International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Combined Fingerprint Minutiae Template Generation for protection

[1]T.Naveen& [2]K.Saidulu
1.M.Tech,Bomma Institute of Technology and Science, Allipuram, Khammam, Telengana, INDIA - 507318
2.ASSOCIATE PROFESSOR, Bomma Institute of Technology and Science, Allipuram, Khammam, Telengana, INDIA – 507318

Abstract:
The primary purpose of using a biometric system is to provide non-reputable authentication. Authentication implies that (i) only legitimate or authorized users are able to access the physical or logical resources protected by the biometric system and (ii) impostors are prevented from accessing the protected resources. While a biometric system can be compromised in a number of ways, one of the potentially damaging attacks is the leakage of biometric template information. The leakage of this template information to unauthorized individuals constitutes a serious security and privacy threat. Therefore in this paper we propose a model of creating 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. The experimental results show that our system can achieve a very low error rate. Compared with the state-of-the-art technique, our work has the advantage in creating a better new virtual identity when the two different fingerprints are randomly chosen.

1. INTRODUCTION

WITH the widespread applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue. Traditional encryption is not sufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker [1]. 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. [2] propose a biohashing 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 [3]. Ratha et al. [4] 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 [2] and [4] are shown to be vulnerable to intrusion and linkage attacks when both the key and the transformed template are stolen [5]. Nanda kumar et al. [6] propose to implement fuzzy fault on the minutiae, which is vulnerable to the key-inversion attack [7]. Our work in [8] 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 protected thinned fingerprint are stolen. 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 for matching 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 [9]. The combined fingerprint issues a new virtual identity for two different fingerprints, which can be matched using minutiae based fingerprint matching algorithms. The rest of the paper is organized as, Section 2 discuss proposed fingerprint privacy system. Section 3 explains how to generate combined fingerprint from two different fingerprints. Section 4 presents experimental results. Finally, Section 5 concludes the paper. 2. FINGERPRINT PRIVACY 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 some existing techniques [10], [11]. Then, by using our proposed coding strategies, a combined minutiae template is generated based on the minutiae positions, the orientation and the reference points detected from both fingerprints. Finally, the combined minutiae template is stored in a database. In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints A' and B' and from fingers A and B. As what we have done in the enrolment, 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 Prabhakara Rao T et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2290-2294 www.ijcsit.com 2290 two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold

RGB TO GRAY CONVERSION Take the input image. And it converts into grayscale image. RGB IMAGES An RGB image represents each pixel color as a set of three values, representing the red, green, and blue intensities that make up the color. In MATLAB, the red, green, and blue components of an RGB image reside in a single m-by-n-by-3 array. m and n are the numbers of rows and columns of pixels in the image, and the third dimension consists of three planes, containing red, green, and blue intensity values. For each pixel in the image, the red, green, and blue elements combine to create the pixel's actual color. An RGB array can be of • Class double, in which case it contains values in the range [0, 1]. •Class uint8, in which case the data range is [0,255].•Class uint16, in which case the data range is [0, 65535]. GRAYSCALE IMAGES Contain only brightness information. No color

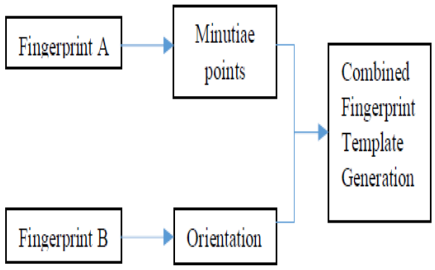
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

information. Typically contain 8 bits/pixel data, which corresponds to 256 (0 to 255) different brightness (gray) levels • Useful when a small section of the image is enlarged. • Allows the user to repeatedly zoom a specific area in the image

C. FINGERPRINT BASICS Fingerprints are known to be unique to every individual. We can extract minutiae and orientation from a fingerprint. ♣ MINUTIAE A Minutia is defined as the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings. Types of ridges: • ridge endings - a ridge that ends abruptly • ridge bifurcation - a single ridge that divides into two ridges Short ridges, island or independent ridge - a ridge that commences, travels a short distance and then ends •ridge enclosures - a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge • spur - a bifurcation with a short ridge branching off a longer ridge • crossover or bridge - a short ridge that runs between two parallel ridges

♣ ORIENTATION An orientation image 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 90o and 270o , since the ridges oriented at 90o and the ridges oriented at 270o in a local neighborhood cannot be differentiated from each other. Given a normalized image, G, the main steps of the algorithm are as follows: 1) Divide G into blocks of size w x w (16 x 16). 2) Compute the gradients at each pixel, (i, j). The gradient operator Sobel is used.

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



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-theart 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.

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.