Improvement of Fingerprint Verification by Using the Similarity Distribution

Seung-Hoon Chae and Sung Bum Pan

Abstract Mobile devices, with their excellent portability and increasing computational power, are increasingly being used for communication and financial transactions. As they are used in close relation to people, their security is becoming more important. Faceless verification systems with improved security performance, including face or fingerprint verification, are recently being required. Fingerprint verification is a suitable method in a faceless environment. However, the commonly used Minutiae-based fingerprint verification shows a drop in the performance of fingerprint verification, due to the decreased number of minutiae, when the number of acquired images is small. Especially since the values around the threshold of similarity are similar in the genuine and imposter, many errors could occur here. The minutiae-based fingerprint verification has a limitation in addressing these problems. A hybrid-based verification method that uses two or more fingerprint matching methods can address these problems better. Therefore, this paper has conducted the binary-image-based fingerprint verification in the partial band around the threshold. From the results of the experiment, it can be seen that the Equal Error Rate (EER) was improved by a total of 42 %, from 3.01 % to 1.73 %, by reducing the False Match Rate (FMR) in the partial band area around the threshold. In addition, it was improved by reducing the FMR by a total of 89 % from 2.77 % to 0.28 %.

Keywords Biometrics · Fingerprint verification · Hybrid fingerprint verification

S.-H. Chae
The Research Institute of IT, Chosun University, 309, Pilmun-daero, Dong-gu,
Gwangju 501-759, Korea
e-mail: ssuguly@gmail.com

S. B. Pan (✉)
Department of Control, Instrumentation, and Robot Engineering, Chosun University,
309, Pilmun-daero, Dong-gu, Gwangju 501-759, Korea
e-mail: sbpan@chosun.ac.kr

J. J. (Jong Hyuk) Park et al. (eds.), *Information Technology Convergence*,
Lecture Notes in Electrical Engineering 253, DOI: 10.1007/978-94-007-6996-0_22,

1 Introduction

Mobile devices such as computer, smart phones, PDAs, and mobile phones are providing a wide range of applications and conveniences to users. With their portability, miniaturization, price fall, diverse applications, and performance improvements, their penetration rate is rapidly increasing. Community websites such as Social Networking Services (SNSs) that are based on mobile devices are recently being developed, and communication activities via mobile devices are increasing. Accordingly, individual activities and financial information can be known by analyzing the mobile device information of an individual. With the increase in the number of activities for which mobile devices are used, the loss or hacking of such devices is resulting in much more mental and financial damage than before. Leaked information often leads to crimes. Thus, mobile device security and privacy protection are the most important issues for mobile devices, which have become very closely related to human life. Also, in the modern society, the importance of faceless verification system has been increased from the development of communication technology. The traditional authentication system of using password and Personal Identification Number (PIN) holds the problem of forgetting and misuse. Especially when the false-matching was successful in the verification with the information illegally acquired, this may raise a security problem. The biometrics draws a lot of attention as a method appropriate to solve these problems. The biometrics can be owned only by oneself and has no risk of forgetting or loss [1, 2].

As shown in Fig. 1, Android of Google, which is the representative operating system for mobile devices, has released an OS that has a face unlock feature that uses face verification, and has developed a smart-phone with a fingerprint sensor for fingerprint verification. The biometric system is increasingly being introduced to mobile devices. With the improvement of mobile device performance, the performance of the camera installed in the device is also improving. Contactless fingerprint verification methods are being studied to enable the use of high-performance cameras in mobile devices to obtain fingerprint images, which eliminates the need for an additional accessory [3, 4].

The fingerprint verification is the most widely used method of various biometrics. The Minutiae-based Fingerprint Verification (MFV) is generally used as the fingerprint verification method. Recently as the fingerprint verification system is miniaturized, the size of fingerprint scan sensor has become small and hence, the acquired size of fingerprint got smaller as well. Accordingly, this can raise the problem that the number of extracted minutiae and region with two fingerprints overlapped may not be sufficient from the fingerprint image acquired, hence reducing the verification performance. The problem with the lack of minutiae cannot be addressed using the conventional MFV that extracts minutiae only from one fingerprint image. The methods that have been proposed to solve these problems, include that of generating a super template by accepting several fingerprints [5], and that of improving the template quality [6]. There is also the

Fig. 1 The smart phones using biometrics

Hybrid-based Fingerprint Verification (HFV) that uses minutiae and phase information [7], which is different from the method of using merely minutiae.

