An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates

N. Lalithamani
Assistant Professor
Department of Computer Science and Engineering
AMRITA School of Engineering
AMRITA Vishwa Vidyapeetham
Coimbatore

Dr. K.P. Soman
Professor & Head
Centre for Excellence in Computational
Engineering and Networking
AMRITA Vishwa Vidyapeetham
Coimbatore

Summary
Unswerving information security mechanisms are the need of the hour for fighting the escalating enormity of identity theft in our society. Besides cryptography being a dominant tool in attaining information security, one of the key confronts in cryptosystems is to preserve the secrecy of the cryptographic keys. The incorporation of biometrics with cryptography will be an effective solution to this problem. Recently generating cryptographic key from biometrics has gained enormous popularity in research community due to its improved performance in providing security. Nevertheless, a biometric is enduringly connected with a user and cannot be altered. Thus, when a biometric identifier is compromised, it is lost everlastingly and probably for every application where that particular biometric is employed. Cancelable biometrics intends to resolve this by building revocable biometric templates. In this paper, we have proposed an effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates. Initially the minutiae points are extracted from the fingerprints. Afterwards, cancelable templates are generated and irrevocable keys are extracted from the cancelable templates. As the cryptographic key is generated in an irreversible manner, obtaining cancelable fingerprint templates and original fingerprints from the generated key is impossible. We have evaluated the effectiveness of our scheme using fingerprints from publicly available sources. We have also presented the security analysis of the proposed scheme.

Keywords:
Biometrics, Cancelable Biometrics, Cryptography, Biometric cryptosystems, Key generation, Irrevocable Key, Fingerprint, Minutiae Points.

1. Introduction

Protecting personal privacy and preventing identity theft are of national precedence. These goals are indispensable to our democracy and our economy, and intrinsically significant to our citizens. Biometrics, a budding set of methodologies, assures an efficient solution. In the domain of computer security, biometrics denotes the authentication techniques that depend on quantifiable physiological and individual features that can be automatically demonstrated. Despite the fact that the field of biometrics is still in its formative years, it's unavoidable that biometric systems will play a significant role in the future of security [1]. A biometric system is fundamentally a pattern recognition system that functions by obtaining biometric data from an individual, extracting a feature set from the obtained data, and evaluating this feature set against the template set in the database [2]. The biometric data comprises of fingerprints [3], facial features [4], iris [5], hand geometry [6], voice [7], signature [8] and the like. Biometrics is extensively employed in forensics, in criminal identification and prison security to quote a few of the instances, and has the prospective to be employed in a wide variety of civilian application areas.

Throughout the last decade biometrics has gained popularity in application employed for identifying individuals. The accomplishment of its relevance in user authentication has signified that numerous benefits could possibly be obtained by integrating biometrics with cryptography [9]. The incapability of human users to keep in mind the powerful cryptographic keys has been an issue restricting the security of systems for decades. This restriction could be resolved in a huge variety range of applications by producing strong cryptographic keys from biometric data, possibly in combination with the entry of a password [10, 11, 12]. Biometric features are highly complicated to duplicate or falsify and impracticable to share. These characteristics of biometrics influence their utilization in cryptographic key generation. In the recent past, researchers have shifted their attention towards merging biometrics with cryptography in order to enhance overall security, by eliminating the necessity for key storage using passwords [8, 4, 9].

The systems that combine biometrics with cryptographic security are known as Biometric cryptosystems, or Crypto-biometric systems [13]. The incorporation of biometrics with cryptography can be widely carried out at two different levels. Considering biometrics-based key release, a biometric matching between an input biometric signal and an enrolled template aids in the release of the secret key. The biometric signals are found to be monolithically

Manuscript received March 5, 2009
Manuscript revised March 20, 2009

bounded to the keys in case of biometrics-based key generation [14]. The principal complexity in biometric cryptosystems lies in the accommodation of the deviations intrinsic in measuring biometrics, or in the biometrics themselves, despite iteratively generating the same key [7]. Lately numerous researchers have attempted to design cryptosystems on basis of biometrics to eradicate some of the problems however have not yet been victorious in exploiting the power of biometrics in a complete manner [15].

Despite possessing benefits including the non-repudiation and convenience of utilization and the like, biometrics comprises certain issues [13] that limit its utilization as a key to a cryptosystem. A significant issue in the utilization of biometrics is that the number of biometrics that can be acquired from a person is restricted and the conciliation of it would mean that that specific biometric is rendered futile perpetually. Once the biometric features are lost, a replacement is unfeasible. It is entirely evident, once an old fingerprint is gone missing, a new fingerprint for the same person is not attainable. It is possible to revoke or replace compromised credit cards and passwords however biometrics are enduringly connected with a user and are impossible to replace. Cancelable biometrics [16] has been projected in literature so as to address this issue. Cancelable biometrics intends to resolve this by building revocable biometric templates [17], [18].

