CRYPTO KEY GENERATION USING CONTOUR GRAPH ALGORITHM

M.S. ALTARAWNEH, L.C.KHOR, W.L.WOO and S.S DLAY

School of Electrical, Electronic and Computer Engineering
University of Newcastle
Newcastle upon Tyne, NE1 7RU
UNITED KINGDOM

Email: {mokhled.al-tarawneh, l.c.khor,w.l.woo,s.s.dlay}@ncl.ac.uk

ABSTRACT

Cryptography and biometrics have been identified as two of the most important aspects of digital security environment, for various types of security problems the merging between cryptography and biometrics has led to the development of Bio-Crypto technology. In this paper we propose a cryptography key generating methodology based on graph construction and adjacency matrix of extracted minutiae. The formation of graph relies on contour division of minutiae points area. Minutiae points area is studied on both scenarios (with singular point, and without singular point detection). Results show that with singular point detection the average of minutiae points area dimension is less than in the other case and at some points of threshold, it show an improvement performance comparing to the other one. 100% uniqueness key was achieved on both cases.

Key-Words: Biometric, Fingerprint, Minutiae, Contouring, Adjacency matrix, String matching, Security.

1. INTRODUCTION

With the rapid diffusion of information technology (IT) and its outputs, biometrics-based security systems that use physiological or behavioral traits are used in many applications of IT ranging from financial transactions to computer security. Even though these techniques have much superiority compared to traditional methods (token or knowledge based schemes) such as increased user convenience and robustness against impostor users, they are vulnerable to attacks from a template production to the storage database through a communication channels. Thus possibility of biometric database is compromised is one of the main concerns to protect biometric template during its journey from enrolment to matching. It is difficult to control and to trace hacking and cracking by unauthorized people. E-commerce, computer security and financial transaction applications need secure mechanism for accurate accessing sensitive information e.g. template database, financial database, for this purpose biometric based systems are applied [1]. The classical biometric systems have already been used for various tasks and in this paper we extend fingerprint enrolled template to generate combined encapsulated cryptographic key based on reforming graph and adjacency matrix of extracted minutiae data. Our proposed technique uses the information leaked by the fingerprint extractor based on advance image processing e.g. rotation, scaling and enhancement. We assume that matching difficulties, fingerprint variations are solved with a high quality images and noise free template of fingerprint is available at the enrolment time. When a fingerprint image is enrolled, only parts of the information e.g. location, orientation and types are stored. Extracted information could be used to defense itself by extract or extend new information based on the graphical and mathematical reformation. Contour based construction graph algorithm (CBCG) is proposed for generating the encapsulation cryptography key and this is illustrated in Figure 1.

![Figure 1. Contour Based Construction Graph algorithm block diagram.](image-url)

The process of generating the key comprises all necessary functions to achieve no-repudiation, encryption, digital signing and strong authentication in an open network [1]. Fingerprint base is seen as the best solution with regards to convenience, cost efficiency and reliability [2]. Among
The standard deviation of the Gaussian envelope $\sigma$ is the minutiae points area, $\mu$. The major novelty of the proposed approach consists in keeping minutiae points away from several attacks as a first security level of crypto-key generation life cycle. A formulation of fingerprint extracted information is used by CBCG, where the graph relation based on vertices and edges are formulated by minutiae points (1), and minutiae point area size for formatting a contour based graph as shown in Figure 2.

$$\mu = \{ \mu_i \mid \mu_i = (x_i, y_i, t_i) \mid i = 1, ..., N \}$$  \hspace{1cm} (1)

Where $x_i$ is the x-coordinate position, $y_i$ is the y-coordinate position and $t_i$ is the type of a particular minutiae.

In the graphical phase, we setup the minutiae points in setting area (200x200) in the case of singular point detection which is detected at the maximum of filtered orientation tensor field:

$$S(x, y) = \exp \left( -\frac{x^2 + y^2}{2\sigma^2} \right) \left( x + iy \right)^m$$  \hspace{1cm} (2)

where the positive sign between the real and the imaginary parts is associated to the core type, $m$ is the order filtration, and $\sigma$ is the standard deviation of the Gaussian envelope [5]. On the other case the image size is the area of tracing minutiae, crossing number (CN) method is used to perform minutiae extraction. CN extracts the ridge points from the skeleton image by examining the local neighborhood of each ridge pixel using a 3x3 window as follows:

$$\text{CN} = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}|, \quad P_9 = P_1$$  \hspace{1cm} (3)

where $P_i$ is the pixel belonging to the neighborhood of $P$. Extracted minutiae $\mu$ (NxM) pixels are grouped according to their coordinate $(x, y)$ within contours.

