

Fusion Recognition

Fingerprints and Handwritten Signature Recognition Fusion Based on the Bayesian Algorithm

Xiaojie Yang, Yunyun Zhou, Mandan Liu

School of Information Science and Engineer
East China University of Science and Technology
Shanghai, China

xiaojieyang1989@gmail.com, yunyun.Zhou@Honeywell.com, liumandan@ecust.edu.cn

Abstract—This paper puts forward the fusion recognition using fingerprints and handwritten signature method, using Bayesian decision theory establishment decision-making optimization mathematical model to calculate the decision-making level fusion.

Keywords—component; Bayesian, Fingerprints recognition, Signature recognition

I. INTRODUCTION

Biometric technology has an excellent performance in accuracy, reliability and safety^[1]. A single kind of biometric not only has problem in overcoming its own shortcoming, but also has a limit of its range of applications, that's why people use multiple biometrics to improve the performance of recognition. This article uses the fusion recognition between fingerprint recognition and handwritten signature. Fingerprint and signature each with pros and cons, up to now, the fingerprint recognition is more skillful, and its recognition rate is higher also. Fusion fingerprint with signature can improve the accuracy of identification, and reduce the FAR (False Acceptance Rate) and FRR (False Rejection Rate) at the same time.

II. PRINCIPLE AND IMPLEMENTATION OF THE DECISION-MAKING ALGORITHM

The technology of multi-biometric fusion and identification is about dealing the data from multiple sensors whit multi-faceted, multi-level processing and multi-level, to get more complete information. This paper using the decision-making level fusion method, the features from fingerprint and signature will be extracted separately, and fusion will happen in decision-making level.

A. Fingerprint recognition based on the Gabor filter

The Gabor filter-based fingerprint recognition algorithm in this paper is based on the feature extraction method for fingerprint identification which is based on the structure. In 1998, Anil Jain, et al were created a fingerprint recognition algorithm based on the method of fingerprint codes^[2]. This article will use the Gabor filter for fingerprint image in eight different directions in order to achieve the global and local features extracted.

B. Gabor filter

The Gabor filter is a band-pass filter having directional selectivity and frequency selectivity. It can remove the noise, and retain the fingerprint ridge line and the valley line of information^[3]. The Gabor filter is defined as follow^[3]:

$$G_w(x, y) = \frac{k^2}{\delta^2} \exp\left[-\frac{k^2(x^2 + y^2)}{2\delta^2}\right] \exp[ik(x, y) \exp(-\frac{\delta^2}{2})] \quad (1)$$

The real part and the imaginary part of the Gabor function can be respectively expressed as dual Gabor function and odd Gabor function^[4]. In order to enhance the fingerprint ridge, in this paper, only the dual Gabor function will be used.

$$G(x, y, f, \theta) = \exp\left\{-12\left[\frac{x'^2}{\delta_{x'}^2} + \frac{y'^2}{\delta_{y'}^2}\right]\right\} \cos(2\pi f x') \quad (2)$$

$$\begin{cases} x' = x \sin \theta + y \cos \theta \\ y' = x \cos \theta - y \sin \theta \end{cases} \quad (3)$$

Where f represents the frequency parameter of fingerprint ridge on the angle θ , which is defined as the reciprocal of the averages width of the ridge line λ (that is $1/\lambda$). θ is the direction of the filter factor; $\delta_{x'}$ and $\delta_{y'}$ respectively denotes the standard deviation in x' axis and y' axis in Gaussian function.

C. Fingerprint feature extraction

The Gabor filter in 4 directions $\{0^\circ, 45^\circ, 90^\circ, 135^\circ\}$, is already to extract the global features of fingerprint^[5]; the Gabor filter in 8 directions can also extract the characteristics from local ridge line of the fingerprint.

If the gray value of the pixels located within the sector S_i is represented by $F_{i\theta}(x, y)$, where $\theta \in \{0^\circ, 22.5^\circ, 45^\circ, 67.5^\circ, 90^\circ, 112.5^\circ, 135^\circ, 157.5^\circ\}$, $i \in \{0, 1, \dots, 79\}$. Thus, the characterized in the circle region $V_{i\theta}$ as shown in Formula 4:

$$V_{i\theta} = \frac{1}{ni} \left(\sum_{ni} \|F_{i\theta}(x, y) - M_{i\theta}\| \right) \quad (4)$$

Wherein, $M_{i\theta}$ represents the mean value of the pixel gray values within the region S_i ; n_i indicates the number of pixels within the annular area S_i . AAD (Average Absolute Deviation), is the characterized $V_{i\theta}$ after calculation. After using the Gabor filter in one direction of a fingerprint image,

there are 32 features can be extracted from the filtered image.

