A New Technique to Encrypt-Decrypt Digital Color Images Using One-Dimensional Matrix

Khdega A.Yosef Galala

kdebh@yahoo.com

Department of Computer Science, College of Education, Al Jufrah University, Libya

Received: 22 April 2018 / Accepted: 6 May 2018

A B S T R A C T

Due to digital technologies, the usage of images in modern industrial life is increasing rapidly. Therefore, the security of digital image has been a major issue in the modern digital world. Image encryption methods are one of the strong techniques recommended in this domain. These techniques try to convert an image to another image that is difficult to recognize and to understand. This art aims fundamentally to achieve the storage and transmission of image securely over the network. In this study a new image security technique is presented. As first step, the new technique extracts the red, green, and blue (RGB) components from the original color image. Then the XOR operation is used to change the RGB values of each pixel and then the RGB pixel positions are also changed randomly according to the key matrix. MATLAB R2012a was used to get the experimental results. The evaluation of this technique was done using some color images which differ in size and type. Simulation results show that, the performance of the proposed technique is high and the original image was retrieved without any distortion.

Keywords: image encryption; image decryption; color images; network security.

1 Introduction

In recent years, with the explosive growth of both computer and internet technology, a huge amount of sensitive and valuable data is being exchanged over unsecured networks. Data not just text it also includes digital images, video, graphical objects, audio and other the multimedia data [1]. Digital image is the most important multimedia data, it is widely used for many aspects of our daily life such as online personal photograph album, internet communication, pay-per-view TV, digital signatures legal, medical imaging systems, military image systems, etc [2]. Digital images are sent, treated automatically and shared across the internet. So the protection of these images from unauthorized access is offering a great challenge to governments, individuals and companies alike[3].

To meet this challenge, various image security techniques such as encryption, stenography, secret sharing, watermarking, etc were proposed. Among these all, image encryption (IE) become one of eminent technique especially using over the internet. These techniques try to

convert an image to another image that is difficult to recognize and to understand; while the image decryption is the result of retrieving original image from the encrypted one [4]. Generally, the image encryption applies two basic methods: replacement methods or scrambling methods [5]. Digital image scrambling is a useful method for providing high protection to image data by scrambling image into an unintelligible format [6].

Since 1990s, many existing image encryption techniques have been developed based on scrambling techniques like key based scrambling techniques, Rubik Cube matrix transformation, image scrambling based on 2D, etc [7]. One of them was proposed by [8] to encrypt image by generate random key sequence. Then the rows and columns of the image are scrambled using this key and then circular shifting of the rows and columns are done using the same key. The authors of [5] also uses scrambling method to encrypt the grey level image based on random number generation as matrix. In [9], a new technique based on one-dimensional random scrambling and combined with XOR operation is developed.

Although, there are various image encryption techniques available for executing images encryption but, there is still a lack of appropriate techniques for images encryption [10]. So we still need to develop more and more powerful techniques. Therefore, the main goal of this paper is to propose a new image encryption technique based on one-dimensional scrambling method. Thus, the rest of the paper is organized as follows: in section 2 the proposed technique is discussed in details; section 3 focuses on the experimental results of the new technique; section 4 gives explains the features of proposed technique and conclusion is presented in section 5.

2 The Proposed Technique

The new image encryption technique is based mainly on true color images, free from image size and type. It consists of two main phases which are encryption and decryption phase as shown in figure 1 below. The first phase can be described as follows:

2.1 Encryption phase

The proposed method of encryption consists of ten main steps as shown below:

Step 1. Input original color image and get its size.

Step 2. Based on the size of the original image, generate a random single array with unique values varies from 1 to the original image size (i.e. If an image is 150×120 then the array will have 18000 elements). Save it as the secret key matrix 'SKM' which will be used later for image scrambling.

Step 3. Extract red 'R', green 'G', and blue 'B' components of the original image.

Step 4. Apply the XOR operation between the red matrix 'R' and the green matrix 'G' to get the new green matrix 'G1' , ' G1= R $\oplus$G '.

Step 5. Apply the XOR operation between the red matrix 'R' and the blue matrix 'B' to get the new blue matrix 'B1', ' B1= R $\oplus$B '.

Step 6. Apply the XOR operation between the red matrix 'R' and the matrix obtained in the previous step to get the new red matrix 'R1', ' R1= R $\oplus$ B1 '.

