ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 9 September 2013 Page No. 2733-2736

A DISCRETE CHAOTIC ENCRYPTION ALGORITHM USING LORENZ ATTRACTOR

[1]Rahul Ramakrishna and [2]Rajeswari Seshadri

[1] III rd Year B.E Department of Computer Science and Engineering
[2] Professor & Head, Department of ComputerApplications
Sir M Visvesvaraya Institue of Technology , Bangalore India
Email: [1] rahul8590@gmail.com & [2]oviaraji@yahoo.com

Abstract— **This Communication of critical information over global computer network needs encrypting the digital information before transmitting through the network. In this research article, a novel idea is proposed for a Discrete Chaotic Data encryption/decryption Algorithm using Lorentz attractors. The encryption system consists of a chaos generator, which takes the input message as the plain text and produces an independent output message known as cipher text. In the present approach the data to be transmitted is digitally modified by the chaotic system to produce the cipher text, which is sent through the transmission medium and the reverse process occurs at the reception end to decrypt the data. The essence of the present procedure is to use complex dynamics but simple mathematical descriptions and algorithms of chaotic systems for the purpose of encryption. The combination of these techniques results in a system that is extremely simple to implement, yet results cryptographically very robust. Also it will be highly resistive to differential and statistical attacks. The algorithm is independent of the data size to be encrypted and has been verified for several sets of input data consisting of all allowable characters. A preliminary test is also made to check the strength of the key and the results are very encouraging. Several analysis is been carried out to validate the strength, arbitrariness and the entropy of this newly proposed algorithm.**

Keywords; ***chaotic system, encryption methods, computer network***.

I. INTRODUCTION

With the development of information technology and the proliferation of the Internet and maturation of digital signal processing technology, the research on Data security is becoming more and more vital.

Chaos theory based data encryption is given much attention in the current research on information security. Complex systems like chaotic systems possess intrinsic characteristics that are reliable and very highly secure. Supplementing active parameters to a chaotic system makes the encryption dynamically changing and impregnable, even slight changes in input parameters will never lead to identical series and delivers unpredictable trajectories.

Data encryption is widely used to ensure security. A large number of encryption technologies have been suggested and investigated in the literature[1,2,3]. These technologies are not very reliable for secure transmission of data any more.

The currently adopted encryption schemes like RSA — Rivest - Shamir - AdelmanAES—Advanced Encryption Standard, and IDEA -International Data Encryption algorithm, cannot handle the latest challenges [4]. However the rapid development of networking systems and telecommunication services demand more high standards of reliability, security and privacy in data communication against statistical and differential attacks [5].

II. CHAOTIC SYSTEMS

A. Chaos Theory

Chaos theory is a scientific discipline that focuses on the study of nonlinear systems that are highly sensitive to initial conditions, and it is highly deterministic, unpredictable, nonlinear and very sensitive to initial conditions and perceptual random behaviour. These properties make chaos theory a good and attractive option for cryptography.

In 1989, Matthews [1] was the first one to propose discrete chaotic dynamic systems in cryptography. Poincaré was the first to address [*] the possibility of chaos, in which a deterministic system exhibits a periodic behaviour that depends sensitively on initial conditions, thereby rendering long term prediction impossible.

B. *Chaotic Schemas*

The chaotic schema represents the output from the following mathematical models.

1. Logistic Mapping

This map is a simple idealized ecological model for yearly variations in population of an inspect species. For its

$X_n = \lambda X_{n-1} (1 - X_{n-1})$ where $\lambda \varepsilon \{1,4\}$, $X \varepsilon \{0,1\}$ (1)

