IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

Color Image Encryption-Decryption using RANDOM Noise and PMT

Prof. Yousif Eltous[1], Dr. Akram Moustafa Hamarchi[2], Dr. Mohammad S. Khrisat[3], Dr. Saleh A. Khawatreh[4], Prof. Ziad Alqadi[5]

Albalqa Applied University, Jordan[1, 3, 5]

Al Al-Bayt University, Jordan[2]

Al-Ahliyya Amman University, Jordan[4]

Abstract: RGB color images are among the most important types of digital data circulating in the Internet and through various social media. RGB color image may contains confidential information, or the signal may be of a personal nature, which requires preventing its understanding from unauthorized entities or persons and therefore this signal must be encrypted. In this paper, we will discuss a new method for encrypting the RGB color images based on adding a random noise and image rearrangement. The method will be run to measure its efficiency and the extent to which it achieves the level of security and protection. The experimental results will be analysed to prove the proposed method efficiency factors.

Keywords: RGB color image, YIQ image, random noise, PMT, MSE, PSNR, encryption time, decryption time, requirements.

I. Introduction

The color digital image [1], [2], [3], [4] is considered one of the most important types of digital data circulating in the Internet and through most of the available social media [5], [6], [7]. In many cases, the digital image can be confidential or be of a personal nature or be carrying some important and confidential information [23], [24], [25] which requires preventing any A third person or entity not authorized to understand the image or know the data therein, not to mention some computer systems that use digital images, and this requires providing an easy way to protect it and not to penetrate the information it carries [8], [9], [10]. The digital image is represented by a three-dimensional matrix, where the first dimension indicates red color; the second indicates green color, while the third dimension indicates blue color [11], [12], [13]. Therefore, the image can be considered as three two-dimensional matrices, one for each of the three colors, and therefore we can deal with each color separately, or it can even be reconfigured into an array and as we see fit for the treatment process [14], [15]. Figure 1 shows an RGB color image with its colors histograms [16], [17].

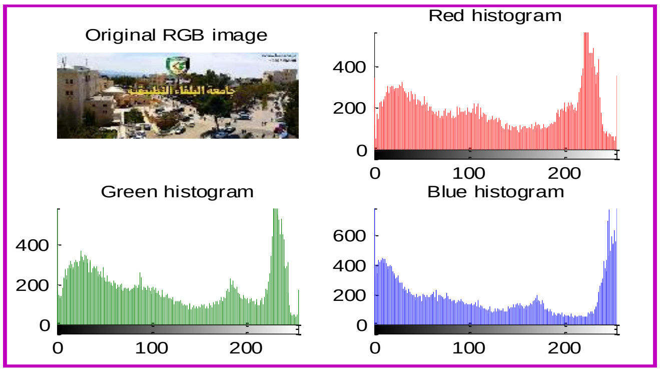

Figure 1: RGB color image and colors histogram

RGB color image pixels values are within the rang 0 to 255 and they are integer values, so it is difficult to add a random noise to it, and here we have to convert the RGB image to YIQ which accepts the random noise addition or subtraction, here we can use formula 1 to get YIQ image from RGB one, and formula 2 to get back RGB image, and here we have to multiply the obtained image by 255 and take the integer part [18], [19], [20].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 5, May 2020

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.000 & 0.956 & 0.621 \\ 1.000 & -0.272 & -0.647 \\ 1.000 & -1.106 & 1.703 \end{bmatrix} \begin{bmatrix} Y \\ I \\ Q \end{bmatrix} \quad (2)$$

Figures 2 and 3 illustrate outputs examples of the conversion process:

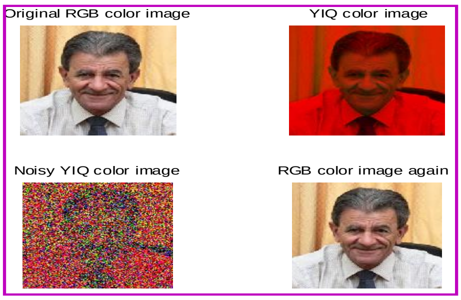

Figure 2: Conversion process

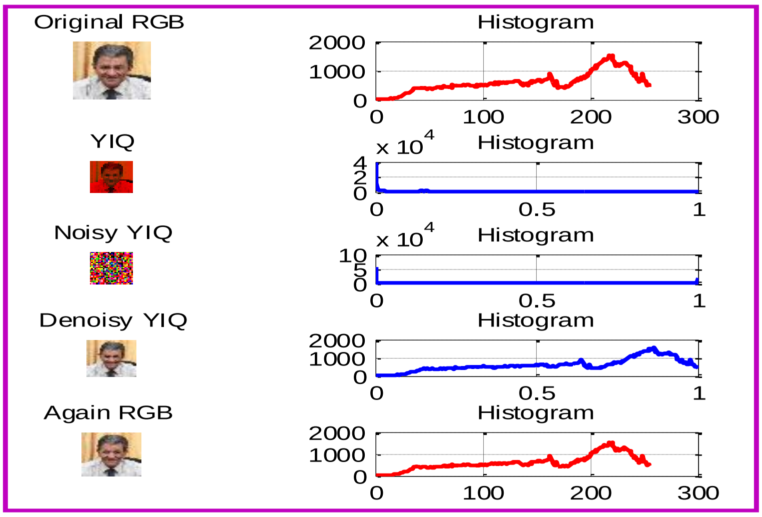

FIGURE 3: OUTPUT IMAGES AND THERE TOTAL HISTOGRAM

II. IMAGE ENCRYPTION-DECRYPTION

The digital image encryption process [21] is the process of destroying the original image so that it becomes distorted and prevents any outsider from understanding it or knowing its contents [25], [26], [27]. As for the decoding process, it means retrieving an image that is completely identical to the original image, without losing any information from it [28], [29].

The encryption and decryption process is usually carried out using one or more private keys, as shown in Figure 4. The encryption and decryption method should achieve the following things [22], [30], [31], [32]:

- ✓ High efficiency by maximizing the method speed and throughput or minimizing the encryption and decryption times.
- ✓ High deformation and distortion rate by decreasing peak-to-signal-ratio (PSNR) and increasing mean square error (MSE) between the original and the encrypted images[38], [39].
- ✓ High reliability rate by decreasing MSE and increasing PSNR between the original and the encrypted images.
- ✓ High level of security and protection with hard keys to hack [36].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

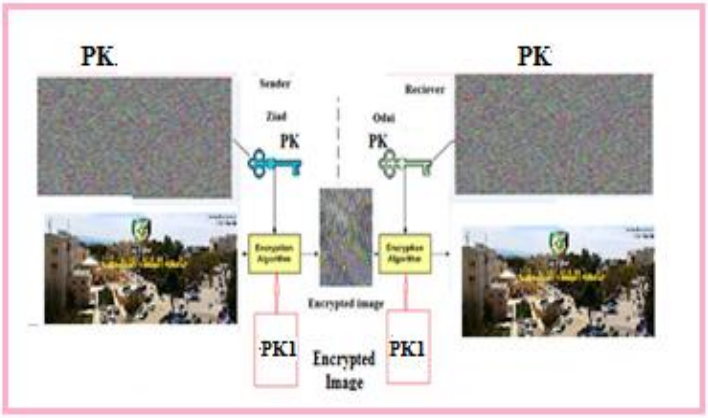

Figure 4: Encryption-decryption process

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.

III. THE PROPOSED METHOD

To increase the level of image security and protection, the proposed method uses two private keys hard to hack. The first PK is a special random noise array with a very huge size to adapt any image with any size. This key is to be generated once and saved by both the sender and receiver, and it contains a values range from -1 to 1. The second PK is a partition map table (PMT) which is to be generated by the sender and sent to the receiver, this key contains information about the image parts or segment, location and size of each partition and how the partitions within the image were arranged.

