International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015

Available at http://internationaljournalofresearch.org

Virtual identity using Biometric templates like Fingerprint for Authentication Minutiae

Sk. Asha[1] ;o. Navajeevan Raju[2] & d. Vijay Kumar [3]

[1]M.Tech, Dept of ECE,Vijaya Engineering College, Telangana, India.
Email:chinnari454@gmail.com

[2]Assistant Professor, Dept of ECE,Vijaya Engineering college, Telangana,India,
Email: navajeevan1116@gmail.com

[3]Associate Professor,HOD, Dept of ECE, Vijaya Engineering college, Telangana,India,
Email: vkumar88.d@gmail.com

Abstract

In recent years use of biometric technologies gains popularity as concern about the privacy and misuse of biometric data increases. Thus protecting biometric data becomes an important issue. The oldest and widely used form of biometric identification is the fingerprints. It has been widely used in both forensic and civilian applications. Though much progress and research has been made in fingerprint authentication systems, the performance of even state-of-the-art recognizer are still low. In addition to this, securing a stored fingerprint template is of paramount importance because once fingerprints are compromised fingerprint cannot be easily revoked. Over the years many template protection schemes have been explored, we made an effort to review existing biometric template protection schemes. The core motive of this paper is to review the various fingerprint privacy protection schemes. This literature also includes vulnerable points in biometric systems and type of fingerprint matching techniques. In our survey, we observed some reliable and robust schemes.

Keyword: Fingerprint; Biometric templates; Virtual identity; Authentication; Minutiae

1. Introduction

In recent years, verification is becoming a security backbone in the modern distributed systems environment. The biometric is a stirring and emerging field of technology that offers solutions in many applications for instance verification, recognition, security monitoring, border control and immigration, financial transactions, law enforcement agencies, retail sales [12]. In authentication systems the fingerprints are the widely used form of biometric identification. Although fingerprint recognition has been studied for many years and many such security techniques have been discovered, the performance of even state-of-the-art matcher is still much low. Furthermore, traditional encryption techniques are not enough for fingerprint privacy protection as decryption is needed before fingerprint matching, which exposes the fingerprint to the opponents. Thus protecting the privacy of the fingerprint becomes an important issue.

Most of the existing techniques exploit the key or token for the fingerprint privacy protection, which creates the difficulty. They may also be open to attacks when both the key or token and the protected fingerprint are stolen. Several approaches have been proposed in the literature to protect biometric templates from revealing important information. Teoh et al. [5] propose a biohashing approach in which the inner products between the user's fingerprint features and a tokenized pseudorandom number (i.e. the key) is computed. The accuracy of this approach primarily depends on the key or token, which assumed to be never shared or stolen [14].Ratha *et al* [6] propose to generate cancellable fingerprint templates by applying noninvertible transforms on the minutiae. The noninvertible transform is guided by a key, which will usually lead to a reduction in matching accuracy. The work in [5] and [6] are shown to be exposed to intrusion and linkage attacks when both the key and the transformed template are stolen [13]. Sheng Li and Alex Cot [7] imperceptibly hide the user identity on the thinned fingerprint using a key. The user identity may also be compromised when both the key and the secured thinned fingerprint are stolen.

There are some schemes [1],[2],[4] and [8]–[11] that are able to protect the privacy of the fingerprint without using a key. These schemes provide security to the fingerprint template by creating a virtual identity. Virtual identity is created with the fusion of features extracted from two or more biometric template which is then stored into the database instead of storing original template. For example as shown in fig. 1 the virtual identity is created by combining features extracted from two fingerprints.

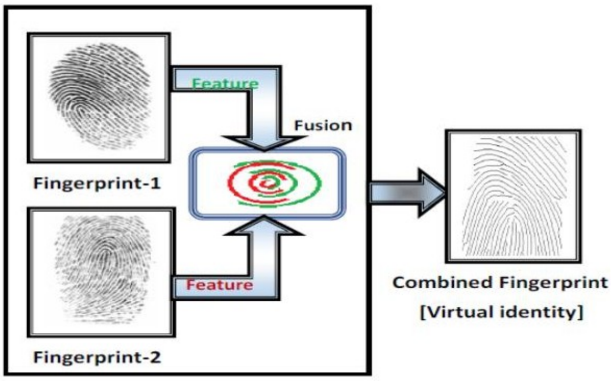

Fig 1: Virtual identity creation by combining features acquired from two fingerprints.

