented applying the following steps:

1) Get the original color image.
2) Retrieve the image size.
3) Reshape original image matrix into one raw matrix.
4) Load PK.
5) Adopt PK to suit the image size.
6) Apply XORING.
7) Select the number of segments and the size of each segment.
8) Build SMT.
9) Reorder the segments and create a new secret SMP.
10) Combine again the image and reshape it to 3D matrix to get the encrypted image.

The decryption phase will be implemented applying the following steps:

1) Get the encrypted color image.
2) Retrieve the image size.
3) Reshape encrypted image matrix into one raw matrix.
4) Load PK.
5) Adopt PK to suit the image size.
6) Get secret SMT
7) Reorder the segments and create a new secret SMP.
8) Apply XORING.
9) Combine again the image and reshape it to 3D matrix to get the decrypted image.

Implementation and experimental results

Several images were taken and implemented using the proposed method, each image was segmented into 5 segments using SMT shown in table 1 (the number of segments can be changed and the contents of SMT can be also changed).

The selected PK was with size (3000*3000*3), figures 5 thru 8 show the outputs after executing each phase of the proposed method:

iJETRM
International Journal of Engineering Technology Research & Management

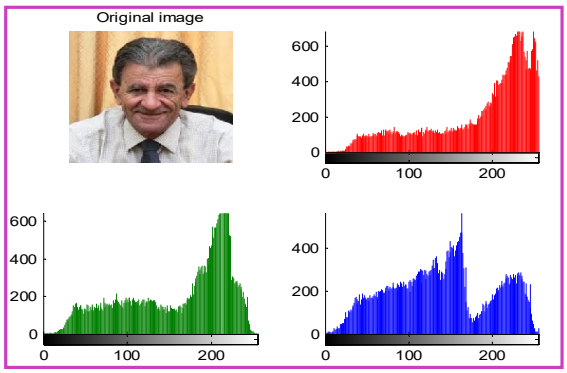


Figure 5: Original image (example)

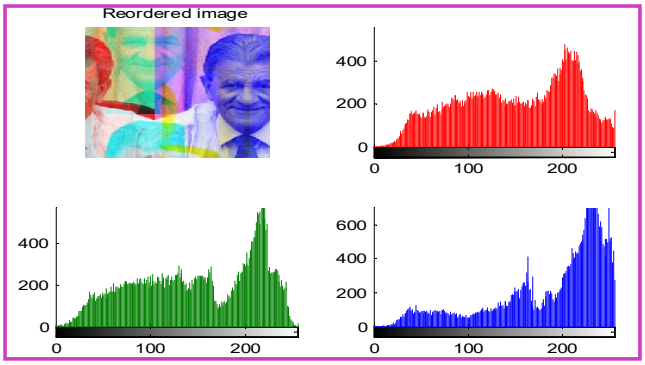


Figure 6: Reordered image (example)

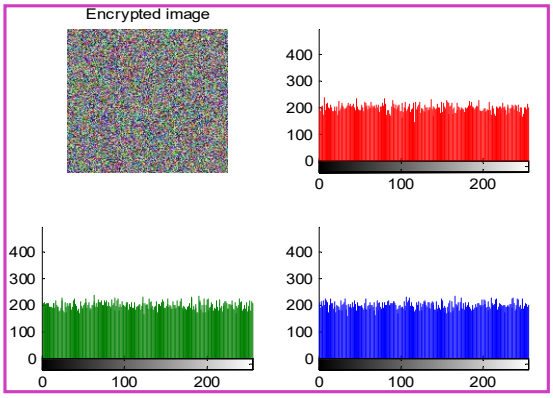


Figure 7: Encrypted image (example)

iJETRM
International Journal of Engineering Technology Research & Management

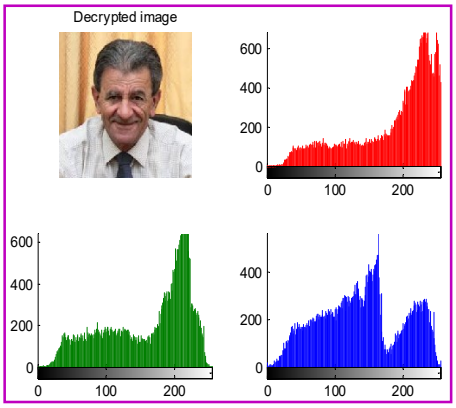


Figure 8: Decrypted image (example)

