Palmprint Recognition Using Geometrical and Texture Properties

Rohit Khokher, Ram Chandra Singh, and Rahul Kumar

Abstract--- This paper proposes an algorithm for biometric palm recognition of an individual using geometrical and texture properties. Biometrics is physiological characteristics of human beings, unique for every individual that are usually time invariant & easy to acquire. Palmprint is one of the physiological biometrics due to its stable & unique characteristics. The physical dimensions of a human palm contains information that is capable of authenticating the identity of an individual. In this study algorithm is proposed to extract a finger length as geometrical feature and principal lines as texture feature. Simulation results shows false accept rate (FAR) is 25%, false reject rate (FRR) as 18.75%, genuine acceptance rate (GAR) 81.25%, half total error rate (HTER) 21.87% and accuracy 78.12% in case of geometrical features whereas accuracy is 92.3% in case of texture feature.

Keywords-- Biometrics, median filter, edge detection, Morphological operation, Maximum Curvature method.

I. Introduction

Automatic personal authentication is a significant component of security systems with many technological challenges. The traditional methods of identification which includes passwords or tokens are not much reliable, but identifying individuals based on his or her unique physical characteristics is much reliable technique. A number of researchers have started the interaction between biometrics and cryptography, two potentially complimentary security technologies.

Biometrics [1-6] guarantees the identification of individuals based on measuring the personal unique features with a high degree of assurance while cryptography assures a high degree of trust in the transactions of information through the communication networks. Any human physiological and behavioral characteristic can be used as a biometric characteristic as long as it satisfies the requirements of universality, distinctiveness, permanence, collectability, performance, acceptability and circumvention [7]. Few biometric traits that are used to authenticate or identify individuals are Fingerprints, Iris, ECG, Retina, Gait, Footprint, Speech, Face, DNA, etc. Palmprint is also one of the physiological characteristic that can be used to distinguish between individuals. Palmprint is a biometric modality which can be used for authentication of a person's identity because of its richness. It has not only the information available on fingers but it has far more amount of details in terms of principal lines, wrinkles and creases. Moreover it can easily be combined with hand shape biometric so as to form a highly accurate and reliable biometric based personal identification system. This type of identification has become an increasingly active research topic over the years. Palmprint based identification systems utilize the geometric features of the palm like length and width of the fingers, area of the distal phalanx, length to width ratio, area of the palm, perimeter of the palm and differences with center ratio. In case of texture features of the palm, principal lines, creases and wrinkles have been utilized for identification.

Several studies on personal-recognition system have been developed using palmprint as a feature. Zhang, et al. [8] developed an online identification system by implementing Gabor filter to obtain palmprint feature information. Duta, et al. [9] separated set of feature points along the main line of palms and calculates a score that fits between a set of related features of the two hands. Li, et al. [10] used Fourier transformation to obtain the features of the palm. Wu, et al. [11] formed a line vector features (LVF) using the gradient magnitude and orientation of points on the main line of the palm to extract the palmprint features. Jain and Duta [12] employed deformable hand shape matching to verify user. Kumar, et al. [13] incorporated two hand geometric features: palmprint and hand geometry to extract salint features and verified users based on the fusion features. Han, et al. [14] used Sobal and morphological operation to extract line like features from palmprint. Huang, et al. [15] proposed the modified finite random transform and extracted principal lines and Yao,et al. [16] combined face features with palmprint and performed feature level fusion. In the geometric feature approach such as feature points, finger length, intersecting points, etc. are sometimes difficult to extract directly from a given palmprint image with low resolution. In the texture based approach the texture features are not sufficient and the extracted features are greatly affected by lightning. These issues motivated us to study the comparison of recognition rates and computational efficiency for palmprint recognition. The complete process of the study is shown in the figure 1.1. The sensor is used to obtain the palmprint images. In this study database is taken from www.coep.org.in [17] College of Engineering, Pune. During preprocessing of an image several operations like orientation, masking, filtering, normalization and edge detection were applied on images to extract finger length features of a palmprint. To extract principal lines of a palmprint image enhancement operations like morphological, masking and segmentation were applied.