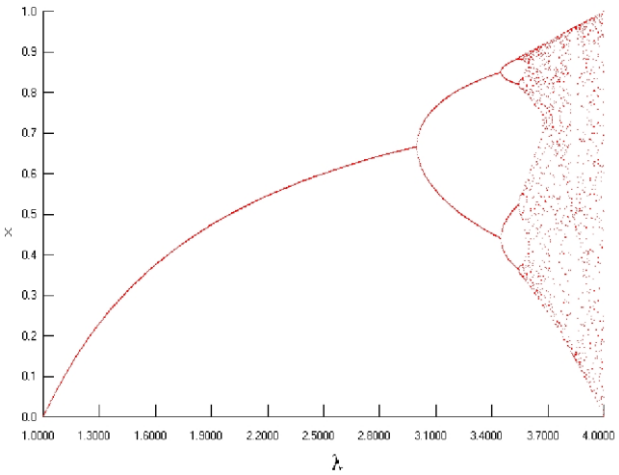

Fig 1. Logistic Mapping Graph

The bifurcation property of the logistic mapping is shown in Fig. 1. As λ increases from 1 to 4, map experiences a period doubling of chaos. If λ > 3.5 it shows chaotic behaviour .The logistic mapping have a significant drawback, since the number of iterations for a chaotic state is finite. A chaotic system built on this mathematical model will be short cycled in spite of its sensitivity to initial conditions. The existence of many short period windows that appear reveals statistical information that causes significant damage for the encryption
system which is helpful for the attackers.

2.Lorenz Equations

The Lorenz equation was proposed by E.N. Lorenz in the year 1963. The equation is the model of thermally induced fluid convection in the atmosphere. The Lorenz equation is given by

$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = rx - y - xz$$
$$\frac{dz}{dt} = xy - bz$$

Where 'x' is proportional to circulatory fluid flow velocity, 'y' characterizes the temperature difference between rising and falling fluid regions, 'z' characterizes the distortion of the vertical temperature profile from its linear with height equilibrium. The parameter 'σ' is related to Prandtl number, the parameter 'ρ' is related to Rayleigh number and 'β' is a geometric factor.

III. Data Encryption Scheme

Detail studies have been carried out and innovative method pertaining to encryption/decryption scheme is proposed as an asymmetric cipher block incorporating the following process.

mathematical simplicity and fair chaotic properties, logistic maps can be used. The logistic map is represented by the equation (1)

System Key Generation using RANROT.
Dynamic generation of Lorenz keys.
An encrypted stream of data.

A. Encryption Methodology

The encryption methodology defines the procedure of encryption process. Initially a seed is generated using RANROT [10], simultaneously the initial condition and the RANROT key are input to the Lorenz equation. The initial condition for the Lorenz equations are influenced by active parameters which makes them dynamic in nature and constantly changing in discrete time periods. Based on the initial conditions the Lorenz co ordinates are generated where in the RANROT key defines the row number to which the Lorenz data has to be extracted. The corresponding X, Y, Z coordinates are denoted as K0, K1, K2 keys as in Fig 2.

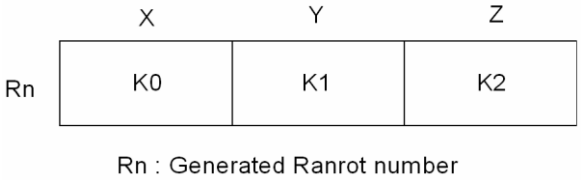

Fig 2. The Extraction of Key from Lorenz Attractor

Table 1, shows a sample data of X, Y and Z coordinates generated for 2000 rows (N=2000) solving the Lorentz equations with the initial conditions (-2,-2,15). If the row number assigned by the key is 1998, for example, the corresponding row is selected and the values of K0, K1 and K2 are 0.0297125844, 0.579474823478 and 12.25340536043, respectively.

