Generation of Image Encryption Key on the basis of Chaos and Strange Attractors

Saurabh Pratap Singh[1], Dr. Devender Jha[2], Sunil kr. Singh[3]

(1) U.G. Research Scholar, NSIT, New Delhi

(2) Senior Scientist, SAG, DRDO, New Delhi

(3) Associate Professor, BVP, Delhi

Abstract—**In the paper, a chaotic key-based algorithm (CKBA) for image encryption methodology is proposed, which is a value substitution cipher. This paper estimates its security and points out that known-plaintext and chosen-plaintext attacks can break it with only one known plain-image making it highly secure and brute force attacks cannot break it. In addition, its security to brute-force attack is very high due to the stochastic behavior occurring in a deterministic system. So this key is secure atall from the strongly cryptographic viewpoints. Lorentz attractors are heavily dependent on initial condition and have the lowest level of predictability lead to use fullness in the encryption of any form of information either image or text.Encryption based on Lorenz strange attractor has been studied and applied.**

Keywords: chaotic systems**,** stochastic, cryptography, stream cipher, lorenz equations

I. INTRODUCTION

THEconsiderations of privacy in the computer environment have given recognition to the need for protecting some communications and stored data from theft and misuse by others. A suitable methodology for protecting communicated or stored data involves the use of cryptographic techniques to secure the data from misuse. Cryptography is the study of mathematical techniques related to the aspects of information security such as confidentiality, entity authentication and data origin authentication. A message is plaintext. The process of disguising a message in such a way as to hide its substance and present in another form is encryption.

The encrypted message is called ciphertext. The process of turning ciphertext back into plain text using a particular key is called decryption. Basic operations that can be carried out in encryption or decryption are: substitution and transposition. Due to advent of computers, these operations are carried out on binary bits and hence bitwise operations are used.

Due to the arrival of internet, there has been development of a worldwide 'Virtual Community' free from the constraints oftime and geography. Due to the Internet there is no distance between a person located in one place and experts all around the globe and information is shared with ease. Through electronic mail / voice mail / video mail it is possible to solicit the opinion of experts from all across the world. Moreover, Telemedicine is becoming popular in the specialties of radiology, pathology and psychiatry, where data is in the form of image and sent through internet. It is hence required to ensure the confidentiality and security for the transmission of image-based data via the Internet. The aim of security management and encryption is to provide authentication of users and integrity, accuracy & safety of data resources of any type. This model for encryption & decryption of an image is designed with the same purposes. The basic working of an encryption algorithm is demonstrated in [6][12][13][14].

II. INTRODUCTION TO CHAOS THEORY

Chaos brings to mind an image of complete randomness, of disorder and anarchy, which cannot be predicted. It is similar to a mob rushing down a city street,messy room and a swarm of bees. Definition of the word "chaos" itself makes it a hot research area.Chaos based bidementional image encryption mechanisms have been developed in the recent past[2][3][10][12].Chaos can be defined as…

Stochastic behavior occurring in a deterministic system

The Greek word stochastikos means `skillful in aiming' and thus conveys the message of using the laws of chance as an assistance.

Stochastic behavior is probabilistic behavior. Probability is the branch of mathematics - the one that can't provide any specific answers to the outcomes of system, but can predict how likely a specific outcome is to occur. In a single die roll probabilistic system: there is a one out of six chance of getting a one on a certain trial. We cannot predict the outcome of the die rollexperiment, but we can attach some numbers to how regularly certain events happen.

By using both stochastic and deterministic together, mathematicians have made a bridge between the two sciences - that were regarded as mutually exclusive. Chaos refers to the study of deterministic systems which are so sensitive to measurement that the output appears random but can be determined.

Lorenz chaos theory was evolved so as to model the weather system using set of dependent differential equations. It isobserved that even the minutest calculation approximations will lead to drastic changes in the output.

The extent of these drastic changes can be estimated even by the name of the publication [5][7][8][9][11] which estimates the randomness of the system.

Sensitive dependence on initial conditions is referred to as ``The Butterfly Effect."

Sensitivity to the initial conditions of the systemis the basic distinction of lorenz system. It states that, each point in such a system is arbitrarily closely approximated by the other points which are significantly different future trajectories. Thus, an arbitrarily and small perturbation of the current trajectory will lead to a significantly different behavior of the curve in the future . The last two properties actually imply sensitivity to initial conditions and if attention is restricted to intervals, the second property leads to the other two (an alternative, and in a weaker, definition of chaos which uses only first two properties). It is very interesting to note that the most practically significant and useful condition, that of sensitivity to initial conditions, is actually redundant in the definition, being implied by two , purely topological conditions, which are therefore of greater interest for the encryption process.

