A Study on the Performance Analysis of Hybrid Fingerprint Matching Methods

Jong Ku Kim, Seung-Hoon Chae, Sung Jin Lim, and Sung Bum Pan

[1] Dept. of Information and Communication Engineering, Chosun Univ., Korea

Abstract. The fingerprint verification methods include minutiae-based and image-based methods. The minutiae-based method has been frequently used, but it has limitations in performance. These days, there have been many studies on enhancement of performance using another information rather than minutiae. This paper analyzed changes in performance according to size and form of binary fingerprint images to be compared for analysis performance of image-based fingerprint verification method. Based on the experiment results, verification performance was superior as there many compare areas. Security performance was superior when comparing the center of a fingerprint.

Keywords: Biometrics, fingerprint verification, image-based matching

1 Introduction

The convenience confidence in fingerprints has been demonstrated through long-term research, and fingerprints have intrinsic features that they do not change for whole life and are personally different. And they are easy to use, cheap and the most suitable for miniaturization. So fingerprint verification is an efficient personal verification method that has been the most widely used in comparison with other biometric information[1-5]. Of the fingerprint verification methods, the most frequently used method is minutiae-based fingerprint verification. As it uses a tiny amount of information of minutiae, it is faster and suitable for small systems. However, the minutiae-based method has errors, such as minutiae which do not exist in the process to extract minutiae and elimination of the wrong one is produced or existing minutiae are eliminated. Errors also occur when the quality of the fingerprint image acquired is low. When few minutiae are produced, as the size of the fingerprint image acquired is small, it has a disadvantage that verification is difficult[6-9]. The errors occurring in fingerprint verification include False Acceptance Rate(FAR) and False Rejection Rate(FRR): for the former, the users who do not register are accepted as registered; for the latter, those who register are accepted as not.

Currently, there have been studies to decrease errors of fingerprint verification. Among them, there are methods that used multi-snapshot, directional image feature and preprocessing enhancement[10-12]. In addition, there are fingerprint verifications

----
Corresponding author: Sung Bum Pan

using minutiae and ridge and using minutiae and shape, using other additional information with minutiae.

The minutiae and image-based fingerprint verification methods are used together, more error can effectively be reduced. If binary image-based fingerprint verification performs with minutiae-based fingerprint verification needs that information of binary fingerprint image adds to expand area of minutiae data standard format. However, as the binary fingerprint image has bigger data than the minutiae, its volume is too large for the standard format and it is not suitable. This study experimented and analyzed verification results according to shape and size of which is not binary image whole to use the other additional information binary fingerprint images with fingerprint information. This paper consists of as follows: Chapter 2 describes the image-based fingerprint verification; Chapter 3 Binary image fingerprint verification performance analysis according to shape and size; and Chapter 4 concludes this study.

2 Image-based fingerprint verification

The minutiae-based fingerprint verification is fast verification execution is possible but though two fingerprints have the same minutia, they do not necessarily have the same ridge. When the range of the fingerprint image input is narrow, as enough minutiae are not extracted, verification confidence decreases. However, the image of fingerprint has more information that can be extracted from images of same size than minutiae. So, though the size of fingerprint image input is small, more exact verification is possible than the minutiae. In general, the fingerprint image input for fingerprint verification is Gray image with lightness of 256. This Gray image is nonlinearly distorted or has a lot of noise such as sweat pores. And as the lightness of the image is not consistent, it is not suitable for it to be used for image comparison[13]. If the gray image is changed into a binary fingerprint image through binarization, the ridge and valley of the fingerprint will have consistent lightness and ridges which are discontinued by wrinkles, sweat pores and finger pressure are connected.

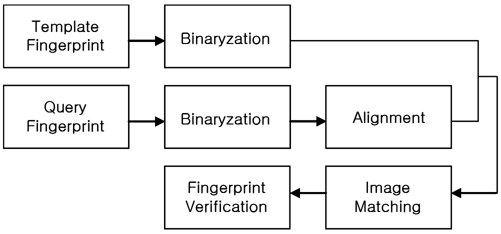
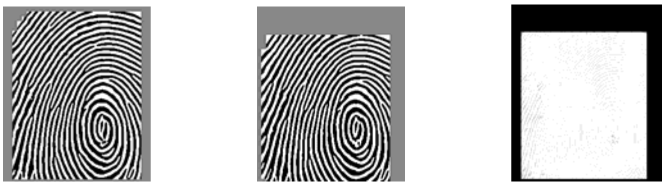


Figure 1. Structure of image-based fingerprint verification

The binarization shows the ridge and valley as 0 and 1, the advantage of the binary image is less than an amount of calculation of gray image. Image-based fingerprint verification contrasts two fingerprint images to compare their pixel values. The image-based verification method is composed as Figure 1.

