Indonesian Journal of Electrical Engineering and Computer Science
Vol. 9, No. 3, March 2018, pp. 771~777
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v9.i3.pp771-777

Using Encryption Square Keywith One-dimensional Matrix for Enhancing RGB Color Image Encryption-Decryption

Mohammad Rasmi AL-Mousa[1], Fadi Al-salameen[2], Khaled Al-Qawasmi[3]
[1]Department of Software Engineering, Zarqa University, Zarqa, 13132, Jordan
[2]Department of Computer Science, Zarqa University, Zarqa, 13132, Jordan
[3]Department of Internet Technology, Zarqa University, Zarqa, 13132, Jordan

Article Info

Article history:

Received Oct 19, 2017
Revised Dec 30, 2017
Accepted Jan 21, 2018

Keywords:

Decryption
Encryption
Matrix multiplication
RGB color image
Square key

ABSTRACT

Recently, the security of digital images becomes an important issue with the rapid growth of digital communication and multimedia application. Recent cryptography algorithms are providing essential techniques to protect information and multimedia data. However, those algorithms are usually suffering from the problem of time-consuming. Encryption algorithms have been growth quickly and many image encryption methods have been used to protect information and multimedia data from unauthorized access. This research presents effective technique for image encryption which employs Red, Green and Blue (RGB) components of the RGB color image. The proposed technique utilizes matrix multiplication and inverse matrices for encryption-decryption purpose. Moreover, the effectiveness of the proposed encryption-decryption techniques lay on minimizing the encryption-decryption time and the square error between the original and the decrypted image. The evaluations of the proposed technique were done using many images with different sizes, while the ex perimental results show that the improved encryption technique time are greatly reduced compared with "RGB Color Image Encryption-Decryption Using Gray Image" method. The proposed technique has a high confidentiality level through using confusion diffusion sequentially with a square matrix key and two vectors keys. However, those keys are generated randomly and make the process of hacking the image very difficult.

Corresponding Author:

Fadi Al-salameen,
Department of Computer Science,
Zarqa University, Zarqa, 13132, Jordan
Email: fadi_islam@yahoo.co.uk

1. INTRODUCTION

Multimedia security has become one of the most important aspects of communications with the increasing volume of digital data transmission. In addition, some applications, such as transmitting digital images and videos, this may be used in many applications. In general, images have been widely used in our life. That concept ends up with the more widely we use image, the more necessary their security will be. Image security has become a prime concern in the current computer world [1-4]. The essential things that a security has to achieved are: integrity availability, confidentiality (CIA) [4-6]. In order to provide real-time and reliable security for digital images and videos, many different encryption algorithms have been proposed to make networked continuous media secure from potential threats such as hackers and eavesdroppers[4-7].

The most of proposed encryption algorithms are characterized by considerable imbalance between security and efficiency [8-10]. In addition, some of them are efficient enough to fulfill the real-time requirements, but they have a limited level of security. On the other hand, some are able to meet security demands adequately, but they have limited encryption efficiency.

In this work, set of enhancements are applied to reduce the time that was spent by [8] and to improve the results of [11].The main goal of this paper is to propose a new techniques which enhance the time of color image encryption – decryption. The proposed techniques are minimizing the encryption-decryption time and the square error between the original and the decrypted image. Furthermore, the proposed technique maintains the encrypted color image confidentiality.

The rest of this paper is structured as follows: Section 2 summarizes the related work. Section 3 introduces the proposed technique. Section 4 describes the implementation of the proposed technique. In section 5, we evaluate the results of the experiments. Finally, in the last section, we present the conclusion and future work.

2. RELATED WORKS

Security issues in multimedia technology have become very important. The level of security required depends on the sensitivity of the information in these applications. Moreover, some applications require a suitable secure transmission system, and achieving secure multimedia transmission over the network is currently receiving a lot of attention from the research community [9, 12-15]. With the dramatic increase in the use of multimedia applications, the exponential increase in security incidents. Recently, there is still a lack of appropriate image encryption algorithms as mentioned in [16].