$$\text{QC} = \frac{\mu A}{C W}$$  \hspace{1cm} (4)

where QC is counters quantity, $\mu A$ is minutiae points area, and $C W$ is contour width.
Function \[\text{minutiae points} = \text{grouping (minutiae points)};\]
\[m = \text{minutiae numbers size};\]
\[\text{For } i=1:m \]
\[\text{Fix the points of X coordinate in width size} \]
\[\text{End} \]
\[\text{End} \]

In the mathematical and key generation phase, Adjacency matrix formatted within traced and grouped points (vertices) according to their connection ordering paths (edges) within the following rules:

On the same contour, \(v_i \rightarrow v_{i+1}\), visiting all vertices at that contour, and so upper and lower one. Adjacency matrix of \(N \times N\) matrix \(A\), in which \(a_{ij} = 1\) if there exists a path from \(v_i \rightarrow v_j\) and \(a_{ij} = 0\) otherwise. This is illustrated in Figure 3.

\[
\begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

**Fig 3.** Adjacency Matrix for given graph in fig 2

The output matrix is taken as an input for crypto generator and some mathematical operations will deal with it. These mathematical operations generate vectors and sub vectors which will be depend on cryptographic module algorithms, exist modules such as symmetric (DES, 3DES) are considered [10]. Another scenario is to partition produced matrix into sub-matrices, those could be used as secure encapsulated headers as shown in Figure 4, without de-capsulation previous headers, cipher text cannot be decrypted into plain one. Suggested encapsulation technique working as associated headers, that change the plain text formatting shape in type of encryption style, forwarding can be thought of one or more messages (locked text) inside locking header. This is illustrated in Figure 4. By applying entire summation of previous generated matrices and finding prime numbers vector, the largest primes can be used for crypto-module algorithm such as RSA [8][10]. Applying RSA rules of encryption and digital signatures generation within its privileges offer maximum security due to the huge key size involved.

The proposed algorithm is extensively tested on DB1, FVC2002 database, 880 fingerprints images (TIFF, format, 374x388 size, and 500 dpi resolution), 800 images was used in our tests. The algorithm is tested on both scenarios (with singular point, and without singular point detection). Figure 5 show that adjacency matrix size under singular point detection is less than in the other case. With average size for Sp=103, and without SP=148.

![Fig 5. Adjacency matrices dimension](image)

Cause of different sizes of generated matrices, the key strength will be higher resistant brute force attack. Uniqueness of the key will be determined by the uniqueness
of the fingerprint minutiae used in the key. Applying string matching algorithm on the generated matrices, it is found that that 100% uniqueness on both cases as input to the crypto module phase. The protocols of FVC2002 is used to evaluate the False accept Rate (FAR) and Genuine Accept Rate (GAR) for overall phases. FAR is ratio of the number of false acceptances divided by the number of identification attempts. While GAR is the ratio number of true positive parameter. Using these parameters, we have plotted the receiver operating characteristic (ROC) curves of both cases when implemented as core point detection as well as without core detection (see Fig. 5).

![ROC curves estimated for both cases](image)

Fig 5. ROC curves estimated for both cases

The curves in Figure 5 show that 100% ratio of both scenarios (with and without singular point). At some points of threshold, first case (area surrounding core point) show an improvement performance comparing to the other case (without singular point detection). Results show that key generation depend completely on quality assurance of images and prefect minutiae extractor such as a minutiae detector (MINDTCT) released by NIST fingerprint image software 2 [11]. Standard software automatically locates and record ridge ending and bifurcation in fingerprint images, it includes minutiae quality assessment based on local image condition.

5. CONCLUSION

In this paper, we tackled one of the most difficult problems for merging cryptography and bio-metrics: how to generate a repeatable string from a biometric in such a way that it can be revoked. It is found that, repeatable key generation is completely depend on the fingerprint image quality, to avoid this problem a proposed approach can be applied on a cluster of acquiring impressions, and optimal distance must be found between produced matrices, length of matrix could be control, if the matrix is partitioning into sub matrices, and apply (XO)ing relation on the generated subs. We have shown how to generate keys robustly from fingerprint using associated biometric measurements. Our approach produces long enough keys so that an attack on one does not give an attack on all. We believe, with the development of acquiring devices, and quality check algorithms, our proposed approach could be released for practical uses. Our future work will concentrate on string production matrices for usage with asymmetric cipher systems.

6. REFERENCES