Access Control System with High Level Security Using Fingerprints

Younhee Gil, Dosung Ahn, Sungbum Pan, Yongwha Chung[1]
Information Security Research Division
Electronics and Telecommunications Research Institute
{yhgil, dosung, sbpan}@etri.re.kr
[1] *Dept. of Computer and Information Science*
Korea University
ychungy@korea.ac.kr

Abstract

Biometric based applications guarantee for resolving numerous security hazards. As a method of preserving of privacy and the security of sensitive information, biometrics has been studied and used for the past few decades. Fingerprint is one of the most widely used biometrics. A number of fingerprint verification approaches have been proposed until now. However, fingerprint images acquired using current fingerprint input devices that have small field of view are from just very limited areas of whole fingertips. Therefore, essential information required to distinguish fingerprints could be missed, or extracted falsely. The limited and somewhat distorted information are detected from them, which might reduce the accuracy of fingerprint verification systems. In the systems that verify the identity of two fingerprints using fingerprint features, it is critical to extract the correct feature information. In order to deal with these problems, compensation of imperfect information can be performed using multiple impressions of enrollee's fingerprints.

In this paper, additional three fingerprint images are used in enrollment phase of fingerprint verification system. Our experiments using FVC 2002 databases show that the enrollment using multiple impressions improves the performance of the whole fingerprint verification system.

1. Introduction

Traditionally, verified users have gained access to their property or service via dozens of PIN/password, smart cards and so on. However, these knowledge based, token based security methods have crucial weakness that can be lost, stolen, or forgotten. In recent years, there is an increasing trend of using biometrics. X9.84 [1] standard defines terminology of biometrics as 'A measurable biological or behavioral characteristic, which reliably distinguishes one person from another, used to recognize the identity, or verify the claimed identity, of an enrollee'. The fingerprint is one of widely used biometrics satisfying uniqueness and permanency [2]. Thus a number of fingerprint verification approaches have been proposed until now. Jain et al. [3] presented a minutiae-based verification, which aligns minutiae using Hough transform and performs minutiae matching by bounding box. Ross et al. [5] proposed hybrid matching method of local-based matching and global-based matching to enhance the performance. Pan et al. proposed an alignment algorithm using limited processing power and memory space to be executed in a smart card, and showed the possibility of match-on-card [4]. In the match-on-card system, as entire verification operation is executed on the smart card, the system doesn't have to maintain central database and the biometric template is prevented from being streamed out of the smart card. Therefore, it can prevent biometric templates from being misused by the fraud.

Although it is true that technical improvement has been achieved, there still exist challenging problems relating to the quality of fingerprint images and reliability of extracted minutiae. Most of input devices get fingerprint images having fingerprints being pressed on it not rolled, as a result, the area of fingerprint images can not help being very limited. Fingerprint mosaicking [6] uses multiple fingerprint images to generate template, augmenting minutiae sets

Proceedings of the 32nd Applied Imagery Pattern Recognition Workshop (AIPR'03)
0-7695-2029-4/03 $ 17.00 © 2003 IEEE

from plural fingerprint images on enrollment stage. But, it does not check the reliability of each fingerprint images.

We proposed enrollment using multiple fingerprint images to extend enrolled fingerprint image and also guarantee the reliability of each fingerprint image. And we have tested our algorithm on the first FVC 2002 database [7,8].

This paper is organized as follows. Section 2 describes fingerprint verification system and the enrollment using plural fingerprints briefly. Section 3 explains proposed methods. The experimental results are shown in Section 4. Finally, Section 5 contains conclusion.

2. User Verification Using Fingerprint

It is widely known that the fingerprint is unique, and invariant with aging, which implies that user authentication can be relied on the comparing two fingerprints [2]. In general, a professional fingerprint examiner relies on details of ridge structures of the fingerprint in order to make fingerprint identifications. And the structural features are composed of the points where ridges end or bifurcate, that are called minutiae. Figure 1 shows small part of an enlarged fingerprint image and two types of minutiae pointed by square marker and circle marker. The minutia marked by square is bifurcation, and that by circle is ending point, and the branch from minutia represents the direction of the minutiae. Usually, each minutia is described by the position in the coordinate, the direction it flows and the type, whether it is ridge ending or bifurcation.

