An Approach to Robust Biometric Key Generation System Design

Nemanja Maček[1], Borislav Đorđević[2], Jelena Gavrilović[3], Komlen Lalović[4]

[1] SECIT Security Consulting, 21 Aksentija Maksimovića Street, 26000 Pančevo, Serbia; e-mail: nmacek@secitsecurity.com

[2] Mihailo Pupin Institute, University of Belgrade, 15 Volgina Street, 11060 Belgrade, Serbia; e-mail: borislav.djordjevic@pupin.rs

[3,4] Faculty of Informatics and Computing, Singidunum University, 32 Danijelova Street, 11000 Belgrade, Serbia,
e-mails: jgavrilovic@singidunum.ac.rs, komlen.lalovic.13@singimail.rs

Abstract: This paper presents a novel approach to the design of robust multimodal biometric cryptosystems. The design objectives behind the system are robustness, privacy of user's biometric templates and stable cryptographic key generation. The framework presented in this paper employs two modalities and a look-up table. The hashes of cryptographic keys generated from a biometric template during the enrollment phase are stored in the look-up table with cancelable templates generated from the sample belonging to different modality of the same subject. During the operation phase, the system releases the key, only if the hash of the key generated from the provided biometric sample is found in the look-up table, and the similarity score between corresponding cancelable templates is less than a predefined threshold. The implementation of the proposed framework with iris and fingerprint biometrics is evaluated with the CASIA biometric template database.

Keywords: biometry; multimodal; cryptography; key generation; robustness

1 Introduction

"Biometrics is the science of establishing the identity of an individual based on physical, chemical or behavioral attributes of the person" [1]. Due to the distinctive nature of biometric traits [2] and the non-repudiation it offers [3], biometry is frequently used to enhance the overall security of the system in which it is implemented: the authentication system or the biometric cryptosystem.

Biometric authentication is the process of validating the uniqueness of individuals according to their physiological or behavioral qualities [4]. Physiological qualities,

such as a fingerprint, an iris or a face, refer to something that an individual is. Behavioral qualities, such as speech, signature and keystroke dynamics refer to something that an individual can do. According to Biggio [5], the generic modular biometric authentication system operates as follows. A user who wants to access some resources provides his identity. The sensor acquires the biometric sample of the user. Features are extracted from the sample and a similarity score is calculated between the provided biometric sample and the one stored in the biometric template database corresponding to the provided user identity. The similarity score is compared with the threshold and the user is identified as genuine or an impostor. According to this decision, the access to resources is granted or denied.

There are several advantages of biometric authentication over traditional authentication methods, such as difficulties in stealing, sharing and reproduction of biometric samples, tolerance to brute force attacks, and non-repudiation (an authenticated user cannot deny his activities) [6].

There are two types of biometric systems: a unimodal, which employs a single biometric sample acquired from the user, and a multimodal, which employs two or more modalities, e.g. an iris and a fingerprint. Multimodal systems prevail over some drawbacks of unimodal systems, such as large false rejection rates (FRR) and unacceptable false acceptance rates (FAR): additional information provided to the classifier increases the recognition accuracy and decreases error rates, while the identity proof is strengthened as data is acquired from different sources [7]. When compared to unimodal, multimodal systems are less prone to spoof attacks [8] and carefully crafted attacks targeted towards modular biometric authentication systems (replaying old data, feature extractor overriding, stored template modification, communication channel interception and providing synthetic vectors to the matching module) [9, 10].

The basis of multimodal biometric authentication systems is the information fusion. The decision level fusion [11] is the initial approach to information fusion in multimodal biometric authentication systems. This approach is based on majority vote scheme that is used to combine classification results from different modalities and make the final decision [12]. At the matching score level [13], the system calculates similarity scores between the sample and the corresponding template for each modality and combines them to verify the identity of an individual. At the feature level, feature vectors extracted from different modalities are integrated into a new vector that represents the identity of the individual [14].

Biometric cryptosystems, such as, key generation and key binding systems, combine a high level of security that is provided by cryptography and non-repudiation provided by biometry. Key generation systems are systems that produce a stable cryptographic key that is extracted from biometric data [15, 16]. Key binding systems are systems that bind a randomly generated cryptographic key to the biometric template [17, 18]; the bound key is released to the application

upon a valid presentation of the appropriate biometric template. Stored biometric samples pose a risk to users' privacy. If stored in an insecure manner, an adversary may carry out an identity theft attack on the cryptosystem. Defense strategies include the protection of stored templates with cancelable biometrics (intentional distortion of biometric features with non-invertible transforms) and the usage of multimodal biometrics.

Again, the main thrust of this paper is a novel approach to robust biometric cryptosystem design. The proposed system is the hybrid multimodal system that employs one biometric sample to generate a stable cryptographic key and another sample belonging to a different modality to authenticate the user. The design objectives are a stable bitstream, improved robustness, biometric template privacy and the reduction of false acceptance rates. According to the design objectives, the system employs a look-up table that stores the hashes of keys generated during the enrollment phase and cancelable biometric templates used for identity verification. This increases the overall security of the system – an adversary cannot obtain the biometric key or the authentication template as the data stored in the look-up table is processed with non-invertible transformations. The implementation of the proposed framework that employs an iris as the key generation biometrics and a fingerprint as the user authentication biometrics has been experimentally evaluated with the samples from the CASIA biometric template database.