The existing image encryption techniques can be classified into three major categories: position permutation, value transformation, and the combination form between position permutation and value transformation. The position permutation algorithms scramble the data position within the image itself and usually have low security. On the other hand, the value transformation algorithms transform the data value of the original signal and have the potential of low computational complexity and low hardware cost. Finally, the combination forms perform both position permutation and value transformation and usually have the potential of high security. In recent years, a number of different image encryption schemes have been proposed in order to overcome image encryption problems. A few image encryption techniques suggested recently are discussed within this section

In 2015 [13] proposed an algorithm to encryption iris image, based on Advanced Encryption Standard algorithm (AES). AES Algorithm is a kind of groping encryption algorithm with changeable block plaintext length and key length. AES is a symmetric encryption algorithm which using the same key for encryption and decryption.The proposed algorithm [13] was compared with scrambling encryption effect of the classic Arnold, The experiment results show that the image encryption security gained by the proposed algorithm of [13] is higher than Arnoled algorithm.

Mrunali [15] proposed a colored image encryption technique using visual cryptography scheme. The main advantage of visual cryptography that's eliminates the complex computation problem in decryption process, while the secret images can be restored by starching operation. This property makes visual cryptography useful for the low computation load requirement. Also, the proposed technique had a process on color image to grayscale image, and then he created the shares of binary image and encrypting those shares using the shared keys. On the other hand, the decryption is just the reverse of the encryption process.

An algorithm was proposed in [14] applies scrambling and substitution processes, that is the proposed algorithm provides more uniform histogram which is different from plain image histograms. The proposed algorithm [14] works in two phases; scrambling phase and substitution phases shown in Figure 2.

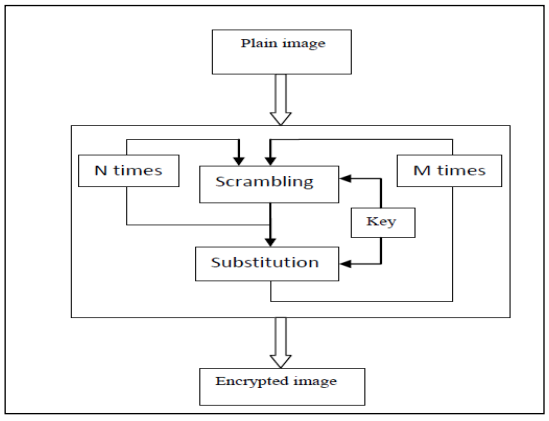

Figure 1.RGB Color Image Encryption Phase R'G'B' Model [14]

A colored image encryption and decryption algorithm proposed by [17] is based on Arnold transformation. The proposed algorithm depends on the encryption key instead of relying on the period of transformation time. Thus, the decryption time of the proposed algorithm is independent of the transformation time, but it's only decided by the encryption time.

Many encryption-decryption algorithms rely on changing the physical location of the image pixels or the changing the pixels values, but the proposed algorithm by [17] changes the physical location of pixels and pixels values as well.

The advantage of the proposed algorithm of [17] that it's more conspicuous when the size of the image is bigger. However, the simulation results show when the size of the image is bigger the encryption-decryption time is reduced. Moreover, the proposed algorithm changes the original image statistical characteristics and makes the image pixels values uniformly distributed in the entire value space.

The proposed algorithm of [16] implemented security for image, by considering reading the image pixels and convert it into pixels matrix of order as height and width of the image. Then, replacing those pixels into some fixed numbers, while the secret key was generated using random generation technique. Theproposed algorithm is based on Ceaser Cipher algorithm, random generation technique, concept of shuffling the rows i.e. rows transposition and Huffman Encoding. Encryption and Decryption of an image by this algorithm protect the image from an unauthorized access.

The image encrypting in [16] was performed using a secret key that is generated from random generation technique, performing random transposition on encrypted image, converting it into one dimensional encrypted array and finally applied Huffman coding on that array, due this size of the encrypted image is reduced and image is encrypted again .The decryption is reverse process of encryption. Hence the proposed method [16] provides a high security for an image with minimum memory space.