Our survey in [3] gives a detail review of schemes that are explored for fingerprint privacy protection without using a key, along with their merits and demerits.

2. Related Work

A number of techniques have been developed to improve the privacy and security of fingerprint templates. There are hardware based and software based solutions. At the very beginning keys were used to protect the privacy of fingerprint information [4]. Biometric cryptosystems is a new technique which combines biometrics and cryptography [5], and is popularly known as crypto-biometric systems. The system is also called helper data-based system. Biometric cryptosystems are classified into two classes based on how helper data is generated: key binding schemes and key generating schemes. In key binding schemes, the key or helper data is obtained by binding a chosen key to the biometric template. At authentication, keys are generated from the helper data by applying a key retrieval algorithm [6]. Fuzzy commitment scheme [7], fuzzy vault scheme [8], shielding functions [9] are various approaches to this technique. While in key generating schemes, the helper data is obtained only from the biometric template. Keys are generated from the helper data and a given biometric template [10]. Various approaches to this technique are private template scheme [11] and quantization schemes [12].

The technique based on cryptosystem is so inconvenient that the original fingerprint can be reconstructed if the key and protected fingerprint is stolen. Teoh *et al.* [13] proposed a biohashing approach in which the fingerprint features are combined with a pseudo random number before storing into the database. The technique has significant advantages than solely biometric systems in the sense that it has zero equal error rate and it makes a clear separation between genuine and imposter users. Hence the technique allows the elimination of false accept rates without suffering from increased occurrence of false reject rates. The work in [13] introduces a novel two factor authentication approach in which the fingerprint feature is combined with user specified tokenized random number or data to generate a unique compact code for each user. Two processes are carried out discretization and wavelet Fourier–Mellin transform (FMT). Direct mixing of pseudo-random number and biometric data—BioHashing is an extremely efficient mechanism with which to incorporate physical tokens, such as smart card, USB token etc. thereby resulting in two factors (token + biometrics) credentials via tokenised randomisation. Hence, it protects against biometric fabrication without adversarial knowledge of the randomisation or equivalently possession of the corresponding token. Tokenised discretisation also enables straightforward revocation via token replacement, and furthermore, biohashing has significant functional advantages over solely biometrics i.e. zero equal error rate (EER) point and eliminate the occurrence of FAR without overly imperil the FRR performance.

Later biometric key generation algorithm [14] were introduced which uses the concept of key generation. The enrolled fingerprint template is transformed to a key and the key is stored instead of the template. During authentication a key is generated from the input template by using the same function that was used during enrolment. The keys are compared using any matching algorithm. The technique has a poor matching performance thereby increasing the FAR. Ratha *et al.* [15] proposed cancellable biometric transforms which are designed in a way that it should be computationally hard to recover the original biometric data. The technique is also called feature transformation. Two main categories of cancellable templates are non-invertible transforms and biometric salting. In non-invertible transforms, biometric dataare obtained by applying a non-invertible function. The advantage of applying this technique is that potential imposters are not able to construct the entire biometric data even if transform is compromised. However, applying non-invertible transforms mostly results in a loss of accuracy. Poor performance is caused by the fact that transformed biometric templates are difficult to align in order to perform a proper comparison and in addition information is reduced. Biometric salting usually denotes transform of biometric templates which are selected to be invertible. Invertible transform of biometric feature vector elements represent an approach to biometric salting even if biometric templates have been extracted in a way that is not feasible to reconstruct the original biometric signal. As a consequence parameters have to be kept secret. If user-specific transforms are applied, the parameters of the transform have to be presented at each authentication. Imposters are able to recover the original template in case the transform parameters are compromised.

2.1 The proposed fingerprint privacy protection system:

Fig. 2 and 3 shows our proposed fingerprint privacy protection system. In the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints A and B from fingers A and B, respectively. We extract the minutiae positions from fingerprint A and the orientation from fingerprint B using proposed techniques. Then, by using our proposed coding strategies, a combined minutiae template is generated based on the minutiae positions and the orientation fields are detected from both fingerprints. Finally, the combined minutiae template is stored in a database.

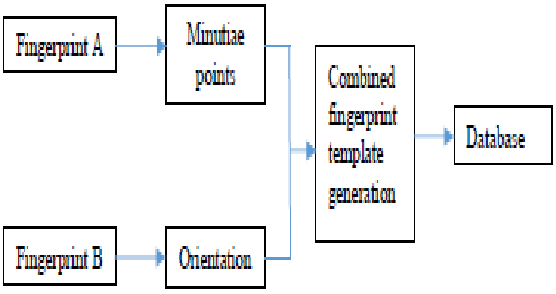

Fig 2: Enrollment Phase.