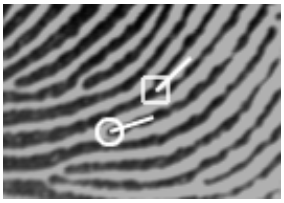


Figure 1: Fingerprint minutiae

Figure 2 presents a fingerprint verification system, which consists of two phases: enrollment and verification. In the off-line enrollment phase, at first, the fingerprint image of an enrollee is acquired and preprocessed. Then, the minutiae are extracted from the raw image and stored as enrolled template. And in the on-line verification phase, it reads the fingerprint from a claimer, and detects the minutiae information through the same procedure as in the enrollment phase. Then, it estimates the similarity between the enrolled minutiae and the input minutiae.

Image preprocessing refers to the refinement of the fingerprint image against the image distortion occurred during the image acquisition and transmission. Minutiae extraction refers to the detection of features in the fingerprint image and finding out of their information, i.e., position, direction and type

Based on the minutiae, the claimed fingerprint is compared with the enrolled fingerprint. Generic minutiae matching is composed of alignment stage and matching stage. In order to match two fingerprints captured with unknown direction and position, the differences of direction and position between two fingerprints should be evaluated, and alignment between them needs to be preceded. In the alignment stage, transformations such as translation and rotation between two fingerprints are estimated, and two minutiae sets are aligned according to the estimated alignment parameters. If the alignment procedure is performed accurately, the remaining matching stage is referred to point matching simply. In matching stage, two minutiae are compared based on their position, direction, and type. Then, a matching score is computed.

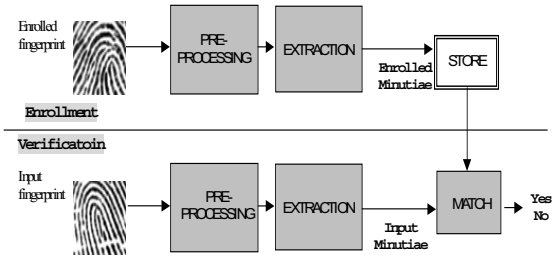


Figure 2: User authentication system using fingerprint

2.1. Minutiae Extraction

Our minutiae extraction algorithm mainly consists of four components: generation of direction map, binarization of fingerprint image, detection of minutiae, and removal of false minutiae.

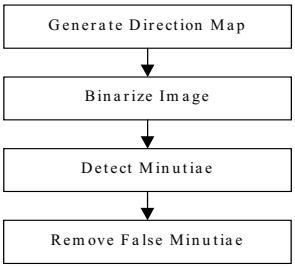


Figure 3: Minutiae Extraction

Besides these steps, it is critical to analyze the image and determine the areas that are degraded and likely to cause problem because the image quality of a fingerprint may vary. Several characteristics can be measured that convey information regarding the quality of localized regions in the image. These include detecting regions of low contrast and determining directional flow of ridges. Using this information, the unstable areas in the image where minutiae detection is unreliable can be distinguished.

Generation of Direction Map. One of the fundamental steps in minutiae extraction is deriving a directional ridge flow map. The purpose of this map is to represent areas of the image with sufficient ridge structure. Well-formed and clearly visible ridges are essential to reliably detecting minutiae. In addition, the direction map records the general direction of the ridges as they flow across the image. The directional information are estimated based on the 8 8 pixel sized windows and their range is 0~15. And background that has no variation of intensity is set as –1. This information can be used to segment images.

Binarization of Image. As our minutiae detection algorithm is working on bi-level image, every pixel in the grayscale input image must be binarized. A pixel is assigned as a binary value based on the ridge flow direction associated with the block the pixel is within. In order to determine whether current pixel should be set to black or white, the pixel intensities of 7 9 pixel grid rotated according to the orientation of it, which surround the current pixel, are analyzed. Grayscale pixel intensities are accumulated along each rotated row in the grid, forming a vector of row sums. The binary value to be assigned to the center pixel is determined by multiplying the center row sum by the number of rows in the grid and comparing this value to the accumulated grayscale intensities within the entire grid. If the multiplied center row sum is lower than the total intensity of the grid, the center pixel is set to black. Otherwise, it is set to white.

