PALM-VEIN AND FINGERPRINT BASED IMPROVED MULTIMODAL FUZZY VAULT SCHEME

Sergey Chidemyan

***Abstract**: Multi-biometric systems are kind of systems, where multiple templates from different biometric sources for the same user are stored. The authentication based on biometrics is a very good mechanism; however, such authentication technology needs large storage of biometric data, which should be protected. Fuzzy Vault is one of the most popular biometric encryption schemes, which aims to encode users' critical information in such a way that only the legitimate users are able to access it. In this paper, multimodal biometric template protection scheme is combined with biometrics, which results a high security. In particular, the approach of feature-level fusion for obtaining single multi-biometric template is described and construction of fuzzy vault scheme for the palm veins and fingerprints is presented. The proposed fuzzy vault scheme has been implemented and tested on the publicly available databases.*

***Keywords**: Palm Vein, Fingerprints, Fuzzy Vault, Template Protection, Multi-biometric systems*

***ACM Classification Keywords**: D.4.6 Security and Protection (K.6.5)*

Introduction

Often there are situations when we need to protect some critical information called key. People cannot remember cryptographically secure keys, so it is a good idea to use physiological features of a person (e.g. fingerprints, palm prints, palm veins, etc.) to provide an access to this kind of information. The authentication based on biometrics is a very good mechanism; however, such authentication technology needs large storage of biometric data, which appears to be the drawback, and also there is a risk of private data leakage and identity theft. It is a big issue, because biometric characteristics are inherent to a person and once lost, they would never be refreshed.

One of the most potentially harmful attacks on a multi-biometric system is against the biometric templates [Brindha & Natarajan, 2012].

In this work we consider multi-biometric systems, the kind of systems, where multiple templates from different biometric sources for the same user are stored. Since in multi-biometric systems multiple templates for the same user corresponding to the different biometric sources are stored template security is even more critical here.

Biometric template protection schemes that are combining cryptography with biometrics are considered to be a promising solution to issues above. Many famous biometric template protection schemes have been proposed such as fuzzy commitment scheme [Juels & Wattenberg, 1999], fuzzy vault scheme [Juels & Sudan, 2002] and fuzzy extractor [Dodis et al, 2008]. Among them the fuzzy vault scheme proposed by Juels and Sudan [Juels & Sudan, 2002] has become one of the most popular key-binding approaches, because it provides high security for biometric template protection. The scheme introduced by A. Juels and M. Wattenberg [Juels & Wattenberg, 1999] is not order invariant, which is the weakest point of the algorithm described in [Juels & Wattenberg, 1999], because the data extracted from the biometric template is not in the same order for the most types of biometrics. In contrast, the fuzzy vault scheme has a property of order invariance.

Multi-biometric fuzzy vault provides better identification and higher security compared to a unibiometric fuzzy vault. The only disadvantage here that the storage of multiple templates for the same user is required; however multi-biometric systems are more secure compared to their single biometric counterparts.

In this paper the approach of feature-level fusion for obtaining single multi-biometric template is described and construction of multi-biometric fuzzy vault scheme for the palm veins and fingerprints is presented.

Fuzzy Vault Scheme

As it was mentioned above the fuzzy vault scheme provides an effective and high security for biometric template protection [Juels & Sudan, 2002] and has a property of order invariance. So it suits the best for our purpose. Let us briefly introduce that scheme.

Let $\mathcal{F}$ be a finite field of size n and biometric template of the user can be written as follows: $\mathrm{X} = (\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_\mathrm{s}),\ \mathrm{where}\ \forall \mathrm{i} = 1 \dots \mathrm{s}: \mathrm{x}_\mathrm{i} \in \mathcal{F}$. Let us denote the secret polynomial by *p(x)*. The degree of *p(x)* is k = s – t - 1, where t < s and coefficients of *p(x)*: $\mathrm{p}_\mathrm{j} \in \mathcal{F}$. Let $\mathrm{r} \in \{\mathrm{s}+1, \dots \mathrm{n}\}$

Locking algorithm

1. Having p(x) of degree k we evaluate it on the points of biometric. Let: $y_i = p(x_i)\ \forall i = 1 \dots s$.
2. Choose r – s distinct random points from $\mathcal{F} \setminus \mathrm{X}$ so called chaff points: $x_{s+1}, \dots\ x_r$.
3. Choose $y_i \in \mathcal{F}$ such that $\forall i = s+1 \dots r: y_i \neq p(x_i)$.
4. Construct vault: $V = \{(x_1, y_1)(x_2, y_2) \dots (x_r, y_r)\}$.

