Chapter 17
Secure Chaotic Image Encryption Based on Multi-Point Row-Column-Crossover Operation

K. Abhimanyu Kumar Patro
National Institute of Technology, Raipur, India

Mukesh Drolia
National Institute of Technology, Raipur, India

Akash Deep Yadav
National Institute of Technology, Raipur, India

Bibhudendra Acharya
National Institute of Technology, Raipur, India

ABSTRACT

In this present era, where everything is getting digitalized, information or data in any form, important to an organization or individual, are at a greater risk of being attacked under acts, commonly known as cyber-attack. Hence, a proper and more efficient cryptosystem is the prime need of the hour to secure the data (especially the image data). This chapter proposes an efficient multi-point crossover operation-based chaotic image encryption system to secure images. The multi-point crossover operation is performed on both the rows and columns of bit-planes in the images. The improved one-dimensional chaotic maps are then used to perform pixel-permutation and diffusion operations. The main advantage of this technique is the use of multi-point crossover operation in bit-levels. The multi-point crossover operation not only increases the security of cipher images but also increases the key space of the algorithm. The outcomes and analyses of various parameters show the best performance of the algorithm in image encryption and different common attacks.

DOI: 10.4018/978-1-7998-6659-6.ch017

INTRODUCTION

In today's information age, the two parties communicate large amounts of multimedia information (particularly images). However, the rapid growth of emerging technologies and developments has made the securities of multimedia information quite vulnerable. Hence, it becomes very necessary to keep such information secure, which otherwise could result in a big loss. In the preliminary research method, scientists have developed numerous traditional image encryption techniques to encrypt images such as RSA, AES, and DES (Coppersmith, 1994; Pub, 2001). The traditional methods are not sufficiently effective for encrypting images, due to the large data requirement and the strong association of neighboring pixels in an image (Gao, Zhang, Liang, & Li, 2006; Samhita, Prasad, Patro, & Acharya, 2016). To address this issue, it is necessary to concentrate on methods that satisfy the need for diffusion and confusion in the encryption process (Zhang & Liu, 2011). Confusion is a cryptographic technique which is intended to increase plaintext vagueness. The technique ensures no indication of the plaintext is given in the ciphertext. The relation between ciphertext statistics and the value of the encryption key is retained as complex as possible in the confusion technique. The confusion can be achieved by using the complex method of permutation or scrambling depending on the key and the plaintext. On the other hand, diffusion is a cryptographic technique developed to enhance the plaintext redundancy in order to conceal the plaintext's statistical structure to protect efforts to reproduce the key.

Chaos-based encryption algorithms have gained much interest in recent years from a large number of researches. There are many essential attributes in chaos systems, such as non-periodicity, ergodicity, randomness, vulnerability to initial values. Despite of these features, the image encryption method based on the chaos principle is found to be more robust and appropriate for strong-security encryption (Guesmi, Farah, Kachouri, & Samet, 2016a, 2016b; Patro & Acharya, 2019a). In general, this method of encryption involves two stages: permutation and diffusion (Wang, Chen, & Wang, 2010; Zhang, Li, Wong, Shu, & Chen, 2012). With the support of chaotic maps, the location of the pixels is modified in the permutation step, where the pixel values are modified with the assistance of chaotic maps as in the diffusion step. Having both permutation and diffusion together is a must for high protection, and this was the research's effort when conducting encryption.

Basically, in the encryption of images, two types of chaotic maps are used like chaotic maps having high-dimensional and chaotic maps having one-dimensional (1D) (Liu, Sun, & Zhu, 2016; Patro, Acharya, & Nath, 2019b). In the encryption of images, 1D maps are appropriate to use because it have simplicity, high-efficiency, limited hardware resources requirement, etc., but they suffer from the problem of small key space (Özkaynak & Özer, 2016; Wang, Wang, Zhang, & Guo, 2017). To avoid this problem, the use of multiple 1D maps in image encryption is suggested. The combination of multiple 1D maps provide large key space to the algorithm. At present, most of the chaotic encryption algorithms are easy to be attacked by exhaustive attack (small key space); hence, the algorithm needs to be given large key space.

At the other hand, due to its simple implementation the genetic algorithm has gained popularity and interest in many recent researches. It is always found to give satisfactory outcomes with high fitness and improved security to images and data (Wang & Xu, 2014). The genetic crossover operation could be one-point, two-point or multi-point as per the requirement upon implementation. Though it has many advantages but it has its own limitations such as it does not go well when large number elements get exposed to mutation and also it increases the search size exponentially. Even though it has limitations, it is still one of the most used image encryption technique.