Chaos Image Encryption Using Transposition and Pixel Shuffling

Pratyaksha Ranawat
Department of Computer Science Engineering
Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

Associate Prof. Sarika Khandelwal
Department of Computer Science Engineering
Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

Abstract- **The advent of wireless communications, both inside and outside the home-office environment has led to an increased demand for effective encryption systems. The beauty of encryption technology comes out in more pronounced way when there is no absolute relation between cipher and original data and it is possible to rebuild the original image in much easier way. As chaotic systems are known to be more random and non-predictable, they can be made utilized in achieving the encryption. The transposition technology of encryption systems requires scrambleness behaviour in order to achieve the encryption of the data. This scrambleness behaviour can be derived from the randomness property of chaos which can be better utilized in the techniques like transposition system. In wireless communication systems, bandwidth utilization is an important criterion. In order to use encryption system in wireless communication; key space plays an important role for the efficient utilization of the bandwidth. In this paper we present a chaos based encryption algorithm for images. This algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data. The position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in decryption process. The same algorithm is tested with two different maps and performance analysis is done to select best suited map for encryption.**
Keywords – chaos, Encryption systems, Transposition technique

I. INTRODUCTION

The amazing developments in the field of network communications during the past years have created a great requirement for secure image transmission over the internet. Internet is a public network and is not so secure for the transmission of confidential data. The advent of wireless communications, both inside and outside the home – office environment has lead to an increased demand for effective encryption systems. The beauty of encryption technology comes out in a more pronounced way when there is no absolute relation between cipher and original data and it is possible to rebuild the original image in much easier way. In wireless communication systems, bandwidth utilization is an important criterion. In order to use encryption system in wireless communication key space plays an important role for the efficient utilization of the bandwidth.

II. PROPOSED ALGORITHM

The image used will have its RGB colours extracted and its RGB values transposed to obtain an image which will then be encrypted to obtain ciphered image. The ciphering of the image for this research will be done using the RGB pixel values of the image only.

In this method, there will be no changes of the bit values of the image used and no pixel expansion at the end of encryption and decryption process. The numerical values of the pixels are displaced from their respective positions and the RGB values are interchanged in order to obtain the ciphered image. This implies that, the total change in the sum of all values in the image is zero. Therefore, there is no change in the total size of the image during encryption and decryption process. The images are looked at as a decomposed version in which the three principle components which form the image were chosen to act upon by the algorithm. The R-G-B components were considered as the triplet that forms the characteristics of a pixel. The pixel is the smallest element of an image that can be isolated and still contains the characteristic found in the image.

The RGB values are shifted out of their native pixel positions and interchanged within the image boundaries. The Shift displacement of the R, G and B Values known as the component displacement factor array was different for

the R, G and B. With the proposed method in this paper, the shuffling of the image was ultimately done by solely displacing the RGB pixels and also interchanging the RGB pixel values.

Algorithm for transposition and shuffling of image pixels

Step 1: Start
Step 2: Import data from image and create an image graphics object by interpreting each element in a matrix.
Step 3:Extract the red component as 'r'
Step 4:Extract the green component as 'g'
Step 5:Extract the blue component as 'b'
Step 6:Reshape red into 1-dimensional array as 'p'
Step 7:Reshape green into 1-dimensional array as 'l'
Step 8:Reshape blue into 1-dimensional array as 'y'
Step 9:Let t=[y; l; p] which is a column matrix.
Step 10: Transpose't'
Step 11: Reshape't' into 1-dimensional array
Step 12: Let n= total number of array
Step 13: Let l=(1st part of n): (1/3 rd part of n) as 1-dimensional array
Step 14. Let y= (1/3 rd part of n): (2/3 rd part of n) as 1-dimensional array
Step 15. Let p= (2/3 rd part of n): (nth) as 1-dimensional array
Step 16. Transform l, p, and y from vector to matrix with the same dimension of 'r' or 'g' or 'b' of the original image.
Step 17. Finally the data will be converted into an image format to get the encrypted image.