Rohit Khokher is with the Department of Computer Science and Engineering, Vidya College of Engineering, Meerut, India (E-mail: khokherrohit@gmail.com).

Ram Chandra Singh is with the Department of Physics, Vidya College of Engineering, Meerut, India.

Rahul Kumar is with the Department of Computer Science and Engineering, Sharda University, Greater Noida, India.

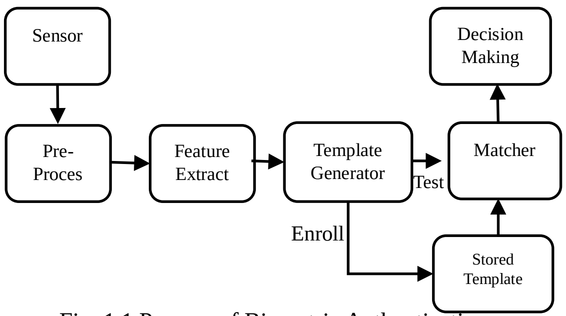
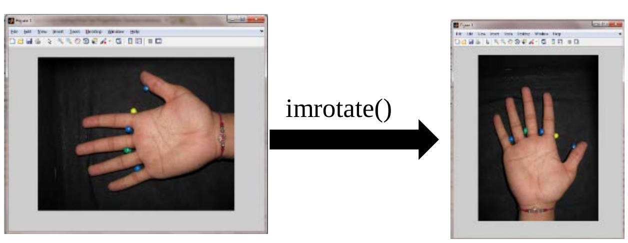


Fig. 1.1 Process of Biometric Authentication

II. Enhancement Of Image

The database obtained from www.coep.org.in, College of Engineering, Pune [17] contains the palm images of 160 individuals. For each individual palm images were captured 8 times i.e. 8 prints of every individual. All the prints are of right hand palm. The images obtained from the database are raw images that need to be pre-processed before gaining any information from them. The images contains noises like dust particles, light reflections or irregular backgrounds due to which accurate feature extraction cannot be done. Therefore the enhancement technique was applied to enhance palmprint impressions for feature extraction. Preprocessing of images involves processes orientation, normalization, masking, filtering and edge detection before extracting the finger length feature of a palmprint.

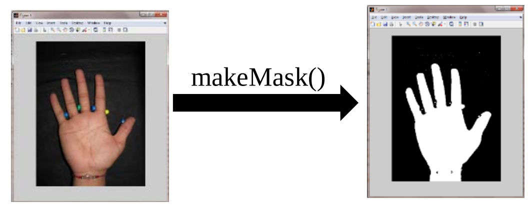
Orientation is required to make the palmprint images aligned in the same fashion so that a generalized algorithm can be applied over the whole database altogether. Orientation is done to rotate palmprint images that aligned at some angle. Figure 2.1 shows the oriented image O(x,y,z) obtained from the original input image I(x,y,z). In MATLAB orientation process can be done by using *imrotate()* inbuilt function



(a) I(x,y,z) (b) O(x,y,z)

Fig. 2.1 Orientation of image

Masking is a process to extract an object from an image, the object is masked using a masking matrix that assigns a value 1(white) to the object to be masked and 0(black) to the rest of the image. Thus a 2-bit black & white image is obtained that clearly shows the masked object. In this study the red layer of the oriented image was masked i.e. Or(x,y) (extracted as O(x,y,1)) using a pre-defined function *makeMask()* in MATLAB. The *makeMask()* function takes as its input the background image, the original input image and the tolerance value and gives the 2-bit masked image as M(x,y). Figure 2.2 shows the masked image M(x,y).



(a) O(x,y,z) (b) M(x,y)

Fig. 2.2 Masking of Image

Filtering is an image enhancement technique that is used to remove unwanted information from the image that had occurred as noise which may be due to dust particles, light reflections or irregular backgrounds. Many noise removal filters are available that removes the noise based on frequency or statistical information of the image. In this study several filters were used to remove the noise from the masked image that is shown in figure 2.3. The resultant image given by median filter is better in comparison to other filter because it is best known for removing "salt and pepper" type of noise which exists in the most of the masked image M(x,y) obtained after masking. The default mask matrix in median filter is of 3x3 in size but in this study it has been increased to 17x17 sized matrix. Figure 2.3 gives the masking matrix.

