Fingerprint Matching Algorithm using String-Based MHC Detector Set

Jae-Won Jeong, In-Hun Jang, and Kwee-Bo Sim
School of Electrical and Electronics Engineering, Chung-Ang University
221, Heukseok-Dong, Dongjak-Ku, Seoul 156-756, KOREA
E-mail: kbsim@cau.ac.kr

***Abstract* – Fingerprints have been widely used in the biometric authentication because of its performance, uniqueness and universality. Lately, the speed of identification becomes a very important point in the fingerprint-based security applications. Also, the reliability still remains the main issue in the fingerprint identification. In this paper, we propose the fast and reliable fingerprint matching algorithm based on the process of the 'self-nonself' discrimination in the biological immune system. The proposed algorithm is organized by two-matching stage. The 1st matching stage does the matching process by the use of the self-space and MHC detector string set that are generated from the information of the minutiae and the values of the directional field. Then the 2nd matching stage is made based on the local-structure of the minutiae. The proposed matching algorithm can reduce matching time while the reliability of the matching algorithm is maintained.**

I. INTRODUCTION

Biometric is a technology for person identification by the use of the extracted his(or her) physiological or behavioral characteristics[1]. Fingerprint, face, iris, retina, hand vein, signature, voice print are called as a 'biometric identifier' and are used in the biometric technologies[2]. Conventional identification systems such as magnetic card, password, user ID are rely on possessions or special knowledge[3]. However, these identification systems can easily fooled relatively and cannot ensure that the authorized person is the reliable user[3]. When using the password or user ID, the user may remember the certain password or ID to authorize. Also, the user must possesses the correct item for using the system based on a card or a key. On the contrary, biometrics can offer more reliable personal identification by the property of using the biometric identifiers. Also, biometrics do not need any possessions or special knowledge for personal identification. Therefore, the biometrics are highlightened as new personal identification methods instead of conventional identification methods.

Fingerprint is one of the biometric identifiers that is a collection of a flow by ridges and valleys of the outer layer of the finger skin. As a biometric identifier, fingerprint has the advantages than other biometric identifiers as face, iris, hand vein....etc for the comparison index that are composed of uniqueness(distinctiveness), permanence and performance[1][2][4]. So the fingerprint identification is the most widely used biometric technology in the field of the security applications[2][4]. Now most of the fingerprint matching and identification are achieved based on the data of the minutiae that are extracted from the fingerprint image[2]. Fingerprint matching algorithms based on the aligning fingerprint image pairs gain good performance in the identification in spite of noisy fingerprint images. However, these matching methods are a computationally intensive task[5]. For this reason, alignment-based matching methods have difficulties to get more fast matching time[6].

In this paper, we propose a fast and reliable fingerprint matching algorithm that is inspired by the MHC protein recognition in the process of the 'self-nonself' discrimination of the biological immune system[7]. The modeling of the 'self-nonself' discrimination is made by the distribution of the minutiae and the local ridge orientations. Also, our proposed algorithm considers the topological structures of minutiae for the robust fingerprint matching against translation and rotation.

II. IMMUNE SYSTEM AND MHC PART FOR SELF-RECOGNITION

Biological immune system (BIS) is the 2nd defensive system of the creatures that defenses the self against foreign invaders (antigen) such as a bacterium, a virus... etc. BIS has the property of the distributed autonomous system and the ability of learning, memorize the information about the antigen [8]. Also, BIS eliminate the antigen through the 'self-nonself' discrimination [9]. These characteristics of the BIS are artificially represented for the industrial application. We refer to the artificial modeling of the BIS as the artificial immune system (AIS).

A function of BIS is accomplished by the operation of B-cell and T-cell. B-cell secrete antibodies to eliminate antigens. T-cell is classified into three classes [10]: helper T-cell, cytotoxic T-cell, and suppressor T-cell. Cytotoxic T-cell recognizes infected cells by antigens and kills infected cells. It has two recognition parts. The MHC recognition part recognizes the MHC protein that tells whether a cell is self cell or not. Also antigen recognition part recognizes the foreign invaders as an antigen. In this paper, the modeling of the MHC recognition part is made based on the minutiae and the directional field of the fingerprint image, and is applied to the fingerprint matching.

III. MINUTIAE EXTRACTION FOR FINGERPRINT IDENTIFICATION

The minutiae based on the topological structure of the ridge are useful characteristics for the fingerprint identification. The ANSI (American National Standards Institute) classifies the minutiae into four kinds: ridge ending, ridge bifurcation, crossover, and undetermined [11]. Fig. 1 shows the examples of the ridge ending and ridge bifurcation.

