Secure Image Encryption Algorithms: A Review

Lini Abraham, Neenu Daniel

Abstract: - Image encryption plays an important role in the field of information security. Most of the image encryption techniques have some security and performance issues. So there is a need to compare them to determine which method is suitable for the application. Chaos based encryption algorithms are employed nowadays because of their better security and performance aspects. Chaotic behavior of a system is the sophisticated nature of a nonlinear system that looks random. This work is a review of two novel chaos based image encryption algorithms, namely a secure image encryption algorithm based on Rubik's cube principle and a new chaos-based fast image encryption algorithm in terms of the parameters like NPCR, UACI, Entropy and Correlation coefficient.

Index Terms: - Cryptography, Image encryption, Decryption, NPCR, UACI, Entropy, NCML.

1 INTRODUCTION

Unlike text messages, the multimedia information including image data has some special characteristics like high capacity, redundancy and high correlation among pixels. In some cases image applications require to satisfy their own needs like real time transmission and processing. One of the main goals that must be achieved during the transmission of information over the network is security. Cryptography is the technique that can be used for secure transmission of data. This technique will make the information to be transmitted into an unreadable form by encryption so that only authorized persons can correctly recover the information. The security of image can be achieved by various types of encryption schemes. Different chaos based and non-chaos based algorithms have been proposed. Among this the chaotic based methods are considered to be more promising. The chaotic image encryption can be developed by using properties of chaos including deterministic dynamics and unpredictable behavior. There are three kinds of encryption techniques namely *substitution*, *transposition* or *permutation* and techniques that include both *transposition* and *substitution*. Substitution schemes change the pixel values while permutation schemes just shuffle the pixel values based on the algorithm. In some cases both the methods are combined to improve security. In [1] an image encryption technique based on Arnold cat map and Chen's chaotic system is proposed. In [2] combinations of three permutation techniques is described, in which bit level, pixel level and block level permutations are applied in some order. Image encryption in [3] is an enhancement to AES algorithm by adding a key stream generator. The method in [4] is chaos based using bit level permutation. Permutation at the bit level not only changes the position of the pixel but also alters its value. In [5] a novel image encryption method based on total shuffling scheme is illustrated. In [6] combinations of two logistic maps are used for improving the security of encryption. Encryption in [7] uses multiple chaotic systems.

- Lini Abraham is currently pursuing masters degree program in computer science and engineering in M.G. University, India. E-mail: linirt33@gmail.com
- Neenu Daniel is currently working as assistant professor CSE department,VJCET, India, E-mail: neenudaniel@gmail.com

But each of these methods has some security issues. As the key space increases the quality and security of encryption also improves. Our work compares two chaos based encryption algorithms that can be applied to gray scale images. The algorithm based on Rubik's cube principle in [8] uses a key of size *M x N,* where *M x N* is the size of the gray scale image. The technique in [9] is based on Nearest Neighbouring Coupled Map Lattices (NCML).

2 COMPARISON CRITERIA

1. Number of pixel change rate (NPCR).
2. Unified average changing intensity (UACI).
3. Entropy.
4. Correlation coefficient.

2.1 Number of pixel change rate (NPCR)

It is a common measure used to check the effect of one pixel change on the entire image. This will indicate the percentage of different pixels between two images. Let $I_o(i, j)$ and IENC(*i*, *j*) be the pixels values of original and encrypted images, *Io* and *I*ENC, at the i^{th} pixel row and j^{th} pixel column, respectively. Equation (1) gives the mathematical expression:

2.4 Correlation coefficient

Correlation computes the degree of similarity between two variables. This parameter is useful for calculating the quality of the cryptosystem. Let *x* and *y* be the gray-scale values of two pixels at the same place in the plaintext and ciphertext images respectively and C.C be the correlation coefficient and Cov be the covariance at pixels *x* and *y*. VAR(*x*) denotes the variance at pixel value *x* in the plaintext image, σ_x the standard deviation, E the expected value operator and *N* the total number of pixels for *N x N* matrix. Then the correlation can be calculated by the equations (4), (5), (6), (7) and (8) as below:

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\ x\ \frac{100\%}{M\ x\ N} \qquad (1)$$

Where D(i, j) = 0 if $I_o(i, j) = I_{ENC}(i, j)$ if not then D(i, j) = 1.

2.2 Unified average changing intensity (UACI)

A small change in plaintext image must cause some significant change in ciphertext image. UACI is helpful to identify the average intensity of difference in pixels between the two images. For the plaintext image $I_o(i, j)$ and encrypted image $I_{ENC}(i, j)$ the equation (2) gives the mathematical expression for UACI.