Detection of Minutiae and Removal of False Minutiae. Before minutiae are detected, the binarized image should be thinned, and the detection step scans the thinned image with some kernels that can detect minutiae. After detection of minutiae, candidate minutiae points are detected. Usually, many false minutiae are included in the candidate list, therefore, removal of them are necessary to increase the performance of the fingerprint verification system. The step includes removing islands, lakes, holes, minutiae in regions of poor image quality, hooks, overlaps, minutiae that are too wide, and minutiae that are too narrow. The more details about minutiae extraction can be found in [2].

2.2. Enrollment with Plural Fingerprint Images

As automatic fingerprint identification and authentication systems rely on representing the two most prominent minutiae, i.e., bifurcation and ridge ending, a reliable minutiae extraction algorithm is critical to the performance of the system. However, although minutiae are detected through not only extraction process but also false minutiae removal process, it is still possible to detect false minutiae and miss true ones. These faults can cause matching failure. In particular, if they occur during enrollment phase and are stored as enrolled template, it will be serious problem, because they will affect the matching phase continuously. In the other word, if the system ensures there are neither false minutiae nor missed minutiae, its reliability will be increased.

We suggested using plural fingerprint images on the enrollment phase to discard the false minutiae and compensate the missed minutiae. The system that adopts the enrollment using multiple fingerprint images is shown in figure 4. As this figure presents, enrolled minutiae are generated from several genuine fingerprint images.

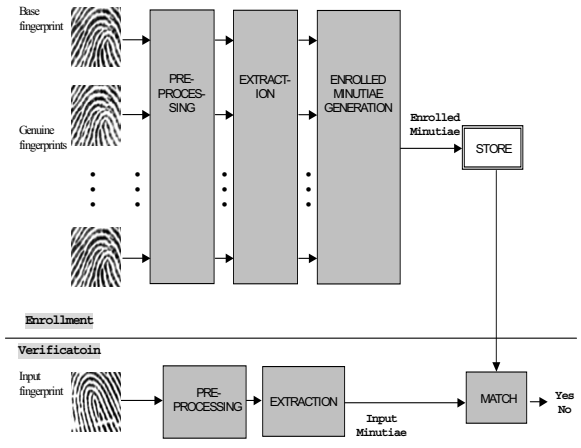


Figure 4: User Authentication system that adopts the enrollment using plural fingerprint images

2.3. Minutiae Matching Algorithm

As mentioned before, minutiae matching is composed of alignment stage and matching stage. In order to make the explanation easier, we define the

notation of two minutiae sets extracted from enrolled and claimed fingerprint images two minutiae sets as P and Q respectively.

$$\mathbf{P} = \{(p_x^1, p_y^1, \alpha^1), \ldots, (p_x^P, p_y^P, \alpha^P)\}$$
$$\mathbf{Q} = \{(q_x^1, q_y^1, \beta^1), \ldots, (q_x^Q, q_y^Q, \beta^Q)\} \quad (1)$$

where (p_x^i, p_y^i, α^i) and (q_x^j, q_y^j, β^j) are the three features (spatial position and direction) associated with the *i*th and *j*th minutia in the set P and Q respectively, and *P* and *Q* are the number of elements in the P and Q set.

The alignment stage gets two minutiae sets, P and Q, as input and estimates how their differences of position and orientation were when the two fingerprints were captured. And then, transforms minutiae set Q for the claimed fingerprint to have same locality as the enrolled fingerprint according to the estimated difference. We denote aligned minutiae set Q as Q^a. For the purpose of proper alignment, the estimation of the rotation and translation parameters must precede. In order to estimate transformation parameters, we find out $(\Delta x, \Delta y)$ and $\Delta\theta$ satisfying formula (2) according to the formula (3).

