



A New Encryption Method Using Chaotic Logistic Map

Kavita Chaudhary
IEC Gr.
Noida, India

Shiv Saxena
Asstt. Prof. in CSE
IEC Gr. Noida, India

Abstract—Encryption is to rearrange the message into difference form so that the message is keep secret. The goal of encryption is to provide an easy and inexpensive means of encryption and decryption to all authorized users in possession of the appropriate key and difficult and expensive means to estimate the plain text without use of the key Nowadays the Internet becomes popular and encryption technology becomes essential to everyone. Traditional encryption methods such as DES, RSA etc are widely used today and it seems to be computationally secure [1].

The Baptista proposed a Chaotic Encryption Method, which seems to be much better than traditional encryption methods used today [1]. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and lot of information. But it still has several problems, such as slow in speed and suffering from floating point operations and has less security. This project is to overcome these problems so that this technique is applicable [3].

The purpose of this project is to learn the method to use chaotic function in security purpose. Thus we can say that the technique of this encryption method for images and data are .more secure as compare to previous encryption method and we are sure that this technique is much more secured and enhanced the security.

Index Terms— Chaos-based RNG, S.N. cryptography, security.

I. INTRODUCTION

Cryptography is an important technique to keep private data secretly in order to avoid unauthorized access. Nowadays the Internet becomes popular and encryption technology becomes essential to everyone. Traditional encryption methods such as DES, RSA etc are widely used today and it seems to be computationally secure [1].

The Baptista proposed a Chaotic Encryption Method, which seems to be much better than traditional encryption methods used today [1]. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and lot of information. But it still has several problems, such as slow in speed and suffering from floating point operations and has less security. This project is to overcome these problems so that this technique is applicable [3].

On analyzing the chaotic cryptography model, there are random numbers generated by iteration method with help of one dimensional logistic equation as:

$$X_{n+1} = \mu X_n (1 - X_n) \dots \dots \dots (1)$$

Where μ varies from 0 to 4 and take initial condition $X_0 = 0.1$. Using the random numbers encrypted the data and messages to generate a secret key for encryption.

In this paper we modified logistic equation as:

$$X_{n+1} = X_n (1 - X_n)^b + (1 - b) X_n \dots \dots \dots (2)$$

And taking the initial value $X_0 = 0.1$, while $0.1 < X_0 < 0.9$. and 'b' is an extra parameter where $b = 0.5$. We generate the random numbers and apply algorithm to encrypted image to generate a secret key and them we are using that secret key for decrypt the image or data. Thus we can say that the technique of this encryption method for images and data are .more secure as compare to previous encryption method and we are sure that this technique is much more secured and enhanced the security.

II. CRYPTOGRAPGY

Cryptography is an important technique to keep private data secretly in order to avoid unauthorized access. Nowadays the Internet becomes popular and encryption technology becomes essential to everyone. Traditional encryption methods such as DES, RSA etc are widely used today and it seems to be computationally secure.

Cryptography is an important technique to keep private data secretly in order to avoid unauthorized access. Nowadays the Internet becomes popular and encryption technology becomes essential to everyone. Chaotic encryption is the new direction of cryptography and only few papers discuss on it. It makes use of chaotic system properties such as sensitive to initial condition and lot of information. There are one dimensional logistic map can be denoted by the following equation:

$$X_{n+1} = \mu X_n (1 - X_n) \dots \dots \dots (1)$$

Where, x_0 is the initial state, and $x_0 \in [0, 1)$; μ is a cryptographic key, X_n is a random number generated by the random number generator, and X_{n+1} is an iterated result. Here, we select $\mu = 4$, where one dimensional logistic map is chaotic equation.

III. CHAOS-BASE CRYPTOGRAPHY

The cryptographic schemes have suggested some new and efficient ways to develop secure data encryption [4]. These schemes have typical structure which performed the permutation and the diffusion stages, alternatively. However, most of algorithms be faced with some problems such as the lack of robustness, key space and level of security. The random number generators are intransitive in cryptography for generation of cryptographic keys, allegorically, secret keys utilized in symmetric cryptosystems [1, 2] and large numbers is intransitive in asymmetric cryptosystems [3, 5], because of unpredictable, should better be generated randomly. In addition, random number generators in many cryptographic protocols, such as to create challenges, blinding values, Monte Carlo methods are used [11, 13, 21]. Also, the random number generators are used more in the diffusion functions of the data encryption for diffused of data. In previous project, My work is to implemented the chaotic encryption program using different methods, evaluate and analyze its performance, try to overcome the problem of chaotic encryption methods, suggest some methods and concerns that is important in using chaotic encryption technique and propose some new methods to enhance chaotic encryption technique.