III. LORENZ SYSTEM

$$\frac{dx}{dt} = -10x + 10y \qquad (1)$$

$$\frac{dy}{dt} = 28x - y + xz \qquad (2)$$

$$\frac{dz}{dt} = -\frac{8}{3}x + xy \qquad (3)$$

Lorenz's system is three-dimensional system, the three variables: x, y and z which represent the geometric location of the points in the space. If the Lorenz's system had been two-dimensional, existing on a plane like this text exists on a page, then only two variables would be required, x and that, is the horizontal and vertical. Here we have three, a space with volume.

Lorenz's system, although simple in the eyes of a physicist or mathematician, but is actually an insolvable problem except by numerical means of solving. To aid in the understanding of the system, since these couldn't have been solved by hand, a simple program is developed to numerically solve Lorenz's system of equations. The program, allows the user to specify a set of initial conditions and outputs data in a suitableformat for importing into a spreadsheet or graphing package. The following plots are the sample runs for the system which are subjected to arbitrary initial condition set of x=y=z=t=0.0001[8][15].

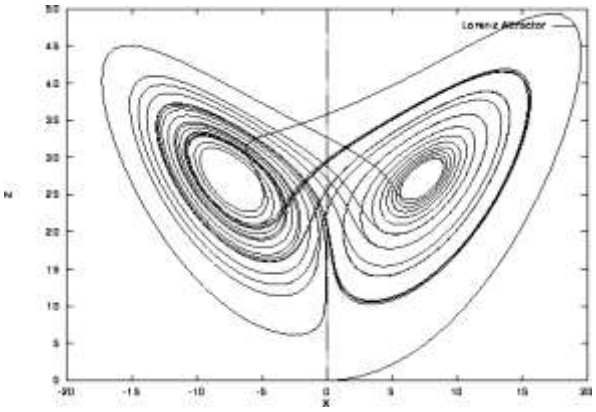

fig.1 :***3 D View Of The LorenzAttractor***

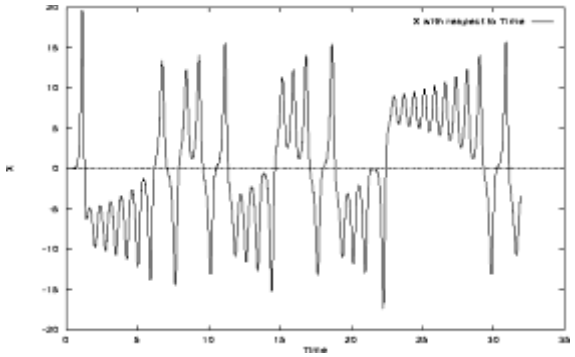

fig.2 : Plot Of X v/s T

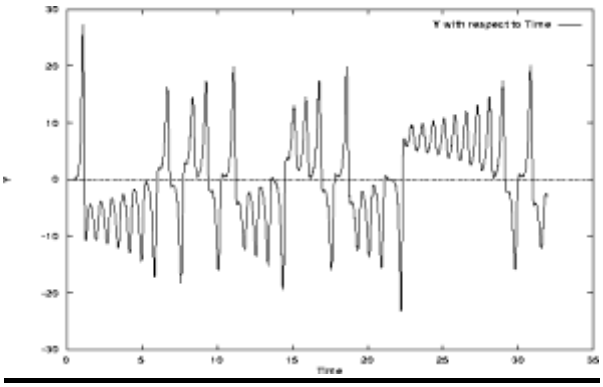

Fig 3: ***Plot Of Y v/s T***

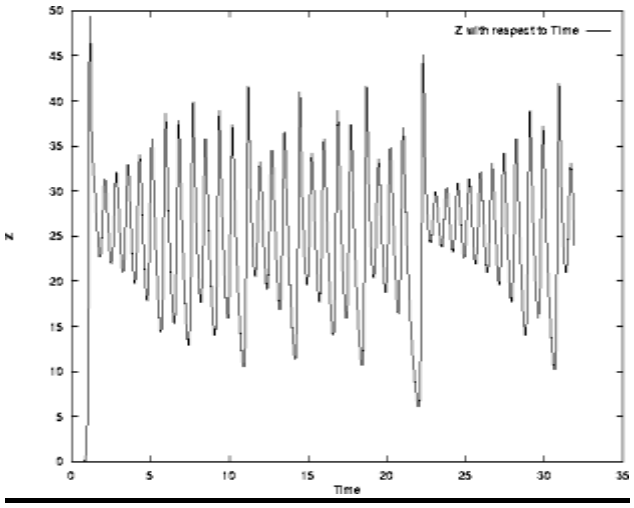

fig.4 :***Plot Of Z v/s T***

IV. Image Encryption Model

To aid in encryption, the function encrypt has been designed. It takes two parameters - the byte value *mybyte*to be encrypted and a long integer *curindex*that is used to parameterize the encryption. The function uses the following algorithm.

