Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Simple Image Scrambling Algorithm Based on Random Numbers Generation

**Makera M Aziz***
Business and management Department,
Ishik University, Erbil, Iraq

**Dena Rafaa Ahmed**
Computer Science Department,
Bayan University, Erbil, Iraq

***Abstract— This paper proposed simple algorithm to encrypt and decrypt the grey level image base on the random number generation. The image encrypt by changing the position of each pixel in the original image without changing the value of grey level. The original image reads row by row pixel by pixel each pixel will take a new position in encrypt image. The new position chose based on random number generation from the random number generators. The key will generate during the encryption process. The key that will used to decrypt image, it will generate as a matrix. The key saves the position of each pixel in encrypt image. The encrypted image will decrypt by using the key. Each pixel in encrypt image return back to its first position in decrypt image position that saved in key then the decrypt image builds. The function "Rand" in Matlab is used to generate the random numbers that need to scramble the image.***

***Keywords— Image scrambling, image encryption, random number generation , grey level image, decrypt image***

## I. INTRODUCTION

The importance of digital image security, increased especially after the networking, internet development and modern communication media. Many decryption algorithms studied to develop processes of encryption and decryption [1]. In internet there are much weakness points of attack and the information these transfers throw the network have to be secret and protected against the attacker [2]. The encryption of data is used to transmit data in safety way through the internet and networks [3]. Many research used different algorithm have been proposed in image encryption in last two decades [8-16]. Encryption of imagery means that make the image something that not understanding or not easy to understand [17]. If the hacker catches the image he/she will not know what this image. The image encryption uses two basic methods: replacement methods or scrambling methods. The first one is changing the value of the pixel in the original image. The scrambling is changing the position of the pixel in original image that make the original image difficult to recognize by an attacker. The only user who has the key can access the content of the original image and can rebuild the original image. Scrambling methods based on permuting coordinates of pixels. This kind of methods usually uses the following steps to scramble an image: (1) construct a matrix with the same size of the image to be scrambled (the matrix size is denoted as s) and every element in it is assigned different natural number from 0 to s-1; (2) the generated matrix is mapped to the image matrix row by row and column by column, where every element's value in the generated matrix is as the coordinate of the corresponding pixel in image matrix; (3) move every pixel to the next position, if the mapped pixel coordinate is x, then move the pixel into the position with the mapped coordinate (x+1) mod s. In these methods, the key step is to generate a matrix as Coordinate shifting path. [4].Image is scrambling disarrange pixel position or pixel color in order to make it unrecognizable and finding the algorithm to rebuild the original image. [5] Two types of scrambling one base on 2D matrix transformation and other is based on 2D Arnold transformation [7].Many researchers are studying the different ways and techniques that be used to encrypt the image [8-16]. In this paper new technique has been suggested to encrypt a grey level value image by using transportation technique and scrambling the image pixel.

## II. LITERATURES REVIEW

[8] In this paper, a novel data hiding mechanism based on the application of the Rubik's cubic algorithm is proposed to achieve the aforementioned goals. The characteristic of our proposed data hiding mechanism is that it possesses the advantages of reversibility and good visual quality. The Arnold cat map method is also studied in this paper. A comparative analysis of both the methods is done in this paper.

[9] A new image scrambling concept is proposed in this paper. To encrypt an image with the help of image scrambling method, security of an image is improved by the even better encryption method. That's what is done in this paper by using multi area scrambling concept by choosing various transform coefficients, which creates a dilemma for the attacker & hence leads to difficulty in deciphering the image since we are not using unique transform coefficients. Statistical results and image shows that extended proposed algorithm is more efficient & hence can be used as digital image information hiding tool i.e. for watermarks. For different attacks, it also shows excellent robust effect which does not affect the original quality of an image, hence can also be used in medical image processing. Hence the above proposed method is extensively used because of its simple mathematical structure.

[10] The proposed digital image scrambling algorithm based on chaotic sequence and decomposition and recombination of pixel values is able to simultaneously scramble pixel positions and pixel values of images. Through de- composition and recombination of pixels, the algorithm scrambles pixel positions and change pixel values. During recombination, of pixel values are avoided By conversion of number systems. Apart from disordering pixel positions and changing pixel values, this algorithm is able to disuse errors, i.e. it is capable of spreading the errors in a particular area of the whole image in the form of noise. From the experimental results, we see that our method is indeed resistant to attacks and relatively safe.