The proposed encryption phase as shown in figure 5 will be implemented applying the following steps:

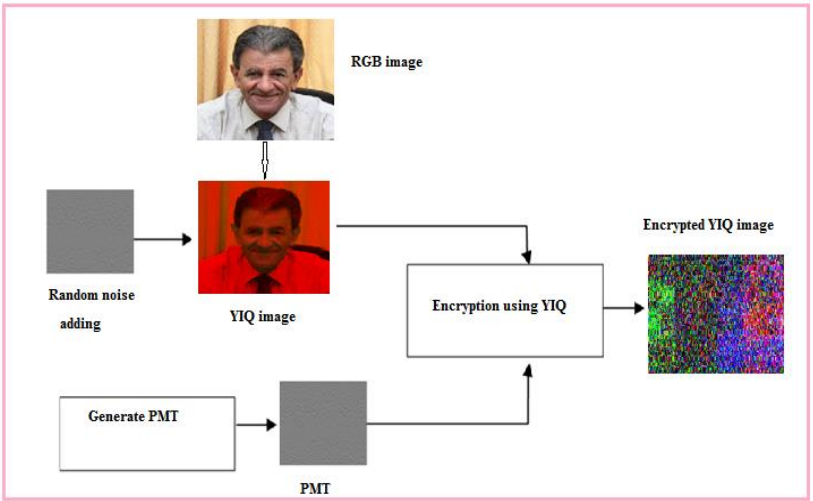

Figure 5: Encryption phase

a) Initialization:
This phase is to be implemented once, the random signal must be generated and saved to be used as a private key, and this key can be updated from time to time.
b) Get RGB color image.
c) Convert the image to YIQ image.
d) Reshape YIQ image matrix to one raw matrix.
e) Load PK.
f) Adopt PK to suit the image size.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

g) Add PK to the raw matrix.
h) Divide the received matrix into partitions.
i) Create PMT.
j) Reorder the partitions.
k) Reshape back the raw matrix to get encrypted YIQ image.
l) Convert YIQ image to RGB image to get the encrypted RGB color image.

The decryption phase as shown in figure 6 can be implemented applying the following steps:

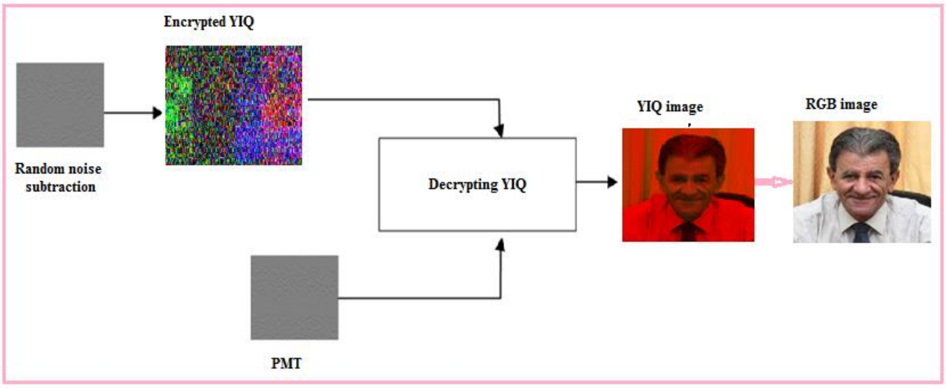

Figure 6: Decryption phase

a) Get Encrypted RGB color image.
b) Convert the image to YIQ image.
c) Reshape YIQ image matrix to one raw matrix.
d) Get PMT
e) Divide the received matrix into partitions as in PMT.
f) Reorder the partitions as in PMT.
g) Load PK.
h) Adopt PK to suit the image size.
i) Subtract PK from the raw matrix.
j) Reshape back the raw matrix to get decrypted YIQ image.
k) Convert YIQ image to RGB image to get the decrypted RGB color image.
l)

