Chapter 26
Chaos-Based Cryptography for Voice Secure Wireless Communication

Sattar B. Sadkhan Al Maliky
University of Babylon, Iraq

Rana Saad
University of Babylon, Iraq

ABSTRACT

Chaos theory was originally developed by mathematicians and physicists. The theory deals with the behaviors of nonlinear dynamic systems. Chaos theory has desirable features, such as deterministic, nonlinear, irregular, long-term prediction, and sensitivity to initial conditions. Therefore, and based on chaos theory features, the security research community adopts chaos theory in modern cryptography. However, there are challenges of using chaos theory with cryptography, and this chapter highlights some of those challenges. The voice information is very important compared with the information of image and text. This chapter reviews most of the encryption techniques that adopt chaos-based cryptography, and illustrates the uses of chaos-based voice encryption techniques in wireless communication as well. This chapter summarizes the traditional and modern techniques of voice/speech encryption and demonstrates the feasibility of adopting chaos-based cryptography in wireless communications.

INTRODUCTION

Due to the increased demand for wireless communications by military and civilian applications, there are studies oriented towards the protection of information from eavesdroppers and attackers. This information is transmitted through communication channels between users. It can be text, image or voice signal (Lawande et al., 2005). The voice signal information is commonly used in the applications of wireless communications. It needs protection more than text/image information against eavesdroppers through wireless channel. The reason for such need arises from the fact that voice encryption process must encrypt all parts of signal information to get on indistinguishable voice (Mosa et al., 2009) (S. Sridhan et al., 1993). Cryptography algorithms must evolve with the

DOI: 10.4018/978-1-4666-8468-3.ch026

development of wireless communication technologies. The reason for this development is to give higher security. Cryptographic techniques can utilize number theory and Chaos theory. One of the new multidisciplinary approaches for designing and implementing a new cryptosystem is based on Chaos Theory (Jian et al,. 2010). It is found that the ideas of chaos have been very fruitful in such diverse disciplines as biology, economics, chemistry, engineering, fluid mechanics, physics, just to name a few. Chaos is a multidisciplinary science, and this is reflected in the fact that the members of the group are affiliated with diverse disciplines such as: Physics, Mathematics, Electrical Engineering, Physical Sciences and Technology (IPST), Electronics and Applied Physics (IREAP), Systems Research (SR), Applied Math and Scientific Computation (AMSC).

The deterministic property means that every next state of chaos function depends on the previous state. The irregular property shows the behavior of chaotic system has irregular continuity. Nonlinear property means that chaos function has nonlinear transformation. The sensitivity to initial conditions property means that some small changes in the initial state of chaotic systems could result dramatically in various behaviors at the final state. The long term prediction means that when achieving irregular and sensitive to initial conditions properties, then the prediction of the system's behavior will have obstacles (Munakata, 2008).

The aim is to show the techniques of three main objectives of this chapter. The objectives are chaos based cryptography, secure wireless communication and voice encryption. Also this aim makes the reader know how to use chaos in cryptography, what the generations of secure wireless communication, which use the chaos based cryptography.

MULTIDISCIPLINARY IN CHAOS BASED CRYPTOGRAPHY

Multidisciplinary is composed of several separate branches of learning or fields of expertise. These different disciplines (fields) can use chaos theory in their applications as illustrated in Figure 1 (David et al., 2012).

Figure 2 gives the schematic presentation of the chaos behavior. It shows the detail of these applications that exploit the chaos behavior. The behavior of chaos can be seen in the labs, in the nature, in an economics (Kyrtsou & Labys, 2006), in finance (Hristu-Varsakelis & Kyrtsou, 2008), in different other studies such as medical studies (White, 1999), quantum chaos theory study (Berry, 2003), electrical engineering and computer science chaotic systems as well as numerical analysis (Strang, 1991).

Chaos theory is an area of study in the competence of mathematics. It is formulated in 1961 (Berry. and Mainieri, 1996). Chaos is short of the term "chaotic system." It is a dynamic system because each outcome depends on one or more of its previous outcomes (Kellert, 1993) (Chesnes, 2001).

Figure 1. Different disciplines (fields) used within the chaos applications