New Image Encryption Method Based on two Stage Scrambling

Zuhair Hussein ALI
Amal Abbbas Kadhim
Collage of Education
Al-Mustansiriya University

ABSTRACT

The purpose of digital image scrambling technology is to put a meaningful image into a disordered one to enhance the resistance ability against illegal attacks. This paper proposed an image scrambling algorithm based on idea of movement of elephant in the chess board the system consist of two main steps the first one rotate each diagonal by key generated from computing the standard deviation the second step include exchange the upper half of image with the lower half of image the proposed system shows a good result and we reach 100 percent accuracy in decryption thus the proposed system can be used by any application for secure transmitting.

Keywords standard deviation, scramble, Encryption

1-Introduction

The advent of personal computers and the Internet has made it possible for anyone to distribute worldwide digital information easily and economically.

Many applications like military image databases confidential video conferencing, medical imaging system ,cable TV, online personal photograph album, etc. require reliable, fast and robust security system to store and transmit digital images[1]. In this environment, there are several security problems associated with the processing and transmission of digital images over an open network it is necessary to assure the confidentiality, the integrity and the authenticity of the digital image transmitted[2]. Also Encryption of images is different from that of text due to some intrinsic features of images such as redundancy of data, strong correlation among adjacent pixels, being less sensitive as compared to the text data i.e. a tiny change in the attribute of any pixel of the image does not drastically degrade the quality of the image and bulk capacity of data. To meet these challenges, a wide variety of cryptographic protocols have been appeared in the scientific literature [3]. In recent years, amount of research in the field of image encryption system is increasing day by day due to technological progress[4]. Image based cryptosystems are different from textual cryptosystems because of large amount of

correlation observed between adjacent pixels in an image. Currently, greater part of the research based on image encryption is performed using chaotic map[5]. Image scrambling disarranges the position or color of pixel in image and the original image cannot be recognized.
But the operator can rebuild the original image from the disordered image by some algorithms[6]

2-**Related work**

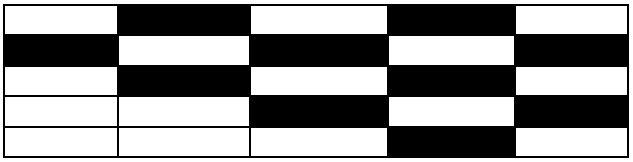
Image scrambling technology includes methods based on Arnold transform, affine transform, magic square transform ,bakers transform, Graycode, generalized Graycode; based on fractal IFS model, Hilbert curve, FASS curve, Tangram algorithm, conway'sgameand knight's touretc. Among these methods, the same characteristic of above Arnold transformation and Fibonacci transform is module operation .These methods spend much time when scrambled[7].

3-Proposed System

The proposed system for image scramble consist of two main stages

A-Stage one

This first stage of scrambling the image which includesthecomputing of standard deviation for each diagonal in the image separately (white and black diagonal as movement of elephant in the chess board)as shown in the figure(1)



Figure(1)

After computing the standard deviation a key is generated to rotate each diagonal this key is generated using

Key=(standard deviation) mod(number of pixels in the diagonal)

This generated key used to rotate the diagonal after rotating the diagonal it put in the same diagonal that for each diagonal there is a unique key generated from the image itself and there is one key to the rotation of diagonal. The following example shows how to implement the first stage of scrambling.

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

Table(1)

Suppose we want to compute the standard deviation for the colored diagonal of the above table first a mean must be computed as follows

Mean=$\sum_{i=1}^{n} xi/n$ Where N representsthe numberof pixels in the diagonal and x represent pixel value

The mean for the colored diagonal= (12+9+3+8) /4=32/4=8

The standard deviation computed as follows

Standard deviation = $\sum_{i=1}^{n}(Xi - mean)^2$

Applying standard deviation to the above diagonal

12	9	3	8

SD=Round((12-8)^2+(9-8)^2+(3-8)^2+(8-8)^2)/4 =(16+1+25)/4=round(10.5)=11

Key=SD mod n= 11 mod 4=3 this key represent the number of rotations to the diagonal the above array will be as follows

8	12	9	3

We apply mod function to get key for rotation less than the length of diagonal sometimes the mod be zero that do not allow rotation to the diagonal in this case the key is computed as follows

