ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Combined Fingerprint Minutiae Template Generation

Guruprakash.V[1], Arthur Vasanth.J[2]

PG Scholar, Department of EEE, Kongu Engineering College, Perundurai-52[1]

Assistant Professor (SRG), Department of EEE, Kongu Engineering College, Perundurai-52[2]

ABSTRACT: We propose here a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. Two fingerprints are captured from two different fingers in the enrollment phase. From one fingerprint we extract the minutiae positions. We extract the orientation from other fingerprint. With the extracted information, a combined minutiae template is created and stored in a database. The system requires two query fingerprints, for authentication, from the same two fingers which are used in the enrollment. Any existing fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. Since the combined minutiae template is used in our method, the features of a single fingerprint cannot be easily retrieved even when the database is hacked. Since the created template is not visually realistic, it is difficult for the attacker to separate the two fingerprints. Thus, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching algorithms. Compared with the existing technique, the proposed method has advantage in creating a better new virtual identity when the two different fingerprints are randomly chosen.

I. INTRODUCTION

Fingerprint techniques have widespread of applications in authentication systems. Hence protecting the privacy of the fingerprint becomes an important issue. Conventional encryption methods are not sufficient for protecting the privacy of the fingerprint, because decryption technique is needed before the fingerprint matching process. This technique exposes the fingerprint to the intruders or attackers. Therefore, to avoid this many methods have been developed which helps in developing specific fingerprint protection techniques. In order to protect the privacy of the fingerprint most of the existing methods make use of key. This creates much inconvenience in the privacy. These techniques become inefficient when both the key and the fingerprint are stolen. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint.

Most of the existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen. Teoh *et al.* [1] propose a bio-hashing approach by computing the inner products between the user's fingerprint features and a pseudorandom number (i.e., the key). The accuracy of this approach mainly depends on the key, which is assumed to be never stolen or shared. Ratha *et al.* [2] propose to generate cancelable 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 [1] and [2] are shown to be vulnerable to intrusion and linkage attacks when both the key and the transformed template are stolen. Nandakumar *et al.* [3] propose to implement fuzzy fault on the minutiae, which is vulnerable to the key-inversion attack.

There are only a few schemes [4]–[8] that are able to protect the privacy of the fingerprint without using a key. Ross and Othman [9] propose to use visual cryptography for protecting the privacy of biometrics. The fingerprint image is decomposed by using a visual cryptography scheme to produce two noise-like images (termed as sheets) which are stored in two separate databases. During the authentication, the two sheets are overlaid to create a temporary fingerprint image for matching. The advantage of this system is that the identity of the biometrics is never exposed to the attacker in a single database. However, it requires two separate databases to work together, which is not practical in same applications. The works in [5]–[7] combine two different fingerprints into a single new identity either in the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

feature level [5] or in the image level [6], [7]. In [5], the concept of combining two different fingerprints into a new identity is first proposed, where the new identity is created by combining the minutiae positions extracted from the two fingerprints. The original minutiae positions of each fingerprint can be protected in the new identity. However, it is easy for the attacker to identify such a new identity because it contains many more minutiae positions than that of an original fingerprint. The experiment shows that the EER of matching the new identities is 2.1% when the original minutiae positions are marked manually from the original fingerprints. A similar scheme is proposed in [8], where the minutiae positions extracted from a fingerprint and the artificial points generated from the voice are combined to produce a new identity. In this work, the EER are shown to be under 2% according to the experimental results.

In this paper, we propose a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. During the enrollment, the system captures two fingerprints from two different fingers. We propose a combined minutiae template generation algorithm to create a combined minutiae template from the two fingerprints. In such a template, the minutiae positions are extracted from one fingerprint, while the minutiae directions depend on the orientation of the other fingerprint and some coding strategies. The template will be stored in a database for the authentication which requires two query fingerprints. A two-stage fingerprint matching process is further proposed formatching the two query fingerprints against a combined minutiae template. By using the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen. In addition, the combined minutiae template share a similar topology to the original minutiae templates, it can be converted into a real-look alike combined fingerprint by using an existing fingerprint reconstruction approach. The combined fingerprint issues a new virtual identity for two different fingerprints, which can be matched using minutiae based fingerprint matching algorithms. The advantages of our technique over the existing fingerprint combination techniques [5]–[8] are as follows:

1. Our proposed system is able to achieve a very low error rate with FRR= 0.4% when FAR= 0.1%.
2. Compared with the feature level based technique [5], [8],we are able to create a new identity (i.e., the combined minutiae template) which is difficult to be distinguished from the original minutiae templates.
3. Compared with the image level based technique [6], [7], we are able to create a new virtual identity (i.e., the combined fingerprint) which performs better when the two different fingerprints are randomly chosen. The organization of the paper is as follows. Section II introduces our proposed fingerprint privacy protection system. Section III explains how to generate a combined fingerprint for two different fingerprints. Section IV presents the experimental results. Section V analyzes the information leakage in a combined minutiae template, followed by the conclusions in the last section.

II. THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

Fig. 1 and 2 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.

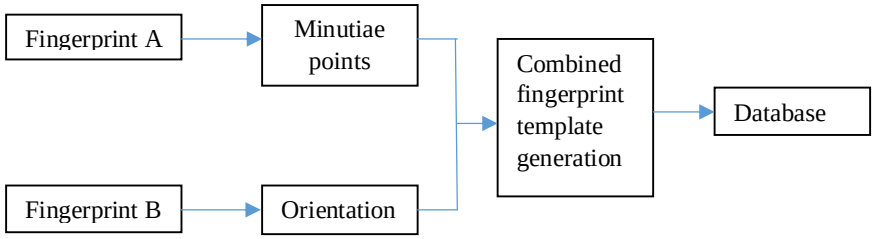


Figure 1. Enrollment Phase.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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 two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold.