There are one dimensional logistic map can be denoted by the following equation:

$$X_{n+1} = \mu X_n (1 - X_n) \dots \dots \dots (1)$$

Where, x_0 is the initial state, and $x_0 \in [0, 1)$; μ is a cryptographic key, X_n is a random number generated by the random number generator, and X_{n+1} is an iterated result. Here, we select $\mu = 4$, where one dimensional logistic map is chaotic equation.

Using equation no. (1), where $X_n \in [0, 1]$, for a control parameter μ set to make (1) have a chaotic behavior, we can quickly and safely encrypt information for further transmission. We propose that the encryption of some character is the number of iterations applied in Eq. (1) to make its trajectory, departing from an initial condition X_0 , reach an interval associated with that character. We show a schematic representation of the way we associate the S-units alphabet with the S intervals. The number of iterations (ciphertext) is used together with the secret keys. The random number generators are used more in the diffusion functions of the data encryption for diffused of data. The chaotic encryption program using different methods, evaluate and analyze its performance.

IV. PROBLEMS

Cryptography is about communication in the presence of an adversary. It encompasses many problems like encryption, authentication, and key distribution to name a few. The field of modern cryptography provides a theoretical foundation based on which one can understand what exactly these problems are, how to evaluate protocols that purport to solve them and how to build protocols in whose security one can have confidence.

The most ancient and basic problem of cryptography is secure communication over an insecure channel. Party A wants to send to party B a secret message over a communication line, which may be tapped by an adversary

V. PROPOSED METHOD

In this proposal paper, we proposed a chaotic data encryption method based on Complex Random Number Generators (CRNG). These Super Random Numbers be generated by the iteration method with help of modified simple one dimensional logistic equation. In this paper, we have added an extra variable parameter 'b' in one dimensional logistic equation to modified this equation, where the values of extra parameter (variable) 'b' varies from 0 to 1 that means ($0 < b < 1$), but we are putting the value of variable 'b'=0.5, and initial condition value $X_0=0.1$, we generated complex random numbers (CRNG) by introducing the Iteration methods for chaotic cryptography model.

The modified logistic equation is as:

$$X_{n+1} = X_n (1 - X_n) * b + (1-b) * X_n$$

i.e. $X_{n+1} = f(X_n) * b + (1-b) * X_n \dots \dots \dots (2)$

Here b is an extra parameter which value may be 0 to 1. but take b=0.5 to generate sequence no.

So in the project, we used the chaotic cryptography model to encrypt the data and sending the value of secret keys as like X_n and value of 'b' by the sender to receiver. Hence there two values are needed to receiver as X_n and value of 'b' as compare to previous one value are needed to decrypted the data and messages. Thus we can say that with the value extra parameter (variable) 'b', we increases one level security as compare to previous one key encryption method and we are sure that this technique is much more secured and enhanced the security.

- Chaos theory suggests that small change in system, then ripple effect and change the long term behavior of the system [12].
- This is new method for generated chaotic sequences.
- Confuse the relation between Original Image and Encryption Image. Varying the pixel values and pixel position for image encryption technique [15].

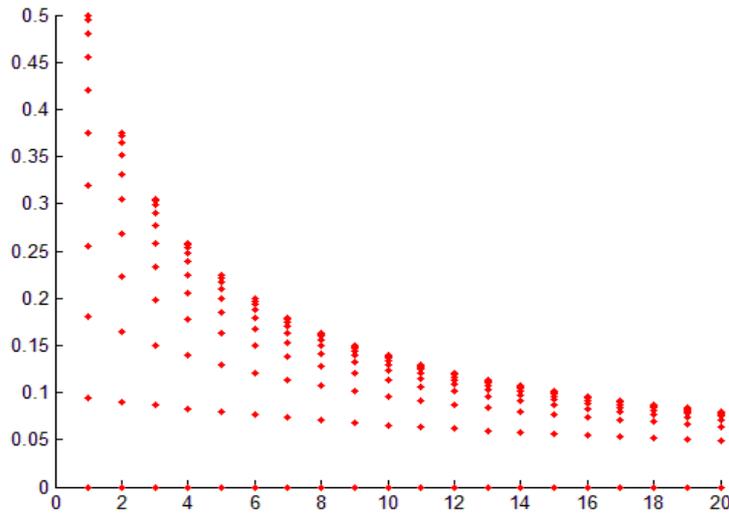


Fig.: Modified Logistic Behavior

VI. USED ALGORITHM

The step by step procedure by algorithm is discussed below as:

Step 1: Generate n number of chaotic sequences $x_i = \{x_1, x_2, x_3, \dots, x_n\}$ in the range 0 to 1 using modified logistic map with initial condition x_0 and taking the parameter $\mu = 3.999$.

Step 2: Transform the image of size $M \times N$ pixel into an array of $P_i = \{P_1, P_2, P_3, \dots, P_n\}$, where $i = 1, 2, \dots, n$ and $n = M \times N$.

