Defence Science Journal, Vol. 66, No. 6, November 2016, pp. 600-604, DOI : 10.14429/dsj.66.10800

Biometrics in Cyber Security

Jaspreet Kour[!], M. Hanmandlu[#], and A.Q. Ansari[*]

[!]Galgotias College of Engineering and Technology, Greater Noida - 201 306, India
[#]Indian Institute of Technology Delhi, New Delhi - 110 016, India
[*]Jamia Millia Islamia, New Delhi - 110 025, India
[*]E-mail: aqansari62@gmail.com

ABSTRACT

Computers play an important role in our daily lives and its usage has grown manifolds today. With ever increasing demand of security regulations all over the world and large number of services provided using the internet in day to day life, the assurance of security associated with such services has become a crucial issue. Biometrics is a key to the future of data/cyber security. This paper presents a biometric recognition system which can be embedded in any system involving access control, e-commerce, online banking, computer login etc. to enhance the security. Fingerprint is an old and mature technology which has been used in this work as biometric trait. In this paper a fingerprint recognition system based on no minutiae features: Fuzzy features and Invariant moment features has been developed. Fingerprint images from FVC2002 are used for experimentation. The images are enhanced for improving the quality and a region of interest (ROI) is cropped around the core point. Two sets of features are extracted from ROI and support vector machine (SVM) is used for verification. An accuracy of 95 per cent is achieved with the invariant moment features using RBF kernel in SVM.

Keywords: Cyber security, biometrics, fingerprint recognition, fuzzy features, invariant moment features

1. INTRODUCTION

The rapid growth of internet and computer interconnectivity for various applications such as online banking, e-commerce, m-commerce has lead to the concern of security attacks associated with these transactions. Along with enormous benefits offered by fast growing digital world, there are significant threats and risks to the government, defense and other critical departments in the country. Cyber security is a major issue in todays digital world with cyber crime is increasing day by day. The losses and distress caused by cyber attacks are prompting the pioneers in the field of information security to look for reliable and robust security measures.

The growing use of online banking, e-commerce has led to the use of biometric technology to secure these transactions. Biometrics provides a strong defense against cyber security attacks. Biometrics is considered as a safeguard against cyber crime. Now a day, banks encourage the use of fingerprint to authenticate transactions. Applications are available in the markets which are used to unlock computer or phones using facial recognition, fingerprint recognition or iris recognition.

A biometric system recognises a person using a specific physiological and or behavioral characteristic possessed by a person[1]. A biometric system is called either a verification system or an identification system depending on the application where it is used. A verification system verifies an individual by comparing its test biometric characteristic with the biometric template stored in the database whereas an identification system recognises an individual by searching the entire database for a match[1]. Physiological biometrics includes fingerprint, face, palm print, knuckle print, iris, ear, hand geometry etc whereas behavioral biometrics includes signature, gait, keystroke dynamics, speech, gesture etc. A biometric modality must satisfy properties such as universality, distinctiveness, permeance and collectability to be used in a biometric system.

Finger print has several desirable properties to be considered for an effective recognition system. Fingerprint recognition is one of the oldest and mature biometric technology and has applications in many areas. Ridges and valleys on the surface of a fingertip form a pattern, ridges are dark and valleys are bright. Ridges and valleys generally run in parallel, bifurcating and terminating at various points. Minutiae are the endpoints and crossing points of ridges. Finger prints possess one or more regions where the ridge lines assume distinctive shapes called singularities. These regions are classified as loop, delta and whorl as shown in Fig. 1. The core is defined as the point on the innermost ridge and a point where three different direction ridges meet is defined as the delta. The information provided by singular points is used for alignment, authentication and classification of fingerprints.