In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints A’ and B’ from fingers A and B. As what we have done in the enrollment, we extract the minutiae positions from fingerprint A’ and the orientation from fingerprint B’. Reference points are detected from both query fingerprints. These extracted information will be matched against the corresponding template stored in the database by using a twostage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold

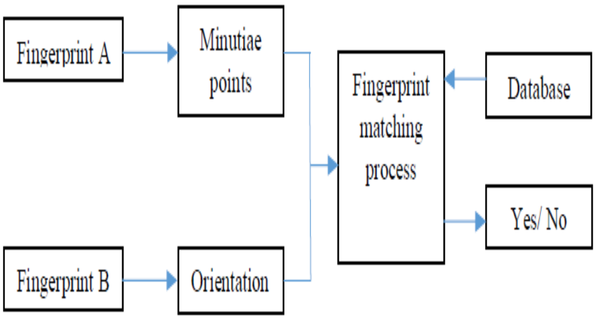

Fig 3: Authentication Phase.

3. Implementation

3.1 Minutiae point extraction:

A fingerprint is the pattern of ridges and valleys; each individuals has unique fingerprints. The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. The two most prominent local ridge characteristics, called minutiae, are the ridge ending and the bifurcation ending and the ridge bifurcation. The first is defined as the point where a ridge forks or diverges into branch ridges. A good quality fingerprint typically contains about 40-100 minutiae points. Fingerprint recognition, is an application in pattern recognition, and is used in security to identity authentication. Fingerprint matching has three different Categories, namely, Correlation Based, Minutiae Based, Ridge feature Based. Minutiae based fingerprint matching is the most widely used fingerprint matching algorithm, and this algorithm too is minutiae based.

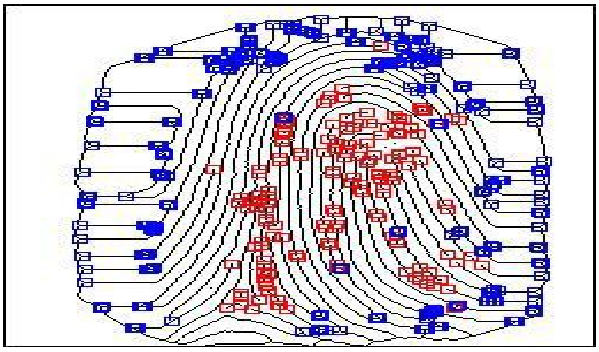

Fig 4: Minutiae Points.

To implement a minutia extractor, a three-stage approach is widely used by researchers. These stages are preprocessing,minutia extraction and post processing stage.

The pre-processing of FRMSM uses binarization to convert gray scale image into binary image by fixing the threshold value. The binarized image is thinned using Block Filter to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. Thinning does not change the location andorientation of minutiae points compared to original fingerprint which ensures accurate estimation of minutiae points. To calculate the bifurcation angle, the advantage of the fact that termination and bifurcation are dual in nature is used. The termination in an image corresponds to the bifurcation in its negative image hence by applying the same set of rules to the negative image, the bifurcation angles is obtained.

The minutiae location and the minutiae angles are derived after minutiae extraction. The terminations which lie at the outer boundaries are not considered as minutiae points, and Crossing Number is used to locate the minutiae points in fingerprint image. Crossing Number is defined as half of the sum of differences between intensity values of two adjacent pixels. If crossing Number is 1, 2 and 3 or greater than 3 then minutiae points are classified as Termination, Normal ridge and Bifurcation respectively. The cross numbering points are shown in figure 4.

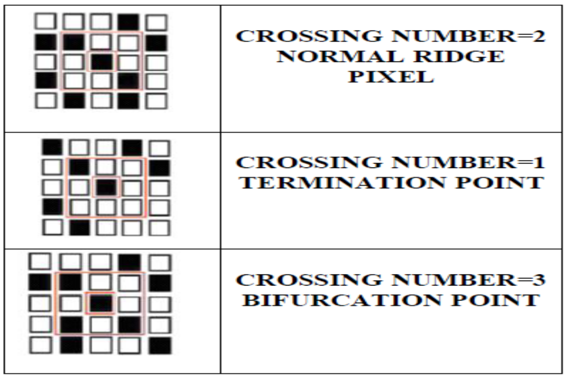

Fig 4: Cross Numbering Technique.

