

Mobile Fingerprint Template Protection: Progress and Open issues

J. Hu

School of Computer Science and IT, RMIT University
Melbourne, VIC 3001, Australia
Email: Jiankun.Hu@rmit.edu.au

Abstract- In this paper, we will discuss relevant research progress in the field of mobile fingerprint template protection. The discussion will cover three main stream schemes called biometric key generation, fuzzy schemes and noninvertible transforms. Some pitfalls and open issues for future research in these areas are pointed out.

I. INTRODUCTION

Information security has been a growing concern in recent years accompanied by ever increasing reports on security breaches. A fundamental component in a security system is authentication which provides effective access control to the system resources. Conventional authentication mechanisms are primarily based on what you know, i.e., secret password or personal identity number (PIN), and/or in conjunction of what you have (tokens). There are several problems with these mechanisms. First, tokens can be easily lost. Secondly, it is difficult to manage passwords. A long password can have a strong security but hard to memorize. A short password is easy to memorize but compromises the security. Usability is also an issue as many different passwords are needed for many accounts. Finally, the best this authentication mechanism can do is verifying that the presenter possesses the token or knows the PIN. There is no way knowing whether this presenter is really the owner of the PIN or the token. Biometrics shows to be a promising solution in addressing the above issues. Biometrics authentication is based on people's physiological and behavioral characteristics such as fingerprint, keystroke, face, hand geometry etc. In principle, biometrics cannot be forgotten or lost, difficult to duplicate or share among different users. Biometrics authentication system requires physical presence of the individual in presenting the biometrics. The most popular application of biometric authentication is using biometric templates where individual biometrics is stored. Therefore the mobile biometric template itself has become a critical issue of security. In the remaining of this paper, mobile template protection refers to the protection of sensitive data including fingerprint biometrics stored in a mobile device. In most cases, it refers to the protection of cryptographic keys stored in the mobile device using fingerprint biometrics technologies. This paper will present research issues related to the mobile fingerprint biometric template protection. The remaining sections of this paper are: Section II provides coverage of Evolution of

Mobile Template Protection, and Section III is devoted to Discussions. The final section is the Conclusions.

II. EVOLUTION OF MOBILE FINGERPRINT TEMPLATE PROTECTION

In principle, a cryptosystem based on mobile biometric fingerprint authentication has the following operational flow chart as shown in Fig. 1. A fingerprint is captured via live scan and then its features are retrieved. This process is usually conducted within an external terminal such as an ATM machine that is physically secure and computing resource rich. In the current commercial market, the predominant or perhaps exclusive fingerprint features are minutia because of the maturity of this technology. The retrieved fingerprint features are then fed into the smart card for further processing. Within the smart card, the biometric template that has been stored prior will be compared with the retrieved fingerprint features of the captured fingerprint. If a match is made, the cryptographic key that has been stored prior will be released to perform conventional cryptographic applications such as encryption of messages and communication with application servers.

From this architecture it is clearly observed that two secrets, namely private cryptographic key and fingerprint template are stored in the smart card which is vulnerable to attacks. In the first generation of smart card based applications, which is still the most popular one at the moment, the biometric authentication component is not included. Because smart cards are easily lost or stolen, the attackers can have the physical access to the smart card. With such a physical access, hardware attacks or API attacks on the token's software can retrieve the private key stored in the smart card [1]. Encryption of the private key seems to be a solution. However, the management of the decryption key is problematic. A common practice is to use a password for the decryption. However, the whole system is just as strong as the password which will inherit the same troubles as the password. The emerging mobile biometric authentication application embeds biometric authentication such as fingerprint authentication component. While the inclusion of the embedded biometric authentication component can enhance the overall security of the system, e.g. lost token cannot be used directly, it generates more security problems if attackers have the physical access to the smart card that embeds a biometric template.

