International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2021.3733

E-ISSN : 2454-6135

Volume.7, No. 10
October -2021

Method of Image Encryption By using Scrambling and Slant Transform

Sally Ali Abdulateef

Department of Computer Science

University of Al-Mustansiriyah

Baghdad- Iraq

ABSTRACT

New image encryption methods such as Stage Scrambling and Slant Transform are allowing images to be scaled in new and powerful ways. The process of scaling image points, taking an average of the points' value and then identifying how many points have changed, can increase the capabilities of image encryption.

Slant Transform image coding possesses a "discrete saw tooth-like basis vector which efficiently represents linear brightness variations along an image line; A fast computational algorithm has been found for the transformation" [1].

Slant Transform is when the first row and column, and last line and column were moved clockwise. The two rows and columns before them were carried out in the same mathematical operations and have been scaled with the rest, while the second line and column, and the line and column before the last were moved counter clockwise. The process was continued in opposite directions to all the lines and columns in the image, where the image is distorted and then applied slant transform in the image.

Keywords: Mean, Encryption, Slant Transformation.

1. INTRODUCTION

The internet has made it possible for anyone and everyone to share digital files and images with ease [2] and in today's world, images play an important role in everyday life. Due to the constant sharing of images across various platforms, security is essential when transferring them across networks. Therefore, various encryption and decryption algorithms are utilized to protect the files from unauthorized access [3]. Security of systems is required in many applications such as medical imaging systems, and highly sensitive images held in military databases. Encryption is used to sustain high levels of security [4]. Encryption is a technique which converts the original image into a form which is hard to understand for any unauthorized user or interceptor. The legitimate end-user is therefore the only user that can access the image via decryption [5]. This is made possible by image scrambling. This process disarranges the position or color of pixels in an image so that the original image cannot be recognized during transfer. However, the operator can rebuild/decrypt the original image from the disordered image by some algorithms [6]. Image-based cryptosystems vary from textual cryptosystems because of the large correlations observed between adjacent pixels in an image. Currently, research into image encryption is increasingly being performed using chaotic mapping [7].

1.1 Related work

Following are the list of similar work carried out in the field of Scrambling and Slant Transform.

- Image scrambling technology includes methods such as:
- Arnold Transform
- Affine Transform
- Magic Square Transform
- Bakers transform
- Gray Code
- Generalized Gray Code; based on fractal IFS model
- Hilbert curve
- FASS curve
- Tangram algorithm
- Conway's Game and Knight's tour

Among these methods, the same characteristic of above Arnold transformation and Fibonacci transform is module operation. These methods spend much time when scrambled [7].

2. PROPOSED APPROACH

In this paper we have initially used Image Scales to scramble and encrypt the image. Then, by using a Slant Transform matrix, we can apply color to the images. After converting the image values into a one-dimensional matrix, the values of the image are scaled with the number of mod values. This is shown in the example below (the type of images used in this work are JPG).

Table 1.

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

3. PROCESS

Part A:

The first movement of values is clockwise as the rest of division one, scales by one.

Computed by using (Mean=$\sum_{i=1}^{n} xi/n$) 220/mod 28 = 7.8

(220 mod 28 = 1), move one step clockwise

Before

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

After

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

Part B:

The counter-clockwise direction scales by the rest of the division

While 163/20 = 8.15 (163 mod 20 = 3), move three step counter clockwise

Before

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

After

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

Part C:

The third movement towards the clockwise

DOI : 10.31695/IJERAT.2021.3733

97 /12=8 (97mod 12= 1) move one step clockwise

Before

6	**11**	**12**	**14**	**2**	**11**	**3**	**7**	**9**	**10**	**3**	**11**

After

11	**6**	**11**	**12**	**14**	**2**	**11**	**3**	**7**	**9**	**10**	**3**

Part D:

The counter-clockwise direction scales by the rest of the division

43/4 = 10 (43 mod 4 = 3) move three step counter clockwise

Before

13	15	7	8

After

8	13	15	7

3.1 Slant Transform

Slant Transform occurs when a value has orthogonal matrices. The value also must have a constant function for the first row, and have a second row which is a linear. The matrices are formed by an iterative construction that exhibits the matrices as products of sparse matrices, which ' in turn leads to a fast transform algorithm. The slant-transform 'matrix of order two consisting of a constant and a slant 'basis vector is given by [8].

