# Multi-Factor Authentication Using Fingerprints and User-Specific Random Projection

Esla Timothy Anzaku, Hosik Sohn, Yong Man Ro

Image and Video Systems Lab, Korea Advanced Institute of Science and Technology (KAIST)
Yuseong-gu, Daejeon, 305-732, South Korea

slaco@kaist.ac.kr
sohnhosik@kaist.ac.k
ymro@ee.kaist.ac.kr

*Abstract*— **Alarming increase in identity theft cases calls for the use of secure authentication systems that can clearly distinguish between authorized users and unauthorized users who are in possession of valid security tokens or passwords. To this end, we propose a multi-factor authentication system using user-specific pseudo-random numbers and fingerprints to generate revocable and privacy preserving biometric templates, which in turn are used for authentication. We evaluated the performance of the proposed system on the publicly available Fingerprint Verification Competition (FVC) 2000 database using Receiver Operating Characteristic (ROC) curves. Experimental results show that Equal Error Rates (EER) less than 0.4% can be achieved.**

## I. INTRODUCTION

Authentication, which is a process of verifying if the user or identity is who they claim to be, can be based on the following factors: possession factor – something the user has, such as Identity cards and security token; knowledge factor, such as passwords and Personal Identification Numbers (PIN); biometrics, such as face, fingerprint and iris. Usually, multi-factor authentication, which requires the combination of two or more of the authentication factors, is required. For instance, using a smartcard and a PIN for authentication at an automated teller machine is an example of a multi-factor authentication

One major disadvantage of authentication systems that rely only on possession or knowledge or both factors is their inability to distinguish between authorized users and unauthorized users who are in possession of valid tokens and passwords. Biometric systems can solve this problem. Biometrics is a technology that uniquely identifies individuals based on their physiological or behavioural traits [1]. Authentication systems based on biometrics are increasingly been deployed, however, there are increasing concerns about the security and privacy of these systems.

Several research efforts are being channelled at designing authentication systems that combine possession factors, such as a cryptographic key, with biometrics. Soutar et al. [2] presented a method which binds cryptographic keys with users' fingerprint images during enrolment. The keys are released on successful verification. An approach that combines the legitimate user's typing patterns with the user's password to generate a hardened password was proposed by Monrose et al [3]. Juels et al. [4] proposed the fuzzy commitment scheme, where a codeword of an error correcting code is combined with the biometric template using bitwise XOR. The biometric is supposed to be an ordered set.

A method similar to fuzzy commitment scheme, the fuzzy vault, which is compatible with unordered sets, was proposed by Juels et al. [5]. Clancy et al. [6] used the fuzzy vault to build and analyse a secure authentication scheme using fingerprints and smartcards. They showed that it is difficult to ensure the security envisioned in [5]. In another approach, Teoh et al. [7] used biohashing method and claimed zero EER. It was, however, shown in [8] that the claim of zero EER of the biohashing method was based on the assumptions that the hash keys are not compromised. It was further shown in [8] that under a more realistic scenario, when hash keys are compromised, the performance of the biohashing method can be worse than that of systems using only biometrics.

In this paper, we propose an authentication system that combines user-specific pseudo-random numbers (PRN) and fingerprints to effectively authenticate individuals. The motivation for this work stems from the observation on the deficiencies of previous works with fingerprints which fall into one of these categories: they provide only theoretical framework with no clear implementation with real fingerprint-biometrics; yield unacceptable performance or the design does not allow for the provision of revocability.

The proposed authentication system uses the concept of random projection [9] and fixed length fingerprint feature extraction [10] to generate revocable and privacy preserving templates that yield high authentication accuracy. This feature vector is known as fingercode. The fingercode extraction in [9] is a texture-based fingerprint feature extraction method that captures both the local and global ridge characteristic present in the fingerprint. To the best of our knowledge, there has been no published work that proposed a multi-factor authentication system based on fingercodes; most of the approaches are based on minutiae features. Our proposed multi-factor system based on fingercode extraction is very efficient and achieves high accuracy as is shown in section III.

The following is the outline of this paper. The proposed multi-factor authentication system is presented in section II. In section III, the experiments carried out were presented. Finally, conclusions were drawn in section IV.

