Secret Sharing Using Biometric Traits

Alisher Kholmatov, Berrin Yanikoglu, Erkay Savas and Albert Levi

Sabanci University, Istanbul, 34956, Turkey

ABSTRACT

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. There are many 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, 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 come together. The revealed secret can then be used for encryption or authentication (if the revealed key is verified against the previously registered value).

In this work we propose a method for the biometric based secret sharing. Instead of splitting a secret amongst participants, as is done in cryptography, a single biometric construct is created using the biometric traits of the participants. During authentication, a valid cryptographic key is released out of the construct when the required number of genuine participants present their biometric traits.

Keywords: Biometrics, Key, Sharing, Privacy, Cryptography, Fuzzy, Vault

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. 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 come together. The revealed secret can then be used for encryption or authentication (if the revealed key is verified against the previously registered value).

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] and implemented with fingerprints by Uludag et al..[3] Juels et al.'s construct is an example of recent research which focus on combining cryptography and biometrics (**bio-crypto systems**) to take advantage of the benefits of both fields.[2,4–7] 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. These bio-crypto systems also provide privacy, as the biometric templates are no longer kept in raw form.

Further author information: (Send correspondence to Alisher Kholmatov)
Alisher Kholmatov: e-mail: alisher@su.sabanciuniv.edu, web: http://students.sabanciuniv.edu/∼alisher
Berrin Yanikoglu: e-mail: berrin@sabanciuniv.edu, web: http://people.sabanciuniv.edu/berrin
Erkay Savas: e-mail: erkays@sabanciuniv.edu, web: http://people.sabanciuniv.edu/erkays
Albert Levi: e-mail: levi@sabanciuniv.edu, web: http://people.sabanciuniv.edu/levi

2. RELATED WORK

Secret Sharing

Shamir first proposed a method[1] known as *threshold scheme* for the secret sharing, which can be defined as follows in the most general form:

Definition: Let T, N be positive integers with $T \leq N$. A (T, N)-**threshold scheme** is a method of sharing a secret S among a set of N participants such that any subset consisting of T participants can reconstruct the secret S, but no subset of smaller size can reconstruct S.

Shamir's scheme is based on encoding the secret S as the constant term of a polynomial of degree $T-1$, whose coefficients are secret and smaller than a certain prime p. The polynomial can be given as follows:

$$P(x) = S + c_1 x + c_2 x^2 + \ldots + c_{T-1} x^{T-1} \pmod{p}$$

Then the polynomial is evaluated for N randomly chosen distinct integers $x_1, x_2, \ldots x_N \pmod{p}$ and each participant is given a pair (x_i, y_i) with $y_i \equiv P(x_i) \pmod{p}$, where $i = 1, 2, \ldots, N$. The prime p is known to all participants, but the polynomial $P(x)$ is kept secret. The polynomial, $P(x)$, whose degree is $T-1$ can be reconstructed if any T distinct evaluation pairs $(x_{L_1}, y_{L_1}), \ldots, (x_{L_T}, y_{L_T})$ are known using *Lagrange interpolation method*. Consequently, any T participants from the set of N participants can come together and reconstruct $P(x)$ and hence find out the secret S which is the constant term. The secret can be used in many ways in security context such as encryption, decryption, authentication, signatures, etc.

In this paper, we demonstrate the use of Juels et al.'s fuzzy vault scheme to implement biometrics-based secret sharing. In our proposed scheme, the distinct integers x_i $(i = 0, \ldots, N)$ for which the polynomial $P(x)$ is evaluated are not chosen at random any more, but derived from the biometrics of the participants and all of the evaluated pairs are kept in fuzzy vault as described in the subsequent sections.

