INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

CHAOS-BASED IMAGE ENCRYPTION APPROACH USING BAKER'S MAP

Nalini Tiwari* and Karan Singh
Dept of Electronic & Telecommunication Engineering
Chhattisgarh Swami Vivekananda Technical University, Bhilai, (CG) - India

ABSTRACT

Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and (RSA) appear not to be ideal for image related areas, due to some internal features of images such as bulk data capacity and high redundancy, which are troublesome for traditional encryption, computational time and high computing power. Most of the these encryption schemes require extra operations on compressed image data, thereby demanding long computational time and high computing power. The chaotic cryptography is obtaining more attention than the others because of its lower mathematical complexity & better Security. It also avoids the data spreading hence reduces the transmission cost & delay. The digital image cryptography which is based on chaotic systems utilizes the discrete non-linear system dynamics generally called chaotic mapping. By combining them a large number of cryptographic techniques could be designed in this paper presents a chaotic baker map based cryptography technique, in the proposed technique; confusion and diffusion applied on spectral domain on DCT (Discrete Cosine Transform) coefficients hence the encryption can be achieved quickly without applying the large number of confusion and diffusion cycle as it is needed in spatial domain. Diffusion template is also created by random number generator based on Gaussian distribution. The technique is using Bakers map and it is capable to provide the key length of 128 bits although it's length can be extended further. The proposed technique is simulated using Matlab and the results will prove its robustness with all type of cryptanalytic tests and faster execution.

Key words: Image, Chaos, Baker map, Cryptography, Encryption, Security.

INTRODUCTION

For the past few decades, Chaos theory has been a branch of mathematics that has generated much interest, the notion of being able to describe complex nonlinear phenomena, such as the weather or stock market, using a series of deterministic dynamical equation is intriguing for many fields of study. The ability to generate _chaotic' unpredictable data using a series a relatively simple deterministic equation is attractive from a cryptographic point of view[8].Cryptography is the art and study science of securing messages. It an also be say that it is the practice and study of hiding information from others. Mathematically, cryptography has some certain unique requirements: diffusion, confusion and keys dependency. A chaotic system represents an ergodic behavior and a high sensitivity with respect to the initial conditions and the control parameters.

***Corresponding Author**
Email – nnt.tiwari@gmail.com
karanbains2002@yahoo.co.in

These are the main characteristics of chaos which have been exploited in the design of new strategies or ideas to encrypt information. Nevertheless, the efficiently good design of new chaos-based encryption systems cannot be done just by selecting a dynamical system that shows a chaotic behavior. Indeed, it is necessary to select the adequate dynamical system for the chosen encryption architecture. To have a good performance, the selected chaotic system is expected to be robust, which means it remains chaotic in a continuous range of the parameter space [10]. A lot of works about the chaotic cryptography develop the theories and methods concerned highly. The chaotic signal behaves as noise-like when observed as a whole, though, it follows deterministic rules defined by certain chaotic maps. These rules could be found as long as sufficient iteration details are gathered, the security system built on the chaotic maps is then broken [9]. Chaotic systems runs when on a computers, the finite precision effect will make the

chaotic orbits depart from the theoretic ones in a random manner. Eventually, the chaotic orbits converge to fixed values after necessary iterations and result in key in weak manner in the whole key space of the chaotic cryptosystem. This case is also well familiar as the dynamical degradation of chaotic systems. The feasibility of chaos used in cryptographic algorithm design lies on the selection of chaotic states in chaotic iteration trajectory to hide the deterministic rule among them, and differential analysis is a useful tool for the selection [9].This paper is intended to offer a chaotic map i.e. Baker map overview for the exploration of chaos-based cryptography.

Introduction to Chaos

Chaos theory is a branch of mathematics that deals with non-linear phenomena. These phenomena include weather, financial markets, weather, and organizational behavior, predicting epileptic seizures, fractals and other complex real world physical phenomena. To fully understand chaos based theory in cryptography, it is necessary to understand the key concept behind chaos. Chaotic phenomena are characterized by the fact that they are highly noticeable random, but have a precise mathematical formulation. Hence, given some other parameters they are repeatable/reproducible/predictable and yet apparently random. The properties required by cryptography are readily satisfied by chaotic functions via their properties of-

(a) Sensitive dependence on initial conditions (function parameters),

(b) Topological transitivity

(c) Ergodicity (randomness)

This makes chaos theory a good and highly preferable option for cryptography.

