An Improved Cryptography Scheme for Secure Image Communication

Bhaskar Mondal
Computer Sc. and Engineering
National Institute of Technology, Jamshedpur
India- 831014

Akash Priyadarshi
Computer Sc. and Engineering
National Institute of Technology, Jamshedpur
India- 831014

D Hariharan
Computer Sc. and Engineering
National Institute of Technology, Jamshedpur
India- 831014

ABSTRACT

The traditional chaos algorithm is based on the logistic maps and has some drawbacks. In order to enhance the security, improved chaos system is used. It is based on location Transform and pixel value alteration using random sequence. The proposed algorithm shuffles the image based on the chaotic sequence and change the value of each pixel. The key generates 16 chaotic sequences from given sequence using a secret look-up matrix. Key used for encryption improves efficiency by acting on n sub-parts of image. The Matlab is used for simulation of image encryption algorithm. The algorithm's safety is analyzed from different aspects such as histogram comparison, correlation coefficient and secret key sensitivity. The algorithm proposed is robust against statistical attack, brute force attack and plain text attack.

.General Terms

Pseudo random sequence based encryption.

Keywords

Image Encryption; chaotic sequence; location transform; random sequence.

1. INTRODUCTION

Rapid development in the field of internet and graphics opened new dimensions of communications. The multimedia communication has gradually become the crucial way to exchange information among people. Digital image accounts 70% [1] of the information transmission on the internet and hence brings Image encryption in picture.

Traditional encryption algorithm such as DES, IDES, and IDEA are against the plain text and are not suitable for digital image encryption [2]. In order to safely transmit images, numerous encryption algorithms have been developed. In 1989, R Mathews proposed discrete chaotic dynamical system in cryptography first [3]. In 1997, Fredric applied chaos to encryption of digital image for first time.[4].Due to desirable properties of non-linear dynamic system such as periodicity, sensitive dependence on initial conditions and good pseudo-random properties, the chaos based encryption has suggested a new and efficient way to deal with intractable problem of fast and highly secure image encryption.

In 1991 Habutsu et al. [5] developed crypto system based on a piecewise linear chaotic tent map. In Habutsu cryptosystem, it is made of the parameter of the tent map as a secret key and the encryption and forward iteration of the chaotic tent map. But the cryptosystem can be easily broken using a ` chosen cipher text attack' and `known plaintext attack'.

Zhang et al. [6] presented a new image encryption algorithm based on chaotic system with the image using technique of permutation transform. Then 2-D non-linear map is utilized to circularly iterate grey value pixels. Problem with this algorithm is, it is not robust against `shear attack' and inefficient magic matrix generating algorithm.

This paper put forward a new image encryption algorithm based on chaotic systems and shuffle exchange. This algorithm shuffle and change each and every pixel based on 2-D key. The simulation results show that the encrypted image is robust against `brute force attack', `known plaintext attack' and ` statistical attack'.

In Section 2.1 principle of key generation algorithm is discussed in detail. In this section pseudo-random function is used to generate first a 1-D and then convert it into 2-D key with the help of lookup matrix. In Section 2.2 Image encryption with the help of 2-D matrix is explained. Section 3 and Section 4 presents the simulation results of encryption and shows the robustness of encrypted image. The conclusion is given in Section 5..

2. Proposed Scheme:

Developments in the networking technology result in drastic changes in modes of communication. Image becomes dominant mode for information interchange. Hence it is more vulnerable to Digital image duplicating and re-distributed by hackers. Many algorithms are developed over time to solve this problem. Some of them are Multiple Huffman table, block ciphers such as AES, DES, IDEA, RC, Digital fingerprint encryption Technique, optical encryption Technique etc. Many of these show vulnerability against one type of attack or other.

To overcome some of these Cipher attacks pseudo random sequence based chaos encryption is introduced here. In this scheme Image is encrypted using chaotic sequence generated using pseudo random sequence and lookup matrix.

2.1 Key generation Algorithm:

The first step of the algorithm is a generating a key for encryption. Key is generated using Horowitz *et. al*[7] integer value random sequences generating algorithm based on real number random sequence in range [0,1].

Key generation algorithm is as follow:

Step 1:Generate a 16-node link list with node values represented by K_i. Here k = {0,..,15}. Also create a 1-D matrix M[16].

Step 2: Put count ←16 and use Random sequence generating algorithm to generate real number in range of [0,1].

Step 3: Put N ← count * Random[0,1].

Step 4: Retrieve N^{th} node value from link list and put it in M[i]. Here i={0,1,2,3,…….,15} and remove N^{th} Node from the link list.

Step 5: Decrement value of count by 1 and iterate Step 4.