2 Related Work

Chang et al. [16] proposed a framework for stable cryptographic key generation from unimodal biometric traits that are unstable in nature. The main contribution of their research is the approach to generating distinguishable biometric features, resulting in a stable cryptographic key. Although the performance of the proposed framework is evaluated with the face database containing facial expressions and head motion variations, the authors have stated that the framework is applicable to other biometric modalities as well.

Many studies that examine the usage of fingerprints in key generation systems and cancelable biometrics are reported in the literature. Tuyls et al. [19] have extracted consistent and reliable information bits from fingerprint samples using a set of four complex Gabor filters and BCH (Bose-Chaudhuri-Hocquenghem) error correction codes. However, FAR ranging from 2.5% to 3.2% is an unacceptable result for generated 45 bit and 89 bit keys. According to Solanki and Patel [20] it is possible to generate a 128 bit cryptographic key from fingerprint biometrics using Gabor filtering, but no FRR or FAR rates are reported. Ratha et al. [21] presented several methods to generate multiple cancelable identifiers from fingerprint images. Authors compared the performance of Cartesian, polar, and surface folding transformations of the minutiae positions and provided a proof that

the transforms are non-invertible. The fingerprint authentication system presented by Ang et al. [22] employs a key-dependent transformation of biometric data. Key-dependent transforms allow different templates to be stored for different applications, reducing the chance to link biometric template to an individual.

Hao et al. [23] developed a two-layer error correction technique that merges Hadamard and Reed-Solomon codes, thus providing a secure way to incorporate the iris biometrics into cryptographic applications. According to authors, an error-free 140 bit key can be reproduced from biometric samples with acceptable 0.47% FRR and 0% FAR rates, while a 192 bit key can be reproduced with 3.65% FRR and 0% FAR rates. Bae et al. [24] presented a novel feature extraction algorithm, based on independent component analysis for iris recognition. According to the authors, the proposed method has a similar Equal Error Rate (EER) to conventional methods based on Gabor wavelets, while the iris code size and feature extraction time have been significantly reduced.

Wu et al. [25] have developed a novel face biometric cryptosystem that uses a 128-dimensional principal component analysis vector and error correction codes (ECC) generated by Reed-Solomon algorithm. During the decryption phase, a biometric key is generated using the look-up table created at the encryption stage and the final key is obtained using both the biometric key and ECC. Sashank Singhvi et al. [26] developed a technique that exploits an entropy dependent feature extraction process coupled with Reed-Solomon error correction, resolving an issue resulting from the different acquisition of similar biometric samples. The authors have evaluated this technique with 3D face data and have concluded that the technique reliably produces 128 bit AES keys. The non-conventional methods of face feature extraction are presented by Ban et al. in [27]: HLO (hidden layer output) images are generated by the feature extraction of the multilayer perceptron in auto-association mode, while INDEX images are formed by a self-organized map used for image vector quantization.

Although the majority of research in multimodal biometrics is related to authentication, there are several researches related to cryptographic key generation reported in the literature, e.g. the feature fusion of an iris and minutiae [6], combining biometric features of an iris and a retina [28], or an iris and a face [29].

3 Proposed Framework

The main idea behind our approach is to combine a unimodal key generation system and a unimodal biometric authentication system into a robust multimodal biometric cryptosystem that will generate a stable bitstream with a 0% false acceptance rate. The framework of the proposed system that employs a strict decision level fusion approach is presented in Figure 1 (enrollment phase) and

Figure 2 (operating phase). During the enrollment phase, a user provides two biometric samples to the system. One sample is used to generate the key and another (belonging to different modality) is used to authenticate the user. In the enrollment phase the following steps are performed:

1) Biometric data used to generate the key is acquired by the sensor.
2) Data is preprocessed, features are extracted, and a cryptographic key is generated from the biometric template.
3) The hash of the cryptographic key is calculated.
4) Biometric data used for the authentication is acquired by another sensor.
5) Data is preprocessed and a cancelable biometric template is generated with non-invertible transforms.
6) The hash of the generated key and a cancelable biometric template are stored in the look-up table.

