International Journal of Fuzzy Logic and Intelligent Systems, vol. 7, no. 2, June 2007, pp. 109-114

Fingerprint Matching Algorithm using String-Based MHC Detector Set

Kwang-Eun Ko*, Young-Im Cho, and Kwee-Bo Sim*†**

*** School of Electrical and Electronic Engineering, Chung-Ang University**
221, Heukseok-Dong, Dongjak-Gu, Seoul, 156-756, Korea
**** Department of Computer Science, The University of Suwon**

Abstract

Fingerprints have been widely used in the biometric authentication because of its performance, uniqueness and universality. Lately, the speed of identification has become a very important aspect in the fingerprint-based security applications. Also, the reliability still remains the main issue in the fingerprint identification. A fast and reliable fingerprint matching algorithm based on the process of the 'self-nonself' discrimination in the biological immune system was proposed. The proposed algorithm is organized by two-matching stages. The 1st matching stage utilized the self-space and MHC detector string set that are generated from the information of the minutiae and the values of the directional field. The 2nd matching stage was made based on the local-structure of the minutiae. The proposed matching algorithm reduces matching time while maintaining the reliability of the matching algorithm.

Key words : Fingerprint, Matching Algorithm, Self-Nonself, Biological Immune System, MHC Detector

1. Introduction

Biometric is a technology for 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 rely on possessions or special knowledge[3]. However, these identification systems can be fooled relatively easily and cannot ensure authenticity of the user[3]. When using the password or user ID, the user must remember the password or ID to authorize him/herself as well as possess the correct item for using the system based such as a card or a key. On the contrary, biometrics can offer more reliable personal identification by the property of using the biometric identifiers without any possessions or special knowledge to use the system. Therefore, the biometrics is emerging to replace conventional identification methods.

Fingerprint is a collection of a flow by ridges and valleys of the outer layer of the finger skin that can be used as a biometric identifier. The fingerprint has the advantages than other biometric identifiers such as face, iris, hand vein because of its comparison index that are composed of uniqueness (distinctiveness), permanence and performance[1][2][4]. Therefore, the fingerprint identification is the most widely used biometric technology in the field of the security applications[2][4]. Currently, 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 yield accurate identification in spite of incomplete fingerprint images. However, these matching methods are a computationally intensive task[5]. And the alignment-based matching methods take a relatively long time[6].

Therefore, inspired by the MHC protein recognition in the process of the 'self-nonself' discrimination of the biological immune system, a fast and reliable fingerprint matching algorithm was proposed[7]. The modeling of the 'self-nonself' discrimination is made by the distribution of the minutiae and the local ridge orientations. Also, the proposed algorithm considered the topological structures of minutiae for the robust fingerprint matching against translation and rotation of the fingerprint image.

2. Artificial Immune System

2.1 Immune System and Related Works

Biological immune system (BIS) is the 2nd defensive system that defenses 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, and memorizing the information about the antigen[8]. The BIS also

Manuscript received Apr. 4, 2007; revised May. 25, 2007.
† Corresponding author
This research was supported by the Development of Social Secure Robot using Group Technologies of Growth Dynamics Technology Development Project by Ministry of Commerce, Industry and Energy, Korea.

eliminates the antigen through the 'self-nonself' discrimination[9]. These characteristics of the BIS are artificially represented for the industrial application. The artificial modeling of the BIS is referred as the artificial immune system (AIS). AIS can be widely used in the various application such as, network security[9], distributed autonomous robot system, searching (searching what?), pattern recognition, and etc. Also, the AIS for the image processing and pattern recognition has been actively studied by researchers[10], [11], [12]. For example, an image registration for sensor fusion is accomplished by the Genetic Algorithm(GA) based on the AIS[10]. Reference [11] demonstrated that the color image classification can achieved by the binary string-based AIS. The comparison of the negative selection algorithm with the GA based on the AIS is shown in [11]. (Instead of referring to the references as 'Refereene [11], state the name of the authors of the research) Although the results in [11] have not satisfied our expectation yet, those results show affirmative potential of the AIS adaptation for the image processing and pattern recognition.