Step 6: Create a 2D matrix M'[16][16] where elements of M' is given by:

$$M'[i][j] = M[j]+[16*i]$$

Here (i, j) Є[01,2,…….,15].

Step 7: Shuffle M' using secret Lookup matrix Convert M' into 1D matrix M'' by using M''_{ij} = (i)*16+ j.

Based on the result of the above algorithm a 256 values key M'' is generated in which any two values of elements are not equal. Now image is encrypted using key M''.

2.2 Image Encryption Algorithm:

Suppose the image that is being encrypted is noted Image and its size is (m, n). The Encrypted Image is noted EImage and its dimension are same as Image. The proposed algorithm shuffle image pixels based on chaotic sequence and alter value of each and every pixel. Confusion and Transposition is further increased by using sliding window. The algorithm for image reading is as follow:

Step 1: If m<128 AND n<128 then pass the matrix to shuffle matrix .Else go to step2.

Step 2: If m>128 then take two factors of m and mark it Row and Slide, such that Row = 2 * slide AND Row<128If no such factor of m exist then increment m by 1 and repeat. Else put ROW ← m.

Step 3: If n>128 then take two factors of n and mark it Col and Slide, such that Col = 2*slide AND Col<128If no such factor of n exist then increment n by 1 and repeat. Else put ROW ← n.

Step 4: Use sliding window on Image to pass Sub-matrixes to shuffle algorithm for shuffling. Window size is given by (Row, Col) and horizontal slide and vertical slide is given by:

Horizontal slide = Col\2.

Vertical slide = Row\2.

Sub-matrix is accepted by shuffle algorithm and key is used to shuffle these matrixes. Now we describe the algorithm for transposition and substitution as follows:-

Step 1:Store the dimension of sub-matrix into row and col.

Step 2:Take factors of row and col. Mark it as r and c respectively. Factors selected should satisfy following relation: row*c<256 AND col*r<256.

Step 3: Now divide matrix into row-wise 1 Dimension blocks of size r and mark it r_i where i Є {0,1,……,m*n/r}.

Step 4: Move r_i to location M_i'' and add $M''[M_i'']$ to it.

Step 5: Now again divide matrix into column-wise 1 D blocks of size c and mark c_i where i Є {0,1,2,……,m*n/c}.

Step 6: Move c_i to location M''_I and add $M''[M''_i]$ to it.

In the above algorithm if the key value is greater than no of blocks (m*n/c or m*n/r) then skip the key value and continue.

Once image is encrypted, key is transferred to the receiver through secure channel. Only M[16] is transferred to receiver as key. At receiver end original key is reconstructed from M by using same secret lookup matrix. Advantage of transferring the partial key is, even if a unauthorized person get access to this key he will be unable to decrypt the EImage without the secret lookup matrix.

The decryption process is just reverse process of encryption process. Suppose the decrypted image is DImage. Then its size is (m, n).

3 Experimental Results:

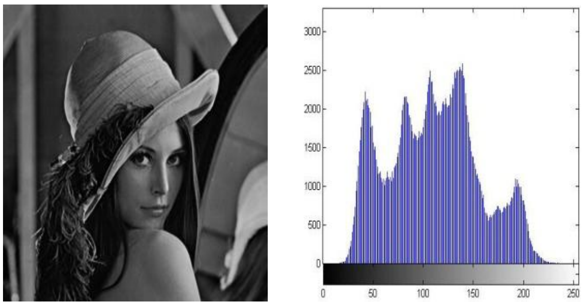
The algorithm was simulated in MATLAB. From the analysis of the encrypted image we can observe that encryption algorithm has completely changed the characteristics of the original image. However after decryption, decrypted image and the original image shows similar characteristics. Image characteristics are analyzed from two aspects – histogram comparison and correlation coefficient. Apart from this operational speed of algorithm is also analyzed:

3.1 Histogram:

Histogram is the graphical representation of the frequency of occurrenceof each gray level in the image.Consider an image f(j,k) that has N_x pixels per line , with N_b bits per pixel. The

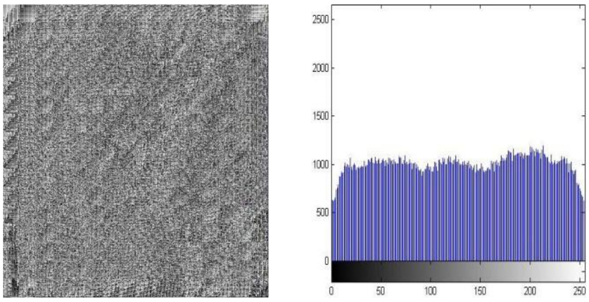
Histogramh_f(I) for each code value I , represents no. of time the code value represent in theimage.