Cancelable biometric templates are necessary for biometric authentication systems, particularly for the ones that are operated under unsupervised and/or over networked environments [19], [20]. In case of cancelable biometrics, the biometric image is distorted in a repeatable yet nonreversible fashion prior to the generation of the template. When the cancelable template is compromised, the distortion characteristics are altered, and the same biometrics is mapped to a fresh template, which is utilized consequently. A cancelable biometric template needs to accomplish four significant criteria before being measured as valuable [21]. Diversity: No equivalent cancelable template can be utilized in two distinct applications. Reusability: Straightforward revocation and reissue at the occurrence of compromise. One-way transformation: Non-invertibility of template computation to avoid recovery of biometric data. Performance: The formulation should not worsen the recognition performance.

This paper discusses an effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates. As the fingerprints are one of the most widely used biometric modality today, we have employed the fingerprint biometrics in our scheme. Owing to the fact that majority of the fingerprint authentication systems work on basis of minutiae, which are feature points obtained from a raw fingerprint image, we have utilized the minutiae points in the cancelable fingerprint template formation and cryptographic key generation. As discussed above, initially the minutiae points are extracted from the fingerprint images using the approach discussed. Then, the cancelable fingerprint templates are formed from the extracted minutiae points. Subsequently, the irrevocable cryptographic key is generated from the cancelable fingerprint template using the proposed approach. The fingerprint images from publicly available sources are used in evaluating the proposed scheme. The security analysis of the proposed scheme is also presented.

The rest of the paper is organized as follows. A brief review of the works related to the proposed scheme is given in Section 2. The approach to extract the minutiae points from the fingerprint image is discussed in Section 3. The cancelable fingerprint template generation from the extracted minutiae points is explained in Section 4. The irrevocable cryptographic key generation from the cancelable fingerprint template is presented in Section 5. Security Analysis of the proposed scheme is presented in Section 6 and experimental results are given in Section 7. Finally, the conclusions are summed up in Section 8.

2. Review of Related Works

Our work is inspired by a number of previous works related to cryptographic key generation from biometrics and cancelable biometrics. A brief review of some of the works is given below:

A cancelable biometric approach, called PalmHashing was projected by Connie Tee et al [22] in order to solve the problem non-revocable biometric. The method hashes palmprint templates with a set of pseudo-random keys to arrive at a distinctive code known as palmhash. It is possible to store the palmhash code in portable devices like tokens and smartcards for verification purposes. Furthermore, PalmHashing provides numerous advantages over present-day biometric approaches like, unambiguous partition of the genuine-imposter populations and zero EER occurrences. They also delineated the implementation details of the method besides emphasizing its potentials in security-critical applications.

A practical and secure way to integrate the iris biometric into cryptographic applications was presented by Hao, F. et al [23]. They deliberated the error patterns within iris codes and introduced a two-layer error correction technique that merges Hadamard and Reed-Solomon codes. The key was produced from a subject's iris image using auxiliary error-correction data that do not disclose the key and can be stored in a tamper-resistant token, like a smart card. They assessed the system with the aid of iris samples from 70 different eyes, with 10 samples from each eye.

They figured out that it is possible to reproduce an error-free key dependably from genuine iris codes with a 99.5 percent success rate.

The application of handwritten signature to cryptography on basis of recent works displaying the probability of key generation employing biometrics was studied by M. Freire-Santos et al [14]. A cryptographic construction known as fuzzy vault was implemented in the signature-based key generation scheme. The utilization of distinguishing signature characteristics suited for the fuzzy vault was conferred and evaluated. The results of experimentation were reported along with the error rates involved in releasing the secret data with the aid of both random and skilled forgeries from the MCYT database.

A two-factor cancelable formulation was proposed by Teoh AB et al [25], where in, the biometric data are distorted in a revocable but non-reversible fashion by initially converting the raw biometric data into a fixed-length feature vector and then projecting the feature vector onto a sequence of random subspaces that were obtained from a user-specific pseudorandom number (PRN). The procedure was revocable and made the replacement of biometrics appear as simple as replacing PRNs. The formulation was established under numerous situations (normal, stolen PRN, and compromised biometrics scenarios) with the aid of 2400 Facial Recognition Technology face images.

A straightforward mechanism for the generation of digital signatures and cryptography communication through the aid of biometrics was proposed by Je-Gyeong Jo et al [26]. It is necessary to generate the digital signature in such a way that it can possibly be verified by the prevailing cryptographic algorithm like RSA/ElGamal without altering its own security requirement and infrastructure. It was anticipated that the mechanism will guarantee security on the binding of biometric information in the signature system on telecommunication environments.

Julien Bringera et al [27] have presented the Cancelable biometrics and secure sketches with an identical purpose in mind: to guard the privacy of biometric templates besides maintaining the ability to match the protected data against a reference. The standard beyond cancelable biometrics was to carry out an irreversible transformation over images and to create matching over transformed images. They demonstrated that applying secure sketch error correction to cancelable biometrics permits one to maintain good matching performance.

The concept of cancelable biometrics was proposed by Andrew B. J. Teoh et al. [28] to express biometric templates that can be cancelled and restored with the addition of another independent authentication factor. A kind of cancelable biometrics that merges a set of user-specific random vectors with biometric features is known as BioHash. The quantized random projection collection on basis of the Johnson-Lindenstrauss Lemma was employed to accomplish the mathematical foundation of BioHash. Depending upon this model, they have explained the characteristics of BioHash in pattern recognition in addition to security view points and provided some methods to resolve the stolen-token problem.

