International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 380 – 384

Non Linear Chaotic Map for Secure Data Transmission

S Sankar
Research Scholar, Department of IT
Hindustan University Chennai, India
sankar_jaikissan@yahoo.com

S Nagarajan
Professor, Department of IT
Hindustan University, Chennai, India
snagarajan1960@gmail.com

Abstract : In today's world, Internet plays a major role in people's communication. People nowadays share and transfer variety of multimedia information through the Internet. Although a lot of benefit with it, data transfer over Internet is vulnerable to attack is a major hindrance. Cryptography is the science used to keep the information safe from attack. In the case of text data transfer more number of encryption techniques are existing whereas when it comes to image very less number of techniques are available. Also, the traditional image encryption methods are not viable enough for modern images due to their different storage formats. Hence research on image encryption becomes inevitable. In this paper, we have proposed Non linear chaotic map technique to encrypt the images and performance of the same has been evaluated. This study shows Non linear chaotic map has higher performance for images.

Keywords – *Chaotic map, Cryptography, Image encryption, Data Security*

*****

I. INTRODUCTION

With the rapid development of multimedia and network technologies, the security of multimedia becomes more and more important, since multimedia data are transmitted over open networks more and more frequently. Typically, reliable security is necessary to content protection of digital images. Encryption can be defined as the art of converting data into coded form which can be decode by intended receiver only who poses knowledge about the decryption of the ciphered data. Encryption can be applied to text, image, and video for data protection. Image compression is an application of data compression that encodes the original image with few bits. The objective of image compression is to reduce the redundancy of the image and to store or transmit data in an efficient form.

Even though both data compression and encryption are methods to transform data into different representation, the goals tried to achieve by them are different. Data compression is done with the intension of decreasing the size of data, where encryption is done to keep the data secret from third parties. Data compression offers an approach for reducing communication costs, at the same time it is vulnerable to attack during the transmission. If it is compromised then it is not possible to get actual data during the decompression. Therefore security is needed to preserve the compressed data. Compression always relies on high redundant data in order to gain size reduction. Since encryption destroys redundancy [7], the compression algorithm would not be able to give much size reduction, if it is applied on encrypted data. For that reason, compression before encryption is the highly preferable order. In this chapter, we discuss a unique chaos based crypt analysis.

The complexity inherent in chaotic systems gives rise to the term chaos, which does not indicate complete disorder, as in everyday usage. Rather, chaos is the apparently random behavior of a system which is in fact deterministic. This means that the system has no inherent randomness or noise, and that the irregular behavior arises from its nonlinearity. Given a specific initial condition for a chaotic system, its behavior for all future time is well-defined and predictable. Several important characteristics serve to define a chaotic system. First, such systems are highly sensitive to initial conditions - two states with an arbitrarily small initial separation may have widely different final states, and perturbations from initial conditions grow exponentially. The phase space of a chaotic system is topologically mixing, such that any subset of phase space will eventually overlap with any other given subset. Phase space may contain structures such as regions of stability and points or regions of accumulation which are "strange" or otherwise quite complex. Finally, orbits of a chaotic system in phase space are by definition a periodic.

II. PROPOSED SYSTEM

The existing chaos based algorithms operate on two stages: the shuffling stage and the substitution stage. In the shuffling stage, the position of the pixels from the original image is changed by chaotic sequences [2] or by some matrix transformation,

such as Arnold transformation, magic square transformation, and so forth. These shuffling algorithms can be easily realized. Since these shuffling algorithms just involve changing the position of the pixels but not changing the pixel values it leads to histogram of the encrypted image same as the original image, thus the security of the image is threatened by statistical analysis.

Compared to the method of shuffling the method of substitution is more efficient and more secure as it involves changing the pixel values. Even such shuffling when applied alone, it leads to weaker encrypted image. Thereby in order to improve the security shuffling and the substitution are combined by some researchers [3, 4]. Chaotic Image encryption is a branch of cryptography in which we encrypt image data with the help of cryptographic tools based on chaos theory. Matthews first proposed the chaos-based encryption scheme in 1989 [3], and Fridrich first adopted chaotic map into image encryption in 1997 [4]. Since then, many chaos-based image encryption algorithms have been designed to realize secure communications. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography [4]. Therefore, chaotic cryptosystems have more useful and practical applications.

