Biometrics Based Secret Sharing Using Fuzzy Vault

Gevorg Margarov
State Engineering University of Armenia
Yerevan, Armenia
e-mail: gmargarov@gmail.com

Maha Tolba
State Engineering University of Armenia
Yerevan, Armenia
e-mail:Maha_saad_tolba@yahoo.com

ABSTRACT
In this paper a method for the biometric based secret sharing problem using the fuzzy vault construct is described. The secret is protected using the biometric data of the sharing parties, revealing a secret when a predetermined number of the sharing parties collaborate. The distinction between biometric cryptosystems is discussed. The basic idea of the fuzzy vault scheme is discussed. Finally the secret sharing using fuzzy vault is presented.

Keywords
Authentication, secret sharing, cryptography, security, fingerprint, biometrics.

1. INTRODUCTION
Biometric authentication is the task of verifying the identity of individuals based on their physiological or behavioral traits, such as fingerprint or signature, respectively. Biometric systems are gaining popularity as more trustable alternatives to password-based security systems, since there are no passwords to remember and biometrics cannot be stolen and are difficult to copy. Biometrics also provide non-repudiation, (an authenticated user cannot deny having done so) because of the difficulty in copying or stealing someone's biometrics.

In biometric based authentication, biometric traits of a person are matched against his/her stored biometric profile, and access is granted if there is sufficient match. However, there are other access scenarios, which require participation of multiple previously registered users for a successful authentication or to get an access grant for a certain entity. For instance there are cryptographic constructs generally known as secret sharing schemes [1], where a secret is split into shares and distributed amongst participants in such a way that it is reconstructed/ revealed only when the necessary number of the share holders comes together. The revealed secret can then be used for encryption or authentication (if the revealed key is verified against the previously registered value). One of the potential applications could be sharing of a bank account by family members. In example scenario, a husband and his wife will submit their biometric traits (e.g. fingerprints) to the bank, where the bank will register their traits and open an account. To withdraw money from the shared account both the husband and his wife must present their biometric traits.

In this paper we present a secret sharing method where the secret is protected using the biometric traits of the sharing parties. The method uses the *fuzzy vault* construct suggested by Jules et al. [2]. Fuzzy vault construct is an example of recent research which focuses on combining cryptography and biometrics to take advantage of the benefits of both fields [2:6]: while biometrics provide non-repudiation and convenience, traditional cryptography provides adjustable levels of security and can be used not just for authentication, but also for encryption.

2. BIOMETRIC CRYPTOSYSTEMS
The most popular authentication mechanism used for key release is based on passwords, which are cryptographic key-like strings but simple enough for users to remember. Hence, the plain text protected by a cryptographic algorithm is only as secure as the password (weakest link) that releases the correct decrypting keys. Simple passwords compromise security, but complex passwords are difficult to remember and expensive to maintain. Further, passwords are unable to provide non-repudiation: a subject may deny releasing the key using password authentication, claiming that his password was stolen. Many of these limitations of password-based key release can be eliminated by incorporating biometric authentication. It is inherently more reliable than password-based authentication as biometric characteristics cannot be lost or forgotten. Further, biometric characteristics are difficult to copy, share, and distribute, and require the person being authenticated to be present at the time and point of authentication. Thus, biometrics-based authentication is a potential candidate to replace password-based authentication, either for providing complete authentication mechanism or for securing the traditional cryptographic keys.

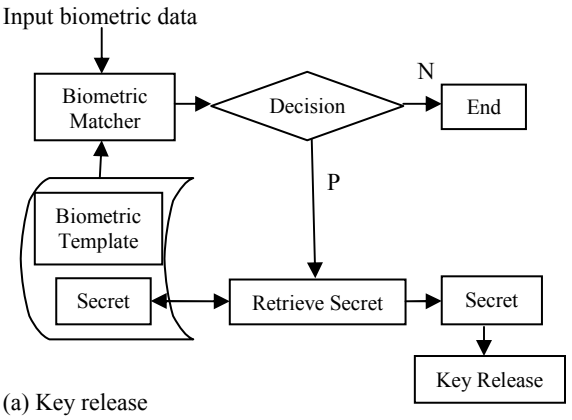
A biometric system and a cryptographic system can be merged in one of the following two modes [7]:

(i) *In biometrics-based key release*, the biometric matching is decoupled from the cryptographic part. Biometric matching operates on the traditional biometric templates: if they match, cryptographic key is released from its secure location, e.g., a smart card or a server. Here, biometrics effectively acts as a wrapper mechanism in cryptographic domain.

