CRYPTOGRAPHY USING CHAOS IN COMMUNICATION SYSTEMS

R. Raja Kumar¹*, R. Pandian¹, T. Prem Jacob¹, A. Pravin¹, P. Indumathi²
¹Sathyabama Institute of Science and Technology, Chennai, India,
²MIT Campus of Anna University, Chennai, India.
*rrajakumar.maths@sathyabama.ac.in

Abstract. A new and unexplored area in the field of cryptography is the use of chaotic systems to encrypt data. The purpose of this paper is to present how the principles of chaos theory can be applied in the field of cryptography. A cipher that uses chaos dynamics is presented that has very good statistical properties.

1. INTRODUCTION
Chaos is a paradigm shift in the aspect of providing security to information. When a butterfly flies in a remote village of say Kanyakumari district of Tamil Nadu, India it may cause whirlwind effects in New York of USA. This is precisely the idea behind chaos. The unpredictability of the output even if there is a small change in the seed value, makes the chaotic approach very rugged.

Protection of data could be through encrypting and decrypting (namely cryptography) of data in current data preserving techniques. They make use of methods such as number theory and algebra. Chaos on the other hand uses nonlinear dynamics. Chaotic behaviour is subtly random. M.S. Bapistadeveloped a chaotic cryptographic technique by dividing the orbital intervals of the logistic map.

2. CHAOS AND CHAOTIC FUNCTIONS
Seemingly random, chaos is deterministic. The other attributes of chaos are non-linearity, dynamical behaviour, non-periodic, non-converging and bounded nature. Chaos is extremely sensitive to its initial conditions; A disturbance as small as $10^{-100}$ will make a chaotic system generate values that completely diverge. Extreme sensitivity to initial conditions is suitable for encryption.

2.1. Chaotic Function
The most simple chaotic function that can be generated is

$$f(x)=p*x*(1-x);$$

It is limited for $0<p<4$.

It is expressed as

$$x_{n+1}=p*x_n*(1-x_n)$$
in iterative form.

Chaotic functions are called as chaotic maps[8] as well.
Fig. 1 shows the chaotic map of [6]. This is a plot of ‘p’ after some number of iterations. For 0 < p < 3, the chaotic function converges to a particular value. As p grows larger than 3 the curve divides into 2 paths. The quantities generated thus fluctuate between two different values. As p increases, the curve bifurcates once more within 4 quantities. As p goes larger and larger, bifurcation speed up becoming 8, 16 then 32. Complete chaos happens at p called ‘known as’ the “point of accumulation”, (here p > 3.57). The chaotic values produced at this point are found to be confined to two different bounds, eventually leading to a single value. Also, the range over which chaotic values are yielded increases consistently as the value of p is increased. Finally, for p = 4, we observe that chaotic values are created in the complete range of 0 to 1. It is precisely this point that we are interested in. As already mentioned, a small change in the initial starting value i.e., x₀, leads to marked differences in the obtained iterated values.

3. CHAOTIC CRYPTO SYSTEM METHODOLOGY

In this paper on chaos and cryptography, Baptista says “It is possible to encrypt a message (and text composed by some alphabet) using the ergodic property of the simple low-dimensional chaotic logistic equation. The basic idea is to encrypt a message as the integer number of iterations performed in the logistic equation, in order to transfer the trajectory from the initial condition towards an interval inside the logistic chaotic attractor.”

3.1. Trajectory Generation and Baptista Method

Baptista uses logistic map below by which the iterates are reproduced

\[ x_{n+1} = p \cdot x_n \cdot (1-x_n) \]  \hspace{1cm} (1)

by choosing the chaotic parameter ‘p’ and initial condition \( x_0 \in (0,1) \). The ergodicity makes the interval (0,1) to be visited often by the iterated values. The density of such points is not varying with time. The scheme for encryption and decryption of messages are given in Fig. 2 and Fig. 3 respectively.
3.2. **Modification**

Baptista cryptosystem was found to be very promising. But several cryptanalysis methods were analysed and later an ingenious method was designed to crack this cryptosystem. Alvarez [7] proved that the ergodic cipher invented by Baptista repetitively uses its key, and hence, easy to break. Attackers can base his strategy on symbolic dynamics of one dimensional quadratic map.

