Role of Assembling Invariant Moments and SVM in Fingerprint Recognition

[1] Supriya Wable, [2] Chaitali Laulkar

[1, 2] Department of Computer Engineering, University of Pune
Sinhgad College of Engineering, Pune-411 041, India

Abstract

Fingerprint identification is one of the most well-known exposed biometrics, because of their uniqueness, distinctiveness and consistency over time. It is the method of identifying an individual and it can be used in various commercial, government and forensic application, such as, medical records, criminal investigation, cloud computing communication etc. In cloud computing communications, information security involves the protection of information elements, only authorized users are allowed to access the available contents. However, traditional fingerprint recognition approaches have some demerits of easy losing rich information and poor performances due to the complex inputs, such as image rotation, incomplete input image, poor quality image enrollment, and so on. In order to overcome these shortcomings, a new fingerprint recognition scheme based on a set of assembled invariant moments i.e., Geometric moment and Zernike moment. These moment features are used to ensure the secure communications. This scheme is also based on an effective preprocessing, the extraction of local and global features and a powerful classification tool i.e. SVM (Support vector machine), thus it is able to handle the various input conditions encountered in the cloud computing communication. A SVM is used for matching the identification of test fingerprint inputs feature vectors with of the database images.

Keywords: *Assembling, Fingerprint recognition, Invariant moments, SVM..*

1. Introduction

Biometrics is described as the science of recognizing an individual based on his or her physical or behavioral attributes. Biometric system broadly provides the three functionalities such as, verification, identification and screening. Biometrics can be used in the face recognition, fingerprint recognition, hand geometry, iris recognition, signature etc. The complexity of designing a biometric system based on three main factors viz., accuracy, scale or size of the database, and usability.

Among all the biometric indicators, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations. Fingerprint recognition is one of the popular and effective approaches for priori authorizing the users and protecting the information elements during the communications. The performance of fingerprint recognition may be greatly affected by the complex input conditions such as image rotation, incomplete input image, poor quality image enrollment, and so on. Both the geometric moments and Zernike moments are invariant to scale, position, and rotation, so they are able to handle the various input conditions.

Remaining part of the paper is organized as follows. In Section 2, geometric and zernike moment analysis is discussed. Section 3 describes overview of system and conclusion is shown in Section 4.

2. Invariant Moments

Geometric moments and Zernike moments are invariant moments which are used in this fingerprint recognition scheme.

2.1 Geometric Moment Analysis

Geometric moments [4] can provide the properties of invariance to scale, position, and rotation. Geometric moment analysis is used to extract invariant features from fingerprint image. This section gives brief description of the moment analysis.

For a 2-D continuous function $f(x, y)$, the moment of order $(p+q)$ is defined as,

$$m_{pq} = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} x^p y^q f(x,y)\, dx dy \quad \text{for } p, q = 0,1,2, \ldots. \tag{1}$$

A uniqueness theorem states that if $f(x, y)$ is piecewise continuous and has nonzero values only in a finite part of the xy-plane, moments of all orders exist, and the moment sequence (m_{pq}) is uniquely determined by $f(x,y)$. Conversely, (m_{pq}) is uniquely determined by $f(x, y)$. The central moments are defined as,

$$\mu_{pq} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}(x - x')^p(y - y')^q f(x,y)dxdy \tag{2}$$

where $x' = m_{10}/m_{00}$ and $y' = m_{01}/m_{00}$.
If $f(x, y)$ is a digital image, then (2) becomes,

$$\mu_{pq} = \sum_x \sum_y (x - x')^p (y - y')^q f(x,y) \tag{3}$$

and the normalized central moments, denoted by η_{pq} are defined as follows:

$\eta_{pq} = \mu_{pq}/\mu_{00}^{\gamma}$, where $\gamma = (p+q)/2+1$ for $p+q = 2,3....$ (4)

A set of seven invariant moments can be derived from the second and third moments. The set consist of groups of nonlinear centralized moment expression and it is a set of absolute orthogonal moment invariants that can be used for a pattern identification invariant to scale, position, and rotation as follows:

$\phi_1 = \eta_{20} + \eta_{02}$
$\phi_2 = (\eta_{20} - \eta_{02})^2 + 4\eta^2_{11}$
$\phi_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - 3\eta_{03})^2$
$\phi_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2$
$\phi_5 = (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2]$
$+ (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2]$
$\phi_6 = (\eta_{20} + \eta_{02})[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2]$
$+ 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03})$
$\phi_7 = (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2]$
$+ (3\eta_{12} - \eta_{30})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2]$ (5)

2.1 Zernike Moment Analysis

Zernike moment [4] can also provide the properties of invariance to scale, position, and rotation. Zernike moment analysis is used to extract invariant features from fingerprint image. This section gives brief description of the Zernike moment analysis.

