International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 06 - Issue 05 || May 2020 || PP. 06-12

Digital color image encryption-decryption using segmentation and reordering

Dr. Majed Omar Dwairi[1], Prof. Ziad Alqadi[2], Dr. Mohammad S. Khrisat[3], Dr. Amjad Hindi[4], Dr. Saleh A. Khawatreh[5]
Albalqa Applied University[1, 2, 3, 4],
Faculty of engineering technology, Jordan, Amman, Al-Ahliyya Amman University[5]

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; the method will be based on image segmentation and reordering using two private keys, it 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 enhancement factors.

Keywords: Color image, encryption, decryption, PSNR, secret key, secret range, encryption time, efficiency measures, speedup, and throughput, MSE, PSNR.

1. Introduction

Digital color Image (DCI) [1],[2], [3], [4]is a famous and important data type and it is usually represented by a 3D matrix [5], [6], [7], [8], the first dimension is reserved for the red color, the second for the green, while the third one is reserved for the blue color [9], [10], [11]. The pixel color is obtained as a result of mixing the three colors. Each individual image color matrix is a 2D matrix and it can be accessed separately if want to, also we can reshape the 3D matrix to 2D or 1D matrices depending on the way of image manipulation, figure 1 shows a sample of DCI with the histogram of each color [12], [13], [14], [15].

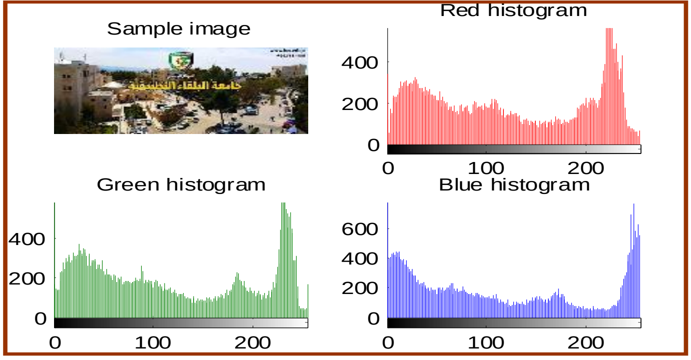

Figure 1: DCI sample

The digital image is one of the most important types of data currently circulating and its importance lies in it being used in many vital applications that need a high level of protection that prevents intruders and unauthorized people from accessing it [16], [17], [18].

The digital image may contain important information [19], [20], [21], or the image may be of a personal nature and has a specific privacy that cancels the process of viewing it from any other party that is not authorized [22], [23], [24], [25], which requires the destruction of the image and deforming it using the encryption process so that the image becomes safe and out of reach of unauthorized persons. Therefore, the encrypting process means that the original image is transformed into a distorted image that cannot be understood with the naked eye and difficult to retrieve using the programmed methods. As for the decrypting process, it means retrieving an image identical to the original, without losing any information from the image [26], [27], [28].

The effectiveness of the coding method is measured by several things, the most important of which are:

- ✓ The time of coding and decoding, the less this pomegranate, the more effective the method [36], [37].
- ✓ The error rate between the original image and the encoded image, which must be very high, which in turn reflects the complete distortion of the image.

- ✓ Zero error ratio between the original image and the re-encoded image [38].
- ✓ A high level of protection prevents intruders from spying on the image [29], [30], [31].

Symmetric data encryption-decryption as shown in figure 2 applies the encryption and decryption processes using the same private key (PK), this key must be known by the sender and the receiver when transferring the data (sometimes we can use more than one PK), the encryption process will take PK and performs some selected operations using the original data and the PK to get the encrypted data, the sequence of performed operations also must be known by the receiver[39], [40], [41].

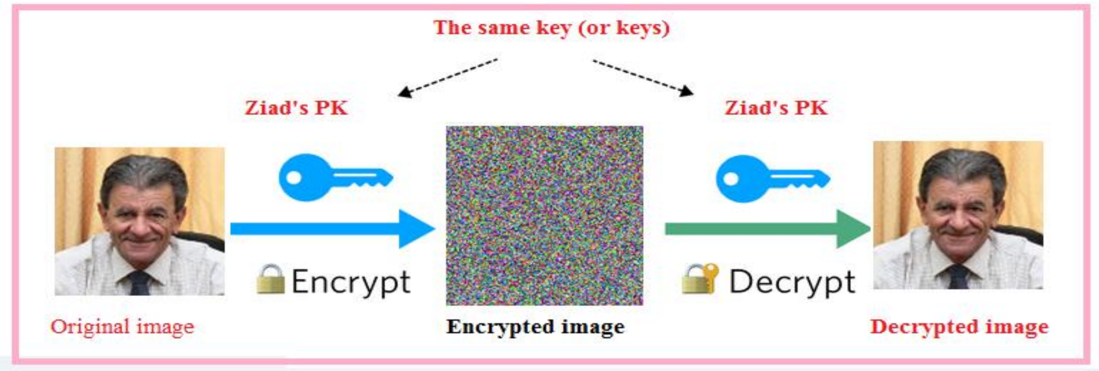

Figure 2: Encryption-decryption process

2. Related works

Many methods were introduced to encrypt-decrypt color 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.