Unlocking algorithm

1. Let we have new biometric $X' = (x'_1, x'_2, \dots, x'_s),\ where\ \forall i = 1 \dots s: x'_i \in \mathcal{F}$

Having vault V, constructed by locking algorithm, the secret polynomial can be reconstructed if X′ has at least s – t common points with the original biometric X, using Lagrange interpolation.

Multi-biometric Fuzzy-Vault scheme construction

Let us briefly introduce the methods of feature extraction from palm-veins and fingerprints and construction of fuzzy vault scheme, based on these features.

✓ Extraction of biometric data from palm-veins

The vein pattern can be well represented by a number of critical points referred as minutiae points. The branching points and the ending points in the vein pattern skeleton image are the two types of critical points to be extracted. Ending points here are mainly ending points of vein skeleton curves that placed at the edge of region of interests (ROI) and resulted from the cropping of hand image while obtaining ROI. Although these ending points are not real ending points of vein on palm, they are taken because they contain geometrical information about the shape of the skeletons of the vein pattern. As for bifurcation points, they are the junction points of three curves. Figure 1 illustrates some of bifurcation and ending points on vein pattern's skeleton representation. Experiments on CASIA database [CASIA, 2015] show that we can extract on average 25 minutiae points from each vein pattern, including 10 bifurcation points and 15 ending points on average for each vein pattern. This quantity of minutiae points is quite enough for our purpose.

