Enhancing RGB Color Image Encryption-Decryption Using One-Dimensional Matrix

Mohammad Rasmi[1], Fadi Al-salameen[2], Mohamad M. Al-Laham[3], Anas Al-Fayomi[4]

[1]*Depart*ment of Software Engineering, Zarqa University, Zarqa, 13132, Jordan

[2]*Depart*ment of Computer Science, Zarqa University, Zarqa, 13132, Jordan

[3]MIS Department, Al-Balqa Applied University,Salt,19117, Jordan

[4]ISD, UNRWA, Amman, Jordan

Abstract: *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 experimental 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*.

Keywords: *RGB color image, encryption, decryption, matrix multiplication.*

1. Introduction

In the last ten years, it is noticed that using of computer networks is growing rapidly across the world; in addition, a lot of data has been transmitted over World Wide Web (www). The data is not only text, there are several types of data such as: image, audio, and other multimedia. But 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 [14, 15]. The essential things that a security has to achieved are: integrity availability, confidentiality (CIA) [17, 18].

Many cryptographic algorithms are available for securing information (E.g. RSA, DES, AES etc). Recently, encryption techniques provide the basic technology for building secure multimedia system. 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[16..18].

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 by [2]. However, the most of proposed encryption algorithms are characterized by considerable imbalance between security and efficiency [1,3]. 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.

Most of these enhancements were concerned to delete any redundant operation and exhaustive search. These enhancements should make the algorithm faster but without reducing the correctness of the algorithm.

In this work, set of enhancements are applied to reduce the time that was spent by [1].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 proposed technique utilizes matrix multiplication and inverse matrices for color image encryption-decryption. However, the proposed technique minimizes the color image encryption-decryption time and the square error between the original color image and the decrypted color image.

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

There are many ways in which Cryptography can protect images. The image is decryption and encryption so that it can be read only by authorized receivers. In order to protect digital images from unauthorized users doing illegal modifications, many of image encryption schemes have been proposed. 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 [4] 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 [4]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[4] is higher than Arnoled algorithm.

However, according to the definition of the scrambling degree which is used to calculate the scrambling degree for image encryption through, the proposed algorithm [4] and Arnold algorithm. The proposed algorithm [4] has larger scrambling degree; because the histogram of the proposed algorithm is flatter than Arnold algorithm that means image encryption security of the proposed is higher than Arnold algorithm.

Mrunali [5] 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 [6]applies scrambling and substitution processes, that is the proposed algorithm provides more uniform histogram which is different from plain image histograms. The proposed algorithm [6] works in two phases; scrambling phase and substitution phase. The scrambling phase had the following steps:

1. Apply interchanging operation among rows with the help of key.
2. Apply interchanging operation among columns with the help of key.
3. Operate circular rotation on all rows with the help of key.
4. Operate circular rotation on all columns with the help of key.

On the other hand, the substitution had the following steps:

1. Convert image matrix to one-dimensional array.
2. Pick 50 pixels in sequence and convert into bits.
3. Apply the XOR operation on these bits with a key of 400 bits.
4. Apply a circular shift operation on the result of step 3 with the help of key.
5. Take the complement of key
6. Apply again XOR operation on the result of step 4 and the complement of key.
7. Decompose the resulting 400 bits of step 6 into 50 segments. Each segment will have 8 bits.

8. Convert each segment to equivalent decimal number. These decimal numbers are encrypted pixels.
9. Replace these encrypted pixels with the old pixels in one-dimensional array.
10. Pick next 50 pixels and repeat step from 3 to 9.
11. If 50 pixels are not available for encryption in the last, then pick the rest pixels and repeat from 3 to 9. But this time key will have the number of bits that will be equal to number of rest pixels multiplied by 8.
12. Convert one-dimensional array into two-dimensional matrix having the same dimension as original image.

A colored image encryption and decryption algorithm proposed by [7] 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 [57] changes the physical location of pixels and pixels values as well.

The advantage of the proposed algorithm of[7] 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 [2] 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. The proposed 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 [2] 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 [2] 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, [8] 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 [8] was transposing and scrambling image encryption algorithm based on hyper-chaotic sequence as the following

1. Reform the original hyper-chaotic sequence with the original image information.
2. Perform separate scrambling operation based on separate scrambling key sequence to image pixels to disrupt the distribution of image pixels; where three times of scrambling operation could achieve the desired result.
3. Perform transposing operation to the gray scale of image pixels, which is to apply modulo addition transformation to the pixels and then perform ex-junction to the result of previous operation and the gray scale transposing key sequence.