The image-based fingerprint verification has binarization for exact compare between the fingerprint images input, and aligned them so that the two fingerprints may exist in the same phase. After such stages, image matching is performed, similarity of the two images is calculated and fingerprints are verified. Figure 2(a) shows registered fingerprint image and figure 2(b) shows alignment image of input image. Figure 2(c) shows image matching of registered image and input image. Black indicates background and is excluded from the comparison. The coordinate with same pixel value is presented in white and that with different pixel values is presented in gray.



(a) Registered image (b) Aligned input image (c) Result image

Figure 2. Binary image-based fingerprint matching

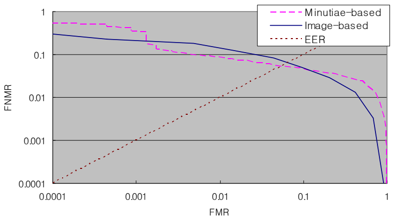


Figure 4. DET of fingerprint verification methods

As there are cases when there are no standard points in fingerprint images, image alignment is more complex and harder than the minutiae-based method. Therefore, to decrease errors of fingerprint verification, image-based verification works better when it is performed with minutiae-based verification together than independent performance of image-based fingerprint verification. Figure 4 shows the Detection Error Trade-off (DET), which presents the results of the image-based verification using the minutiae-based verification and the entire area of the binary fingerprint image. The DET shows the False Match Rate (FMR) and False Non-Match Rate (FNMR) in log. The FMR and FNMR value the more the performances of DET are good are low. Similarity(S) for input binary fingerprint image f(x,y) and aligned binary fingerprint image *h*(*x*,*y*) – both are in size of $M \times N$ – is calculated as in Eq(1). The ‘n’ represents the number of pixels in the comparison area of *f*(*x*,*y*) and *h*(*x*,*y*).

$$S = 1 - \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} |f(x,y) - h(x,y)|}{n} \qquad (1)$$

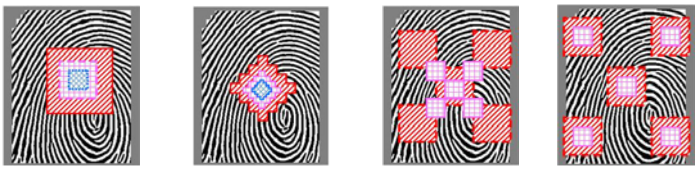
$$if\ (f(x,y), h(x,y) \neq BACKGOUND)$$

As shown in Figure 4, the minutiae-based fingerprint verification shows superior EER while the image-based fingerprint verification has superior Zero False Match Rate(ZeroFMR). As the image-based fingerprint verification has many FRR by change in thickness of ridge and distortion of images, its EER is inferior to that of the minutiae-based fingerprint verification. However, the image-based fingerprint verification using more amount of information of image data performs more exact verification than the minutiae-based fingerprint verification. Because few FAR occur and ZeroFMR shows more superior performs.

3 Binary image fingerprint verification performance analysis according to shape and size

As to the binary image-based fingerprint verification, the security performance is good but the verification performance falls and independently execute is not suitable. Like this, if binary image-based fingerprint verification performs with minutiae-based fingerprint verification needs that information of binary fingerprint image adds to minutiae data standard format. In the minutiae standard format, expand area exists. To this expand area, binary fingerprint image has to be added. However, as the binary fingerprint image has bigger data than the minutiae, its volume is too large for the standard format. Since the data volume is large, it is not suitable for small and high-speed processing systems. So the binary fingerprint image has to be applied for the minutiae data standard format and the size of the comparison area has to be decreased for high-speed verification. This paper performs and analyses fingerprint verification using the shapes seen in Figure 5 to find effective shape and size for verification. And to decrease the size of binary image effectively, we changed subjects to be compared such as ridges and valleys.

This paper performs and analyses fingerprint verification using the shapes seen in Figure 5 to find effective shape and size for verification. And to decrease the size of binary image effectively, we changed subjects to be compared such as ridges and valleys.



(a) square (b) diamond (c) cross (d) dispersed cross

Figure 5. Size and shape of diverse compare areas

For the analysis, we used EER and ZeroFMR for the case of most low FNMR when FMR is 0%. As EER is lower, the verification performance is enhanced, and as ZeroFMR is lower, the security performance of the fingerprint verification is enhanced. We analyzed verification performance according to the size and shape of compare areas, and subjects such as ridges and valleys to be compared. For the binary image used for the test, we used square, diamond and cross as in Figure 5. We changed the sizes of compare areas from 128×128 through 64×64 to 32×32, and we experimented verification results.

