Computers and Electrical Engineering 000 (2018) 1–18

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security[☆]

Gaurang Panchal[a], Debasis Samanta[a,*]

Indian Institute of Technology, Kharagpur, West Bengal, India

ARTICLE INFO

Article history:
Received 21 October 2016
Revised 18 January 2018
Accepted 18 January 2018
Available online xxx

Keywords:
Cryptographic key generation
Biometric-based security
Data security
Bio-crypto system
Information forensics security

ABSTRACT

Existing biometric-based security mechanisms to ensure storage security follow Biometric Enrolment, Key Binding, Secure Sketch, Fuzzy vault or template store along with key of a user. Also, they use threshold based comparison or error calculation to authenticate the user. The storage of biometric data or key put the system under threats. Further, the user verification mechanism may not be accurate as the threshold selection is challenging. To alleviate this problem, we have proposed a novel approach to storage security. In our proposed approach, we extract biometric based statistical features to generate codeword of a user. To generate a codeword, we use Reed-Solomon encoding (RS). Later, this codeword will be used to generate a key. Prio to decryption, we authenticate user using SVM Ranking mechanism without threshold value. The major contributions include generation of unique and strong biocrypto keys from users' biometric data, Reed-Solomon encoding has been used to maintain the codeword and generation of key and SVM based ranking mechanism is used for the user verification where the storage of neither templates nor keys is required.

1. Introduction

Of late, users' data are not necessarily stored in users' own custody, rather stored in remote locations. As a consequence, the privacy of users' data is essential to ensure that data cannot be modified or viewed by other than the owners. Therefore, a reliable mechanism is necessary to ensure data storage security.

Several mechanisms have been proposed to protect user's own data, such as authentication by means of username, password. The problem with such a technique is that users should remember their usernames, passwords or store them in a secure manner. Moreover, such techniques are vulnerable to several attacks. This is because, a user's password can be easily guessed or broken by dictionary attacks [1]. While, simple passwords are easy to crack, complex passwords are difficult to remember. As an alternative to this, use of cryptographic key [2–4] has been advocated to keep the data secret. But in cryptographic systems, key management is a critical issue. In cryptographic systems, if a cryptographic key is too short or simple, then it can be easily cracked. On the other hand, if a key is long and complex, it is not easy to memorize and needs to be stored somewhere, which may be lost, stolen, thus making the system under threat. This motivates us to propose a new

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. G. Martinez Perez.

[*] Corresponding author.
E-mail address: dsamanta@iitkgp.ac.in (D. Samanta).

https://doi.org/10.1016/j.compeleceng.2018.01.028
0045-7906/© 2018 Published by Elsevier Ltd.

data encryption strategy using biometric data of a person. With our proposed technique, it is possible to generate a cryptographic key which is hard to crack. Further, users do not have to remember or store the cryptographic key in their custodies. Our proposed approach essentially uses a user's biometric data in cryptography. In other words, we use the user's biometric trait to generate a cryptographic key. Biometric-based cryptographic key generation, in fact, has many inherent problems. One major problem is that, similar key may not be generated each time because of different biometric sensors [5,6], different orientation of captured biometric trait, different scaling or noise in fingerprint data [7]. In other words, when we extract features from a captured biometric trait [8], some features may not be extracted or may be extracted with errors. Hence, it is not guaranteed to generate exactly the same cryptographic key from one occasion to another. The above-mentioned problem has been addressed in this work. The objective of our work is to generate a cryptographic key from the biometric data of a user. We term such a key as a bio-crypto key. Our approach is then to encrypt and decrypt user's data with the bio-crypto key.

In this work, we consider fingerprint as the biometric trait. We capture the biometric data using block based approach and generate the feature vector. This feature vector is used to generate codeword and cryptography key. Using this bio-crypto key, we encrypt user's data. In addition to this, we embed fingerprint biometric feature attributes namely lengths and angles of lines joining two minutiae points into random codeword using Reed-Solomon encoder. We concatenate this random codeword with the ciphertext. We call it as final ciphertext. In decryption process, we use newly captured fingerprint image and extract the feature vector. This feature vector is compared to the codeword for the user authentication. If user is authenitcated, we generate the key from the decoded form of the codeword.

In this work, we have addressed few research challenges in a succession of our proposed approach. We present an approach to extract the feature vectors from low quality, noisy and rotation-variant fingerprint images. Our approach is fast without compromise the accuracy of the result compared to the traditional approach. We have explored the mechanism to generate a biometric-based cryptographic key, which can be of any arbitrary large size and random enough to qualify for a strong cryptographic key. We present a mechanism to ensure the key bits sequences and a fixed key size in order to make encryption and decryption process successful for a genuine user. Also, we present a mechanism to transform the biometric features of a fingerprint data into the form of codeword using Reed-Solomon coding principle. In fact, the proposed codeword generation mechanism is to overcome the overhead of traditional enrollment mechanism. Apart from this, the security of the codeword which is embedded with the ciphertext is ensured. We present an accurate user verification mechanism using SVM ranking technique whose performance is comparable to that of the existing traditional approaches. Further, in our verification, we don't require any threshold value to be decided as a priory knowledge.

The rest of the paper is organised as follows. Proposed approach is discussed in Section 2. In Section 3, we present experimental results. The analysis of our approach is presented in Section 4. Finally, Section 5 concludes the paper.

2. Proposed Approach

In this section, we discuss our proposed approach. An overview of our proposed approach is shown in Fig. 1. In our approach, the number of errors to be corrected using Reed-Solomon in encryption and decryption phase should be same which may generate error. The different tasks involved in our approach are discussed in details in the following subsections.

2.1. Encryption Process

Our encryption process involves different tasks in order to encrypt a plaintext. The major task includes feature extraction, calculation of attributes of straight lines, obscuring straight lines attributes, biometric-based key generation, codeword generation and encryption. All these tasks are discussed in details as follows.

2.1.1. Feature extraction

We extract minutiae points, core point and delta point for a given fingerprint image. Let P be a set of minutiae points and $p(x,\ y)$ denotes the coordinate of a minutiae point p. We represent a set of minutiae points as $P = \{p_1(x_1, y_1), p_2(x_2, y_2), \cdots, p_k(x_k, y_k)\}$. Here, $p_i(x_i,\ y_i)$, $i = 1, 2, \cdots k$ represents minutiae points. Next, we detect the core and delta points[1] from the input fingerprint image. We represent the core point as $C_p(x_c,\ y_c)$, where x_c is the x-coordinate and y_c is the y-coordinate of the detected the core point C_p. Finally, we detect delta point from the fingerprint image. We represent the delta point as $D_p(x_d,\ y_d)$, where x_d is the x-coordinate and y_d is the y-coordinate of the detected core point D_p.

2.1.2. Calculating straight lines attributes

Our proposed approach is to calculate straight line attributes (i.e. lengths and inclinations) between the points in the set P. To do this, we first divide the fingerprint image into a small number of blocks. Let I be the fingerprint image, then we divide the fingerprint image I into a number of small blocks each of size $m \times m$ pixels, $m \ll M,\ N$, where $M \times N$ being the

[1] http://www.advancedsourcecode.com/orthogonalcore.asp.

Please cite this article as: G. Panchal, D. Samanta, A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security, Computers and Electrical Engineering (2018), https://doi.org/10.1016/j.compeleceng.2018.01.028