The approaches for fingerprint recognition are mainly divided into three categories: minutiae based, non minutiae based (image-based) and hybrid system which combines the minutiae and non-minutiae based approaches. A feature vector in the case of minutiae based approach involves extracting a set of minutiae from fingerprints as shown in Fig. 2 in multi-

Received : 27 February 2016, Revised : 19 May 2016
Accepted : 03 August 2016, Online published : 31 October 2016

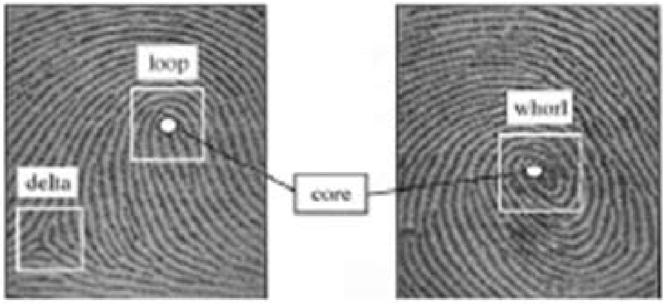

Figure 1. Singular regions and core point[1].

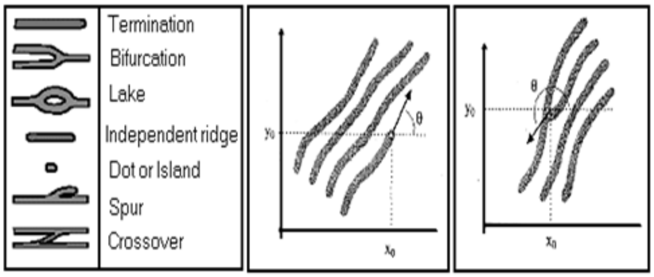

Figure 2. Common minutiae types[1].

dimensional plane. But this approach needs time consuming fingerprint image quality improvement using various enhancement techniques, applying filters, segmentation and also involves binarisation and thinning process and it also suffers from rejection of true or genuine minutiae and introduction of unreal and false minutiae. The rich discriminatory information available in fingerprint is rarely capitalised in this approach having high computational complexity. Image based fingerprint recognition does not involve detection and matching of minutiae points. Features in these methods are extracted using different type of filters like Gabor filter, Sobel filter or by using transforms like Fourier transform ,wavelet transform etc. Apart from fingerprint ridge pattern other features in the category of non minutiae based approach include texture, ridge shape, orientation and frequency of local ridge pattern etc. Global information is exploited in such methods and they require less preprocessing compared to minutiae based methods[2] .Combination of minutiae and non minutiae based methods are categorised as Hybrid methods for fingerprint recognition.

2. RELATED WORK

A bank of Gabor filters is proposed by Jain[3], *et al.* to obtain a compact fixed length finger code which provides both local and global details from a fingerprint. The two corresponding Finger Codes are matched using a distance measure like Euclidean distance. A hybrid fingerprint matching system utilising both minutiae and ridge direction information to represent and authenticate fingerprints is described by Ross[4], *et al.* A set of 8 Gabor filters, whose spatial frequencies correspond to the average inter-ridge spacing in fingerprints, is used to capture the ridge strength at equally spaced orientations.

The feature vector proposed by Tico[5], *et al.* consists of the standard deviations of the Discrete Wavelet Transform coefficients of the whole image at various scales and orientations. K-Nearest Neighbour classifier employing Euclidean distance is used for matching.