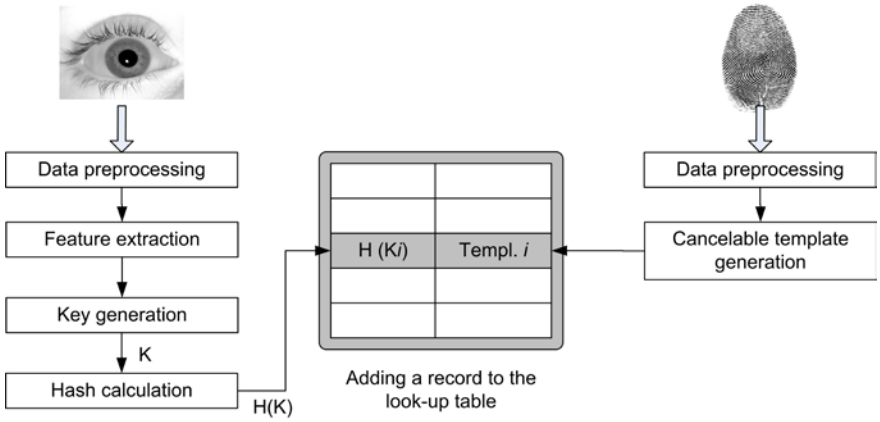

Figure 1
Robust multimodal biometric key generation framework (enrollment phase)

At the operating phase, a user provides two biometric samples to the system. The system performs the same 1-5 operations, as in the enrolment phase. Once the hash of the generated key and the cancelable biometric template are generated from the provided biometric samples, the system seeks the corresponding hash in the look-up table. If no hash matching the calculated one is found in the table, the system releases no key to the application and the user must provide his biometric sample again. If the matching hash is found, the system calculates the similarity score between the generated cancelable biometric template and the one stored in the look-up table corresponding to the hash. According to the similarity score, the system decides whether to release the key to the application or not.

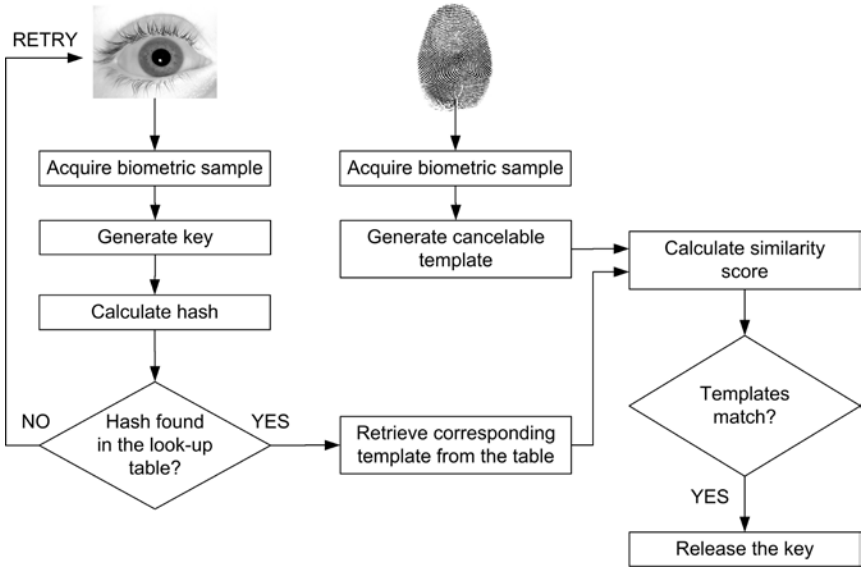

Figure 2
The operating phase of the proposed system

To sum up, the key is released to the application only if:

- The hash calculated from the key produced from the provided biometric sample is found in the look-up table, and
- The similarity score calculated between the generated cancelable biometric template and the one stored in the look-up table is less than the predefined threshold.

3.1 Security Evaluation of the Proposed Framework

Before we present one possible implementation of the framework, some general observations regarding the stability of a generated bitstream and overall system security are discussed.

The system stores hashes of generated keys for each user of the system in the look-up table. A slight modification in results obtained from a key generation process during the operation phase will result in a different calculated hash. As the key is released to the application only if the corresponding hash is found, it can be concluded that the system releases identical keys from the same biometric sample every time the user provides it. According to that, we conclude that the system produces the stable key.

The security of the system and the privacy of biometric templates are provided by one-way hash functions and non-invertible transforms. If an adversary obtains access to the look-up table, it is still impossible for them to regenerate the key or biometric templates that are produced during the enrollment phase. This results in a robust system with a 0% false acceptance rate (excluding brute force attacks). According to the attack taxonomy of Barreno et al. [30], the system cannot be compromised by targeted attacks: even if an adversary obtains access to the look-up table, he cannot select the user ID whose integrity he wants to compromise, as user identities are not stored in the table. The only drawback of the system is possible indiscriminate availability violations, as an adversary might randomly change stored hashes and cancelable templates, which could result in DoS to genuine users. However, all authentication systems are vulnerable during the enrollment phase and the aforementioned conclusions apply only to systems that are not compromised during that phase.

4 Implementation of the Proposed Framework: Iris and Fingerprint

This section presents the implementation of the proposed framework. Iris biometrics is used to generate the cryptographic key and a fingerprint to authenticate the user. Conventional methods are used to generate the key from an iris and extract minutiae points from a fingerprint. A cancelable template is generated by simple and effective non-invertible cell shuffling proposed by authors, which is a key-less modification of Ratha et al. Cartesian transform [21].