In this paper, HFV, which is based on MFV and uses, to a limited degree, the Binary-image-based Fingerprint Verification (BFV), was proposed to improve the fingerprint verification performance. Simultaneously using MFV and BFV for each verification process will improve security, but the resulting increase in the calculation volume will reduce the convenience of the user's fingerprint verification. Therefore, BFV was used to a limited extent to ensure security while addressing the problem of the user's long verification time. Since the value around the threshold of similarity are similar to those of genuine and imposter, the overall fingerprint verification performance could be reduced. In order to improve the verification result of holding the similarity around the threshold of MFV, this paper proposes the HFV that uses the BFV in the band around the threshold of minutiae similarity. Generally although the binary fingerprint image is the information generated and discarded for the extraction of minutiae, the binary fingerprint image holds more information than minutiae. Accordingly when performing the fingerprint verification around the threshold of MFV by using the binary fingerprint image of holding more comparison information than minutiae with the same image size, the false matching error around the threshold could be reduced. According to the result of experiment, we could see that the False Match Rate (FMR) was reduced by 89 % from 2.77 % of the MFV to 0.28 % of the proposed method. Also, we could check that the Equal Error Rate (EER) of fingerprint verification was improved as well from 3.01 % to 1.73 %. The remainder of this paper is organized as follows. In Sect. 2, we describe the HVF used by the proposed method. The experimental results are presented in Sect. 3, and we conclude in Sect. 4.

2 Proposed Hybrid Fingerprint Verification Using Partial Band

In this paper, the conventional MFV and the BFV were combined to improve the fingerprint verification performance. The HFV is described, and then the combined method that uses minutiae and binary images is described.

2.1 Hybrid Fingerprint Verification System

The HFV combines two or more supplemental verification methods. In this paper, the conventional MFV and BFV were used. The hybrid-based verification method that uses both the MFV and BFV methods are described as follows. Let $\omega_1, \omega_2, \cdots, \omega_n$ represent the n users enrolled in the database. Minutiae (M), which is extracted from the input fingerprint image using the minutiae extraction module, is inputted into the matching module of the first system. The result of the first system is $S(\omega_i \mid M)$, wherein $S(\omega_i \mid M)$ is the similarity of the minutiae of the input fingerprint (M) to ω_i. In the second system, matching is conducted using the additional information on the fingerprints. In this paper, the binary image of fingerprint (B) was used as the additional fingerprint information. The user is verified using the result of the first and second systems, $S(\omega_i \mid M, B)$. Figure 2 shows the integration of the two systems. Unlike the conventional verification method that involves only one piece of information and one verification process, the hybrid-based verification method has two or more verification processes that use different pieces of information. Accordingly, it can reduce the security errors that may occur in the conventional verification process.

In order to solve the problem held by the MFV, this paper has used the image-based fingerprint verification method of using fingerprint image. Since the fingerprint image holds more comparable information than minutiae, it can perform

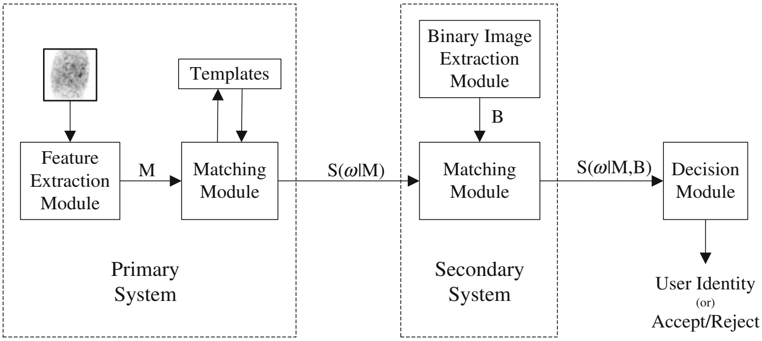

Fig. 2 Integration of BFV with MFV

more accurate verification than minutiae when the overlapped area of two fingerprints is small or the acquired fingerprint image is small.