Image’s statistical distribution is reflected by its histogram, which can be used for statistics analysis attack. By comparing the histograms of original image and encrypted image, great difference has been noticed.The results indicate that the grayscale distribution of the encrypted image in Figure 2 is more uniform than that of original image in Figure 1.



(a) (b)

Figure 1. (a) Original image and (b) Histogram of original Image



(a) (b)

Figure 2. (a) Encrypted Image and (b) Histogram of Encrypted Image

3.2 Correlation Coefficient:

A digital Image is formed by the combination of pixels, where each pixel represent a particular color. Adjacent pixels in the image show a small or large correlation. This correlation is usually a gradual change process between the pixels. Each Image has its own histogram which can be used to compare and predict original Image. This is known as statistical attack. To resist this type of attack the correlation between two adjacent pixels in the encrypted image much be decreased. The correlation of adjacent pixels in horizontal, vertical and diagonal directions can be calculated as follows [8].

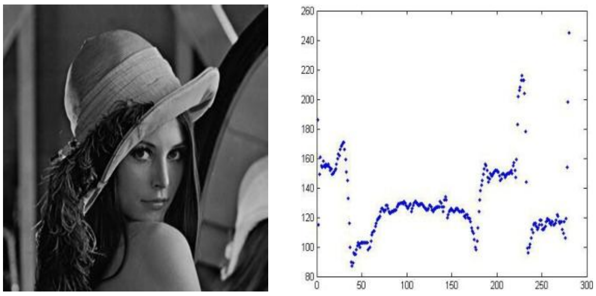
$$\rho_{xy} = \frac{|Cov(x,y)|}{\sqrt{D(x)}.\sqrt{D}(y)}$$

$$E(x) = \frac{1}{N}\sum_{1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{1}^{N}\left(x_i - E(x)\right)^2$$

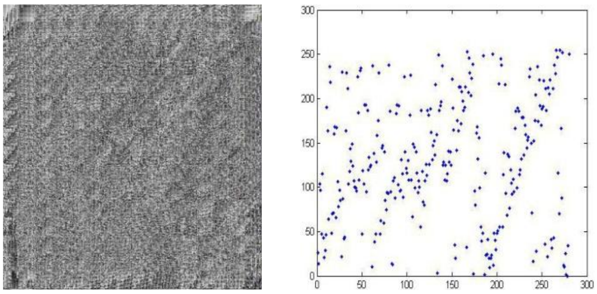
$$Cov(x,y) = \frac{1}{N}\sum_{1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right)$$

In formula, symbol x and y represent the grey values of adjacent pixels. Analysis of algorithm shows high correlation coefficient of pixels in original image and low coefficient in encrypted image. Figure 3 shows grayscale level plot of correlation coefficient of a rowof original image and Figure 4 shows correlation coefficient of a row of encrypted image.



(a) (b)

Figure 3. (a) **Original image and (b) Correlation of a row in original Image.**



(a) (b)

Figure 4. (a) Encrypted image and (b) Correlation of a row encrypted Image.

3.3 Operational Speed Analysis:

Real time algorithms are judged by its execution time. Execution time is also sometime called as Operational Speed of algorithm. Henceoperational speed analysis is a major measure for comparing practical algorithms, and it is a very important factor to consider for large image and real time environment. Table 1 shows execution time of algorithm on Matlab on Intel(R) Core(TM)-i5 CPU M450 at 2.40GHz on Window 7. Table 1 shows different execution time for different image sizes. It can be seen from the table that with the increase in size of the image, there is small change in execution time of algorithm.

Table 1 Operational speed of proposed algorithm

Image Size	Operation time (clock-time) Using 64-bit Key
128X128	0.0936
256X256	0.3276
512X512	0.9934
1024X1024	5.4912

4 Security Analyses:

4.1 Secret-key Set

Shannon information theory has proved that one secret-key for one time of encryption is safe [9]. But this approach is not realistic in practical applications. For example, someone wishes to save a group of encryption images in computer. If each image is encrypted by one different secret-key, the user must remember every secret-key of encryption images, which isneither easy nor safe. Therefore, the more accepted practice is to use the same secret-key for each image, which is more simple and safe for secret-key management.Proposed algorithm uses pseudo random sequence and secret lookup matrix to generate key matrix. Therefor total key space for this algorithm is 256!,which is approximately equal to 10^{506} .It is obvious that the secret-key space of this algorithm is very and can be effectively resist the Brute-force attack.

Algorithm	Key-Space
Proposed algorithm	10^{506}
[10]	10^{135}

4.2 Secret-Key Sensitivity:

Secret Key sensitivity measures the decryption results of almost similar keys from a similar key. Higher your key sensitivity more secure it is from unauthorized access. We use "8956712131104162311514" as the secret-key to encrypt the sample image, then decrypt the encrypted image with the same key "8956712131104162311514" but using different look-up matrix. Figure shows that the decryption result will be significantly different when secrete key has not changed.