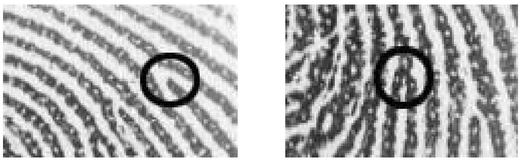
a) Ridge ending b) Ridge bifurcation

Fig. 1. Ridge ending and ridge bifurcation.

Among them, ridge ending and ridge bifurcation are mainly used to match and identify the fingerprints [11]. There are two kinds of the minutiae extraction from the fingerprint image: binarization-based method and direct gray-scale extraction method [2]. In this paper, we use ridge ending and ridge bifurcation that are extracted by the binarization-based method that binarizes the image and then skeletonizes the image for the extraction of the minutiae for the fingerprint identification.

IV. FINGERPRINT MATCHING ALGORITHM USING THE STRING-BASED MHC DETECTOR SET

Fingerprint matching process that makes comparison between input fingerprint image and template fingerprint images and makes a decision of the authentication. In this paper, we propose the fast and robust fingerprint matching algorithm based on the self-recognition model of the artificial immune system. The existing fingerprint matching algorithms based on the minutiae of the fingerprint uses all of the minutiae in the template fingerprint images and in the input fingerprint image for the fingerprint matching. In contrast to the existing methods, proposed matching algorithm in this paper do the 1st matching stage by the use of the self-space that is constructed by the distribution of the minutiae and the directional field of the template fingerprint image and the MHC recognition part that is constructed from the self-space of the input fingerprint image. The 1st matching stage reduces the candidate set of the template images that are used in the 2nd matching stage by the matching scores of the 1st matching stage. Also 2nd matching stage is accomplished by the local structure of the minutiae within the matched area in the 1st matching stage to decide whether they are matched or not. First and 2nd matching stages can reduce the number of the template images and the minutiae to enhance the matching time.

In the 1st matching stage, the algorithm divides the input fingerprint image into the block of size 16×16 pixels. Each block is expressed by the binary numbers and six bits are allocated to each block. Repeat this process to whole divided blocks in the fingerprint image, and then the set of the binary strings are made to organize the self-space. Fig. 2 illustrates the construction of the self-space string set.

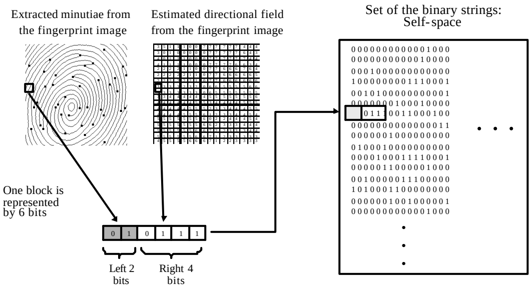

Fig. 2. Construction of the self-space from the fingerprint image.

Table. 1 shows the decision condition of the values of the 6bits that are assigned to each block. Left 2 bits represents whether the minutiae is exist in the block or not. Also, right four bits represents the value of the directional field in the block.

Conditions of the left 2 bits

Bits	Conditions
00	No minutia exists in the block
01	One end-point exists in the block
10	One bifurcation exists in the block
11	At least two minutiae in the block

Conditions of the right 4 bits

Bits	Value of the directional field	Angle	Bits	Value of the directional field	Angle
0000	0	0°	1111	4	90°
0001	1	22.5°	1110	5	112.5°
0011	2	45°	1100	6	135°
0111	3	67.5°	1000	7	157.5°

Table. 1. The decision condition of the value of 6 bits that are assigned to each block.

From the strings that form the 'self-space', bits (the length of bits are arbitrarily selected) are extracted from the center of the binary strings of the ‘self-space’, then the extracted bit strings organize the MHC detector set that is composed of the *N* MHC detector strings of bits long.

MHC detector set that is generated from the input fingerprint image is matched to the binary string set of the ‘self-space’ that is generated from the template fingerprint image (the size of the ‘self-space’ of the template fingerprint image is the same as the size of the ‘self-space’ of the input fingerprint image). One of the MHC detector string in the MHC detector set is matched to the binary string of the ‘self-space’ of the template fingerprint image by the process that is shown in Fig. 3, and then the algorithm finds the position of the best matching score. Als o, the score of the each detector about one of the template images is added up, and those total scores are compared to find the template images with relatively high matching score. These template images that have high matching scores in the 1st matching stage are selected and 2nd matching stage is applied to the selected template images in the 1st matching stage.

