Design of One Dimensional Chaotic Maps Based System for Secret Key Generation

Suhel Mustajab*
Musheer Ahmad**
Ahmad Zia Danish***

Abstract

The quality of the stream ciphers highly depends on the quality of the key-stream. The process of key generation is the major task which defines the level of security of a cryptosystem. A lot of key generation techniques based on linear feedback shift registers have been suggested in the literature. In this paper, we propose a circuit based on one-dimensional chaotic maps for the generation of secret keys. Multiple Logistic maps and Cubic maps are used to design the system which generates the key-stream in a novel manner. The proposed system includes the preprocessing and quantization of the chaotic sequences. The integration of multiple one dimensional chaotic systems is basic thought to secure the data from the unauthorized sources. Further these keys are used in cryptography to encrypt and decrypt the data. The experimental results show that the sequence has desirable autocorrelation property and can be applied in a cryptographic process.

Keywords*—Key Generation, Cryptography, Randomness, Logistic Maps, Cubic Maps*

Introduction

In the era of communication, people require to connect each other via wired or wireless network systems. These systems are sufficient to transfer data from one end to another end but when security is concerned these are less effective due to the lack of good security techniques. Sometimes the speed of transmission and reliability are major issues but poor or ancient technologies of data security are used. This may be harmful for the end users when the useful and important data is transferred. In present world, cryptography is extensively used to secure the data from unauthorized access and usage. However cryptography is not a modern invention even it was used many centuries ago as first time. But the work is going on to search some effective techniques in cryptography which make the data more secure [1, 2].

Cryptography is basically the combination of two operations (1) encryption and (2) decryption. Keys are used to encrypt the original data into cipher form and again the ciphered data is decrypted. Key generation is the major task in cryptography [3]. There are many ways to handle the problem of key generation. Some techniques are simple but less effective. For example in some techniques the encryption is performed by using general/ simple methods and the same methods are used to decrypt the data. These techniques are less complex but easy for unauthorized sources to break the security line. Obviously, to break a simple method is an easy task to find the keys. Once keys are stolen any one can decrypt the data. Hence it is required to create some techniques that must generate the keys in such a way that it could be approximately impossible to reach for any outsider. Randomness in keys may be a solution for this. Minds can not find easily the keys if these are randomly generated. To create the randomness in key generation chaos based systems are appropriate tools [4]. In this paper multiple one dimensional chaotic system is proposed and the image is encrypted.

Types of Encryption

Encryption algorithms can be classified into two types (1) stream cipher and (2) block cipher. In a stream cipher algorithm, the message is encrypted bit-by-bit with the application of a secret key generator. Decryption can be performed using the same algorithm as in encryption, and with the same secret-key generator. In block cipher a group of bits of fixed length are encrypted block-by-block. In data encryption both the algorithms can be used. Block ciphers are complex but are famous for high degree of data security. Stream ciphers are faster than block

*Faculty, Dept. of Computer Science, Aligarh Muslim University, Aligarh, U.P.
**Faculty, Dept. of Computer Engineering, Jamia Millia Islamia, New Delhi
***Faculty, Dept. of Computer Science, Aligarh Muslim University, Aligarh, U.P.

cipher and also use less code than block ciphers. Stream ciphers can be used for average class of data security.

Proposed Design for Key Generation

One–dimensional Logistic maps and Cubic maps are used in the proposed design to generate the key sequences. One dimensional Logistic maps and Cubic maps are considered as a mask. By using some formulae, conversion for input is done in logistic as well as in cubic maps as shown in equation (1) and (2) for logistic and cubic maps respectively. The Circuit diagram is shown in figure 1.

$$x(n+1)=\lambda x(n)(1-x(n)) \quad (1)$$

$$y(n+1)=\lambda y(n)(1-y(n)\times y(n)) \quad (2)$$

x(n) and y (n) are the initial values in the first iteration for Logistic and cubic maps respectively. x(n+1) and y(n+1) are the initial values in the next iterations for logistic and cubic maps respectively. ? is the system parameter defined by user.

In the proposed design there are two logistic maps and two cubic maps. Their equations are given as follows:

(1) $x_1(n+1)=?_1 x_1(n)[1-x_1(n)]$

(2) $x_2(n+1)=?_2 x_2(n)[1-x_2(n)\times x_2(n)]$

(3) $x_3(n+1)=?_3 x_3(n)[1-x_3(n)]$

(4) $x_4(n+1)=?_4 x_4(n)[1-x_4(n)\times x_4(n)]$

The above equation (1) and equation (3) are used for Logistic map1 and Logistic map2 while equation (2) and (4) are used for Cubic map1 and Cubic map2 respectively.