A.T. Beng Jin and Tee Conniea [29] have proposed the Cancelable biometrics in order to describe biometric templates that can possibly be canceled and replaced. A kind of cancelable biometrics that merges a set of user-specific random vectors with biometric features is known as BioHash. The chief disadvantage of BioHash was its immense deprivation in performance when the legitimate token is stolen and is utilized by the pretender to claim as the legitimate user. A modified probabilistic neural network was utilized by them as a classifier to address the aforesaid issue.

Biometric-key generation is a procedure to transform a piece of live biometric data into key with the aid of auxiliary information that is also known as a biometric helper. It is possible to repetitively generate a biometric-key and it is not necessary to physically store the biometric. Beng, A. et al. [30] presented a biometric-key generation system which worked on basis of a randomized biometric helper. The scheme comprises of a randomized feature discretization process and a code redundancy construction. The former facilitates one to manage the intra-class variations of biometric data to the minimal level and the latter additionally lessens the errors. The randomized biometric helper guarantees that a biometric-key was simple to be rescinded when the key was compromised.

The production of biometric keys directly from live biometrics, under specific criteria, by dividing feature space into subspaces and further dividing these into cells, where each cell subspace contributes to the overall key produced, was illustrated by Sanaul Hoque et al. [31]. They assessed the scheme on real biometric data, denoting both genuine samples and attempted limitations. Experimental evaluations illustrated the extent to which the technique can be implemented dependably in possible practical situations.

3. Extraction of Minutiae Points from Fingerprints

The extraction of minutiae points from the fingerprint image is discussed in this section. It is supposed that fingerprints are distinct across individuals and across the fingers of a particular individual [32]. It has been established that even identical twins with identical DNA

possess different fingerprints. Since many existing fingerprint authentication systems are based on minutiae points, which are feature points extracted from a raw fingerprint image, we have employed the minutiae points in our scheme as well. A fingerprint can be defined as a pattern of ridges and valleys on the tip of the finger. A fingerprint is therefore described by the distinctiveness of the local ridge features and their relationships. Minutiae points denote these local ridge characteristics that appear either at a ridge ending or a ridge bifurcation. The point where the ridge comes to an abrupt end is known as ridge ending and the ridge bifurcation is denoted as the point where the ridge divides into two or more branches.

The major steps involved in the minutiae points extraction are as follows:

- Segmentation
- Orientation Field Estimation.
- Image Enhancement
- Minutiae Extraction

3.1 Segmentation

The first step in the minutiae points extraction is segmentation. The input fingerprint image is segmented from the background to actually extract the region comprising the fingerprint, which ensures the removal of noise. Segmentation of an image represents the division or separation of the image into regions that have similar attributes. At first, the image is preprocessed. The preprocessing phase includes the following: histogram equalization and median filtering. Later, the preprocessed image is divided into blocks and segmentation is carried out. The sample fingerprint images are shown in Figure 1.

Fig. 1. Two Sample Fingerprint Images

3.1.1 Preprocessing

The preprocessing of fingerprint images includes the following:

(i) Histogram Equalization
(ii) Median Filtering

(i) Histogram Equalization:
Histogram equalization amplifies the local contrast of the images, particularly when they are represented with very close contrast values. It is possible to distribute intensity through the histogram with the aid of this regulation. Histogram equalization utilizes a monotonic, non-linear mapping that re-assigns the intensity values of pixels in the input image in such a manner that the output image comprises a uniform distribution of intensities (i.e. a flat histogram). The original histogram of a fingerprint image is of bimodal type, the histogram after the histogram equalization transforms all the range from 0 to 255 which results if enhanced visualization effect [33]. The results of histogram equalization are depicted in Figure 2.

Fig 2: Fingerprint Images after Histogram Equalization

(ii) Median Filtering:
The median filter is a non-linear digital filtering methodology frequently employed to eliminate noise from images or other signals. This is carried out with the aid of a window comprising of an odd number of samples. The values present within the window are arranged into numerical order; the median value, the sample in the center of the window, is chosen as the output. The oldest sample is abandoned, a new sample is obtained, and the calculations are redone [34]. The filtering process is applied to the fingerprint image obtained as a result of the previous step by spatially convolving the image with the filter. The results of median filtering are shown in Figure 3.

Fig 3: Fingerprint images after median filtering.

3.1.2 Segmentation

The image obtained after preprocessing has high contrast and enhanced visibility. Subsequently, the preprocessed fingerprint image is divided into non-overlapping blocks

of size 16x16 followed by the calculation of gradient of each block. The standard deviation of gradients in X and Y direction is computed and summed. Eventually, the resultant value is compared against a threshold value. If it is greater than the threshold value the block is filled with ones, otherwise the block is filled with zeros. In our scheme, the threshold value is set as 20.