Because of the inherent characteristics of chaotic systems, the chaos-based encryption seems not a good choice for secure image encryption, [18] proposes a transposing and scrambling image encryption algorithm based on improved hyper-chaotic sequence to provide enhanced security for encrypted image transmission. The algorithm processes the hyper-chaotic sequence according to the pixel information, which makes the keys sensitive to original image. Then scrambling and transposing operations were applied to the pixels in image, according to separate scrambling keys and gray scale transposing keys.

The proposed algorithm [18] was transposing and scrambling image encryption algorithm based on hyper-chaotic sequence. The transposing encryption [18] meets the Kerckhoff's principle, because it is irreversible, and the security is completely dependent on the key sequence. Moreover, the statistical result of encrypted image in [18] is closer to uniform distribution than the original image and the distribution of the original pixels is concealed, which prevents attackers from getting image information through histogram analysis.

A non-chaos based image, simple, fast and secured against any attack encryption scheme was proposed by [19] using an external key of 144-bits is presented. The proposed encryption scheme uses both pixel substitution as well as pixel permutation process. Furthermore, a feedback mechanism is also applied to avoid differential attack and make the cryptosystem more robust. The proposed encryption scheme has high encryption rate, requires less computation and sensitive to small changes in the secret key so even with the knowledge of the approximate key values, there is no possibility for the attacker to break the cipher.

Three processes were used in the proposed algorithm [19]: key mixing process, substitution process and permutation process. In the key mixing process; two kinds of key mixing processes called FKM and BKM are used in the proposed algorithm. In the both processes i.e. FKM and BKM, the image block is divided into sub-blocks and each sub-block is modified by using sub-key, its previous sub-block and sub-block itself. A similar process is used in the BKM process.

The proposed system by [20] carried out pixel position permutation by using Lorenz, chen, and LU. The proposed system has two stages; confusion stage and the diffusion stage. In confusion pixel position is scrambled over the entire image by using chaotic system. The chaotic system was controlled by initial condition and controlled parameters which were derived for 16-bit secret key. Among the three chaotic dynamic system i.e. Lorenz, chen, and LU one is selected by the system parameter which was obtained from the generated secret key. The proposed system had three advantages; bigger key security, small iteration times, and high security analysis.

A new effective method for image encryption was proposed by [21], which employs magnitude and phase manipulation using Differential Evolution (DE) approach. The idea of the proposed work was that encrypted image is obtained by magnitude and phase manipulation of the original image using the secret key. The original image magnitude and phase was uniquely retrieved from the encrypted image if and only if the key is known. This idea makes the cryptosystem secure.

The Authors of [21] carried out the two dimensional (2-D) keyed discrete Fourier transform on the original image, resulting in the first level of image encryption by the use of the secret key. Secondly, a

crossover operation was performed on the two components of the encrypted image, which are selected based on Linear Feedback Shift Register (LFSR) index generator. Crossover make more shuffling to the positions of image pixels leading to fully distorted encrypted image. The LFSR index generator initializes it seed with the shared secret key value to ensure the security of the resulting indices.

The histogram of the cipher image is significantly different from that of the original images, and bears no statistical resemblance to the plain image. On the other hand, it's clear that the histogram of the encrypted image is significantly different from the respective histogram of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

R'G'B' model was proposed by [8, 22, and 23] to convert RGB color image to grey image. The model of [8] can be used also to encrypt-decrypt color image using R'G'B' model and Hue, Saturation, and Intensity (HIS) model. Encryption phase of [8] was implemented using R'G'B' model as shown in figure 2, and decryption phase of [8] was implemented using R'G'B' as shown in figure 3.