4.1 Generating Cryptographic Key from Iris Biometrics

More than 250 distinguishing characteristics of an iris (degrees of freedom) can be used in biometrics, resulting in six times more identifiers than the fingerprint [31]. Before the key is generated from extracted features, the acquired iris image must be preprocessed. The outer radius of iris patterns and pupils are first localized with Hough transform that involves a canny edge detector to generate an edge map. A poorly localized iris will result in unsuccessful segmentation and poor reproducibility of the key. This step is crucial in the enrollment phase, as extreme FRR may result in DoS to legitimate users. A Hough transform identifies the positions of circles and ellipses [32]: it locates contours in an *n*-dimensional space by examining whether they lie on curves of a specified shape. Hough transform for outer iris and pupil boundaries and a set of *n* recovered edge points (x_i, y_i) is defined by:

$$H\left(x_c, y_c, r\right) = \sum_{i=1}^{n} h\left(x_i, y_i, x_c, y_c, r\right), \tag{1}$$

$$h\left(x_i, y_i, x_c, y_c, r\right) = \begin{cases} 1, \left(x_i - x_c\right)^2 + \left(y_i - y_c\right)^2 - r^2 = 0 \\ 0, \left(x_i - x_c\right)^2 + \left(y_i - y_c\right)^2 - r^2 \neq 0 \end{cases}. \tag{2}$$

The circle (x_c, y_c, r) through each edge point (x_i, y_i) is defined as:

$$\left(x_i - x_c\right)^2 + \left(y_i - y_c\right)^2 = r^2. \tag{3}$$

The triplet that maximizes H (x_c, y_c, r) is common to the greatest number of edge points and is a reasonable choice to represent the contour of interest [33]. Similar technique that uses parameterized parabolic arcs is used to detect upper and lower eyelids. Once an iris image is localized, regions of interests are defined and it is transformed into fixed-size rectangular image. The normalization process employs Daugman's homogeneous rubber sheet model that remaps the iris image $I(x, y)$ from Cartesian (x, y) to polar coordinates (r, θ) [34]:

$$I\left(x\left(r,\theta\right), y\left(r,\theta\right)\right) \rightarrow I\left(r,\theta\right). \tag{4}$$

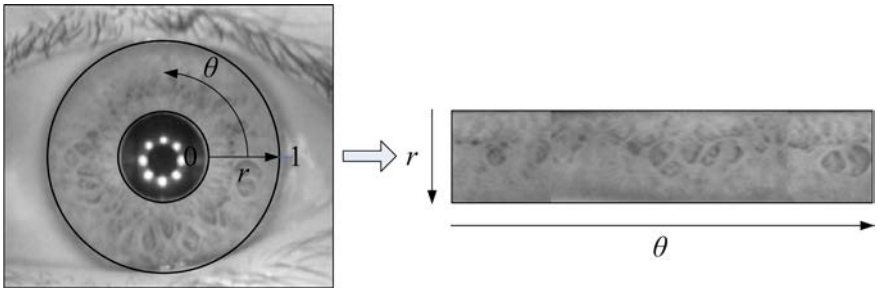

Figure 3
Daugman's rubber sheet model: localized iris (left) and normalized iris (right)

Parameter r is on the interval [0, 1] and θ is the angle [0, 2π]. If iris and pupil boundary points along θ are denoted as (x_i, y_i) and (x_p, y_p), respectively, the transformation is performed according to:

$$x\left(r,\theta\right) = \left(1-r\right) x_p\left(\theta\right) + x_i\left(\theta\right), \tag{5}$$

$$y\left(r,\theta\right) = \left(1-r\right) y_p\left(\theta\right) + y_i\left(\theta\right). \tag{6}$$

The rubber sheet model does not compensate rotational inconsistencies, but it takes into account pupil dilation size inconsistencies in order to produce a normalized representation with constant dimensions [31] set by angular resolution (the number of radial lines generated around the iris region) and radial resolution (the number of data points in the radial direction).

Although various extraction methods are reported in the literature, discriminant features are extracted from a normalized iris using conventional method based on Gabor filtering. This method is validated as suitable feature extraction method in various researches presented by other authors. A normalized image is broken into a number of 1-D signals that are convolved with 1-D Gabor wavelets. The frequency response of 1-D log-Gabor filter, introduced by Field [35] is given by:

$$G(f) = e^{-\left(\log\frac{f}{f_0}\right)^2 \Big/ 2\left(\log\frac{\sigma}{f_0}\right)^2}, \tag{7}$$

where f_0 denotes center frequency, and σ denotes the bandwidth of the filter. Phase quantization is applied to four levels on filtering outputs (each filter produces two bits of data for each phasor) and the quantized phase data is used to encode an iris pattern into a bit-wise biometric template. An error correction code is generated using the Reed-Solomon algorithm and the template is digested into a key. The number of bits in the biometric template depends on angular and radial resolution and the number of used filters, while the template entropy depends on the number of used filters, their center frequencies and the parameters of the modulating Gaussian.

4.2 Minutiae Points Extraction

Minutiae points are extracted from the fingerprint biometrics prior to cancelable template generation. This procedure consists of several steps: preprocessing, segmentation, orientation field estimation, image enhancement and minutiae extraction.

