ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր
Том 115 2015 № 1
Volume

INFORMATICS

УДК 519

S. S. Chidemyan[1], A. H. Jivanyan[2], academician G. H. Khachatryan[3], H. G. Khasikyan[4]

Palm-Vein Based Fuzzy Vault Scheme

(Submitted 12/XII 2014)

Keywords: *palm vein, biometrics, fuzzy vault, template protection, authentication.*

1. 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 or palm veins) 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.

Biometric template protection schemes [1] that are combining cryptography with biometrics are considered to be a promising solution to above issues.In this work we consider the palm veins as this kind of biometrics.Experiments on CASIA database [2] show that the minutiae features extracted from palm veins are discriminating features in the hand vein images.

Many famous biometric template protection schemes have been proposed such as fuzzy commitment scheme [3], fuzzy vault scheme [4] and fuzzy extractor [5]. Among them the fuzzy vault scheme proposed by Juels and Sudan [4] has become one of the most popular key-binding approaches, because it provides effective and provable security for biometric template protection. The scheme introduced by A. Juels and M. Wattenberg [3] is not order invariant, which is the weakest point of the algorithm described in [3], 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.

The rest of this paper is organized in the following manner. In section 2 the construction of fuzzy vault scheme is discussed. In section 3 the fuzzy vault scheme for palm veins is proposed. In section 4 some experimental results of fuzzy vault scheme's implementation are introduced. Finally, in section 5, conclusions are given with some discussions.

2. Fuzzy Vault Scheme. As it was mentioned above the fuzzy vault scheme provides an effective and provable security for biometric template protection [4] and has a property of order invariance. So it suits the best for our purpose. Let us briefly introduce that scheme.

Let F be a finite field of size n and biometric template of the user can be written as follows: $X = (x_1, x_2, \ldots, x_s)$, where $\forall i = 1\ldots s : x_i \in F$. 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 $p(x) : p_j \in F$. Let $r \in \{s+1, \ldots n\}$

Locking algorithm

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

Unlocking algorithm

1. Let we have new biometric $X' = (x'_1, x'_2, \ldots x'_s)$, where $\forall i = 1\ldots s : x'_i \in F$.
2. 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 or Reed Solomon codes.

3. Implementation of the Fuzzy Vault Scheme for palm-veins.

3.1. 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. Fig. 1 illustrates some of bifurcation and ending points on vein pattern's skeleton representation.Experiments on CASIA database [2] 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.

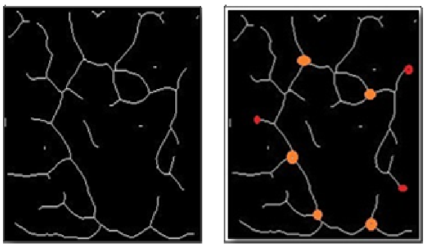

Fig. 1. Some of bifurcation points and ending points are marked by red circle:

3.2. Implementation of fuzzy vault based on the extracted data. The experiments were carried on the database of palm-veins CASIA [2]. This database has been acquired using a contactless imaging device and has images from 100 users. Six images were acquired from each user and these images were acquired in two different data acquisition sessions (three images in each session) with a minimum interval of one month. Since palm veins are most visible under 850 nm wavelength illuminations, only the images under these wavelength illuminations are chosen.

Encoding. The biometric template X, discussed above, is constructed using x and y coordinates of minutiae points. In the current implementation, a randomly generated secret S is 120-bit random key, which is used for constructing the secret polynomial p(x).

For each degree of the polynomial n in range [5, 12] and the number of the minutiae pointss =25, the chaff points were taken r-s= 200.

From this point on, all operations take place in Galois fields GF(2^{10}): we concatenate x and y coordinates of a minutiae (5-bits each) as[x | y] to arrive at the 10-bit locking/unlocking data unit u.

In enrollment phase mosaic matching [9] was used on 5 templates and the last one was used for verification.

Decoding. Here, the user tries to unlock the vault V using the query minutiae. Assume we have s query minutiae (X') and $u'_1, u'_2, \ldots u'_s$ are the points to be used in polynomial reconstruction. These points are found by comparing u_i , i = 1, 2… s. with the values of the vault V, namely $v_1, v_2, ..., v_r$. If any u_i is equal to $v_1, v_2, ..., v_r$, the corresponding vault pointis added to the list of points to be used. Assume that this list has m points,where $m \le r$. Now, for decoding a n-degree polynomial, n + 1 unique projectionsare necessary. We have to find all possible C_m^{n+1} combinationsof $n + 1$ 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 palm-vein are from the same palm.

4. The results of the experiments. Below the results of the tests on the palm-vein database are attached. There are six imprints of the same palm-vein and five of them were used to enroll the user (using mosaic matching) and the last one was used to verify if the user had passed the authentication.

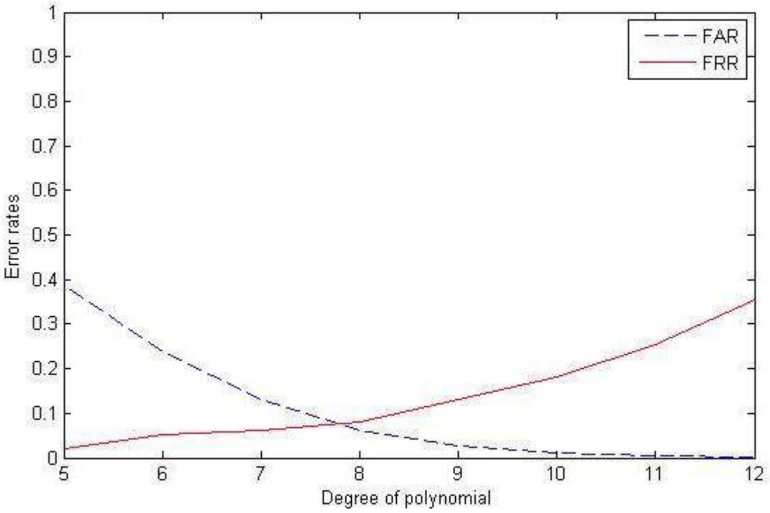

Fig. 2. Error rate curves of palm-veins fuzzy vault scheme.