The transposing encryption [8] 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 [8] 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 [9] 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 [9]: 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 substitution process in [9] is done using bitwise operations which are performed on the pixels of the sub-blocks to change their properties. Finally, in the pixel permutation process; the pixel's positions of sub-image are scrambled within itself using a special procedure to scramble the pixel's position by applying the following pixel swapping function to sub-image.

However, a new chaotic algorithm for digital image encryption and decryption was proposed by [9], Because chaotic image encryption image algorithms suffers from weak security, i.e. small key space and it's one dimensional crypto system, authors developed a new image encryption schema based on three chaotic system; Lorenz; chen , and LU.

The proposed system by [10] 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.

On the hard, the diffusion step was carried out by modifying the shuffled pixel values sequentially using the sequence generated from the three dynamic chaotic systems.

The proposed system in [10] had three advantages; bigger key security, small iteration times, and high security analysis.

The decryption process in [10] is reverse process of encryption. The diffusion is removed first by using the 16-bit secret key then confusion removed using another 16-bit secret key.

A new effective method for image encryption was proposed by [11], 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 [11] 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 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 [1, 12, and 13] to convert RGB color image to grey image. the model of [1] can be used also to encrypt-decrypt color image using R'G'B' model and Hue, Saturation, and Intensity (HIS) model. Encryption phase of [1] was implemented using R'G'B' model according to the following steps as shown in figure 1:

1. Capture the original color image.
2. Apply direct conversion using mathematical model to extract red, green, and grey images.
3. Resize the gray image matrix to get a square matrix.
4. Generate a random matrix key with a size that equals the resized grey image matrix.
5. Multiply the square grey matrix with the generated key matrix to get the encrypted grey image.
6. Resize the image to the original size.
7. Apply inverse conversion to reconstruct the encrypted color image.

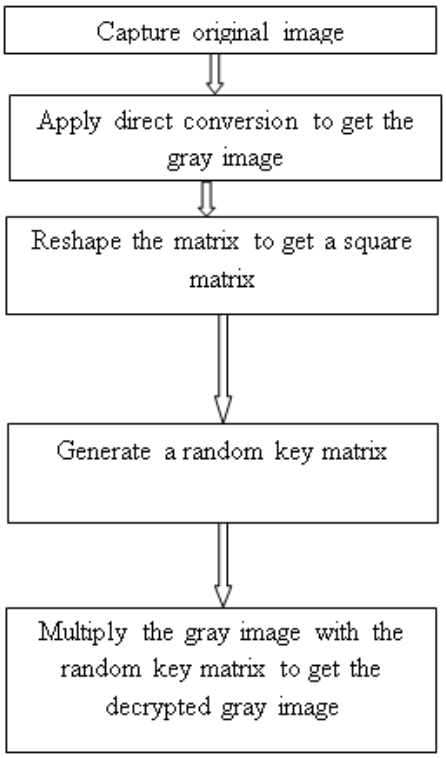

Figure 1.RGB Color Image Encryption Phase R'G'B' Model [1]

Decryption phase of [1]was implemented using R'G'B' according to the following steps as shown in figure 2:

1. Capture the decrypted color image.
2. Use mathematical model to extract red, green, and grey images (apply direct conversion).
3. If the grey matrix is not square, resize the matrix.
4. Multiply the grey matrix with the inverse matrix key matrix to generate the encrypted grey image.
5. Resize the image using the original color image size.
6. Apply inverse conversion to reconstruct the decrypted color image.

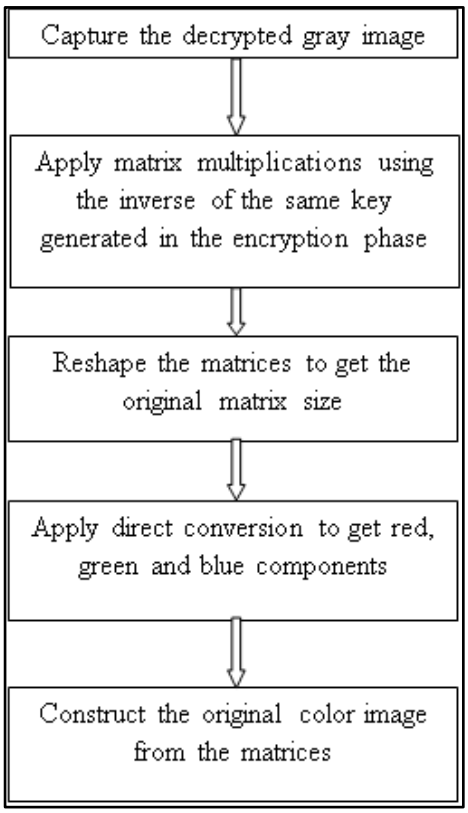

Figure 2.RGB Color Image Decryption Phase Using R'G'B' Model [1]

