IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 4, April 2020

Simple and Highly Secure, Efficient and Accurate Method (SSEAM) to Encrypt-Decrypt Color Image

Prof. Ziad Alqadi[1], Dr. Mohammad S. Khrisat[2], Dr. Amjad Hindi[3], Dr. Majed Omar Dwairi[4]

Albalqa Applied University, Faculty of engineering technology, Jordan, Amman[1, 2, 3, 4]

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 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, SSEAM, decryption, secret key, secret range, encryption time, efficiency measures, speedup, and throughput, MSE, PSNR.

I.INTRODUCTION

Digital color image [1], [2], [3], [4] is a 3D matrix, the first channel as shown in figure 1 represents the red color, the second represents the green color, while the third one represents the blue color [5], [6], [7]. Each element in each channel has a value between 0 and 255 [8], [12] and mixing the 3 values will give a color pixel as shown in figure 2. Getting the image matrix we can easily manipulate it [13], [14], here we can deal with each channel separately at other channels [15], [16], and we can combine the color image from the three channels as shown in figure 3 [19], [21].

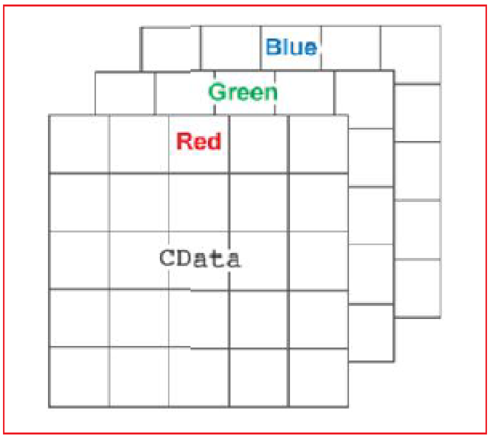

Figure 1: 3D color image matrix

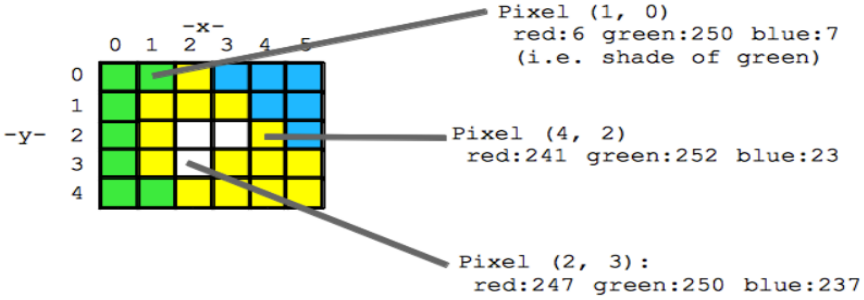

Figure 2: Mixing the colors to get a color pixel

 DOI 10.17148/IJARCCE.2020.9413

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 4, April 2020

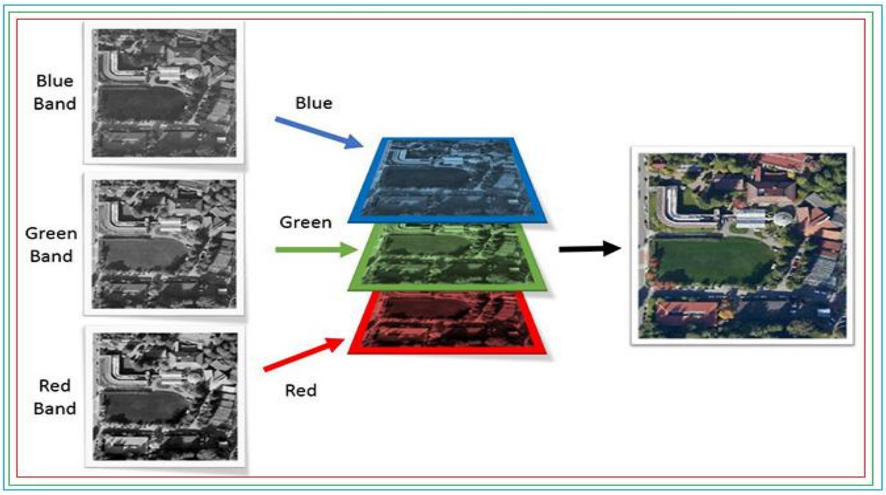

Figure 3: Combing the three color channels

We can also reshape the 3D image matrix to 2D or even convert it to speech signal by reshaping the 3D image matrix to one or two column matrix [17], [18], [20].