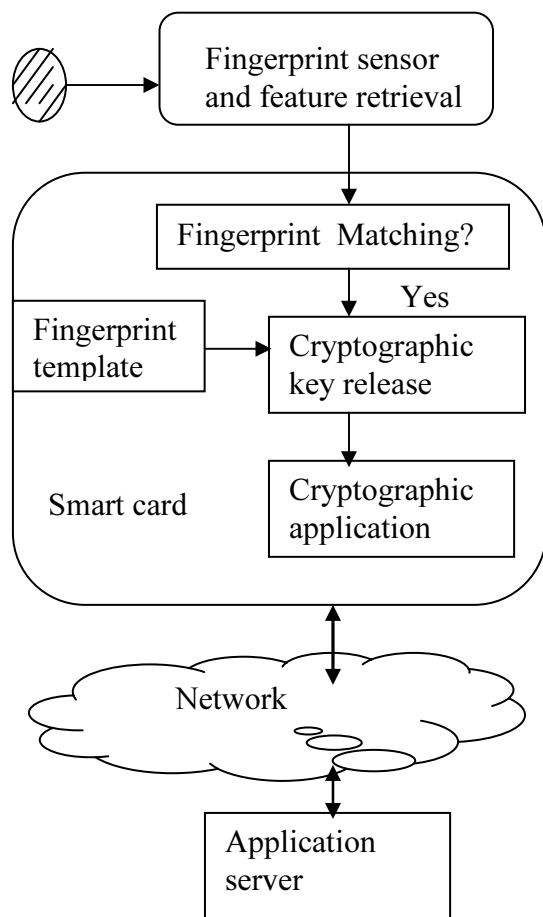


Fig. 1 Operational flow chart for mobile fingerprint template authentication based applications

The first generation biometric smart card adopts a “key release” approach which needs to store a secret key and biometric template separately. This approach will inherit the same problem of aforementioned hardware attacks. Furthermore, because the secret key releasing process is triggered by the “Yes-matching” signal sent from the biometric authentication component, it is possible to bypass this authentication process by injecting a “Yes-matching” signal to the component that contains the secret key if hardware physical access is available. Even worse, this first generation mobile biometric template adds a new issue, i.e., how to protect the embedded biometric features. Biometrics cannot be revoked or canceled. If a biometric is lost, it is compromised forever. Also an individual has very limited biometrics. Ross, et al [2] has demonstrated that a full fingerprint can be restructured from the minutiae points. Therefore the protection of the mobile fingerprint template is becoming a more serious issue. Traditionally, research efforts in protecting mobile fingerprint template are classified into four categories namely salting, key generation and key binding, and non-invertible transform. In this paper, they are further classified into following two general categories: (1) Technologies that do not require the

embedded storage of private cryptographic key and/or fingerprint features. (ii) Technologies that store transformed biometric features.

A. Methods that Do Not Require the Storage of Biometric Features and Secret key

Direct biometric key generation

To avoid the risk of storing the cryptographic private key and biometrics in the mobile template, approaches have been proposed to derive cryptographic private keys from the live scan fingerprint [3][5][6][7]. Biometric key generation schemes normally refer to those that derive cryptographic keys directly from biometrics [4]. Davida et al [3] made the first attempt in providing a framework to generate cryptographic keys from biometrics without stored references. The scheme uses open token-based storage of user-specific error correction codes to rectify uncertainties in the test data. An application example using Iris biometric is provided.

It is well known that fingerprints captured by a sensor have nondeterministic presentations. However, cryptography requires the exactness of the key, which makes the binding between the biometrics and the cryptographic key very challenging. As acknowledged by Davida [3], the biocryptosystem discussed above relies on high accuracy of the retrieved biometric features. Although this scheme has been successfully applied to the Iris case, it is not directly applicable to the fingerprint scenario. This is because that the existing fingerprint features such as the most popular feature, minutiae, exhibit far more variations than the Iris biometrics. Farooq et al [22] has proposed to address this issue by encoding minutiae triangles. However, this scheme has to use a unique personal key for each individual to activate the system. It is unclear how this extra key is managed.