Non linear system is a chaotic system in which output of the system is totally unpredictable and dynamic since it uses chaotic maps. The chaotic maps are getting more attention recently in cryptanalysis since it is easy to solve but the result is bifurcation where at every point it changes from one functional behavior to another functional behavior. The chaotic map when it is iterated by a function f, in a space S then there is a change from one state to another, that is,

$$s_{n+1} = f.(s_n) \tag{1}$$

where sn ∈ S indicates the system state at discrete time. In chaos cryptography, the state space is typically finite binary space

$$S=P=C\ \{0, 1\}^n,\ n=1,2,3,\ \ldots. \tag{2}$$

where P is plain text and C is Cipher text. The initial value of a control parameter s0 ∈ S is maintained throughout the iterations and it results dynamic cn ∈ C. Thus, depending upon the value of input control parameters, the non linear mathematical model gives unpredictable results. With more than one control parameters and initial conditions, high dimensional chaotic systems are most complex and have a big key space. However, complex calculations make the encryption algorithm too slow. To overcome these drawbacks, a nonlinear chaotic map (NCM) [29] is adopted. Encryption method based on nonlinear chaotic algorithm uses tangent and power function to give large key space. The experimental results show that this chaotic map has more complex chaotic behaviors than the linear chaotic map.

$$x_{n+1} = (1-\beta^4).c.tan\left(\frac{\propto}{1+\beta}\right).\left(1+\frac{1}{\beta}\right)^{\beta}.\tan(\alpha x_n).(1-x_n)^{\beta} \tag{3}$$

where α, β are control parameters. When x_n Ɛ (0,1) , α Ɛ (0, 1.4), β Ɛ (5, 43), or x_n Ɛ (0, 1) , α Ɛ(1.4, 1.5), β Ɛ(9, 38), or x_n Ɛ (0, 1), α Ɛ (1.5, 1.57), β Ɛ (3, 15), NCM performs chaotic phenomena.

To get a faster encryption speed, every time NCM is iterated as a result, n bytes random numbers are gained. The standard image data sets are used to test the algorithm. It uses chaotic sequence generated by NCM map to encrypt image data with different keys for different images. Original chaotic sequence $\{x_0,x_1,x_2, \ldots\}$ consists of decimal fractions. However images are all digital. So a map is defined to transform the chaotic sequence to another sequence which consists of integers. Then plain-image image is encrypted by performing XOR operation with the integer sequence. The encryption steps are as follows:

Step 1: Split the square image into n number of blocks of equal size and from left to right and top to bottom, we transform two-dimensional image to one-dimensional.
Step 2: Set encryption key K=(α, β, x_0), with initial values.
Step 3: Do 100 times of chaotic iteration as formula, and obtain n bytes of random numbers.
Step 4: If the encryption work is finished for all blocks, then go to step 6; otherwise do three more times of chaotic iteration; and as a result, a decimal fraction will be generated, which is a double value and we choose its first 15 significant digits.
Step 5: Divide the 15 digits into five integers with each integer consisting of three digits. For each integer, do mod 256 operation, and another 5 bytes of data will be generated.

Step 6: Do XOR operation using the 5 bytes of data with 5 bytes of image block (grey value or color RGB value). Output the calculation result to the object image and go to step 4.
Step 6: Regroup the blocks

III. RESULTS AND DISCUSSIONS

The image is encrypted with initial parameters $(\alpha, \beta, \chi_0) = (1.47, 5, 3)$. In Figure 1a and 1b below, we show the histograms of RGB values of the plain images and those of the cipher images. The ideal histogram of a cipher image is uniform which indicates brute force attack on images make difficult.