Step 7. Reshape the three matrices obtained in steps (4,5,6) to three one-dimensional arrays.

Step 8. Scrambling the pixel position in each matrix obtained in the previous step in the order of randomness of SKM key.

Step 9. Reshape each matrix obtained in the previous step to 2-dimensional array which is the same size as the original one.

Step 10. Finally re-combine separate color channels obtained in step 9 into a single RGB color image to get encrypted image.

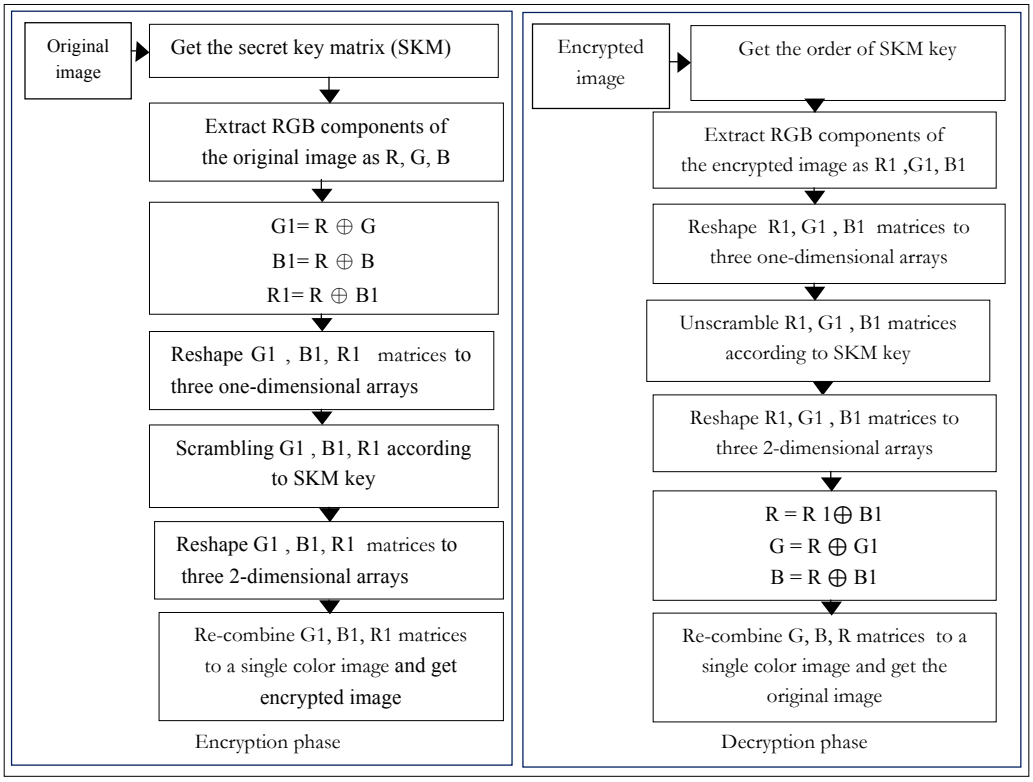

Figure 1: *The proposed technique phases*

2.2 Decryption phase

The decryption stage can be performed according to following steps:

Step 1. Load the encrypted image and get its size.

Step 2. Get the random matrix, sort its elements in ascending order. Get the order of the key matrix by comparing elements of matrix before and after sorting. According to the obtained order of the key matrix 'SKM', we change positions of pixels in the input image to get back the original image.

Step 3. Extract red 'R1', green 'G1', and blue 'B1' components of the encrypted image.

Step 4. Reshape each matrix obtained in the previous step to three one-dimensional arrays.

Step 5. Unscrambling pixels in each matrix obtained in the previous step using SKM key.

Step 6. Convert each matrix obtained in the previous step to 2-dimensional array which is the same size as the original one.

Step 7. Apply the XOR operation between the red matrix‘ R1’ and the blue matrix ‘B1’ obtained in the previous step to get the original red matrix ‘ R’, ‘ R = R1 ⊕ B1’.

Step 8. Apply the XOR operation between the red matrix obtained in the previous step and the green matrix obtained in step 6 to get the original green matrix ‘ G’, ‘G = R⊕G1’.

Step 9. Apply the XOR operation between the red matrix obtained in step7 and the blue matrix obtained in step 6 to get the original blue matrix ‘ B’, ‘B = R⊕B1’.

Step 10. Finally re-combine separate color channels obtained in steps (7,8,9) to a single RGB color image to get back the original image.