Han, Yu and Hu [5] have proposed an image based biometric encryption scheme. A private key is derived from the image pixel distribution and some global structure of the fingerprint such as singular points and frequency of ridges in fingerprint. Intuitively aggregated features proposed above tend to filter out fingerprint variations to a certain extent. Statistics testing for the FAR (False Acceptance Rate) and FRR (false Rejection Rate) performance has not been reported. This scheme also requires a reasonably accurate registration.

In order to address the issue of fingerprint image distortion, Han, and Hu et al [6] have introduced a concept of “fictitious triangle”. The construction of a fictitious triangle is illustrated in Fig. 2 where C, D, E, F, and F represent 5 minutiae near the core. Calculate the distances between any two minutiae points. A fictitious triangle is constructed with the three longest lines, which is shown in Fig. 2b.

The length of the maximal side x_1 , the minimal angle, α_{min} , and the medial angle α_{med} are selected as the fingerprint features.

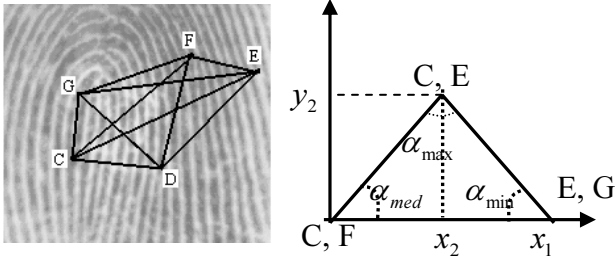


Fig. 2 Minutiae triangle in a fingerprint image:
 (a) FVC2000 Db1_a_8; (b) A minutiae triangle

An error-tolerance quantization scheme is provided to transform these features into binary digits where quantization parameters are experimentally determined by using the FVC2000 database. A 9-bit PIN is constructed where the first 6 bits correspond to the type of the minutiae involved in the three sides of the fictitious triangle and 3 bits are from the quantization process. 50 fingerprints with 8 impressions of each finger are used to test the proposed scheme. With a carefully tuned threshold, 100% Genuine Accept Rate (GAR) has been achieved. The idea behind the concept of “fictitious triangle” is that the length parameter of a long line tends to less affected by distortion and the features of a triangle are invariant against shift and rotation. This is a promising approach. However, there are many open issues. For example, how to select an appropriate quantization threshold? The current threshold chosen is determined by the absolute boundaries through the training process which is optimistic where a high false acceptance tends to occur. The false acceptance rate performance has not been provided. Overall, not many results on direct key generation from fingerprint have been reported. This is perhaps because of the wide variations of existing fingerprint features such as minutiae etc.

Information hiding schemes

Another way of providing cryptographic keys through biometric authentication without storing secrets is to hide the secrets within public available information. As the secret, normally a cryptographic key, is retrieved through biometric matching process, it is also referred to as key binding.

Soutar *et al* [7] proposed a scheme to generate a key from biometric fingerprints, which were the first to commercialize this technology into a product--- Bioscrypt. This scheme extracts the phase information from a fingerprint using a Fourier transform and applies majority coding to reduce the feature variation. Instead of generating the key directly from fingerprint features, a secret key is locked with a biometric sample by forming a phase-phase product. This product can be unlocked by a fingerprint captured from the genuine finger. However, no performance evaluation has been reported [8]. Juels and Wattenberg [21] have proposed a “fuzzy commitment” scheme to tolerate more variations in the biometric characteristics. In this scheme, the user at the enrollment time selects a secret message k . Assume d be the difference vector between the user biometrics and key X

and k . The fuzzy commitment within which the message has been hidden consists of d and $y = \text{hash}(k)$, where hash is a one way hash functions such as SHA-1. At the decryption session with a new biometric sample Y , $Y + d$ is used to decode the nearest codeword k' . With the help of error-correcting techniques, it is hoped that the error in k' can be corrected to obtained the original message k [4]. The major issue with this scheme is that it requires the biometric representations X and Y to be ordered so that their correspondence is obvious. Though this fuzzy commitment scheme applies to many biometrics, the ordering feature requirement is impractical for fingerprint minutia as it is very common to have a fingerprint with missing minutia and fake minutia.

