Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 3; April-June, 2017, pp. 190-192

http://www.krishisanskriti.org/Publication.html

Image Encryption by Using 1-D Chaotic System

***Kalpita Rani Dash*[1] and *Ranjan Kumar Singh*[2]**

SRCEM, Palwal, MDU
E-mail: kalpita.purohit@gmail.com

Abstract—*Due to the development in the field of network technology and multimedia applications, every minute thousands of messages which can be text, images, audios, videos are created and transmitted over wireless network. Improper delivery of the message may leads to the leakage of important information. So encryption is used to provide security. In last few years, variety of image encryption algorithms based on chaotic system has been proposed to protect image from unauthorized access. 1-D chaotic system using logistic maps has weak security, small key space and due to the floating of pixel values, some data lose occurs and proper decryption of image becomes impossible. In this paper different chaotic maps such as Arnold cat map, sine map, logistic map, tent map have been studied. This paper introduces a simple and effective chaotic system using a combination of two existing one-dimension (1D) chaotic maps (seed maps). To investigate its applications in multimedia security, a novel image encryption algorithm is proposed. Using a same set of security keys, this algorithm is able to generate a completely different encrypted image each time when it is applied to the same original image. Experiments and security analysis demonstrate the algorithm's excellent performance in image encryption and various attacks.*

Keywords*: Encryption, Security, Image Encryption, Logistic map, Sine map, Tent map, new chaotic structure.*

1. INTRODUCTION

Protection of multimedia contents from unauthorized access is necessary nowadays. With the help of cryptography readable form of message is converted to the non readable form. And reverse of cryptography in which non readable form of message is converted back to readable form, is called cryptanalysis. The combination of these two techniques is referred as Cryptology. Communication in human language referred as Plain Text which can be easily understandable by anyone else. In order to provide security plain text is coded with suitable encryption shames and the codified message is referred as cipher text.

Encryption techniques can be classified on the basis of key, structure of algorithms and percentage of encrypted data. On the basis of key encryption can be symmetric encryption and asymmetric encryption, on the basis of structure encryption can be block cipher and stream cipher. And on the basis of basis of percentage of encrypted data encryption can be full encryption and partial encryption.Chaos-based image encryption has become one of efficient and excellent encryption methods. This is because chaotic systems/maps have high sensitivity to their initial values and control parameters, chaotic property, non-convergence, and state ergodicity. Therefore, many chaotic image encryption algorithms have been developed by directly utilizing existing chaotic systems/maps to their encryption processes. In general, a chaos-based image encryption algorithm contains two portions: a chaotic system and image encryption. Chaotic systems/maps in the image encryption algorithms can be divided into two categories: one-dimension (1D) and multi-dimension (MD).The MD chaotic maps have increasing application sin image security because of their complex structures and multiple parameters. However, multiple parameters increase the difficulty of their hardware/software implementations and computation complexity. 1Dchaoticsystems, on the other hand, have a simple structure and are easy to implement. But, they also have three problems including: (1)the limited or/and is a continuous range of chaotic behaviors;(2)the vulnerability to low-computation-cost analysis using iteration and correlation functions; and(3)then on uniform data distribution of output chaotic sequences. Hence, developing new chaotic systems with better chaotic performance is needed.

For evaluating an image encryption algorithm, security should be the first and vital principle. Many chaos-based image encryption algorithms have been shown to have the security weakness by cryptanalysis. For example, they are unable to with stand the chosen-plaintext attacks. To address these above-mentioned problems, this paper introduces a new chaotic system with a simple structure. It integrates three existing 1D chaotic maps to generate a number of new chaotic maps. They have excellent chaotic properties, including a wide range of parameter settings and the uniform-distributed variant density function. These can be verified by simulations and analysis of three specific examples of the proposed chaotic system.

This paper is organized as follows. Section 2 briefly reviews several existing chaotic maps. Section 3 contains the structure of new chaotic system. Section 4 shows result. Section 5 reaches conclusion.

2.1. Logistic map: 1-D logistic map was proposed by RM may. This map is simplest non linear chaotic system which can be defined as

$Z_{n+1} = \lambda Z_n(1 - Z_n)$..... (1)

Where Z_0 is initial condition, n is number of iterations and λ is system parameter.

For 3.57 < λ < 4 map is considered as chaotic and Z_{n+1} belong to (0, 1) for all n.

2.2 Sine map: sine map is defined as

X_{n+1}=a $x_n^2 \sin(\pi x_n)$.....(2)

When X_0 = 0.7 and a=2.3, equation 2 has the simplified form. For the interval (0,1) it generates chaotic sequence .

2.3. Tent map: tent map resembles the logistic map. It generates chaotic sequences in (0, 1) assuming the following equation

$$X_{n+1} = \begin{matrix} \mu X_n, & X_n < 1/2 \\ \mu(1 - X_n) & X_n \geq 1/2 \end{matrix} \quad \ldots\ldots (3)$$

Where μ is a positive number and depending on its value tent map exhibit dynamic behavior ranging from predictable to chaotic.

3. NEW CHAOTIC SYSTEM

In this section, a new chaotic system will be proposed to solve the problems discussed in Section 2.