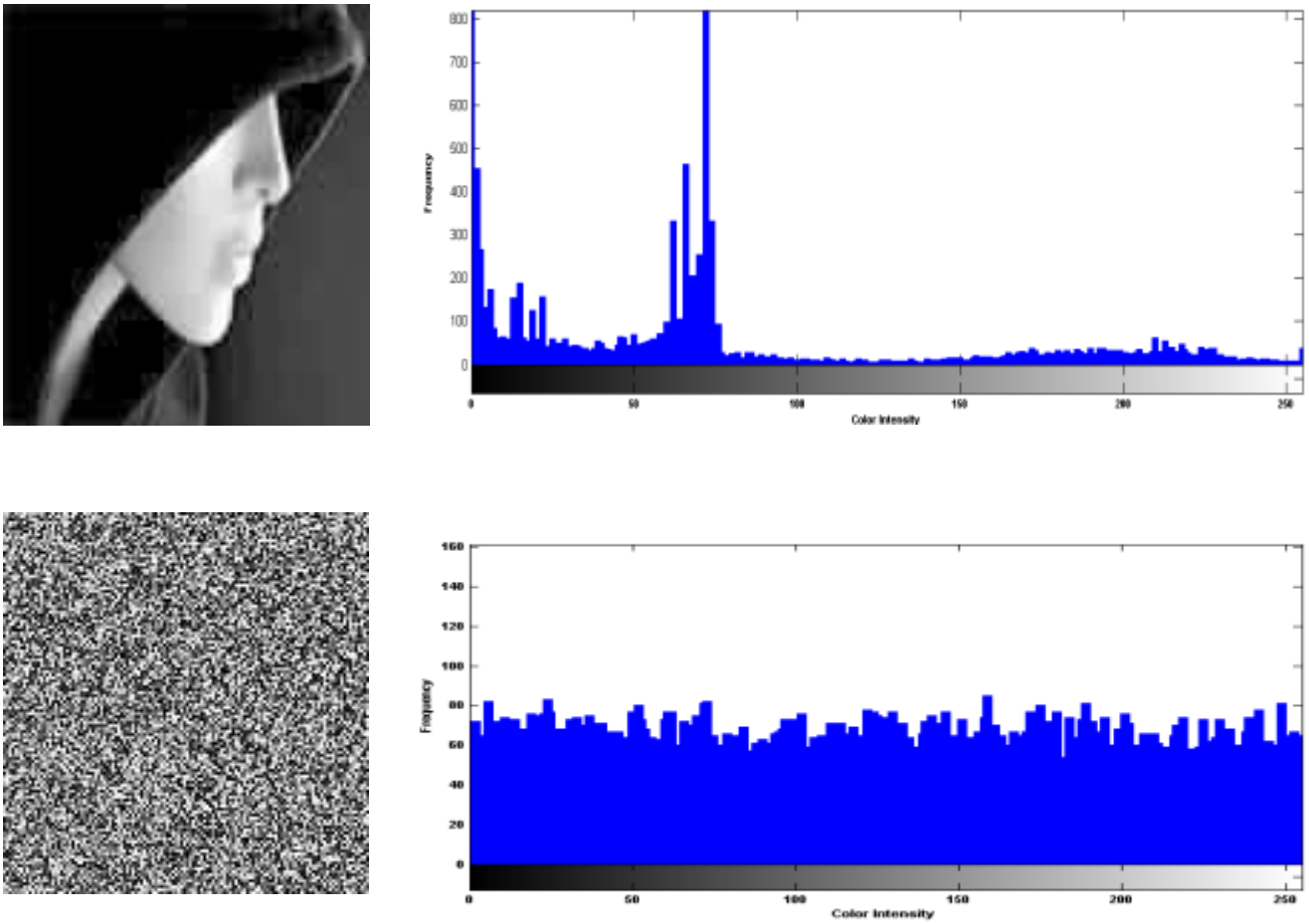

Fig. 1 (a) (b)

The histogram of the encrypted image is reasonably consistent and notably dissimilar from the original image which directly indicates if any statistical attack is performed on encrypted image, and then the attacker will not give any hint to know about original image. Image pixel correlations are calculated using the following formulae to predict the quality of the image after decryption.

$$E(x) = \frac{1}{N}\sum_{i=1}^{n} x_i \tag{4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{n} (x_i - E(x))^2 \tag{5}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{n} \big(x_i - E(x)\big)\big(y_i - E(y)\big) \tag{6}$$

$$\rho_{xy} = \frac{cov(x,y)}{\sqrt{D(x).D(y)}} \tag{7}$$

where E(x) is the expectations of x, D(x) is the variance of x and x, y are two neighboring pixel values, N is the total number of pixels of image. A perfect encryption means there should be no correlation between the neighboring pixels. The following figure 2 shows that.