D. Determine fingerprint threshold and the characterized matching

32*k eigenvalues can be extracted after filtering the original fingerprint image by 8-direction Gabor filter. Using distance method which is based on the Euclidean geometry, to calculate the maximum and minimum vector to get the Euclidean distance value of those largest eigenvectors and minimum eigenvectors, which are the fingerprint feature recognition thresholds.

During the collection the fingerprint, the image may be deflected. So, this paper extracting two sets of characteristics for each fingerprint image, and save it in the database. Finger Code1 extracted from the fingerprint of the original image obtained, Finger Code2 be obtained by extraction after the original image counterclockwise rotation θ . Then rotate both FingerCode1 and FingerCode2 in $R \cdot \theta/2$ ($R=0, 1, \dots, 2k-1$). Comparing the rotation characteristics with the unverified fingerprint features, then take one group which is closest to the fingerprint template as fingerprint identity to be verified. FingerCode can be represented by following formula:

$$V_{i\theta}^R = V_{i'\theta'} \quad (5)$$

$$i' = (i + k + R) \bmod k + (i \div k) \times k \quad (6)$$

$$\theta' = (\theta + 180^\circ + (\frac{2\pi}{k}) \times R) \bmod 180^\circ \quad (7)$$

$$i \in \{0, 1, 2, \dots, 31\}, \theta \in \{0^\circ, \theta, 2\theta, \dots, \pi - \theta\}.$$

E. Handwritten signature recognition base on the dynamic time warping

The dynamic features and structural features of handwritten signature^[6] usually be applied in the recognition of handwritten signature. In the local matching strategy of handwritten signature, in this article uses the DTW algorithm (Dynamic Time Warping algorithm).

F. Signature feature extraction

The handwritten signature parameter features used in this paper are as follow^[7]:

The standard deviation in the X-direction, the standard deviation in the Y-direction, the average velocity in X-direction, the average velocity in Y-direction, the total time for sampling, high-width ratio, the standard deviation of the pressure, the standard deviation of the rotation angle, the standard deviation of the inclination angle, the average pressure, the average front bevel, the average rotation angle, the wavelet pressure energy, the energy of the wavelet rotation angle and the energy of the wavelet inclination angle. This paper using the decision-level fusion, the extraction and the per-processing stage of the signature features and the fingerprint is separately, there is no effect between two sets of data.

After calculate those features are needed, the function of features sequence is:

$$S(t) = [x(t), y(t), p(t), az(t), al(t), btn(t)]^T, t = 1, 2, \dots, N \quad (10)$$

G. Signature features matching base on the DTW algorithm

Dynamic Programming^[8] is a mathematical algorithms usually used to solve the multi-stage decision-making process optimization. The main idea is that to link every best sub-path together, to constitute an optimal path and get the results of recognition eventually.

There are two signal sequence $R = \{r(i) \mid 1 \leq i \leq I\}$ and $T = \{t(j) \mid 1 \leq j \leq J\}$. Wherein, I and J is respectively represents the length of the handwritten signature features of the template sequence and the length of the handwritten signature features waiting to be recognized. i is the timing reference numeral of the handwritten signature template sequence; r is the unrecognized handwritten sequence numeral; R is the features signal sequence of the template of the handwritten signature.

And, the relationship between the T and R with the time change can be represented by time regularization function (i.e. $F = \{f(k) \mid 1 \leq k \leq k+f\}$), where, $f(k) = (i(k), j(k))$. Time warping function represents the comparison between the $j(k)$ frame in r and $f(k)$ frame in R . $f(k)$ can be regarded as a point in the plane which forming a curved path with the parameter k . As shown in figure 1.