$$F_{\theta,\Delta x,\Delta y}((q_x, q_y, \beta)^T) = (p_x, p_y, \alpha)^T \quad (2)$$

$$F_{\theta,\Delta x,\Delta y}\begin{pmatrix} x \\ y \\ \theta \end{pmatrix} = \begin{pmatrix} \cos\Delta\theta & \sin\Delta\theta & 0 \\ -\sin\Delta\theta & \cos\Delta\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ \theta \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \\ \Delta\theta \end{pmatrix} \quad (3)$$

where $(\Delta x, \Delta y)$ and $\Delta\theta$ are the translation and rotation parameters; $(p_x, p_y, \alpha)^T$ represents the enrolled minutiae and $(q_x, q_y, \beta)^T$ represents the claimed minutiae.

The evaluated transformation parameters $(\Delta x, \Delta y, \Delta\theta)^T$ are used to align claimed minutiae by

$$\begin{pmatrix} q_x^a \\ q_y^a \\ \beta^a \end{pmatrix} = \begin{pmatrix} \cos\Delta\theta & \sin\Delta\theta & 0 \\ -\sin\Delta\theta & \cos\Delta\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} q_x \\ q_y \\ \beta \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \\ \Delta\theta \end{pmatrix} \quad (4)$$

where $(q_x^a, q_y^a, \beta^a)^T$ is the aligned of the claimed minutiae.

After alignment step, the comparison of the information of two minutiae sets, P and Q^a, is accomplished by point pattern matching in the polar coordinate system with respect to the center of foreground. Such a point matching can be accomplished by placing bounding box [3] around enrolled minutiae. When an aligned minutia is placed within the bounding box, the minutia is considered as a candidate of the mated one with the enrolled minutiae. And two additional conditions will be checked: whether the difference between their directions is below predetermined tolerance, and whether their types are the same. Their results affect the matching score. It depends on the size of bound box that how many candidates match. The smaller the size is, the stricter matching stage gets and it can be happened that the rate of falsely non matching is increased, and the opposite case is the same way likewise. It is possible that there is more than one candidate for one enrolled minutia. In this case, the candidate with the largest score is selected as mated minutiae. Figure 5 shows an example of mating of two minutiae. Assume that m_1, m_2 are enrolled minutiae and n_1, n_2 are input minutiae to be mated and the kinds of four minutiae are same. The direction of each minutia is marked as branch from minutia, and they are assumed to be similar enough so that their difference is within the tolerance. Then, consider the mating result. In this case, it is reasonable that n_1 is mated with m_1 and n_2 with m_2. Although both n_1 and n_2 are candidates of the mated minutiae with m_2, n_2 must be regarded as mated minutia with m_2 because n_2 is nearer to m_2 than n_1. Also, correlation of n_1 with m_1 should be considered. Even if n_1 is a mated candidate of not only m_1 but also m_2 and it is nearer to m_2 than m_1, it should be mated with m_2, as m_2 has been mated with n_1 already.

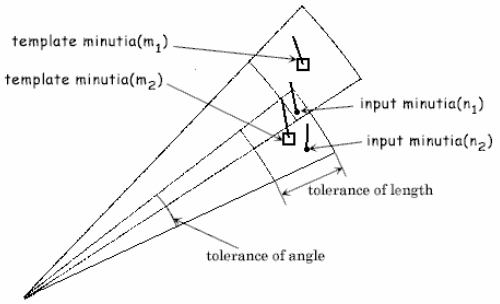
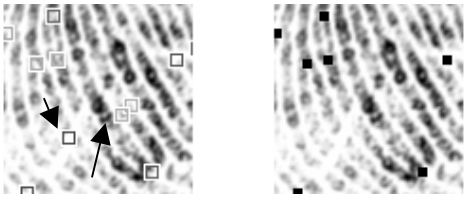


Figure 5: Mating of minutiae

3. Multiple Fingerprint Images and Enhanced Matching Method

Usually, even superior extraction process including removal of false minutiae have some false minutiae remained still. And it can miss the true ones. The performance of fingerprint verification is influenced by both of them. Figure 6 is enlarged part of fingerprint images and shows some extracted minutiae. In Figure 6 (a), examples of false minutiae are presented being pointed out with black arrows. They are neither the bifurcation nor the ending of ridges, are just points on the middle of ridges. They should not have been detected. These are caused by couple of reasons such as failure in extraction stage or noise of fingerprint image itself. However, these can be eliminated based on the fact that they are temporal and no false minutia

on the same position in one image as another fingerprint image may merely be detected. Therefore, plural fingerprint images are used on the enrollment phase in order to discard the false minutiae.