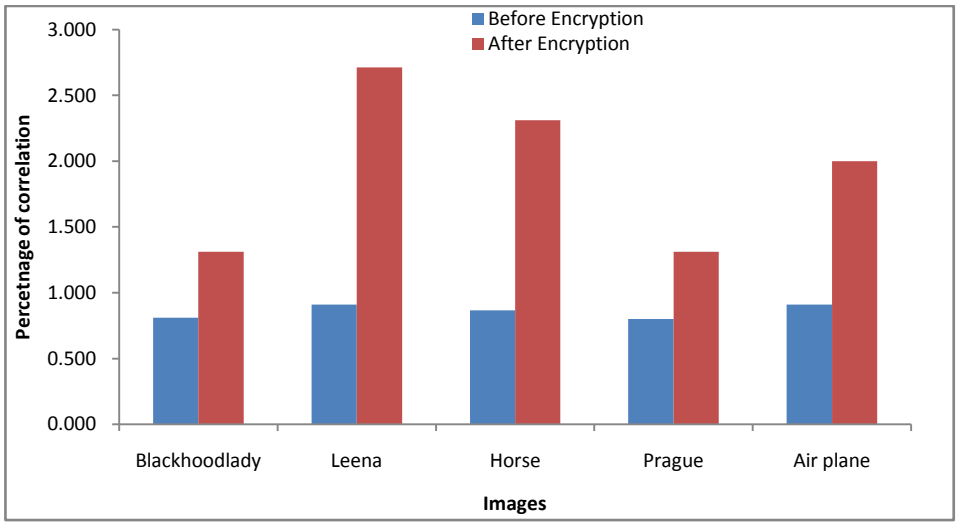

Fig. 2. Correlation Before and After Encryption

The percentage of correlation of both original and reconstructed image is close to each other which indicate quality of reconstruction of image from encrypted image is perfect. Since the complexity of the chaotic map is simple and even if it is introduced into an iterative function several times, the time for creating key space is negligible (less than 5 msec). This directly shows the encrypting and decrypting an image using NCM is more comfortable than the linear maps. For testing the sensitivity of the key, a wrong key is used to decrypt the encrypted image with same initial parameter values and it is important to note that image is still strange as seen in figure 4.

The difference of Number of Pixel Change Rate (NPCR) is estimated between the image which is encrypted using original key and wrong keys and we identified that the difference is random. During the each iteration, the algorithm generates 32 bit precision value among which first 15 precisions were taken into consideration as a key and it is XORed with pixel values. In addition to that 3 control parameters are used in the algorithm. If n is the number of digits of a key and the number of control parameters are m then 10^n^m possible keys can be generated which makes brute force attack impractical.