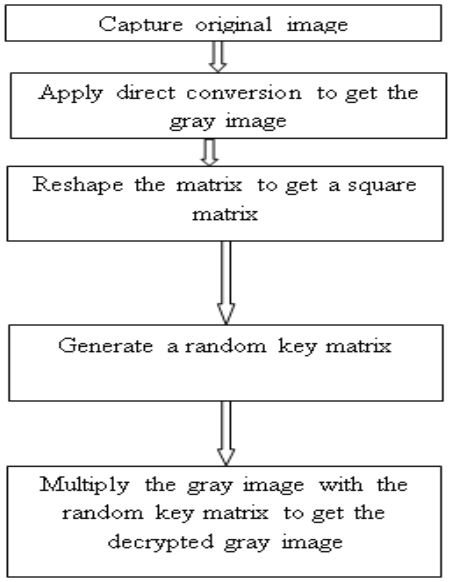

Figure 2. RGB Color Image Encryption Phase R'G'B' Model [8]

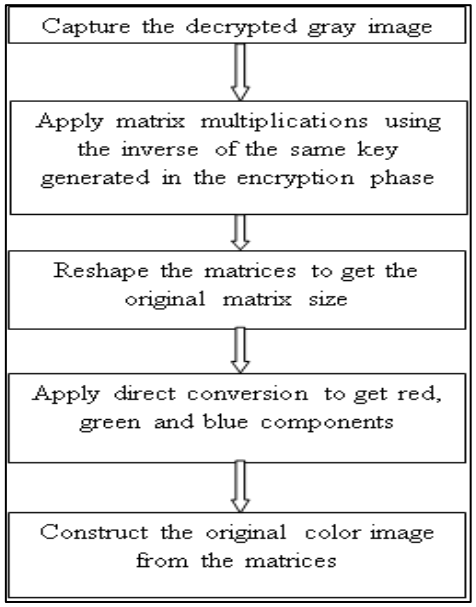

Figure 3.RGB Color Image Decryption Phase Using R'G'B' Model

3. THE PROPOSED TECHNIQUE

The proposed technique is suggested in order to eliminate the conversion from RGB to gray. In addition, the one-dimensional matrix is multiplied with the encryption square matrix key and then the columns and rows order will be changed.The proposed technique implemented into two phases; encryption phase and decryption phase.

The first phase of the proposed technique is the encryption phase which contains the following sequence of steps:

1. Convert the original three-dimensional (RGB) color image with a size (L×W×3) to one-dimensional matrix.
2. Generate a random square matrix key (EK) with a size (W×W).
3. Generate a random vector key (RK) with a length that equals the length of the one-dimensional matrix with unique values varies from 1 to the length of the one-dimensional matrix.
4. Generate a random vector key (CK) with a width that equals the width of the one-dimensional matrix with unique values varies from 1 to the width of the one-dimensional matrix.
5. Multiply the one-dimensional matrix with EK key.
6. Change the rows order of the result matrix in step 5 according to RK key.
7. Change the columns order of the result matrix in step 6 according to CK key.

The second phase of the proposed technique is the decryption phase which contains the following sequence of steps:

1. Change the columns and rows order of the encrypted image according to CK and RK keys.
2. Multiply the result matrix with EK inverse matrix.
3. Reshape the one-dimensional matrix to three-dimensional (RGB) color image.

4. IMPLEMENTATION

To illustrate the correctness of the proposed technique let us take the following worked example. Let us take the following 20 color pixels (5×4×3) where ″Image(:,:,1) =″ is the red component, ″Image(:,:,2) =″, and ″Image(:,:,3) =″ is the blue component, as shown below:

Image(:,:,1) =

178	175	173	169
178	175	173	169
178	175	173	169
178	175	173	169
176	173	172	169

Image(:,:,2) =

168	165	161	157
168	165	161	157
167	164	161	157
167	164	160	157
167	165	161	156

Image(:,:,3) =

57	54	49	45
57	54	51	45
59	56	53	47
61	56	55	49
62	58	56	51

To encrypt the image:

1. Convert the original three-dimensional to one-dimensional matrix.
2. Generate a random square matrix key (EK) with a size (W×W) i.e (4×4).
3. Generate a random vector key (RK).
4. Generate a random vector key (CK).
5. Multiply the one-dimensional matrix with EK key.
6. Change columns order rows order of the result matrix according to CK and RK.

