A Practical Approach on Human Authentication Using Biometrics

Marcelo Fornazin
UNESP – Sao Paulo State University
Computer Science Department
fornazin@fc.unesp.br

Danilo B. S. Netto Junior
UNESP – Sao Paulo State University
Computer Science Department
balzaque@gmail.com

Marcos A. Cavenaghi
UNESP – Sao Paulo State University
Computer Science Department
marcos@fc.unesp.br

Abstract

This is a work in progress, presenting concepts and techniques directly related to the practical use of the Fuzzy Vault Scheme (FVS) biometrics cryptosystem on human authentication using biometrics. Many applications handle confidential information from their users. These information need to be handled in a secure way. One way of handling information securely is through cryptography, where the use of passwords is a common practice. Passwords are the weakest link on a conventional cryptosystem, because passwords can be easily copied or stolen. Biometrics is a way to overcome issues regarded the usage of passwords. Biometrics signals are more secure, but they also need to be protected. To protect biometrics signals one can use cryptography based on biometrics keys. But, due to the variability of the biometrics signal, biometrics cannot be directly used as cryptographic keys of a traditional cryptosystem. Cryptosystems that address to overcome these issues are called Biometrics Cryptosystems.

1. Introduction

Human beings always use body characteristics such as voice and face to identify themselves [1]. The idea behind Biometrics is the same: the use of physiological and/or behavioral characteristics in order to authenticate people.

The physiological and/or behavioral characteristics used in biometrics are known as Biometrics Characteristics. Through these biometrics characteristics it is possible to establish a metric. The metric is used to numerically describe an individual characteristic.

Biometrics cryptosystems can use this metric to handle human beings physiological/behavioral characteristics in order to authenticate a user on a system (bank account, website, e-mail account, etc.).

This work presents concepts and techniques directly related to the practical use of a biometrics cryptosystem known as the FVS to overcome the deficiencies presented by conventional methods of human authentication, such as the use of passwords. The FVS has been chosen due to its popularity among research groups. Example of another biometrics cryptosystem can be found in [3].

2. The Fuzzy Vault Scheme

In the cryptographic construction named a FVS or simply Fuzzy Vault [2], a secret can be locked in a vault by a set *A*. Another set *B*, which overlaps substantially with *A*, can unlock the vault and recover the secret successfully.

Such error-tolerant cryptographic algorithm can be useful in many circumstances in which the exactitude represents a drawback, such as secret protection using biometrics data and other types of noisy data, biometrics template protection, and so on.

A. Juels et al.'s FVS constitutes of LOCK algorithm and UNLOCK algorithm. In the LOCK algorithm, a polynomial $p(x)$ of degree less than k over a finite field F is selected such that $p(x)$ encodes the secret in some way (e.g., has an embedding of in its coefficients) at first.

The locking set *A* is projected onto the polynomial and those points on the polynomial are stored along with some noise points such that the locking set *A* is concealed. The real points and the noise points consist of the vault *VA*.

In the UNLOCK algorithm, the unlocking set *B* is used to pick out a candidate set *Q* from the vault *VA* at first. Input the candidate set *Q* into a Reed-Solomon (RS) decoder to reconstruct the polynomial $p(x)$ and recover the secret as well (RS code is a typical linear error correction code, so the RS decoder just works for the valid RS codeword). If the locking set *A* and the unlocking set *B* are close enough, the RS decoding will succeed, and vice versa [2].

A more detailed description of the FVS is beyond the scope of this work. Readers can find all its formalism in [2].

3. Practical Approach

The FVS is a cryptography construction that addresses the issues regarded to the signal variability and security. Today, there is some proposal of biometrics cryptosystems based on the FVS, most of them for fingerprints [4] and handwritten signatures [5].

But, none of them have been evaluated in real world applications, with the use of a real human to "donate" the biometric characteristic. Instead, they are implemented in MatLab and the evaluations have been made with image databases. The use of MatLab imposes a performance issue on such systems due to the way MatLab deals with implemented mathematical functions.

To address this performance issues, this project is focused on the development of an application based on the FVS, but developed in C++, instead of MatLab functions, called the FVLib.

This application will allow humans to be authenticated based on their biometric characteristics instead of a single password. Biometrics characteristics are extracted using a U.are.U 4000 device and inserted into the FVLib as parameters. If the fingerprint matches, the corresponding stored password is returned.

3.1. The Fuzzy Vault Lib (FVLib)

The Fuzzy Vault Lib (FVLib) has been implemented to carry on MatLab performance limitations. FVLib is a library that implements the FVS, allowing it to be integrated with real world security applications. It has been implemented in C++ (*Microsoft Visual C++*). There is also a work in progress, which main goal is its implementation in Java for use with smartcards.

The next steps are focused on the FVLib integration with fingerprint extraction algorithms and authentication systems, resulting in a complete set of tools to authenticate human beings through biometric characteristics.

As a final approach, the tool developed will be tested in a real world scenario. Its performance on several working conditions will be evaluated and a commercial prototype will be created.

4. Conclusion

This work presented a work in progress. Its main goal is the implementation of a complete tool directly related to the practical use of a biometrics cryptosystem known as the FVS to overcome the deficiencies presented by conventional methods of human authentication, such as the use of passwords.

In this stage of development, the FVLib has already been implemented, exploring all the FVS functionalities. Its integration with fingerprints extraction algorithms and authentication systems has just started.

Also, a Java version is almost finished and the tests with smartcards will start by October, 2007. It is expected that the work with fingerprints will be finished by March, 2008. After that, the work will be extended to use iris information as the biometrics characteristics for the FVLib input.

When finished, the main contribution of this work will be the implementation of a real cryptosystem, integrating biometrics and cryptography.

5. Acknowledgements

The authors would like to thank FAPESP (PROC. 2006/07062-8) and FUNDUNESP for the financial support.

6. References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics,* Vol. 14, 1, pp. 4-20, 2004.

[2] A. Juels, and M. Sudan, "A fuzzy vault scheme", Proceedings of the IEEE International Symposium on Information Theory, pp.408. Piscataway, NJ, 2002.

[3] G. I. Davida, et al., "On the relation of error correction and cryptography to an off-line biometric based identification scheme", Proceedings of WCC99, Workshop on Coding and Cryptography, 1999.

[4] U. Uludag, and A.K. Jain, "Securing Fingerprint Template: Fuzzy Vault with Helper Data", Computer Vision and Pattern Recognition Workshop. pp. 163-163, 2006.

[5] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Cryptographic key generation using handwritten signature", Defense and Security Symposium, Biometric Technologies for Human Identification, BTHI, Proc. SPIE, Vol. 6202, pp. 255-231, 2006.