Mathematical Problems of Computer Science 43, 47--51, 2015.

A Modified Fuzzy Vault Scheme for Increased Accuracy

Hovik G. Khasikyan

Institute for Informatics and Automation Problems of NAS RA
e-mail: hkhasikyan@aua.am

Abstract

In this paper a new "Fuzzy Vault" scheme is proposed, which improves the False Rejection Rate of the original scheme. When constructing the vault of the original scheme there was a need to trim the biometric data, which is an information loss and affects the performance of the system. This was resolved in the suggested version of this construction. The schemes were implemented for fingerprint data, and the comparisons are brought in the last section of this paper.

Keywords: Biometrics, Fuzzy Vault, Fingerprints.

1. Introduction

Conventional passwords are usually simple and, as a rule, easy to guess or to break. People remember only short passwords. What is more, they tend to choose passwords, which are easily cracked by dictionary attacks [1, 2, 3]. Thus, there was a suggestion to use some biometric properties of a user to provide an access to the personal data. The biometric characteristics of a person, such as DNA, palm vein, fingerprints, face and iris features can be used to generate passwords or lock secrets.

Such schemes were introduced by A. Juels and M. Wattenberg [4], which was not order invariant, and this was the weakest point of the algorithm described in [4] as the data extracted from the biometric template is not in the same order each time. Thereafter A. Juels and M. Sudan presented a new scheme called "A Fuzzy Vault Scheme"[5], which already had a property of order invariance. The notion of *fuzzy vault* was first given by Juels and Sudan. For analysis of the concepts False Acceptance Rate (FAR) and False Rejection Rate (FRR) are used.

FAR is the probability that a random vector is accepted as valid biometric data at the authentication phase.

FRR is the probability that the observed genuine biometric data has too many errors and is rejected at the authentication phase.

The scheme in [5] can be modified for decreasing the False Rejection Rate (FRR) while keeping the FAR of the system the same.

The rest of this paper is organized as follows. Section 2 gives a review of the fuzzy vault construction. Section 3 outlines the modified construction of Fuzzy Vault. In section 4 the experimental results of the two schemes are introduced. Section 5 gives the summary of the paper.

2. Review of Fuzzy Vault

The fuzzy commitment scheme is presented by Juels and Wattenberg [4], which as it was already mentioned is not order invariant. Order invariance is a very important property, because not always we can obtain biometric data of a user in the same order. Then Juels and Sudan presented their new Fuzzy Vault construction [5]. The brief description of the scheme is given below.

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

A. Enrollment Phase

1. Take the secret polynomial *p(x)* of degree $\mathrm{k} = \mathrm{s} - \mathrm{t} - 1$, $t \in \{1, \dots, s\}$ and evaluate it on the points of the biometric data. Let $y_i = p(x_i),\ i = 1,2 \dots, s$.

2. Add $r - s$ distinct random points from the set $F - w$. Let them be $x_{S+1}, \dots, x_r$. These points are called chaff points.

3. Choose $y_i \in$F ,$i = s + 1 \dots r$ such that $y_i \neq p(x_i)$.

4. Store $ss(w) = \{(x_1, y_1), \dots, (x_r, y_r)\}$ as a reference. The $ss(w)$ is called a vault.

B. Authentication Phase

Let the new biometric be $w' = (x'_1, x'_2, \dots, x'_s)$. If it has at least $s - t$ common points with the original biometric using Lagrange interpolation or Reed Solomon codes the secret polynomial can be reconstructed.

3. The Proposed Scheme

Again F is a finite field of size n. The biometric template for enrollment is $w = (x_1, x_2, \dots, x_s)$, however, in this scheme the condition $x_i \in F$ is not mandatory. The secret polynomial is the *p(v)*. The degree of *p(v)* is $\mathrm{k} = \mathrm{s} - \mathrm{t} - 1, \mathrm{t} < s$, and the coefficients belong to F. The enrollment and authentication phases are the following.

A. Enrollment Phase

1. Take the secret polynomial *p(v)*, generate s random values $q = (v_1, v_2, \dots, v_s)$, where $v_i \in F$ and evaluate the *p(v)*on$q$. Let $y_i = p(v_i),\ i = 1,2 \dots, s$.

2. Add $r - s$ distinct random points from the set $F - q$. Let them be $v_{S+1}, \dots, v_r$. Add $r - s$ distinct random points, which are not in the set of w, but are within the possible set of the points of the considered biometric data. Let them be $x_{S+1}, \dots, x_r$.

3. Choose $y_i \in$F ,$i = s + 1 \dots r$ such that $y_i \neq p(v_i)$.

4. Store $\{(x_1, y_1, v_1), \dots, (x_r, y_r, v_r)\}$ as a reference in database. Let's denote this vault by $ms(w)$.

B. Authentication Phase

Now suppose the new biometric measurement is $w' = (x'_1, x'_2, \dots, x'_s)$ and we want to recover the secret polynomial *p(v)*. Thus, in case the w'coincides with at least $s - t$ points with original biometrics, the corresponding triplets(x_i, y_i, v_i) can be chosen from the vault $ms(w)$ and using the pairs (y_i, v_i) the secret can be recovered.