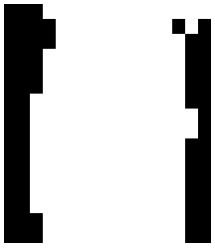


Fig 4: Segmentation result of fingerprint image

3.2. Orientation Field Estimation

The next step in the extraction of minutiae points is the estimation of orientation field. A fingerprint field orientation map may be described as an ensemble of two-dimensional direction fields. They denote the directions of ridge flows in regular spaced grids. It is possible to neglect the magnitudes of these fields and the angle information alone is of interest [35]. Basically there are two methodologies to compute the orientation field of fingerprint namely the filter-bank based approaches and gradient-based approaches. We have employed gradient based approaches in our scheme. In case of the gradient-based methods, initially, the gradient vectors are determined by considering the partial derivatives of image intensity at every pixel. The gradient vectors can be represented as $[g_x, g_y]^T$. In case of a fingerprint image, the gradient vectors indicate the highest deviation of gray intensity that is perpendicular to the edge of ridge lines [35]. Conventionally, an orientation map is denoted in the form of a matrix $\{\theta_{XY}\}$, where $\theta_{XY} \in [0, \pi]$. The orientation θ is orthogonal to $\overline{\varphi}$, in which $\overline{\varphi}$ is the dominant gradient angle of a local base block.

3.3 Image Enhancement

Following the orientation field estimation, the fingerprint image is enhanced to extract the minutiae points effectively. The enhancement of fingerprint images involves the following: Average filtering and Gabor filtering. Initially the image is filtered with the help of average filter to correct the frequency of the image. Subsequently, Gabor filtering is applied to the image for further enhancement.

3.3.1 Averaging Filter

The impact of noise can be decreased through simple averaging. Provided a noisy yet bounded measurement sequence it is possible for us to take a huge number of readings of the variable and employ its average to provide improved estimate of its true value (given that there is no systematic error or bias in the measurements). This is in fact the standard process in experimental work, where numerous readings are taken at a sampling instant and the average of these readings utilized as the measurement [36].

3.3.2 Gabor Filter

A Gabor filter can be described as a linear filter whose impulse response is given by a harmonic function multiplied by a Gaussian function. Owing to the multiplication-convolution property (Convolution theorem), the Fourier transform of a Gabor filter's impulse response is the convolution of the Fourier transform of the harmonic function and the Fourier transform of the Gaussian function [37].

$$g(x, y; \lambda, \theta, \psi, \sigma, \gamma) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right) \cos\left(2\pi \frac{x'}{\lambda} + \psi\right)$$

Where,

$$x' = x\cos\theta + y\sin\theta$$

and

$$y' = -x\sin\theta + y\cos\theta$$

Here, λ denotes the wavelength of the cosine factor, θ denotes the orientation of the normal to the parallel stripes of a Gabor function, Ψ corresponds to the phase offset, γ denotes the spatial aspect ratio and enumerates the ellipticity of the support of the Gabor function. The Gabor filter comprises of both frequency-selective and orientation-selective properties and constitutes optimal joint resolution in both spatial and frequency domains. Thus the Gabor filter is capable of removing the noise and conserve true parallel ridges structures taking the benefit of the local orientation and local frequency [38].

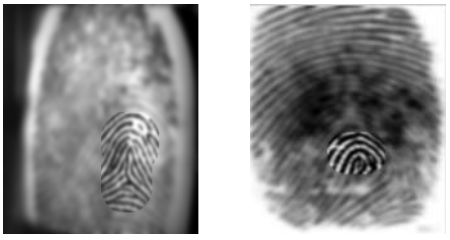


Fig 5: Enhanced Images Clearly showing Delta Region

3.4 Minutiae Points Extraction

Finally, the minutiae points are extracted from the enhanced fingerprint image. The steps involved in the extraction of minutiae points are as follows:

- Binarization
- Morphological Operations
- Minutiae points extraction

Initially, the enhanced image is binarized. After binarization, morphological operations are performed on the image to remove the obstacles and noise from it. Finally, the minutiae points are extracted using the approach discussed.

3.4.1 Binarization

The binary images with only two levels of interest: The black pixels that denote ridges and the white pixels that denote valleys are employed by almost all minutiae extraction algorithms. A grey level image is translated into a binary image in the process of binarization, by which the contrast between the ridges and valleys in a fingerprint image is improved. Hence, the extraction of minutiae is achievable. The grey-level value of every pixel in the enhanced image is analyzed in the binarization process. Then, the pixel value is set to a binary value one when the value is greater than the global threshold, or else a zero is set as the pixel value. The foreground ridges and the background valleys are the two level of information held by the ensuing binary image. Removal of distortions present in the image is performed followed by the retrieval of the exact skeleton image from the image.

3.4.2 Morphological Operation

The binary morphological operators are applied on the binarized fingerprint image. Elimination of any obstacles and noise from the image is the primary function of the morphological operators. Furthermore, the unnecessary spurs, bridges and line breaks are removed by these operators. Then thinning process is performed to reduce the thickness of the lines so that the lines are only represented except the other regions of the image. Clean operator, Hbreak operator, Spur operator and Thinning are the morphological operators applied.