The first operation applied to the acquired sample is histogram equalization, which increases the local contrast of the image. The Wiener filter removes blur and additive noise from the picture without altering ridge structures of the fingerprint biometric sample. Let $H(u, v)$ denote the Fourier transform of the point spread-function of the degradation process $h(x, y)$ and $H^*(u, v)$ the complex conjugate of degradation function. The Wiener filter [36] in frequency domain is given by:

$$W(u,v) = \frac{H^*(u,v)}{\left|H(u,v)\right|^2 + P_n(u,v)/P_s(u,v)}, \tag{8}$$

where $P_n(u, v)$ denotes the power spectrum of the noise and $P_s(u, v)$ is the power spectrum of the under-graded image $f(x, y)$. If blur is negligible and only additive noise needs to be removed, the filter takes the form:

$$W(u,v) = \frac{P_s(u,v)}{P_s(u,v) + \sigma_n^2}, \tag{9}$$

where σ_n^2 is the noise variance. The output of the Wiener filter is divided into equal-sized non-overlapping blocks. Let N denote the size of the block and $\mu(I)$ the mean pixel value of the block. The block I is considered to be a foreground block if its variance is greater than the threshold τ_s:

$$\sigma^2(I) = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(I(i,j) - \mu(I)\right)^2 > \tau_s \tag{10}$$

This process is referred to as segmentation and is used to separate the regions of interest from the rest of the image. The next step in the extraction process is the estimation of orientation field (the local orientation of ridge valley structures), which is also a block-wise operation. The approach to orientation field estimation used in this research is gradient based. Gradient vectors indicate the highest deviation of gray intensity that is normal to the edge of ridge lines [37]. Let g_x and g_y denote gradient vectors of the block centered at pixel (i, j) in horizontal and vertical directions, respectively. The orientation θ of each block is given by:

$$\theta = \frac{1}{2}\tan^{-1}\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N} 2g_x(i,j)\,g_y(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}\left(g_x^2(i,j) - g_y^2(i,j)\right)}\right) + \frac{\pi}{2} \tag{11}$$

The image is enhanced by the Gaussian low-pass filter followed by the 2-D Gabor filter [38]. Let f_0 denote the ridge frequency, θ the orientation of the filter, σ_x and σ_y standard deviations of the Gaussian envelope along the x and y axes, and $[x_\theta, y_\theta]$ coordinates of $[x, y]$ after the clockwise rotation of the Cartesian axes by $0.5\pi–\theta$. The 2-D Gabor filter is given by:

$$G(x, y, \theta, f_0) = e^{-\frac{1}{2}\left(\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right)}\cos(2\pi f_0 x_\theta) \tag{12}$$

$$x_\theta = x\sin\theta + y\cos\theta \tag{13}$$

$$y_\theta = -x\cos\theta + y\sin\theta \tag{14}$$

As minutiae extraction algorithms operate on binary images, the filtering output is binarized. Gray level of each pixel is compared to a global threshold, resulting in the image with two levels of interest: ridges (black pixels) and valleys (white pixels). Morphological operators are further applied to the binarized image in order to eliminate noise resulting from spurs and line breaks. The thinning algorithm presented by Lam et al. [39] reduces the width of ridge lines. The image is segmented into two subfields as in the checkboard pattern. Let p_1, p_2, ... $p_8 \in [0, 1]$ denote neighbor pixels of pixel p as shown in Figure 4, and let b_i=1 if:

$$p_{2i-1} = 0 \wedge \left(p_{2i} = 1 \vee p_{2i+1} = 1\right) \tag{15}$$

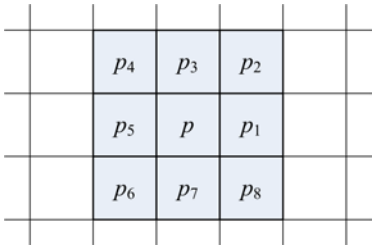

Figure 4
Eight neighbor pixels of p in a binarized image

Crossing number $X_H(p)$, according to the definition of Hilditch, is the number of times one crosses from white to black point when points are traversed in order. Four pixel removal conditions used in the iterations of the algorithm are defined as follows:

$$X_H(p) = \sum_{i=1}^{4} b_i = 1 \tag{16}$$

$$2 \le \min\left\{\left(\sum_{i=1}^{4} p_{2i-1} \vee p_{2i}\right), \left(\sum_{i=1}^{4} p_{2i} \vee p_{2i+1}\right)\right\} \le 3 \tag{17}$$

$$\left(p_2 \vee p_3 \vee \overline{p_8}\right) \wedge p_1 = 0\,. \tag{18}$$

$$\left(p_6 \vee p_7 \vee \overline{p}\right) \wedge p_5 = 0\,. \tag{19}$$

The condition $X_H(p)=1$ implies that p is a contour point [39]. Each iteration of the algorithm has two sub-iterations. Pixel p is deleted from the first subfield in the first sub-iteration only if conditions (16), (17) and (18) are satisfied. The pixel p is deleted from the second subfield in the second sub-iteration only if conditions (16), (17) and (19) are satisfied. The result of the algorithm is an image composed of one pixel wide ridges, with clearly visible ridge terminations and bifurcation points (valley endings). Crossing number $X_R(p)$ is calculated for each pixel in the resulting image, according to definition of Rutovitz, as the number of transitions from white to black and vice versa when points in are traversed in order. The pixel p is identified as ridge termination point if:

$$X_R(p) = \sum_{i=1}^{8} \left| p_{i+1} - p_i \right| = 2 \tag{20}$$

The pixel p is identified as bifurcation point if:

$$X_R(p) = \sum_{i=1}^{8} \left| p_{i+1} - p_i \right| = 6 \tag{21}$$

4.3 Cancelable Template Generation

Non-invertible transforms are used to preserve the privacy of biometric templates. The transform produces a cancelable template that does not match the original and the original cannot be reconstructed from the cancelable template. If the stored template is compromised, a new cancelable template is generated by changing distortion characteristics of the non-invertible transform. The transformation applied to a fingerprint template is invertible if the post-transformation minutiae positions after are highly correlated to minutiae positions before transformation [21]. According to the aforementioned statement, the goal of the transform is to eliminate minutiae correlation to the maximum possible extent. Additionally, tolerance to brute force attacks is required.

Let (x_i, y_i), i=1, ... n denote the coordinates of minutiae i for n identified minutiae points. The two-dimensional vector of extracted minutiae points is given by:

$$F = \{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\} \tag{22}$$

The non-invertibility of proposed transformation comes from cell shuffling. The coordinate system is divided into N_x x N_y cells, each containing n_{xy} minutiae points. Cells are shuffled as follows: circular shift right is performed to each cell according to the number of minutiae in that cell. Once horizontal shifting is finished, circular shift down is performed in the same manner. More than one cell can be mapped into the same cell after the transformation, as shifting depends on the number of points in the cell and no key is employed as a transformation matrix. The transform is non-invertible at this point, as is impossible to determine the original cell of the minutiae. This transform also satisfies the condition of local smoothness. The strength of the transform depends on the number of cells: an adversary performing brute force attack would have to try $(N_x N_y)^{NxNy}$ possibilities. For example, brute force attack against 4x4 cells shifting transform would require 18.5 x 10^{18} attempts, and against 4x5 cells transform 1.05 x 10^{26} attempts.

Let (x^T_i, y^T_i), i=1, ... n denote the coordinates of minutiae i after cell shuffling. Generated cancelable template is given by:

$$F^T = \{(x^T_1, y^T_1), (x^T_2, y^T_2), ..., (x^T_n, y^T_n)\}. \tag{23}$$

Templates are matched in the operating phase by discarding missing points, calculating the sum of the squared differences between two vectors, normalized by the number of remaining non-discarded values, and comparing the matching score with a threshold.

4.4 Experimental Evaluation

The implementation of the proposed framework is experimentally evaluated using MATLAB (version R2011b). As this research does not deal with acquisition hardware, images from CASIA-IrisV4 and CASIA-FingerprintV5 [40], collected by the Chinese Academy of Sciences' Institute of Automation, are used as inputs. It should be noted that different implementation of the proposed framework (different employed modalities, algorithms or parameters) will result in different error rates, key generation template entropy and cancelable template security.

The iris image subset used in our experiments consists of 500 samples from 50 subjects. Each iris image is normalized into an 8-bit 240x20 pixel image, and a 1-D log-Gabor filter with σ=0.5 and 12 pixel center wavelength is subsequently applied, resulting in a 9600 bit template. These parameters were found to provide high local entropy and optimum encoding on CASIA database [41]. Fingerprint image subset used in our experiments also consists of 500 samples from 50 subjects, with a resolution of 328x356 pixels. The optimal number of cells used in the non-invertible transform is selected as a compromise between the template security to brute force attacks and Equal Error Rate (EER), as presented in Fig. 5.

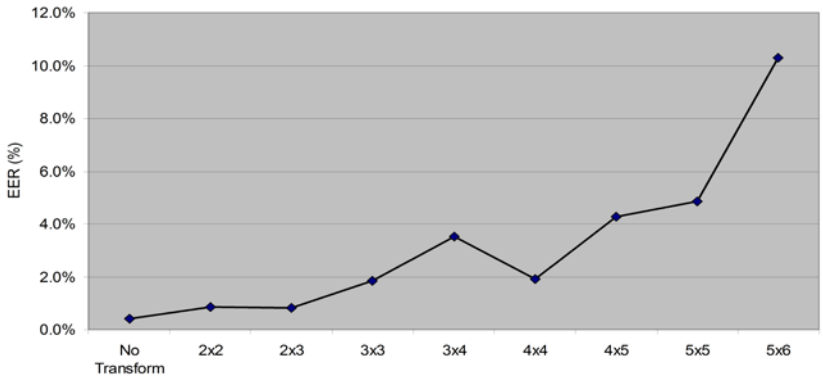

Figure 5
Determining optimal number of cells used in non-invertible transform

According to Figure 5, the optimal number of cells used in non-invertible transform is 4x4, resulting in less than 2% EER (1 reject in 50 authentication attempts) and the sufficient level of biometric template security. Five look-up tables are initially generated for different key lengths, each containing 50 rows of key hashes, correction codes from the Reed-Solomon algorithm output and cancelable templates generated from one fingerprint image for each subject. System was further tested as follows: FAR and FRR rates for different key sizes, without hash verification, are given in Table 1 and the overall system-wide performance is given in Table 2. Tolerance to brute force attacks takes into

account the fact that an adversary knows the length of the key. Otherwise, they would have to seek hash collision, which would make an attack even more complicated if the hash produces digest larger than the key.