[11] used spiral filling of bits to design image scrambling algorithm. The proposed algorithm able to recover the scrambling images without distortion. The scrambling image pixel values have a homogeneous distribution and the pixel value distribution of the recovered images and the original image is the same. Pixel position switching algorithm proposed in this image scrambling. Realize the algorithm is easy with simple, efficient, with low security. But the security of this algorithm can be enhanced by combined with the existing image scrambling method base on pixel grey value transformation.

[12] this method based on unauthorized access to the image by converting it into another format which is difficult to understood by another user except the one who has the authority to use the image. This software gives the authority to the user to keep his images protected which are meant for private purpose. Even the user has the authority and authentication for image usage, the scrambled images are difficult to decode. Hence this application has high security and low complexity of for estimating such a sequence to unscramble the image will be practically impossible because the size of the M-Sequence matrix is larger and random.

In [13] new algorithm proposed base on Rubik's cube rotation and logistic system, it changes the size of the image and partition this image to six blocks the cube is generated this blocks. 25 steps are used to rotate the cube. A chaotic system is used in controlled different methods to rotate these cubes.

In [14] this algorithm changes the grey image to one dimensional vector and does the scrambling on this vector. This algorithm is simple to realize in software and hardware. it will give better result if executed more than one.

In [15] new algorithm suggests it scramble the image on full array and combine the scrambling and LSB algorithm. The experiment shows that the algorithm has high performance on the internet and high performance in information hiding.

In [16] proposed algorithm is used to chaotic map to discretised real value generation. Experimental tests are carried out with detailed numerical analysis, which demonstrates that the proposed scrambling algorithm it's fast and secure.

## III. METHODOLOGY

The methodology of this algorithm will create, encrypt image with a secret key in encrypt process and create decrypt image in decrypting process. Two algorithms are suggested one for the encrypt original image, second is for decrypt image. The original image will read row by row. The encrypted image will build randomly and the decrypt image will rebuild row by row. In encrypt processing two random number generates for each pixel one for the row the range of this number starts from 1 to the total number of rows and the following equation to generate the number from a two b. a=1 and b= total number of rows. (Matlab 2011a is used to generate the random numbers)

n1=round ((b-a). *rand+a);The second number of the columns in the range of these numbers start from 1 to total numbers of columns and the same equation use to generate numbers from 1 to see when c equals the total amount of columns.

The Algorithm that used to encrypt the image include the following steps:

1- Input original image
2- Find the size of the original image (the total number of rows and column)
3- Point to the first pixel in the original image.
4- Let counter equal to 1.
5- Generate new position of the current pixel in the encrypt image by generating two random (n1, n2) numbers, one for row the other for the column.
6- While the new position of encrypt image is generated before go to step 4 otherwise go to step6.
7- Save the value of n1 in the array k1 (counter).
8- Save the value of n2 in the array k2 (counter).
9- The current pixel of the original image will take the position (n1, n2) in encrypt image.
10- While all the pixels of original image finished, go to 13 otherwise go to 10
11- Point the next pixel in the original image.
12- Increment counter by 1
13- Go to step 5
14- End

Decryption algorithm

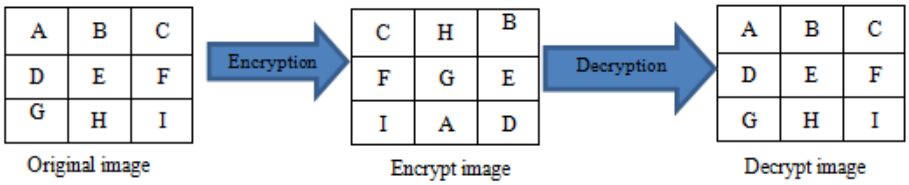
1- Input the encrypt image
2- Input the key k1 & k2
3- Set counter equal to 1
4- Point to the first pixel of the decrypt image
5- n1=k (counter)
6- n2=k2 (counter).

7- Get the value of the position (n1, n2) from the encrypt image and put it in the current position of decrypt image
8- While the counter is not the last position of k1 and k2 go to 9 otherwise go to 13
9- begin
10- Increase counter by one
11- Point to the next pixel of encrypt image
12- Go to 5
13- end
14- end

**Practical example**

To make the algorithm more clear, we will apply an algorithm for this segment of the image the pixel of the original image will scramble to build the encrypt image.