Fuzzy Vault

Jules and Sudan proposed a scheme called *fuzzy vault*, which they call an error tolerant encryption operation.[2] Fuzzy vault scheme provides a framework to encrypt ("lock") some secret value (eg. cryptographic key) using an unordered set of locking elements as a key, such that some one who possesses a substantial amount of the locking elements will be able to decrypt the secret. It is based on the difficulty of the polynomial reconstruction problem. The encoding and decoding are done as follows:

Assume that Alice wants to secure her cryptographic key S (a random bit stream) using an arbitrary set of elements A. She selects a polynomial $P(x)$ of degree D and encodes S into the polynomial's coefficients. Encoding can be achieved by slicing S into non-overlapping bit chunks and then mapping these onto the coefficients. The mapping must be invertible meaning that the coefficients can be unambiguously mapped back to the corresponding bit chunks, which when concatenated will reconstruct the S. Then, Alice evaluates the polynomial at each element of her set A and stores these evaluation pairs into the set G, where $G = \{(a_1, P(a_1)), (a_2, P(a_2)), ..., (a_N, P(a_N))\}$, $a_i \in A$ and $|A| = N$. Finally, she generates a random set R of pairs such that non of the pairs in that set lie on the polynomial; and she merges the sets G and R into a final set, obtaining the vault, which then she makes public.

Now suppose that Bob has his own set of elements B and he wants to find out ("unlock") Alice's secret locked in the vault. He will be able to do so only if his set B largely overlaps with Alice's A so as to identify a substantial number of the pairs that lie on the polynomial, from the vault. Given at least $D+1$ pairs that lie on the polynomial, he applies one of the polynomial reconstruction techniques (eg. Lagrange interpolating polynomial) to reconstruct the polynomial and thus extract her secret S. If Bob does not know which of the points of the vault lie on the polynomial, it should be computationally infeasible for him to unlock the vault.

Whereas perturbation of a single bit in a key of a classical cryptosystem (eg. AES, RSA) hinders decryption completely, the fuzzy vault allows for some minor differences between the encryption & decryption keys, here the unordered sets used to lock & unlock the vault. This fuzziness is necessary since different measurements of the same biometric often result in quite different signals, due to noise in the measurement or non-linear distortions; for instance two impressions of the same fingerprint can be substantially different from each other. Besides, for

most of the known biometric signals, it is hard to establish a consistent ordering within measured features, and the number of these features may vary between different acquisition sessions (eg. missing/spurious fingerprint minutiae). However, fuzzy vault implementation using biometric traits is not straight forward, since it is not a trivial task to match template and query biometric signals (i.e. locking and unlocking sets, respectively) due to the presence of affine transformations and non-linear distortions,

Fuzzy Vault with Fingerprints

Uludag et al.[3] demonstrated a preliminary implementation of the fuzzy vault scheme using fingerprints. Minutia points of template & query fingerprints were used as locking & unlocking sets, respectively. More precisely, the values obtained by concatenation of corresponding x & y minutia coordinates were used as set elements.

Uludag et al. aimed to lock 128 bit long data (S). To make sure that the desired S was unlocked from the vault through an error-prone process, cyclic redundancy check bits (16 bits) were concatenated to S. Then, S, together with its check bits, was divided into non-overlapping chunks (16 bits each), giving the coefficients, of an 8th degree polynomial. To lock the secret, template minutiae set was projected onto this polynomial and random chaff points not lying on the polynomial are added, to form the vault. Based on their empirical estimations, they used only 18 minutia points and 200 chaff points.

To unlock the secret, i.e. reconstruct S, they first match the query minutia set with the abscissa part of the vault and identify candidate points lying on the polynomial. Since $D + 1$ points are required to reconstruct a polynomial of degree D, all possible 9 point combinations out of the candidate set are tried, to find the one with the correct check bits. S is successfully unlocked when the check bits verify. Authors report a 79% of correct reconstruction rate with 0% false accept rate.

To bypass the problem of matching the minutiae points and finding an upper bound to the scheme, the authors have used a fingerprint database where minutia points and the correspondence between template & query fingerprints were established by an expert. During their experiments, the minutiae sets of mating fingerprints were pre-aligned (i.e. rotated & translated) according to the established correspondence, and used as such.

3. PROPOSED SCHEME: SECRET SHARING USING FUZZY VAULT

In this section we present a secret sharing method[1] 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] and implemented with fingerprints by Uludag et al..[3] As the most general form, the method implements *threshold scheme*, revealing the secret when a predetermined number of the sharing parties collaborate.

The contribution of this paper is demonstrating how secret sharing can be implemented with biometrics, adding convenience to traditional secret sharing schemes.