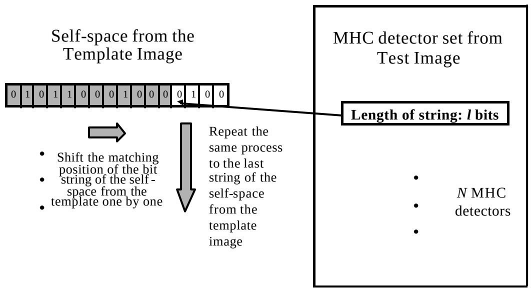
Self-space from the Template Image
0 1 0 1 1 0 0 0 1 0 0 0 0 1 0 0
• Shift the matching position of the bit string of the self-space from the template one by one
Repeat the same process to the last string of the self-space from the template image
MHC detector set from Test Image
Length of string: *l* bits
N MHC detectors

Fig. 3. MHC detector set from the input fingerprint image is matched to the self-space of the template.

4.1 Detector testing algorithm

However, by the characteristics of the bit-pattern matching and the matching process in Fig.3, the possibility that the MHC detector from the input fingerprint image is matched in the ‘unexpected’ position of the self-space from the template fingerprint image cannot be neglected. So the additional process that is showed in the next is applied for the correction of this problem.

[Step 1] When the process in Fig. 5 is finished, calculate the *PD*(*i*) for each MHC detector by Eq. (1). PD(i) means that the difference of the best-scored matching position between the self-space and MHC detector.

$$PD(i) = j - i \tag{1}$$

i(*i* = 0, 1, …, *N*-1) indicates the row number of the MHC detector, and *j* is the row number of the self-space. *N* is the total number of the MHC detector string.

[Step 2] Use the *PD*(*i*) that are calculated in Step 1 to evaluate the PD_{av} by the following Eq. (2).

$$PD_{av} = \frac{\sum_{i=0}^{N-1} PD(i)}{N} \tag{2}$$

[Step 3] Using *PD*(*i*) and PD_{av}, calculate the diff(i) for each MHC detector by Eq. (3). *i* is the row number of the MHC detector.

$$diff(i) = PD(i) - PD_{\mathrm{av}} \tag{3}$$

If $|diff(i)| > B$ (*B* is the boundary value that is decided by empirical results), the matching score of that MHC detector is set to zero and that detector is excluded from the matching process. Else the matching score of that MHC detector remains unchanged and applies to the matching process.

The number of μ template images that are selected by the matching score of the 1st matching stage are used to the 2nd matching stage to reduce the matching time. In the process of the 1st matching stage to match the self-space from the template images with the MHC detector set from the input fingerprint image, for the matched position of the MHC detector and selected self-space in the 1st matching stage with the best score, the algorithm generates the local structure that is composed of the minutiae in the input and template fingerprint images. Also the local structure considers the minutiae in the matched blocks as a center point. Then the proposed algorithm does the 2nd stage matching toward the constructed local structures [12][13].

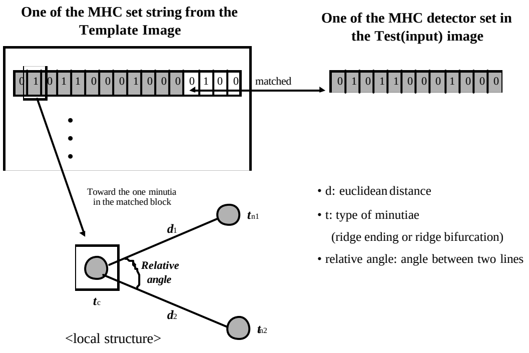
One of the MHC set string from the Template Image
0 1 0 1 1 0 0 0 1 0 0 0 0 1 0 0
matched
One of the MHC detector set in the Test(input) image
0 1 0 1 1 0 0 0 1 0 0 0
Toward the one minutia in the matched block
t_{n1}
d_1
Relative angle
t_c
d_2
t_{n2}
<local structure>
• d: euclidean distance
• t: type of minutiae (ridge ending or ridge bifurcation)
• relative angle: angle between two lines

Fig. 4. The 2nd matching stage that is based on the local structure of the two neighborhood points and the parameters of the local structure

Fig. 4 shows the process of the 2nd matching stage based on the local structure and the form of the local structure that have two neighborhood points. The parameters of the local structure in the 2nd stage are invariant against rotation and translation. So using the local structure in the 2nd matching stage guarantees the robust fingerprint matching against translation, rotation, and other transformations of the fingerprint image. The matching scores of the 2nd matching stage are compared to find the template image that have the best 2nd matching score, and the algorithm regards that as the authenticated fingerprint image.

V. Experimental Results

In our experiments, we used the fingerprint image of size 288 (wid)×320 (hgt) pixels that is scaned from the optical fingerprint sensor with 500 DPI. We assume that the fingerprint images in the experiments are aligned. To apply the 1st matching stage of the proposed algorithm in this paper, fingerprint image is divided into the block of size 16×16 pixels, and the fingerprint image has total of 18 (row)×20 (column) blocks. Then the most outer blocks in the fingerprint image are excluded from the process, and self-space is made of 18 binary strings. Each binary string has a length of 96 bits (16 blocks). 10 MHC detector strings(N=10) are made from the self-space of the input fingerprint image, and each MHC detector has a length of 72 bits.