Table 1
Average FAR and FRR for different key lengths (key generation without hash verification)

Key length	FAR (%)	FRR (%)
128	0.04%	0.31%
160	< 0.01%	1.29%
192	0%	4.01%
224	0%	11.52%
256	0%	14.83%

Table 2
System-wide performance for different key lengths and optimal number of cells (4x4)

Key length	Hash	Security (brute force)	FAR (%)	FRR (%)
128	RIPEMD-160	6.29×10^{57}	0%	2.62%
160		2.70×10^{67}		3.83%
192	SHA-224	1.61×10^{77}		6.75%
224		4.99×10^{86}		13.41%
256	SHA-256	2.14×10^{96}		15.97%

Conclusions

Although lower error rates, generated by other systems, are reported in the literature, no system that generates a 100% stable cryptographic key with a 0% false acceptance rate is reported, to the best of our knowledge. According to the experimental evaluation of the proposed implementation, that employs iris and fingerprint biometrics, as well as conventional key generation and authentication methods, the system will falsely identify one out of 38 users as an impostor while generating a 128 bit key and one out of 6 users while generating a 256 bit key. Although these error rates might not be suitable while attempting to generate the key that will, for example, open the classroom or office door, they are more than acceptable in critical environments where false acceptance may result in severe consequences, while the legitimate users are allowed to retry. Furthermore, the system protects stored identities with cancelable biometrics and is resistant to all attack types, with the exception of indiscriminate availability violations, as it is discussed in section 3.1. If the system generates a 128-bit key, an adversary trying to perform a brute force attack would have to try 6.29×10^{57} possibilities, while for the 256-bit key the number of possibilities increase to 2.14×10^{96}.

To conclude, the main contribution of the proposed framework is stable generated key, robustness, biometric template privacy and 0% false acceptance rate.

Our further research in biometric cryptosystems will be focused on the implementation of the iris-face key generation system according to the framework presented in this paper and the reduction of false rejection rates.

References

[1] A. K. Jain, A. Ross: Introduction to Biometrics. In "Handbook of Biometrics", A. Jain et al. (Eds), Springer, 2008

[2] Y. C. Feng, P. C. Yuen, A. K. Jain: A Hybrid Approach for Face Template Protection. In Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, Vol. 6944, pp. 325, 2008

[3] P. Balakumar, R. Venkatesan: A Survey on Biometrics-based Cryptographic Key Generation Schemes. International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85, 2012

[4] A. K. Jain, A. Ross, S. Prabhakar: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, pp. 4-20, 2004

[5] B. Biggio: Adversarial Pattern Classification. Doctoral dissertation, University of Cagliari, Cagliari, Italy, 2010

[6] A. Jagadeesan, K. Duraiswamy: Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. International Journal of Computer Science and Information Security, Vol. 7, No. 2, pp. 28-37, 2010

[7] L. Hong, A. K. Jain, S. Pankanti: Can Multibiometrics Improve Performance? In Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, pp. 59-64, NJ, USA, 1999

[8] A. K. Jain, A. Ross: Multi-Biometric Systems: Special Issue on Multimodal Interfaces that Flex, Adapt, and Persist. Communications of the ACM, Vol. 47, No. 1, pp. 34-40, 2004

[9] A. K. Jain, K. Nandakumar, A. Nagar: Biometric Template Security. EURASIP J. Adv. Signal Process, 2008:1-17, 2008

[10] J. Galbally, C. McCool, J. Fierrez, S. Marcel, J. Ortega-Garcia. On the Vulnerability of Face Verification Systems to Hill-Climbing Attacks. Pattern Recogn., 43(3) pp. 1027-1038, 2010

[11] S. Prabhakar, A. Jain: Decision-Level Fusion in Fingerprint Verification. Pattern Recognition, Vol. 35, pp. 861-874, 2002

[12] Z. Wang, E. Wang, S. Wang, Q. Ding: Multimodal Biometric System Using Face-Iris Fusion Feature. Journal of Computers, Vol. 6, No. 5, pp. 931-938, 2011

[13] K. Toh, J. Kim, S. Lee: Biometric Scores Fusion Based on Total Error Rate Minimization. Pattern Recognition, Vol. 41, pp. 1066-1082, 2008

[14] A. Ross, R. Govindarajan: Feature Level Fusion in Biometric Systems. In proceedings of Biometric Consortium Conference, September 2004

