Fuzzy Fingerprint Vault

Umut Uludag and Anil K. Jain
Computer Science and Engineering, Michigan State University, East Lansing, MI, 48824, USA
{uludagum, jain}@cse.msu.edu

Abstract

Biometrics-based authentication has the potential to eliminate illegal key exchange problem associated with traditional cryptosystems. In this paper, we explore the utilization of a fingerprint minutiae line based representation scheme in a new cryptographic construct called fuzzy vault. Minutiae variability is quantified for a fingerprint database marked by a human expert.

1. Introduction

In traditional cryptography, one or more keys are used to convert the plain text (data to be encrypted) to cipher text (encrypted data): the encrypting key(s) maps the plain text to essentially a sequence of random bits, that can be mapped back to the plain text using the decrypting key(s). Without the knowledge of the correct decrypting keys, the conversion of cipher text to the plain text is *infeasible* (considering time and cost limitations) [1].

Current cryptographic algorithms (e.g., Advanced Encryption Standard (AES) [2], RSA [1]) have a very high proven security but they suffer from the key management problem. All these algorithms fully depend on the assumption that the keys will be kept in absolute secrecy. If the secret key is compromised, the security provided by them immediately falls apart. Another limitation of the these algorithms is that they require the keys to be long and random for higher security, e.g., 128 bits for AES [2], which makes it impossible for users to memorize the keys. As a result, the cryptographic keys are stored somewhere (e.g., in a computer or on a smart card) and released based on some alternative authentication mechanism. The most popular authentication mechanism used for this purpose is based on passwords, which are again cryptographic key-like strings but simple enough for users to remember. Hence, plain text (e.g., multimedia content, email records, financial records, and private encryption keys) protected by a cryptographic algorithm is only as secure as the passwords (weakest link) used for authentication that release the correct decrypting key(s). Simple passwords compromise security; complex passwords are difficult to remember and expensive to maintain. Also, passwords are unable to provide non-repudiation.

Many of these limitations can be eliminated by incorporation of better methods of user authentication. Biometric authentication [3], [4] refers to verifying individuals based on their physiological and behavioral traits such as face, fingerprint, voice, etc. 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 by providing the complete authentication mechanism or by securing the traditional cryptographic keys that contain the plain text.

An interesting cryptographic construct, called *fuzzy vault*, was proposed by Juels and Sudan [5]. This construct, as explained in later sections, has the characteristics that make it suitable for applications that combine biometric authentication and cryptography. In this paper, we explore the use of a fingerprint minutiae representation scheme in this construct (that we call *fuzzy fingerprint vault*). In Section 2, we summarize the related literature. In Section 3, we give specifications about the line-based fingerprint minutiae representation scheme that can be used in securing the fuzzy fingerprint vault. In Section 4, we objectively characterize the variations in fingerprint data using a database that has been marked by a human expert. This helps in quantifying the amount of tolerance that should be introduced into the vault construction. Section 5 concludes the paper.

2. Previous Work

Juels and Sudan's fuzzy vault scheme [5] is an improvement upon the previous work by Juels and Wattenberg [6]. In [5], Alice can place a secret value κ (e.g., private encryption key) in a vault and lock (secure) it using an unordered set A. Bob, using an unordered set B, can unlock the vault (access κ) only if B overlaps with A to a great extent. The procedure for constructing the fuzzy vault is as follows: First, Alice selects a polynomial p of variable x that encodes κ (e.g., by fixing the coefficients of p according to κ). She computes the polynomial projections, $p(A)$, for the elements of A. She adds some randomly generated chaff points that do not lie on p, to arrive at the final point set R. When Bob tries to learn κ (i.e., finding p), he uses his own unordered set B. If B overlaps with A

substantially, he will be able to locate many points in R that lie on p. Using error-correction coding (e.g., Reed-Solomon [7]), it is assumed that he can reconstruct p (and hence κ). The security of the scheme is based on the infeasibility of the polynomial reconstruction problem (i.e., if Bob does not know many points that lie on p, he can not feasibly find the parameters of p, hence he cannot access κ). Note that since this fuzzy vault can work with unordered sets (common in biometric templates, including fingerprint minutiae data), it is a promising candidate for biometric cryptosystems.