Integrated wavelet and fourier mellin transform (WFMT) is used for the feature extraction by Jin[6], *et al.* Multiple WFMT features constitute a set of reference invariant features. Euclidean distance is calculated between various WFMT feature vectors for obtaining the percentage match. Nanni and Lumini[7] used linear binary patterns (LBP) as a feature descriptor. Alignment of fingerprint images ,which is based on minutiae is done before dividing the image into several overlapping windows. Gabor filter with LBP is the feature vector for the fingerprint recognition system. The fingerprint descriptor as proposed by Nanni and Lumini[8] is based on HOG that represents an image by a set of local histograms containing occurrences of gradient orientation at each local cell of image. Decision level fusion of orientation, texture and spectral features of fingerprint image is proposed by Helfroush and Ghassemian[9]. Whole fingerprint image is used extracting features instead of using only points around core. Yang and Park[10] discussed moment features having fixed length as the feature vector extracted from tessellated cells around the core point of the fingerprint image. Similarity measure based on the eigen value weighted cosine distance is used to find the matching percentage of query and template. Fingerprint matching is based on the measures of similarity to the eigen value-weighted cosine distance to match the two corresponding feature vectors of the test and template. In the image based fingerprint matching method as presented by Kour and Awasthy[2], the orientation field is used as a feature vector and the Euclidean distance is employed as a classifier. In fingerprint recognition system developed by Khalil[11], *et al.* 16 co-occurrence matrices are used to compute four statistical descriptors namely, correlation, contrast, energy and homogeneity and Euclidean distance is used as a classifier. Fusion of spectral and directional features is discussed by Helfroush[12] and Mohammad pour. Hartley transform is used for feature extraction by Bharkad[13] and Kokare. Hartley transform is faster than the Gabor filter requiring a set of filters oriented at different angles and frequencies. Finally, city block distance is used for computing the similarity between two fingerprint images. Discrete wavelet transform (DWT) based fingerprint recognition system as described by Kumar[14], *et al.* has been used as feature vector followed by Euclidean distance as a classifier. The features of fingerprints such as Directional Information, Centre Area and Edge Parameters are obtained by considering three DWT levels at four sub bands. Two features used for fingerprint verification are wavelet and Pseudo Zernike Moments in Pokhriyal[15], *et al.* The hybrid approach has the advantage of combining the most discriminating features for fingerprint recognition. Multi resolution features of aligned fingerprints are computed using 2-D discrete wavelet transform. Principal component analysis (PCA) is used for dimensionality reduction followed by Euclidean classifier for verification. Pseudo Zernike moments are used to create invariant features and Bayesian classifier is used to validate the moments in Deepika[16], *et al.*

3. PROPOSED METHOD

The main steps involved in the proposed fingerprint recognition system are: Preprocessing, extracting region of interest (ROI), feature extraction and verification. The block diagram of the proposed system is shown in Fig. 3. The Short Time Fourier Transform (STFT) is applied to fingerprint image for enhancement which analyses it in space and frequency domain. The Fourier domain-based block wise contextual filter enhances the fingerprint images[17]. After preprocessing a landmark point is needed in fingerprint image like core point around which to earmark a region of interest (ROI). The core point is defined as point of maximum curvature on the convex ridge. Maximum curvature is detected using complex filter methods to obtain accurate and reliable core point in a fingerprint image[18]. After core point detection, area around the core point is cropped for feature extraction. The choice of ROI is made to ensure the availability of rich information available around the core point for fingerprint matching. The ROI of size 64 by 64 pixels extracted from the whole fingerprint image is shown in Fig. 4.

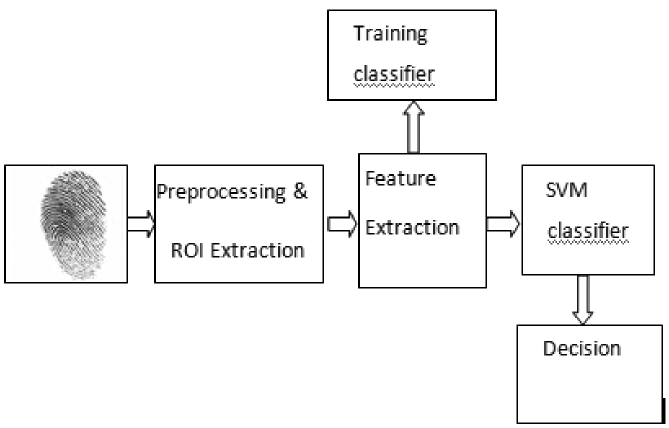

Figure 3. Block diagram of proposed method.

Figure 4. Fingerprint Image and ROI extracted image.

Two set of features namely fuzzy features and invariant moment features are obtained from the region of interest (ROI) of the fingerprint image.

3.1 Feature Extraction

Two non-minutiae descriptors are presented here for extracting features from cropped images which are ROIs. These descriptors overcome the shortcomings of the minutiae based approach for fingerprint recognition.

