BIOMETRIC CRYPTOSYSTEMS – APPROACHES TO BIOMETRIC KEY-BINDING AND KEY-GENERATION

NEMANJA MAČEK
School of Electrical and Computer Engineering of Applied Studies, Belgrade; Graduate School of Computer Sciences, Megatrend University, Belgrade; SECIT Security Consulting; macek.nemanja@gmail.com

IGOR FRANC
Belgrade Metropolitan University, Faculty of Information Technologies; SECIT Security Consulting; igor.franc@metropolitan.ac.rs

MILAN GNJATOVIĆ
University of Novi Sad, Faculty of Technical Sciences; milangnjatovic@uns.ac.rs

BRANIMIR TRENKIĆ
School of Electrical and Computer Engineering of Applied Studies, Belgrade; btrenkic@viser.edu.rs

MITKO BOGDANOSKI
Military Academy General Mihailo Apostolski, Skoplje, Macedonia; mitko.bogdanoski@ugd.edu.mk

ACA ALEKSIĆ
Belgrade Metropolitan University, Faculty of Information Technologies; aca.aleksic@metropolitan.ac.rs

Abstract: *Biometric cryptosystems are emerging technology that allow user to generate or unlock cryptographic key using biometric data, such as iris or fingerprint. In other words, biometric cryptosystems provide mechanisms for biometric-dependent key-release. A comprehensive survey of biometric cryptosystems is presented in this paper, i.e. state of the art approaches, such as fuzzy commitment, fuzzy vault are reviewed and discussed. Finally, a brief discussion of biometric cryptosystems security is given as a concluding remark to this paper.*

Keywords: *Biometry, Cryptosystems, Key Binding, Key Generation*

1. INTRODUCTION

Biometric cryptosystems require the storage of public information that is dependent on biometrics. This information is applied to retrieve or generate keys, which is referred to as helper data [1]. Due to biometric variance (see Image 1) it is not feasible to extract keys from biometric characteristics directly.

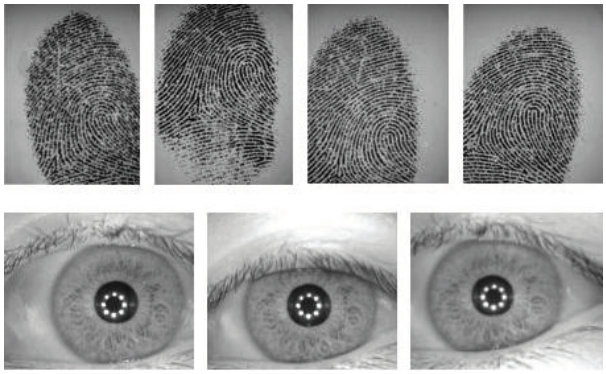

Image 1: Biometric invariance (samples originating from FCV and CASIA databases)

Helper data, which does not reveal significant information about original biometric templates is therefore used to reconstruct cryptographic keys. Biometric comparisons are performed indirectly by verifying key validities, where the output of an authentication process is either a key or a message about failure. Since the verification of keys represents a biometric comparison in encrypted domain [2], biometric cryptosystems are applied as a means of biometric template protection, in addition to providing biometric-dependent keyrelease.

Within biometric cryptosystems acceptance requires the generation or retrieval of hundred percent correct keys, while conventional biometric systems response with “Yes” or “No”.

In addition, the majority of biometric cryptosystems introduce a higher degree of quantization at feature extraction, compared to conventional biometric systems, which are capable of setting more precise thresholds to adjust recognition rates.

There are two types of biometric cryptosystems, depending on how helper data are derived: key-binding systems and key-generation systems. More detailed information on those are given in sections 2 and 3 of this paper.

2. KEY-BINDING SYSTEMS

In key-binding systems, helper data are obtained by binding a chosen key to a biometric template. As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. Applying an

appropriate key retrieval algorithm, keys are obtained from the helper data at authentication [3]. Since cryptographic keys are independent of biometric features these are revocable while an update of the key usually requires re-enrolment in order to generate new helper data.

