Chapter 39

Fast Chaotic Encryption Using Circuits for Mobile and Cloud Computing:

Investigations Under the Umbrella of Cryptography

Shalini Stalin
Aisect University, India

Piyush Kumar Shukla
University Instituter of Technology RGPV, India

Priti Maheshwary
Aisect University, India

Akhilesh Tiwari
Madhav Institute of Technology, India

Ankur Khare
M. K. Ponda College of Business and Management, India

ABSTRACT

In last few decades, a lot of work has been done in the field of cryptography; it is being considered one of the safe methods to protect data. It was first used to protect communication by individuals, armies, and organizational companies. With the help encryption method, anyone can protect their data from a third-party attack. Images are used in various areas like biometric authentication, medical science, military, etc., where they are being stored or transferred over the network and the safety of such images are very important. The newest movement in encryption is chaos-based, which is a better encryption technique than AES, DES, RSA, etc. It consists of different property such as sensitive independence on original situation, non-periodicity, non-convergence, etc. In recent times, many chaos-based image encryption algorithms have been proposed, but most of them are not sufficient to provide full protection to data. In this chapter, a survey of different chaos-based image encryption techniques is discussed.

DOI: 10.4018/978-1-7998-7705-9.ch039

INTRODUCTION

A clandestine distribution plan (Abirami,2005; Elshamy, 2003; Orue, 2002) is a convention to share a mystery among members such that just specified subsets of members can recoup the mystery. In considering the security ideas of mystery sharing plans, a few creators have published ideas of security for mystery sharing plans taking into account diverse data measures. These data measures incorporate four imperative data measures: Shannon entropy, min entropy, Renyi entropy and Kolmogorov multifaceted nature. Shannon entropy is the most broadly utilized data measure, which is utilized to demonstrate limits on the offer size and on the data rate in mystery sharing plans (Fitwi, 2011; Akhvan, 2013; Pande, 2011; Soleymani,2014). As of late, min and Renyi entropies are additionally utilized as a part of investigation of the security of mystery sharing plans (Cristina, 2014; Pande, 2011).Picture stowing is a type of steganography that works by inserting information into a computerized media with the end goal of ID, annotation, and copyrighting. This paper presents a novel picture steganography framework, which implants (RGB) mystery picture inside (RGB) spread picture picked by an improved flexible back engendering neural system. The proposed framework incorporates inserting and extraction stages. Three principle stages are incorporated inside the inserting stage, which are; best cover picture determination and handling stage, mystery picture choice and preparing stage and best implanting limit choice stage separately. Best cover picture is performed utilizing SOM and ERBP calculations. Mystery picture is handled by isolating it into (Red, Green, and Blue) shading layers and DWT is then connected. The shading layers are then changed over to bit streams; altered FLFSR in turns will be utilized to scramble these streams to get more secure framework. ERBP is again used to choose the best implanting edge values. The execution has been assessed amid inserting and extraction stages considering utilizing a few spread and mystery pictures and considering a few sizes (Bakhache, 2011; Khare & Shukla, 2015).

A few scientists used ordinary cryptosystems to straight forwardly encoding pictures. However, this is not prudent because of huge information size and continuous imperatives of picture information. Ordinary cryptosystems oblige a great deal of time to specifically encode a large number of picture pixels esteem. Then again, not at all like literary information, an unscrambled picture is generally satisfactory regardless of the fact that it contains little levels of contortion. For all the afore mentioned reasons, the calculations that capacity well for printed information may not be suitable for media information (Palacios & Juarez, 2002). Numerous studies have been performed on the utilization of printed encryption calculations for pictures by altering the calculations to adjust with picture attributes. One such alternative for encoding a picture is to consider a 2D variety of picture pixels esteem as a 1D information stream and to then scramble this stream with any customary cryptosystem (Bakhache, 2012; Mondal, 2016). This would be viewed as an innocent methodology and more often than not is suitable for content and event associate for little pictures records that are to be transmitted more than an armada devoted channel (Xia & Song, 2013). Subramanyan (2011) states that a picture encryption calculation in light of AES-128 in which the encryption procedure is a bitwise XOR operation on an arrangement of picture pixels. This system utilizes a starting 128-bit key and an AES key extension transform that progressions the key for each arrangement of pixels. The mystery keys are produced freely at both the sender and the collector sides in light of the AES key development process. In this manner, the introductory key alone is shared instead of the entire arrangement of keys (Bakhache, 2011).

Sensors are basic, little, modest gadgets for catching tactile information. A gathering of these sensors cooperating shape a sensor system. Sensor hubs are intended to self-sort out into a system after sending. Remote sensors have constrained assets as far as capacity, handling, memory, battery force, and transmis-