Step 3: Next convert x_i into unsigned integer in the range of 0 to 255 using mod operation.

Step 4: Confusing the pixel values using bitwise XOR logical operations.

Step 5: Transform $C_i = \{C_1, C_2, C_3, \dots, C_n\}$ to an 2D array of size $M \times N$ to get the encrypted image.

So this is proposed algorithm by which we are generating the encrypted image to make secure

VII. SECURITY ANALYSIS

Security is a big issue in chaotic cryptographic algorithms. The aim of this paper is to produce a more secured algorithm for chaotic cryptography and its practical implementation. The generation of complex-random numbers is an important and common task in computer programming. While cryptography and certain numerical algorithms require a very high degree of apparent randomness, many other operations generated by iteration methods which depend on two values, first with the help of initial condition value $X_0 = 0.1$ and with the value of extra parameter (variable) 'b'=0.5. Using this super random numbers for encrypting the data to generates a secret key.

In previous paper random numbers depended only on initial condition value X_0 but in this paper we added extra parameter 'b', which is valuable for generating super random numbers so value of 'b' is needed for generates super random numbers that means the value of 'b' is needed for receiver so that's why one level security is increased as compare to previous proposed and cryptography technique is more secure. The one time pad-the only provably-secure encryption system uses as much key material as ciphertext and requires that the key stream be generated from a truly random process. Random numbers play an important role in the use of encryption for various network security applications so encryption method is secure and enhanced the securities in chaotic cryptography model. There is some security analysis as:

i) Key Space Analysis:

A key space is depending on the seed value from which we are generating the sequence numbers. The size of key is small as compare to other secret key.

ii) Key Sensitivity Analysis:

A good encryption process should be sensitive to a small change in secret keys i.e. a small change in secret keys in decoding process, the results will be completely different decoded image.

iii) Histogram Analysis

An image histogram is a type of histogram that acts as a graphical representation of number of pixels in a digital image. For right key, histogram will be same as plaintext's histogram but for change key it will be wrong histogram.

VIII. SIMULATION TOOL

All coding is done in MATLAB according to the given procedure. The proposed encryption algorithm is implemented in MATLAB for computer simulations. The matlab is easy for calculating mathematical results for given equation. All experiments are done in MATLAB using different original images to prove the validity of proposed algorithm.

IX. CONCLUSIONS

This encryption algorithm is secure because seed value applied on modified logistic map to generate sequence numbers then encrypted images. Security of the chaotic sequence totally depends on the seed value key. We will use this chaotic encryption technique for videos encryption in future work. I am going to summarize and propose the methods to improve the chaotic encryption base on the result collected in this paper. I will also describe the concerns and problems of chaotic encryption technique in this paper. So we can say that the security of an image encryption is increased.

- Chaotic method is necessary to increase their security for cryptography system.
- A high security Image encryption technique using modified logistic map function.