Several counter-measure treatments to overcome the disadvantage of Baptista cryptosystem is analysed widely. A simple but effective measure is discussed in this paper. In this method, a new chaotic map is brought into discussion. This chaotic map is used to change the key continuously throughout the algorithm for every character or value. Hence key reusing is nullified by this chaotic map and the performance of baptista cryptosystem is well maintained. The chaotic map used for this purpose is

\[ x_{n+1} = f(x_n) = 1 - (2 \times x_n)^2, x_n \in (-1,1); \]
This improved logistic-map is aperiodic and is not converging; it is sensitively dependent on initial value. The values of this map $x_n$ belongs to the interval $(-1,1)$. As this logistic map is applied on the key of Baptista method, which lies in the interval $x_o \in (0,1)$, the mod function is applied over the map to make it belong to the interval $(0,1)$.

4. IMPLEMENTATIONS

The Baptista method, along with the modification specified, is implemented using MATLAB as tool. Alphabetic encryption, image, audio and video bit encryption are performed. The encrypted values are again decrypted using the decryption algorithm.

The advantage of using an extra chaotic map for changing the key value not only improves the traditional Baptista method, but also prevents the encryption algorithm from preserving the frequency of the values in the encrypted values.

These are illustrated in the MATLAB outputs shown in figures. The traditional Baptista method and the modified method are used to encrypt an image and the outputs are shown in Fig. 4 and Fig. 5 respectively.
Figure 4. Image encryption using traditional Baptista method.

Figure 5. Image encryption using modified method

It is clear from the figures that the frequency of the values in the encrypted values is not preserved. The original image and reconstructed image using decryption algorithm are shown in Fig. 6 and Fig. 7 respectively. It is evident that the image is decrypted perfectly.

Figure 6. Original image.

Figure 7. Reconstructed/Decrypted image.
The output of the alphabetic encryption and a capture of frame during video encryption are respectively shown in Fig. 8 and Fig. 9.

```python
enter the key:0.45
enter the plaintext:CRYPTOGRAPHY

cipher_text =
IEVMTUSWNZK
decrypted_text =
CRYPTOGRAPHY
```

**Figure 8.** Alphabetic encryption using modified method.

**Figure 9.** A frame in video encryption using modified method.

### 5. EVALUATION

The important advantage of this method is that the key is analog in nature; not digital like a PN sequence. The different keys that are produced by the algorithm may be extremely random and non-determinable. Let’s understand the security of the algorithm. As the key sequences are absolutely different, it is impossible for the hawker to crack the key. For the given algorithm, the number of decimal places supported can be between 30 and 100; the first value of the start iteration may be from 100 and 1000. Hacker has to try roughly $10^{37}$ tries to crack the algorithm; DES requires only
10^19. When delay is not a problem, this secure algorithm is useful, like bank transactions and defence applications.

6. CONCLUSIONS

Traditional Baptista method was a huge success at the time of its invention. Later, however, several cryptanalysis techniques were analysed to question the efficiency of the Baptista method. After its success many modifications were proposed and brought into the algorithm to enhance the efficiency. A very simple, but effective and easy to implement technique, is proposed in this paper and its performance is analysed. With the advent of aggressive research into Chaos, we believe that Chaos Cryptography, like its counterparts in conventional cryptosystems; face the same danger of being easily broken with the advent of modern technology. However, there is currently no technology to talk of and a threat is currently not of significant concern.

References
[1] M.S. Baptista, Cryptography With Chaos, Physics Letters A 240(1-2) (1998) 50–54.
[2] W.K. Wong, L.P. Lee, K.W. Wong, A Modified Chaotic Cryptographic Method, Computer Physics Communications 138(3) (2001) 234–236.
[3] W. Wong, L. Lee, K. Wong, Reply To The Comment “Keystream Cryptanalysis Of A Chaotic Cryptographic Method”, Computer Physics Communications 156(2) (2003) 208.
[4] K.-W. Wong, A Fast Chaotic Cryptographic Scheme With Dynamic Look-Up Table, Physics Letters A 298(4) (2002) 238–242.
[5] K.-W. Wong, A Combined Chaotic Cryptographic And Hashing Scheme, Physics Letters A 307(5-6) (2003) 292–298.
[6] K. W. Wong, S. W. Ho, C. K. Yung, A Chaotic Cryptography Scheme For Generating Short Cipher Text, Physics Letters A 310(1) (2003) 67–73.
[7] G. Alvarez, F. Montoya, M. Romera, And G. Pastor, 2003(B). Cryptanalysis Of An Ergotic Chaotic Cipher, Phys. Lett. A, 311: 172-179.
[8] Gleick James Chaos, Making A New Science, Minerva Limited, 1988.
[9] S. Li, Analyses And New Designs Of Digital Chaotic Ciphers, Ph. D. Thesis, School Of Electronics And Information Engineering, Xi’an Jiaotong University, Xi’an, China, 2003.
[10] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis Of Dynamic Look-Up Table Based Chaotic Cryptosystems, Physics Letters A 326(3-4) (2004) 211–218.