(a) (b)

Figure 6: Extracted minutiae including false minutiae superimposed on the enlarged fingerprint image and discarded result of false minutiae

In the enrollment phase using multiple impressions, at first, one fingerprint image is acquired and set as base image, and minutiae from it are extracted. Then after segmentation of image, find out the center of foreground, which will be the reference point of polar coordinate system. And then, minutiae set from base fingerprint image are transformed into polar coordinate system. Once finishing above processes to the base image, a few genuine fingerprint impressions are acquired. And minutiae from each fingerprint image are extracted, and each minutiae set is aligned with base fingerprint image. Then, they are converted into polar coordinate system with respect to the center of base image. Now, each minutia from one fingerprint image is examined if it can be mated with the minutia from the other fingerprint image. To do this, it is required to compute similarity between two minutiae. The minutia is regarded as false minutia if it has been mated with no minutia during whole examinations, and discarded. Figure 6 (b) shows the false minutiae have been discarded through our false minutiae discard step. The simple flowchart of false minutiae discard algorithm is shown in Figure 7.

Another factor reducing the accuracy of the verification is limited contact area of fingerprint scanner. As input device is getting smaller, the size of window acquiring image has been shrunk. And owing to the tiny window, the verification system use only partial regions of fingerprint images. Therefore, two identical fingerprint images can be misjudged they are from different fingerprints if two images are scanned from the opposite parts of the fingertip. Besides the extreme case like this, when the overlapped area of two images is small, it causes low matching score.

In order to compensate one minutiae set from the identical fingerprint images that have little common area, padding method of minutiae in non-overlapped area is used. This method first measures the overlapped area of two fingerprint images, and then finds out minutiae pairs in the area. To estimate the intersected area, segmentation of two images should precede. Next, it estimates the ratio of minutiae pairs to total enrolled minutiae. It regards two fingerprint images as ones from the same finger when the ratio is over the predetermined threshold. And in the case when two minutiae sets are determined to be identical, it appends the enrolled minutiae in the non-overlapped area to the claimed minutiae set. Then more mated pairs can be found and it will improve matching performance.

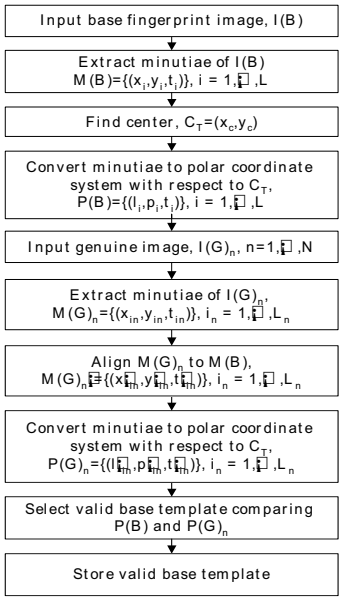


Figure 7: Enrollment using multiple impressions

4. Experimental Results

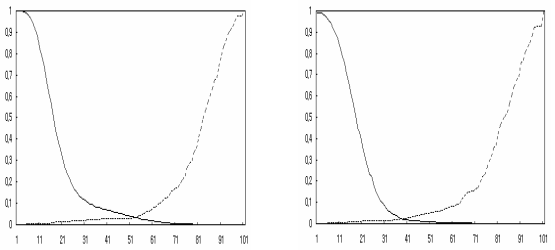
We have tested our fingerprint verification algorithm using one of the FVC 2002 databases [7,8]. There are four different databases in the FVC 2002 databases, each of which were collected by different scanners or generated by using SFinGE software. Hence, they have different image size and resolution. Every database consists of two classes, set A for evaluation and set B for training. Set A is composed of eight fingerprint images per one finger from 100 individuals for a total of 800 fingerprint images and set B from 10 individuals for a total of 80 images. The details about FVC 2002 databases are in [8]. Among them, A set of DB1 was used in our experiment. The size of fingerprint images of DB1 was 388 374 at 500dpi.