Method

N people who want to share a secret S submit their biometric traits. We use their biometric signals G_1 through G_N and the secret S to construct the fuzzy vault, as follows: Assume for simplicity that the biometric signal is one dimensional such that $G_i = \{g_{i1}, g_{i2}, ...g_{iL_i}\}$, where i denotes the participant's ID; g_{ij} denotes a scalar measurement in the signal; and L_i denotes length of the signal. We assume that the length of each party's biometric signal is greater than or equal to some fixed length K, i.e. $L_i \geq K$. We select K out of L_i measured features and the rest are discarded.

The selection of K of the features can be done in a couple of different ways: according to the significance of corresponding features (i.e. select K most discriminative features for each party) or randomly, if each feature conveys an equal amount of information. During the selection process it may happen that some of the K features selected for different parties do clash (i.e. $g_{ah} = g_{bf}$). To resolve this, different strategies can be followed: i) if available, replace g_{ah} or g_{bf} with another feature of its corresponding party, which will be selected from previously discarded, ii) transform (eg. affine) g_{ah} or g_{bf}, iii) reduce K, or iv) reduce degree of the polynomial accordingly. Selection of a strategy will depend on biometric signal used, number of participants (N), and security level.

Next, we pick a polynomial $P(x)$ of degree D such that $(T-1)K \leq D \leq TK-1$, where $P(x) = c_D x^D + c_{D-1}x^{D-1} + \ldots + c_1 x + c_0$, c_i denotes the i'th coefficient of the polynomial. Coefficients may be determined

as described in Section 2, where S can be used as the constant term. The other way is to divide S into non-overlapping bit chunks and then map these chunks onto the coefficients.

After fixing the polynomial, we compute projections of each participant's biometric signal (i.e. G_i's) onto the polynomial, and obtain evaluation pair sets denoted by $A_i = \{(g_{ij}, P(g_{ij}), \ldots (g_{iK}, P(g_{iK})\}$. Next we create a set ($C$) of M random chaff points, where $C = \{(r_1, P(d_1)), \ldots, (r_M, P(d_M))\}$, where r_i and d_i are random numbers. Random points are generated in such a way that non of them lie on the polynomial i.e. $r_l \neq d_l$ and $r_l \neq g_{ij}$. Finally, the genuine sets A_i's and the set of chaff points C are merged and shuffled to constitute the fuzzy vault , FV.

The number of chaff points M must be selected such that identifying the required number of genuine evaluation pairs (i.e. $D + 1$ of these) without possessing the required number of genuine biometric traits will be computationally hard for an adversary or a malicious group of genuine participants (a group smaller than T).

When a group of T genuine participants decide to reconstruct the secret, they submit their corresponding biometrics, which are used to match the abscissa part of the fuzzy vault points. The identified points of the vault are then used for the polynomial reconstruction, and the secret will be extracted, in the way described by.[3] Security analysis as well as implementation details and experimental results of proposed method using fingerprints will be provided in the full version of the paper.

4. SUMMARY AND CONCLUSION

We have presented a method explaining how to implement a secret sharing scheme using biometric traits and the framework proposed by Juels et al..[2] The resulting scheme enhances the traditional secret sharing scheme proposed by Shamir,[1] in that it benefits from the properties of biometrics.

Even though our method is a relatively straightforward extension of the fuzzy vault scheme implementation by Uludag et al.,[3] it is an important application of the fuzzy vault and has been first to implement secret sharing using biometrics. Furthermore, the difficulties in expanding previous work to multiple people and threshold scheme is non-trivial.

ACKNOWLEDGMENTS

We would like to thank TÜBİTAK (The Scientific and Technical Research Council of Turkey) for its Ph.D. fellowship support granted to Alisher Kholmatov through out this research.

REFERENCES

1. A. Shamir, "How to share a secret," *Communications of the ACM* **22**, pp. 612–613, 1979.
2. A. Juels and M. Sudan, "A fuzzy vault scheme," *IEEE International Symposium on Information Theory* , p. 408, 2002.
3. U. Uludag, S. Pankanti, and A. Jain., "Fuzzy vault for fingerprints," *Proceeding of International Conference on Audio- and Video-Based Biometric Person Authentication* , pp. 310–319, 2005.
4. 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.
5. 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.
6. 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.
7. J. 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.