The magnitudes of Zernike moments have been treated as rotation-invariant features. It has also been shown that Zernike moments can have translation and scale invariant properties by their simple geometric transformations.

The Zernike radial polynomials of order n with repetition m, $V_{nm}(x,y)$, are given by,

$$V_{nm}(x,y) = R_{nm}(x,y)e^{jm\theta} \tag{6}$$

where

$$j = \sqrt{-1},\ \theta = \tan^{-1} y/x \tag{7}$$

and

$$R_{nm}(x,y) = \sum_{s=0}^{(n-|m|)/2} \times \frac{(-1)^s(x^2+y^2)^{(n-2s)/2}(n-s)!}{s!(n+|m|-2s)/2)!(n-|m|-2s)/2)!} \tag{8}$$

where $s = 0,1,...,(n-|m|)/2$, $n \geq 0$, $|m| < n$, and $n - |m|$ is even.

The angle θ is between 0 and 2π and is measured with respect to the x-axis in counterclockwise direction. The origin of the coordinate scheme is at the center of an image.

For a digital image, the Zernike moments of order n and repetition m are given by,

$$A_{nm} = \frac{n+1}{\pi}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)V^*_{nm}(x,y) \tag{9}$$

where $V^*_{nm}(x,y)$ is the complex conjugate of $V_{nm}(x,y)$.

One of the major properties of Zernike moments is that the image can be reconstructed by using the inverse transformation.

$$f^{\wedge}(x,y) = \sum_{n=0}^{n_{max}}\sum_{m=-n}^{n} A_{nm}V_{nm}(x,y) \tag{10}$$

where n_{max} is the maximum order of the Zernike moments considered for a particular application.

The magnitudes of the Zernike moments $|A_{nm}|$ are rotation invariant. They also can be invariant to translation and scale.
The Zernike moment $|A_{nm}|$ is order n with repetition m, where n is a nonnegative integer, m is an integer and subject to the constraint $n-|m|$ = even, $m| \leq n$. It has been found that low-order Zernike moments are stable under linear transformations while the high-order moments have large variations, therefore choose the order n which is less than 5, and the first ten Zernike moments ($n \leq 5$) can be defined as $A_{0,0}$, $A_{1,1}$, $A_{2,0}$, $A_{2,2}$, $A_{3,1}$, $A_{3,3}$, $A_{4,0}$, $A_{4,2}$, $A_{4,4}$, and $A_{5,1}$.

3. Overview of System

Figure 1. shows an overview [7] of the proposed fingerprint recognition system. Fingerprint image is input to the system. Extract the features of input image and check those extracted features with already stored features of fingerprint images in the database.

Following figure contains two stages, offline processing and online processing. In the offline stage, fingerprint images of the different individuals are first processed by

the feature extraction module and then their extracted features are stored as templates in the database for later using. In the on-line stage, a fingerprint image of an individual is first processed by the feature extraction module, its extracted features are then fed to the matching module with one's identity ID, which matches them against one's own templates in the database.

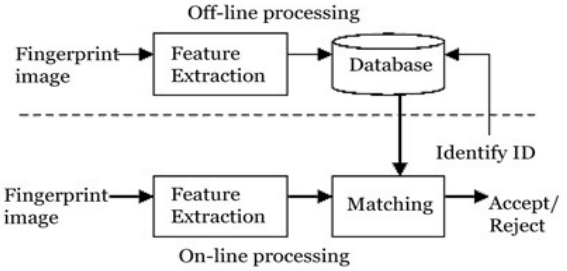

Fig. 1 Overview of the fingerprint recognition system

Both online and offline process contains feature extraction module, which consists of four stages as shown in Figure 2. viz., image enhancement, determination of reference point, assembling of invariant moment analysis, and PCA (Principal component analysis).

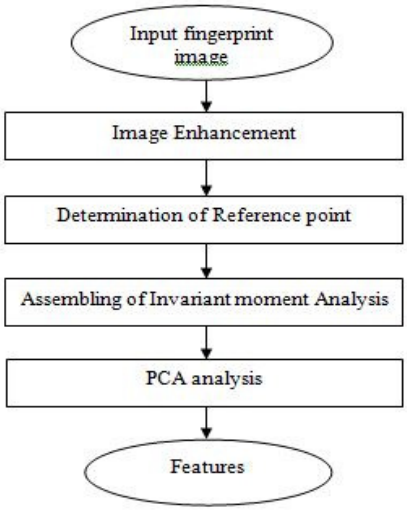

Fig. 2 Flowchart of the feature extraction module

3.1 Image Enhancement

This algorithm consists of two stages, STFT (short time Fourier transform) analysis and Enhancement. The performance of a fingerprint recognition system depends on the quality of the input images and it roughly corresponds to the clarity of the ridge structure in the fingerprint image, hence it is necessary to enhance it in advance. The algorithm simultaneously estimates all the intrinsic properties of the fingerprints such as the foreground region mask, local ridge orientation and local ridge frequency, and used these properties to enhance the fingerprint image. Thus, it can enhance the image completely.