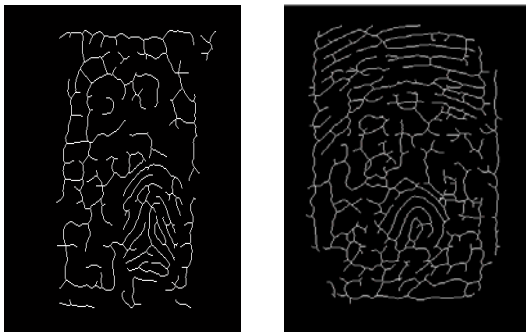


Fig 6: Fingerprint Images after Morphological Operations

Thinning is a morphological operation that proficiently wears away the foreground pixels until they become one pixel wide, thus, the thickness of every line of pattern is minimized to a single pixel width [39] the process of removal of redundant pixels till the ridges become one pixel wide is facilitated by ridge thinning. The Ridge thinning algorithm utilized for Minutiae points' extraction in our scheme is employed by the authors of [40]. The image is divided into two dissimilar subfields that bear a likeness to a checkerboard pattern. In the initial sub iteration, only when all three conditions, G1, G2, and G3 are satisfied the pixel p from the initial subfield is erased. Whereas, in the second sub iteration, only when all three conditions, G1, G2, and G3' are satisfied, the pixel p from the foremost subfield is erased.

Condition G1:

$$X_H(P) = 1$$

Where

$$X_H(P) = \sum_{i=1}^{4} b_i$$

$$b_i = \begin{Bmatrix} 1 \text{if } x_{2i-1} = 0 \text{ and } (x_{2i} = 1 \text{ or } x_{2i+1} = 1) \\ 0 \quad \text{otherwise} \end{Bmatrix}$$

$x_1, x_2, ..., x_8$ are the values of the eight neighbors of p, starting with the east neighbor and numbered in counter-clockwise order.

Condition G2:

$$2 \le \min\{n_1(p), n_2(p)\} \le 3$$

where

$$n_1(p) = \sum_{k=1}^{4} x_{2k-1} \vee x_{2k}$$

$$n_2(p) = \sum_{k=1}^{4} x_{2k} \vee x_{2k+1}$$

Condition G3:

$$(x_2 \vee x_3 \vee \bar{x}_8) \wedge x_1 = 0$$

Condition G3':

$$(x_6 \vee x_7 \vee \bar{x}) \wedge x_5 = 0$$

One iteration of the thinning algorithm combines the two subiterations.

The fingerprint images with minuatie points marked are shown in Figure 7. The locations i.e) the coordinates of the extracted minutiae points are obtained and used in the subsequent processes.

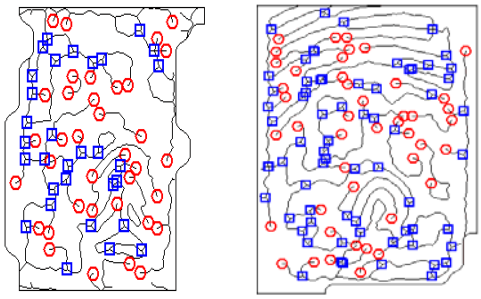


Fig 7: Fingerprint Images With Minutiae Points

4. Generation of Cancelable Fingerprint Templates

The generation of cancelable fingerprint templates from the extracted minutiae points is explained in this section. The minutiae points extracted from the fingerprint image are represented as follows:

$$M_P = \{P_1, P_2, P_3, ..., P_n\}$$

and their corresponding x, y coordinates are specified separately as

$$M_{P_1}(x_1, y_1), M_{P_2}(x_2, y_2), M_{P_3}(x_3, y_3), ..., M_{P_n}(x_n, y_n)$$

With the aid of these x, y coordinates the distance between each point with respect to the other points is calculated.

$$\begin{Bmatrix} Mp_1 \\ Mp_2 \\ Mp_3 \\ \vdots \\ Mp_n \end{Bmatrix} = \begin{Bmatrix} (P_1, P_j) \\ (P_2, P_j) \\ (P_3, P_j) \\ \vdots \\ (P_n, P_j) \end{Bmatrix} \qquad j = 1 \ to \ m, \ P_i \neq P_j$$

The distance between two points is computed using the following equation:

$$Dis\tan ce(P_i, P_j) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

Where (x_i, y_i), (x_j, y_j) are the co-ordinates of the points P_i and P_j respectively. Once the calculation of the respective distances for each point is done, the values are sorted in a separate array and the unique values are represented as the array elements. The array is denoted as:

$$\begin{Bmatrix} D_1 \\ D_2 \\ D_3 \\ \vdots \\ D_n \end{Bmatrix} = \begin{Bmatrix} (d_{11}, d_{12}, \cdots, d_{1m}) \\ (d_{21}, d_{22}, \cdots, d_{2m}) \\ (d_{31}, d_{32}, \cdots, d_{3m}) \\ \vdots \\ (d_{n1}, d_{n2}, \cdots, d_{nm}) \end{Bmatrix}$$

and the values obtained are denoted as

$$D = [D_1 \ D_2 \ D_3 \ \cdots \ D_n]$$

The values thus obtained are sorted further and the formula for sorting them is given as

$$S_D = Sort(D)_{Asc}$$

Where as the unique values are represented as

$$U_D = \cup S_D = [u_{D_1} \ u_{D_2} \ \cdots \ u_{D_n}]$$

The UD thus formed is known as the cancelable fingerprint template. This cancelable template is employed in the generation of irrevocable cryptographic key.