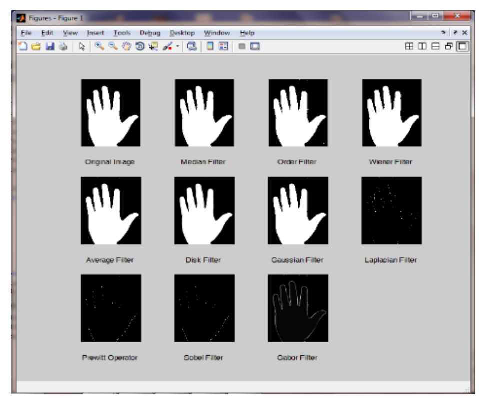


Fig. 2.3 Comparative results of different filters

$$\begin{bmatrix} 1 & 2 & 3 & . & . & . & 17 \\ 2 & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] \\ 3 & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] \\ . & [\ ] & [\ ] & Median\ Value & [\ ] & [\ ] & [\ ] \\ . & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] \\ . & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] \\ 17 & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] & [\ ] \end{bmatrix}_{17\times 17}$$

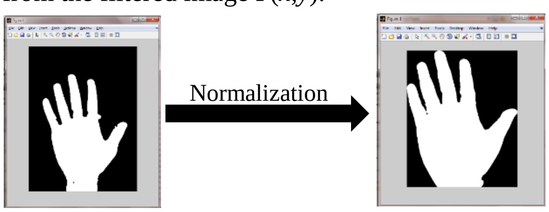
Fig. 2.4 Median Filter Matrix

This filter is also known as order-statistical filter as it takes the middle value from the set of sorted values that comes in a mask at a time. Thus irregular or sudden changes in the pixel values which represents noise is cleared. In this study an inbuilt function *medfilt2()* of MATLAB is used to filter the Masked image M(x,y). This function takes as input the masked image M(x,y) and the size of the matrix (17×17) and gives as output the filtered image F(x,y). Figure 2.5 shows the filtered image.

(a) M(*x*,*y*) (b) F(*x*,*y*)

Fig. 2.5 Filtering using median filter

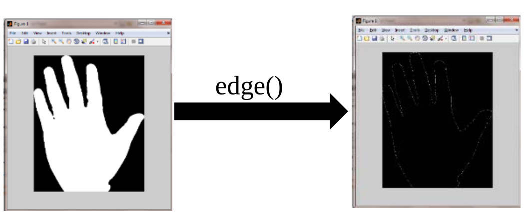
The process of normalization is done over a filtered image F(*x*,*y*) to make it fit to a standard which may be in respect of its dimensions or frequency. Normalization is done so that operations can be applied over it irrespective of any environmental disturbances like empty spaces, irrelevant color layers, etc. In this process the filtered image F(*x*,*y*) is normalized by removing empty regions from the left, right, top and the bottom of the image and the normalized image N(*x*,*y*) is obtained. In this study normalization helps to estimate the correct length of the palm and the fingers irrespective of the area of the palm visible which differs from one image to the other. Figure 2.6 shows the normalized image N(*x*,*y*) obtained from the filtered image F(*x*,*y*).



(a) F(*x*,*y*) (b) N(*x*,*y*)