The Fig. 3 shows the HFV that uses the minutiae and binary image proposed in this paper. Since the fingerprint information is not aligned properly, this requires a process of aligning two fingerprints. As for the alignment methods that use only the finger image, there are the method [8] of using ridges and the method [9] of using the singular points such as core and delta. However, the method of using only the image has some limitations since this requires a lot of calculations and there may be the cases that the singular points do not exist. Therefore, the fingerprint correction of using only the image is less efficient than the method of using minutiae. And, the BFV used in this paper has required more processing time than the method of using minutiae. Accordingly, the BFV should be conducted only to a limited extent. Also while the performance of MFV was excellent in the place of high minutiae similarity, the fingerprint verification error has occurred around the threshold low in the similarity. In this case, this paper refers the area around the threshold as partial band. Accordingly as for the area excluding the partial band high in the reliability, this paper intends to propose the HFV that uses the BFV for the fingerprints holding the minutiae similarity of partial band without performing the BFV. As for the fingerprint image, this paper has used the binary fingerprint image that has gone through the fingerprint quality improvement and binarization occurring in the process of MFV. The binary fingerprint image is small in the data size as compared to that of gray-scale image. And, the contrast of fingerprint image is more obvious than that of gray-scale. Also while going through the image quality improvement and binarization process, it becomes more appropriate for the fingerprint verification as the small noises such as skin wrinkles and pores are removed. For these reasons, in this paper image verification stage is done after the binarization of images.

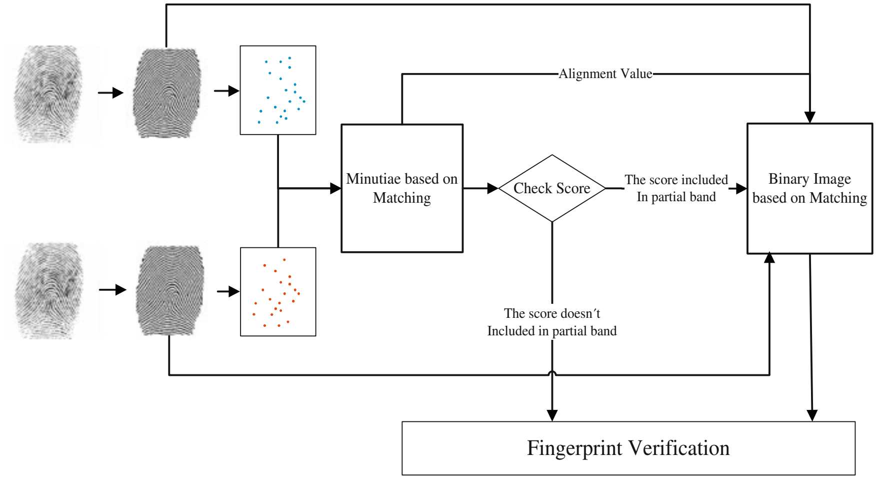
Alignment Value
Minutiae based on Matching
Check Score
The score included In partial band
Binary Image based on Matching
The score doesn′t Included in partial band
Fingerprint Verification

Fig. 3 Proposed HFV system

2.2 Partial Band of Similarity Distribution

The proposed method in this paper has first performed the MFV. And then, this paper determines whether or not to perform the BFV. If the minutiae similarity is held in the partial band necessary to have the BFV, the verification is performed by using the result of BFV after executing the BFV. However when the result of MFV holds the minutiae similarity of the area excluding the reliable partial band, the matching is performed only with the MFV. As for the correction phase of BFV, this paper has used the correction result of MFV. The partial band, which determines execution of the BFV, uses the similarity distribution of MFV. The Fig. 4a shows the similarity distribution of MFV.

The errors in the MFV are distributed around the threshold value th as shown in the Fig. 4a. The cases, which errors have occurred in the MFV, were the case that