5. **Conclusion.** In this paper we have presented the results of actual implementation of the fuzzy vault using palm-vein minutiae data. Experiments on CASIA database show that we can extract on average 25minutiae 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 enough for 120-bit key generation and for the practical accuracy of the system (FAR < 0.01). Compared with fingerprint based schemes the FRR of this system is lower, however there are other benefits of this biometrics, such as stability of the vein patterns over a long period of time and, what is more important, invisibility to the human eyes (what makes it much harder to copy the features).

Acknowledgement. This work was supported by State Committee Science MES RA, in frame of the research project SCS 13-1B352.

[1]Russian Armenian (Slavonic) University, serchch@gmail.com
[2]American University of Armenia, ajivanyan@aua.am
[3]American University of Armenia, National Academy of Sciences of Armenia, gurgenkh@aua.am
[4]National Academy of Sciences of Armenia, hkhasikyan@aua.am

S. S. Chidemyan, A. H. Jivanyan, academician G. H. Khachatryan, H. G. Khasikyan

Palm-Vein Based Fuzzy Vault Scheme

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, the template protection scheme is combined with biometrics, which results a provable security for the key binding problem. In particular, in this paper the approach for constructing a fuzzy vault scheme for the palm veins is presented. The proposed fuzzy vault scheme has been implemented and tested on the publicly available database of palm vein patterns derived from infrared scanner. The results are presented in the last section of the paper.

Ս. Ս. Չիդեմյան, Ա. Հ. Ջիվանյան, ակադեմիկոս Գ. Հ. Խաչատրյան,
Հ. Գ. Խասիկյան

Ձեռքի ափի երակների վրա հիմնված «ոչ հստակ» պահոցների սխեմա

Ոչ հստակ պահոցների սխեման ծածկագրման ամենահայտնի սխեմաներից է, որի նպատակն է ծածկագրել օգտագործողի կարևոր ինֆորմացիան այնպես, որ միայն օրինական օգտագործողները ստանան դրան հասանելիություն:

Այս հոդվածում շաբլոնների պաշտպանության գաղափարը միավորված է կենսաչափական բնութագրերի հետ, ինչը բերում է բարձր անվտանգությանը բանալու կցման խնդրի համար: Մասնավորապես, այս հոդվածում ներկայացված է ձեռքի ափի երակներից ստացված բնութագրերի հիման վրա «ոչ հստակ» պահոցների սխեմայի կառուցման մեթոդը: Առաջարկված սխեման իրականացվել էր ծրագրային և թեստավորվել բաց հասանելիության մեջ գտնվող ձեռքի ափի երակների բազայի վրա: Արդյունքները ներկայացված են այս հոդվածի վերջին բաժնում:

С. С. Чидемян, А. А. Дживанян, академик Г. А. Хачатрян,
О. Г. Хасикян

Схема “нечетких хранилищ”, основанная на венах ладони

Схема “нечетких хранилищ” – одна из самых популярных схем шифрования, целью которой является кодирование важной информации пользователя таким образом, чтобы только легальные пользователи имели доступ к ней.

Схема защиты шаблонов используется вместе с биометрическими данными, что приводит к высокой безопасности проблемы связывания ключа. Представлен метод построения схемы “нечетких множеств” для вен ладони. Представленная схема была программно реализована и протестирована на находящейся в открытом доступе базе вен ладоней. Результаты представлены в последнем разделе статьи.

References

1. *Uludag U., Pankanti S., Prabhakar S., Jain A. K.* - Proceedings of the IEEE. 2004. V. 92. N. 6. P. 948–960,
2. CASIA MS Palmprint V1 Database, [Online]. Available: http: // biometrics. idealtest.org/dbDetailForUser.do?id=5.
3. *Juels A., Wattenberg M.* In: Proceedings of the 1999 6th ACM Conference on Computer and Communications Security (ACM CCS ’99). November 1999. P. 28–36.
4. *Juels A., Sudan M.* In: Proceedings of the IEEE International Symposium on Information Theory. July 2002. P.408.

5. *Dodis Y., Ostrovsky R., Reyzin L., Smith A.* - SIAM Journal on Computing. 2008. V. 38. N 1. P. 97–139.
6. *Wanga L. Y., Leedhamb G., Choa D. S. Y.* Minutiae feature analysis for infrared hand vein pattern biometrics. Pattern Recognition Society, Published by Elsevier Ltd, All rights reserved, 2007.
7. *Hassan Soliman, Abdelnasser Saber Mohamed, Ahmed Atwan* –International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS. 2012. V. 12. N 01 28. P.28-39.
8. *Yingbo Zhou, Ajay Kumar* - IEEE Transactions on Information Forensics and Security. December 2011. V. 6. N 4. P. 1259-1274., 2011.
9. *Jainv A. K., Ross A.*- Proc. IEEE-ICASSP 2002. P.4064-4067. May 2002.