Chapter 3
Biometric Image Security Using Chaos Algorithm

Sugandha Agarwal
Amity University, India

O.P. Singh
Amity University, India

Deepak Nagaria
Bundelkhand Institute of Engineering and Technology, India

ABSTRACT

In this world of Advanced Technology, the Biometrics are proved to be a significant method for user identification. However, the use of biometric is not new, but these days, with the increase in multimedia applications, it has gained its popularity in analysing human characteristics for security purposes. Biometric Encryption using Chaos Algorithm is a technique used to make it more convenient to the user and to provide high level security. The most prominent physical biometric patterns investigated for security purposes are the fingerprint, hand, eye, face, and voice. In the proposed image encryption scheme, an external secret key of 160-bit is used. The initial conditions for the logistic map are derived using the external secret key. The results obtained through experimental analysis provide an efficient and secure way for real-time image encryption and transmission.

INTRODUCTION

In recent years, the communication has become easier, but hackers are smarter than anyone can think of. It is more important to get aware of and use the best techniques for secure image transfer. With the escalation of information exchange across the Internet, and the storage of sensitive data on an open network, cryptography has become an increasingly important feature of computer security. In this paper, we have focused on biometric encryption using chaos algorithm. A biometric is defined as a unique, measurable, physical or biological trait for automatically recognizing or authenticating the identity of a human being.

DOI: 10.4018/978-1-7998-1763-5.ch003

It includes data such as retina, iris, fingerprint, face, DNA, vein patterns, hand geometry, typing rhythm, mouse dynamics and voice. The main applications of biometrics are access controls, national ID card, passport control, border control, criminal investigation, and terrorist identification. Biometric is a very powerful tool for security purposes because of its property of uniqueness. Thus, biometric authentication can replace the use of passwords to secure a key. It provides a strong link between an individual and a claimed identity. This offers convenience and secure identity confirmation. If biometrics are used in most of the security systems for example bank locker systems, online transactions etc. then one can get a relief from remembering various passwords. It provides direct connection between the password and the user. A password is not tied to a user, the system running the cryptographic algorithm is unable to differentiate between the authorised user and an attacker who fraudulently acquires the password of an authorised user. As an alternative to password protection, biometric authentication provides a new mechanism for key security by using a biometric to secure the cryptographic key. Instead of entering a password to access the cryptographic key, the use of this key is guarded by biometric authentication. When a user wishes to access a secured key, he or she will be prompted to allow for the capture of a biometric sample. Biometric authentication is becoming the most popular and most reliable user authentication mechanism, even it is vulnerable to attacks.

LITERATURE REVIEW

Several encryption algorithms (Maniccam & Bourbakis, 2001; Jiun-In & Cheng, n.d.; Gu & Han, 2006; Seyedzade et al., 2010; Zhou et al., 2014; Younes & Jantan, 2008; Sinha & Singh, 2003; Zeghid et al., 2007; Xiao & Zhang, 2006; Alsafasfeh & Arfoa, 2011) have been proposed including Lossless image compression and encryption using SCAN by S.S.Maniccam, N.G. Bourbakis (Maniccam & Bourbakis, 2001), Mirror-like image encryption algorithm by Jiun-In Guo, Jui-Cheng Yen (Jiun-In & Cheng, n.d), Image encryption based on hash function by Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchak (Seyedzade et al., 2010) and Image encryption using Block-Based Transformation Algorithm by Mohammad Ali, Bani Younes and Aman Jantan (Younes & Jantan, 2008), but Chaos-based encryption techniques (Gu & Han, 2006; Zhou et al., 2014; Alsafasfeh & Arfoa, 2011) are considered good for practical use as these techniques provide a good combination of speed, high security, complexity and computational power etc. Consequently, the traditional ciphers like AES, DES, and RSA etc. are not suitable for real time image encryption as these ciphers require a large computational time and high computing power. For real time image encryption, only those ciphers are preferable which take lesser amount of time and at the same time without compromising security.

To ensure the privacy and security of the biometric system, many scholars have conducted researches to explore the possible risk of biometric network and feasible measurement to guarantee the security. Uludag et al. analysed the challenges involved in biometric application in authentication system and limitations of the biometric cryptosystems (Uludag et al., 2004). Many techniques have been introduced since to reduce the vulnerability of biometric data. Alok a Sinha and Kehar Singh introduced a technique for Image Encryption using Digital Signatures, Soutar et al. (1996), proposed an algorithm on biometric encryption. Alghamdi et al. (2010) states that image encryption cannot be used for large amount of data and high resolution images. Hao et al. (2005) presented a secure way to integrate iris biometric with cryptography. Chaos-based cryptography is the latest and efficient way to develop fast and secure cryptography for image encryption. The chaotic behaviour is the random behaviour of a nonlinear system