TABLE 1

Coordinates Computed from Lorentz Equations

Rw No.	X-coordinate K0	Y-Coordiante K1	Z-Coordinate K2
IC	-2.000000000	-2.00000000000	15.0000000000
1.	-1.9982196969	-1.964747373587	14.78142991679
2.	-1.9937052779	-1.938765328252	14.56585186360
3.	-1.9875820638	-1.921697293347	14.35348699984
.	. . .	. . .	
.	. . .	. . .	
N-2	0.0297125844	0.579474823478	12.25340536043
N-1	0.08160263792	0.5712159790549	12.01141142357
N	0.12793491903	0.5664015509300	11.77475425697

The plain text entered by the user is been referred to a one-one mapped data structure exclusively designed for our encryption scheme where it is converted to its number equivalent. Each of the digits generated will be treated as a single entity. The generated Lorenz keys are converted into

stream of numbers from where the pairs of the streamed numbers will be formed in such a manner that they do not exceed the maximum limit defined in the one-one mapped data structure. The pairs generated by the keys are then summed up to the number equivalents of plain text, thus forming a ciphered text.

B. Decryption Methodology

When the encrypted data is received by the genuine user , the Lorenz parameter and the RANROT key is extracted from the data from which the key is again derived. The derived keys are again streamed into pairs. The encrypted text is been converted to its number equivalent and then subtracted from the stream of keys generated from the Lorenz to fetch the plain text.

C. Advantages of Present Encryption Algorithm

The present approach overcomes various key exchange methods. In DH key exchange methods and others, it is assumed that the key is communicated through a secure channel and then the data is transmitted through insecure channel, where the attacker is vigilant. Although the contention is apparently impregnable, it is very unlikely that the attacker might not be able to lay hands on secure channel. For this we have developed a unique approach of communicating keys, by sending the initial parameters of the

Lorenz equation and the generated RANROT key with the encrypted text. Even if the attacker manages to fetch the data during transmission, the sent parameters will be apparent to be keys, although they are means to generate the keys to decipher the encrypted text. In the worst cases, if the attacker gets to know they are Lorenz parameters, he still may not be able to completely decipher since, the Lorenz generation method is discrete and clandestine.

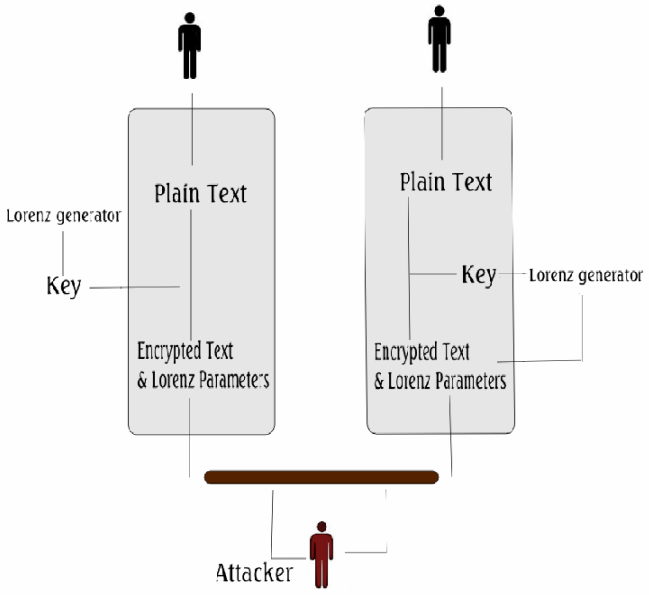

Fig 2: Illustration of Chaotic cryptosystem

To make sure that the decryption process gives the correct data from the encrypted text, the genuine user is also supplied with the Lorenz generation method used for encryption.

There are many unique ways to generate Lorenz data and there are finer nuances in generation of keys. Thus our Algorithm on dynamic chaotic encryption system based on chaos theory provides protection of data from unauthorized modification during transmission.

IV ANALYSIS

The present analysis is done, by solving the Lorentz equations with the fourth order Runge-Gutta method of solving non-linear differential equations. The initial values considered for our calculations is (-2, -2, 15). The solutions are generated for 2000 steps and are stored as an input data for our entire encryption analysis. How ever, the present algorithm can be applied to any permissible initial conditions and K0, K1 and K2 can be generated for any given row number specified by RANROT.

