Chapter 4
Chaotic-Based and Biologically Inspired Cryptosystems for Secure Image Communication and Storage

El-Sayed M. El-Alfy
King Fahd University of Petroleum and Minerals, Saudi Arabia

ABSTRACT

Protecting confidentiality of sensitive data is growing in importance in many personal, commercial, governmental, medical and military applications. Data encryption remains the most prevalent mechanism for this goal in cybersecurity to store and communicate data in unintelligible form. However, images are known to have intrinsic characteristics different from text, which limit the applicability of conventional cryptographic algorithms. This chapter provides a review of the work related to image cryptosystems based on chaos theory and biologically-inspired algorithms. Then, a case study is presented using ideas from genetic crossover and mutation to confuse and diffuse images to generate secure cipher images with very low correlation between pixels.

INTRODUCTION

Nowadays, digital images are prevalent in many areas such as remote sensing, satellite imagery, astrophysics, seismology, agriculture, radiology, telemedicine, ecosystems, industrial processes, military communications, medical imagery, and image archiving systems. A stringent requirement for the successful deployment of these systems is secure storage and transmission of image data. This field is gaining growing importance in recent years due to the proliferation of multimedia network applications and services.

Cryptographic algorithms have been the heart of the security techniques for protecting confidentiality, checking integrity, and authenticating the origin of the data (Forouzan, 2007; Menezes et al., 2010). Encrypted images are stored or transmitted over public transmission lines but only intended recipients can decrypt and view them in comprehensible form. Although several conventional techniques and stan-

DOI: 10.4018/978-1-4666-9426-2.ch004

dards (such as DES, AES and RSA) have been developed, they are mainly for text and short messages. Applying such techniques to images has been found to be inefficient due to the bulk size of image data. Additionally, image pixels often have higher redundancy and correlation which can enable reasonable pixel value prediction from neighboring pixels (Mao and Chen, 2005; Younes and Jantan; 2008). Therefore, new image encryption schemes have been introduced in the literature to take into consideration these special requirements (Patel and Belani, 2011; Jawad and Sulong, 2013).

Some approaches are just modifications of exiting techniques to improve their performance when applied to bulk data in general and images in particular. Other remarkable approaches utilize chaos theory and biologically-inspired approaches (Delman, 2004; Mao and Chen, 2005; Kumar and Ghose, 2009; Agarwal, 2012; Ratan, 2014). The principal idea of image encryption is *confusion* of image pixels and *diffusion* of pixel values to become more immune for the common attacks on cryptographic systems. Chaotic-based cryptography is one of the rapidly growing areas with several proposals for image encryption (Kocarev, 2001; Vohra and Patel, 2012). Thus, image encryption can take advantage of the fascinating properties of a chaotic dynamic system including randomness, and high sensitivity to system parameters and initial conditions. Biological processes, which are evolution-based (such as genetic algorithms, differential evolution and memetic algorithms), swarm based (such as particle swarm, ant colony, and immune systems), or neurosystem-based (such as artificial neural networks) have inspired many powerful computational algorithms for optimization, function approximation, learning or soft computing. These approaches have found promising applications in many complex systems including cryptography and cryptanalysis (Olariu and Zomaya, 2005; Laskari et al. 2005; Dadhich and Yadav, 2014).

In this chapter, after a brief background on chaos theory, we are going to first review the state-of-the-art of image cryptosystems with focus on chaotic-based and biologically-inspired approaches, whether used separately or combined. Although several approaches are reviewed and cited, this chapter is not meant to be comprehensive. We then provide a case study for image encryption utilizing ideas of genetic evolution such as mutation and crossover. We share some empirical results demonstrating and motivating the reader into this research field.

BACKGROUND: CHAOS THEORY

Over years since the early work of Herni Poincare in 1890, several attempts have been made toward developing understating of behavioral patterns associated with complex natural phenomena that are apparently unpredictable in the long term (Ditto and Munakata, 1995; Ott, 2002). Common characteristics of such phenomena are recurrence and extreme sensitivity to initial conditions, which is popularly referred to as a butterfly effect (this term is coined by Edward Lorenz to describe the potential influence on a hurricane caused by flapping the wings of a distant butterfly). Various systems have been investigated in the discrete and continuous time domains. Among the popular chaotic systems are:

- Chaotic maps (e.g. logistic map, Henon map, Arnold's cat map, Baker's map),
- Strange attractors (e.g. Lorenz weather model, Chau's circuit, Rossler attractor), and
- Double pendulum.