Definition of Chaos

In the introduction part as we already stated that chaos theory involves deterministic dynamical system parameter equations that behave in chaotic, seemingly random ways. Chaos are generally defined over all,(or a subset of),real numbers and rely on floating point algebraic operations. Chaotic systems are defined as dynamical systems with the following three properties: sensitivity to initial conditions, topological mixing, and density of periodic orbits[8]. In the other way by physics science chaos can be defined as the property of a complex system whose behavior is so unpredictable as to appear random, owing to great sensitivity to small changes in conditions.

Introduction to Chaotic Maps

In mathematics, a chaotic map is a map (evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical systems. Chaotic maps often generate fractals. Although a fractal may be constructed by an iterative procedure, some fractals are studied in and of themselves, as sets rather than in terms of the map that generates them. This is often because there are several different iterative procedures to generate the same fractal.

Type of chaotic map

Arnold's cat map. Baker‘s map. Bogdanov map. Chossat- Golubitsky symmetry map. Circle map. Complex quadratic map. Complex squaring map. Complex Cubic map. Degenerate Double Rotor map. Double Rotor map. Duffing map. Duffing equation. Dyadic transformation. Exponential map. Gauss map. Generalized Baker map. Gingerbreadman map. Gumowski/Mira map. Hénon map. Hénon with 5th order polynomial. Hitzl-Zele map. Horseshoe map. Ikeda map. Interval exchange map. Kaplan-Yorke map. Linear map on unit square. Logistic map. Tangent map. Tent map. Zaslavskii rotation map.[11]

Baker’s Map

In dynamical systems theory, the baker's map is a chaotic map from the unit square into itself. It is named after a kneading operation that bakers apply to dough: the dough is cut in half, and the two halves are stacked on one-another, and compressed. The baker's map can be understood as the bilateral shift operator of a bi-infinite two-state lattice model.

The baker's map is topologically conjugate to the horseshoe map. In physics, a chain of coupled baker's maps can be used to model deterministic diffusion. The Poincare recurrence time of the baker's map is short compared to Hamiltonian maps. As with many deterministic dynamical systems, the baker's map is studied by its action on the space of functions defined on the unit square. The baker's map defines an operator on the space of functions, known as the transfer operator of the map. The baker's map is an exactly solvable model of deterministic chaos, in that the Eigen functions and Eigen values of the transfer operator can be explicitly determined. There are two alternative definitions of the baker's map which are in common use. One definition folds over or rotates one of the sliced halves before joining it (similar to the horseshoe map) and the other does not.

The folded baker's map acts on the unit square as

$$S_{\text{baker-folded}}(x,y)=\begin{cases}(2x,\,y/2) & \text{for } 0\le x<1/2\\ (2-2x,\,1-y/2) & \text{for } 1/2\le x<1\end{cases}$$

When the upper section is not folded over, the map may be written as

$$S_{\text{baker-unrotated}}(x,y)=\left(2x-\lfloor 2x\rfloor,\frac{y+\lfloor 2y\rfloor}{2}\right)$$

The folded baker's map is a two-dimensional analog of the tent map

$$S_{tent}(x) = \begin{cases} 2x \text{ for } 0 \le x < 1/2 \\ 2(1-x) \text{ for } 1/2 \le x < 1 \end{cases}$$

while the non-rotated map is analogous to the Bernoulli map. Both maps are topologically conjugate. The Bernoulli map can be understood as the map that progressively lops digits off the dyadic expansion of x. Unlike the tent map, the baker's map is invertible.

Let X = [0,1)2 = [0,1)x [0,1) be the unit square. consider the following two dimensional map F:X → X.

a generalized two dimensional bakers map is defines as-symbols.

$$F(x,y) = \begin{cases} \left(2x, \frac{y}{2}\right) & \text{if } 0 \le x < \frac{1}{2}, \\ \left(2x-1, \frac{y+1}{2}\right) & \text{if } \frac{1}{2} \le x < 1. \end{cases}$$

Graphical representation of Bakers Map is shown in figure-1[5].

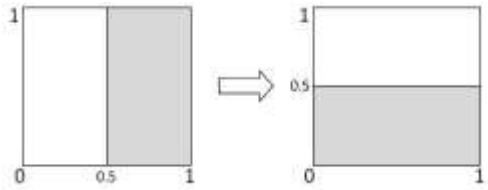

Fig. 1: Graphical representation of Bakers Map

After above discussion about the baker map we can conclude that how baker map can also be useful in chaotic map cryptography.