Mathematical Implementation of the Algorithm

Step 1 : Start.
Step 2 : Importing data from image and creating an image graphics object by interpreting each element in a matrix.
Let Q=an image=Q(R,G,B)
Q is a colour image of m*n*3 arrays

$$\begin{pmatrix} R & G & B \\ ri1 & gi2 & bi3 \\ . & . & . \\ . & . & . \\ . & . & . \\ rn1 & gn1 & bn1 \end{pmatrix}$$

Where Q(R, G, B) = m x n
Where R, G, B ϵ R
(R o G) ij = (R) ij . (G) ij
Where R = r = first value of R
r = [ri1] (i=1, 2, ...m)
$x \epsilon : [a ,b] = \{x \epsilon I : a \leq x \geq b\}$
a = 0 and b = 255
R = r = Q(m, n, 1)
Where G = g = first value of G
g = [gi2] (i=1, 2, ...m)
$x \epsilon : [a, b] = \{x \epsilon I : a \leq x \geq b\}$
a = 0 and b = 255
G = g = Q(m, n, 1)
And B = b = first value of B

b = [bi3] (i = 1, 2, ...m)
$x \epsilon : [a, b] = \{x \epsilon I : a \leq x \geq b\}$
a = 0 and b = 255
B = b = Q(m, n, 1)
Such that R = r = Q(m, n, 1)
Step 3 : Extracting the red component as 'r'
Let size of R be m x n [row, column] = size (R) = R(m x n)

rij = r = Q(m, n, 1) =

$$\begin{pmatrix} R \\ ri1 \\ . \\ . \\ . \\ rn1 \end{pmatrix}$$

Step 4 : Extracting the green component as 'g'
Let size of G be m x n [row, column] = size(G) = g(m x n)

gij = g = Q(m, n, 1) =

$$\begin{pmatrix} G \\ gi2 \\ . \\ . \\ . \\ gn2 \end{pmatrix}$$

Step 5 : Extracting the blue component as 'b'
Let size of B be m x n [row, column] = size(B) = B(m x n)

bij = b = Q(m, n, 1) =

$$\begin{pmatrix} B \\ bi3 \\ . \\ . \\ . \\ bn3 \end{pmatrix}$$

Step 6 : Reshaping red into 1-dimensional array as 'p'
Let size of R be m x n [row, column] = size(R) = R(m x n)

p = rij = r = Q(m, n, 1) =

$$\begin{pmatrix} R \\ ri1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots rn1 \end{pmatrix}$$

Step 7 : Reshaping green into 1-dimensional array as 'l'
Let size of G be m x n [row, column] = size(G) = G(m x n)

l = gij = g = Q(m, n, 1) =

$$\begin{pmatrix} G \\ gi2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots gn2 \end{pmatrix}$$

Step 8 : Reshaping blue into 1-dimensional array as 'y'

Let size of B be m x n [row, column] = size(B) = B(m x n)

y = bij = b = Q(m, n, 1) = B

bi3 .....bn3

Step 9 : Let t = [p; l; y] which is a column matrix

t =

p	l	y
ri1	gi2	bi3
.	.	.
.	.	.
.	.	.
rn1	gn2	bn3

Step 10 : Transpose of 't'
t = t' [p; l; y]

t =

ri1 .....rn1
gi2 .....gn2
bi3 .....bn3

This transposed matrix 't' so obtained acts as the input for the next level of encryption which is using chaos.
This algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data. The position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in the decryption process.
First we convert the matrix t into single array vectors, separating the R, G, B components. We get three vectors. For encryption, we generate elements from chaos map equal to 3 x m x n matrix. In this algorithm we use Henon Map to generate elements. The Henon Map can be generated using the equation give below which is iterated for n = 1 to the number of elements we have in the matrix.
$x(n + 1) = 1 – a * x(n) ^ 2 + y(n)$
$y(n + 1) = b * x(n)$
using the values a = 1.76 and b = 0.1
The table below shows elements generated from Henon Map taking iterations for 'n' from 1 to 27

Table 1

0.819	0.912	1.234	0.486	0.298	0.421	0.581	1.456	1.834
0.412	2.814	3.453	2.166	1.281	1.481	0.893	0.921	0.110
0.234	0.822	1.625	1.435	1.893	1.205	0.891	0.717	0.625

Now divide the generated elements into three blocks. The table below shows how the obtained elements from the previous steps are divided into three separate arrays each of 9 elements.