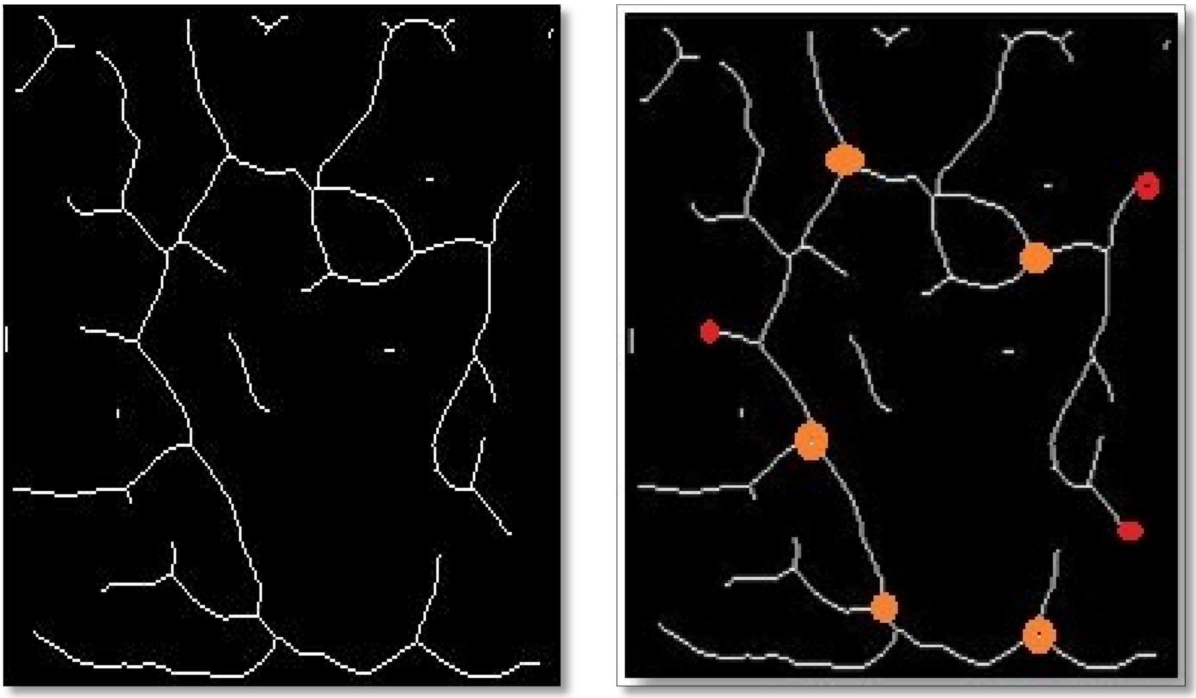

Figure 1. Some of bifurcation points and ending points are marked by red circle

✓ Extraction of biometric data from fingerprints

The most popular matching approach for fingerprint identification is usually based on lower-level features determined by singularities in finger ridge patterns called minutiae [Więcław, 2009]. In general, the two most prominent used features are ridge ending and ridge bifurcation (Figure 2). More complex fingerprint features can be expressed as a combination of these two basic features. Particularly, each detected minutiae m can be described by three parameters:

$$\mathrm{m} = (\mathrm{x}, \mathrm{y}, \theta), \tag{1}$$

where (x,y) are coordinates of minutiae point, θ is minutiae direction typically obtained from local ridge orientation (Figure 3).

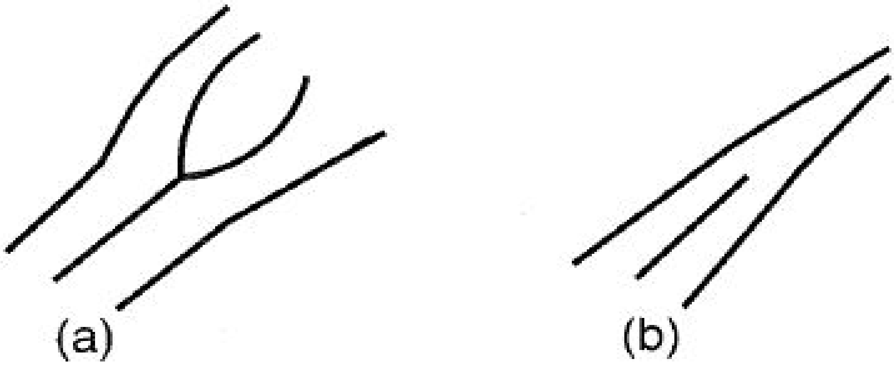

Figure 2. Features extracted from fingerprint: (a) ridge bifurcation; (b) ridge ending

The experiments show that we can extract on average 30 minutiae points from each imprint of fingerprint.