The advantage of this scheme is that in this case there is no need to concatenate the biometric template, as it should be done with the most types of biometrics for the fuzzy vault [6, 7, 8]. In addition, the user is free to choose the Galois Field he wants to use in this system. As a result of these modifications there is no information loss in the enrollment stage, which leads to the increased accuracy of verification.

4. Experimental Results for Fingerprints

The experiments were conducted on GF(2^{16}). In the case of the original scheme the minutiae point descriptors are formed by concatenating some parts of x, y coordinates and some part of the minutiae angle θ. In order to form a 16 bit value, 5 bits were taken for x coordinate, 5 bits for y and 6 bits for θ angle.

In the case of the new scheme, the coordinates are kept in the original form and the 16 bit values are random. In all experiments FVC 2000 DB2 pre-aligned database of fingerprints was used. The results of the experiments are illustrated in the Table1.

Table 1

	Juels-Sudan scheme	***The Proposed scheme***
FAR (%)	0.2%	0.2%
FRR (%)	20.4%	13.8%
secret size	128 bit	128 bit
reference size	960 Byte	1700 Byte
r (the size of vault)	240	240

5. Conclusion

In this paper an improvement was suggested for increasing the performance of a well-known scheme for biometric key binding. It was shown that during the vault construction the concatenation of biometric data affects the accuracy of the system. To overcome this issue, in the new scheme the reference data were kept as triplets; first is the biometric data in its original form, the second is a random value and the third is the evaluation of the value. The scheme was implemented for fingerprints and the experiments have shown that it provides better FRR, while maintaining the FAR of the system the same.

Acknowledgement

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

References

[1] E. Spafford, “Observations on reusable password choices”,*Proceedings of the 3rd USENIX Security Symposium*, September, pp. 299--312, 1992.

[2] T. Wu, “A real-world analysis of Kerberos password security”, Proceedings of the 1999 Network and Distributed System Security Symposium,February 1999.

[3] R. Morris and K. Thompson, “Password security: A case history,” *Communications of the ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[4] A. Juels and M. Wattenberg, “A fuzzy commitment scheme”,*Proceedings of the 6th ACM Conference on Computer and Communications Security*, pp. 28–36, 1999.

[5] A. Juels and M. Sudan, “A fuzzy vault scheme”, *Proceedings of IEEE International Symposium of Information Theory*, Lausanne, Switzerland, p. 408, 2002.

[6] U. Uludag, S. Pankanti and A. K. Jain, “Fuzzy vault for fingerprints”, *Proceedings of Audio- and Video-Based Biometric Person Authentication*, Rye Town, NY, pp. 310–319, July 2005.

[7] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park and J. Kim, “Biometric key binding: fuzzy vault based on iris images”,*Proceedings of 2nd International Conference on Biometrics, Seoul*, South Korea, pp. 800–808, August 2007.

[8] A. Kumar and A. Kumar, “Development of a new cryptographic construct using palmprint-based fuzzy vault”, *EURASIP Journal on Advances in Signal Process*,vol. 2009, Article ID 967046, 11 pages, 2009.

Submitted 10.11.2014, accepted 12. 02. 2015.

Չևափոխված թերորոշ բանալային պահոցով սխեմա ճշգրտության բարձրացման համար

Հ. Խասիկյան

Ամփոփում

Այս աշխատանքում առաջարկվում է «Fuzzy Vault» սխեմայի մոդիֆիկացված տարբերակ, որը բարելավում է օրիգինալ սխեմայի սխալ մերժման գործակիցը: Օրիգինալ սխեմայի կառուցման ժամանակ կարիք կար կարճացնել կենսաչափական տվյալները, ինչը ինֆորմացիայի կորուստ էր և ազդում էր համակարգի արդյունավետության վրա: Այս խնդիրը լուծվել է սխեմայի նոր առաջարկվող տարբերակում: Սխեմաները իրականացվել են մատնահետքային տվյալների հայտնի պահոցների վրա, իսկ համեմատությունները բերված են վերջին բաժնում:

Модифицированный вариант схемы "нечеткого хранилища" для увеличения точности

О. Хасикян

Аннотация

В этой работе предлагается модифицированный вариант схемы "нечеткого хранилища", в котором улучшается коэффициент ложного отказа в доступе. При построении оригинальной схемы была необходимость в сокращении биометрических данных, что само по себе потеря информации и влияет на эффективность системы. Эта проблема разрешена в новом предложенном варианте схемы. Схемы были реализованы для известных баз отпечатков пальцев, а сравнения приведены в последнем разделе.