Clancy et al. [8] proposed a *fingerprint vault* based on the fuzzy vault of Juels and Sudan [5]. Using multiple minutiae location sets (typically 5), they first find the canonical positions of minutia, and use these as the elements of set A. They added the maximum number of chaff points to find R that locks κ. Note that their system inherently assumes that fingerprints (the one that locks the vault and the one that tries to unlock it) are pre-aligned. This is not a realistic assumption for fingerprint-based authentication schemes (even for iris biometric, this is not true), and limits the applicability of their scheme.

The registration of fingerprints is one of the biggest barriers in the implementation of any fingerprint vault (or any biometrics-based vault). In addition to the possible translational and rotational transformations (see Section 4) and non-linear deformation between two impressions of the same finger, it is possible to have different number of feature points (e.g., missing or spurious minutiae).

In the next section, we propose a *fuzzy fingerprint vault* that uses minutiae lines to lock a secret, using Juels and Sudan's fuzzy vault scheme [5] as the basis.

3. Line-based Minutiae Features

We propose to use a variant of the line-based minutiae representation scheme proposed by Malickas and Vitkus [9] in securing the fuzzy fingerprint vault. Fig. 1 shows the block diagram of the proposed system.

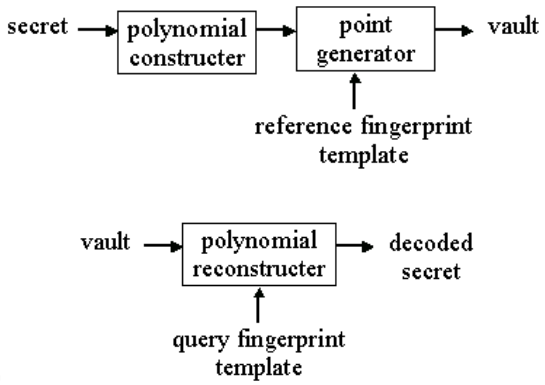

Fig. 1. System block diagram: (a) locking the secret, (b) unlocking the secret.

As explained above, Clancy et al. [8] used only the location of individual minutiae as the locking and unlocking sets for their fingerprint vault. Whereas, in [9], both location and angle of minutiae are used to extract lines for forming the templates. Malickas and Vitkus' method is based on an earlier paper [10] on generic image registration. The main idea is to decompose the registration process into elementary stages and to eliminate only a single transformation parameter (e.g., scaling, translation, or rotation) at each stage [9]. Let I and I' denote the two images to be registered. Assume the current stage of transformation is T_θ. Consider a pair of features f (from I) and f' (from I') of the same type (e.g., point, line). If f and f' have the attributes α and α' (e.g., length, angle) such that $\alpha' = g_\theta(\alpha)$, where g is a bijective function, the parameter θ is called *observable* with respect to the associated feature class and attribute class. The function g allows the current parameter to be estimated as $\theta = h(\alpha, \alpha')$. Each feature pair ($f$, f') votes for one estimate of the parameter. The final transformation parameter is estimated by locating the maximum of the *consensus function* $H(\theta)$ that accumulates the votes.

Malickas and Vitkus [9] assume that minutiae locations (x, y) and angles (φ) are given for reference and query fingerprints, respectively, as:

$$Q = \{(x_1^K, y_1^K, \varphi_1^K), ..., (x_N^K, y_N^K, \varphi_N^K)\} \text{ and}$$
$$P = \{(x_1^L, y_1^L, \varphi_1^L), ..., (x_M^L, y_M^L, \varphi_M^L)\}.$$

Then, the line K_{ij} between minutiae i and j of reference fingerprint is defined as

$$K_{ij} = (x_i^K, y_i^K, \varphi_i^K, x_j^K, y_j^K, \varphi_j^K, d_{ij}^K, \Phi_{ij}^K, \omega_i^K, \omega_j^K)$$

where the first three fields code minutia i, the second three fields code minutia j, d_{ij}^K is the distance between minutiae i and j, Φ_{ij}^K is the line direction and the last two fields code the angles between the line directions and minutiae directions.