A sample text fed into our present algorithm and their ciphered texts are shown in Table 2. The same text when encrypted with a single character change in the key gives an entirely different ciphered text. Hence, even if an attacker tries the brute force attack, and gets all possible key values to decrypt one or more blocks of data he can never get a sensible value of the text at all. The reason is that a stream cipher converts the plain text and transforms in to a cipher text by generating what is known as the KEY stream.

TABLE 2
Sample Encryption for a Plain Text

Plain Text	Encrypted Version
The fox jumps over the dog	W0s&lv5+tunrv%t1j%}$wv=w 81

Cipher Strength or Encryption Strength is referred to is the length of the key. In order to demonstrate the value of a long key, let's say that one is using an 8-bit key. In this case, the attacker only has to perform a maximum of 256 guesses before he knows the key. In reality, though, he'll only have to perform less than half that many steps before his chances of success begins to exceed 50%. In the case of a 40-bit key, the attacker will have to perform a maximum of just over a trillion steps, but in reality, about 500 billion would give him a good chance of success. This is completely feasible given time and the power of modern processing. Even 64-bit keys are now being considered weak, and 128-bit is pretty much the standard today. All these are possible because of the rapid advance of processing technology, a process that is likely to continue for the foreseeable future.

This is taken care of in our present methods of communicating keys, by sending the initial parameters of the Lorenz equation and the generated RANROT key with the encrypted text. Even if the attacker manages to fetch the data

during transmission, the sent parameters will be apparent to be keys, although they are means to generate the keys to decipher the encrypted text. Table 3 gives the strength of our key generation indicating the fact that a very slight change in the initial conditions can give rise to a totally different cipher text.

TABLE 3
Encrypted Text with one character change in keys

Plain Text	Encrypted Version
The fox jumps over the dog	(i)W0s&lv5+tunrv%t1j%}$wv=w81 (ii) Xmk)i97?kwpty)9(z$?!yt<pzq (iii)Ujh%ku4*s468 =5"r5!yth%i.! (iv)Vkf%kv5+j0yq3,2!z.Gx/+Q4)0 (v) bKj16&* &=^tyf$RaQ>7fgb0(uY

It can be seen from the table that the cipher text generated are completely disjoint between themselves For, the sample text 'Hello', the encryption fetched by other ciphers and the frequency distribution of their characters are given in Fig. 3.