978-0-7695-4012-2/10 $26.00 © 2010 IEEE
DOI 10.1109/APWeb.2010.44

## II. PROPOSED AUTHENTICATION SYSTEM

The proposed multi-factor authentication system (see Fig. 1) comprises of two phases: the enrolment and verification phases. In the enrolment phase, the two inputs required are the fingerprint and the secret key (user-specific PRN). The PRN is used to generate a user-specific random matrix $\boldsymbol{R} \in \mathbb{R}^{m \times n}$, and it can be stored in a smartcard. A fixed length vector $\boldsymbol{x} \in \mathbb{R}^n$ is extracted from the fingerprint and subsequently projected onto a random subspace using the user-specific $\boldsymbol{R}$, to generate a revocable and privacy preserving biometric template $\boldsymbol{t} \in \mathbb{R}^n$, which is then stored in template database. Random projection is a tool for dimensionality reduction. It can also be used to generate revocable and privacy preserving biometric templates.

In the verification phase, the user claims an identity and inputs a fingerprint and a PRN. Then, the same procedures for template generation carried out in the enrolment phase are used to generate a template $\boldsymbol{t}' \in \mathbb{R}^n$. The similarity between $\boldsymbol{t}$ and $\boldsymbol{t}'$ is computed. The Euclidean distance between two vectors was used. The users are verified to be who they claim to be if the Euclidean distance between their query and enrolled templates are lower than a predetermined threshold.

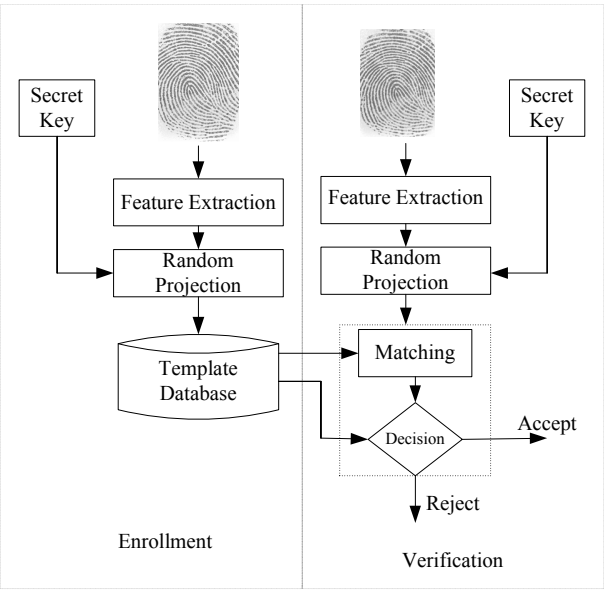


Fig. 1 Proposed multi-factor authentication system.

### A. Fingerprint Feature Extraction

The fingerprint feature extraction is based on the method proposed by Anil el al. [10] which, unlike minutiae based methods, utilizes both the global and local ridge characteristics to generate fixed length code known as fingercode. The following are the main steps involved in the originally proposed fingercode extraction with little modifications; we included fingerprint enhancement and used an improved reference point detection algorithm:

- Enhancement of the fingerprint image [11] to improve its quality. This increases the accuracy of the next step – reference point location;
- Location of a reference (core) point in the fingerprint based on the method of complex filtering that was proposed in [12].
- Tessellating an ROI around the reference point. The ROI comprises of series of *B* concentric bands, with each band subdivided into *k* sectors. The width and number of the bands are chosen according to the size of the fingerprint images. For this work, *B = 2* and *k = 6*. The innermost band with a radius of 10 pixels was excluded because it contains only a small number of pixels;
- Normalization of the ROI in each sector to a constant mean and variance value, to remove effects of sensor noise and gray level deformation due to finger pressure differences;
- Filtering of the ROI using eight even symmetric real-valued Gabor filters; thereby, obtaining eight filtered images $F_\theta$. The eight different values of $\theta$ used are $0^o$, $22.5^o$, $67.5^o$, $90^o$, $112.5^o$, $135^o$, $157^o$. These eight directional-sensitive filters are used to capture both the global and local ridge characteristics that are present in the fingerprint with the ROI. In the spatial domain, an even symmetric real-valued Gabor filter has the following characteristics:

$$G(x, y, f, \theta) = \exp\left\{-\frac{1}{2}\left[\frac{x'^2}{\delta_x^2} + \frac{y'^2}{\delta_y^2}\right]\right\}\cos\left(2\pi f x'\right) \quad (1)$$

$$x' = x\sin\theta + y\cos\theta \quad (2)$$

$$y' = x\cos\theta - y\sin\theta \quad (3)$$

where $f$ is the frequency of the sinusoidal plane wave along the direction $\theta$ from the x-axis, and $\delta_x$ and $\delta_y$ specify the Gaussian envelop along x and y axes, repectively. In our work, $f = 1/10$ and $\delta_x = \delta_y = 4$;