Table 2

0.819	0.912	1.234	0.486	0.298	0.421	0.581	1.456	1.834

0.412	2.814	3.453	2.166	1.281	1.481	0.893	0.921	0.110

0.234	0.822	1.625	1.435	1.893	1.205	0.891	0.717	0.625

Now sort the elements of each block in ascending or descending order and compare the misorder between the original and sorted elements of each block and tabulate the index change. Following table shows the tabulated values of first block and the index change obtained after arranging them in descending order. This procedure is repeated for all the three colours.

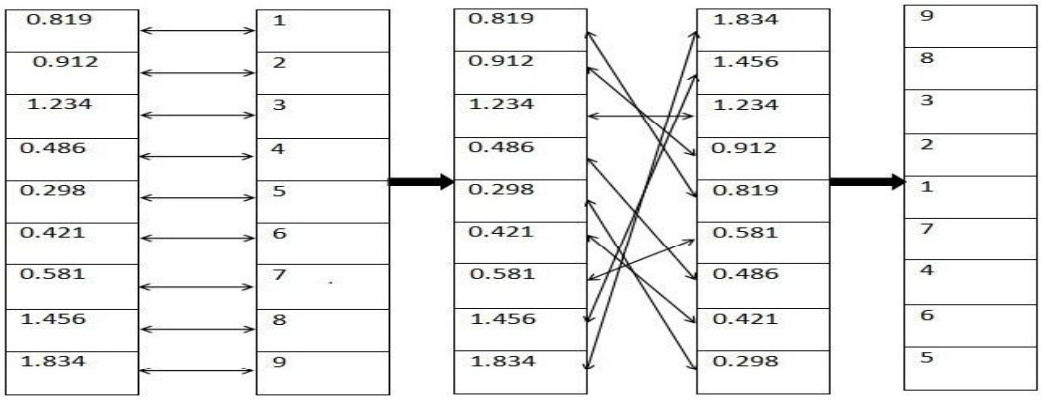

Fig 1(a) Fig 1(b)

In figure 2 column 1 represents intensity value of image, column 2 represents the tabulated index value obtained from the previous step and column 3 represents the arranged intensity value according to column 2.

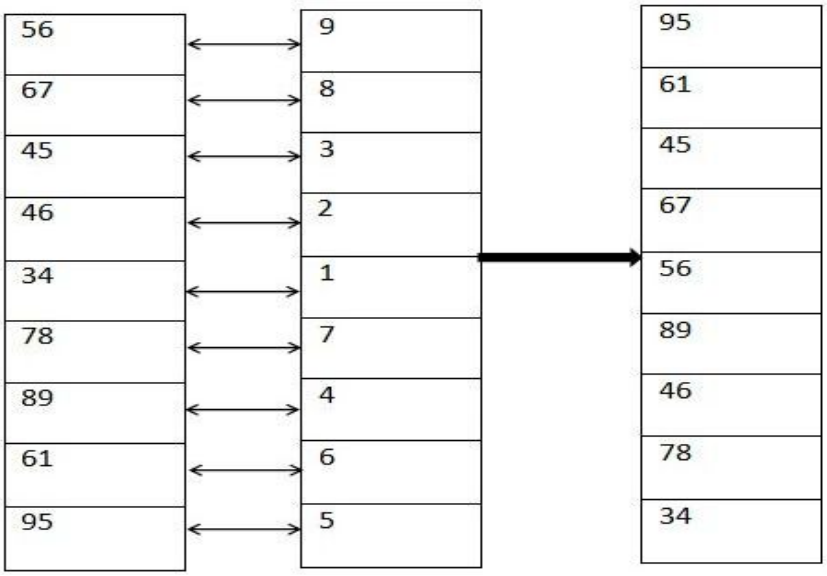

Fig 2

Decryption is done by the reverse process followed for encryption. In fig 3(a) column 1 represents the sequence of received elements; column 2 represents sorted index elements and column 3 represents resorted index elements. This resorted index values are used to obtain the original pixel values as shown in fig 3(b).