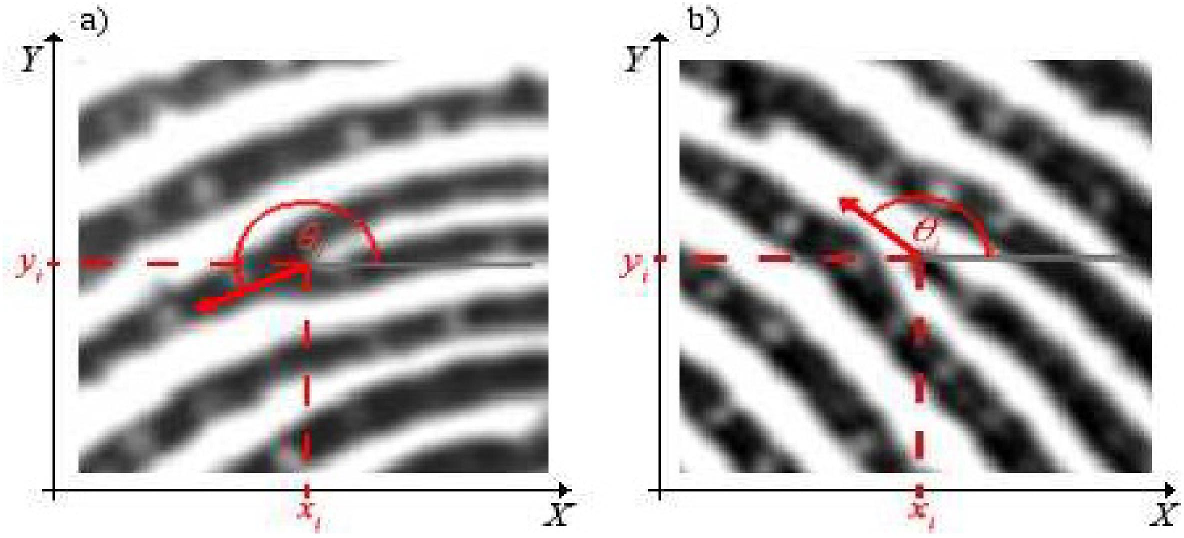

Figure3. θ component of minutiae feature for a) ridge bifurcation, b) ridge ending

✓ Implementation of fuzzy vault based on the extracted data

As it was mentioned above we consider multi-biometric systems, where multiple templates from different biometric sources for the same user are stored. We introduce the feature-level fusion for palm-veins and fingerprints to obtain a single multi-biometric template.

Let $\mathrm{X_F}$ and $\mathrm{X_{PV}}$ are sets of feature points extracted from fingerprints and palm-veins respectively. Here all elements $\mathrm{x_F^i} \in \mathrm{X_F}$ are in Galois fields GF (2^{16}). Note that 5 bits are taken from x coordinate, 5 bits from y coordinate and 6 bits from θ. The elements $\mathrm{x_{PV}^i} \in \mathrm{X_{PV}}$ are also in Galois fields GF (2^{16}). Here 8 bits are taken from coordinate x of palm-vein minutiae point and 8 bit from coordinate y. The union X, of the two sets $\mathrm{X_F}$ and $\mathrm{X_{PV}}$ is formed such that the Hamming distance between any two elements in the union is greater than or equal to 2 [Nandakumar, 2008].

Encoding

The biometric template X, discussed above, is constructed using 16 bits from minutiae points. In the current implementation, a randomly generated secret S is 224-bit random key, which is used for constructing the secret polynomial p(x).

For each degree of the polynomial n in range from 8 to 14 and the number of the minutiae points in X is s = 55, the chaff points were taken r-s = 550.

Decoding

Here, the user tries to unlock the vault V using the query minutiae. Assume we have s query minutiae (X') and $\mathrm{u'_1, u'_2, \dots,\ u'_s}$ are the points to be used in polynomial reconstruction. These points are found by comparing $\mathrm{u_i}$, i = 1, 2… s. with the values of the vault V, namely $v_1, v_2, \dots, v_r$. If any u_i is equal to $v_1, v_2, \dots, v_r$, the corresponding vault point is added to the list of points to be used. Assume that this list has m points, where m ≤ r. Now, for decoding a n-degree polynomial, n + 1 unique projections are necessary. We have to find all possible $\mathrm{C_m^{n+1}}$ combinations of n + 1 points, among the list with size m. For each of these combinations, we construct the Lagrange interpolating polynomial.

If the query minutiae list (X') overlaps with template minutiae list (X) in at least (n+1) points, for some combinations, the correct secret will be decoded. This indicates the desired outcome when query and template multi-biometric data are from the same user.

The results of the experiments

There are six imprints of the same palm-vein and one of them was used to enroll the user. The one imprint of fingerprint is also used to enroll the same user.

Let us check the probability that attacker can decode the secret using all possible combinations of points in our vault. In case we have a secret of a size 224 bit, 55 genuine minutiae points and 550 chaff points, the probability that a random combination of points decodes the secret is:

$$C_{55}^{15} \Big/ C_{605}^{15} \approx 2^{-55}$$

This gives approximately 55 bits of security.

Below the results of the system performance tests on virtual database, which generated from the palm-veins and fingerprints databases, are attached (Figure 4).

