Network Security: Pattern Recognition Approach
(Biometrics based Person Authentication)

[1]Jayant V. Kulkarni, [2]Raghunath. S. Holambe, [2]Bhushan D. Patil

[1]Instrumentation and Control Engg. Deptt.
Vishwakarma Institute of Technology, Pune
[2]Department of Instrumentation Engg. S. G. G. S Institute of Engg. And Tech. Nanded

Abstract

The provision of security measures in military as well as in civilian applications is an integral part of the system. Network security is one of the important areas. The password hacking could be avoided, by adopting the biometrics based person authentication.

Multiple biometric features are combined to construct a robust identification system. Fingerprint and facial features of a person are combined (fuse) to find a suitable match in. This paper will focus on the various pattern recognition approaches for the person identification using fingerprint as a biometric feature.

Key words: Fingerprint, FAR (False Acceptance Rate), FRR (False Rejection Rate), identification, verification.

1. Introduction

Person authentication became an integral part of the security system. Fingerprints have been used for forensic, criminal investigation and proved its importance.

Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. By using biometrics it is possible to establish an identity based on `who you are', rather than by 'what you possess' (e.g., an ID card) or `what you remember' (e.g., a password). Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermo grams, signature, voiceprint, gait, palmprint, etc. to establish a person's identity [1,2].

The use of biometrics based person identification in the network security could avoid the misuse of the system and can avoid further consequences. The level of security required can decide the type of biometrics feature or combination of more than two biometrics features may be used for identification.

The identification system characteristic parameters (FAR, FRR) will be adjusted based on the applications like for money transactions the FAR should be as minimum as possible i.e. a imposter will not be allowed to interact with the system. An identification system could be designed dedicatedly for identifying and providing access to particular people only, in such cases the FAR has to be 0 percent while the higher value of FRR could be tolerated.

This paper discusses various methods of biometric based person identification using fingerprint as biometric feature. Fingerprints have one of the highest levels of reliability [3] and have been extensively used by forensic experts in criminal investigations [4]. Although not scientically established, fingerprints are believed to be unique across individuals, and across fingers of the same individual.

2. Fingerprint representation

A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits anomalies in local regions of the fingertip, and it is the position and orientation of these anomalies that are used to represent and match fingerprints.

The uniqueness of a fingerprint is determined by the topographic relief of its ridge structure and the presence of certain ridge anomalies termed as minutiae points. Typically, the global information (location of core and delta points) defined by the ridge structure is used to determine the class [5,6] of the fingerprint, while the distribution of minutiae points is used to match and establish the similarity between two fingerprints [7,8].

Automatic fingerprint identification systems, which matches a query image against a large database of images. The minutiae points to determine an exact match. The ridge flow pattern itself is seldom used for matching fingerprints.

3. Fingerprint feature extraction

Plenty of work has been reported in fingerprint feature extraction. Minutiae and output of filter (image based features) are the two primarily used fingerprint features for verification. Minutiae feature detection heavily depends on the quality of input fingerprint image while the image-based techniques do not rely much on the quality of input fingerprint.

3.1 Minutiae extraction

The most commonly used minutiae for verification are ridge bifurcation and ridge endings. The fingerprint is viewed as a flow pattern with definite texture. Fingerprint image is an oriented texture. The orientation field of a fingerprint image represents the directionality of ridges. The local dominant orientation is computed as an optimal estimate of direction vectors at each pixel in a local window. Orientation field is useful in the process of feature extraction as well as in post processing. Fingerprint image typically divided into number of non-overlapping blocks and an orientation representative of the ridges in the block is assigned to the block based on analysis of grayscale gradients in the block. The block size depends on the inter-ridge distance i.e. it should include at least one ridge and one valley in a block. The block orientation could be determined from the pixel gradient orientations based on averaging, voting or optimization. The orientation field is given by

$$\theta(i,j) = 0.5\tan^{-1}\left(\frac{v_x(i,j)}{v_y(i,j)}\right) \qquad ----(1)$$

where

$$v_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}} 2G_x(u,v)G_y(u,v) \qquad ------(2)$$

$$v_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}} \left(G_x^2(u,v)G_y^2(u,v)\right) \qquad ------(3)$$

Where, w is the size of block or cell. G_x and G_y are the gradient magnitudes in x and y directions respectively. The orientation field of a typical fingerprint image is shown in figure 1. Orientation field is useful in extracting both the minutiae features and image-based features.

Following steps are involved in minutiae feature extraction.

3.1.1 Segmentation
3.1.2 Thinning
3.1.3 minutiae detection
3.1.4 Post processing

Segmentation includes the foreground separation, ridge segmentation and directional smoothing.

Foreground segmentation could be done using thresholding, adaptive thresholding. The novel techniques proposed by Ratha *et.al* [9] where variance has been used for segmentation of region of interest. A combined approach using variance and direction was proposed by Mehtre *et. al* [10] The algorithm proposed by Ratha *et. al.* will be discussed in this paper.

The fore ground needs to be segmented from the background. For this the variance of gray levels in a direction orthogonal to the orientation of each block. The region of interest exhibits very high variance in a direction orthogonal to orientation and low variance along the ridges. The background exhibits uniform variance. In other words background has low variance in all directions. Foreground is segmented by selecting a proper value of variance as threshold. Threshold may be local or global.

Consider the window with its projection in a direction orthogonal to the orientation. The ridge pixel attains local maxima (peak) in a direction orthogonal to orientation. Two neighboring pixels on either side of the peak are also retained along a direction perpendicular to the orientation field. Before projecting, the image the image is smoothed using a 1-dimensional averaging mask on each line oriented along a direction orthogonal to orientation of the window. The ridge pixels are assigned value 1, while remaining pixels 0.