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed method was implemented using the images shown in table 1:

Table 1: RGB color images information

Image	1	2	3	4	5	6	7	8	9	10	11	12
Resolution (pixel)	50283	518400	1713600	1442070	40755	172800	50325	50325	50451	630000	2039752	50292
Size (byte)	150849	172800	5140800	4326210	122265	518400	150975	150975	151353	1890000	6119256	150876

Figure 7 shows a sample output of the implementation:

Figure 7: Sample output

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

The images were treated using PMT 1 shown in table 2:

Table 2: PMT 1

Partition number	Location	Size	Order after rearrangement
1	1	2000	3
2	2001	5500	5
3	7501	27500	2
4	35001	60000	4
5	95001	Variable depending on image size	1

Table 3 shows the results of implementation:

Table 3: Experimental results 1

Image number	ET	MSE between original And encrypted image	PSNR between original And encrypted image	Throughput (byte per second)
1	0.0050	2.1625e+004	4.8152	37712000
2	0.0160	1.1309e+004	7.6306	30494000
3	0.1620	1.3738e+004	6.7855	31733000
4	0.1360	2.0336e+004	5.0821	31810000
5	0.0070	1.3270e+004	6.9362	17466000
6	0.0190	1.1403e+004	7.5948	27284000
7	0.0080	2.2001e+004	4.7404	18872000
8	0.0090	1.5874e+004	6.1579	16775000
9	0.0070	1.2757e+004	7.1072	21622000
10	0.0610	2.4520e+004	4.2695	30984000
11	0.1960	2.0037e+004	5.1465	31221000
12	0.0070	2.4340e+004	4.3016	21554000
Average	**0.0528**	**1.7601e+004**	**5.8806**	**26461000**

From table 3 we can see that the proposed method satitsfies the requirements of good encryption-decryption processes, the extraction time is significantly small, which leads to increase the method efficiency. The proposed method is highly secure by using two private hard to hack keys. The proposed method provides high deformation and distortion rate by providing a small value of PSNR and a high value of MSE between the orignal and the encrypted images. The caculted PSNR between the original and decrypted images was always infinte (while the MSE was always zero), which means that the proposed method is highly reliable.

The proposed method was tested also using another PMT shown in table 4, and the proposed method perfprmance remain excellent as shown in table 5.

Table 4: PMT 2

Partition number	Location	Size	Order after rearrangement
1	1	1000	3
2	1001	13000	8
3	14001	50000	7
4	64001	10000	2
5	74001	15000	6
6	79001	5000	5
7	85001	6000	4
8	91001	Variable depending on image size	1

Table 5: Results using PMT 2

Image number	ET	MSE between original And encrypted image	PSNR between original And encrypted image	Throughput (byte per second)
1	0.0080	2.1620e+004	4.8162	18856000
2	0.0200	1.1305e+004	7.6322	25920000
3	0.1610	1.3738e+004	6.7854	31930000
4	0.1360	2.0333e+004	5.0827	31810000
5	0.0070	1.3272e+004	6.9355	17466000
6	0.0190	1.1398e+004	7.5967	27284000
7	0.0080	2.1978e+004	4.7450	18872000
8	0.0070	1.5872e+004	6.1586	21568000
9	0.0070	1.2758e+004	7.1070	21622000
10	0.0620	2.4521e+004	4.2694	30484000
11	0.1930	2.0037e+004	5.1464	31706000
12	0.0080	2.4346e+004	4.3005	18859000
Average	**0.0530**	**1.7598e+004**	**5.8813**	**24698000**

V. CONCLUSION

A method for RGB color image encryption-decryption was proposed, implemented and tested, the experimental results showed that this method is efficient, highly secure, and provides a high level of protection. The proposed method satisfies the requirements of a good method of image encryption-decryption and it is easy and simple to be adopted in any computer application that deals with secret images.

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.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 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 Modelling, Tijuana, 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.