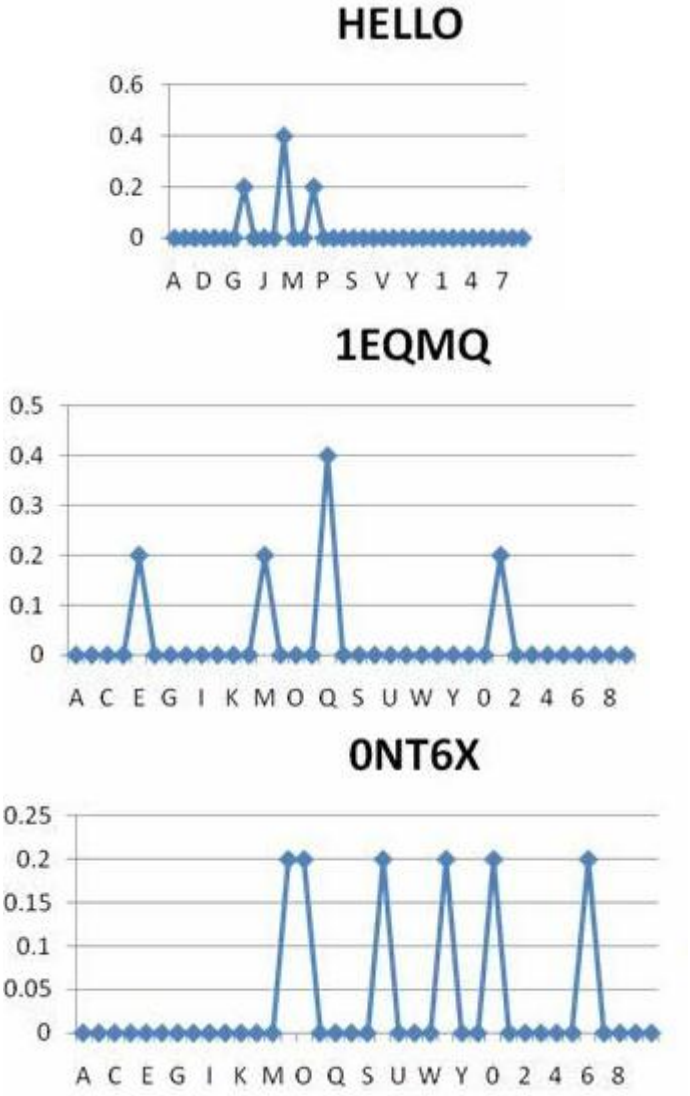

Fig. 3 Frequency Distribution of Characters for the Plain Text 'Hello' and its encrypted texts using two different Initial Conditions

We have tested various other substitution ciphers like Caesar/ Rot 13 , Vigenere, Hill and Substitution. Caesar Cipher gives 'yvccf' (When the intial key entry is r). From frequency distribution of the ciphered text, the cipher is susceptible to brute force attacks, which in turn makes the cipher weak. Vigenere Cipher gives 'lrncm' (when key provided is "encrypt"). An extension of Caesar cipher, even though it tries to hide the frequencies of the occurrence of the characters, there exist a pattern. Besides a truly random and strong key is required to strengthen the cipher.

In our cipher, on testing the same "hello" text, the code fetched was "0NT6X". The novel idea of our cipher is that, it is not dependent on a fixed key basis, rather the length and the comprehensiveness of our data structure which is a one to one mapped correspondence.

For example, if the user decides to create the data structure to be of length 86, then there is 86 combinations. Larger the Data structure, more the number of combinations will be provided. Thus, making the cipher independent of key size. In our approach, since it's based on truly random Lorenz equation, the key generated to encrypt the text is always random and different.

V Conclusions

In this paper, we proposed a new dynamic data encryption scheme using a chaos theory based Lorenz attractor model. The strength behind this scheme is the use complex dynamics can be employed to protect sensitive information and maintain security and privacy information. Thus, this is best suited to computer networks.

We are also trying to implement this cipher augmenting with the concept of network processors , where in the network processor will hold the complete network stack and an encryption engine to be built within it to ensure the data is completely secured and the host processor is relieved from the burden of processing the network stack.

References

[1]. G. A´ lvarez, F. Montoya, G. Pastor, and M. Romera, *Proc. IEEE*

[2]. Int. Carnahan Conf. Security Tech. (1999) 332.

[3]. P.M. Binder and R.V. Jensen, *Phys. Rev. A* **34** (1986) 4460.

[4]. I.J. Cernak, *Phys. Lett. A* **214** (1996) 151.

[5]. G. Jakimoski and L. Kocarev, *IEEE Trans. Circ. Syst.-I* **48**(2001) 163.

[6]. G. Jakimoski and L. Kocarev, *Phys. Lett. A* **291**(2001) 381

[7]. N.K. Pareek, V. Patidar, and K.K. Sud, *Phys. Lett. A* **309** (2003) 75

[8]. M. Yang, N. Bourbakis, and S. Li, *IEEE Potentials* (2004) 28.

[9] T. Habutsu, Y. Nishio, I. Sasase, S. Mori: A Secret Key Cryptosystem by Iterating a Chaotic Map, *Proc. Eurocrypt*, 127-139, 1991.

[10] A.Fog, Chaotic random number generators with Random cycle *lengths*. http://www.agner.org/random/theory/chaosran.pdf