The local structures of the minutiae are used in the 2nd matching stage. Each local structure is constructed by the center minutia that exists in the matched position and two neighborhood minutiae that are more closer to the center minutia than others. The parameters of the local structure is showed in table. 2[12].

Table. 2. The parameters of the local structure.

Types of minutia	Parameters	
Center minutia	types of minutia	end-point or bifurcation
Neighborhood minutia	types of minutia	end-point or bifurcation
	distance to the center minutia	$\sqrt{dx^2 + dy^2}$ $dx = x_n - x_c$ $dy = y_n - y_c$
	relative angle	$q = \tan^{-1}\frac{dy}{dx} - q_c$ q_c is the angle of the center minutia

Total of 1000 fingerprint images are used in the experiments. m is a number of selected template images that have high matching scores in the 1st matching stage. Experimental results are shown in table. 3.

Table. 3. First and 2nd matching results by the change of the parameter 'm'

m	The result of the 1st matching stage: The percentage that the result includes the proper template image.(%)	The result of the 2nd matching stage: The final identification rate that the input image is authenticated properly. (%)
1	91.0	91.0
2	99.7	99.7

VI. Conclusion

In this paper, we suggested the fingerprint matching algorithm based on the self-recognition model by the MHC recognition part of the cytotoxic T-cell from the biological immune system. 1st stage matching is obtained by the use of the 'self-space' of the template and the MHC detector set of the input fingerprint image. Also this process reduces the candidate set of the minutiae and the template images that are used to the 2nd matching stage for the fast matching. In the 2nd matching stage, MHC detector string that is matched to the binary string of the 'self-space' of the template is used to construct the local structure which regards the minutia in the matched MHC detector as the center minutia. The parameters of the constructed local structure are invariant against rotation and translation of the fingerprint image, and these parameters of the local structure is used to the 2nd stage matching for an improvement of the reliability in the matching process.

Future works are the elevation of the identification rate, and the comparison of our algorithm with the other algorithm for more fast and reliable fingerprint identification system.

Acknowledgement

This research was supported by the Small & Medium Business Administration (SMBA) of Korea.

REFERENCES

[1] A. K. Jain, Lin H., S. Pankanti and R. Bolle, "An identify-authentication system using fingerprints," *Proc. of the IEEE*, vol. 85, pp. 1365-1388, 1997.

[2] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.

[3] R. M. Bolle, J. H. Connell, N. K. Ratha, "Biometric perils and patches," Pattern Recognition, vol. 35, no. 12, pp. 2727-2738, 2002.

[4] K. B. Sim, C. B. Ban and J. Y. Sim, "Development of Intelligent Fingerprint Recognition System," *The Journal of KASBIR*, vol. 1, no. 2, pp. 111-119, 2001.

[5] A. Ross, A. Jain, J. Reisman, "A hybrid fingerprint matcher," Pattern Recognition, vol. 36, no. 7, pp. 1661-1673, 2003.

[6] A. Wahab, S. H. Chin, E. C. Tan, "Novel Approach to automated fingerprint recognition," Proc. of IEEE Conf. on Vision, *Image and Signal Processing*, vol. 145, pp. 160 -166, 1998.

[7] K. B. Sim and D. W. Lee, "Change detection algorithm based on positive and negative Selection of developing T-cell," *Journal of Fuzzy logic and Intelligent Systems*, vol. 13, no. 1, pp. 119-124, 2003.

[8] D. Dasgupta, *Artificial Immune Systems and Their Application*, Springer-Verlag Berlin Heidelberg, 1999.

[9] J. W. Yang, D. W. Lee, K. B. Sim, Y. S. Choi and D. I. Seo, "Intrusion detection algorithm based on artificial immune system," *Proc. on ICCAS2002*, pp. 110-114, 2002.

[10] T. Tomio, *The Meaning of the Immune System*, Han-Wool, 1998.

[11] Alessandro Farina, Zsolt M. Kovacs-Vajna* and Alberto Leone, "Fingerprint minutiae extraction from skeletonized binary images," *Pattern Recognition*, vol. 32, no. 5, pp. 877-889, 1999.

[12] X. Jiang and W. Y. Yau, "Fingerprint minutiae matching based on the local and global structires," *IEEE Proc. on Pattern Recognition*, vol. 2, pp. 1038-1041, 2000.

[13] D. P Mital and E. K. Teoh, "An automated matching technique for fingerprint identification," *Proc. on KES '97.*, vol. 1, pp. 142-147, 1997.