- Generation of the fixed length feature vector from the eight filtered images $F_\theta$. The length of the feature vector is 96 (*B x k x 6*). The components of the feature vector are formed from the average absolute deviation of each sector in each of the eight $F_\theta$. Let $F_{i\theta}(x, y)$ be the $\theta$ - directional filtered image for sector $S_i$. Each component of the feature vector is computed as

$$V_{i\theta} = \frac{1}{n_i}\left(F_{i\theta}(x, y) - P_{i\theta}\right) \quad (4)$$

where $i \in \{0,1,.....,11\}$, $n_i$ is the number of pixels in $S_i$, $P_{i\theta}$ is the mean of the pixel values in $S_i$, $\theta \in \{0^o, 22.5^o, 67.5^o, 90^o, 112.5^o, 135^o, 157^o\}$.

### B. Random Projection

Random projection is essentially a dimensionality reduction tool. It originates from the Johnson-Lindenstrauss Lemma, which is stated as follows:

For any $0 < \varepsilon < 1$ and any interger s, let m be a positive interger such that $m \geq \frac{4\ln(s)}{\varepsilon^2/2 - \varepsilon^3/3}$. Then for any set S of s =|S| data point in $\mathbb{R}^n$, there exists a linear mapping $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ such that all $u, v \in S$,

$$(1-\varepsilon)\|\boldsymbol{u}-\boldsymbol{v}\|^2 \leq \|f(\boldsymbol{u})-f(\boldsymbol{v})\|^2 \leq (1+\varepsilon)\|\boldsymbol{u}-\boldsymbol{v}\|^2,$$

where $\|\cdot\|$ denotes the vector 2-norm.

According to this Lemma, any set of points in $\mathbb{R}^n$, which in our case is the set of extracted feature vectors, with a defined metric (the Euclidean distance), can be embedded into $\mathbb{R}^m$, with distortion not greater than $\varepsilon$ using a randomly generated linear mapping. Refer to [8] for the proof of Johnson -Lindenstrauss Lemma.

Random projection involves the projection of a vector $\boldsymbol{x} \in \mathbb{R}^n$ onto a random subspace using the random matrix $\boldsymbol{R} \in \mathbb{R}^{m \times n}$. This is simply the multiplication of $\boldsymbol{x}$ by the random matrix $\boldsymbol{R}$. That is $\boldsymbol{t} = \boldsymbol{R}\boldsymbol{x}$. Each component of $\boldsymbol{R}$ is independent and identically distributed (i.i.d) according to the Gaussian distribution with zero mean and unit variance. In our case, random projection was not used for dimensionality reduction ($m = n$). It was used for binding the user-specific PRN to the fingerprint data; we refer to this as user-specific random projection. The extracted feature vectors are projected to different random spaces based on the random matrices generated with the PRN for each user. User-specific random projection has the property of preserving the Euclidean distance of feature vectors from the fingerprint samples of the same user, while increasing the distance between fingerprints of two different users [12].

### C. Matching

Matching the query and enrolled templates is based on the Euclidean distance between them. To effectively match two fingercodes, the translation and rotation of the fingerprints need to be accounted for.

By using a reference point, the fingercode is translation invariant but not rotation invariant. During matching, five templates are generated and are projected onto the user-specific random subspace. The generation of the template is aimed at compensating the rotation of fingerprint images, and it is achieved by the cyclic rotation of the fingercode of the query fingerprint as follows:

$$V_{i\theta}{}^{R} = V_{i'\theta'} \tag{5}$$

$$i' = (i + k + R) \bmod k + (i \operatorname{div} k) \times k \tag{6}$$

$$\theta' = \left(\theta + 180 + 11.25^{o} \times R\right) \bmod 180 \tag{7}$$

where k is the number of sectors in a band, $i \in \{0,1,.....,11\}$, $\theta \in$ {0°, 22.5°, 67.5°, 90°, 112.5°, 135°, 157°}, and $R \in \{22.5^{o}, 11.25^{o}, 0, -11.25^{o}, 22.5^{o}\}$.