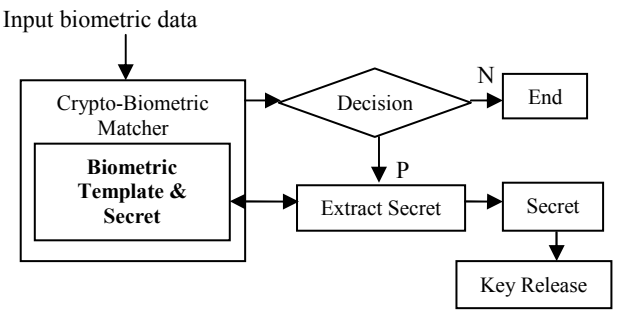
(ii) *In biometrics-based key generation*, biometrics and cryptography are merged together at a much deeper level. Biometric matching can effectively take place within cryptographic domain; hence there is no separate matching operation that can be attacked; positive biometric matching *extracts* the secret key from the conglomerate (key/biometric template) data. An example of the biometric-based key generation, called *fuzzy vault,* was proposed by Juels et.al. This cryptographic construct has the characteristics that make it suitable for applications that combine biometric authentication and cryptography: the advantages of cryptography (e.g., proven security) and fingerprint-based authentication (e.g., user convenience, non-repudiation) can be utilized in such systems.

Generating a cryptographic key from a biometric template (say fingerprints) has not been very successful, as it involves obtaining an *exact* key from a highly variable data. For instance Feng and Wah have been able to generate a 40-bit private key from online signatures with an 8% equal error rate [8]. Recent work of Juels et al. and Tuyls et al. [2, 3] are also classified as biometrics-based key generation, allowing for a tight coupling of cryptography and biometrics. Jules

and Wattenberg proposed the fuzzy commitment scheme [9]; later Juels and Sudan extended it to the *fuzzy vault* scheme [2] and described how it can be used to release/construct an encryption key using one's biometrics: a secret (cryptographic key) is *locked* using a biometric data of a person, such that someone who possesses a substantial amount of the locking elements (e.g. another reading of the same biometric) would be able to decrypt the secret [2].



(a) Key release



(b) Key generation

Fig.1. Two modes of combining biometrics with cryptography: (a) key release and (b) key generation.

3. THE FUZZY VAULT SCHEME

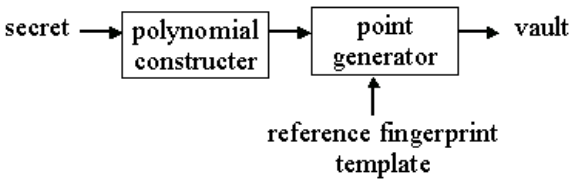
Given that the biometric system (like any other security system) is vulnerable to a number of adversary attacks, it is important to address the issue of secure design of the biometric system. Specifically, one would like to know whether there is a secure method of combining biometric authentication and cryptographic techniques. In a simplistic biometrics-based key release method [10], a successful biometric template match releases a cryptographic key as shown in Fig.1. (a). This method is vulnerable to attacks on the biometric template database, cryptographic key database, and the biometric matcher.

A more monolithic combination would entail generating a combined biometric-cryptographic key that is cryptographically secure (e.g., will not reveal inform about a biometric template or about the cryptographic key) from intruders while, for legitimate users, will permit access to the protected resource (e.g., key). The advantage of the second method, called the biometrics-based key generation method [10], is that since secret and biometric templates are securely stored in the crypto-biometric template as shown in Fig.1.(b). The matching of biometric identifiers within a cryptographic framework is a very challenging problem. In traditional (symmetric) cryptography, if the encryption and decryption keys are not identical, the decryption operation will produce useless random data.

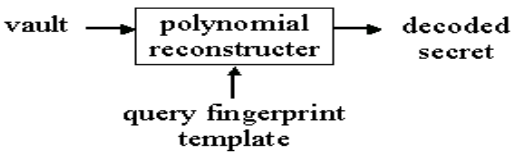
When biometric identifiers are employed as "keys" in the context of the cryptographic system, demanding such exactitude is impractical, that is, for the same biometric entity (e.g., the right index finger) that is analyzed during different acquisitions, the extracted biometric data will significantly vary due to acquisition characteristics. The issue dealing with the variability of the biometric data within the context of the cryptographic (biometric key generation) system has not been studied until recent years [10].