It can be concluded from Figure 5 and figure 6 that it is almost impossible to decrypt the decrypted image correctly by exhaustive search when secrete key and look-up matrix is unknown.

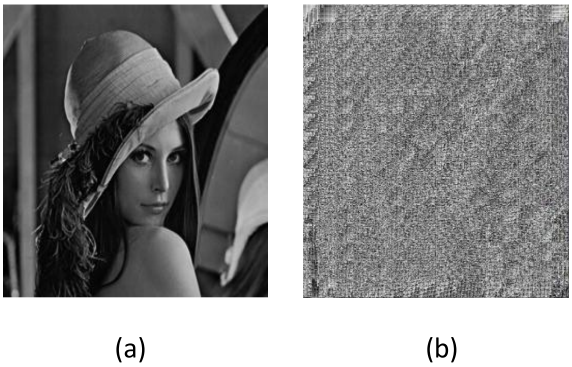


Figure 5. (a) Original image and (b)Encrypted Image

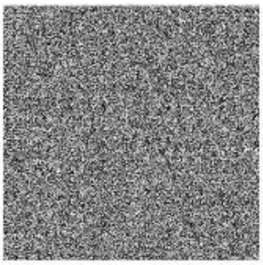


Figure 6.Decrypted Image with wrong look-up matrix

5 Conclusions:

In this paper, we put forward new image encryption algorithm based on pseudo-random sequence, transposition and confusion. Proposed algorithm is compared with different image encryption scheme using constant parameters. Experimental results showthis algorithm has low computational complexity, a large key-space and good effect on encryption. The original image and encrypted image shows different characteristics. The encrypted image can resist various attacks like statistical attack, brute force attack and chosen cipher text attack.

6 Acknowledgements:

This paper is developed under Computer Science and Engineering branch of National Institute of Technology, Jamshedpur, India.

7 REFERENCES

[1] Philip P. Dang and Paul M. Chau. Image Encryption for Secure Internet Multimedia Applications [J]. IEEE Transactions on consumer electronics 2000, 395-443.

[2] HuaZhong Based on the chaotic image encryption technology research [D]. Changsha Polytechnic University, Master's Thesis, Hunan, Changsha, 5-6.

[3] R. A. J. Matthews. On the derivation of a chaotic encryption algorithm [J]. Cryptologia.1989, 13(1): 29- 42.

[4] Fredrich J. Image Encryption Based on Chaotic Maps[C] , IEEE , 1997 , 1105-1110.

[5] T. Habutsu, Y. Nishio, I. Sasase, *et al*. A secret cryptosystem by iterating a chaotic map [A]. Advances in Cryptology EURCRYPT'91[C]. Berlin: Springer-Verlag. 1991:127-140.

[6] Zhang Han, Wang XiuFeng*et al.* A new image encryption algorithm based on chaos system[C]. *Proc.*IEEE*Int. Conf.* Robotics, Intelligent Systems and Signal Processing. Changsha, China, October 2003:778-782.

[7] Ellis Horowitz, SartajSahni, and Dinesh Mehta. Fundamentals of Data Structures in C++[M].W H Freeman , NY. 1995.

[8] Ai-hong Zhu and Lian Liu. Improving for chaos Image Encryption Algorithm based on logistic maps[C]. Environmental Science and Information Application Technology (ESIAT), 2010 International Conference. Page(s): c1 - c4

[9] Shannon CE. Communication theory of security systems [J].the Bell System Tech J, 1949,28, pp.656-715.

[10] Zhang Jun, Li Jinping, Wang Luqian. A New Compound Chaos Encryption Algorithm for Digital Images[C].Information Technology and Applications (IFITA), 2010 International Forum.2010 , Page(s): 277 – 279

AUTHOR'S PROFILE

Akash Priyadarshi is pursuing his B.E degree in Computer Science and Engineering from the National Institute of India, and has worked on some of major project as development of software for Aakash+ in IIT Mumbai, India. His research interests include Artificial Interest, Security analysis and secure communication

Bhaskar Mondal was born in West Bengal, India in July 1986. He received B. Tech. degree in Computer Science and Engineering from West Bengal University of Technology in 2008 and M. Tech. degree in Computer Science and Engineering from Kalyani Government Engineering College, West Bengal, India in the year of 2010.

He is working at National Institute of Technology, Jamshedpur as Assistant Professor in the department of Computer Science and Engineering since January 2011. His research interest includes Secret Image Sharing, Security and NLP.

D Hariharan is pursuing his B.E degree in Computer Science and Engineering from the National Institute of India, and has worked on some of major project as development of debian based operating system. His research interests include Artificial Interest, compiler design and secure communication.