Table 1. The ridge and valley comparison result according to the size and shape

Comparative form	Compare area size	EER(%)	ZeroFMR(%)
Image-based matching	Total area	6.6	30.2
figure 5(a)	128×128	11.9	52.9
	64×64	16.7	79.1
	32×32	24.5	87.4
figure 5(b)	128×128	12.1	52.0
	64×64	15.2	90.0
	32×32	23.1	94.8
figure 5(c)	64×64×5	9.3	53.9
	32×32×5	12.3	54.6
figure 5(d)	64×64×5	11.5	69.5
	32×32×5	14.4	86.9

Table 1 shows the experiment results according to the shapes and sizes of the comparison areas, and subjects compared. As cross shapes in Figure 5(c) and 5(d) exceeded the whole range of 248×292 image when we used 128×128×5, they were excluded. As shown in the Table 1, in the same shape, it is seen that the performance of 128×128 area is more superior to 32×32 area. Likewise, performance good of 64×64×5 areas than 32×32×5 areas. Like this, in the size aspect of the compare area, since comparison data are increased, the more exact comparison becomes available and the verification performance and security performance are good. Moreover, among them, shape of compare area, it was good verification performance of diamond shape of figure 5 (b) than square shape of figure 5 (a). And security performance was good diamond shape more many compare area. And the results of Figure 5(c) where the compared areas are concentrated in the center of fingerprint image showed higher performance in verification performance and security performance comparison with Figure 5(d) where compare areas were decentralized outside the fingerprint images. In general, the center of the fingerprint images has many minutiae that help comparison of two fingerprints. And, many nonlinear distortions of images occur outside the fingerprint images, and at the boundaries between fingerprints and background, much background that is unnecessary for comparison is included. Like this, the security performance was enhanced like figure 5 (a), 5 (b), and 5 (d) if the center area of an image was included. Particularly, when the size of the compared area was large, the verification performance was enhanced like figure 5 (d) and the center of an image was included.

4 Conclusion

In this paper, information of binary image analyzed effective size and shape for adding to the standard format. The image-based fingerprint verification is the fingerprint alignment difficult and complex. And the minutiae-based fingerprint verification is wrong extracted minutiae and when the range of the fingerprint image input is narrow, verification confidence may decrease. Therefore, by together using a minutiae and image-based fingerprint verification, the image size and shape, and the image-based fingerprint verification performance according to the comparative object were experimented. As a result, confirmed that the verification performance and security performance of the fingerprint were enhanced as the size of the compared area was larger. And the security performance using the center area rather than the outside area of the fingerprint image was good. The verification performance was good when as the compared area was larger and the center area was included. And when fingerprint matching is made in a diamond shape rather than square, though data volume decreases in comparison with the verification in square shape, there is no significant difference in verification performance. In the future, we are going to study the minutiae-based and image-based fingerprint verification systems using standard formats based on the results of this study.

References

1. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.
2. S. Prabhakar and A. K. Jain, *Automatic Fingerprint Recognition System*, Springer, 2007.
3. S. Pankanti, S. Prabhakar, and A. K. Jain, “On the individuality of fingerprints,” *IEEE Trans. Pattern Analysis Machine Intelligence*, vol. 24, no. 8, pp. 1010-1025, 2002.
4. A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics-Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999
5. A. K. Jain, L. Hong, and R. Bolle, “On-Line fingerprint verification,” *IEEE Trans. Pattern Analysis Machine Intelligence*, vol. 19, no. 4, pp. 302-313, 1997.
6. X. Xie, F. Su, and A. Cai, “Ridge-based fingerprint recognition,” *Lecture Notes in Computer Science*, vol. 3832, pp. 273-279, 2005.
7. A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, “Filterbank-based fingerprint matching,” *IEEE Trans. Image Processing*, vol. 9, no. 5, 2000.
8. C. J. Lee and S. D. Wang, “Fingerprint feature extraction using Gabor filters,” *Electronics Letters*, vol. 35, no. 4, pp. 288-290, 1999.
9. M. Tico, P. Kuosmanen, and J. Saarinen, “Wavelet domain features for fingerprint recognition,” *Electronics Letters*, vol. 37, no. 1, pp. 288-290, 2001.
10. Y. Gil, D. Ahn, C. Ryu, S. Pan, and Y. Chung, “User enrollment using multiple snapshots of fingerprint,” *Lecture Notes in Computer Science*, vol. 3316, pp. 344-349, 2004.
11. C. H. Park, J. J. Lee, and K. H. Park, “Fingerprint matching based on directional image feature in polar coordinate system,” *Lecture Notes in Computer Science*, vol. 2756, pp. 293-300, 2004.
12. J. Yin, E. Zhu, X. Yang, G. Zhang, C. Hu, “Two steps for fingerprint segmentation,” *Image and Vision Computing*, vol. 25, no. 9, pp. 1391-1403, 2007.
13. S. B. Pan, Y. H. Gil, D. Moon, Y. Chung, and C. H. Park, “A memory-efficient fingerprint verification algorithm using a multi-resolution accumulator array,” *ETRI Journal*, vol. 22, no. 3, pp. 179-186, 2003.