Considering that the same sensor is typically used for capturing reference and query fingerprints, estimating the scaling parameter is not necessary. The rotation angle θ is observable for the line direction Φ_{ij}^K via

$$\Delta\Phi_{K_{ij}L_{kl}} = (\Phi_{ij}^K - \Phi_{kl}^L) \bmod 360 .$$

Using the consensus function, it is possible to obtain an estimate for θ. By rotating the lines from reference fingerprint according to this estimate, K_{ij}^R line set is found. Finally, the translation (Δx , Δy) is observable for minutiae locations via

$$\Delta x_{K_{ij}L_{kl}} = \frac{(x_i^R - x_k^L) + (x_j^R - x_l^L)}{2}$$
$$\Delta y_{K_{ij}L_{kl}} = \frac{(y_i^R - y_k^L) + (y_j^R - y_l^L)}{2}.$$

Using this representation for the proposed fuzzy fingerprint vault, we plan to use quantized location and angles, to account for non-linear distortion and eliminate the necessity to use two line feature sets.

4. Experimental Results

In this section, we assess the requirements of a typical fingerprint-based vault application, in terms of the variability of the fingerprint minutiae data. We used a moderate sized database (denoted as GT henceforth) consisting of 450 mated fingerprint pairs collected in a realistic setting and acquired in multiple sessions. The images were obtained with a DBI optical sensor with 500 dpi resolution. The minutiae in all of the images were identified (their location and angle) by a human expert. Further, the expert determined the minutiae correspondence information between minutiae of every mated pair. We decided to use a database where the features were extracted by a human expert since we did not want the characteristics of an automatic minutiae extractor to affect the statistics we wanted to compute. As a result, the minutiae information that we use is the *ground truth* (hence, the database is named GT).

In the following, we present several statistics that we calculated from this database. Note that these statistics are useful in assessing the applicability of fingerprint minutiae features for any fingerprint-based vault.

Fig. 2 shows the minutiae distributions for three sets: total number of minutiae in the images, number of matching minutiae in the images, and the number of minutiae added-to/missed from the originals. We see that in this database, the average number of minutiae is 40. Note that, the missing and added minutiae may eliminate some possibilities for using minutiae representation as locking keys, since even if all of the translational, rotational, and non-linear distortions in the prints are eliminated, the representations for reference and query will not be the same.

We measured the translational and angular differences (measured in pixels and degrees, respectively) between mated minutiae in all of the fingerprint pairs. Note that no preprocessing (e.g., aligning) of images was done here. We wanted to analyze the difference between minutiae pairs originating from the same finger before carrying out such operations. Note that, inherently, such preprocessing is not applicable to fuzzy vault, as the construct inputs just one feature set, not two that can be compared, aligned, etc. We found that the translational difference can be quite large, with a mean difference of nearly 20 pixels. The maximum difference can be as much as 45 pixels, with a relatively high probability of approximately 0.09. For assessing the magnitude of the necessary alignment, the rigid transformation (optimal in the Least Mean Square sense) between mated fingerprint pairs is estimated using the ground truth information. This yields 2D translation and rotation components of the transform. We found that a translation of nearly 20 pixels and a rotation of nearly 3 degrees are needed, on the average, for aligning (hence effectively eliminating) the cited rigid transform. Then, we measured the translational and angular differences between the minutiae of mated pairs after this alignment. As expected, the translational differences decrease considerably, but there is still a mean difference of nearly 4 pixels. This *residual* difference may create correspondence problems for fingerprint-based vaults, since even the alignment is not able to completely eliminate the variability in minutiae features.

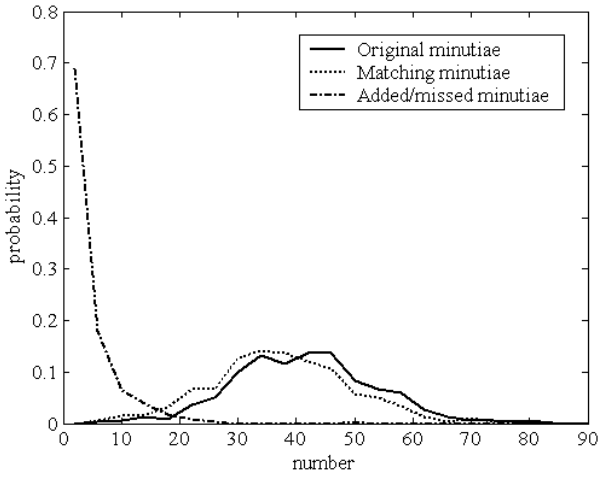

Fig. 2. Minutiae distributions: the curves show the distributions for the number of original minutiae, matching minutiae and added/missed minutiae.