Jules and Sudan [9] proposed a *fuzzy vault* scheme to address this ordering problem. The scheme works as follows: Suppose Alice wants to lock a secret k under set A . She selects a polynomial p in a single variable x such that p encodes k in its coefficients. Treating the elements of A as distinct x -coordinate values, she computes evaluation of p on the elements of A . Alice then creates a number of random chaff points that do not lie on p . The entire collection of points, we call R set, constitute a commitment of p . The set A can be viewed as identifying those points in R that lie on p , thus reconstructing p and the secret k . The chaff points have the effect of concealing p from an attacker.

If Bob has a set B that overlaps substantially with A , then he can identify many points in R that lie on p . Therefore Bob can recover a set of points that is largely correct but perhaps contains a small amount of noise. Using error correction, he is able to reconstruct p exactly and retrieve the secret k consequentially. If B does not overlap substantially with A , it is computational infeasible for Bob to retrieve k .

This scheme has established a general theoretic framework for mobile biometric template protection although it does not even discuss any specific applications in biometric authentication. It is considered as the best framework in addressing bio-cryptography [23]. Clancy *et al* [10] proposed a fingerprint fuzzy vault which provided a concrete method for the implementation of the fuzzy vault framework. In this fingerprint fuzzy vault, minutiae positions are extracted from each fingerprint. To address the problem of minutiae locations, a bounded nearest-neighbor algorithm is used for the minutiae matching. These genuine minutiae plus a number of chaff points will constitute a fuzzy vault. Reed-Solomon error-correcting codes are used for error correction. A false negative rate of about 20—30% has been reported. One issue with this approach is that fingerprint registration or alignment is needed to find the correspondence minutiae pair between the query fingerprint and the fingerprint template. This is problematic as we do not want to reveal any information about the stored template.

A transformed template can prevent information leakage. However, the transformed template does not have sufficient information for the alignment [11].

Uludag *et al* [11][12] proposed a fingerprint fuzzy vault that uses fingerprint orientation field to assist alignment or registration. The authors acknowledge that the orientation field does not reveal the minutiae template. Also a more direct method for the implementation of the fuzzy vault framework is provided. The basic idea is to convert the secret key k into a secret message sc via error-correction encoding such as Cyclic Redundancy Check. Then divide a secret message sc into non-overlapping 16-bit segments and use each segment as a polynomial coefficient

$$p(u) = c_0 + c_1u + \dots + c_{D+1}u^D \quad (1)$$

$$c_i, \quad i=1, \dots, D+1$$

Use one 8-bit integer to represent x or y coordinate of a minutia. Concatenate them into a 16-bit integer as an input u . A genuine set is established as in the following

$$G = \{[u_1, p(u_1)], \dots, [u_N, p(u_N)]\}, \quad u_i \neq u_j \quad (2)$$

We then generate Chaff Point Set

$$C = [(c_1, d_1), \dots, (c_M, d_M)], \quad d_i \neq p(c_i) \quad (3)$$

A fuzzy Vault set is generated by scrambling the order of pairs from G and C which leads to

$$VS = [(v_1, w_1), \dots, (v_{N+M}, w_{N+M})] \quad (4)$$

For decoding, given an input fingerprint sample, we retrieve N minutia points

$$u_1^*, \dots, u_N^* \quad (5)$$

Add the matching list

$$(v_i, w_i) \quad \text{if} \quad u_i^* = v_i \quad (6)$$

Coefficients can be found directly if the length of matching list is larger than the order of the polynomial. Reconstruction of the polynomial is infeasible if no sufficient genuine pairs are found. This proposed scheme has been evaluated on DB2 database of FCV 2002 study [13]. With two impressions per finger for decoding it can achieve GAR to 84.5% at 0% FAR. Although orientation field oriented registration can avoid storing the minutiae template, it is unclear how distortion would affect the results. The centre of mass of maximum curvature points used for the registration in this scheme tends to be sensitive to the accurate locations of

these points. This could be problematic as the detection of a maximum curvature point is very sensitive to noise.