Several approaches to biometric key-binding will be briefly discussed in this paper: Mytec1 and Mytec2, fuzzy commitment scheme and fuzzy vault.

The first sophisticated approach to biometric key-binding based on fingerprints was proposed in [4-6]. The presented system was called Mytec2, a successor of Mytec1 [7], which was the first biometric cryptosystem but turned out to be impractical in terms of accuracy and security. The basis of the Mytec2 (and Mytec1) algorithm is the mechanism of correlation. The algorithm behind Mytec2 was summarized in a patent [8], which includes explanations of how to apply the algorithm to other biometric characteristics such as iris. However, no performance measurements are reported in publications.

Juels and Wattenberg [9] combined techniques from the area of error correcting codes and cryptography to achieve a type of cryptographic primitive referred to as fuzzy commitment scheme.

A fuzzy commitment scheme consists of a function F, used to commit a codeword $c \in C$ and a witness $x \in \{0,1\}n$. The set C is a set of error correcting codewords c of length n and x represents a bitstream of length n, termed witness (biometric data). The difference vector of c and x, $\delta \in \{0,1\}n$, where $x=c+\delta$, and a hash value $h(c)$ are stored as the commitment termed $F(c,x)$ (helper data). Each x', which is sufficiently "close" to x, according to an appropriate metric, should be able to reconstruct c using the difference vector δ to translate x' in the direction of x. A hash of the result is tested against $h(c)$. With respect to biometric key-binding the system acquires a witness x at enrolment, selects a codeword $c \in C$, calculates and stores the commitment $(c,)$ (δ and $h(c)$). At the time of authentication, a witness x' is acquired and the system checks whether x' yields a successful de-commitment. Enrolment and authentication phases are depicted on Images 2 and 3, respectively.

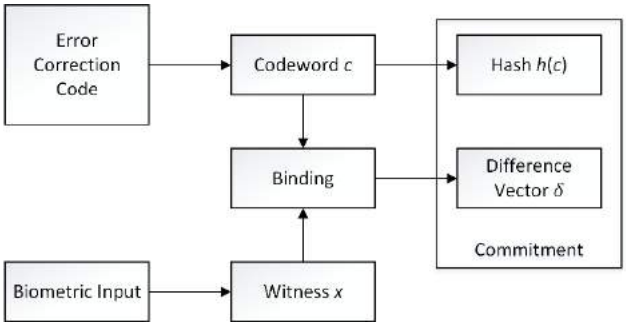

Image 2: Fuzzy commitment scheme (enrolment phase)

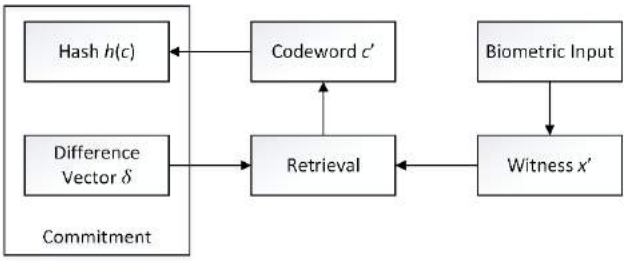

Image 3: Fuzzy commitment scheme (authentication phase)

Fuzzy Vault is an encryption scheme proposed by Juels and Sudan [10] which leverages some of the concepts of error-correcting codes, to encode information in such a way as to be difficult to obtain without the "key" used to encode it, even if the methods used for encoding are publicly known. Although this approach can work with any code, the Fuzzy Vault scheme is often used with Reed-Solomon codes, so we will focus on them for this exposition. A secret is encoded using a set of values (the "key"), and can then be unlocked with another set of values only if it has substantial overlap with the set used to lock it. This approach offers order invariance, meaning that the sets used to lock and unlock the secret are unordered. Because of this property, the Fuzzy Vault scheme has been seen application in biometric encryption [11], namely fingerprint authentication.