Fig. 3 shows two fingerprint images from the GT database, along with the overlaid lines, obtained via the method given in Section 3. Using the calculated rotation (see Fig. 4) and translation consensus functions, the rotation angle is found to be 2.8 degrees, horizontal translation is found to be 10 pixels and vertical translation is found to be 31 pixels. These values agree closely with the actual parameters. We are currently working on

obtaining performance estimates for the proposed fuzzy fingerprint vault system.

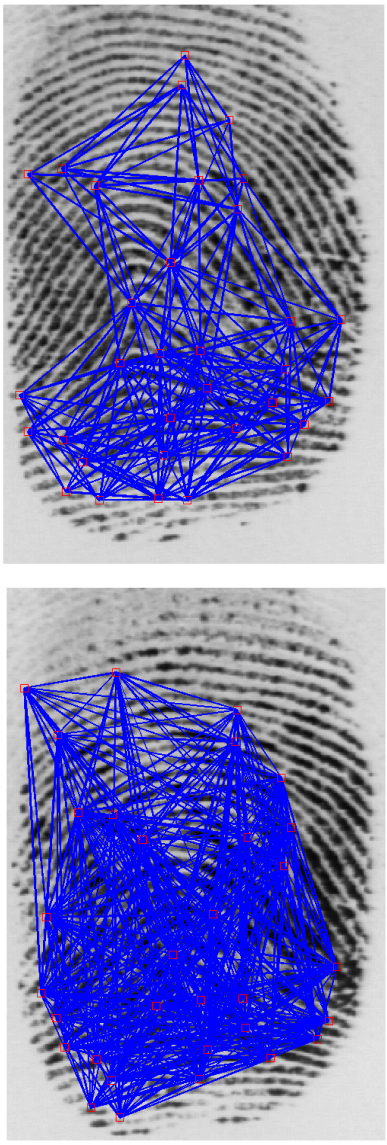

Fig. 3. Fingerprint images with overlaid minutiae lines (top: reference, bottom: query).

5. Conclusions

Based on a new cryptographic construct called fuzzy vault, a fuzzy fingerprint vault system using fingerprint minutiae based lines is proposed. This construct has several characteristics (such as order invariance) that increase its applicability for use with biometric data. Using a fingerprint database marked by a human expert, the variability of minutiae data (before and after alignment) and the alignment parameters are quantified.

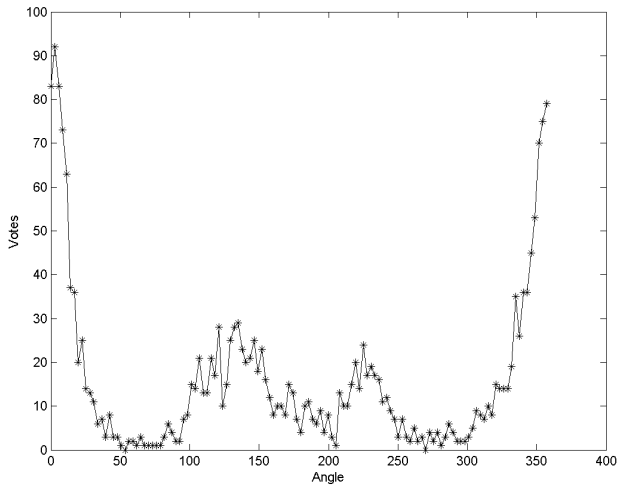

Fig. 4. Rotation consensus function for the fingerprint pair in Fig. 3.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3. Ed., Prentice Hall, 2003.

[2] NIST, Advanced Encryption Standard (AES), 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[3] A. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*, Kluwer, 1999.

[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.

[5] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", *Proc. IEEE Int'l. Symp. Information Theory*, A. Lapidoth and E. Teletar, Eds., pp. 408, 2002.

[6] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme", In G. Tsudik, Ed., *Sixth ACM Conf. Computer and Comm. Security*, pp. 28-36, 1999.

[7] S. Lin, *An Introduction to Error-Correcting Codes*, Prentice-Hall, 1970.

[8] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure Smartcard-Based Fingerprint Authentication", *ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, pp. 45-52, 2003.

[9] A. Malickas and R. Vitkus, "Fingerprint Registration Using Composite Features Consensus", *Informatica, Institute of Mathematics and Informatics (Vilnius)*, vol. 10, no. 4, pp. 389-402, 1999.

[10] C. Shekhar, V. Govindu, and R. Chellappa, "Multisensor Image Registration by Feature Consensus", *Pattern Recognition*, vol. 32, pp. 39-52.