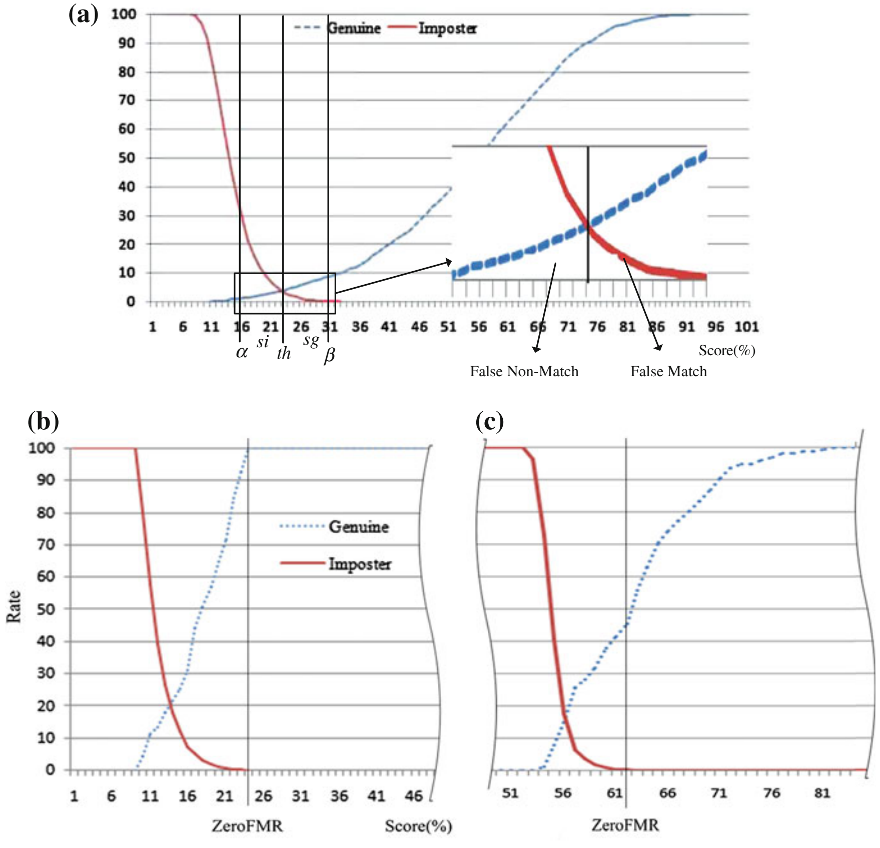

Fig. 4 Similarity distribution of fingerprint verification. **a** Similarity distribution of MFV, **b** Similarity distribution of MFV within the partial band, **c** Similarity distribution of BFV within the partial band

the similarity of genuine becomes below the threshold value as well as the case that the similarity of imposter exceeds the threshold value. These errors are respectively referred to as 'False Non-Match' and 'False Match'. As shown in the Fig. 4a, this paper has used the partial band between the similarity α (where the 'False Non-Match' becomes '0') and similarity β (where the 'False Match' becomes '0') as the maximum band. The S_i and S_g hold the similarity value between th and α and the value between th and β, which are in the similarity range of partial band. Since the similarity values of genuine and imposter around the threshold within the partial band are similar from each other, this is the range that errors occur most frequently. When performing the BFV excellent in the performance of rejecting false matching within this partial band, the verification performance could be improved.

Since the BFV has a lot of comparison information, the FMR could be reduced. However as the False Non-Match Rate (FNMR) is raised, the EER performance could be reduced as compared to the MFV. However as for the minutiae similarity distribution, the gain obtained by the reduction of FMR is larger than the loss by the mismatching error when performing the BFV within the partial band around the threshold. Accordingly from the result of the BFV performed within the partial band, the MFV holds the Zero False Match Rate (ZeroFMR) of 100 % as shown in the similarity distribution of Figs. 4b and c. However since the ZeroFMR of BFV holds the performance of 60 %, it is better than the BFV. Accordingly, this paper has improved the security performance of fingerprint verification by reducing FMR within the partial band area around the threshold. Also, the EER performance was improved by the FMR reduction effect.

3 Experimental Results

This paper has performed the experiment by using the Set A of FVC [10]-DB1 fingerprint database [10]. In case of genuine and imposter, the test was performed respectively for 2,800 times and 4,950 times. As for the similarity partial band of the minutiae to execute the binary image fingerprint verification, this paper has used the similarity distribution. The minutiae similarity partial band that holds the P distribution is selected by using the Eq. (1).

$$\begin{gathered} P = \frac{I(th, S_i) + G(th, S_i)}{I(th, \alpha) + G(th, \alpha)} \times 100 = \frac{I(th, S_g) + G(th, S_g)}{I(th, \beta) + G(th, \beta)} \times 100 \\ I_{(i,j)}\ :\ \text{Number of imposter between the similarity } i \text{ and } j \\ G_{(i,j)}\ :\ \text{Number of imposter between the similarity } i \text{ and } j \end{gathered} \tag{1}$$

In other words, the fingerprint verification performance was tested on the basis of threshold value after finding the similarity below the threshold and above the threshold that hold as many fingerprints for the P ratio. The Fig. 4 shows the