REFERENCES

- [1] K. Marton, A.Suciui, Christian Sacarea (NOV. 4/2012)“Generation & Testing of Random Numbers for Cryptographic Applications”. Romanian Academy, Series A, Volume 13, pp. 368–377.
- [2] A. Talha Yalta and Sven Schreiber (AUG. 2012). “Random Number Generation in gretl.. Journal of Statistical Software, Volume 50.
- [3] Sodeif, Y. Sadra and Zahra (MAR. 2012) “A Novel Chaotic Image Encryption using Generalized Threshold Function”. International Journal of Comp. Application Vol.42-No.18. Page No.(0975-8887)
- [4] R. Kadir & Mohd Aizaini Maarof(2011). “Randomness Analysis of Pseudorandom Bit Sequences”.
- [5] A.Kanso,H.Y.&M. Almulla(2011). “Keyed hash function based on a chaotic map”, Information Sciences, Vol. 186, Page No. 249–264.
- [6] Baptista, M. S. (1998 March 16). Cryptography with chaos, Physics Letters A, 240 (1-2), 50-54.
- [7] D. Chattopadhyay, M. K. Mandal, and D. nandi, “Robust chaotic image encryption based on perturbation technique,” ICGST-GVIP, Vol. 11, pp. 41-50, Apr. 2011.
- [8] M. Amin, O. S. Faragallah, and A. A. El-Latif, “A chaotic block cipher algorithm for image cryptosystems” Common Nonlinear Sci Numer Simulat, Vol. 15, pp.3484-97, 2010.
- [9] Z. Lin. and H. Wang, “Efficient image encryption using a chaos-based PWL meristor,” IETE Technical Review, Vol. 27, pp. 318-25, Jul-Aug 2010.
- [10] C. K. Huang, and H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” Optical communications, Vol. 282, pp. 2123-7, Feb. 2009.
- [11] A. Kanso, and N. Smaoui, “Logistic chaotic maps for binary numbers generations,” Chaos, Solitons and Fractals, Vol. 40, pp. 2557-68, 2009.
- [12] A. Kanso, N. Smaoui, Logistic chaotic maps for binary numbers generations, Chaos, Solitons and Fractals 40 (5) (2009) 2557–2568.
- [13] G. Alvarez, and S. Li, “Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption,” Common Nonlinear Sci Numer Simulat, Vol. 14, pp. 3743-9, Nov. 2009.
- [14] X. Y. Wang, and Q. Yu, “A block encryption algorithm based on dynamic sequences of multiple chaotic systems,” Common Nonlinear Sci Numer Simulat, Vol. 14, pp. 574-81, 2009.
- [15] T. Geo, and Z. Chen, “Image encryption based on a new total shuffling algorithm,” Choas, Solitons and Fractals and Vol. 38, pp. 213-20, Jan 2008.
- [16] R. Rhouma, and S. Belghith, “Cryptanalysis of a new image encryption algorithm based on hyper chaos,” Phys Lett A, Vol. 372, pp. 5973-8. 2008.
- [17] D. Knuth, The Art of Computer Programming, Sorting and Searching, second ed., vol. 3, Addison-Wesley, 1998.
- [18] P. L’Ecuyer, R. Simard, TestU01: a C library for empirical testing of random number generators, ACM Transactions on Mathematical Software 33 (4) (2007). Article No. 22.
- [19] Y. Wang, X. Liao, D. Xiao, K. Wong, One-way hash function construction based on 2D coupled map lattices, Information Sciences 178 (2008) 1391– 1406.
- [20] A. Kanso, N. Smaoui, Irregularly decimated chaotic map(s) for binary digits generations, International Journal of Bifurcations and Chaos 19 (4) (2009) 1169–1183.
- [21] H. Kwok, W. Tang, A chaos-based cryptographic hash function for message authentication, International Journal of Bifurcation and Chaos 15 (2005) 4043–4050.
- [22] Gonzalo Alvarez and Shujun Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” Int. J. Bifurc. Chaos, vol. 16, no. 8, pp. 2129– 2151, 2006.
- [23] S. Lian, G. Chen, A. Cheung, Z. Wang. A chaotic-neural-network-based-encryption algorithm for JPEG2000.
- [24] M. K. Khan and J. S. Zhang. Investigation on pseudorandom properties of chaotic stream cipher. Proc. IEEE.
- [25] International Conference on Engineering of Intelligent Systems, 2006, pp. 1-5.
- [26] X. F. Liao, X. M. Li, J. Peng, et al., A digital secure image communication scheme based on the chaotic Chebyshev map, Int. J. Common. System. 2004, 17 (5): 437-445.
- [27] H. Jian, Y. Mao and Z. Wang. A Novel Chaos-Based Video Encryption Algorithm. Proc. of Trim Size: 9in x 6in, 2004.
- [28] J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.
- [29] C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software 58 (2001) 83–91.

- [30] S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method, in: Proceedings of the IEEE International symposium on circuits and systems, Scottsdale, AZ, USA, 2002.
- [31] S. Li, X. Zheng, X. Mou, Y. Cai, Chaotic encryption scheme for real time digital video, Proceedings of the SPIE on electronic imaging, San Jose, CA, USA, 2002.
- [32] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption based on 3D chaotic maps, *Chaos Solitons Fractals* 21 (2004) 749–761.
- [33] N.K. Pareek, Vinod Patidar, K.K. Sud, Discrete chaotic cryptography using external key, *Phys. Lett. A* 309 (2003) 75–82.
- [34] N.K. Pareek, Vinod Patidar, K.K. Sud, Cryptography using multiple onedimensional chaotic maps, *Commun. Nonlinear Sci. Numer. Simul.* 10 (7) (2005) 715–723.
- [35] Ercan Solak , et.al have recently proposed, an encryption algorithm based on two-dimensional discretized chaotic maps, vol. 313, pp. 162–189, 2003.
- [36] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, Nov. 1976, pp: 644–654.
- [37] James Gannon, *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*, Washington, D.C., Brassey's, 2001, ISBN 1-57488-367-4.
- [38] Carlo Piccardi, "On parameter estimation of chaotic systems via symbolic time-series analysis," *Chaos*, vol. 16, pp. 043115:1–10, 2006.
- [39] Kai Wang, Wengjiang Pei, Shaoping Wang, Yiu- Ming Cheung, and Zhenya He, "Symbolic vector dynamics approach to initial condition and control parameters estimation of coupled map lattices," *IEEE Transactions on Circuits and Systems-I: Regular Papers*, vol. 55, pp. 1116– 1124, 2008.