The directional smoothing is applied to the detected ridges. A 3 by 7 mask of values all 1 is placed along the direction of each window. If the count of all 1 exceeds 25% of total then the ridge point is retained. The size of the window is decided empirically.

The binary image is thinned to have one pixel fingerprint image using skeletonization, which results in to spurious minutiae. The skeleton needs to be smoothed before minutiae point to be located. The box shaped morphological filter with size 3 by 3 with all 1 is used for smoothing.

The minutiae points are located in a 3 by 3 block. If a pixel consists of at least three neighbors, then its ridge bifurcation

And a ridge ending has only one neighbor. A Post processing stage filters the false minutiae

Post processing stage eliminates spurious points based on structural and spatial relationship of the minutiae like ridge break, spike elimination and boundary effects.

Usually the orientation of minutiae point and its x and y location are used to form the feature vector.

3.2 Image based features

Filters having both orientation and frequency localization are suited for fingerprint feature extraction. Fingerprint is an oriented pattern with a band of spatial frequency. There have been some techniques reported for the estimation of spatial frequency. Spatial frequency is a measure of average inter ridge distance (typically it is 9 to 11 pixels for 500 dpi scanners). 2D Gabor transform have been used for fingerprint feature extraction. The orientation and frequency selectivity of Gabor transform preserves the ridge information. The use of complex Gabor filter for fingerprint feature has been suggested by Lee and *et. al* in [11]. Anil K. Jain and *et. al* proposed a even symmetric Gabor filter for future extraction of texture images.

The spatial form of a 2D Gabor transform is given by

$$G_{\theta,f}(x,y)=\exp\left\{-1/2\left[\frac{x'^2}{\delta_x{}^2}+\frac{y'^2}{\delta_y{}^2}\right]\right\}\cos\left(2\pi f x'\right) \qquad --(4)$$

where

$$x' = x\cos\theta + y\sin\theta$$

$$y' = x\cos\theta - y\sin\theta$$

where *f* is the frequency of the sinusoidal plane wave at an angle θ with the *x*-axis, and δx and δy are the standard deviations of the Gaussian envelope along the x and y axes, respectively

Gabor filter are tuned to particular orientation and frequency to extract ridge information.

Fingerprint image has been filtered by Gabor filters those are tuned to eight different orientations (0, 22.5, 45, 67.5, 90, 112.5, 135, 157.5 degrees) with a spatial frequency = 1/average inter-ridge distance. The values of δx and δy decides the spread of Gaussian and needs the tread off. For the larger values more robust to noise but will not capture ridge information at finer level and to lower values it is less robust to noise but captures fine ridge information. Determinations of different features from the filter output have been discussed and compared in [12].

The magnitude response may be treated as features, variance is the novel feature computed from the filtered image as variance gives the measure of energy.

The variance features of all eight Gabor filtered fingerprint images constitutes the feature map or vector, and is used for verification.

4. Person Authentication

Minutiae-based person authentication techniques attempt to align two sets of minutiae points and determine the total number of matched minutiae.

This kind of matching heavily depends on the extraction of genuine minutia and the effect of translation and rotation on the fingerprint image. However such system requires less memory space and also relatively time required for authentication is also less. Also the minutiae-based authentication is suitable for smaller databases.

The Gabor feature requires sufficiently large space. The approach of feature extraction is global hence it is not sensitive to the local changes in the gray level in the fingerprint image. The feature vector may compared using classifiers like

Euclidian norm, Mahalabonis distance metric, K-NN classifier, K-mean classifier etc.

The authentication system will be tested for different values of FAR and FRR as per the requirements. Ideally the values of FAR and FRR should be as low as possible.

Two or more fingerprints of the same person could be combined for authentication, which will be more robust and reliable in the most secured systems and may provide an alternative to the conventional password, PIN number etc.

References

[1] A. K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[2] J. L. Wayman, “Fundamentals of biometric authentication technologies," International Journal of Image and Graphics, vol. 1, no. 1, pp. 93,113, 2001.

[3] J. Berry, D.A. Stoney, “The history and development of fingerprinting,” in: H.C. Lee, R. Gaensslen (Eds.), Advances in Fingerprint Technology, 2nd Edition, CRC Press, Boca Raton, FL, 2001, pp. 1–40.

[4] Federal Bureau of Investigation, The Science of Fingerprints: Classification and Uses, Government Printing Office, Washington, DC, US, 1984.

[5] K. Karu and A. K. Jain, “Fingerprint classification," *Pattern Recognition*, vol. 29, no. 3, pp. 389{404, 1996.

[6] A. Senior, “A combination fingerprint classifier," *IEEE Transactions on PAMI,* vol. 23, pp. 1165{1174, Oct 2001.

[7] A. K. Jain, L. Hong, and R. Bolle, “On-line fingerprint verification," *IEEE Transactions on PAMI*, vol. 19, pp. 302{314, April 1997.

[8] Z. M. Kov_acs-Vajna, “A fingerprint verification system based on triangular matching and dynamic time warping," *IEEE Transactions on PAMI,* vol. 22, pp. 1266{1276, Nov 2000.

[9] N. K. Ratha, S. Chen, A. K. Jain, “Adaptive flow orientation based texture extraction in fingerprint images, *Pattern Recognition*, 28(11): 1657-1672,Nov 1995.

[10] B. M. Mehtre,” Fingerprint image analysis for automatic identification,” *Machine Vision and Applications,* Vol.6, pp.124-139, 1993.

[11] Chiegh-Lee, Sheng D. Wang, “Fingerprint feature extraction using Gabor filters,” *Electronics Letters*, Vol. 35, No. 4, 1999.

[12] David A. Clausi, M. Ed Jernigan, “Designing Gabor filter for optimal texture seperability,” *Pattern Recognition*, 33 (2000) 1835-1849.