For the enrollment, the first four fingerprint images among eight were used, and the remaining four were

used for verification. Therefore, when a matching was labeled GENUINE if the matching was performed between fingerprint images from same finger, and IMPOSTER otherwise, 400 GENUINEs were able to be performed. And 9900 IMPOSTERs were performed, i.e., 99 IMPOETERs have been tested for one fingerprint using the other 99 fingerprints.

We performed two matching tests in order to show the effect of the adoption of enrollment using multiple impressions, matching after enrollment using single impression and matching after enrollment using multiple impressions. Figure 8 presents the distribution of false match rate and false non-match rate. Vertical axis represents the normalized distribution of matching scores, and horizontal axis represents the score ranging from 0 to 100. As shown in the curve of Figure 8 (b), it is observed that equal error rate is lower by 1.38% when using multiple impressions on enrollment than when using single impression.

When false non-match rate is set 1%, false matches happen at the rate of about 40% in the former. In the other hand, the false match rate of the latter is 6.15%.



(a) (b)

Figure 8:FMR/FNMR curve, (a) case when using one fingerprint image on the enrollment, (b) case when using four fingerprint images on the enrollment

5. Conclusion and Future Work

This article shows the comparison between matching performances when using single fingerprint image on enrollment phase and when using multiple fingerprint images. If plural fingerprint images are used during enrollment, extracted and stored minutiae can be quaranteed becuase false minutiae are discarded and missed ones are added in the final minutiae set. And we confirmed this by experiments. On using multiple impressions on enrollment, equal error rate decreased by 1.38% as compared with the case when using single impression, and its FMR 100[7] is 6.15%.

The enrollment phase using multiple impressions can be part of match-on-cord [4] system. The match-on-card system is shown in Figure 9. In the match-on-card system, the whole matching step should be executed in the smart card and the processing power of smart card is very limited [4]. Therefore, it is essential to extract reliable minutiae in order to make matching more accurate even though matching step uses only simple information of minutiae such as the position, direction and type.

Although the performance of matching adopting the proposed enrollment was improved considerably, the result is not satisfied yet. Thus, it is required to enhance the algorithm and study new method.

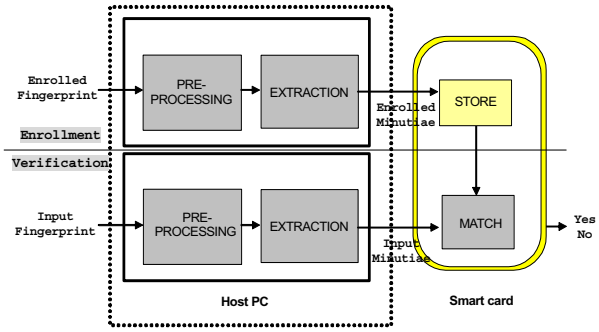


Figure 9: Fingerprint based Match-on-Token

References

[1] ANSI web site, http://www.ansi.org/

[2] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.: Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press LLC, (1999)

[3] Jain, A., Hong, L., Bolle, R.: On-line Fingerprint Verification. IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol.19, No.4 (1997) 302–313

[4] Pan, S.B., Gil, Y.H., Moon, D., Chung, Y., Park, C.H.: A Memory-Efficient Fingerprint Verification Algorithm using A Multi-Resolution Accumulator Array, ETRI Journal, Vol. 25, No. 3, (2003) 179–186

[5] Ross, A., Jain, A. K., Reisman, J.: A Hybrid Fingerprint Matcher, Pattern Recognition, Vol. 36, No. 7, (2003) 1661-1673

[6] Jain, A. K., Ross, A.: Fingerprint Mosaicking, Proc. ICASSP, (2002)

[7] FVC 2002 web site, http://bias.csr.unibo.it/fvc2002

[8] Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain, A.K.: FVC2002:Second finger-print verification competition, Proc. ICPR, (2002)