[15] G. I. Davida, Y. Frankel, B. J. Matt: On Enabling Secure Applications through Off-Line Biometric Identification. In Proceedings of the IEEE Symposium on Privacy and Security, pp. 148-157, 1998

[16] Y. J. Chang, W. Zhang, T. Chen: Biometrics-based Cryptographic Key Generation. In Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on (Vol. 3, pp. 2203-2206) IEEE

[17] A. Juels, M. Sudan: A fuzzy vault scheme. In Proc. IEEE Int. Symp. Information Theory, IEEE Press, p. 408, 2002

[18] Y. Dodis, L. Reyzin, A. Smith: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In Proceedings of the Eurocrypt 2004, pp. 523-540, 2004

[19] P. Tuyls, A. Akkermans, T. Kevenaar, G-J. Schrijen, A. M. Bazen, R. Veldhuis: Practical Biometric Authentication with Template Protection. In Proc. of 5th Int. Conference on Audio- and Video-based Person Authentication (AVBPA) pp. 20-22, 2005

[20] K. H. Solanki, C. Patel: Biometric Key Generation in Digital Signature of Asymmetric Key Cryptographic To Enhance Security Of Digital Data. In International Journal of Engineering Research and Technology, Vol. 2, No. 2, 2013. ESRSA Publications

[21] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle: Generating Cancelable Fingerprint Templates. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(4), pp. 561-572, 2007

[22] R. Ang, R. Safavi-Naini, L. McAven:. Cancelable Key-based Fingerprint Templates. In C. Boyd & J. Gonzalez Nieto (Eds.), Australasian Conference on Information Security and Privacy, pp. 242-252, 2005

[23] F. Hao, R. Anderson, J. Daugman: Combining Crypto with Biometrics Effectively. IEEE Transactions on Computers, Vol. 55, pp. 1081-1088, 2006

[24] K. Bae, S. Noh, J. Kim: Iris Feature Extraction using Independent Component Analysis, 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, pp. 838-844, 2003

[25] L. Wu, X. Liu, S. Yuan, P. Xiao: A Novel Key Generation Cryptosystem based on Face Features. In Signal Processing (ICSP) 2010 IEEE 10th International Conference on, pp. 1675-1678. IEEE

[26] R. Sashank Singhvi, S. P. Venkatachalam, P. M. Kannan, V. Palanisamy: Cryptography Key Generation using Biometrics. International Conference on Control, Automation, Communication and Energy Conservation (INCACEC), pp. 1-6, 2009

[27] J. Ban, M. Féder, M. Oravec, J. Pavlovičová: Non-Conventional Approaches to Feature Extraction for Face Recognition. Acta Polytechnica Hungarica, Vol. 8, No. 4, pp. 75-90, 2011

[28] P. Balakumar, R. Venkatesan: Combining Biometric Features of Iris and Retina for Better Security Cryptography. Digital Image Processing, 3(16), 1083-1089, 2011

[29] A. S. Gokulakumar, C. Venkataraghavan., S. Kavya Priya, T. Suganya: Encryption of Cryptographic Key Technique by Crossover of Iris and Face Biometric Key. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Special Issue 1, pp. 354-362, 2014

[30] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, J. D. Tygar: Can Machine Learning be Secure? In Proc. of the 2006 ACM Symposium on Information, computer and communications security (pp. 16-25) ACM, 2006

[31] G. Amoli, N. Thapliyal, N. Sethi: Iris Preprocessing. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 6, pp. 301-304, 2012

[32] D. J. Kerbyson, T. J. Atherton: Circle Detection using Hough Transform Filters, Fifth International Conference on Image Processing and its Applications, Edinburgh, UK, 04 – 06 July 1995, pp. 370-374

[33] R. P. Wildes: Iris Recognition: an Emerging Biometric Technology. Proceedings of the IEEE, 85(9) pp. 1348-1363, 1997

[34] J. Daugman: How iris recognition works. Circuits and Systems for Video Technology, IEEE Transactions on, 14(1) pp. 21-30, 2004

[35] D. J. Field: Relations between the Statistics of Natural Images and the Response Properties of Cortical Cells. Journal of the Optical Society of America, Vol. 4, No. 12, 1987

[36] H. Furuya, S. Eda, T. Shimamura: Image Restoration via Wiener filtering in the Frequency Domain. WSEAS transactions on signal processing, 5(2), pp. 63-73, 2009

[37] Y. Wang, J. Hu, F. 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, 2007

[38] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar: Handbook of Fingerprint Recognition, Springer-Verlag, 2003

[39] L. Lam, S. W. Lee, C. Y. Suen: Thinning Methodologies - a Comprehensive Survey. IEEE Transactions on pattern analysis and machine intelligence, 14(9), pp. 869-885, 1992

[40] Biometrics Ideal Test, http://biometrics.idealtest.org

[41] S. Adamović, M. Milosavljević: Information Analysis of Iris Biometrics for the Needs of Cryptology Key Extraction. Serbian Journal of Electrical Engineering, Vol. 10, No. 1, pp. 1-12, 2003