Chapter 2
A Survey on Chaos Based Encryption Technique

Anandkumar R
Pondicherry Engineering College, India

Kalpana R.
Pondicherry Engineering College, India

ABSTRACT

Information security is an important field among the pervasive use of applications namely internet banking, mobile services, emails, viz., chaos-based encryption techniques play an important role in many security processes, namely: military systems, robotics, and other real time computing services. The secure transmission of audio, image and video are processed with unique characteristic of a third-party which makes the encryption and decryption highly secure for the users. In this chapter, a detailed survey on the various chaos-based encryption techniques is discussed and analyzed.

INTRODUCTION

Information security ensures the security, integrity, and availability of public data among the users on the web. In the present scenario of digital era, information security is an important concern that too with the pervasive use of potential applications such as internet banking, and emails. This necessitates cryptography which is a very essential part in any communication and networking systems will ensure the security, integrity, authenticity and availability of the data over the cloud environment. Lot of progressive research works are found in the literature by the individuals, academicians, and researchers for the past two decades on cryptographic algorithms. The security of any cryptographic protocol depends on the strength of cryptographic key and strength of cryptographic key depends on the length of a key. In the traditional cryptography, a random key is generated and the key will not be linked with the user, in turn it is very difficult to remember as the key as it is not linked with the user. The data will be initially encrypted, and the information will be secured with minimal crypto security features when the data is propagated in the network. The information will be more secured with public and private keys and dur-

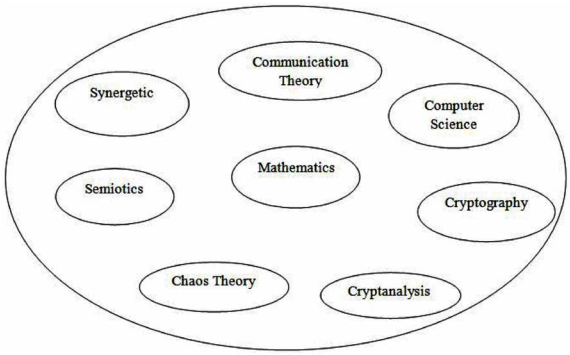
DOI: 10.4018/978-1-7998-7705-9.ch002

ing retrieval; the data will be decrypted with the same key. In the other hand the privacy of the data is network concern. Data shared in the network to be private is more secured. The data may be preserved using privacy techniques in any channel and transmit it with security including standards.

Contributing Areas of Cryptology

Cryptology is a part of mathematics. Cryptography and cryptanalysis comes under the mathematical study of cryptology. Cryptology is the process of hiding the data or information from the intruder. The combination of cryptography and cryptanalysis is called as cryptology. It has several research sections namely like information theory, computer science, cryptography, cryptanalysis, communication theory, semiotics, chaos theory and synergetic. The classification of cryptology is presented in Figure 1. (Shukla, Khare, Rizvi, Stalin, & Kumar, 2015).

Figure 1. Areas of Cryptology



1. Cryptography

Cryptography is a process of secret writing which is used to convert the original text message into a coded cipher manuscript message and is called as enciphering; converting of the plain text from the cipher manuscript is deciphering. In cryptography, the source user and the destination user uses the matching key is called as symmetric or secret key encryption. If source user and the destination user uses a dissimilar key which called as asymmetric or public-key encryption. The general cryptographic system is deputed in Figure 2.

Figure 2. View of Cryptography System