Any good method for color image encryption-decryption must have the following features [24], [25], [26]:

- Efficient by minimizing the encryption-decryption times, and maximizing the method throughput and speedup.
- Simple by using simple procedures to handle the process of encryption-decryption.
- Accurate by minimizing mean square error (MSE) and maximizing peak-signal-to-noise-ratio (PSNR) between the original image and the decrypting one, so the decrypted image is completely identical to the original image [28].
- Secure to make it impossible or very difficult to hack the encrypted image, and destroying the original image, so the encrypted image not became understandable to seeing with the eye, here the method must provide a maximum MSE value and a minimum PSNR value [27].

3. The proposed method

The proposed method is based on reshaping the original color image into one raw matrix, dividing this matrix into segments with different sizes, inverting the segment elements and then applying XORING of each segment with the associated part of the private key.

The proposed method uses two private keys as shown in figure 3, the first private key (PK) is a huge matrix to be used as a data bank for extracting a sub-keys for the segments. The second private key is secret ranges (SR) to be used to separate the image into different segments, the two keys are to be kept in secret and they are known only by the sender and receiver.

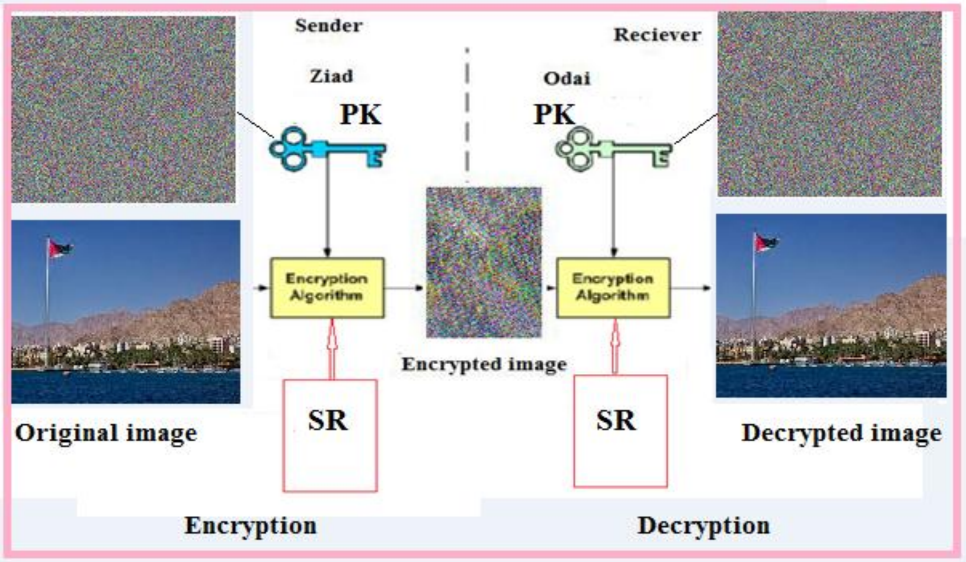

Figure 3: Proposed method diagram

The encryption process will be implemented applying the following steps:

1) Load PK.
2) GET SK.
3) Reshape the original image into one raw matrix.
4) Divide the raw matrix into segments depending on SK.
5) Reorder the elements of each segment.
6) From PK extract a sub-key for each segment.
7) Apply XORING using each segment and the associated sub-key.
8) Combine the segments into one raw matrix.
9) Reshape one raw matrix into 3D matrix to get the encrypted image.

The decryption process will be implemented applying the following steps:

1) Load PK.
2) GET SK.
3) Reshape the encrypted image into one raw matrix.
4) Divide the raw matrix into segments depending on SK.
5) From PK extract a sub-key for each segment.
6) Apply XORING using each segment and the associated sub-key.
7) Reorder the elements of each segment.
8) Combine the segments into one raw matrix.
9) Reshape one raw matrix into 3D matrix to get the decrypted image.