3 Experimental Results

The simulation of the above technique has been achieved by using MATLAB R2012a. The test images applied in this work was analyzed using histogram and operational speed of technique. The details of those processes as described below:

3.1 Histogram

At this stage, two images were used in this performed analysis. They are 300 * 300 RGB image named ‘Ahmed Al Bashir’ and 600 * 450 RGB image named ‘ Tree’. Figure 2 and figure 5 show the original images with the histogram of each channel of the original color image. Figure 3 and figure 6 show encrypted images with the histogram of each channel of the encrypted color image while figure 4 and figure 7 show the decrypted images with the histogram of each channel of the decrypted color image.

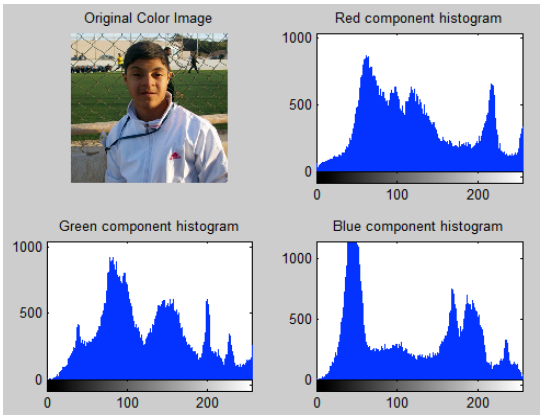

Figure 2: *Original image of Ahmed*

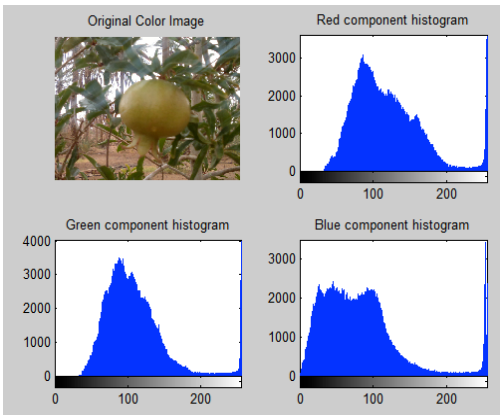

Figure 5: *Original image of tree*

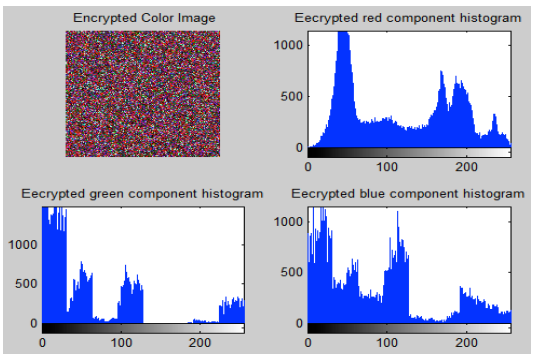

Figure 3: *Encrypted image of Ahmed*

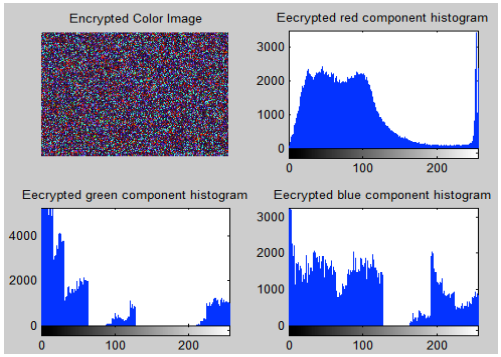

Figure 6: *Encrypted image of tree*

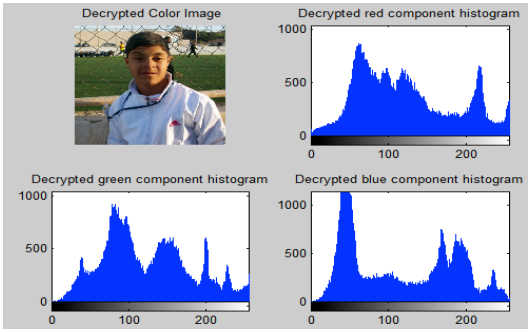

Figure 4: *Decrypted image of Ahmed*

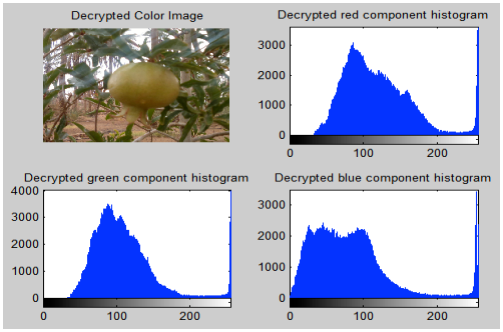

Figure 7: *Decrypted image of tree*

The histogram analysis indicates that, for both images the original image and its encrypted image has different statistics. As we see, the histograms of encrypted images are great different from the histograms of the original images, which will make it difficult to apply any statistical attack on the image encrypted.