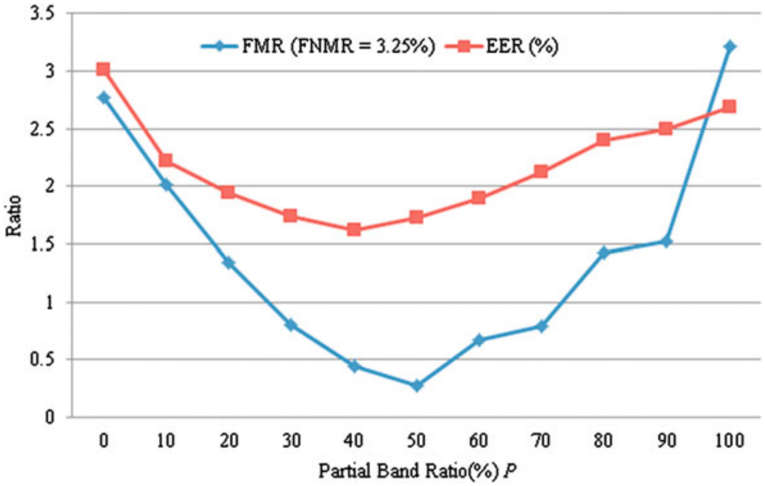

Fig. 5 Fingerprint verification performance by the value of *P*

fingerprint verification performance in accordance with the *P* ratio. As for the partial band ratio, this experiment has checked the performance after measuring the matching result within the partial band for the *P* value of 0 % up to 100 %. Binary fingerprint matching used Dice overlap, define as 2(R ∩ B)/(R + B) where R is registration binary fingerprint image and B is input binary fingerprint image [11].

From the Fig. 5, the case with the partial band ratio *P* of 0 shows the experimental result that has used only the MFV without using the BFV. In order to check the improvement effect of FMR, this experiment has tested the changes in FMR by fixing FNMR and has measured EER to evaluate the verification performance.

According when having fixed FNMR to 3.25 %, the FMR performance was improved more than having used the MFV. Especially when having used only the partial band ratio of 50 %, we could see that the performance was improved from 2.77 % to 0.28 %. Also, the EER of proposed method was improved to 1.62 % from 3.01 %. Through these experimental results, we have verified that the proposed fingerprint verification method not only improves the FMR but also the verification performance.

4 Conclusions

The MFV is the fingerprint verification method most widely used due to its excellent performance and quick processing speed. However, the verification performance is reduced in the case when the acquired image is small. Likewise in order to solve the problem of MFV and to improve the FMR in security, this paper has proposed the HFV that uses both the MFV and BFV methods. In order to combine two verification methods effectively, we have performed the BFV only within the partial band with similar minutiae. After using the proposed method by using the band ratio of 50 %, we could see that the FMR of proposed method was improved by 89 % from 2.77 % to 0.28 % as compared to the MFV and the EER performance was improved by 42 % when having fixed FNMR to 3.25 %. In the future, we plan to study on the image comparison method to improve the processing speed of image based fingerprint verification method.

Acknowledgments This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0023147).

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2010-0005091).

References

1. Jin C, Kim H (2009) High-resolution orientation field estimation based on multi-scale gaussian filter. IEICE Electron Express 6(24):1781–1787
2. Lee S, Choi WY, Moon D, Chung Y (2009) Secure fuzzy fingerprint vault against correlation attack. IEICE Electron Express 6(18):1368–1373
3. Palma J, Liessner C, Mil'Shtein S (2007) Contactless optical scanning of fingerprints with 180°view. Scanning 28(6):204–301
4. Labati, RD (2011) A neural-based minutiae pair identification method for touch-less fingerprint images. In: Computational intelligence in biometrics and identity management, pp 96–102
5. Ryu C, Han Y, Kim H (2005) Super-template generation using successive bayesian estimation for fingerprint enrollment. In: Kanade T, Jain AK, Ratha NK (eds) AVBPA 2005, LNCS, vol 3546. Springer, Heidelberg, pp 261–277
6. Lee K, Park KR, Jang J, Lee S, Kim J (2005) A study on multi-unit fingerprint verification. In: Kanade T, Jain AK, Ratha NK (eds) AVBPA 2005, LNCS, vol 3546. Springer, Heidelberg, pp 141–150
7. Ito K, Morita A, Aoki T, Nakajima H, Kobayashi K, Higuchi T (2005) A fingerprint recognition algorithm combining phase-based image matching and feature-based matching. In: Zhang D, Jain AK (eds) ICB 2006, LNCS, vol 3832. Springer, Heidelberg, pp 316–325
8. Uludag U, Jain AK (2006) Securing fingerprint template: fuzzy vault with helper data. In: CVPRW 2006, pp 163–163
9. Jain AK, Prabhakar S, Hong L, Pankanti S (2000) Filterbank-based fingerprint matching. Image Process 9:846–859
10. FVC2002 database. http://bia.csr.unibo.it/fvc2002/databases.asp
11. Dice L (1945) Measures of the amount of ecologic association between species. Ecology 26(3):297–302