The digital image is considered one of the most important types of data, as it may contain confidential information that is ethical in it or that it has privacy, and it is necessary to prevent anyone who is not authorized to view it [6], [9], [10], [11]. The digital image has many important uses. For example, the digital image is used in banking systems and in police systems and these systems require good protection [22]. Therefore, we had to search for a safe way to encrypt the image and prevent any person or entity not authorized to understand the image or retrieve the hidden data in it [23].

1- Existing encryption decryption methods

Digital color image encryption means destroying the digital image so that it does not become understandable to seeing with the eye, and the original is not retrieved without obtaining the method and information with which the image encryption process was performed. As for the decryption, it means retrieving the original image without losing any of the information, so that the retrieved image is completely identical to the original image.

Any good method for color image encryption-decryption must have the following features [240, [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].

Many methods of color image encryption-decryption were proposed, some methods were based on matrix multiplication [30], other methods used blocking feature and xoring [31], [32], [33], [35], [41], in [34] a method based on image scrambling was introduced, while in [36],[38] the authors used logistic maps to encrypt-decrypt the image. 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 a comparisons with the proposed here method.

II.THE PROPOSED SSEAM

The proposed SSEAM for color image encryption will be applied implementing the following phases:

Phase 0: Initialization

In this phase we have to generate a huge secret key which is capable to cover any high resolution image (in our experiment we use a key of 1000x1000x3 matrix), this key must be reshaped to one raw matrix, and saved. This key must be known only by the sender and the receiver, and it is subjective to be changed any time needed.

Phase 1: Encryption phase

This phase can be implemented applying the following tasks:

1) Get the original image.
2) Get the image size.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 4, April 2020

3) Reshape the image into one raw matrix.
4) Get the secret key
5) Select the segmentation ranges (the ranges are to be kept in secret) (in our experiments we used one range to form a 3 segments).
6) Divide the raw image into variable in length segments using the selected ranges.
7) Invert each segment values.
8) Apply segment XORING with the associated key extracted from the secret key.
9) Reshape the raw matrix into 3D matrix to get the encrypted color image.

Phase 2: Decryption phase
This phase can be implemented applying the following tasks:
1) Get the encrypted color image.
2) Get the image size.
3) Reshape the image matrix into one raw matrix.
4) Get the secret key.
5) Get the ranges.
6) Divide the raw matrix into variable segments according the ranges.
7) XOR each segment with the associated part from the secret key.
8) Invert the values of each segment.
9) Reshape the raw matrix into 3D matrix to get the decrypted image.

Figure 4 illustrates the proposed method layout:

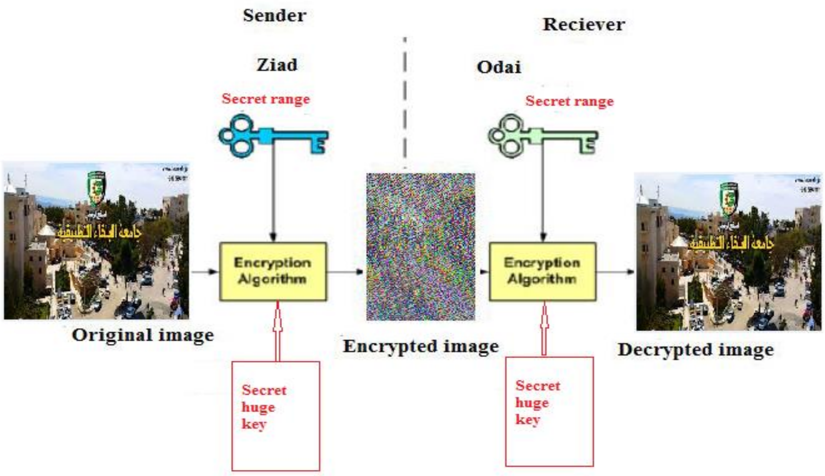

Figure 4: Proposed SSEAM of encryption-decryption

2- Implementation and experimental results

The proposed method was implemented using various images; figure 5 shows the results of image segmentation using one range, while figure 6 shows an example of original, encrypted and decrypted images.