3.2 Operational Speed Analysis

This work also measures the CPU time taken by the new technique to encrypt and decrypt color images. Seven different image sizes are selected to be used in this test. Table 1 shows the results of compared the CPU time to encrypt and its decryption for each image.

Table 1: *Consumed time for encryption and decryption processes*

Image size	Encryption time (sec.)	Decryption time (sec.)	Total time (sec.)
259*194*3	0.003495	0.013511	0.017006
276*182*3	0.003214	0.012671	0.015885
299*168*3	0.003232	0.014378	0.01761
300*200*3	0.004063	0.014976	0.019039
300*300*3	0.005545	0.027047	0.032592
600*450*3	0.018416	0.083314	0.10173
940*627*3	0.040704	0.188611	0.229315

As can be seen in the table 1 above, the proposed technique gives the best speed to encrypt and decrypt color images and has been observed a slight increase in execution time of technique with the increase in image size.

The consequences disclose that, the proposed technique was implemented successfully and all original images were recovered without any loss. So it could be used effectively to encrypt any color image.

4 Features

A prominent features of the new technique are:

1. The proposed technique is a very effective and simple technique to encrypt color images.
2. It is adaptable to encrypt images differ in size and type.
3. It has high operation speed to execute both encryption and decryption processes.

5 Conclusions

In this work, a new technique to encrypt digital color images has been introduced. Statistical analysis was done using histograms and operational speed analysis to get the experimental results. Simulation results confirmed that the new technique has been successfully implemented and it could be used effectively for encryption purposes. For the future work the proposed technique could be used to encrypt other images types such as binary images and gray images.

References

[1] W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images, " *Pakistan Journal of Information and Technology*, Vol. 2, pp. 191-200, 2003.

[2] Rojo, M.G., G.B. García, C.P. Mateos, J.G. García and M.C. Vicente, "Critical comparison of 31 commercially available digital slide systems in pathology," *International journal of surgical pathology*, Vol. 14, pp. 285-305, 4 October 2006.

[3] A. Mitra, Y V. Subba Rao and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques, " *Journal of computer Science*, Vol. 1, pp.127, 2006.

[4] Madhu B., Ganga Holi and Srikanta Murthy K., "An overview of image security techiques, " *International Journal of Computer Applications,* Vol.154, pp. 37- 46, November 2016.

[5] Makera M Aziz and Dena Rafaa Ahmed, "Simple image scrambling algorithm based on random numbers generation, " *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 5, pp. 434 - 438, September 2015.

[6] Prarthana Madan Modak and Vijaykumar Pawar, " A comprehensive survey on image scrambling techniques, " *International Journal of Science and Research (IJSR)*, Vol. 4, pp.814 -818, December 2015.

[7] Sandeep Kaur and Sumeet Kaur, "Four level image encryption using scrambling and key based methods, " *IJCSC*,Vol. 3, pp. 187-190, 2012.

[8] P. Premaratne and M. Premaratne, "Key-based scrambling for secure image communication, " *Emerging Intelligent Computing Technology and Applications, P. Gupta, D. Huang, P. Premaratne & X. Zhang, Ed. Berlin: Springer*, Vol. 304, pp.259-263, 2012.

[9] Qiudong Sun, Ping Guan, Yongping Qiu and Yunfeng Xue, "A Novel digital image encryption method based on one-dimensional random scrambling," *9th International Conference on Fuzzy Systems and Knowledge Discovery*, pp. 1669-1672, May 2012.

[10] T. Bhaskara Reddy, Hema Suresh Yaragunti, T. Sri Harish Reddy and S. Kiran, "An effective algorithm of encryption and decryption of images using random number generation technique, " *International Journal of Computer Technology & Applications*, Vol. 4, pp. 883-891, 2013.