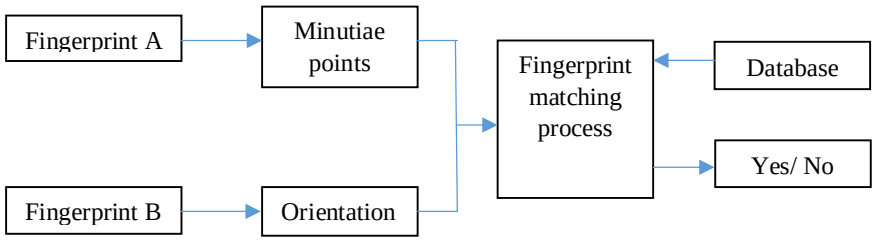


Figure 2. Authentication Phase.

2.1 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.

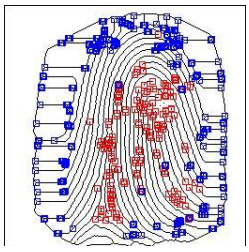


Figure 3. Minutiae Points.

To implement a minutia extractor, a three-stage approach is widely used by researchers. These stages are pre-processing, minutia extraction and post processing stage. The following Flowchart 4.1 shows the algorithm for Minutiae point extraction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

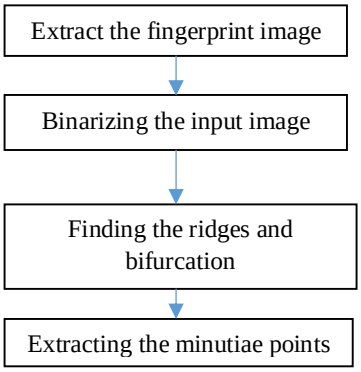
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014



Flowchart 1. Minutiae Point Extraction Algorithm.

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 3.

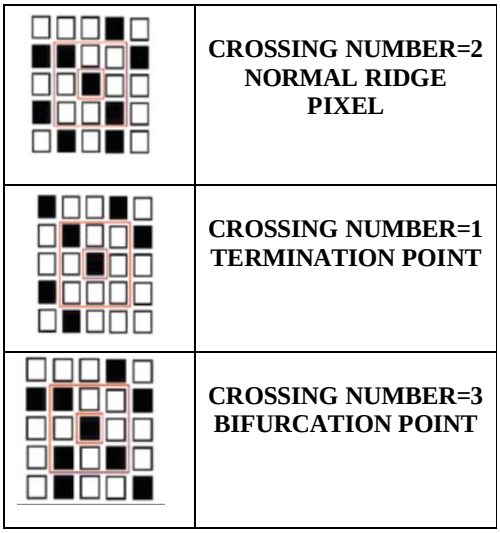


Figure 3. Cross Numbering Technique.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

2.2 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.

2.2.1 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.

2.2.2 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 × Wcentered 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

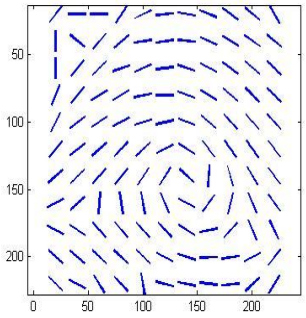


Figure 4. Orientation Fields Using the Method Proposed.

2.3 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.

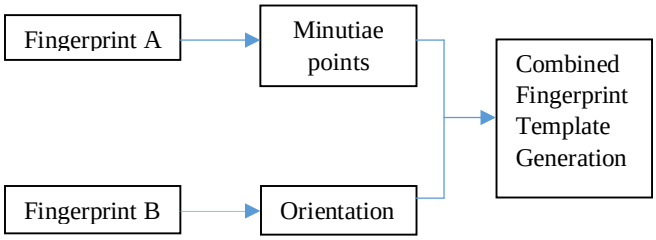


Figure 5. Proposed Method for Combined Fingerprint Template Generation.

III. CONCLUSION

A novel system for fingerprint privacy protection by combining two fingerprints into a new identity is proposed. 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. The combined minutiae template has a similar topology to an original minutiae template. It is difficult for an attacker to break other traditional systems by using the combined minutiae templates. Compared with the state-of-the-art technique, this technique can generate a better new virtual identity (i.e., the combined fingerprint) when the two different fingerprints are randomly chosen.

The future scope of the project may be to enhance the quality of the image, so that the minutiae points and orientations can be calculated in an efficient way.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. ACKNOWLEDGMENT

We are grateful to the management Kongu Engineering College, Perundurai for providing the facilities in the Department of Electrical and Electronics Engineering to carry out the research work. We acknowledge Prof. S. Kuppuswami, Principal, for his constant encouragement and guidance provided in all respects.

REFERENCES

[1] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.
[2] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.
[3] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–57, Dec. 2007.
[4] A. Ross and A. Othman, "Visual cryptography for biometric privacy,"IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70-81,Mar. 2011.
[5] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004.
[6] A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, Aug. 29–Sep. 2, 2011.
[7] A. Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.
[8] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric templates using fingerprint and voice," Proc. SPIE, vol. 69440I, pp. 69440I-1–69440I-9, 2008.
[9] K. G. Larkin and P. A. Fletcher, "A coherent framework for fingerprint analysis: Are fingerprints holograms?",Opt. Express, vol. 15, pp. 8667–8677, 2007.
[10] L. Hong, Y. F. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.
[11] K. Nilsson and J. Bigun, "Localization of corresponding points in fingerprints by complex filtering," Pattern Recognit. Lett, vol. 24, no. 13, pp. 2135–2144, 2003.
[12] 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.