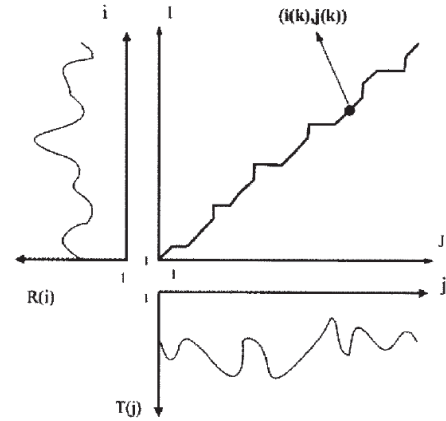


Figure 1. Dynamic time warping algorithm schematic diagram

In the process of calculating the $D(R, T)$, the local matching distance between the f -th frame in the template and the j -th frame in the recognition sequence is set to $d(i(k), j(k))$ (i.e. $d(f(k))$). When the relatively instantaneous time between the two features sequence change, in order to maximize admit this volatility, the idealized results of the dynamic time warping should be able to find a way to meet the overall average of the two features sequence matching.

Treat the matching path of the $D(R, T)$ as the matching path P between the template signal sequence R and the signal sequence T to recognition. At the same time the matching distance is used as the matching distance of the sequence of the test signal T and the template sequence R .

$$D(R, T) = \min \frac{\sum_{k=1}^k d(f(k))u(k)}{\sum_{k=1}^k u(k)} \quad (9)$$

Here, $u(k)$ is the weighting coefficients of the matching distance of matching point $f(k)$.

H. Bayesian Decision Fusion

There is a sample space S , and D_1, D_2, \dots, D_n is a partition of the sample space. The $p(D_i)$ ($p(D_i) > 0$, ($i=1, 2, \dots, n$)) indicates the probability of occurrence of event D_i . For any single event X , there is $p(x) > 0$:

$$P(D_j|x) = \frac{p(x|D_j)P(D_j)}{\sum_{i=1}^n p(x|D_i)P(D_i)} \quad (10)$$

If the identification of individual state is denoted by H , and illegal individuals to be identified as H_0 , be identified legitimate individual H_1 ; two kinds of decision in decision-making space on the biometric decision-making is:

The individual is recognized as legitimate instance (represented by $d=1$), the individual is identified as an illegal individual (represented by $d=0$). The decision-making system can be divided into four situations: the legitimate individual to be identified is considered lawful $P(d=1/H_1)$; illegally individual to be identified is considered as illegal individual $P(d=0/H_0)$; illegal individual to be identified is considered legitimate $P(d=1/H_0)$; legitimate individual to be identified the illegal $P(d=0/H_1)$.

The False Acceptance Rate is FAR, the False Rejection Rate is FRR. W_{FRR} is the loss of FRR, W_{FAR} is the loss of FAR, and the Bayesian expected risk R can be represented by the following equation:

$$R = 0 * P(d=0/H_0) + W_{FAR} * P(d=1/H_0) + W_{FRR} * P(d=0/H_1) + 0 * P(d=1/H_1) \quad (11)$$

In this paper, $W_{FAR} = W_{FRR} = 1$, so, formula (11) can change into:

$$R = FAR_{fus} + FRR_{fus} \quad (12)$$

The decision of the fingerprint recognition and the decision of the handwritten recognition can be represented by d_1 and d_2 , respectively. Using the Bayesian rules, the result of the integration of decision-making fusion of fingerprint recognition and handwritten signature recognition can be calculated by the following formula:

$$\sum_{i=1}^N [d_i \times \log(\frac{1-FRR_i}{FAR_i}) + (1-d_i) \log(\frac{FRR_i}{1-FAR_i})] > \log(\frac{W_{FRR}}{2-W_{FAR}}) \quad (13)$$

If Eq.13 is true, then $d_{fus}=1$; else $d_{fus}=0$.

III. EXPERIMENTAL RESULTS AND ANALYSIS

A. Database Introduction

In this experiment, all the fingerprint data is come from the fingerprint images in the FVC2004 (Fingerprint Verification Competition 2004) fingerprint database, the

Handwritten signature data obtain from SVC2004 (Signature Verification Competition 2004) handwritten signature database directly. The sequence length of each signature is stored in the first line in the TXT files. They are, in the order, X-coordinate, Y coordinates, and time stamp, the status flag of the signature, the inclination angle of the stylus, the rotation angle, and stylus pressure information.

