Chapter 34
Image Encryption Method Using Dependable Multiple Chaotic Logistic Functions

Ranu Gupta
Jaypee University of Engineering and Technology, Guna, India

Rahul Pachauri
Jaypee University of Engineering and Technology, Guna, India

Ashutosh K. Singh
Thapar Institute of Engineering and Technology University, Punjab, India

ABSTRACT

This article explores an efficient way of image encryption using chaotic logistic function. A set of two chaotic logistic functions and a 256 bit long external secret key are employed to enhance the security in the encrypted images. The initial condition of first logistic function has been obtained by providing the suitable weights to all bits of the secret key. The initial condition of second logistic function has been derived from first chaotic logistic function. In this proposed algorithm, ten different operations are used to encrypt the pixel of an image. The outcome of the second logistic map decides the operation to be used in the encryption of the particular image pixel. Various statistical parameter comparisons show that the proposed algorithm provides an image encryption method with better security and efficiency for all real-time applications.

1. INTRODUCTION

With the fast development in the technology of computer network and advancement in the information technology, a huge amount of image-based data is sent through unsecured channels in the public network. The security and the confidentiality of the information becomes the prime aspect while transmitting the data. The nature of chaotic signals has attracted many cryptographers. Its behavior resembles with the

DOI: 10.4018/978-1-7998-7705-9.ch034

cryptographic properties. The ergodicity property of chaotic signal is similar to the confusion property in cryptography. The random behavior which appears to be noise in chaotic sequence resembles with the key sequence that is used in cryptography. The sensitiveness of chaotic signal towards the initial condition resembles with the diffusion property in the cryptography. Since encryption plays a vital role while transmitting the information in the form of images, thus the purpose of this paper is to develop such a method which would secure the confidential information and would be simple to implement.

Various methods of image encryption have been proposed in the last few years. There are simple as well as complex encryption schemes. Simple encryption schemes have a drawback of weak synchronization at the receiver end and there is always a threat of information being hacked. But if the system is too robust then there is a loss of time while encrypting the message in the form of image. Thus, such an encryption system should be developed such that there is a balance between the synchronization at the receiver end and time loss. Mao et al. (2004) has used symmetric block encryption scheme. A three-dimensional (3D) baker map has been proposed while maintaining its high degree of security. It has been found that 3D baker map is faster than 2D baker map. L. Zhang et al. (2005) has proposed the method of confusion and diffusion for image pixels by using discrete exponential chaotic map. A non-linear chaotic algorithm has been proposed by Gao et al. (2006). The power function and tangent function is used in the chaotic function instead of linear function as well as a large key of 150 bit long is used for the encryption of the image. Zhou et al. (2008) has proposed a parallel image encryption framework. The discrete Kolmogorov flow map was used for parallel image encryption. Borujeni (2009) has proposed a permutation-substitution process using chaotic map and Tomkins-Paige algorithm. A 2D permutation using logistic map is used to generate a bit sequence which in turn is used to generate pseudorandom numbers in Tompkins-Paige algorithm. A Tent map is also used in substitution method to produce a pseudorandom image, which is mixed with the permuted image to produce encrypted image. Two keys are used for permutation and substitution process. Q. Zhang et al. (2010) has presented an image encryption scheme using deoxyribionucleic acid (DNA) sequence addition operation in combination with chaotic function. In this, using DNA sequence a matrix is formed by encoding the original image and then DNA sequence addition operation is used. After that DNA sequence complement operation is used by using two chaotic logistic maps to get the final encrypted image. H. Khanzadi et al. (2010) has done image encryption using chaotic maps and gyrator transform. Chaotic logistic and tent map are used to generate the random bit sequence. After that pixels of image are encrypted using gyrator transform. A skew tent chaotic map for diffusion of the pixels in the image and permutation is done by choosing P box of same size of plain image was proposed by G. Zhang (2011). H. Liu et al. (2012), has proposed the method of permutation of rows and columns by the arrays generated by piecewise linear chaotic map and then each pixel is encoded by DNA coding and then the matrix is complemented by chebshev maps. Pareek et al. (2013) has done the mixing of image after which it is divided into blocks and then diffusion and substitution is done based on secret key of 128 bits length. Enayatifar et al. (2014) uses hybrid model of DNA and logistic map function to create initial condition for DNA masking and then genetic algorithm is applied to do the encryption of the image. H. Khanzadi et al. (2014) used the chaotic logistic and tent map to generate random bit sequence and the pixels of the image are permutated and substituted according to the random bit and random numbers generated. Wang (2014) has done the shuffling and diffusion of the image simultaneously. The image is divided into two blocks. The left block is diffused using logistic map. The right block is diffused with other logistic function and plain text. Finally, after the Xor operation the two blocks are merged. Tong et al. (2015) has proposed perturbed high-dimensional chaos system for image encryption according to Devaney and topological conjugate definition. A cat