Table 3 shows the experimental results of implementation, and from this table we can see that the proposed method satisfies the factors of encryption-decryption efficiency and security.
The results were compared with other methods results, table 4 shows how this method has an advantages and how it improve the process of encryption-decryption.

Table 3: Experimental results

Image	Size (byte)	ET(seconds)	DT(seconds)	PSNR between original and encrypted images	Throughput(byte per second)
1	151875	0.0020	0.0020	7.8342	75937000
2	150849	0.0020	0.0020	7.1020	75424000
3	518400	0.0050	0.0050	7.7367	64800000
4	5140800	0.0740	0.0740	8.3368	69470000
5	4326210	0.0600	0.0600	8.3765	72104000
6	122265	0.0020	0.0020	8.9170	61132000
7	518400	0.0070	0.0070	7.3474	74057000
8	150975	0.0020	0.0020	8.4069	75487000
9	151353	0.0020	0.0020	7.3284	75676000
10	1890000	0.0270	0.0270	7.5659	70000000
11	6119256	0.0860	0.0860	9.6703	71154000
12	150876	0.0020	0.0020	8.0780	75438000
13	150738	0.0020	0.0020	8.6319	75369000
14	151875	0.0020	0.0020	6.7169	75938000
15	2500608	0.0360	0.0360	7.3243	69461000
Average	**1479632**	**0.0207**	**0.0207**	**7.9582**	**72096000**

Table 4: Results comparisons

Method	Encryption time (s)	Decryption time (s)	Throughput (M bytes)	Speedup of the proposed method	Order
Proposed SSEAM	0.0207	0.0207	72.096000	`1	1
Ref. [27]	0.0513	0.0513	29.2398	4.4609	2

iJETRM
International Journal of Engineering Technology Research & Management

Ref. [34]	0.06469	0.062727	23.1876	5.6252	3
Ref. [36]	0.23	0.23	6.5217	20.0000	5
Ref. [37]	0.5	0.5	3	43.4783	7
Ref. [38]	0.4	0.4	3.7500	34.7826	6
Ref. [39]	0.12	0.12	12.5000	10.4348	4
Ref. [40] v.1	0.56	0.56	2.6786	48.6957	8
Ref [40] v.2	1.01	1.01	1.4852	87.8261	9

Conclusion

A new based on SMT method of color image encryption-decryption was proposed and implemented; the obtained experimental results showed that the proposed method is simple, highly secure by providing the use secret huge key and changeable ranges of color image segmentation. The proposed method is very efficient by providing a very small time of encryption-decryption and a very high value of method throughput. The proposed methods satisfies the requirement for MSE and PSNR values in the encryption and decryption phases and it has a better performance comparing with some other existing methods