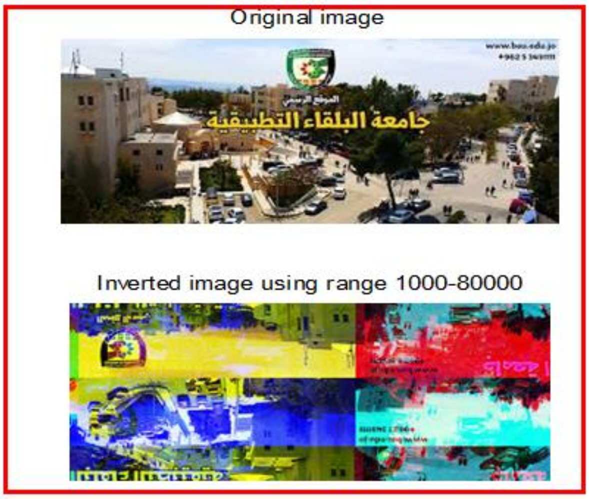

Figure 5: Inverted image using one range

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 4, April 2020

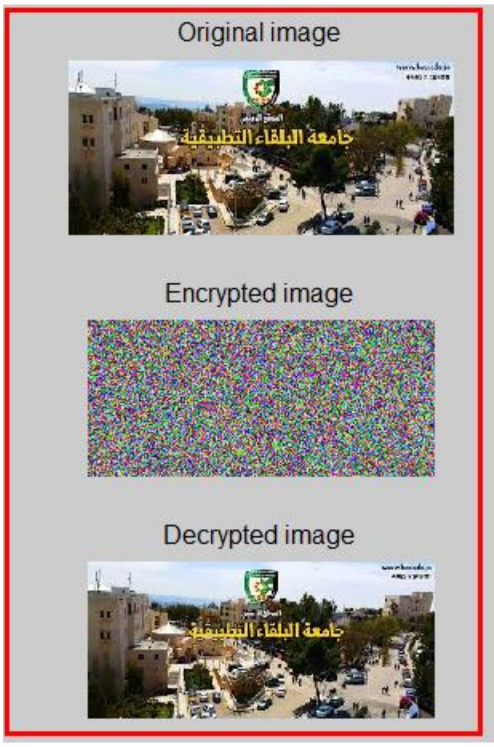

Figure 6: Generated images (example)

Experiment 1: Using different ranges to encrypt-decrypt the same image
A color image with size 151 X 33 X 3(150849 byte) was taken and treated using the proposed SSEAM varying the secret range, table 1, shows the experimental results:

Table 1: Experiment 1 results

Range	Encryption time (seconds)	Decryption time (seconds)	MSE between original and encrypted image	PSNR between original and encrypted image	Throughput(M byte per second)
500-30000	0.0020	0.0020	12716	16.3188	71.9304
1000-40000	0.0020	0.0020	12813	16.2429	71.9304
2000-50000	0.0020	0.0020	12811	16.2449	71.9304
5000-60000	0.0020	0.0020	12797	16.2556	71.9304
10000-90000	0.0020	0.0020	12782	16.2672	71.9304
1000-50000	0.0020	0.0020	12789	16.2619	71.9304
11000-120000	0.0020	0.0020	12708	16.3255	71.9304
30000-130000	0.0020	0.0020	12703	16.3294	71.9304
6000-125000	0.0020	0.0020	12729	16.3089	71.9304
Average	0.0020	0.0020	12761	16.2839	71.9304

From table 1 we can see that SSEAM destroy the original image giving a high MSE and a LOW PSNR values, and the method has a good performance by having a small encryption time and high throughput value, the obtained MSE between the original and the decrypted images was always 0, while the PSNR was always infinite which means that there no lose of information and the decrypted image is identical as the original image.

Experiment 2: Taking various images with range equal 1000-80000
In this experiment we took several image and apply the encryption-decryption phase using the same secret key, table 2 shows the implementation results of this experiment:

Table 2: Experiment 2 results

Image number	Size in byte	Encryption time (seconds)	MSE between original and encrypted image	PSNR between original and encrypted image	Throughput(M byte per second)
1	150849	0.0020	12716	16.3188	71.9304
2	518400	0.0090	11009	17.7604	54.9316
3	518400	0.0070	12094	16.8206	70.6264
4	150975	0.0020	11234	17.5587	71.9905
5	150975	0.0020	9451.8	19.2857	71.9905
6	151353	0.0030	12174	16.7551	48.1138
7	1890000	0.0290	11476	17.3451	62.1533
8	2500608	0.0380	12121	16.7986	62.7570
Average	753945	0.0115	11534	17.3304	64.3117

From table 2 we can see that the proposed method satisfies the following:

- 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 MSE and maximizing PSNR between the original image and the decrypting one, so the decrypted image is completely identical to the original image.
- 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.

The obtained results were compared with other methods result, and the proposed method has a good improvement as shown in table 3:

Table 3: Methods comparisons

Method	Encryption time (s)	Decryption time (s)	Throughput (Mbits)	Speedup of the proposed method	Order
Proposed SSEAM	0.0115	0.0115	64.3117	`1	1
Ref. [27]	0.0513	0.0513	29.2398	4.4609	2
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

III.CONCLUSION

SSEAM 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.
[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.