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|Io(i,j)-I_{ENC}(i,j)|}{255}\right] \times \frac{100\%}{M \times N} \quad (2)$$

2.3 Entropy

It is an important concept for analyzing an encryption scheme. Entropy gives an idea about self information. The entropy of a message *m* can be indicated as H(*m*). If there are M symbols and p(m_i) as the probability of occurrence of symbol m_i, then the equation (3) for entropy is given as:

$$H(m) = \sum_{i=0}^{M-1} p(m_i)\, log\, \frac{1}{p(m_i)} \quad (3)$$

$$C.C = \frac{Cov(x,y)}{\sigma_x \times \sigma_y} \quad (4)$$

$$\sigma_x = \sqrt{VAR(x)} \quad (5)$$

$$\sigma_y = \sqrt{VAR(y)} \quad (6)$$

$$VAR(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (7)$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\,(y_i - E(y)) \quad (8)$$

3 OVERVIEW

We compare two novel image encryption algorithms that are used for gray scale images. In this section we are giving a brief outline of the two methods in [8] and [9].

3.1 A secure image encryption algorithm based on Rubik's cube principle

The method in [8] uses two secret keys equal to the number of rows and columns of the plaintext image. Based on the principle of Rubik's cube the image pixels are scrambled. Then XOR operator is applied on the rows and columns. The basic scenario of Rubik's cube encryption is given below:

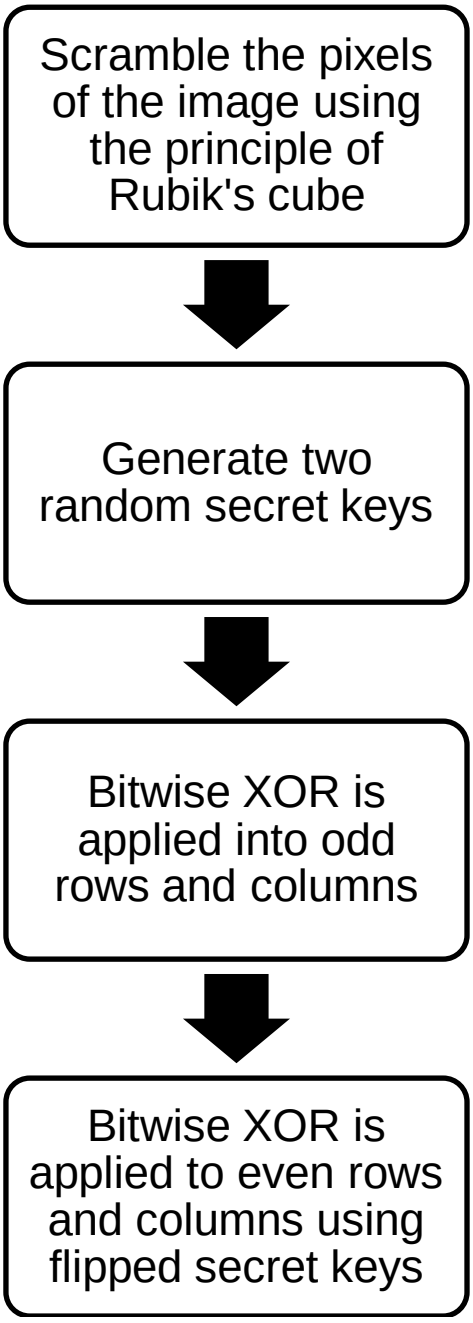

Fig.1. Rubik's cube Encryption

3.2 A new chaos-based fast image encryption algorithm

The spatiotemporal chaos is used for generating the random sequence for the purpose of encryption, due to which the periodicity problems in simple chaotic systems are avoided. Also the permutation and substitution operations are performed simultaneously for fast encryption. A brief idea about the encryption technique proposed in [9] is given in the following figure 2. A 128-bit key is used for the algorithm. For converting the floating point numbers generated from the chaotic map into integer form, the basic operations having less processor time are used. So the algorithm performs well by reducing the time needed for the entire process.

