Chapter 26
Preserving Information Security Using Fractal-Based Cryptosystem

Shafali Agarwal
Independent Researcher, Plano, USA

ABSTRACT

The chapter intends to propose a hybrid cryptosystem based on a chaotic map and a fractal function. The sequential order of process execution provides a computationally less expensive and simple approach that still designed a secure cryptosystem. A one-dimensional Ricker map and its modified form are employed to initially shuffle the image pixels twice, and also a pseudo-random sequence is generated using both maps. The algorithm implemented a sequence of pixel confusion-diffusion steps using the image rotation and a transcendental anti-Mandelbrot fractal function (TAMFF) and its Mann-iterated fractal function (Sup-TAMFF). Finally, the pixel value of an image obtained in the last step and the recent two pixels of the encrypted image is XORed with the corresponding pseudo-random matrix value to get the cipher image. Subsequently, various performance tests are conducted to verify the suitability of the given method to be used in real-world information transmission.

INTRODUCTION

Today's internet world is glorified with the use of vast digital media communication, resulting in the transmission of enormous data over the network. An organization having a growing network of interconnected devices strengthen the protection requirement of its cybersecurity assets. They must be aware of the cybersecurity laws and regulations to formalize the applicable security standards to secure and protect their organizational data. Failing to which, could arise the threatening situation for the association.

With the advancement in the internet world, digital media transmission has increased tremendously. It can be in the form of text, images, audio, or video. The data transmitted over the channel is expected to be received securely on the receiver side. The number of cyber threats challenges to create a credible secure system to protect the sensitive and confidential information produced in various fields like in

DOI: 10.4018/978-1-7998-5728-0.ch026

the military, medical, financial and many more. There have been many conventional ciphers like Data Encryption Standard (DES) (Smid & Branstad, 1988), International Data Encryption Algorithm (IDEA) (Lai & Massey, 1991), RSA algorithm (Rivest, Shamir, & Adleman, n.d.), Advanced Encryption Standard (AES) (*FIPS 197, Advanced Encryption Standard (AES)*, n.d.), etc., provide high data security measure. However, the above-mentioned algorithms provide effective results to encrypt text data but are expensive and time consuming for image encryption. Due to the inherent image features such as large data volume, strong pixels correlation, high redundancy, etc., need a high computational efficient and time-sensitive image encryption algorithm.

In the past decade, a dynamical chaotic system was studied extensively by the researchers. The non-linear complex chaotic map has ergodic property, unpredictable trajectories, pseudo-randomness, sensitiveness and dependence on its initial condition. There will be completely a different chaotic sequence for a minute changed map's initial parameter which implies its great importance in the cryptography field. These characteristics make the chaotic map advantageous in many disciplines such as mathematics, physics, computer science, and engineering. A competent image cryptosystem generally designed using confusion and diffusion processes. The confusion property or pixel permutation is achieved by the random pixel shuffling within the image to minimize the correlation between the adjacent pixels. It helps to enhance the computational complexity of a chosen-plaintext attack. The diffusion property or pixel replacement is obtained by changing pixel values in such a manner that by making a small change in a plain image effect in almost all pixels in the cipher image. One can design a cryptosystem by applying single or multiple rounds of confusion/diffusion process depending upon the system requirement.

The chapter discusses a cryptosystem which combines the complex features of the chaotic map and a fractal function. A fractal image is the graphical representation of a complex function at the local and the global irregularity level (Pickover, 2001). It is generated by iterating a mathematical function for a pre-determined number of times. Because of the non-linear behavior and fractional dimension, the fractal function has been popularized to solve complex mathematical problems. Fractal functions can be visualized in the whole universe in different forms which further help to investigate the things on the practical ground. Few examples include the Coast of Britain, Alzheimer's brain, special effects in shows such as Star Trek and Star Wars, a biological pattern like growth patterns of bacteria and so on (Addison, 1997). Unlimited resources are available to generate fractal images including ChaosPro, Fractint, Fraqtive, Ultra Fractal, etc.

To date, several chaotic maps-based image encryption algorithms have been proposed. Some might have good chaotic behavior, but the complex structure requires high computational cost. This work utilizes the complex chaotic properties of a simple one-dimensional Ricker chaotic map and its modified function. These chaos-generated sequences are applied in both pixel permutation and diffusion phases. Additionally, these chaotic sequences are computed to generate a pseudo-random matrix which is used in image pixel diffusion to get the cipher image at the final stage. To introduce multi-steps pixel confusion-diffusion, TAMFF and Sup-TAMFF along with image rotation (90 degrees clockwise and anti-clockwise) are executed alternatively. Finally, to enhance the security level, the image pixel obtained in the previous step was diffused with the pseudo-random matrix and the recent two pixels of a concurrent encrypted image to generate the ultimate cipher image. The multistep execution of image pixel repositioning and replacement makes the given method resilient to the cyber-attacks. Hence, it can be applied in real-world secure image transmission and image storage.

The paper is organized in sections as follows: The subsequent section covers the related image encryption algorithms discussed in past decades. Section 3 incorporates the basic theories related to the