Uludag and Jain [14] have made an attempt in addressing the registration issue by adopting line-based minutiae features proposed by Malicks and Vitkus [15]. ROC performance has not been provided. It should be pointed out that this line based registration scheme needs both location and angle of minutiae. Boulton *et al* [23] has proposed the concept of revocable fingerprint biotokens. The biometrics uncertainty removal in this scheme depends heavily on the Bozorth matcher where matching is based on the intra-fingerprint minutia pair table and inter-fingerprint minutia pair table. To address the revocable issue and the issue of doppelganger threat, a user passcode can be added to the biotoken. This is actually the idea of biometric salting techniques [24][25]. Apparently the Bozorth matcher is not suitable in the mobile environment due to its high demand in computing resource. Also simple line-based schemes that rely on minutia angle such as [14][15][23] have problems in dealing with elastic distortion. Our preliminary investigation using the VeriFinger toolkit from Neurotechnologija Ltd [16] shows that it is common to have 20% difference in minutiae distributions retrieved from different impressions of the same finger. Also minutia angles detection are very unreliable. Also many fuzzy schemes are subject to an attack if the same print is used multiple times [23][26]. We believe that a non-registration dependent and also elastic distortion tolerant fuzzy fingerprint vault approach is desirable.

B. Technologies that store transformed biometric features

Another main stream of mobile biometric template protection is using transformed biometric features, which is also called a approach of cancelable fingerprint templates [3][4][5][6][7][17]. The idea of cancelable fingerprint template is to use noninvertible (cancelable) transforms to transform biometrics into a new domain where authentication is conducted. The transformation can be performed either in the signal domain or in the feature domain. If a biometric is compromised, it can be easily replaced with another transformation, thus providing revocability. It can also prevent cross-matching between the database as each application can have a different transformed biometric. Also one-way transformation can prevent attackers recover the original fingerprint features [17].

In addition to the requirement of noninvertible transform, there are following challenges in designing a cancelable template scheme [17][19]: (i). Registration. In order to ensure matched minutiae pair also overlaps in the transformed domain, an accurate registration is needed. (ii) Intrauser variability tolerance. The probability of a false reject should ideally not increase in the transformed domain. (iii) Entropy retention. The probability of a false accepts should not increase in the transformed domain. Ratha *et al* [17] proposed three transform methods: Cartesian, polar, and surface.

Cartesian Transformation

In this scheme, a Cartesian framework is built with the position of the singular point as the origin and the x -axis is aligned with the orientation of the singular point. This coordinate system is partitioned into cells of fixed size and numbered in a fixed sequence. Minutiae are distributed, according to their locations, among these cells. When the cell positions are changed, all the minutiae within the cells retain their relative positions, i.e., only cell-minutiae binding relationship changes. For noninvertible characteristics, it is required that more than one cell be mapped to the same cell.

Polar Transformation

The idea is similar to the Cartesian transformation. The difference is that minutiae positions are measured in polar coordinates with reference to the core position. The cell partition and transformation are based on the concept of polar sector.

Functional Transformation

Both the Cartesian and polar transformation suffer a drawback that a small change in minutiae position in the original fingerprint can lead to a large change in the transformed domain if the point crosses a sharp boundary. This will lead to increased intra-user variation [17]. It is believed that smooth but noninvertible transformation would achieve a higher performance [17]. In [17], two surface folding functions are designed. Experiments are conducted using the IBM-99 optical database for transform analysis. The database used has 188 fingerprint pairs after rejecting poor quality fingerprints. Compared with matching performance without transformations, functional and polar transforms are slightly lower. Cartesian transform has significantly downgraded the performance.