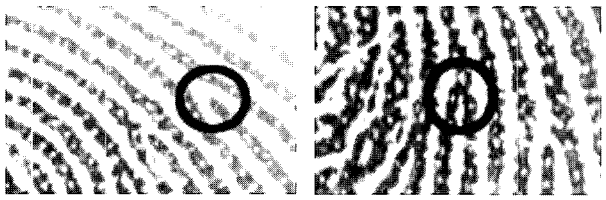
2.2 MHC Recognition Part for Self-Recognition

A function of BIS is accomplished by the operation of B-cell and T-cell. The B-cell is generated in the bone marrow to creates antibodies to eliminate antigens. The T-cell is generated in the thymus and is classified into three categories[13]: helper T-cell, cytotoxic T-cell, and suppressor T-cell. The Helper T-cell activates B-cell to accelerate the secretion of antibodies. Cytotoxic T-cell recognizes infected cells by antigens and kills infected cells. Also Suppressor T-cell suppresses the activity of the immune system after the immune system is activated by antibodies. Cytotoxic T-cell has two recognition parts to tell whether a cell is a self cell or not and to examine whether an antigen exists in the self or not. 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.

3. 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 categories: ridge ending, ridge bifurcation, crossover, and undetermined [14]. Fig. 1 shows the examples of the ridge ending and ridge bifurcation.

Among them, the ridge ending and ridge bifurcation are mainly used to match and identify the fingerprints [14]. There are two kinds of the minutiae extraction methods that can be used from for the fingerprint image: binarization-based method and direct gray-scale extraction method [2]. The ridge ending and ridge bifurcation extracted by the binarization-based method was used. This method binarized the image and then skeletonized the image for the extraction of the minutiae for the fingerprint identification.



(a) Ridge ending (b) Ridge bifurcation

Fig. 1. Ridge ending and ridge bifurcation

4. Fingerprint Matching Algorithm using the String-based MHC Detector Set

Fingerprint matching process compares an input fingerprint image to each template fingerprint image and confirms its authenticity. Thefore, the fingerprint matching process is the most important process in the fingerprint identification system. In order to achieve a more efficient fingerprint matching procedure, a fast and robust fingerprint matching algorithm based on the self-recognition model of the artificial immune system was proposed. 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, the 1st matching stage of the proposed matching algorithm used 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 reduced 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, the 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. The first and second matching stages can reduce the number of the template images and the minutiae to reduce 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. This process is repeated to all the 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.

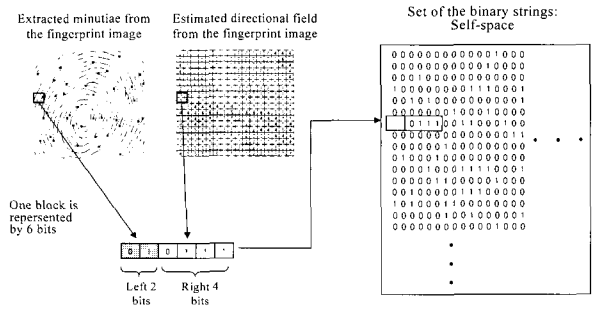


Fig. 2. Construction of the self-space from the fingerprint image

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 exist in the block or not. The four bits on the right represent the values of the directional field in the block.

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

From the strings that form the 'self-space', l 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 that are l bits long. Fig. 3 shows the generation of the MHC detector set.

MHC detector set 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. 4. Then the algorithm finds the position of the best matching score. Also, the scores of each detector about of one of the template images are added up, and those total scores are compared to find the template images with relatively high matching score. The template images that have high matching scores in the 1st matching stage are selected to undergo 2nd matching stage.