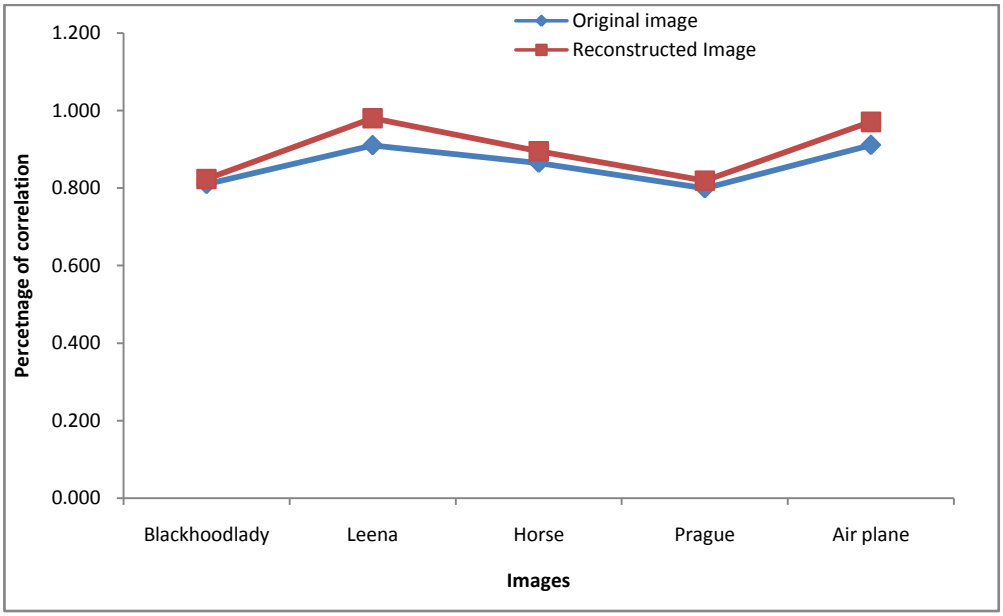

Fig. 3. Correlation between Original and Reconstructed Images

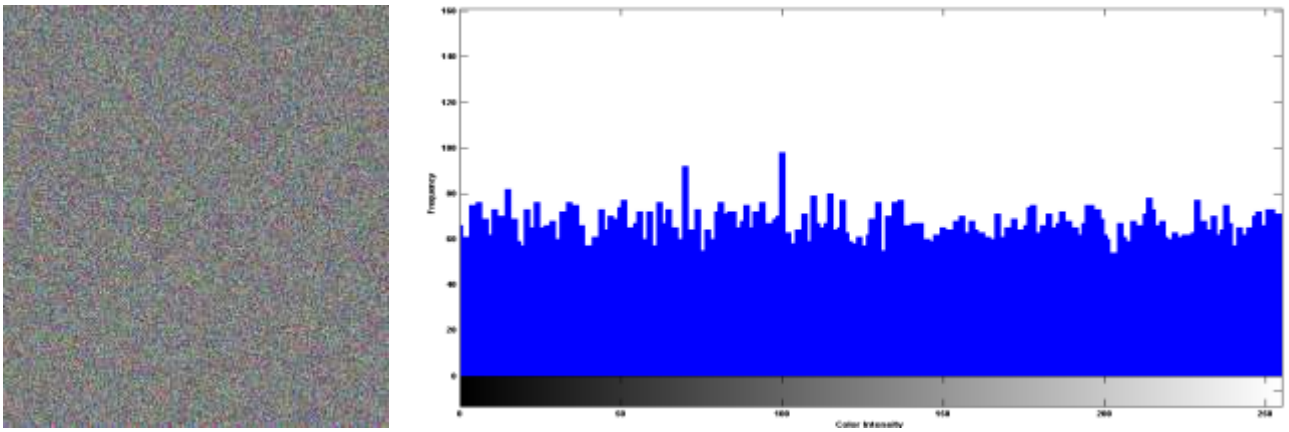

Fig. 4 Decryption using wrong key

IV. CONCLUSION

Non linear chaotic map is used in this paper to encrypt images, the result shows that the proposed method is performing well in terms of security. The key space generated by the algorithm is high enough against the several attacks. The percentage of correlation of both original and reconstructed image is close to each other which indicate quality of reconstruction of original image from encrypted image is perfect.

REFERENCES

[1] Somaya Al-Maadeed, Afnan Al-Ali, and Turki Abdalla, A New Chaos-Based Image-Encryption and Compression Algorithm, Journal of Electrical and Computer Engineering, Article ID 179693, 2012.

[2] H.E.Ren, Z. Shang, Y. Wang, and J. Zhang, 2007 ―A chaotic algorithm of image encryption based on dispersion sampling,‖ in Proceedings of the 8th International Conference on Electronic Measurement and Instruments, 2, 2007, 836–839.

[3] C. Fu and Z. Zhu, 2008 ―A chaotic image encryption scheme based on circular bit shift method,‖ in Proceedings of the 9thInternational Conference for Young Computer Scientists (ICYCS'08), 522, 2008, 3057–3061.

[4] H.E.Ren,J.Zhang,X.J.Wang,andZ.W.Shang, 2007 ―Block sampling algorithm of image encryption based on chaotic scrambling, Proceedings of the International Conference on Computational Intelligence and Security Workshops (CIS '07), 109, 2007, 773–776.

[5] Xia Huang, Tiantian Sun, Yuxia Li and Jinling Liang, A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System, Entropy, 17(1), 2015, 28-38.

[6] http://wwwmpa.mpa-garching.mpg.de/~dnelson/storage/ucb.phy111.spr2007/dnelson.nld.pdf

[7] S Sankar, and S Nagarajan, ZZRD and ZZSW: Novel hybrid scanning paths for squared blocks, International Journal of Applied Engineering, vol. 9, issue 21, pp. 10567-10582, 2014.