5. Generation of Irrevocable Cryptographic Key

The irrevocable cryptographic key is generated from the cancelable fingerprint template formed with the aid of the approach discussed in this section. The cancelable fingerprint template U_D is divided into two equal parts of same size for shuffling purpose. The first part of the divided values are represented as,

$$U_{D_1} = [u_{D_1} \ \cdots \ u_{D_n/2}]$$

and the other half values are denoted as

$$U_{D_2} = [u_{D_{\frac{n}{2}+1}} \ \cdots \ u_{D_n}]$$

The elements of U_{D_1} and U_{D_2} are shuffled and stored in SU_{D_1} and SU_{D_2} respectively. The shuffling is performed as follows. An element of U_{D_1} is taken and the modulo operation is performed between the current element and

$N/2$, where N represents the total number of elements in U_D. The resultant value is denoted as ind. Subsequently the current element of U_{D_1} is placed in SU_{D_2} at ind th position. The aforesaid process is repeated for all the elements of U_{D_1} and U_{D_2}. Consequently the SU_{D_1} and SU_{D_2} are combined to form a vector SU_D.

$$SU_D = [SU_{D_1} \cup SU_{D_2}]$$

The shuffled vector SU_D is converted into a matrix MU_D of size $sqrt(|SU_D|) * sqrt(|SU_D|)$.

$$MU_D = (a_{ij}) sqrt(|SU_D|) * sqrt(|SU_D|)$$

Finally, the irrevocable key vector IK_V is generated from the matrix MU_D as follows:

$$IK_V = \{k_i : P(k)\}, \mathrm{i} = 1,....,|\mathrm{SU_D}|$$

Where

$P(k) = |SM_{ij}| \bmod 2,$

$\mathrm{SM_{ij}} = MU_D\ \mathrm{i, j : i + size, j + size, -1 < i, j < sqrt(|SU_D|)}$

The final key thus generated is more secured and irrevocable. Obtaining cancelable fingerprint template from the generated key is impossible.

6. Security Analysis

The security of the proposed scheme is strengthened by the following two robust features.

- Cancelable Transform
- Irreversible Analysis

6.1 Cancelable Transform

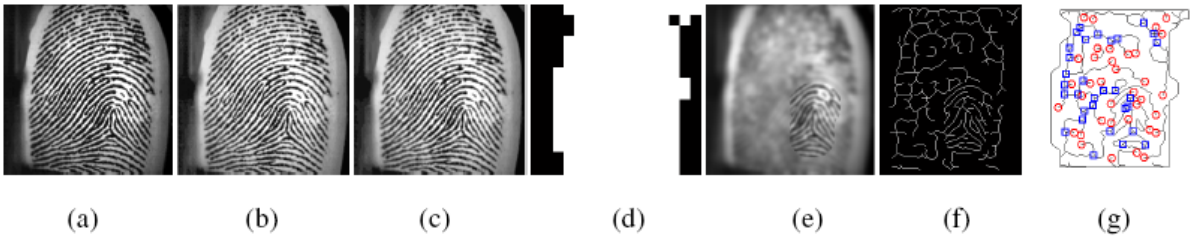
Cancelable transform [24] is employed to produce a cancelable template. The key target of the cancelable transformation is to proffer cancelable skill to a "non-invertible" transform. Generally, it is found to reduce the discriminative power of the original template. Thus, the cancelable templates and the secure templates of an individual in dissimilar applications will be diverse. However, the cross matching across databases will not be possible. Furthermore, it is possible to cancel and reissue the protected template by altering the cancelable transform parameters.

6.2 Irreversible Analysis

In order for the enunciation of the concept further, the tracing of the matrix with the aid of determinant or reorganizing shuffled data is entirely impracticable, analogous to attempting the generation of original document through hashed bits once hashing function is applied. The innate irrevocable nature reinforces the protection of our scheme. Hence, it is virtually unfeasible to trace the cancelable fingerprint template from the generated keys. The projected scheme is further appropriate and explicit for data such as the ones employed for managing minutiae points arrived at through the aforesaid procedure.

7. Experimental Results

In this section we have presented the experimental analysis of our proposed scheme. Our scheme is programmed in Matlab (Matlab7.4). We have tested the proposed system with diverse fingerprint images from publicly available sources. The minutiae points are extracted from the fingerprint images using the approach discussed in the paper. Initially, the fingerprint image is segmented from the background to extract the region that actually contains the fingerprint. Further the orientation field is estimated and the fingerprint image is enhanced using average filtering and Gabor filtering. Subsequently, the minutiae points are extracted and their coordinates are obtained. The coordinates of the minutiae points are then employed in the generation of cancelable fingerprint template. Eventually, the irrevocable cryptographic key is generated from the cancelable fingerprint template. The input image, extracted minutiae points, the intermediate results and the generated irrevocable cryptographic key of two different fingerprint images are shown in Figure 8 and Figure 9 respectively.




```
10011111111111111110011111111111111000111111111111110001111111111111100011111111111111100011
11111111111110111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111101111111111111100011111111111111111111111111111111111111111111111111111111111111111111111
```

(h)

Figure 8: (a) Input Fingerprint Image (b) Histogram Equalized Image (c) Median Filtered Image (d) Segmented Image (e) Enhanced Image (f) Morphological Processed Image (g) Fingerprint images with Minutiae Points (h) Generated irrevocable key


```
10101111111111111001111111111111111101111111111111101111111111111111001111111111111111110111
11111111111001111111111111110001111111111111111111111111111111101111111111111111000111111111
11111100111111111111101111111111111111111111111111111111111111111111111111111111111111111111
```

(h)

Figure 9: (a) Input Fingerprint Image (b) Histogram Equalized Image (c) Median Filtered Image (d) Segmented Image (e) Enhanced Image (f) Morphological Processed Image (g) Fingerprint images with Minutiae Points (h) Generated irrevocable key.