The cyclic rotation is equivalent to rotating the input fingerprint by five different angles R, and then computing their respective fingercodes. Among the five templates, the one closest to the claimed enrolled template in terms of the Euclidean distance, is considered as the best aligned; the other four are discarded. The user's claim is verified if the Euclidean distance is less than a predefined threshold that is stored in the template database. This approach, unlike the approach for template matching in [10] that used ten templates for each enrolled user, requires the storage of only one template in the database for each user; thereby, reducing the amount of storage needed for storing the enrolled templates.

### D. Security and privacy

Consider the following equation $\boldsymbol{t} = \boldsymbol{R}\boldsymbol{x}$, $\boldsymbol{R} \in \mathbb{R}^{m \times n}$, $\boldsymbol{x} \in \mathbb{R}^n$.

Since $m = n$ in our work, when the PRN and the templates are compromised, the feature vector can be computed, but the privacy preserving property of the proposed system comes from the nature of fingercode extraction. The components of the fingercode are formed from the average absolute deviation of each sector in each of the eight filtered images; therefore, it is almost impossible to reconstruct the original fingerprint from the fingercode. Revocability comes from using a different random matrix to generate a new template when the PRN and template are compromised.

## III. EXPERIMENTS

The experiments were carried out on the FVC 2000 database, specifically, on the sets labelled Db1a and Db4a. Each of these sets comprise of the fingerprints of 100 persons with 8 samples per person. The fingerprint images in Db1a (300x300 pixels) were captured using a low cost optical sensor, while those in Db4a (240x320) were synthetically generated. All fingerprint images were used for the experiments. The extraction of the feature vectors and the matching of any two templates were carried out as explained in section II.

Receiver Operating Characteristic (ROC) curves that plot Genuine Acceptance Rates (GAR) against the False Acceptance Rates (FAR) was used to evaluate the performance of the proposed system. Each template was match with all the other templates in the database. The probability of accepting match scores of any two templates of the same person to be a true match is the GAR, while FAR is the probability of accepting match scores of any two templates of two different persons to be a true match. These where computed for different threshold values.

Fig. 2 shows the ROC curves for Db1a and Db4a. The curves labelled 'only biometrics' represents the ROC when only biometric traits are used. This curves were plotted to show the performance of the system in a worst case scenario when the PRNs are compromised. In this case the performance of the system reverts back to that of the original

biometrics. It can be seen from Fig. 2 that the proposed system achieved about 99% GAR at zero FAR for the database used. The relatively poorer performance using only biometrics is due to the downsides of the fingercode extraction algorithm. These downsides includes: location of the reference points very close to the edge of the fingerprint; error in reference point detection due to the very poor quality of some fingerprints, and the inability of the proposed template matching to handle the rotation of certain fingerprints. This, however, has little effects on the proposed algorithm is reflected in Fig. 2.

Table 1 shows the computed EERs for the Db1a and Db4a. EER is the rate at which False Rejection Rate (FFR) equals FAR; FRR = 1-GAR. Low EERs were obtained as expected. To improve the security of the system to cater for the worst case, when PRNs are compromised, it is recommended that threshold values at very low FAR be used. At this threshold, most of the attempts made by imposters with stolen PRNs will be denied, and since, the genuine users are in the possession of the valid PRN, the system will accept their claims. By doing so, the overall performance of the system can be improved.

TABLE 1
EER FOR Db1a and Db4a

| DATABASE | Db1a | Db4A |
|---|---|---|
| EER (ONLY BIOMETRICS) | 21.38 | 12.48 |
| EER (PROPOSED) % | 0.38 | 0.31 |

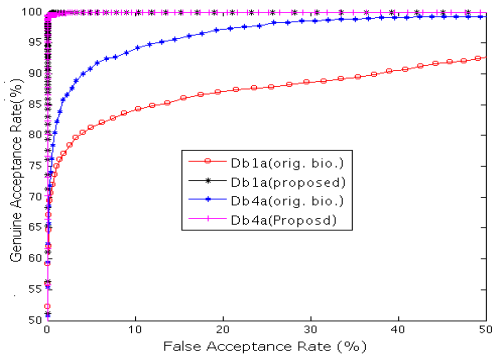

Fig. 2. Receiver Operating (ROC) Characteristic curves for Db_1a and Db_4a.