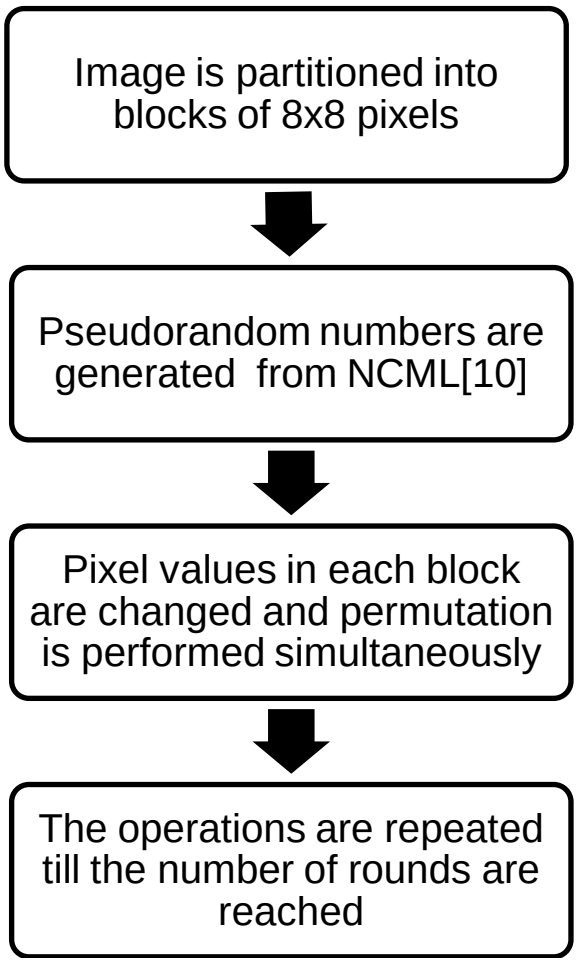

Fig.2. Summary of encryption process

4 PERFORMANCE ANALYSES

The parameters used for the comparison are given in section II. The test image is of size 256×256. The results after encrypting the image using two iterations are given. The diffusion characteristics including NPCR, UACI, correlation coefficients and entropy are used for the evaluation. A key space analysis is also added at the end of the assessment.

4.1 Diffusion Characteristics

The results are given in Table 1. Higher NPCR values are desired for ideal encryption schemes. The UACI values must be in the range of 33%. Two images are taken for comparison.

Table 1
NPCR and UACI (%)

Algorithm	NPCR		UACI	
	Lena	Baboon	Lena	Baboon
Scheme in [8]	99.641	99.609	28.620	27.409
Scheme in [9]	99.607	99.606	33.463	33.470

4.2 Entropy Analysis

For gray scale image having 256 levels, the theoretical value of entropy is 8 bits. The following table shows the results.

Table 2
Entropy (Sh)

Algorithm	Entropy	
	Lena	Baboon
Scheme in [8]	7.9935	7.9968
Scheme in [9]	7.9994	7.9992

4.3 Correlation coefficient

Correlation coefficient of the original image is usually high (close to one). Weaker the correlation coefficient of the encrypted image better the algorithm. The Table 3 shows the outcome.

Table 3
Correlation coefficient

Correlation	Horizontal	Vertical	Diagonal
Lena (original)	0.9864	0.9886	0.9776
Scheme in [8]			
Lena(encrypted)	0.0068	0.0091	0.0063
Scheme in [9]			
Lena(encrypted)	0.0007	0.0021	0.0148

4.4 Key space analysis

One of the parameters used to measure the security of an image encryption algorithm is its key space. As the key space increases the security of encryption improves. The method in [8] describes an encryption technique that uses an 8-bit gray scale image of size 256 × 256 pixels and iteration count = 1, in which the key space is determined by the combination of image size and the number of iterations. This key space is large enough to resist exhaustive attacks. The technique in [9] uses an input key size of 128-bits and the lattice values of the NCML are exchanged according to the cipher values after each block is encrypted.

5 CONCLUSIONS

In this paper we analyzed two novel chaos based image encryption algorithms. The technique using Rubik's cube principle has a large key space and its implementation is quite simple. The new fast chaos based image encryption algorithm combines the permutation and diffusion for fast processing and uses NCML which reduces the problem of periodicity in the generation of pseudorandom sequences. Each of the image encryption techniques has its own advantages. Identification of the suitable algorithm for a particular application depends on the prerequisites of that application. To make a precise observation, more parameters need to be evaluated and compared.

6 REFERENCES

[1] Zhi-Hong Guan, Fangjun Huang, Wenjie Guan, "Chaos-based image encryption algorithm", *Physics Letters A 346, Elsevier*, 2005.

[2] Mitra, Y. V. Subba Rao and S. R. M. Prasanna, "A New Image Encryption Approach using Combinational

Permutation Techniques", *International Journal of Electrical and Computer Engineering 1:2, communications on ACM*, 2006.

[3] M.Zeghid, M.Machhout, L.khriji, A. Baganne, and R.Tourki," A modified AES based algorithm for image Encryption", *World Academy of Science, Engineering and Technology 3,* 2007.

[4] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", *Information Sciences 181 1171–1186 Elsevier*, 2010.

[5] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme*," Optics Communications, vol. 284, no. 12, pp. 2775–2780*, 2011.

[6] Ismail1, Mohammed Amin, Hossam Diab, " A Digital Image Encryption Algorithm Based A Composition Of Two Chaotic Logistic Maps", *Proc. 27th IEEE Int'l Conf. Signal Processing., pp. 733-739*,2011.

[7] H.Alsafasfeh, and, A.A.Arfoa, Image encryption based on the general approach for multiple chaotic system, *Journal of Signal and Information Processing 2, 238-244*, 2011.

[8] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", *Department of Electrical and Computer Engineering, Laval University, QC, Canada G1K 7P4*, 2011.

[9] Yong Wanga, Kwok-Wo Wong, Xiaofeng Liaoc, Guanrong Chen, "A new chaos-based fast image encryption algorithm", *Applied Soft Computing, Elsevier*,2011.

[10] K. Kaneko, Pattern dynamics in spatiotemporal chaos: pattern selection, diffusion of defect and pattern competition intermittency, *Physica D (34)* (1989)