Steps for fuzzy features

1. Divide the cropped image into various non-overlapping square blocks of size W x W.
2. Calculate the mean intensity, I_{av} in k^{th} window using:

$$I_{av} = \frac{1}{WXW} \sum_{i=1}^{W} \sum_{i=1}^{W} I(i,j) \tag{1}$$

3. Obtain the maximum intensity, $I_{\max}$ in the k^{th} window.
4. Obtain the membership function, μ_{ij} for every pixel in k^{th} window from:

$$\mu_{ij} = \frac{\left|I(i,j) - I_{av}\right|}{I_{\max}} \tag{2}$$

5. Compute the complement of the above membership function as this has values in the low range from 0 to 0.2 using

$$\left(\mu_{ij}\right)_1 = 1 - \mu_{ij} \tag{3}$$

6. Compute the fuzzy feature from k^{th} window from:

$$I_{\mu k} = \frac{\sum\sum\left(\left(\mu_{ij}\right)_1 \cdot I(i,j)\right)}{\sum\sum\left(\mu_{ij}\right)_1} \tag{4}$$

The number of features obtained is equal to the number of square blocks in the cropped image.

It may be noted that with cropped image of size 65x65 and window size (W) of 5x5, the number of features extracted is 169.

Steps for invariant moment features

1. Divide the cropped image into various non- overlapping square blocks of size W x W.
2. Find seven invariant moments invariant to translation, scale change, mirroring and rotation for each window. This set of moments[19] is given by

$$\phi_1 = \eta_{20} + \eta_{02} \tag{5}$$

$$\phi_2 = \left(\eta_{20} - \eta_{02}\right)^2 + 4\eta^2_{11} \tag{6}$$

$$\phi_3 = \left(\eta_{30} - 3\eta_{12}\right)^2 + \left(3\eta_{21} - \eta_{03}\right)^2 \tag{7}$$

$$\phi_4 = \left(\eta_{30} + \eta_{12}\right)^2 + \left(\eta_{21} + \eta_{03}\right)^2 \tag{8}$$

$$\begin{aligned}\phi_5 &= \left(\eta_{30} - 3\eta_{12}\right)\left(\eta_{30} + \eta_{12}\right) \\ &\left[\left(\eta_{30} + \eta_{12}\right)^2 - 3\left(\eta_{21} + \eta_{03}\right)^2\right] \\ &+ \left(3\eta_{21} - \eta_{03}\right)\left(\eta_{21} + \eta_{03}\right)\left[3\left(\eta_{30} + \eta_{12}\right)^2 - \left(\eta_{21} + \eta_{03}\right)^2\right]\end{aligned} \tag{9}$$

$$\begin{aligned}\phi_6 &= \left(\eta_{20} - \eta_{02}\right)\left[\left(\eta_{30} + \eta_{12}\right)^2 - \left(\eta_{21} + \eta_{03}\right)^2\right] \\ &+ 4\eta_{11}\left(\eta_{30} + \eta_{12}\right)\left(\eta_{21} + \eta_{03}\right)\end{aligned} \tag{10}$$

$$\begin{aligned}\phi_7 &= \left(3\eta_{21} - \eta_{03}\right)\left(\eta_{30} + \eta_{12}\right) \\ &\left[\left(\eta_{30} + \eta_{12}\right)^2 - 3\left(\eta_{21} + \eta_{03}\right)^2\right] \\ &+ \left(3\eta_{120} - \eta_{30}\right)\left(\eta_{21} + \eta_{03}\right) \\ &\left[3\left(\eta_{30} + \eta_{12}\right)^2 - \left(\eta_{21} + \eta_{03}\right)^2\right]\end{aligned} \tag{11}$$

3. Reduce dynamic range of the moments using the logarithmic function by

$$\phi_i = \left|\log\left(\phi_i\right)\right| \tag{12}$$

where $i = 1,2,...7$.

It may be noted that for ROI of size 64 x 64 and window size (W) of 16 x 16, the number of features extracted is 112.

3.2 Verification

Support vector Machine (SVM) is a widely used tool in pattern reconition field. It makes use of the Structural Risk Minimisation (SRM) principle. It provides very good performance in non linear patterns by transforming the input vectors into a high dimension feature space with the help of a kernel. It locates optimal hyper plane for linearly separable data and extends to nonlinearly separable data by mapping them to high dimension feature space. SVM has many applications like biometric based authentication, information management, text categorisation, bioinformatics etc. SVMs are based on the principle of Structural Risk Minimisation rooted in the statistical learning theory. Details about SVM are available in Vapnik[20] and also in Byun[21] and Lee.