Chaotic Image Encryption for Baker map

The chaotic Baker map for image encryption proposed in reference [12] is of high efficiency: a few rounds of iterations will encrypt an image completely. In order to demonstrate the idea clearly,the encryption procedure in [12] is introduce in this section.

Firstly, take a square image as example. The square image consists of NxN pixels with L levels of gray. The method for developing an image chaos-based consist of the following three steps:

1. Choosing the basic map: The two-dimensional Baker map B is shown in Fig.1,mathematically is described as

$$F(x,y) = \begin{cases} \left(2x, \frac{y}{2}\right) & \text{if } 0 \le x < \frac{1}{2}, \\ \left(2x-1, \frac{y+1}{2}\right) & \text{if } \frac{1}{2} \le x < 1. \end{cases}$$

2. Generalization: A set of parameters which characterized by a sequence of integers is introduced into the map to create part of the ciphering key.
3. Discretization: The discrete map takes each pixel and assigns it to other pixel in a bijective manner. The discretized version is a permutation of pixels.

The permutation of pixels is an one-to-one two-dimensional mapping, while a three-dimensional (3D) mapping introduced in this subsection acts both on the pixels and on their gray levels. The extension can be achieved by a slight modification of the chaotic map and it significantly contributes to the security of the whole cipher. The resulting substitution cipher can create a random looking image with uniform histogram in only one round of iteration.

CONCLUSION

In the paper presented here we discussed chaos-based image encryption approach using baker‘s map to understanding the chaotic theory. we concluded that depending upon the different points discussed in the paper as introduction to chaos. chaos theory, chaotic baker map and its used for image encryption that chaotic map provides more efficient encryption choices for images.

As for discussion it is concluded that there are wide features of chaos systems as its randomness, robust nature and sensitivity to keys which can further improved in different field where security is more concern. High dimension chaotic map can also be used for better performance.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their valuable discussions and suggestion.

REFERENCES

[1] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li―A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process‖ International Journal of Advancements in Computing Technology Volume 3, Number 5, June 201.1

[2] Mina Mishra & V. H. Mankar ―Review on Chaotic Sequences Based Cryptography and Cryptanalysis‖ International Journal of Electronics Engineering, 3 (2), 2011, pp. 189– 194.

[3] G.A.Sathishkumar ,Dr.K.Bhoopathy bagan and Dr.N.Sriraam―Image Encryption Based on Diffusion and multiple Chaotic Maps‖International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011

[4] Musheer Ahmad, M. Shamsher Alam,‖A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping‖ International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.

[5] Alexander N. Pisarchik,Massimiliano Zanin ―Chaotic map cryptography and security‖ In: Encryption: Methods, Software and Security Editor: Editor Name, pp. 1-28, 2010 Nova Science Publishers, Inc.
[6] David Arroyo_,a, Shujun Lib, Jos´e Mar´ıa Amig´oc, Gonzalo Alvareza, Rhouma Rhoumad, ―Image encryption with chaotically coupled chaotic maps‖ in Physica D, vol. 239, no.12, pp. 1002-1006, 2010, DOI:10.1016/j.physd.2010.02.010.
[7] Rogelio Hasimoto-Beltran, Fadi Al-Masalh2, and Ashfaq Khokhar,Performanc‖ Evaluation of Chaotic and Conventional Encryption on Portable and Mobile Platforms‖ © Springer-Verlag Berlin Heidelberg 2011
[8] Sara Bredin,‖Paper on chaotic theory and cryptography‖, Cryptography-II,spring, 2013.
[9] George Makris , Ioannis Antoniou,‖ Cryptography with Chaos‖ Proceedings, 5th Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens Greece
[10] Igor Mishkovski and Ljupco Kocarev,‖ Chaos-Based Public- Key Cryptography‖
[11]http:/ / www. maths. ox. ac. uk/ ~mcsharry/ papers/ dynsys18n3p191y2003mcsharry. Pdf
[12] Fengling Han,Xinghuo Yu,Senior Member,IEEE,and Songchen Han,‖Improved Baker map for image encryption‖ and Technology Volume 2 No. 1, pp 93-98January, 2012.
[8]" Power Quality Enhancement of Three-Phase Front-End Rectifier of UPS System Using Current Injection Technique", Visvesvaraya National Institute of Technology, Nagpur, India pp 33-39.
[9] " Enhancement of Performance Parameters of Three Phase Induction Motor by Current Source Inverter: An Overview and Key Issues", IJCSAI Vol.1 Issue 1 2011 PP.18-26.