3. The Proposed Technique

The proposed technique is suggested in order to eliminate the conversion from RGB to gray and it's 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
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. Change the rows order of the one-dimensional matrix according to RK key.
6. Change the columns order of the result matrix in step 5 according to CK key.

7. Multiply the result matrix with EK key.

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

1. Get the encrypted image and multiply it with EK inverse matrix.
2. Change columns and rows order of the result matrix in step 1 according to CK and RK keys.
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:

- Convert the original three-dimensional to one-dimensional matrix:

178 169 161 54
178 169 161 54
178 169 161 56
178 169 160 56
176 169 161 58
175 168 157 49
175 168 157 51
175 167 157 53
175 167 157 55
173 167 156 56
173 165 57 45
173 165 57 45
173 164 59 47
173 164 61 49
172 165 62 51

- Generate a random square matrix key (EK) with a size (W×W) i.e (4×4):

0.1909 0.5895 0.2518 0.8244
0.4283 0.2262 0.2904 0.9827
0.4820 0.3846 0.6171 0.7302
0.1206 0.5830 0.2653 0.3439

- Generate a random vector key (RK):

[8 14 2 11 12 6 10 13 9 1 7 15 5 4 3]

- Generate a random vector key (CK):

[1 4 2 3]

- Change the rows and columns order of the one-dimensional matrix according to RK and CK:

175 53 167 157
173 49 164 61
178 54 169 161
173 45 165 57
173 45 165 57
175 49 168 157
173 56 167 156
173 47 164 59
175 55 167 157
178 54 169 161
175 51 168 157
172 51 165 62
176 58 169 161
178 56 169 160
178 56 169 161

- Multiply the result matrix with EK key:

155.5428 270.9120 204.1627 372.2872
140.4231 211.7077 175.1791 331.5049
157.9903 276.0079 207.5039 378.5790
138.7097 208.8556 173.5733 326.9290
138.7097 208.8556 173.5733 326.9290
154.3118 270.3919 203.6180 369.0868
156.3251 269.8286 204.2651 373.2426
139.3254 210.0893 174.0676 328.8518
156.3993 271.3644 204.7436 374.2526
157.9903 276.0079 207.5039 378.5790
155.1683 270.8443 204.1989 371.0522
141.6913 212.5382 176.3905 333.7200
159.3214 275.7336 208.1620 380.8609
158.7262 275.8773 207.8195 380.2005
158.8468 276.4603 208.0848 380.5444

To decrypt the image:

- Get the encrypted image and multiply it with EK inverse matrix.

Where EK inverse equals:

-12.4548 9.7051 -4.5799 11.8502
-2.8788 2.1304 -2.0401 5.1456
6.6370 -6.9629 5.4624 -7.6135
4.1289 -1.6443 0.8511 -4.0986

And the result of multiplication is:

175 53 167 157
173 49 164 61
178 54 169 161

173 45 165 57
173 45 165 57
175 49 168 157
173 56 167 156
173 47 164 59
175 55 167 157
178 54 169 161
175 51 168 157
172 51 165 62
176 58 169 161
178 56 169 160
178 56 169 161

- Change columns and rows order of the result matrix according to CK and RK keys.

178 169 161 54
178 169 161 54
178 169 161 56
178 169 160 56
176 169 161 58
175 168 157 49
175 168 157 51
175 167 157 53
175 167 157 55
173 167 156 56
173 165 57 45
173 165 57 45
173 164 59 47
173 164 61 49
172 165 62 51

- 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 [1] 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 and the results of measuring are listed in Table 1.