Slant Transform

- The N×N Slant transform matrices are defined by the recursion

$$\mathbf{S}_n = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & \mathbf{0} & 1 & 0 & \mathbf{0} \\ a_n & b_n & & -a_n & b_n & \\ \mathbf{0} & \mathbf{I}_{(N/2)-2} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{(N/2)-2} & \\ 1 & 0 & \mathbf{0} & 1 & 0 & \mathbf{0} \\ -b_n & a_n & & b_n & a_n & \\ \mathbf{0} & \mathbf{I}_{(N/2)-2} & \mathbf{0} & \mathbf{0} & -\mathbf{I}_{(N/2)-2} & \end{bmatrix} \begin{bmatrix} \mathbf{S}_{n-1} & \mathbf{0} \\ & \\ \mathbf{0} & \mathbf{S}_{n-1} \end{bmatrix} \qquad \mathbf{S}_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

where $N=2^n$ and $\mathbf{I}_M$ denotes an M×M identity matrix

- Parameters a_n dan b_n are defined by the recursions:

$$b_n = (1 + 4a^2_{n-1})^{-1/2} \qquad a_1 = 1$$
$$a_n = 2b_n a_{n-1}$$

- The 4×4 Slant transformation matrix: $\mathbf{S}_2 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ \frac{3}{\sqrt{5}} & \frac{1}{\sqrt{5}} & \frac{-1}{\sqrt{5}} & \frac{-3}{\sqrt{5}} \\ 1 & -1 & -1 & 1 \\ \frac{1}{\sqrt{5}} & \frac{-3}{\sqrt{5}} & \frac{3}{\sqrt{5}} & \frac{-1}{\sqrt{5}} \end{bmatrix}$