To decrypt the image:

7. Change the columns and rows order of the encrypted image according to CK and RK.
8. Get the encrypted image and multiply it with EK inverse matrix.
9. Reshape the one-dimensional matrix to three-dimensional (RGB) color image.

```
Dec_Image(:,:,1) =
178  175  173  169
178  175  173  169
178  175  173  169
178  175  173  169
176  173  172  169
Dec_Image (:,:,2) =
168  165  161  157
168  165  161  157
167  164  161  157
167  164  160  157
167  165  161  156
Dec_Image (:,:,3) =
  57   54   49   45
  57   54   51   45
  59   56   53   47
  61   56   55   49
  62   58   56   51
```

5. RESULTS AND DISCUSSION

A method of [8] was proposed for color image encryption decryption. This method has based on converting color image to grey image then grey image was encrypted. In addition, it was measured for each color image.

Each time MSE was calculated and the results show that in each time of the decrypted image, 100% matches the original image (MSE=0).For performance analysis, the required total time for encryption-decryption was measured for each color image and the results of measuring are listed in Table 1.

Table 1. Encryption-decryption time for the proposed technique

Image size	Encryption time (sec.)	Decryption time(sec.)	Total time (sec.)
183*276*3	0.019869	0.032922	0.052791
164*308*3	0.020085	0.035708	0.055793
186*270*3	0.020403	0.030344	0.050747
225*225*3	0.017683	0.030168	0.047851
214*235*3	0.018194	0.028399	0.046593
333*360*3	0.046512	0.075357	0.121869
183*275*3	0.019788	0.090026	0.109814
300*400*3	0.054724	0.085799	0.140523
198*255*3	0.018708	0.036348	0.055056
160*160*3	0.008378	0.010348	0.018726

The encryption-decryption rate of the proposed technique wascomparedwith the proposed technique [8] that using direct inverse conversion. Table 2 shows the results of comparisonsusingsome images of differentsize.

Table 2. Comparison results between the proposed technique and the proposed technique by [8]

Image size	Encryption speed up using the proposed technique	Decryption speed up using the proposed technique	Total speed up using the proposed technique
183*276*3	4.614575469	2.664904927	7.279480396
164*308*3	6.208414239	4.315167469	10.52358171
186*270*3	3.939812773	2.797389929	6.737202701
225*225*3	2.046994288	1.977360117	4.024354405
214*235*3	2.396174563	1.222895172	3.619069735
333*360*3	6.072303922	1.644638189	7.71694211
183*275*3	4.654032747	2.032268456	6.686301203
300*400*3	6.535651634	3.042937563	9.578589197
198*255*3	3.355195638	1.722323099	5.077518737
160*160*3	1.774767248	5.411577116	7.186344364

The proposed technique enhancedthe RGB color image encryption by 4.159792 times comparing with the “RGB Color Image Encryption-Decryption Using Gray Image” method which developed by [8]. Furthermore, the proposed technique enhanced the RGB color image decryptionby 2.683146 times comparing with the [8].

6. CONCLUSION AND FUTURE WORK

This paper demonstrates the need for enhancing the color image encryption and decryption techniques in terms of time and security. This paper investigate the modern method called "RGB Color Image Encryption-Decryption Using Gray Image" which developed by [8]. Accordingly, this study proposes an effective technique for image encryption. The proposed technique employs Red, Green and Blue (RGB) components of the RGB color image in order to utilize matrix multiplication and inverse matrices for encryption decryption purpose through designing a new color image encryption-decryption technique using encryption square matrix key.

As for future work, we can enhance the encryption-decryption time for the proposed approaches and adds more enhancements to maximum confusion and diffusion of the encrypted image.

ACKNOWLEDGEMENTS

This research is funded by the deanship of scientific research at Zarqa University/Jordan.