8. Conclusion

The steadily escalating reports on security infringements have necessitated the increase in concern for the security of information. Despite cryptography being a powerful tool attains information security, one of the chief demands in cryptosystems is to sustain the secrecy of the cryptographic keys. Combining biometrics with cryptography has provided an effective solution to this problem. Generation of cryptographic key from biometrics has gained enormous popularity in research community. Lately, the cancelable biometric systems have been widely recognized in the applications that are highly demanding in terms of privacy and security of biometric templates. We have presented an effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates in this paper. Initially the minutiae points are efficiently extracted from the fingerprints followed by the generation of cancelable templates and extraction of irrevocable keys from the cancelable templates in a successful manner. As the cryptographic key is generated in an irreversible manner, obtaining cancelable fingerprint templates and original fingerprints from the generated key is impossible. We have evaluated the effectiveness of our scheme using fingerprints from publicly available sources successfully. Moreover, we have as well presented the security analysis of the proposed scheme.

References

[1] John Chirillo and Scott Blaul, "Implementing Biometric Security," Wiley Red Books, ISBN: 978-0764525025, April 2003.

[2] Jain, A.K., Ross, A. and Prabhakar, S, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp: 4- 20, 2004.

[3] T.C. Clancy, N. Kiyavash and D.J. Lin, “Secure smart card-based fingerprint authentication,” Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Application, WBMA 2003.

[4] A. Goh, D.C.L. Ngo, “Computation of cryptographic keys from face biometrics,” International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1–13, 2003.

[5] Wildes, R.P., "Iris recognition: an emerging biometric technology," In Proceedings of the IEEE, Vol. 85, No. 9, pp:1348 - 1363, Sep 1997.
[6] Övünç Polat and Tülay Yıldırım, "Hand geometry identification without feature extraction by general regression neural network," Expert Systems with Applications, Vol. 34,No. 2, pp. 845-849, 2008.
[7] F. Monrose, M.K. Reiter, Q. Li and S. Wetzel, "Cryptographic key generation from voice," Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.
[8] F. Hao, C.W. Chan, "Private Key generation from on-line handwritten signatures," Information Management & Computer Security, Issue 10, No. 2, pp. 159–164, 2002.
[9] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces," 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp:394 - 401, 3-5 Dec,2007.
[10] G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric identification. In Proceedings of the 1998 IEEE Symposium on Security and Privacy, pages 148–157, May 1998.
[11] A. Juels and M. Wattenberg. "A fuzzy commitment scheme". In Proceedings of the 6th ACM Conference on Computer and Communication Security, pages 28–36, November 1999.
[12] F. Monrose, M. K. Reiter, and S. Wetzel. "Password hardening based on keystroke dynamics". In Proceedings of the 6th ACM Conference on Computer and Communications Security, pages 73–82, November 1999.
[13] U. Uludag, S. Pankanti, P. S., and A. Jain, "Biometric cryptosystems: Issues and challenges," Proceedings of the IEEE 92, pp. 948–960, June 2004.
[14] M. Freire-Santosa, J. Fierrez-Aguilara, J. Ortega-Garciaa, "Cryptographic key generation using handwritten signature", In Proc. SPIE, volume 6202, pages 225–231, 2006.
[15] Nagar, A. and Chaudhury, S, "Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme," 18th International Conference on Pattern Recognition, Vol. 4, pp: 537-540, 2006.
[16] M. Savvides, B.V.K. Vijaya Kumar, and P.K. Khosla, "Cancelable biometric filters for face recognition", ICPR, pp. 922-925 Vol.3, 23-26 Aug. 2004.
[17] Nalini Ratha, Jonathan Connell, Ruud M. Bolle, Sharat Chikkerur, "Cancelable Biometrics: A Case Study in Fingerprints", Proceedings of the 18th International Conference on Pattern Recognition, vol:4, Pages: 370 - 373,2006.
[18] Russell Ang, Reihaneh Safavi-Naini, Luke McAven: "Cancelable Key-Based Fingerprint Templates." ACISP, pp: 242-252, 2005.
[19] Cheung King-Hong , Kong Adams ,Zhang David , Kamel Mohamed , You Jane , LAM Toby , LAM Ho-Wang , "An analysis on accuracy of cancelable biometrics based on biohashing" ,International Conference on Knowledge-Based Intelligent Information and Engineering Systems ,September 14-16, 2005.
[20] Ratha, N.K., Connell, J.H., Bolle, R.M.: "Enhancing security and privacy in biometrics- based authentication systems", IBM Systems Journal 40, pp: 614-634, 2001,.
[21] Andrew Beng Jin Teoh, Kar-Ann Toh and Wai Kuan Yip,"2^N Discretisation of BioPhasor in Cancellable Biometrics", Advances in Biometrics, Springer Berlin / Heidelberg, Vol. 4642, 2007.
[22] Connie Tee, Teoh Andrew, Goh Michael, Ngo David, "Palmhashing: a novel approach for cancelable biometrics", Information processing letters, vol. 93, no:1, pp. 1-5, 2005.
[23] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.
[24] Y C Feng, Pong C Yuen, and Anil K Jain, "A Hybrid Approach for Face Template Protection," in Proc. of SPIE Conference of Biometric Technology for Human Identification, Orlando, FL, USA, vol. 6944, 18 March 2008.
[25] Teoh AB, Yuang CT., "Cancelable biometrics realization with multispace random projections.", IEEE Trans Syst., vol:37, no:5, pp:1096-106, 2007.
[26] Je-Gyeong Jo, Jong-Won Seo and Hyung-Woo Lee, "Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint ", Lecture Notes in Computer Science, Springer, Vol: 4613, Pages 38-49, 2007.
[27] Julien Bringera, Hervé Chabannea, Bruno Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics", Science of Computer Programming, Volume 74, Issues 1-2,Pages 43-51, 2008.
[28] Andrew B. J. Teoh, Yip Wai Kuan, Sangyoun Lee," Cancelable biometrics and annotations on BioHash ", Pattern Recognition, Vol: 41, Issue 6, pp: 2034-2044, 2008.
[29] Andrew Teoh Beng Jin, Tee Conniea, "Remarks on Bio-Hashing based cancelable biometrics in verification system", Neurocomputing, Vol: 69, no: 16-18, Pages 2461-2464, 2006.
[30] Beng, A., Jin Teoh, Kar-Ann Toh, "Secure biometric-key generation with biometric helper", 3rd IEEE Conference on Industrial Electronics and Applications, pp: 2145-2150, 2008.
[31] Sanaul Hoque, Michael Fairhurst, Gareth Howells "Evaluating Biometric Encryption Key Generation Using Handwritten Signatures", Bio-inspired, Learning and Intelligent Systems for Security, pp: 17-22, 2008.
[32] S. Pankanti, S. Prabhakar, A.K. Jain, "On the individuality of fingerprints", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 8, pp.1010–1025, 2002.
[33] Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S., "Filterbank-based fingerprint matching", IEEE Transactions on Image Processing, vol. 9, no. 5, pp: 846-859, May 2000, Doi: 10.1109/83.841531.
[34] J. Patrick Fitch, Edward J Coyle and Neal Gallagher, "Median filtering by Threshold Decomposition", IEEE Transactions on Acoustics, Speech and Signal Processing (ASSP), vol. 32, no.6, pp. 1183 - 1188,1984
[35] Yi Wang, Jiankun Hu and Fengling Han, "Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields," Applied Mathematics and Computation, Special Issue on Intelligent Computing Theory and Methodology, Vol. 185, No. 2, pp. 823-833,15 February 2007.
[36] M.Tham, "Averaging Filter," University of Newcastle from http://lorien.ncl.ac.uk /ming/filter/filave.htm