3.2 Orientation Estimation:

From the second fingerprint the orientation field has to be calculated. Least mean square algorithm is proposed for finding the orientation field. In order to find the orientation normalization of the fingerprint is required. Normalization can be done either locally or globally. The following diagram 4.5 shows the processing steps in estimation of fingerprint orientation field. The scheme consists of two steps: local normalization, local orientation estimation, which are summarized as follows.

3.2.1 Local Normalization:

This step is used to reduce the local variations and standardize the intensity distributions in order to consistently estimate the local orientation. The pixel-wise operation does not change the clarity of the ridge and furrow structures but reduces the variations in gray-level values along ridges and furrows, which facilitates the subsequent processing steps. The global normalization method is also used for the fingerprint enhancement employing a Gabor filter. It can normalize all the values into a defined mean and variance. However, because of the quality of the different parts of the fingerprint image, using the global mean and variance for normalization may not be appropriate. Therefore, we propose using a local normalization to reduce local variations in gray level values.

3.2.2 Local Orientation:

An orientation image, O, is defined as an N x N image, where O (i, j) represents the local ridge orientation at pixel (i, j). Local ridge orientation is usually specified for a block rather than at every pixel; an image is divided into a set of w x w non-overlapping blocks and a single local ridge orientation is defined for each block. Note that in a fingerprint image, there is no difference between a local ridge orientation of 90-degreeand 270-degree, since the ridges oriented at 90-degreeand the ridges oriented at 270-degreein a local neighborhood cannot be differentiated from each other.

This step determines the dominant direction of the ridges in different parts of the fingerprint image. This is a critical processing, and errors occurring at this stage are propagated to the frequency filter. The gradient method for orientation estimation and an orientation smoothing method with a Gaussian window to correct the estimation are used. For a number of non-overlapping blocks with the size of $W \times W$, a single orientation is assigned corresponding to the most probable or dominant orientation of the block. For each pixel in a block, a simple gradient operator, such as the Sobel mask, is applied to obtain the horizontal gradient value Gx (u, v) and vertical gradient value Gy (u, v). The block horizontal and vertical gradients, i.e., Gxx and Gxy, are obtained by adding up all the pixel gradients of the corresponding direction. Then, the block orientation $O(x, y)$ is determined using the block horizontal and vertical gradients.

Each block uses a single-orientation value to reduce the computational complexity. This block-wise scheme, however, may be coarse, and it may be difficult to obtain a fine orientation field. In order to estimate orientations more accurately, we use a pixel-wise approach. For each pixel, a block with W × Centered on the pixel is used to compute the average orientation of the pixel. Because of the ambiguity of the orientation values for each position, an orientation smoothing method with a Gaussian window is used to correct the estimation, rather than a simple averaging.

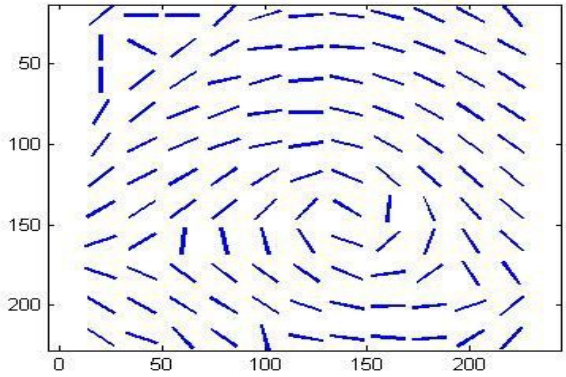

Fig 5: **Orientation Fields Using the Method Proposed.**

3.3 Combined Fingerprint Minutiae Template Generation:

The Combined Fingerprint Template is generated by combining the minutiae points extracted from the first fingerprint and the orientation field extracted from the second fingerprint. The combined fingerprint template is generated for various combination of fingerprints. The templates can then be stored in a database which can be used as a reference during the authentication. The following figure shows the basic block diagram of my proposed method.