III. DISCUSSIONS

- Fuzzy fingerprint vault based approach is very promising and is currently predominating. However, a pitfall exists which has never been reported in the literature. This issue is related to the application of error-correcting component adopted in the fuzzy fingerprint vault architecture. As adopted in all existing fuzzy fingerprint vaults, the secret message is encoded using error-correction coding. At the decoding side, a message has been decoded from the polynomial decoding and then is sent through error-correction decoder for recovering the original message. The principle of error-correction coding assumes that an original digital message has been distorted by certain bits which have made the distorted message fails closest to the correct codeword (Hamming Distance). While in the fuzzy fingerprint vault system, the secret k is locked in the vault without experiencing any distortion. To find the

coefficients of polynomial of degree n , $(n+1)$ unique projections are necessary. If the size of matched query minutiae set is smaller than $(n+1)$, it results in authentication failure. Otherwise, a number of sets of coefficients will be generated which leads to a set of secret k' unlocked. Finally error-correction code will make error corrections. The issue here is that the error or noise distortion is induced by the variation of fingerprint minutiae. The difference between minutiae variation and communication channel variation is that the minutiae variation can be introduced because of the genuine difference in two fingerprints, i.e., two different fingers. While in communication case, error is definitely introduced by genuine noise. In the minutiae variation case, there is no way to tell whether the error between true secret k and the unlocked secret k' is introduced by the genuine noise or by genuine different fingerprints. In fact, the unlocking set is selected from the pre-stored fuzzy vault. An error in the decoded secret implies that chaff points have been used in the decoding process. It is more likely a non-genuine fingerprint has been presented. Error-correction coding seems to be misleading.

- In principle, fuzzy fingerprint vault can address minutiae missing and fake minutiae effectively as it requires only enough of genuine minutiae to unlock the secret. However, it cannot solve the distortion problem and also relies on accurate registration. As discussed above, error-correction cannot resolve this issue as what it has been designed for. New mechanisms are needed to address this distortion issue. Exploring biometric fingerprint features that are distortion tolerant and registration error tolerant seems to be a logic direction.
- Transformation based approaches enjoy the benefit of the ease of producing cancelable templates. However, its dependence on the accurate registration presents a challenge as accurate registration has long been considered as a very difficult problem. Wang and Hu et al [18] provided a new fingerprint model which is promising in addressing the singular point detection. As in the context of mobile template protection, information that can leak critical features of the fingerprint cannot be stored on the template. This will make transformation based approach even more challenging to find the accurate singular point detection. We believe that features that are registration error tolerant can help resolve this issue.

IV. CONCLUSIONS

In this paper, research issues related to mobile fingerprint template protection have been presented. Both biometric key generation methods and fuzzy fingerprint vaults do not require a fingerprint template stored on the smartcard. We believe that the fuzzy fingerprint vault scheme can effectively deal with the case of minutiae missing and/or

fake minutiae, but is limited in addressing minutiae distortion. The error-correction coding component cannot resolve this issue as it is expected, as it is impossible to tell whether an error in the decoded message is caused by the noise or genuine biometric difference. New efforts need to be made to address this issue. Exploring new stable fingerprint features seems to be a promising solution to both direct biometric key generation and fuzzy fingerprint vault. Transformation methods have an advantage of easily producing cancelable fingerprint templates. However, its dependence on accurate registration faces a challenge as the accurate registration has been considered non-trivial. We believe fingerprint features that are insensitive to registration error and elastic distortion can greatly enhance such approaches.

ACKNOWLEDGMENT

The author wishes to acknowledge that the work presented here is financially supported by the ARC (Australia Research Council) Linkage project LP0455324. The project title is "Developing a Scalable Infrastructure for Embedded E-Security Incorporating Cryptography and Biometric Authentication".