Key=(length of diagonal) div 2

The following table shows the details for each diagonal to the above 8*8 table where there are (13) diagonals. The computing starts from the diagonal which consist of two elements (discarding the diagonal with one element because there is no rotation for such diagonal)

Length of diagonal	Mean	Round of Standard deviation	Key
2	12.5	2	1
3	9	11	2
4	8	11	3
5	7	23	2
6	7.5	23	5
7	9.4	19	5
8	9.25	22	6
7	6.7	12	5
6	7.1	7	1
5	6.4	17	2
4	12.2	6	2
3	7.3	18	1
2	3	1	1

Table**(2)**

The above (8*8) table after applying the rotation according to the generated key will be as follows

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

Table(3)

This step represent the endof stage one

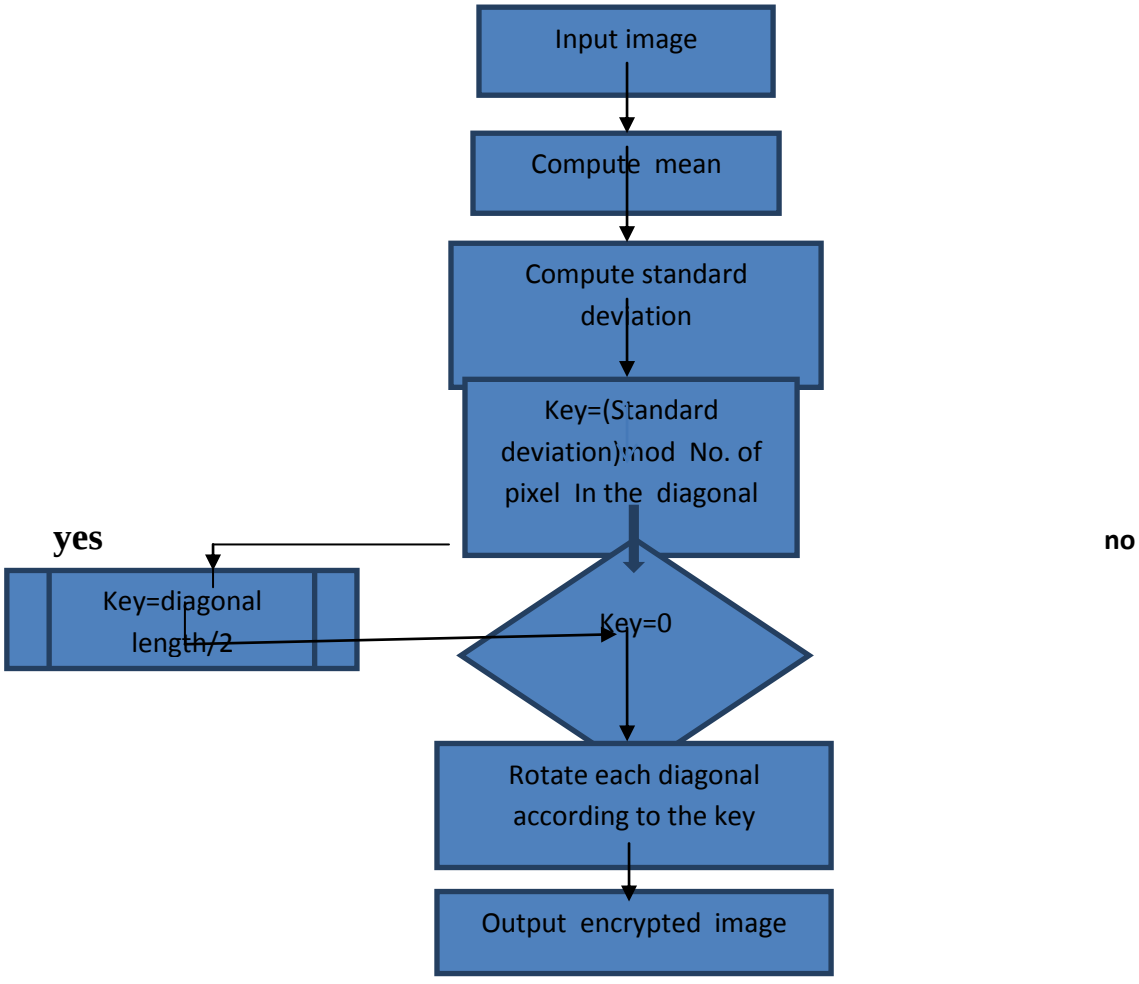
B .Stage two

In this stag which represent a second phase of scrambling the image where the triangle which is above the main diagonal exchange with triangle under the main diagonal each one with it's similar diagonal that for this technique the image must be equal in width and height to implement this stage this process increase the complexity of encryption the image the above table will be as follows after applying the second stage

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

Table(4)

This represent the end of the new proposed system. The following flowchart illustrate the main steps of the proposed system.