Fig. 2.6 Normalization

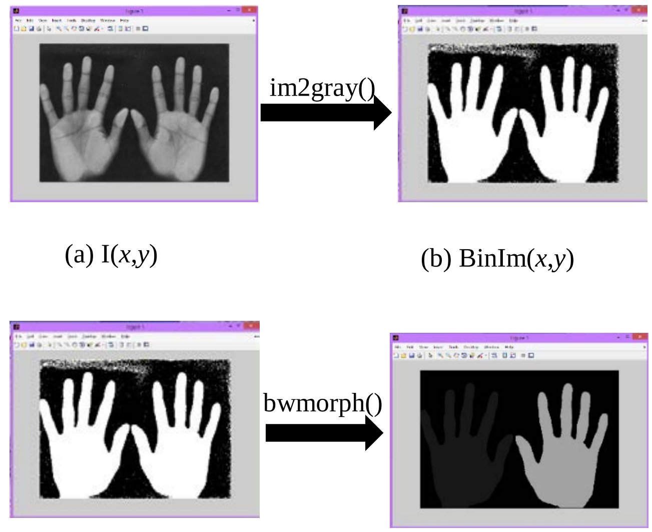
The final and the most important technique used for image enhancement is the edge detection. Edge detection is the name for a set of mathematical methods which aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The points at which image brightness changes sharply are typically organized into a set of curved line segments termed edges [18]. In this study the edges of the normalized image N(*x*,*y*) was obtained using an inbuilt function *edge()* in MATLAB. The function takes as input the normalized image N(*x*,*y*) and gives the output image E(*x*,*y*) that has a single pixel thick edge of the input palm. Figure 2.7 shows the detected edge of the palm.



(a) N(x,y) (a) E(x,y)

Fig. 2.7 Edge Detection

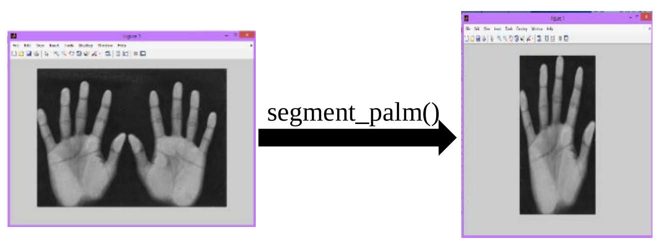
To extract the principal lines as texture features of a palmprint following image enhancement operations have been applied: morphological, masking and segmentation operation. In the enhancement operation, the RGB input image I(*x*,*y*) was converted into grayscale image GIm(*x*,*y*) using *rgb2gray()* and grayscale image into binary image BinIm(*x*,*y*) using *im2bw()* of MATLAB. Morphological operation is applied on the binary image BinIm(*x*,*y*) to remove the foreground pixels and return the mask image M(*x*,*y*). This operation was done using *bwmorph()* function



(c) BinIm(*x*,*y*) (d) M(*x*,*y*)

Fig. 2.8 Enhancement

Segmentation operation has been applied on masked image M(*x*,*y*) to extract the region of interest as shown in Fig 2.9 and is stored as S(*x*,*y*).



(a) I(*x*,*y*) (b) S(*x*,*y*)

Fig. 2.9 Segmentation

III. Algorithm To Extract Feature

The final image obtained after image enhancement techniques is E(*x*,*y*) that contains the fine edge of the palmprint which was given as an input image to feature extraction algorithm to compute the length of four fingers L_1, L_2, L_3 and L_4 as a geometrical features. The following steps of an algorithm are involved to find out the length of four fingers:

Step1: Obtain the set of points a[1...n] from the image edged E(*x*,*y*) such that their neighborhood pixels in the y-coordinate are of the same frequency.
Step 2: Cluster the set points in a[1...n] such that they are away from each other by a threshold value i.e. 20 pixels, so that only tip of the fingers are obtained as a1[1...m].

Step 3: Replace a by a1 and repeat the process of clustering until only 4 values are not obtained in the set of points under a1[1...m].

Step 4: The respective positions of these 4 values gives the length of fingers as L_1, L_2, L_3 and L_4 and shown in figure 3.1 and are stored as template in database for matching purpose.

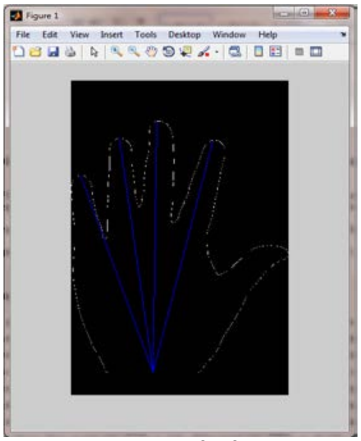


Fig. 3.1 Length of 4 fingers

The image obtained after the segmentation image enhancement techniques is S(x,y) that contains the enhanced image of the palmprint which was given as an input image to feature extraction algorithm to compute the principal lines of the palmprint. The following steps of an algorithm are involved to find out the principal lines as texture feature of the palmprint:

Step1: The segmented image S(x,y) and the masked image M(x,y) was given as an input the maximum curvature function which extracts the curvature patters from the palmprint and stored as CF(x,y).