LIBSVM[22] has been used for verification. Four built in kernels that we have at our disposal are; linear, polynomial, radial basis function, and sigmoid.

Parameter tuning is required in Support Vector Machines like other learning algorithms so as to find the optimal parameters which result in improved accuracy on the test data. Three kernels are used and for each kernel, 5-fold cross validation is performed on the training set. A logarithmic 'grid search' is made to get the parameters c and γ. The values of c and γ giving the best average cross-validation accuracy are employed at the testing phase.

4. EXPERIMENTAL RESULTS

4.1 Database

The benchmark database FVC2002DB1B[23] has been used in our experiments. It consists of ten users with eight impressions each. The database is divided into training and testing set. The training set consists of seven fingerprint images and testing set consists of one fingerprint image. The images are taken with an optical sensor having a size of 388 x 374 at a resolution of 500dpi.

4.2 Experiments

Different fingerprints are selected for training and testing and this process is repeated four times. The mean of the four experimental trials is considered as the final performance. Each set of features is set aside for verification using SVM.

Different window sizes (W) have been experimented on ROIs. The best results are obtained on fuzzy features for a window size of 5x5 and on invariant moments for a window size of 16x16. The features are normalised before inputting to SVM

Table 1. Accuracy of proposed system

FVC2002	Accuracy(%)		
	Linear	RBF	Polynomial
Fuzzy features	75	87.5	77.5
Invariant moment features	92.5	95	90

5. CONCLUSION

This paper presents a fingerprint recognition system which can be used for computer login, access control, internet banking or other such applications where security is a concern. Biometrics is being effectively used as a safeguard against cyber crime. In this work a fingerprint recognition system is developed using non-minutiae features: fuzzy features and invariant moment features extracted from ROIs as these result in fixed length feature vectors and are computationally simple. SVM is used for verification. A comparative study shows that fuzzy features give an accuracy of 87.5 per cent whereas the invariant moment features give an accuracy of 95 per cent both with RBF kernel. Biometrics is a key to the future of cyber security.

REFERENCES

1. Maio, D. & Maltoni, D. Handbook of fingerprint recognition. Springer Verlag, 2009.
2. Kour, J. & Awasthy, N. Non minutiae based fingerprint matching. *In* International Association of Computer Science and Information Technology –IEEE Spring Conference, 2009, 199 – 203. doi : 10.1109/IACSIT-SC.2009.127
3. Jain, A.K.; Prabhakar, S.; Hong, L. & Pankanti, S. Filterbank-based fingerprint matching. *IEEE Trans. Image Proces.*, 2000, **9**(5), 846-859. doi : 10.1109/83.841531
4. Ross, A.; Jain, A.K. & Reisman, J. A hybrid fingerprint matcher. *Pattern Recog.,* 2003*,* **36**(7), 1661-1673. doi : 10.1016/S0031-3203(02)00349-7
5. Tico, M.; Kuosmanen, P. & Saarinen, J. Wavelet domain features for fingerprint recognition. *Electron. Lett.*, 2001, **37**(1), 21–22. doi : 10.1049/el:20010031
6. Jin, A.T.B.; Ling, D.N.C. & Song, O.T. An efficient fingerprint verification system using integrated wavelet and fourier-mellin invariant transform, *Image Vis. Comput.*, 2004, **22**(6) 503–513. doi : 10.1016/j.imavis.2003.12.002
7. Nanni, L. & Lumini, A. Local binary patterns for a hybrid fingerprint matcher. *Pattern Recognition,* 2008, **41**(11), 3461-3466. doi : /10.1016/j.patcog.2008.05.013
8. Nanni, L. & Lumini, A. Descriptors for image-based fingerprint matchers. *Expert Sys. Appl.,* 2009*,* **36**(10), 12414-12422. doi : 10.1016/j.eswa.2009.04.041
9. Helfroush, S. & Ghassemian, H. Nonminutiae based decision level fusion for fingerprint verification. *EURASIP J. Adv. Signal Proces.*, 2007. doi : 10.1155/2007/60590
10. Yang, J.C & Park, D.S. A fingerprint verification algorithm using tessellated invariant moment features. *Neurocomputing* , 2008, **71**, 1939– 1946. doi : 101016/j.neucom.2007.12.034
11. Khalil, M. S.; Mohammed, D.; Khan, M. K. & Al-Nuzaili, Q. Fingerprint verification using statistical descriptors. *Digital Signal Proces.*, 2009, **20**(4),1264-1273. doi : 10.1016/j.dsp.2009.12.002
12. Helfroush, M.S. & Mohammadpour, M. Fingerprint verification system: a non-minutiae based approach. *In* International Conference on Computer, Control and Communication , 2009, pp. 1-4