3.1. System structure

The new chaotic system is shown in Fig. 1.It is a nonlinear combination of three different 1D chaotic maps which are considered as seed maps. The system is defined by the following equation:

$X_{n+1} = A_{FGH} = \big(F(a, X_n) + G(b, X_n) + H(c, X_n)\big)$..... (4)

Where $F(a, X_n), G(b, X_n)$ *and* $H(c, X_n)$ are three 1D chaotic maps (seed maps) with parameters a, b and c; mod is modulo operation, and n is the iteration number.

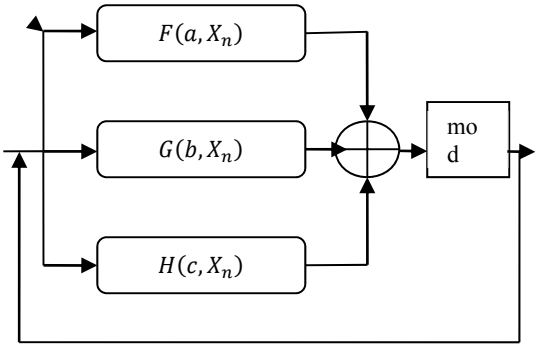
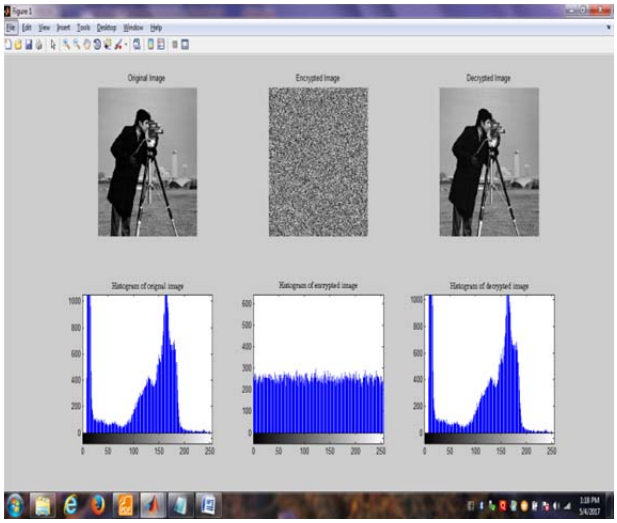


Fig. 1: The new chaotic system

Combining outputs of three seed maps, the new chaotic system shows a mixed chaotic property. Here, the 'mod' operation is to ensure its output data within range of [0, 1].

Using different seed maps, this system is able to generate many new chaotic sequences. Compared with its corresponding seed maps, this system has more complex chaotic properties. When one of its seed maps is out of the chaotic range, this chaotic system can still have excellent chaotic behaviors.

4. RESULT



The above figure shows the original image, encrypted image and decrypted image in first row and histogram of the respective images in second row. We used the combination of three chaotic maps as encryption and decryption key.

5. CONCLUSION

The proposed chaotic system has at least three advantages compared with its corresponding seed maps.

First, the distribution of its density function is more uniform than its corresponding seed maps. All seed maps have the limited data ranges within (0,1). As the output sequences of the new chaotic system spread out in the entire data range between 0 and 1. This property ensures the proposed system well suitable for different applications such as information security.

Second, the proposed chaotic system has a wider chaotic range. Even if one seed map is out of the chaotic range, the proposed system still keeps chaotic behaviors.

Lastly, the proposed system has better chaotic behaviors.

REFERENCES

[1] Yicong Zhou, C.L.Philip Chen, A new 1D chaotic system for image encryption, Published by Elsevier,2013

[2] Rekha Raj, Salim Paul, Image encryption using chaotic maps of various dimensions: review, Published by International Journal of Research in Engineering and Technology (IJRET), 2014

[3] Nitin Kumar, Deepika, Divya Wadhwa, Deepak Tomer and S. Vijayalakshmi, Review on Different Chaotic Based Image Encryption Techniques, International Journal of Information and Computation Technology(IJICT), 2014

[4] Komal D Patel, Sonal Belani, Image encryption using different techniques, International Journal of Emerging Technology and Advanced Engineering,2011

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

[6] Haojiang Gao , Yisheng Zhang, Shuyun Liang, Dequn Li, A new chaotic algorithm for image encryption, ©2005 Published by Elsevier Ltd.

[7] Encryption Technique Based on Chaotic Map", Lalita Gupta1, Rahul Gupta and Manoj Sharma, "Low Complexity Efficient Image International Journal of Information & Computation Technology,2011

[8] Rajinder Kaur1, Er. Kanwalpreet Singh,"Comparative Analysis and Implementation of Image Encryption Algorithms", International Journal of Computer Science and Mobile Computing (IJCSM) April 2013

[9] Shoaib Ansari1, Neelesh Gupta2, Sudhir Agrawal, "An Image Encryption Approach Using Chaotic Map in Frequency Domain", International Journal of Emerging Technology and Advanced Engineering-Volume 2, Issue 8, August 2012

[10] Priyanka Gupta, Sonia Singh and Isha Mangal, "Image Encryption Based On Arnold Cat Map and S-Box", International Journal of Advanced Research in Computer Science and Software Engineering-Volume 4, Issue 8, August 2014