Reed-Solomon codes work by encoding the values in a message as the coefficients of a polynomial and then evaluating that polynomial at a set of points to obtain the codeword for that message. By using a number of evaluation points greater than the degree of the polynomial, it will be possible to obtain the polynomial (and therefore the message) by interpolation even in the presence of missing or erroneous values. However, if there are too many errors, there will not be a unique interpolating polynomial of the proper degree. These properties are leveraged in the Fuzzy Vault scheme.

Numerous enhancements to the original concept of the fuzzy vault have been introduced. Moon et al. [12], for example, suggest to use an adaptive degree of the polynomial. Nagar and Chaudhury [13] arrange encoded keys and biometric data of fingerprints in the same order into separate grids, which form the vault. Chaff values are inserted into these grids in appropriate range to hide information.

3. KEY-GENERATION SYSTEMS

In key-generation systems, helper data is derived only from the biometric template. Keys are directly generated from the helper data and a given biometric sample. While the storage of helper data are not obligatory the majority of proposed key-generation schemes does store helper data (if key-generation schemes extract keys without the use of any helper data these are not updatable in case of compromise).

The prior idea of generating keys directly out of biometric templates was presented in a patent by Bodo [14]. An implementation of this scheme does not exist and it is expected that most biometric characteristics do not provide enough information to reliably extract a sufficiently long and updatable key without the use of any helper data.

Helper data-based key-generation schemes are also referred to as “fuzzy extractors” or “secure sketches”, for both primitives formalisms (and further extensions) are defined in [15, 16]. A fuzzy extractor reliably extracts a uniformly random string from a biometric input while stored helper data assist the reconstruction. In contrast, in a secure sketch, helper data are applied to recover the original biometric template.

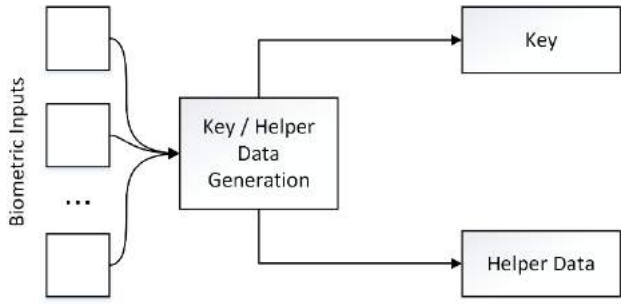

Image 4: Key-generation system (enrolment phase)

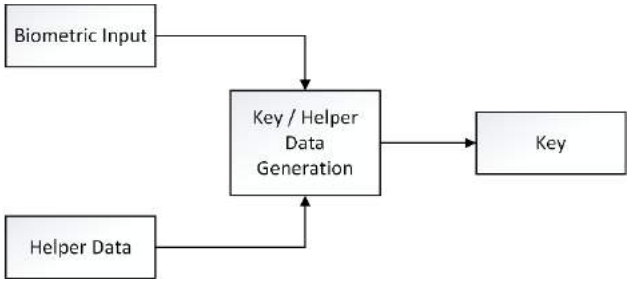

Image 5: Key-generation system (authentication phase)

There are two schemes that employ helper data. The private template scheme, based on iris, was proposed by Davida et al. [17, 18] in which the biometric template itself (or a hash value of it) serves as a secret key. The storage of helper data which are error correction check bits are required to correct faulty bits of given iris-codes. In another group of schemes, called quantization schemes, helper data are constructed in a way that is assists in a quantization of biometric features in order to obtain stable keys.