B. Fingerprint Recognition

Take 10 random samples of fingerprint data from the FVC2004 database. There are total of $10 * (8+8) = 160$ fingerprint images. In this database, the size of each image are $256 * 256$ pixels, the resolution of the fingerprint image is 500dpi.

Depends on the experience, during the conduction of fingerprint image, each concentric ring is divided into 8 sectors in this paper. In the image preprocess, those values of parameter in accordance with the resolution and experience, which are shown in Table 1.

Pick 5 random images from 8 known true ones, extracting and synthesizing into a set of feature, as a template to match. And at the same time, sequentially 16 fingerprint feature extraction, and matching with the template.

TABLE I. TABLE TYPE STYLES THE SELECTION OF PRE-PROCESS PARAMETERS

parameter	Parameter value (pixel)
The number of concentric rings (B)	4
The width of concentric ring (b)	20
Normalized variance (V0)	100
Mean normalized (M0)	100
Filter frequency (f)	1/10
The size of the filter template	33×33
Standard deviation of Gaussian function ($\delta x'$ and $\delta y'$)	4.0

Using the Gabor filter to filter the fingerprint image feature extraction area in 8 directions (i.e. $\{0^\circ, 22.5^\circ, 45^\circ, 67.5^\circ, 90^\circ, 112.5^\circ, 135^\circ, 157.5^\circ\}$), those fingerprint features from 8 directions are the characteristics of the fingerprint image.

One direction Gabor filter can extract 32 features from an image. After finish the filtering in 8 directions about one fingerprint image, there will be $8 * 32 = 256$ AAD features.

In order to ensure the rotation invariance of the fingerprint image, should counterclockwise rotation of 11.25° for each user's 5 fingerprint images, then to extract for fingerprint image again. FingerCode1 extract from the image of the original fingerprint image, and FingerCode2 extract from the images after rotation.

First, obtain the threshold value of the original fingerprint image d_1 . Then extract the maximum eigenvalue of each column to compose the maximum feature vector, extract the minimum eigenvalue of each column to compose the minimum feature vector, these are the threshold value of the fingerprint matching d_2 . Rotate respectively the original

sample template feature and the sample template feature after rotation for $R \times 22.5^\circ$ (wherein, $R=0,1,2,3,\dots,15$). Then to matching the fingerprint feature waiting for identify for $16 \times 2 = 32$ times, and match the results with threshold d1 and d2. That's the way to judge the fingerprint authenticity. The result of matching are shown in Table 2

TABLE II. RESULT OF FINGERPRINT RECOGNITION

team	FAR (%)	FRR (%)	Fingerprint recognition rate (%)
U1	12.5	0	87.5
U2	12.5	0	87.5
U3	6.25	0	93.75
U4	0	0	100
U5	6.25	0	93.75
U6	6.25	6.25	87.5
U7	6.25	0	93.75
U8	6.25	0	93.75
U9	12.5	0	87.5
U10	0	12.5	87.5

The experimental results show that the average recognition rate of the FVC2004 fingerprint database under this recognition algorithm was 91.25%. The highest recognition rate was 100%, the lowest identification rate was 87.5%, the average false acceptance rate of 6.875%, the average false rejection rate of 1.875%.

C. Handwritten signature recognition

Taking 10 random sample of handwritten signature data from SVC2004 database, 5 of them are chose from the true samples. Then through the interpolation and wavelet functions to extract energy strategy, there are 36 eigenvalues vector can be extracted, which will compose the feature vector.

Every user has 5×36 feature vectors, because of the same feature is in the same column, in this paper, through compare the absolute value of minus for one to another, can find the smallest feature in the handwritten signature from 5 signature to compose a new feature vector. And that feature vector will be used as the eigenvector sample template in the extraction handwritten signature matching. The 8 real handwritten signatures and 8 forged handwriting signature as handwritten signature test set.