In the proposed design, the initial values are taken as follows:

$x_1(0)=0.735, \quad \lambda_1=3.995$

$x_2(0)=0.372, \quad \lambda_2=2.50$

$x_3(0)=0.519, \quad \lambda_3=3.975$

$x_4(0)=0.694, \quad \lambda_4=2.45$

When the final iteration is performed, the values produced by multiple one dimensional maps are transmitted to the 1-bit quantizers. There are two inequalities followed by quantizers:

(1) If $x<0.5$, x is replaced by 0

(2) If $x>=0.5$, x is replaced by 1

In Figure 1, these new values are represented as b_i's, i= 1, 2, 3, 4.

Finally these bits are passed over a 4×1 multiplexer where $S= S_1S_0$ is selected for output.

Here S_0 and S_1 are described as follows

$$S_0=b_1 \text{ 丿 } b_3 \text{ and } S_1=b_2 \text{ 丿 } b_4$$

Symbol "丿 "is used to represent the XOR operation.

Finally the resultant Z_{out} is produced.

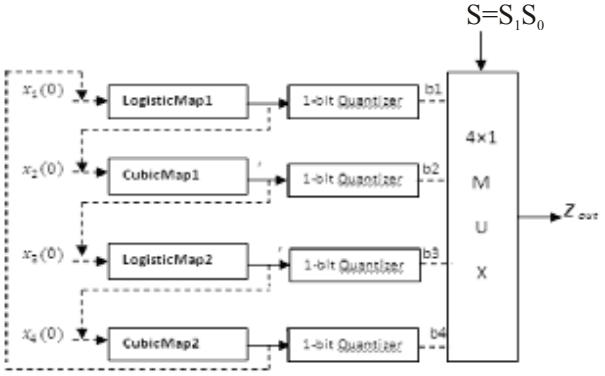

Figure1. Proposed Design for Key Generation

Experiments and Results

The proposed design of key generation is used to encrypt the original image as shown in figure 2. By using the initial values as described in the previous section, we finally get the key sequences. These secret keys are applied on the original image. Figure 3 represents the encrypted image of the original image.

Figure 2.Original image Lena

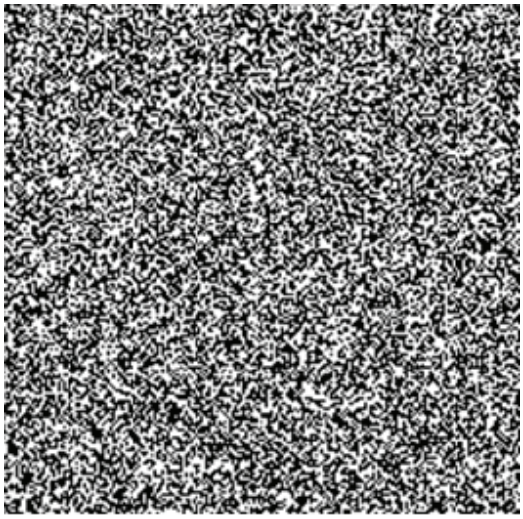

Figure 3.Encrypted Image Lena

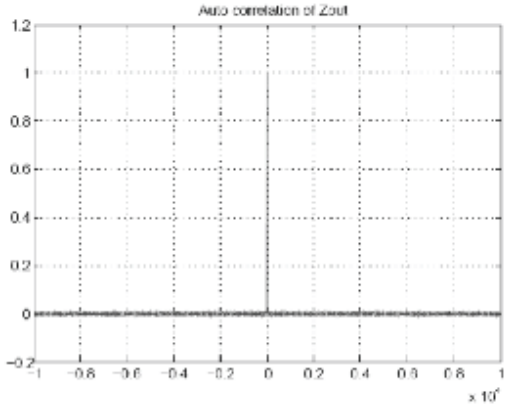

Figure 4. Autocorrelation Function

The same key streams are used to decrypt the encrypted image and finally we get the original image as output. In figure 4, the autocorrelation function is shown which is calculated near to 0.030099.

Conclusion

A multiple one dimensional key-stream generator circuit is proposed in this paper which works dynamically. The multiple logistic and cubic maps produce arbitrary values as output. These arbitrary values further causes for more secured data. It is obtained that the keys generated by implementing the chaotic maps are having good correlation property and hence can be beneficial in cryptography.

References

1. Schneier B (1996), Applied Cryptography, John Wiley & Sons, Inc. Singapore.
2. Menzes A.J. Oorschot P.C.V and Vanstone S.A..Handbook of Applied Cryptography. CRC Press. Boca Raton 1997.
3. Stallings W (2004), Cryptography and Network Security-principles and practice, Prentice Hall of India Pvt. Ltd. New Delhi.
4. Pareek N. K., Patidar Vinod and Sud K. K. Discrete chaotic cryptography using external secret key.