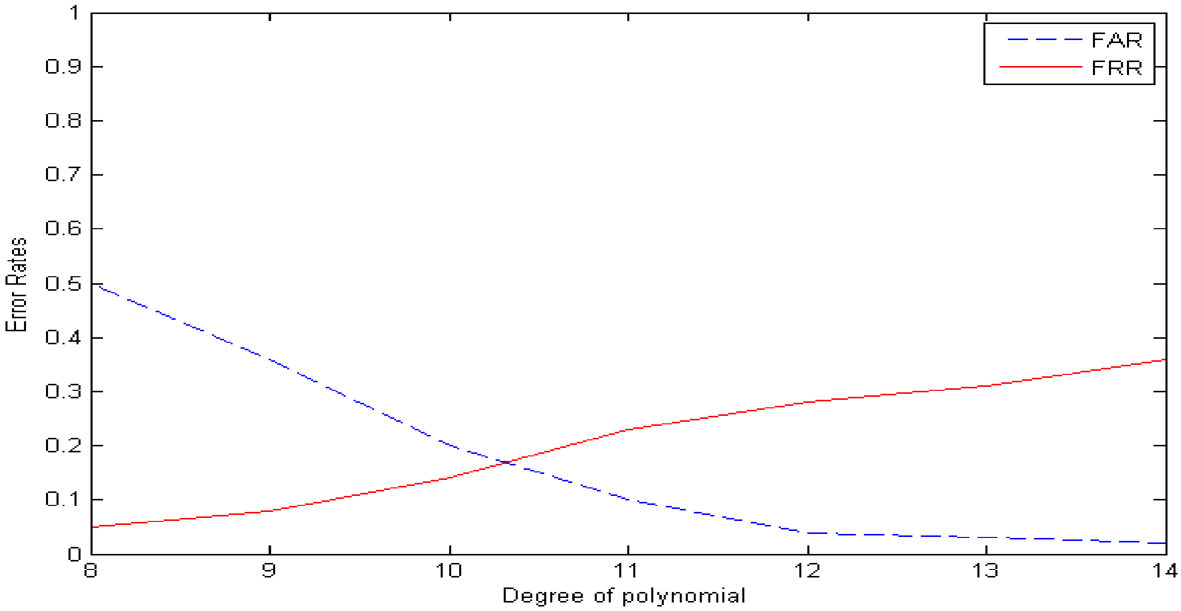

Figure 4. Error rate curves of palm-vein and fingerprint based multimodal fuzzy vault scheme

Conclusion

In this paper we have presented the results of actual implementation of the multimodal fuzzy vault using palm-vein and fingerprint biometric data. In particular, the fusion mechanism of palm-vein and fingerprint minutiae sets is proposed. Experiments show that there is 55 points on average after described feature-level fusion has been applied. This quantity of points is enough for 224-bit key generation and for the practical accuracy of the system (FAR < 0.01). In the last section proposed multi-biometric scheme is discussed in term of security bits and how it follows from experiments our scheme guarantees high security.

Bibliography

[Brindha & Natarajan, 2012] E. Brindha, A. M. Natarajan, “Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault”, Journal of Biometrics and Biostatistics, Vol.5, Issue 4, Aug 2012, pp. 1 - 6

[CASIA, 2015] CASIA MS Palmprint V1 Database, Available: http://biometrics.idealtest.org/dbDetailForUser.do?id=5.

[Dodis et al, 2008] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: how to generate strong keys from biometrics and other noisy data,” SIAM Journal on Computing, vol. 38, no. 1, 2008, pp. 97 – 139

[Juels & Sudan, 2002] A. Juels and M. Sudan, “A fuzzy vault scheme,” in Proceedings of the IEEE International Symposium on Information Theory, July 2002, 408 p.

[Juels & Wattenberg, 1999] A. Juels and M. Wattenberg, “Fuzzy commitment scheme,” in Proceedings of the 1999 6th ACM Conference on Computer and Communications Security (ACM CCS ’99), November 1999, pp. 28 – 36

[Nandakumar, 2008] K. Nandakumar, “Multibiometric Systems: Fusion Strategies and Template Security”, PhD thesis, Department of Computer Science and Engineering, Michigan State University, January 2008

[Więcław, 2009] Ł. Więcław, “A Minutiae-Based Matching Algorithms In Fingerprint Recognition systems”, Journal Of Medical Informatics & Technologies, Vol. 13, 2009, pp. 65 - 72

Authors' Information

***Sergey S. Chidemyan** – Russian – Armenian (Slavonic) University; e-mail: serchch@gmail.com*