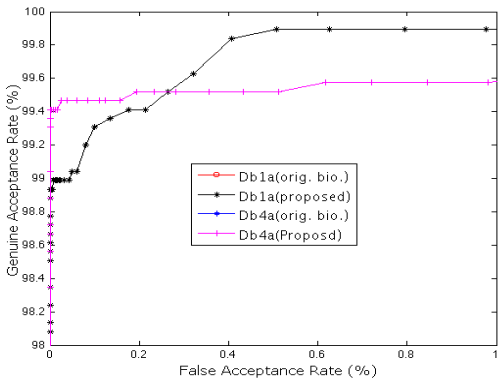

Fig. 3. A magnified portion of Fig. 1 highlighting GAR at 0 FAR.

## IV. CONCLUSIONS

We proposed a multi-factor authentication system that uses user-specific PRNs and fingerprints to generate revocable and privacy preserving templates. Results showed that the proposed system can achieve very low EER when the PRNs are not compromised. We also suggest using threshold values that yield very low FAR to improve the performance of the system in the worst case scenario, when the PRNs are compromised. For future work, we will investigate more efficient methods for fingercode matching and do a more thorough analysis of the worst case scenario.

## REFERENCES


[1] A. K. Jain, A. Russ, and Salil Prabhakar, An Introduction to Biometric Recognition, IEEE Trans. Circuit and Systems for Video Technology, vol. 14, no. 1, January, 2004.

[2] C. Soutar, D. Roberge, A. Stoinav, A. Gilroy, and B. V. K. Kumar, *Biometric Encryption using image processing*, SPIE, volume 3314, pages 174-188, 1999.

[3] F. Monrose, M. K. Reiter, and S. Wetsel. *Password Hardening Based on Keystroke Dynamics*, in Proc. Conference on Computer and Communications Security, 1999.

[4] A. Juels and M. Wattenberg, *A Fuzzy Commitment Scheme*, in Proc. Sixth ACM Conference on Computer and Communications Security, pages 28-36, ACM Press, 1999.

[5] A. Juels and M. Sudan, *A Fuzzy Vault Scheme*, in Proc. Conference on Computer and Communications Security, 2002.

[6] T.C. Clancy, N. Kiyavash, and D. J. Lin, *Secure Smartcard Fingerprint Authentication*, in Proc. ACM SIGMM, Multimedia, Biometrics Methods and Applications Workshop, 2003.

[7] A. B. J Teoh, D. C. L. Ngo, and A. Goh, *Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number*, Pattern Recognition, vol. 37, no. 11, pages 2245 - 2255, November, 2004.

[8] A. Kong, K. H. Cheung, D. Zhang, M. Kamel, J. You, *Analysis of Biohashing and its Variants*, Pattern Recognition, vol. 39, no. 7, pages 1352-1368, 2006.

[9] R. I. Arriaga and S. Vempala, *An Algorithmic Theory of Learning Robust Concepts and Random Projection,* in Proc. 40th Annual Symposium on Foundations of Computer Science, pages 616-623, IEEE Computer Society Press, 1999.

[10] A. K. Jain, L. Hong, and S. Pankanti, *Filterbank-Based Fingerprint Matching,* IEEE Trans. Image Processing, vol. 9, no. 5, pages 848-859, 2000.

[11] S. Chikkerur, C. Wu, V. Govindaraju, *A Systematic Approach for Feature Extraction in Fingerprint Images*, in Proc. ICBA, pages 344 – 350, December, 2004.

[12] K. Nilson, J. Bigun, *Localization of Corresponding Points in Fingerprints by Complex Filtering*, Pattern Recognition letter, vol. 24, pages 2135 – 2144, 2003.

[13] A. B. Teoh, C. T. Young, *Cancelable Biometrics Realization with Multispace Random Projections*, IEEE Trans. Syst., vol. 37, no. 5, pages 1096 – 1106, 2007.