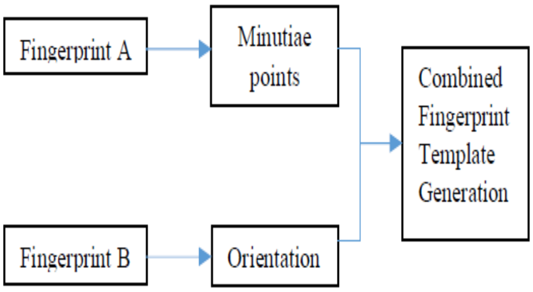

Fig 6: **Proposed Method for Combined Fingerprint Template Generation.**

4. Conclusion

In this paper, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process. In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Our combined minutiae template has a similar topology to an original minutiae template.

Therefore,we are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template. The experimental results show that our system achieves a very low error rate with FRR=0.4% at FAR=0.1%. It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates. Compared with the state-of-the-art technique, our technique can generate a better new virtual identity (i.e., the combined fingerprint) when the two different fingerprints are randomly chosen. The analysis shows that it is not easy for the attacker to recover the original minutiae templates from a combined minutiae template or a combined fingerprint.

5. References

[1] B. Fasel and J. Luettin, “Automatic facial expression analysis: A survey,”*Pattern Recognit.*, vol. 36, no. 1, pp. 259–275, 2003.

[2] P. Ekman, E. T. Rolls, D. I. Perrett, and H. D. Ellis, “Facial expressionsof emotion: An old controversy and new findings discussion,” *Phil.Trans. Royal Soc. London Ser. B, Biol. Sci.*, vol. 335, no. 1273, pp.63–69, 1992.

[3] A. Mehrabian, *Nonverbal Communication*. London, U.K.: Aldine, 2007.

[4] M. Pantic and I. Patras, “Dynamics of facial expression: Recognitionof facial actions and their temporal segments from face profile imagesequences,” *IEEE Trans. Syst., Man, Cybern. B*, vol. 36, no. 2, pp. 433–449, Apr. 2006.

[5] J. Wang, L. Yin, X. Wei, and Y. Sun, “3-D facial expression recognitionbased on primitive surface feature distribution,” in *Proc. IEEE Conf.Comput. Vis. Pattern Recognit.*, Jun. 2006, pp. 1399–1406.

[6] Y. Lijun, C. Xiaochen, S. Yi, T. Worm, and M. Reale, “A high-resolution3-D dynamic facial expression database,” in *Proc. 3rd Int. Conf. FaceGesture Recognit.*, Amsterdam, The Netherlands, Sep. 2008, pp. 1–6.

[7] S. M. Lajevardi and Z. M. Hussain, "Emotion recognition from colorfacial images based on multilinear image analysis and Log-Gaborfilters," in *Proc. 25th Int. Conf. Imag. Vis. Comput.*, Queenstown, NewZealand, Dec. 2010, pp. 10–14.

[8] L. Torres, J. Y. Reutter, and L. Lorente, "The importance of the colorinformation in face recognition," in *Proc. Int. Conf. Imag. Process.*,vol. 2. Kobe, Japan, Oct. 1999, pp. 627–631.

[9] P. Shih and C. Liu, "Comparative assessment of content-based faceimage retrieval in different color spaces," *Int. J. Pattern Recognit. Artif.Intell.*, vol. 19, no. 7, pp. 873–893, 2005.

[10] Z. Liu and C. Liu, "A hybrid color and frequency features method forface recognition," *IEEE Trans. Image Process.*, vol. 17, no. 10, pp. 1975–1980, Oct. 2008.

[11] C. J. Young, R. Y. Man, and K. N. Plataniotis, "Color face recognitionfor degraded face images," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*,vol. 39, no. 5, pp. 1217–1230, Oct. 2009.

[12] S. Chikkerur and N. Ratha, "Impact of singular point detection on fingerprint matching performance," in Proc. Fourth IEEE Workshop on Automat. Identification Advanced Technologies, Oct. 2005, pp. 207–212.

[13] Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 1, pp. 72–87, Jan. 2011.

[14] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," IEEE Trans. Pattern Ana

l. Mach. Intell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

Authors Profiles

SK. ASHApursuing ,
M.Tech.
Vijaya Engineering
College, Telangana,
India.

Email:chinnari454@gmail.com

O.NAVAJEEVAN
RAJU, M.Tech
Assistant
Professor,Vijaya
Engineering college
Telangana,India,
Email: navajeevan1116@gmail.com

D. Vijay Kumar
M.Tech,
Associate Professor,
HOD,
14-years Experience.
Vijaya Engineering
college, Telangana,India,
Email: vkumar88.d@gmail.com