REFERENCES

- [1] R.J. Anderson, *Security Engineering: A Guide to Building Distributed Systems*. New York: Wiley, 2001.
- [2] A. Ross, J. Shah and A.K. Jain, "From template to image: reconstructing fingerprints from minutiae points," *Special Issue on Biometrics: Progress and Directions, IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No.4, April 2007, pp.544-560.
- [3] G.I. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," *Proc. IEEE Symposium Security and Privacy*, 1998, pp.148-157.
- [4] U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, No.6, June 2004, pp.948-960.
- [5] F. Han, X. Yu, and J. Hu, "A new way of generating grid-scroll chaos and its application to biometric authentication," *The 31st Annual Conference of the IEEE Industrial Electronics Society, (IECON'05)*, Raleigh, North Carolina, USA, 6-10 November, 2005, pp.61-66.
- [6] F. Han, J. Hu, L. He and Y. Wang, "Generation of reliable PINs from fingerprints," *IEEE International Conference on Communication (ICC)*, Glasgow, Scotland, June, 2007, pp.1191 – 1196.
- [7] C. Souta, D. Boberge, A. Stoianov, R. Gilroy, and B.V.K. Vijaya Kumar, "Biometric Encryption," *ICSA Guide to Cryptography*, McGraw-Hill, 1999, http://www.bioscrypt.com/assets/Biometric_Encryption.pdf.
- [8] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no.9, Sept. 2006, pp. 1081-1088.
- [9] A. Jules and M. Sudan, "A fuzzy vault scheme," *Proceedings IEEE International Symposium Information Theory*, A. Lapidoth and E. Teletar, Eds., 2002, p.408.
- [10] T.C. Clancy, N. Kiyavash, and D.J. Lin, "Secure smartcard-based fingerprint authentication," *Proceedings of ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, pp. 45-52.
- [11] U. Uludag, and A. Jain, "Securing fingerprint template: fuzzy vault with helper data," *Proc. IEEE Workshop on Privacy Research In Vision*, June 22, 2006, p.163.
- [12] U.Uludag, S. Pankanti, and A.K. Jain, "Fuzzy vault for fingerprints," *Proceedings of Audio and Video-Based Biometric Personal Authentication*, Rye Town, NY, July 2005, pp.310-319.
- [13] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer, New York, 2003.
- [14] U. Uludag and A.K. Jain, "Fuzzy fingerprint vault," *Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice*, pp. 13-16, Cambridge, UK, August 2004.
- [15] A. Malickas and R. Vitkus, "Fingerprint registration using composite features consensus," *Informatica, Institute of Mathematics and Informatics (Vilnius)*, vol. 10, no.4, 1999, pp. 389-402.
- [16] VERIFIER. Neurotechnologija Ltd. [Http://www.neurotechnologija.com](http://www.neurotechnologija.com)
- [17] N. Ratha, S. Chikkerur, J.H. Connell and R.M.Bolle, "Generating cancellable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no.4, April 2007, pp.561-572.
- [18] Y. Wang, J.Hu and D. Philip, "A fingerprint orientation model based on 2D Fourier Expansion (FOMFE) and its application to singular-point detection and fingerprint Indexing," *Special Issue on Biometrics: Progress and Directions, IEEE Transactions on Pattern Analysis and Machine Intelligence*, April 2007, Vol. 29, no.4, pp.573-585.
- [19] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," *Proceedings of the 10th Australian Conference on Information Security and Privacy*, July 2005, pp.242-25.
- [20] S. Chikkerur and N.K. Ratha, "Impact of singular point detection on fingerprint matching performance," *Proceedings of the Fourth IEEE Workshop Automatic Identification Advanced Technologies*, July 2005, pp.207-212.
- [21] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *Proc. 6th ACM Conf. Computer and Communications Security*, G. Tsudik, ed., 1999, pp.28-36.
- [22] F. Farooq, R.M. Bolle, T.Y. Jea and N. Ratha, "Anonymous and revocable fingerprint recognition," *IEEE Conference on Computer Vision and Pattern Recognition, CVPR'07*, 2007, pp. 1-7.
- [23] T.E. Boulton, W.J. Scheirer and R. Woodworth, "Revocable biotokens: accuracy and security analysis," *IEEE Conference on Computer Vision and Pattern Recognition*, June 2007, pp.1-8.
- [24] C. Lee, J.Y. Choi, K.A. Toh, S. Lee and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutia information," *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics*, vol. 37, no.4, August, 2007, pp.980-992.
- [25] A.B.J. Teoh, A.Goh, and D.C.L. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, December 2006, pp. 1892-1901.
- [26] W.J. Scheirer and T.E. Boulton, "Cracking fuzzy vaults and biometric encryption," *Tech. Report, VAST Lab, University Colorado at Colorado Springs*, Feb. 2007.