**Explaining of Encryption**

The original image will read row by row. The first pixel in the original image will use to build the first pixel in encrypt image by changing the position. The new position of the pixel will chose randomly by generating two random numbers (n1, n2), when n1 represent the row number for a new position and n2 represent the column number of new positions. In our example the first pixel of the original image in position (1,1) when position is read like (row_number, column_number) include the element "A" ", two random number will generate (n1, n2) in our example "n1=3" and "n2=2" the new position of the element "A" in encrypt image is (2,3). Two arrays (k1, k2) will use to save the new positions for each pixel and they will use as a key in decryption process. The first position of k1 will include the value of n1 in our example k1 (1) = 2. First position of k2 will include the value of n2 in our example k2 (1) = 3. For the next pixel of original image (1,2) (read image row by row) include element "B". Two random numbers generated "n1=1" and "n2=3" the new position of the pixel is (1,3). K1 (2) =1, K2 (2) =3. The same procedure will do for all pixels. We will get:

K1 [3 1 1 3 2 2 2 1 3]
K2 [2 3 1 3 3 1 2 2 1]

**Decryption process**

Initial c=1In this process the decrypt image will build row by row.The first pixel in decrypt image (1,1) will take the value of position (b1, b2) when "b1=k (c) & "b2=k2 (c) " in our example b1=3 and b2=2. The element of position (3,2) in encrypt image is "A". "A" will be the first element of decrypt image position (1,1). Increase c by 1. Built the second pixel of decrypt image in position (1,2). Now c = 2, b1=1 and b2=3, the element of position (1,3) in encrypt image is "B".B will be the second element of decrypt image. Increase c by 1. The same procedure will do for all pixels till last element of k1, k2.

## IV. EXPERIMENT AND RESULTS

The proposed algorithm is implemented by Matlab. Three grey level images with different size and type has been selected. The result of each image implementation are shown in figures (1,2,3)

The image have been selected are shown in table 1:

TABLE I

| Image Name | Image Type | Image Size |
|---|---|---|
| Cameraman | TIF | 256*256 |
| Mandi | TIF | 3039*2014 |
| Lifting body | PNG | 512*512 |

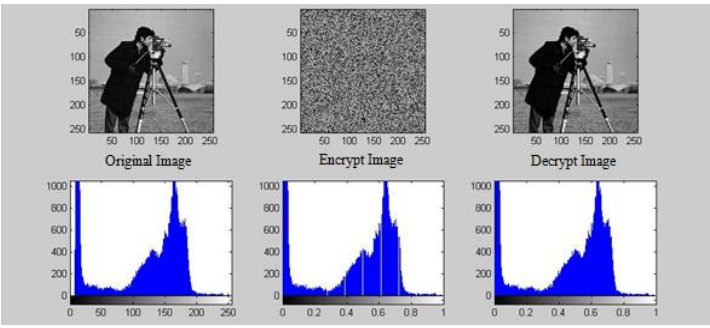



Fig. 1 Result of proposed algorithm implementation on image (cameraman.tif, 256*256)

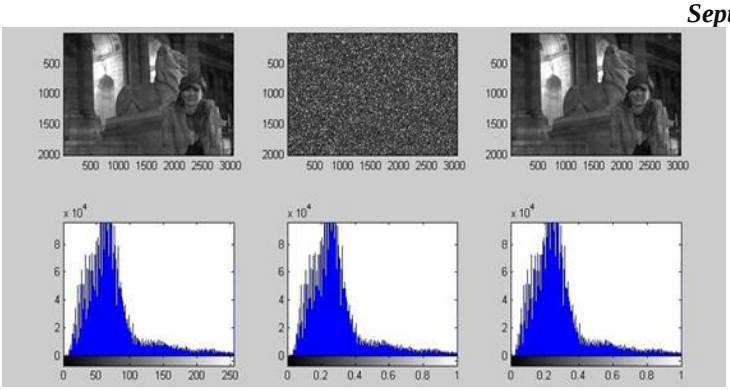


Fig. 2 result of implement the algorithm on image(mandi.tif, 3039*2014)

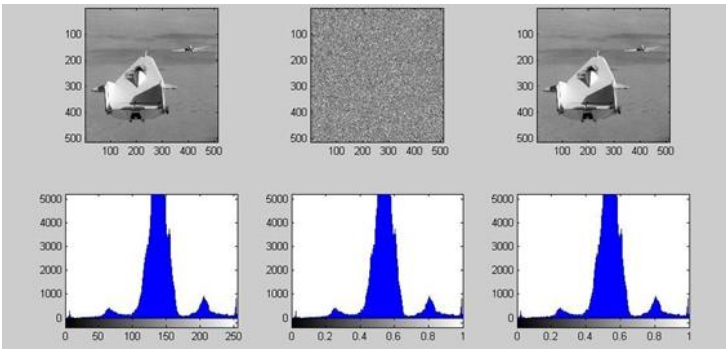


Fig. 3 result of implement the algorithm in (liftingbody.png, 512*512)

From the histogram of each image in three cases (original image, encrypt the image and decrypt image) are showing that there is no change of the grey value only the change in position only. We get the decrypt image without any noise or damage. The algorithm implemented successfully the encrypt image is not understood. The decrypt image is clear without noise.