4. BIOMETRIC KEY GENERATION IMPLEMENTATION

In this section, we summarize a biometric (fingerprint) key generation system implementation by Uludag *et al.* [11], a cryptographic construct called the fuzzy vault (see Juels and Sudan [2]). The technique suggested by the authors is very preliminary, but the concept is rather powerful. For simplicity, let us assume that the system uses 8-bit – coordinates of fingerprint minutiae features but it can be extended to include other minutiae information as well. Further assume that x-coordinates have been appropriately coarsely quantized (e.g., to the nearest number divisible by 5).



(a) Locking the secret



(b) Unlocking the secret

Fig.2. Fuzzy vault system block diagram: (a) locking the secret, (b) unlocking the secret.

4.1. Encoding

Secret S is any secret data that needs to be protected (e.g., secret encryption key). The fuzzy vault built by Uludag *et al.* [11] begins by concatenating 16-bits CRC data from the initial secret S (56-bits key) to produce SC (72 bits). This concatenation reduces the chance of a random error being undetected (i.e., failing to identify incorrect decoding). SC is used to find the coefficients of the polynomial P: 72-bits SC can be represented as a polynomial with 8 (72/9) coefficients, with degree D=7, $p(x)=c_7x^7+c_6x^6+\ldots+c_1x+c_0$, by decomposing SC into non overlapping 9-bit segments, and each segment is declared as a specific coefficient c_i, i=0,1,2,…,7. Assuming that there are N unique template minutiae, $x_1,x_{2,\ldots},x_N$, the authors find a set of ordered pairs $G=\{(x_1,p(x_1)),\ (x_2,p(x_2)),\ldots\ (x_N,p(x_N))\}$. A second set of ordered pairs, called the chaff set C, is then generated from random x-coordinates $c_1,c_2,\ldots,c_M$ (distinct from $x_1,x_{2,\ldots},x_N$) such that $C=\{(c_1,d_1),\ (c_2,d_2),\ldots\ (c_M,d_M)\}$ and, $d_i\neq p(c_i)$, $\forall$ i. The union of these two sets G *and* C is randomized to produce vault set VS.

4.2. Decoding

Here, a user tries to unlock the vault V using the query minutiae features. Given N query minutiae (Q) $x_1^*, x_2^*, \ldots, x_N^*$, the points to be used in polynomial reconstruction are found by comparing x_i^*, i= 1,2,…, N, with the abscissa values of the vault V , namely v_l, l=1,2,…, (M+N): if any x_i^*, i=1,2,…, N is equal to v_l, l=1,2,…, (M+N), the corresponding vault point (v_l, w_l) is added to the list of points to be used. Assume that this list has K points, where K≤N.

Now, for decoding a degree D polynomial, (D+1) unique projections are necessary. All possible combinations of (D+1) points, among the list with size K are considered, resulting in $\binom{k}{D+1}$ combinations. For each of these combinations, the Lagrange interpolating polynomial is constructed,
Yielding:

$$P^*(x)=c^*_7x^7+c^*_6x^6+\ldots+c^*_1x+c^*_0 \qquad (1)$$

The coefficients are mapped back to the decoded secret SC*. If the CRC remainder on is not zero, we are certain that there are errors. If the remainder is zero, with very high probability, there are no errors. For the latter case, SC* is segmented into two parts: the first 56 bits denote S* while the remaining 16 bits are CRC data. Finally, the system outputs S*. If the query minutiae list overlaps with the template minutiae list in at least (D+1) points, for some combinations, the correct secret will be decoded, namely, S*=S will be obtained. This denotes the desired outcome when the query and template fingerprints are from the same finger. Fig.2. shows the block diagram of a fingerprint fuzzy vault system.

5. SECRET SHARING USING FUZZY VAULT

In this section we demonstrate the utilization of the fuzzy vault described above, for secret sharing. In the sample scenario, 3 users share a secret such that at least 2 of them must present their fingerprints to reveal the secret. During the locking phase, for each participant we select 13 of his/her minutiae points, discarding the rest. The selection of minutiae is performed around the center of mass of the corresponding fingerprint, to reduce possible matching errors caused by occlusions. Totally 39 (13x3) minutiae are used as the locking set.