TABLE III. HANDWRITTEN SIGNATURE RECOGNITION RESULTS

Team	FAR (%)	FRR (%)	Handwritten signature recognition rate (%)
U1	6.25	0	93.75
U2	0	6.25	93.75
U3	6.25	6.25	87.5
U4	12.5	6.25	81.25
U5	0	6.25	93.75
U6	6.25	6.25	87.5
U7	0	12.5	87.5
U8	6.25	6.25	87.5
U9	0	18.75	81.25
U10	12.5	6.25	81.25

The experimental results are shown in Table 3. The average recognition rate of the SVC2004 fingerprint database under this recognition algorithm was 87.5%. The highest recognition rate was 93.75%; lowest recognition rate

of 81.25%; false acceptance rate of 5% on average; false rejection rate of 7.5%.

D. Result of Bayesian Fusion

TABLE IV. THE RESULTS OF BAYESIAN DECISION-MAKING LEVEL FUSION

team	FRR (%)	FAR (%)	Recognition rate (%)
U1	0	0	100
U2	0	0	100
U3	6.25	0	93.75
U4	0	0	100
U5	6.25	6.25	87.5
U6	6.25	6.25	87.5
U7	6.25	12.5	81.25
U8	6.25	0	93.75
U9	12.5	0	87.5
U10	0	12.5	87.5

Bayesian decision fusion results: average recognition rate of 91.875%; highest recognition rate of 100%; lowest recognition rate of 81.25%; false acceptance rate of 3.75% on average; average false rejection rate of 4.375%.

E. Analysis of experimental results

Compare the experimental results of fingerprint recognition, handwritten recognition and Bayesian decision-making fusion recognition, the average recognition rate of the fusion recognition is higher than other two. Bayesian decision algorithm can converge a high recognition rate, the false rejection rate is relatively decreased.

IV. CONCLUSION

Biometric with a high security and reliability, which it is currently a research focus. In this paper, using Bayesian decision theory to establish minimum risk Bayesian optimization function model, in order to minimum the fingerprint and handwriting signature false acceptance rate and false rejection rate, so that the efficiency of the fingerprint and handwritten signature fusion recognition can be improved. The combination of fingerprint, signature recognition technology and other biometric technology is also a currently hot research field of biometrics.

But using the fusion method in this paper, which is belonging to the decision level fusion, just simply make the second judgment base on the result of two recognitions, without using the information in features. To some extent, this may cause a certain amount of information loss, and over-reliance on the results of the separately identifiable. If the fingerprint recognition or handwritten signature recognition error in the identification process, and may result in the secondary judge's mistakes.

REFERENCES

- [1] Z. Wu, J. ZENG, J. ZOU, X. YANG, Y. ZHANG. Biometric Identification Technology Based on Body Biology Character. In: Modern electronic technology (2007), vol. 14(253). pp: 121-124.

- [2] L. Hong, Y. Wan, .I Jain. Fingerprint Image Enhancement: Algorithm and Performance Evaluation. Transactions on pattern analysis and machine intelligence (1998), vol. 20(8). pp: 777-789.
- [3] J. Zhang. Automated fingerprint identification algorithm and system design. In: the master degree thesis from Southwest Jiaotong University. (2007).
- [4] F. Luo, K. Li, S. Ma, L. Lin. On-line Handwritten Signature Verification System Based on DTW. In: journal of Chinese Computer Systems (2009), vol. 30(9).
- [5] W. WANG, J. LI, F. HUANG, H. FENG. Fingerprint Image Enhancement by Log-Gabor filtering. In: Computer Science (2007), vol. 34(7).
- [6] A. Moenssens. Fingerprint techniques. London: Chilton Book Company (1971). pp: 130-149.
- [7] C. Lee, H. Wang. Fingerprint feature extraction using Gabor filters. in: ELECTRONICS LETTERS(1999), vol. 35(24) .
- [8] K. I. Chang, K. W. Bowyer, P. J. Flynn. Face recognition using 2D and 3Dfacial data. Santa Barbara, In: Workshop in Multimodal User Authentication, California, 2003. pp: 25—32.
- [9] H. Ma, M. Liu, C. Zhang. A Method of On line Handwritten Signature Verification Based on Wavelet Packet Analysis and SVM. in: Journal of East China University of Science and Technology (2007), Vol.33(4).
- [10] Y. Zhou. Identification technology based on the fusion of fingerprint and handwriting signature. The master degree thesis from East China University of Science and Technology(2010).
- [11] Z. Hong. Algebraic feature extraction of image for recognition .Pattern Recognition, 1991,24(3) pp:211-219.