5. CONCLUSION

Concluding remarks are focused on the security of biometric cryptosystems. Most biometric cryptosystems aim at binding or generating keys, long enough to be applied in a generic cryptographic system (for example, at least 128-bit length of keys for AES algorithm). To prevent biometric keys from being guessed or brute-forced, these need to exhibit sufficient size and entropy. System performance of biometric cryptosystems is mostly reported in terms of false reject and false acceptance rates, since both metrics and key entropy depend on the tolerance levels allowed at comparison, these three quantities are highly interrelated. A second factor which affects the security of biometric cryptosystems is privacy leakage, i.e., the information that the helper data contain (leak) about biometric data. Ideally, privacy leakage should be minimized (for a given key length), to avoid identity fraud. The requirements on key size and privacy leakage define a fundamental trade-off within approaches to biometric cryptosystems, which is rarely estimated (this trade-off is studied from in an information-theoretical prospective). Additionally, stored helper data have to provide un-linkability. However, attacks on biometric cryptosystems are much more complex when compared to traditional biometric authentication. The goal is to reduce the search space, obtain the key or create a masquerade version of biometrics.

REFERENCES

[1] A. K. Jain, K. Nandakumar, A. Nagar, “Biometric template security”, EURASIP J, Adv Signal Process 2008, pp. 1-17.

[2] A. K. Jain, A. Ross, U. Uludag, “Biometric template security” Challenges and solutions”, In Proc. of European Signal Processing Conf (EUSIPCO) 2005.

[3] U. Uludag, S. Pankant, S. Prabhakar, A. K. Jain, “Biometric cryptosystems: issues and challenges”, In Proc. IEEE 2004, 92 (6), pp. 948-960.

[4] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. Kumar, “Biometric encryption–enrollment and verification procedures”, In Proc. SPIE, Optical Pattern Recognition IX 1998, 3386, pp. 24-35.

[5] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy R, B. V. Kumar, “Biometric encryption using image processing”, In Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II 1998, 3314, pp. 178-188.

[6] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy R, B. V. Kumar, “Biometric encryption”, ICSA Guide to Cryptography, 1999.

[7] C. Soutar, G. J. Tomko, G. J. Schmidt, “Fingerprint controlled public key cryptographic system”, US Patent 1996, 5541994.

[8] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy R, B. V. Kumar, “Method for secure key management using a biometrics”, US Patent 2001, 6219794.

[9] A. Juels, M. Wattenberg, “A fuzzy commitment scheme”, In Proc. 6th ACM Conf on Computer and Communications Security 1999, pp. 28-36.

[10] A. Juels A, M. Sudan, “A fuzzy vault scheme”, In Proc. 2002 IEEE Int. Symp. On Information Theory 2002, 408.

[11] K. Nandakumar K, A. K. Jain, S. Pankanti, “Fingerprint-based fuzzy vault: implementation and performance”, IEEE Trans. Inf. Forensic. Secur. 2007, Vol 2, pp. 744-757.

[12] D. Moon D, W-Y. Choi, K. Moon, Y. Chung, “Fuzzy fingerprint vault using multiple polynomials”, IEEE 13th Int Symposium on Consumer Electronics, ISCE ‘09 2009, pp. 290-293.

[13] A. Nagar, S. Chaudhury, “Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme”, In Proc. 18th Int. Conf. on Pattern Recognition (ICPR’06) 2006, ICPR 4, pp. 537-540.

[14] A. Bodo A, “Method for producing a digital signature with aid of a biometric feature”, German patent DE 4243908 A1 1994.

[15] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”, In Proc. Eurocrypt 2004, pp. 523-540, (LNCS: 3027).

[16] E. A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, B. Ŝkorić, “Key extraction from general nondiscrete signals. IEEE Trans Inf Forensic Secur 2010, 5(2):269-279.

[17] G. Davida, Y. Frankel, B. Matt, “On enabling secure applications through offline biometric identification”, In Proc. of IEEE, Symp on Security and Privacy 1998, pp. 148-157.

[18] G. Davida, Y. Frankel, B. Matt, “On the relation of error correction and cryptography to an off line biometric based identication scheme” In Proc. of WCC99, Workshop on Coding and Cryptography 1999, pp. 129-138.