[37] “Gabor Filter” from http://en.wikipedia.org /wiki/Gabor_filter.
[38] Lin Hong, Wan Yi-fei and A. Jain,”Fingerprint Image Enhancement: Algorithm and Performance Evaluation,” IEEE Transaction on Pattern Analysis and Matching Intelligence, vol. 20, no.8, pp: 777-789, 1998.
[39] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, " Fingerprint Verification System using Minutiae Extraction Technique", in proc. of World Academy of Science, Engineering and Technology, vol. 36, December 2008
[40]L. Lam, S. W. Lee, and C. Y. Suen, “Thinning Methodologies-A Comprehensive Survey”, IEEE Transactions on Pattern analysis and machine intelligence, vol. 14, no. 9, 1992.

Lalithamani was born in 1975. She received her Masters degree in 1998. She holds a University rank as a part of her post graduate programme. Her fields of interest include (active) databases, automated biometrics, security systems and computers, reconfigurable computing architectures and performance evaluation. In 1999, she received an award for her exemplary service to the department. She is currently an Assistant Professor in Computer Science and Engineering Department, AMRITA School of Engineering, AMRITA Vishwa Vidyapeetham, Coimbatore. She has finished several courses related to computer system management, database searched, object oriented analysis and design, Software Engineering and Project Management. She worked on several projects concerning e-learning.

Dr. K.P. Soman B.Sc. (Engg.), P.M.Dip. (SQC&OR, ISI-Calcutta), M.Tech. (IIT-Kgp.), Ph.D (IIT-Kgp.) Professor & Head, Centre for Excellence in Computational Engineering and Networking, AMRITA Vishwa Vidyapeetham , Coimbatore. 20 years of research & teaching experience at IIT-Kharagpur and Amrita. Has around 100 publications in national & international journals and conference proceedings. Has organized a series of workshops and summer schools in e-commerce, fractals, chaos, neural networks, and wavelets for industry and academia. Authored books are “Insight into Wavelets”, “Insight into Data mining” and “Support Vector Machines and Other Kernel Methods” published by Prentice Hall, New Delhi, Project Investigator of the ongoing consortia project for Automated Machine Translation.