The degree (*D*) of the polynomial to which the secret is to be encoded must satisfy following condition:

$$(T - 1)\,K \le D \le TK - 1$$

Where *T* denotes the minimum number of sharers required to reveal the secret and *K* denotes number of features each sharer possesses. Thus, any degree between 13 and 25 will satisfy the requirements, and we preferred to encode a secret into a polynomial of degree 17.
The locking set is then projected onto the polynomial, forming the vault's genuine points. In the next step, random chaff points are generated. We should mention that, during chaff point generation, discarded genuine minutiae are also considered as if they were present in the vault. This is done to reduce false reject rate (FRR), since chaff points generated close enough (less than inter-ridge distance) to places where the discarded minutiae were located may match with minutiae of unlocking set thus harden decoding phase.

During the unlocking phase, 2 participants must present their minutiae. Each of the minutiae set is then matched with the vault. Matched vault points are discarded before subsequent match. Fig.3. demonstrates the vault (left) and the result of matching the vault with unlocking minutiae sets (right). As a result of matching, a candidate set of points is obtained, which is then used for decoding the secret.

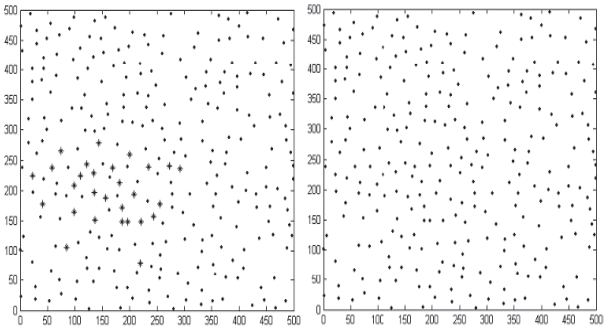


Fig.3. Fingerprint Fuzzy Vault: minutiae (stars) and chaff (dots) points are represented separately on the left for the sake of clarity. The actual vault, shown on the right, only contains the points, without any information about their source (genuine or chaff).

6. CONCLUSION

We presented a method explaining how to implement a secret sharing scheme using biometric fuzzy vault. The resulting scheme enhances the traditional secret sharing scheme proposed by Shamir [1], in that it benefits from the properties of biometrics (convenience & non-repudiation).

REFERENCES

[1] A. Shamir, "How to share a secret," Communications of the ACM 22, pp. 612–613, 1979.

[2] Juels and M. Sudan, "A fuzzy vault scheme, "in Proc. IEEE Int. Symp. Information Theory, A. Lapidoth and E. Teletar, Eds., 2002, p. 408.

[3] P. Tuyls, E. Verbitskiy, T. Ignatenko, D. Denteneer, and T. Akkermans, "Privacy protected biometric templates: Acoustic ear identification," Proceedings of SPIE: Biometric Technology for Human Identification Vol. 5404, pp. 176–182, 2004.

[4] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through on-line biometric identification," In IEEE Symposium on Privacy and Security, p. 408, 1998.

[5] C. Soutar, D. Roberge, S. Stojanov, R. Gilroy, and B. V. Kumar, "Biometric encryption using image processing," In Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II Vol. 3314, pp. 178– 188, 1998.

[6] Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," Proceeding of AVBPA (LNCS 2688), pp. 393–402, 2003.

[7] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosystems: Issues and challenges," 2004.

[8] H. Feng and C. Wah, "Private key generation from on-line handwritten signatures," Information Management & Computer Security, 10/4, pp. 159–164, 2002.

[9] A. Juels and M.Wattenberg, "A fuzzy commitment scheme," Conference on Computer and Communications Security, ACM Press. , pp. 28–36, 1999.

[10] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, “Biometric cryptosystems: issues and challenges,” Proc. IEEE (Special Issue on Multimedia Security for Digital Rights Management), vol. 92, no. 6, pp. 948–960, Jun. 2004.

[11] U. Uludag, S. Pankanti, and A. Jain, “Fuzzy vault for fingerprints,” in Proc. Audio- and Video-based Biometric Person Authentication, Rye Brook, NY, Jul. 2005, pp. 310–319, 310-319.