References

[1] Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.
[2] 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, vol. 153, issue 2, pp. 31-34, 2016.
[3] 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.
[4] Mohammed Ashraf Al Zudool, Saleh Khawatreh, Ziad A. Alqadi, Efficient Methods used to Extract Color Image Features, IJCSMC, vol. 6, issue 12, pp. 7-14, 2017.
[5] Akram A. Moustafa and Ziad A. Alqadi, Reconstructed Color Image Segmentation, Proceedings of the World Congress on Engineering and Computer Science, WCECS 2009, vol. II, 2009.
[6] 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, vol. 96, issue 13, pp. 4081-4091, 2018.
[7] Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.
[8] Dr Rushdi S Abu Zneit, Dr Ziad AlQadi, Dr Mohammad Abu Zalata, A Methodology to Create a Fingerprint for RGB Color Image, IJCSMC, vol. 6, issue 1, pp. 205-212. 2017.
[9] RA Zneit, Ziad Alqadi, Dr Mohammad Abu Zalata, Procedural analysis of RGB color image objects, IJCSMC, vol. 6, issue 1, pp. 197-204, 2017.
[10] Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, vol. 9, issue 6, pp. 4942-4945, 2019.
[11] Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. AlQadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering, Technology & Applied Science Research, vol. 9, issue 1, pp. 3681-3684, 2019.
[12] Dr. Amjad Hindi, Dr. Ghazi M. Qaryouti, Prof. Yousif Eltous, Prof. Mohammad Abuzalata, Prof. Ziad Alqadi, Color Image Compression using Linear Prediction Coding, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 13 – 20, 2020.
[13] Ziad Alqadi, Mohammad Abuzalata, Yousf Eltous, Ghazi M Qaryouti, Analysis of fingerprint minutiae to form fingerprint identifier, International Journal on Informatics Visualization, vol. 4, issue 1, pp. 10-15, 2020.
[14] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TO CREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.
[15] Prof. Ziad Alqadi, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Dr. Mohammad S. Khrisat, Features Analysis of RGB Color Image based on Wavelet Packet Information, IJCSMC, vol. 9, issue 3, pp. 149 – 156, 2020.

iJETRM
International Journal of Engineering Technology Research & Management

[16] Ziad Alqadi Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, VALUABLE WAVELET PACKET INFORMATION TO ANALYZE COLOR IMAGES FEATURES, International Journal of Current Advanced Research, vol. 9, issue 2, pp. 2319-6505, 2020.
[17] Amjad Hindi, Majed Omar Dwairi, Ziad Alqadi, Analysis of Digital Signals using Wavelet Packet Tree, IJCSMC, vol. 9, issue 2, pp. 96-103, 2020.
[18] Amjad Y. Hindi, Majed O. Dwairi, Ziad A. AlQadi, Creating Human Speech Identifier using WPT, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 117 – 123, 2020.
[19] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Efficiency analysis of color image features extraction methods, International Journal of Software & Hardware Research in Engineering, vol. 8, issue 2, pp. 58-65, 2020.
[20] Ziad A. AlQadi Amjad Y. Hindi, Majed O. Dwairi, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.
[21] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.
[22] Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.
[23] Ziad Alqad, Prof. Yousf Eltous Dr. Ghazi M. Qaryouti, Prof. Mohammad Abuzalata, Analysis of Digital Signal Features Extraction Based on LBP Operator, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 1, pp. 1-7, 2020.
[24] Ziad A. AlQadi, A Highly Secure and Accurate Method for RGB Image Encryption, IJCSMC, vol. 9, issue 2, pp. 12-21, 2020.
[25] Belal Zahran Rashad J. Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, pp. 3228-3235, 2020.
[26] Ziad Alqad, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.
[27] Majed O Al-Dwairi, A Hendi, Z AlQadi, An efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.
[28] Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, A novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp. 232-238, 2019.
[29] Ziad Alqadi, Ahmad Sharadqh, Naseem Asad, Ismail Shayeb, Jamil Al-Azzeh, Belal Ayyoub, A highly secure method of secret message encoding, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 3, pp. 82-87, 2019.
[30] Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, IJCSMC, Vol. 8, Issue 6, pp. 106 –123, 2019.
[31] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, IJCSMC, vol. 8, issue 3, pp. 14-26, 2019.
[32] 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, issue 1, pp. 86-93, 2019.
[33] Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION, VOL 3 (2019) NO 3, pp. 262-265.
[34] 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.
[35] 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.

iJETRM
International Journal of Engineering Technology Research & Management

[36] 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.
[37] T. Sivakumar, R. Venkatesan, "A Novel Image Encryption Approach using Matrix Reordering", WSEAS Transactions on Computers, Vol. 12, No. 11, pp. 407-418, 2013.
[38] H. Gao, Y. Zhang, S. Liang, D. Li, "A New Logistic maps for Image Encryption", Chaos- Solitons & Fractals, Vol. 29, No. 2, pp. 393- 399, 2006.
[39] 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.
[40] 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.
[41] 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.