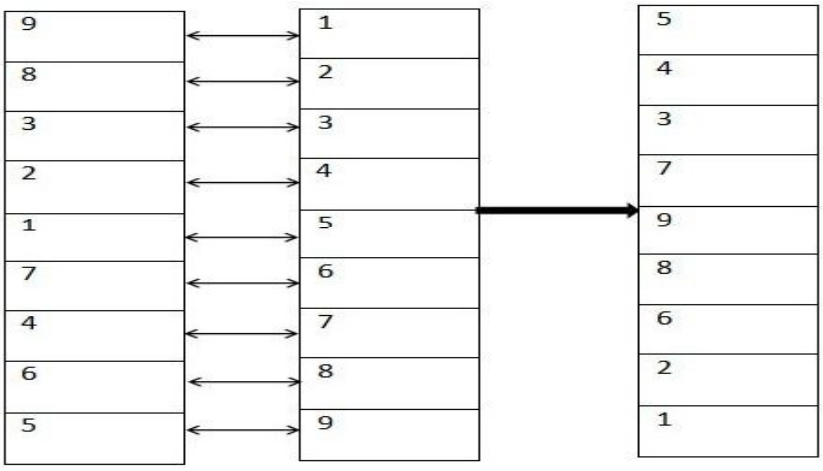

Fig 3(a)

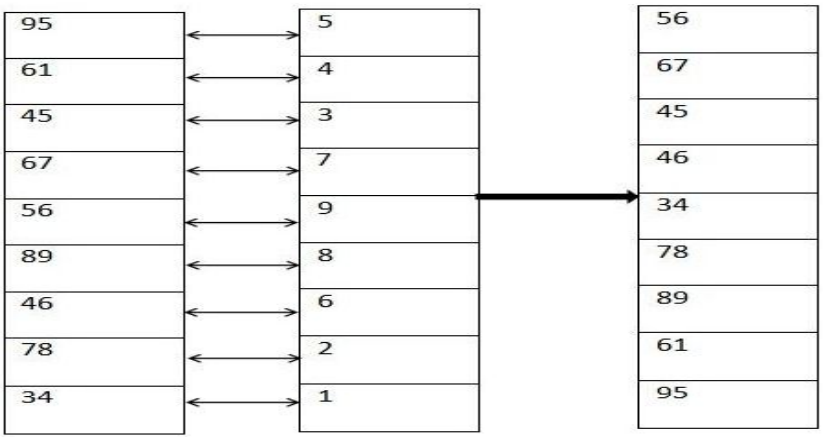

Fig 3(b)

These pixel values obtained are then converted into a matrix combining the R, G, B components and then the transpose of this matrix is done to finally obtain the original image.

IV.CONCLUSION

This paper describes about a novel image encryption technique using the concept of non-linear dynamic system (chaos). The chaos system is highly sensitive to initial values and parameters of the system. The proposed method utilizes the randomness of the chaos maps in order to encrypt the image. In this algorithm the pixel position is changed according to the randomness of the chaotic elements, which is derived by comparing sorted and unsorted chaotic elements generated from chaos map. This algorithm completely removes the outlines of the encrypted images, blurs the distribution characteristics of RGB-level matrices.

REFERENCES

[1] Victor Grigoras1 , Carmen Grigoras "Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems" Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bucharest, Romania, October 16-18, 2006.

[2] Mintu Philip, Asha Das "Survey: Image Encryption using Chaotic Cryptography Schemes" *IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.*

[3] E. N. Lorenz, " Deterministic nonperiodic flow," J.Atmospheric Sci. 20 (1963) 130.

[4] Chen Wei-bin; Zhang Xin; "Image encryption algorithm based on Henon chaotic system" Image Analysis and Signal Processing, 2009. IASP 2009. International Conference, Publication Year: 2009 , Page(s): 94 – 97.

[5] Nien, H.H.; Huang, W.T.; Hung, C.M.; Chen, S.C.; Wu, S.Y.; Huang, C.K.; Hsu, Y.H.; "Hybrid image encryption using multi-chaos-system" Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on digital identifier Publication Year: 2009 , Page(s): 1 – 5.

[6] Xiaomin Wang; Jiashu Zhang; " An image scrambling encryption using chaos-controlled Poker shuffle operation" Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on Publication Year: 2008, Page(s):1- 6.