Table 1.Encryption-decryption time for the proposed technique by [1]

Image size	Encryption time (sec.)	Decryption time (sec.)	Total time (sec.)
183*276*3	0.091687	0.087734	0.179421
164*308*3	0.124696	0.154086	0.278782
186*270*3	0.080384	0.084884	0.165268
225*225*3	0.036197	0.059653	0.09585
214*235*3	0.043596	0.034729	0.078325
333*360*3	0.282435	0.123935	0.40637
183*275*3	0.092094	0.182957	0.275051
300*400*3	0.357657	0.261081	0.618738
198*255*3	0.062769	0.062603	0.125372
160*160*3	0.014869	0.055999	0.070868

The method of [1] has some disadvantages such as:

1. The red and green components obtained in direct conversion phase must be saved, because they are used to construct the color image in inverse conversion phase.
2. The saved components in the previous disadvantage require an extra memory space.
3. The saved components in 1 require an extra time for data transmission.
4. The red and green components obtained in direct conversion phase must be sent and they are not secure.

Taking these disadvantages into consideration we can conclude that the proposed method is not secure and there is no need to apply direct and inverse conversion.

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 2.

Table 2.Encryption-decryption time for the proposed technique

Image size	Encryption time (sec.)	Decryption time (sec.)	Total time (sec.)
183*276*3	0.053058	0.028311	0.081369
164*308*3	0.019292	0.036199	0.055491
186*270*3	0.017635	0.090094	0.107729
225*225*3	0.015099	0.023772	0.038871
214*235*3	0.016024	0.021182	0.037206
333*360*3	0.046076	0.071606	0.117682
183*275*3	0.018003	0.079245	0.097248
300*400*3	0.047738	0.076285	0.124023
198*255*3	0.017306	0.027277	0.044583
160*160*3	0.008093	0.011722	0.019815

The encryption-decryption rate of the proposed technique was compared with the proposed technique [1]that using direct inverse conversion. Table 3 shows the results of comparisons using some images of different size:

Table 3.Comparison results between the proposed technique and the proposed technique by [1]

Image size	Encryption speed up using the	Decryption speed up using the	Total speed up using the proposed

	proposed technique	proposed technique	technique
183*276*3	1.72805232	3.098936809	4.826989129
164*308*3	6.46361186	4.256636924	10.72024878
186*270*3	4.558208109	0.94217151	5.500379619
225*225*3	2.39731108	2.509380784	4.906691864
214*235*3	2.720668997	1.63955245	4.360221447
333*360*3	6.129763868	1.730790716	7.860554584
183*275*3	5.115480753	2.308751341	7.424232094
300*400*3	7.49208178	3.422442158	10.91452394
198*255*3	3.627007974	2.29508377	5.922091744
160*160*3	1.837266774	4.777256441	6.614523215

6. Conclusions 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[1]. 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.

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.

References

[1] Ahmad A.M Sharadqah. (2015), RGB Colored image Encryption-Decryption Using Gray Image, International Journal of Computer Science, IJCSI.1694-0784.

[2] 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.

[3] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.

[4] Xie, R, Wang, M., & Hai, B. (2015), Image Encryption Research Based on Key Extracted from Iris Feature, IJSIA, 9(6), 157-166.

[5] Mrunali T. Gedam. (2014), Image Encryption Technique Based on Visual Cryptography, International Journal of Research (IJR), Vol-11, No.1.

[6] 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.

[7] Jinping Fan, Yonglin Zhang. (2013), Colored image Encryption and Decryption Based on Journal of Computer Applications, 97(12), 18-22.

[8] YU, M. (2013), Image Encryption Based on Improved Chaotic Sequences, Journal Of Multimedia, 8(6).802-808. http://dx.doi.org/10.4304/jmm.

[9] K Pareek, N. (2012), Design and Analysis of a Novel Digital Image Encryption Scheme, Key Generation Method Using Image Features, Journal of Information Technology.

[10] Sankaran, K., Krishna, B. (2011), A New Chaotic Algorithm for Image Encryption and Decryption of Digital Colored images, IJIET, 137-141.

[11] 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.

[12] Waheeb, A. and ZiadAlQadi. (2009), Gray Image Reconstruction. Eur. J. Sci. Res., 7:167173.

[13] 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.

[14] S Jayaraman, S Esakkirajan and T Veerakumar, (2010). Digital Image Processing, 3rd Reprint, Tata McGraw Hill.

[15] E. Reinhard, E. A. Khan, A. O. Akyüz, and G. M. Johnson, (2008). Color Imaging: Fundamentals and Applications. Wellesley: AK Peters Ltd.

[16] 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.

[17] Bosworth, S., &Kabay, M. (2002). Computer Security Handbook. New York: John Wiley & Sons.

[18] Bradley, T., &Carvey, H. (2006). Essential Computer Security. Rockland, MA: Syngress Pub.