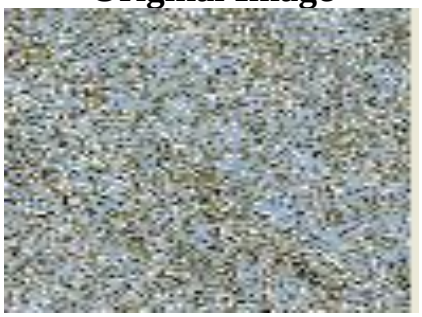
Figure(2)

To retrieve the original image the two stage applied in reverse order when first stage two applied then be exchange the upper and lower of the diagonal then stage one applied by computing the mean ,standard deviation and generate the key as described previously the same key number will generated because the mean and standard deviation for the diagonal remain same but the order of diagonal change after generating a key a rotation to diagonal will done in reverse order this procedure allowed to retrieve the original image without any change.

4. Experimental Results

The image used in the proposed system are colored image

Original Image



Encrypted image

5.Conclusion

1-Applyin the proposed system showed that the original image retrieved without any change because there is no change in the pixels value but only change it's positions in the image.

2-There is a few computation time for scrambling and descrambling the image only required compute mean, standard deviation and rotation of each diagonal.

3-The proposed system gave a good encrypted image which is difficult to be retrieved by any attack.

4- Another statistical computation such variance and skewness may be used toGenerate the key.

5- Generating more than one key from the image itself make it difficult to be discovered

6-The proposed system reach 100 percent in decryption because there is no change in pixel value but only in position

7-One limitation in the proposed system that the image must be of equal in height and width a modification to proposed system can lead to overcome this limitation.

6.References

1-N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN pattern, Pattern Recogn 1992.

2-G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption based on 3D chaotic maps Chaos Solitons Fractal 2004

3-Aaronson, L, "Sudoku Science", IEEE Spectrum, vol.43

pp. 16-17, Feb.2006. .

Li Zhang. The Research and Development of Information Hiding 4-

and Digital Watermarking, Macao: Macao university of Science

and Technology, Faculty of Information Technology, May, 2010

5-Di Xiao, Xiaofeng Liao, Pengcheng Wei. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons, and Fractals, vol.40,pp .2191-2199,2009

6-Cahit Cokal, Ercan Solak. Cryptanalysis of a chaosbased image encryption algorithm. Physics Letters A,

vol. 373,pp. 1357-1360,2009

7-LI Min,FEIYaoping. A New Class of Digital Image Scrambling Algorithm Based on the Method of Queue Transformation. Computer Engineering, 2005

طريقة جديدة لتشفير الصور باستخدام مرحلتين للتزحيف

م. زهير حسين علي م.امل عباس كاظم

الجامعة المستنصرية/ كلية التربية

الخلاصة

الغرض من التزحيف الصوري هو وضع صورة مفهومة إلى صورة غير مفهومة وذلك بتوزيعها من جديدة لتكون غير قابلة للكشف. في هذا البحث تم استخدام طريقة جديدة بالاعتماد على حركة الفيل في رقعة الشطرنج حيث تكون حركته قطرية وتتكون من مرحلتين أساسية المرحلة الأولى تعتمد على تدوير كل قطـــر حسب مفتاح يتم استخراجه بحساب ألانحراف المعياري لذلك القطر وبعد الانتهاء من التدوير لكل الأقطار تبدأ المرحلة الثانية التي تتضمن أبدال النصف العلوي الواقع فوق القطر الرئيسي من النصف السفلي. أظهر النظام المقترح نتائج جيدة وتم الوصول الى نسبة 100 دقة استرجاع الصورة الأصلية يمكن استخدام النظـــام بـــاي تطبيق لنقل المعلومات بصورة سرية.

مفاتيح الكلمات الانحراف المعياري, البعثرة ,التشفير