The STFT [2] image enhancement algorithm consists of two stages as summarized in Algorithm I.

Algorithm I: Enhanced the fingerprint image with STFT algorithm

Input: Fingerprint image
Output: Enhanced fingerprint image

Stage 1: STFT analysis
For each overlapping block in an image.

1) Generate and reconstruct a ridge orientation image by computing gradients of pixels in a block, and get a ridge frequency image by applying FFT into the block, then take an energy image by summing the power of FFT value.
2) Smooth the orientation image using average vector and generate a coherence image using smoothed orientation image.
3) Generate a region mask by thresholding the energy image.

Stage 2: Enhancement
For each overlapping block in an image.

1) Generate the angular filter F_a which is centered on the orientation of the smoothed orientation image.
2) Generate the radial filter F_r centered on the frequency image.
3) Apply the filter, $F = F * F_a * F_r$ into the block in the FFT domain.
4) Generate the enhanced block by inverse Fourier transform IFFT(F).
5) Reconstruct the enhanced image by composing enhanced blocks, and get the final enhanced image by applying the region mask.

3.2 Determination of Reference Point

Core and delta are singular points and they are unique landmarks of fingerprints as a global feature. They are commonly used as reference points for fingerprint indexing, classification, and matching. However, some of the partial fingerprint images or plain-arch-type fingerprints may exists without the delta points. It may possible to get two core points from the whorl type fingerprints. This step determines a reference point from the enhanced image instead of from the original image directly.

The orientation field obtained from the enhanced image will increase the reliability and accuracy for detection. The reliable detection of a reference point can be

accomplished by detecting the maximum curvature using complex filtering methods [8] and it is summarized as Algorithm II.

Algorithm II: Reference point determination
Input: Enhanced fingerprint image
Output: Reference point determination in the fingerprint image

1. For each overlapping block in an image.
   1) Generate and reconstruct a ridge orientation image with the same method in enhancement stage.
   2) Apply the corresponding complex filter, $h = (x + ty)^m g(x,y)$, centered at the pixel orientation in the orientation image, where m and $g(x,y) = \exp\{-((x^2 + y^2)/(2\sigma^2))\}$ indicate the order of complex filter and Gaussian window, respectively.
   3) For m=1, obtain filter response of each block by a convolution, $h * O(x,y) = g(y) * ((xg(x))^c * O(x,y)) + tg(x)^c * ((yg(y) * O(x,y)))$, where O(x, y) represents the pixel orientation in the orientation image.

2. Reconstruct the filtered image by composing filtered blocks.
3. The maximum response of complex filter in the filtered image can be considered as the reference point. Since there is only one unique output point is taken as reference point of an image.

3.3 Assembling Invariant Moments analysis

At the third step, apply the geometric moments and Zernike moments analysis introduced in Section II on fingerprint image. Geometric moments provide a set of seven invariant moments and Zernike moments provide ten features.

Let $\phi_{k,l}$ for k = 1, 2, 3, 4and l = 1, 2, 3,...,17, where $\phi_{k,l}$ for l = 1, 2, 3,...,7 consist of geometric moments, and $\phi_{k,l}$ for l = 8, 9, 10,...,17 consist of Zernike moments, *k* is used for index of image.

3.4 PCA Analysis

PCA analysis reduces the dimension of feature vector, which examines feature covariance matrix and then selects the most distinct features. It is one of the oldest and greatest known techniques in multivariate analysis. Let x ϵ R_n be a random vector. where n is dimension of the input space. Covariance matrix of x is defined as, $\Xi = E\{[x - E(x)][x - E(x)]^T\}$. let $u_1, u_2, \ldots, u_n$ and $\lambda 1, \lambda 2, \ldots \lambda n$ be eigenvectors and eigenvalues of Ξ, respectively and $\lambda 1 \geq \lambda 2 \geq \cdots \geq \lambda n$, then PCA factorizes Ξ into $\Xi = U\Lambda U^T$, with $U = [u_1, u_2, \ldots . u_n]$ and $\Lambda = \mathrm{diag}(\lambda 1, \lambda 2, \ldots, \lambda n)$. One important property of PCA is its optimal signal reconstruction in the sense of minimum mean squared error. Then $y = P^T x$ will be an important application of PCA in dimensionality reduction.