REFERENCES

[1] Sukirman, E., Suryadi, M. T., & Mubarak, M. A. (2014).The implementation of henon map algorithm for digital image encryption. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 12(3), 651-656.
[2] S Jayaraman, S Esakkirajan and T Veerakumar, (2010). Digital Image Processing, 3rd Reprint, Tata McGraw Hill.
[3] E. Reinhard, E. A. Khan, A. O. Akyüz, and G. M. Johnson, (2008). Color Imaging: Fundamentals and Applications. Wellesley: AK Peters Ltd.
[4] Rasmi, M., & Al-Qawasmi, K. E. (2016). Improving Analysis Phase in Network Forensics by Using Attack Intention Analysis. *International Journal of Security and Its Applications*, 10(5), 297-308.
[5] Bosworth, S., &Kabay, M. (2002). Computer Security Handbook. New York: John Wiley & Sons.
[6] Bradley, T., &Carvey, H. (2006). Essential Computer Security. Rockland, MA: Syngress Pub.
[7] Elminaam, D S Abd; Kader H M Abdual, Hadhoud, M Mohamed (2010). Evaluating the Performance of Symmetric Encryption Algorithms, *International Journal of Network Gollmann, D*. (1999). Computer Security. Chichester: Wiley.
[8] Ahmad A.M Sharadqah. (2015), RGB Colored image Encryption-Decryption Using Gray Image, *International Journal of Computer Science, IJCSI*.1694-0784.
[9] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.
[10] Prasetio, B. H., Setiawan, E., & Muttaqin, A. (2015). Image Encryption using Simple Algorithm on FPGA. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 13(4), 1153-1161.
[11] Mohammad Rasmi, Fadi Al-salameen, M. Al-Laham, & Anas Al-Fayomi (2016). Enhancing RGB Color Image Encryption-Decryption Using One-Dimensional Matrix, The 17th *International Arab Conference on Information Technology (ACIT'2016)*, Beni-Mellal, Morocco, 2016.
[12] Khodadadi, T., Islam, A. M., Baharun, S., & Komaki, S. (2016). Evaluation of Recognition-Based Graphical Password Schemes in Terms of Usability and Security Attributes. *International Journal of Electrical and Computer Engineering*, 6(6), 2939.
[13] Xie, R, Wang, M., & Hai, B. (2015), Image Encryption Research Based on Key Extracted from Iris Feature, IJSIA, 9(6), 157-166.
[14] Kumar, M. Chahal, A. (2014), An Image Encryption Technique to Remove the Drawback of the One-Dimensional Scrambling Method of Image Encryption, *International Journal of Computer Applications*, 97(12), 18-22.
[15] Mrunali T. Gedam. (2014), Image Encryption Technique Based on Visual Cryptography, *International Journal of Research (IJR)*, Vol-11, No.1.
[16] T Bhaskara; Yaragunti, Hema Suresh; Reddy, T Sri Harish; Kiran, S.(2013), An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique *International Journal of Computer Technology*, 4.6883-891.
[17] Jinping Fan, Yonglin Zhang. (2013), Colored image Encryption and Decryption Based on Journal of Computer Applications, 97(12), 18-22.
[18] YU, M. (2013), Image Encryption Based on Improved Chaotic Sequences, *Journal Of Multimedia*, 8(6).802-808. http://dx.doi.org/10.4304/jmm.
[19] K Pareek, N. (2012), Design and Analysis of a Novel Digital Image Encryption Scheme, Key Generation Method Using Image Features, *Journal of Information Technology*.
[20] Sankaran, K., Krishna, B. (2011), A New Chaotic Algorithm for Image Encryption and Decryption of Digital Colored images, *IJIET*, 137-141.
[21] S I Abuhaiba, I., & A S Hassan, M. (2011), Image Encryption Using Differential Evolution. Approach in Frequency Domain, an International Journal, 2(1), 51-69.
[22] Waheeb, A. and ZiadAlQadi. (2009), Gray Image Reconstruction. Eur. J. Sci. Res., 7:167173.
[23] M.AL-Laham, M. (2015). Encryption-Decryption RGB Color Image Using Matrix Multiplication. *International Journal of Computer Science and Information Technology*, 7(5), 109-119. http://dx.doi.org/10.5121/ijcsit.2015.7508.