DOI : 10.31695/IJERAT.2021.3733

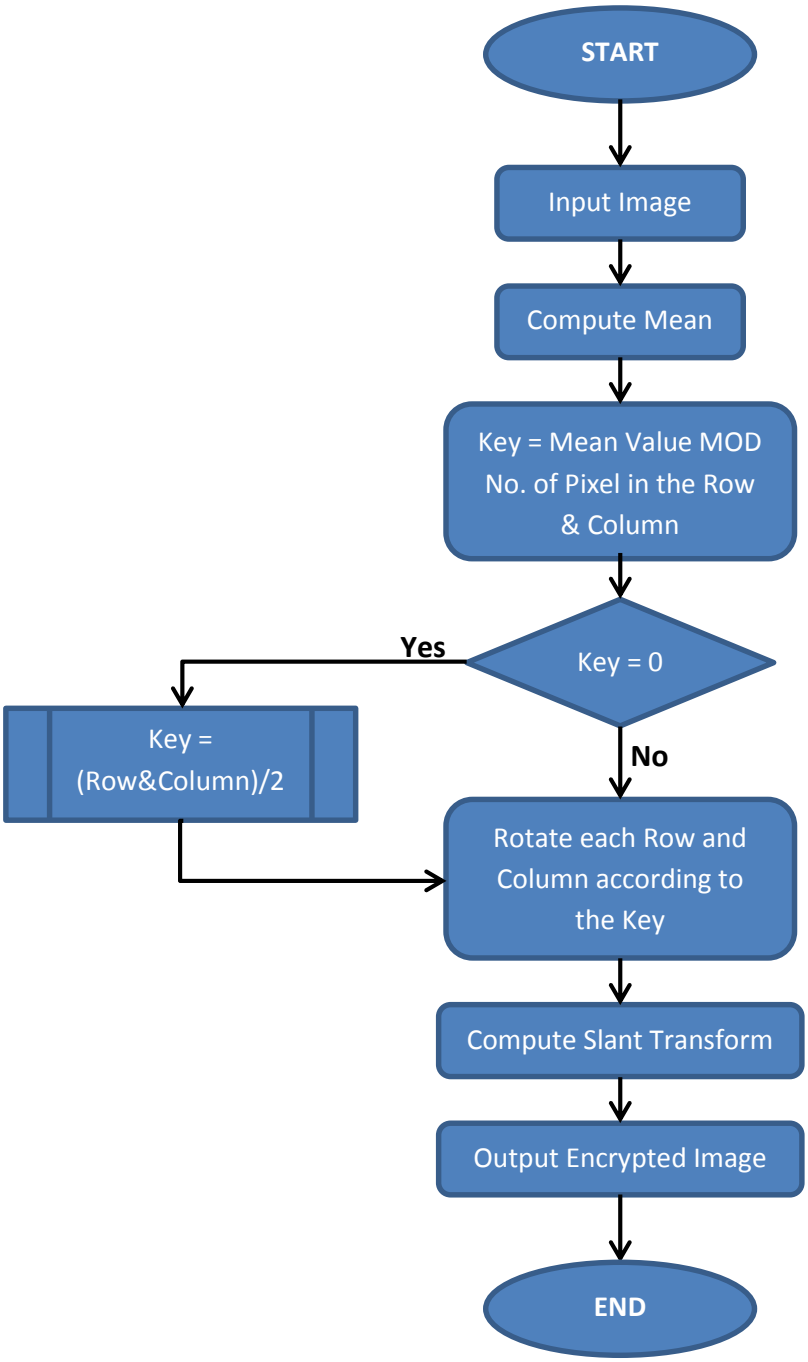


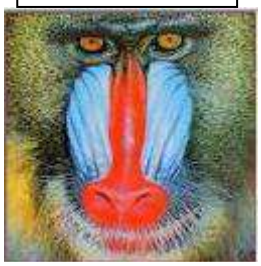
Fig (1): The Image Encryption Flow Chart

DOI : 10.31695/IJERAT.2021.3733

4. EXPERIMENTAL RESULTS

In this paper we have simulated the image processing part of encryption and decryption. First of all we would take an image and then obtain its corresponding matrix. We would then encrypt the image matrix using a modification of the crypto system. The result is shown below.

Original Image



Encrypted Image

5. CONCLUSION AND LIMITATIONS OF THE STUDY

Applying the proposed system demonstrated that the original image was retrieved in decryption without any change. This occurred due to only the positions of the pixels being re-ordered, and the actual value of them remaining constant. The original image was therefore 100% maintained in decryption.

Little computation time is required for scrambling/encrypting and descrambling/decrypting the image at the receiving end of transfer.

The proposed system produced a high quality, encrypted image which would be difficult to be intercepted and understood in an attack or breach of security.

Another statistical computation such variance and skewness may be used to generate the key. Generating more than one key from one image would make it increasingly more difficult to be discovered.

Slant Transform and Seeped method give accurate and high quality results throughout the encryption and decryption process.

One limitation in the proposed system is that the image must be of equal height and width. This limitation can however be eliminated with the introduction of a modification to the system.

REFERENCES

[1] Pratt, William, Wen-Hsiung Chen, and Lloyd Welch. "Slant transform image coding." IEEE Transactions on Communications 22.8 (1974): 1075-1093.

[2] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN pattern, Pattern Recogn 1992.

[3] Dr. Parma and Astya1, Ms. Bhairvee Singh2, Mr. Divyanshu Chauhan3
Image Encryption and Decryption Using Elliptic Curve Cryptography, International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.3, Issue No.10, October 2014 ISSN-2319-8354(E).

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

[5] Noor Dhia Kath Al-Shakarchy1, Hiba Jabbar Al- Eqabie2, Huda Fawzi Al- Shahad. Classical Image Encryption and Decryption, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

[6] Cahit Cokal, Ercan Solak. Cryptanalysis of a chaosbased image encryption algorithm. Physics Letters A,vol. 373,pp. 1357-1360,2009

[7] 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.

DOI : 10.31695/IJERAT.2021.3733

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

[9] Digital Image Processing Fundamentals of Digital Image Processing, A. K. Jain, E. Fatemizadeh, Sharif University of Technology, 2011

DOI : 10.31695/IJERAT.2021.3733