4. Implementation and experimental results

The proposed method was implemented using various images, figures 4, 5, 6 and 7 show a sample of the output generated after processing various method steps:

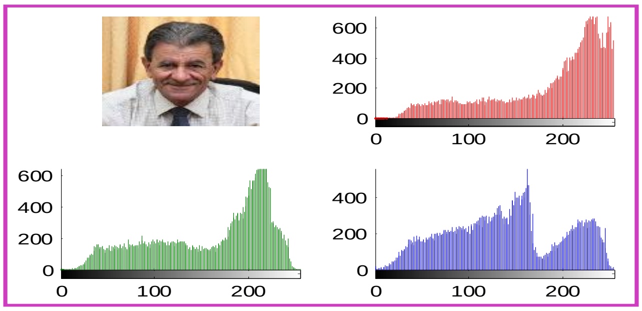

Figure 4: Original image

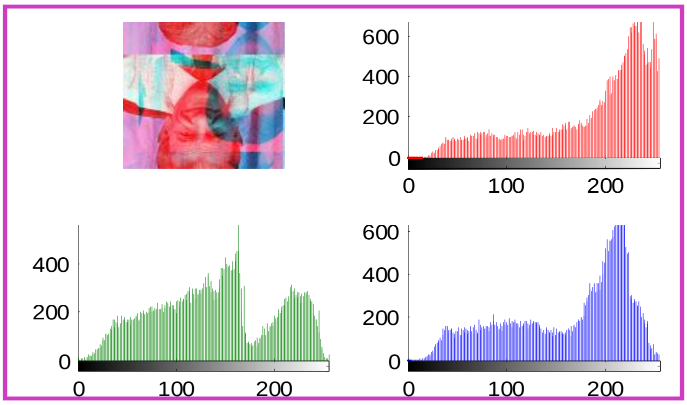

Figure 5: Reordered segmented image

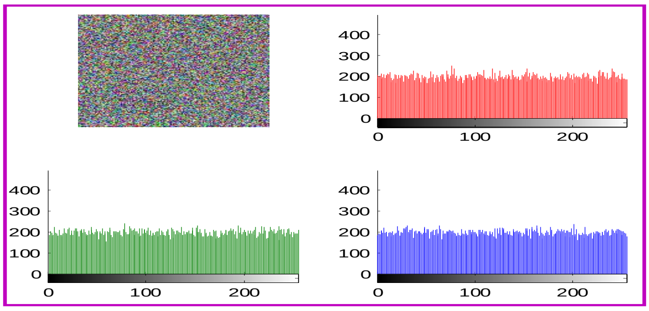

Figure 6: Encrypted image

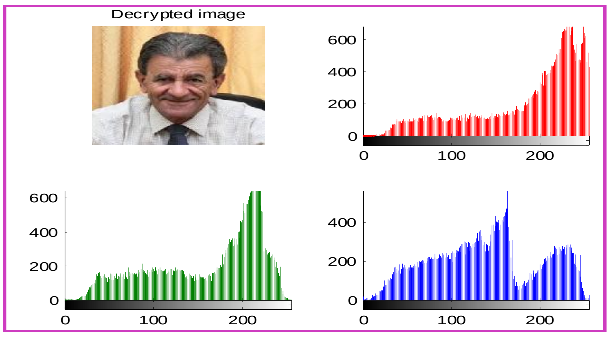

Figure 7: Decrypted image

We selected several color images, then we implemented the proposed method of encryption-decryption, the experimental results are shown in table 1:

Table 1: 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**

From the obtained experimental results we can raise the following facts:

- The proposed method is very efficient by providing significant small times for encryption and decryption.
- The proposed method is highly secure by using various keys of encryption-decryption: the PK and SR.
- The received encrypted image was a damaged and destroyed version of the original, because PSNR value between the original image and the encrypted one was always low.
- PSNR value between the original image and the decrypted one was always infinite, which means that there is no loss of information, and the decrypted image is identical the original one.
- The average throughput is very high and it reaches 72 M byte per second.

For comparisons purposes the proposed method results were compared with other methods results, table 2 shows the results of comparisons.

Table 3: Methods comparisons

Method	Encryption time (s)	Decryption time (s)	Throughput (M bytes)	Speedup of the proposed method	Order
Proposed	0.0207	0.0207	72.096000	`1	1
Ref. [27]	0.0513	0.0513	29.2398	2.4783	2
Ref. [34]	0.06469	0.062727	23.1876	3.1251	3
Ref. [36]	0.23	0.23	6.5217	11.1111	5
Ref. [37]	0.5	0.5	3	24.1546	7
Ref. [38]	0.4	0.4	3.7500	19.3237	6
Ref. [39]	0.12	0.12	12.5000	5.7971	4
Ref. [40] v.1	0.56	0.56	2.6786	27.0531	8
Ref [40] v.2	1.01	1.01	1.4852	48.7923	9

From table 3 we can see that the proposed method adds a good enhancement to process of color image encryption-decryption.

Conclusion

A method of color image encryption decryption based on multiple private keys was proposed, tested and implemented. The obtained experimental results showed the proposed method is efficient, accurate and highly secure, it can added some enhancements in the encryption-decryption process by providing a high level of image protection.

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.

[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.

[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.