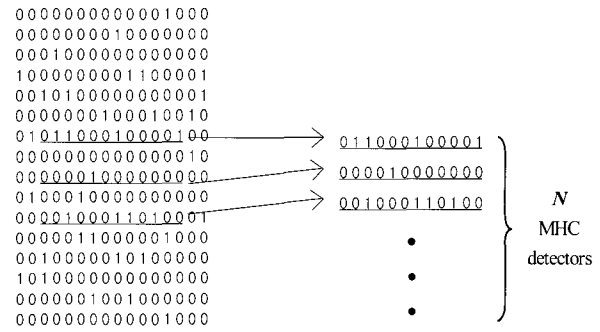


Fig. 3. Generation of the MHC detector set from the self space

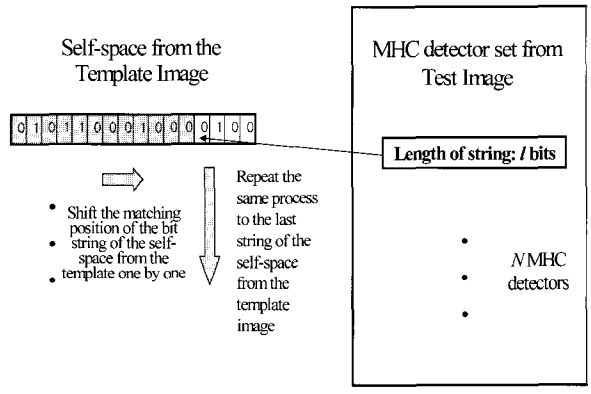


Fig. 4. MHC detector set from the input fingerprint image is matched to the self-space of the template

4.1. Detector testing algorithm

However, the bit-pattern matching and the matching process in Fig. 4 poses a problem because there is a 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. Therefore, the additional process is applied to correct this problem.

[Step 1] When the process in Fig. 4 is completed, calculate the PD(i) for each MHC detector by (1). PD(i) represents that the difference of the best-scored matching position between the self-space and MHC detector.

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

$i(j = 0,1,\cdots,N-1)$ 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 eq. (2).

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

[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.

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

If $|diff(i)| > B$ (B is the boundary value determined by empirical results), the matching score of that MHC detector is set to zero and that detector is excluded from the matching process. Otherwise, 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 is used on 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 proceeds to the 2nd stage matching toward the constructed local structures [15], [16].

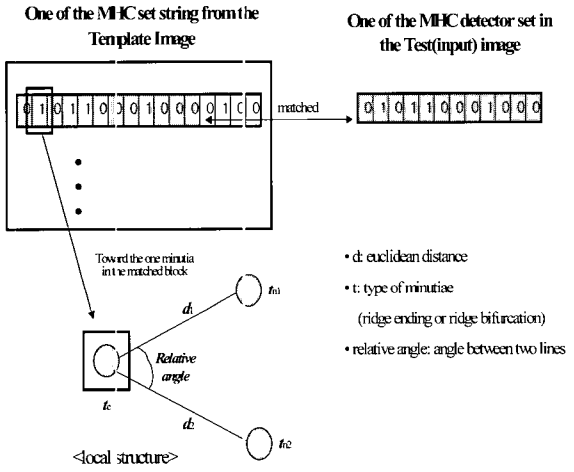


Fig. 5. The 2nd matching stage that is based on the local structure of the two neighborhood points and the parameters of the local structure.

Fig. 5 shows the process of the 2nd matching stage based on the local structure and the form of the local structure that has two neighborhood points. The parameters of the local structure in the 2nd stage are invariant against rotation and translation. Therefore, 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 has the 2nd best matching score, and the algorithm regards that as the authenticated fingerprint image.

5. Experiment Results

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

The local structures of the minutiae were used in the 2nd matching stage. Each local structure was constructed by the center minutia that existed in the matched position and two neighborhood minutiae that were closer to the center minutia than others. The parameters of the local structure is shown in Table. 2[15].