3.4 Matching with SVM

Support vector networks or SVM [6] are supervised learning models with associated learning algorithms used in machine learning. It analyzes the data and recognize different patterns. It is used for classification and regression analysis. The basic SVM takes a set of input data and predicts for each given input. SVM is used for classifying data sets. Viewing input data as two sets of vectors in an *n*-dimensional space, then SVM will construct a separating hyperplane in that space, one which maximizes the margin between the two data sets. To calculate the margin, two parallel hyperplanes are constructed, one on each side of the separating hperplane, which are "pushed up against" the two data sets. Instinctively, a good separation is achieved by the hyperplane that has the largest distance to the neighboring data points of both classes, since in general the larger the margin the better the generalization error of the classifier.

Usually, there are four kinds of SVM types: the linear SVM, radial-basis SVM, polynomial SVM, and sigmoid SVM. Most of the time nonlinear types of SVM, such as radial-basis SVM, polynomial, and sigmoid SVM can be used for fingerprint matching to achieve high recognition rate.

For each input fingerprint and its template fingerprint, compute the geometric and zernike moments. Since the output is to judge whether the input fingerprint is match or non-match according to the identity ID, So it consider being as matching process as two-class problem. SVM is used to verify a matching between feature vectors of input fingerprint and of template fingerprint.

There are mainly 2 stages training and testing, In the training stage, training samples are fed to the SVM with indicating their corresponding class. The features are computed from the training data, each contains vector from the training fingerprint. Whereas in the testing stage, test samples are fed to the SVM to produce the

output values. Similarly, the features are computed from the testing data, each contains vector from the test fingerprint with the querying ID. The element of the output values is restricted in the class number. If the output number is equal ID, then it means fingerprints are matched, otherwise they are non-matched.

4. Conclusion

In order to protect the multimedia contents for security, this new fingerprint recognition scheme based on a set of assembled geometric and Zernike moment features in cloud computing communications. This scheme can also used to protect the data or security-focused resources for safety communications. This fingerprint recognition scheme is based on the effective pre-processing, the extraction of local and global invariant moment features and the powerful SVM classification tool, thus it is able to handle the various input conditions. SVM is used to verify matching between fingerprints.

A pre-processing enhancement with the STFT analysis makes the algorithm highly robust to poor-quality fingerprint images and it improves the matching accuracy. Because of the image enhancement, the reference point can be reliably and accurately determined by the complex filtering methods. The features extracted by using assembled invariant moment analysis have covered both local and global properties of fingerprints.

Acknowledgments

I humbly thanks to Prof. C. A. Laulkar (Sinhgad College of Engineering, Pune) for lending her invaluable expertise by refereeing this project. I also thankfull to my institution for providing guidance and opportunities.

References

[1] A. K. Jain, S. Prabhakar, and S. Pankanti, “Filterbank-based fingerprint matching.” IEEE Trans. Image Process., vol. 9, no. 5, May 2000, pp. 846-859.

[2] C. Sharat, N. C. Alexander, and G. Venu, “Fingerprint Enhancement using STFT analysis.” Pattern Recognit., vol. 40. no. 1, 2007, pp. 198-211.

[3] D. Maio, D.Maloni and R. Cappelli, “FVC2002: Second fingerprint verification competition.” In proc. 16th Int. Conf. Pattern Recognit., 2002, vol. 3, pp.811-814.

[4] J. C. Yang and D. S. Park, “Fingerprint verification based on Invariant moment features and nonlinear BPNN.” Int. journal of control automation. Syst. vol. 6, no. 6, 2008, pp. 800-808.

[5] J. C. Yang and D. S. Park, “A fingerprint verification algorithm using tessellated invariant moment features.” NeuroComputing, vol. 71. nos 10-12, 2008, pp. 1939 - 1946.

[6] J. Shawe-Taylor and N. Cristianini, “Support Vector Machines and Other Kernel-Based learning Methods.”Cambridge, U.K: Cambridge Univ. Press, 2000.

[7] Jucheng Yang, Naixue Xiong, “A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications.” Jiangxi University of Finance and Economics, IEEE systems journal, vol. 5, no. 4, December 2011.

[8] N. Kenneth and B. Josef, “Localization of corresponding points in fingerprints by complex filtering.” Pattern Recognit. Lett., vol. 24, no. 13, 2003, pp. 2135-2144.

[9] X. Jang and W. Y. Yau, “ Fingerprint minutiae matching based on the local and global structures.” In proc. Int. Conf. Pattern Recognit., 2000, vol. 2, pp. 1024-1045.

Supriya Wable received B.E. degree in Computer Engineering from Pune University in the year 2011 and currently pusuing for M.E. in Computer Networks from Sinhgad College of Engineering, Pune University. Her current research interests include image processing and fingerprint recognition.

Chaitali Laulkar is currently working as Asst. Professor in Computer Department with the Sinhgad College of Engineering in Pune University and pursuing for Ph.D. degree. She received B.E. degree from Bamu, Aurangabad University in the year 1995 and received M.E. degree from Pune University in 2005.