## V. CONCLUSIONS

This algorithm is used to encrypt and decrypt the grey level image.it reads the original image, then scrambling the pixel position the scrambling methods base on random number generation. The function and in Matlab is used to generate the random numbers.This algorithm can use for different grey level image with different size. The key is represented in a one dimensional array for row and one dimensional array of columns. The decrypt image is clear without any noise. The algorithm is implemented successfully for different image size and types.

## REFERENCES


[1] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic imageencryption method," *Circuits and Systems, IEEE International Symposium on* ,Vol.2 ) , pp.708-711, may. 2002.

[2] V.V.Divya, S.K.Sudha and V.R.Resmy ," Simple and Secure Image Encryption*" International Journal of Computer Science Issues*, Vol. 9, pp. 186-289, November .2012.

[3] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya" A Survey On Different Image Encryption and Decryption Techniques*." International Journal of Computer Science and Information Technologies*, Vol. 4, pp.113-116 , February. 2013.

[4] S.Liping,Qin, Z. Liu Bo, Q. Jun, L.Huan," Image Scrambling Algorithm Based on Random Shuffling Strategy*" 3rd IEEE Conference on Industrial Electronics and Applications*, 2008,pp. 2278 – 2283.

[5] ZHAO Xue-feng, Digital image scrambling based on the baker's transformation. *Journal of Northwest Normal University* (Natural Science),vol.39, pp26-29, February .2003.

[7] D.X. Qi, "Matrix Transformation and Its Applications to Image Hiding*," Journal of North China University of technology*, Vol. 11, pp. 24-28, 1999.

[8] R. Rhine, N.Bhuvan "Image Scrambling Methods for Image Hiding: A Survey", *International Journal of Computer Science and Network Security*, vol.15,pp.86-91, February .2015.

[9] G.Artist, M.Porwa " Dual Layer Image Scrambling Method Using Improved Arnold Transform"*American International Journal of Research in Science, Technology, Engineering & Mathematics*, vol .3, pp. 258-264 , February. 2015.

[10] D.Wang1, C.Chang, Y.Liu, G.Song, and Y.Liu," Digital Image Scrambling Algorithm Based on Chaotic Sequence and Decomposition and Recombination of Pixel Values" , *International Journal of Network Security*, vol.17, PP.322-327, May. 2015.

[11] H.Yuan and L.Jiang " Image Scrambling based on Spiral Filling of Bits" *International Journal of Signal Processing, Image Processing and Pattern Recognition* , vol.8, pp.225-234 , March. 2015.

[12] Anup, Akash, Abhishek, Padmakar, Priyanka, Suchita" A NOVEL APPROACH OF IMAGE SCRAMBLING USING M-SEQUENCE GENERATOR" *International Journal of Application or Innovation in Engineering & Management* , vol3, pp.261-265, March .2014.

[13] X. Feng, X. Tian, S. Xia" An Improved Image Scrambling Algorithm Based On Magic Cube Rotation and Chaotic Sequences",4th International Congress on Image and Signal Processing 2011, pp,1021-1024 .

[14] Qiudong Sun, Ping Guan, Yongping Qiu, Yunfeng Xue," A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling" 9th International Conference on Fuzzy Systems and Knowledge Discovery 2012 ,pp 1669-1672.

[15] L.Anguan, W. Sheng, Z. lie" A New Method for Image Information Hiding Based on Image Scrambling and LSB Technology" International Conference on Computer Application and System Modeling 2010 ,pp 349-355

[16] B.Radu, D. Cristina, P.Iustin and F. Cristina "A New Fast Chaos-Based Image Scrambling Algorithm" 10th international conference on communication , 2014, , pp 1-4.

[17] M. Al-Husainy " A Novel Encryption Method for Image Security*" International Journal of Security and Its Applications,*vol. 6 ,January. 2012.