doi : 10.1109/IC4.2009.4909271

13. Bharkad, S. &. Kokare, M. Hartley transform based fingerprint matching. *J. Info. Proces. Sys.*, 2012, **8**(1). doi : 10.3745/JIPS.2012.8.1.085
14. Kumar, S.; Raja, K.B.; Chhotaray, R.K. & Pattanaik, S. DWT based fingerprint recognition using nonminutiae features. *Int. J. Comput. Sci.*, 2011, **8**(2), 257-265. ISSN (Online): 1694-0814.
15. Pokhriyal, A. & Lehri, S. A new method of fingerprint authentication using 2-D wavelets. *J. Theoretical Applied Info. Technol.*, 2010, **13**(2), 131 – 138.
16. Deepika, C.L.; Kandaswamy, A.; Vimal, C. & Sathish, B. Invariant feature extraction from fingerprint biometric using pseudo zernike moments. *In* International Joint Journal Conference on Engineering and Technology, 2010 .
17. Chikkerur, S.; Cartwright, A.N. & Govindraju, V. Fingerprint enhancement using STFT analysis. *Pattern Recognition*, 2007, **40**(1), 198-211. doi :10.1016/j.patcog.2006.05.036
18. Nillson, K. &. Bigun, J. Localisation of corresponding points in fingerprints by complex filtering. *Pattern Recog. Lett.* , 2003, **24**(13), 2135-2144. doi : 10.1016/S0167-8655(03)00083-7
19. Gonzalez, R.C. & Woods, R.E. Digital image processing, second ed., Prentice-Hall, 2002
20. Vapnik, V.N. Statistical learning theory. New York: Wiley-Interscience, 1998.
21. Byun, H. & Lee, S. SVM survey applications of support vector machines for pattern recognition: A Survey. LNCS 2388, Springer-Verlag Berlin Heidelberg, 2002, pp. 213-236.
22. Chih-Chung, Chang & Chih-Jen, Lin. LIBSVM: a library for support vector machines, 2001. http://www.csie.ntu.edu.tw/~cjlin/libsvm (Accessed on 5 Feburary 2011).
23. FVC2002 Web site: http://bias.csr.unibo.it/2002 (Accessed on 3 Feburary 2012).

CONTRIBUTORS

Dr Jaspreet Kour received her BTech, MTech from REC (NIT) Bhopal and UPTU Lucknow respectively and PhD from Jamia Millia Islamia, New Delhi. Currently working as an Associate Professor in the Department of Electronics and Instrumentaion Engineering at Galgotias College of Engineering and Technology, Greater Noida, U.P. Her research areas are : Pattern recognition, image processing and biometrics.
In the current study, Kour has designed the study and performed the experiments and drafted the mauscript.

Dr Madasu Hanmandalu received BE (Electricals Engineering) from Osmania University, Hyderabad, in 1973; MTech in Power systems from R.E.C. Warangal, Jawaharlal Nehru Technological University, in 1976, and PhD from Indian Institute of Technology, Delhi, in 1981. Currently working as a Professor in the Department of Electrical Engineering at Indian Institute of Technology, New Delhi. His current research interests mainly include : Soft computing, biometrics, and medical imaging.
In the current study, he has provided direction and guidance in the study and revised the manuscript.

Dr Abdul Quaiyum Ansari received his BTech, MTech, and PhD from AMU, Aligarh, IIT Delhi and JMI, New Delhi, respectively. is a Professor in the Department of Electrical Engineering at Jamia Millia Islamia, New Delhi. His research interests include : Computer networks, networks-on-chip, fuzzy logic, and image processing.
In the current study, he has revised the manuscript for important technical content and guided throughout the study.