A. The Length of the Key is Calculated

The image size decides the length of the encryption key since the key is to be implemented on all the pixels so the length of the key is kept same as that of the number of pixels.

For instance if the image is of resolution 256x256 has a encryption key of the same length.

B. The grey levels of the image to be encrypted are extracted

The gray levels of the image are brought down in the form of an array giving information of all the pixels in the image.

C. The encryption key is developed

An interval of a particular duration(here 100 sec) is chosen along with a particular axis(here x axis).the 100 sec is divided in intervals such that the number of intervals become equal as the number of pixels.

This provides us with an array of elements and the array having the size of the image. It should be taken care that the value of the array elements is not exceeding the gray scale limit. If such a case is there the complete array is divided by an appropriate factor.

D. XOR the arrays

Once the 2 arrays are generated they are bitwise XOR operation is performed, generating a new array which is having all its elements in the gray scale range.

fig. 5 ***:Original Image***

fig.6 :***Encrypted Image***

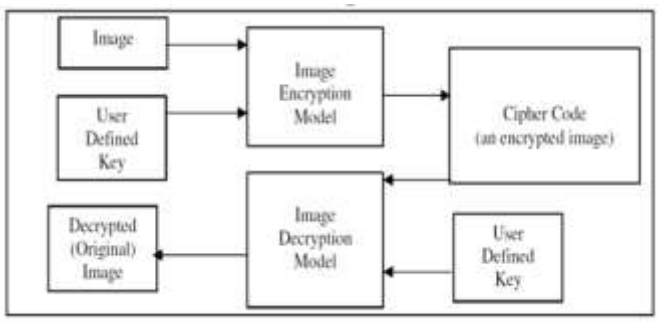

Fig. 7 ***:The Architecture of the image encryption and decryption model***

V. Application and Usability

The models for encryption and decryption of an image is used for transforming an image into cipher code by the user-supplied key, which allows users to have confidentiality and security in transmission and usage of the image based data as well as in storage in the data warehouse which has to protected from misuse.

An image encryption and decryption model uses user-defined key in generating a cipher code from an image. Hence, the same image may have different cipher codes, depending on the key supplied by the user without which the image or the data cannot be retrieved back.

REFERENCE

[1] Homomorphic image encryption.
Ibrahim F. Elashry, Osama S. Farag Allah, Alaa M. Abbas, S- El-Rabaie, Fathi E. Abd El-Samie.

[2] A new chaotic bidimensional map suitable for images encryption Lect. RaduBoriga.

[3] The RC6 TM Block Cipher
Ronald L. Rivest1, M.J.B. Robshaw, R. Sidney, and Y.L.Yin

[4] Security Analysis of a Block Encryption Algorithm Based on Dynamic Sequences of Multiple Chaotic Systems
DU Mao-Kang, HE Bo, WANG Yong

[5] Security Analysis of A Chaos-based Image Encryption Algorithm ShiguoLian, Jinsheng Sun, Zhiquan Wang

[6] Image encryption & decryption model, Dr. D. M. Shah, Reader, G.H.Patel Post Graduate Department of Computer Science and Technology Sardar Patel University, Vallabh

[7] Predictability: Does the Flap of a Butterfly's Wings in Brazil Set Off a Tornado in Texas?" by lorenz

[8] http://www.gweep.net/~rocko/sufficiency/node10.html

[9] A.S. Alghamdi, H. Ullah, M. Mahmud, and M.K. Khan, "Bio-Chaotic Stream Cipher- Based Iris Image Encryption," Proceedings of the International Conference on Computational Science and Engineering, 2009, pp. 739–744.

[10] H.H. Ahmed, H.M. Kalash, and O.S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images," Journal of Optical Engineering, vol. 45, 2006.

[11] A.N. Pisarchik and M. Zanin, "Image Encryption with Chaotically Coupled Chaotic Maps," Physica D, vol. 237, no. 20, 2008, pp. 2638–2648.

[12] C. I. Rancu, A. Serbanescu "Chaos – Based Cryptography. A solution for information Security", Buletin of the Transilvania University of Brasov, 2009.

[13] R. Boriga, A.C. Dascalescu, "Automated system for testing the period and randomness of a pseudorandom number generator", Megabyte, 2010.

[14] A. Jolfaei and A. Mirghadri, "An Applied Imagery Encryption Algorithm Based on Shuffling and Baker's Map," Proceedings of the 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR- 10), Florida, USA, 2010, pp. 279–285.

[15] G. Seroussi; CO. Hewlett-Packard, P Alto, "Elliptic curve cryptography", Information Theory and Networking Workshop, 1999.