Table 2. 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	$\sqrt{dx^2 + dy^2}$ $dx = y_n - y_c$ $dy = y_n - y_c$
	relative angle	$\theta = \tan^{-1}\frac{dy}{dx} - \theta_c$ θ_c is the angle of the center minutia

Total of 1000 fingerprint images were used in the experiments. μ is a number of selected template images that had high matching

scores in the 1st matching stage. Experimental results are shown in table 3.

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

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

5. Conclusion

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 was suggested. The 1st stage matching was obtained by the use of the 'self-space' of the template and the MHC detector set of the input fingerprint image. Also this process reduced the candidate set of the minutiae and the template images that were used to the 2nd matching stage for the fast matching. In the 2nd matching stage, MHC detector string that was matched to the binary string of the 'self-space' of the template was used to construct the local structure which regarded the minutia in the matched MHC detector as the center minutia. The parameters of the constructed local structure were invariant against rotation and translation of the fingerprint image, and these parameters of the local structure was used for the 2nd stage matching to improve the reliability in the matching process.

The increase in the identification rate, and the comparison of our algorithm with the other algorithm for a more fast and reliable fingerprint identification system will be studied in the future.

References

[1] M. K. Jain, H. Lin, "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, 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 System 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 ICCAS 2002*, pp. 110-114, 2002.

[10] Guiliang Yin, Q. M. J. Wu, "The multi-sensor fusion: image registration using artificial immune algorithm," *IEEE intl. workshop on SCIMA 2003*, pp. 32-36, 2003.

[11] S. Sathyanath, F. Sahin, "An AIS approach to a color image classification problem in a real time industrial application," *Proc. of the IEEE Conf. on Systems, Man, and Cybernetics*, vol. 4, pp. 2285-2290, 2001.

[12] David F. McCoy, "Artificial immune systems and aerial image segmentation," *Proc. of the IEEE Conf. on Computational Cybernetics and Simulation*, vol. 1, pp. 867-872, 1997.

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

[14] 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.

[15] 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.

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

Kwang-Eun Ko

He received his B.S degree in the Department of Electrical and Electronics Engineering from Chung-Ang University, Seoul, Korea, in 2007. He is currently Master course in the School of Electrical and Electronics Engineering from Chung-Ang University. His research interests include machine learning, multi agent robotic system, intelligent home and home networking, etc.

Young-Im Cho

She received her B.S, M.Sc. and Ph.D degree in the dept. of computer Science from Korea University, KOREA, in 1988, 1990 and 1994 respectively. She worked at Samsung electronics as a senior researcher from 1995 to 1996. She visited the University of Massachusetts as a post-doc from 1999 to 2000. She was a professor at the dept of computer science at Pyeongtaek University in Korea from 1996 to 2005. Now, she is a professor in the dept of computer science at University of Suwon in Korea. Her research interests include privacy information agents, neuro-fuzzy system, and artificial life, etc. She is a director Korea Fuzzy and Intelligent Systems Society and ICASE.

Kwee-Bo Sim

He received his B.S. and M.S. degrees in the Department of Electronic Engineering from Chung-Ang University, Korea, in 1984 and 1986 respectively, and Ph.D. degree in the Department of Electrical Engineering from The University of Tokyo, Japan, in 1990. Since 1991, he has been a faculty member of the School of Electrical and Electronics Engineering at Chung-Ang University, where he is currently a Professor. His research interests are in artificial life, emotion recognition, ubiquitous intelligent robot, intelligent System, computational intelligence, intelligent home and home network, ubiquitous computing and Sense Network, adaptation and machine learning algorithms, neural network, fuzzy system, evolutionary computation, multi-agent and distributed autonomous robotic system, artificial immune system, evolvable hardware and embedded system etc. He is a member of IEEE, SICE, RSJ, KITE, KIEE, KFIS, and ICASE Fellow. He is currently President of the KFIS.

Phone : +82-2-820-5319
Fax : +82-2-817-0553
E-mail : kbsim@cau.ac.kr