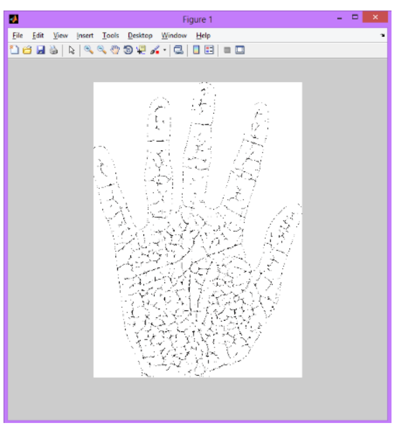


Fig. 3.2 Curvature patterns on palmprint, CF(x,y)

Step2: The curvature patters CF(x,y) contains unwanted data which was further processed using morphological operation in specific pattern which gives the required principal lines and stored as PF(x,y) as template in database for the evaluation of performance parameters.

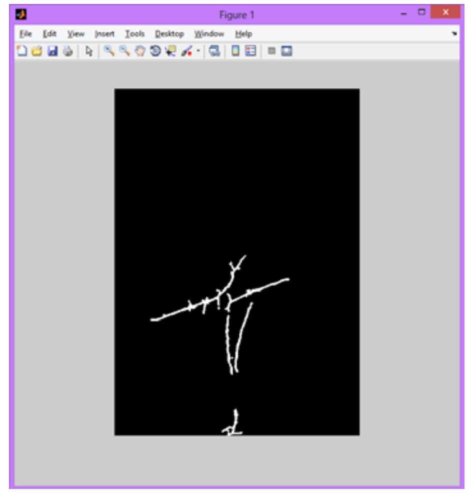


Fig. 3.3 Principal lines, PF(x,y)

Step3: The principal lines PF(x,y) were then stored as template for further matching purpose. The pixel index value were used for comparison.

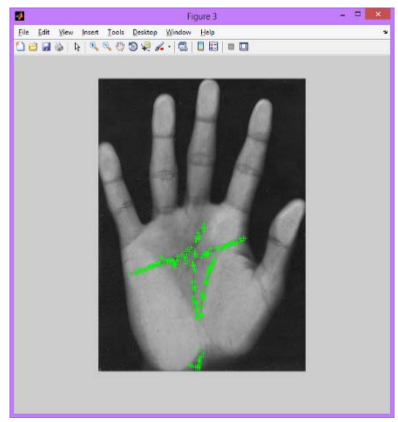


Fig. 3.4 Principal lines plotted on palmprint during matching

IV. Result Analysis

The performance of biometric security key generated by a system can be evaluated on the basis of biometric authentication parameters such as false accept rate, false reject rate, genuine accept rate, half total error rate, accuracy, etc. [19-21].

False Accept Rate (FAR) is the percentage of faulty recognized users, it is a measurement that explains the percentage of faulty recognized individuals.

$$FAR = \frac{No.of\ false\ acceptance\ found}{Total\ No.of\ Comparisons} \times 100$$

In this study out of 10176 comparisons 2544 were wrongly accepted. Hence, FAR computed is 25% in case of geometrical features and 10.20% in texture feature as shown in table 4.1.

False Reject Rate (FRR) is a statistic used to measure biometric performance when operating in the verification task and it usually calculated as the percentage of times the system produces a false reject. The FRR is calculated as,

$$FRR = \frac{No. of\ false\ rejections\ found}{Total\ No. of\ Comparisons} \times 100$$

In this study out of 1120 comparisons 210 were rejected when they were the legitimate user. Hence, FRR computed is 18.75% in case of geometrical features and 5.20% in texture feature as shown in table 4.1.

Genuine acceptance rate (GAR) is the percentage of genuine matches and is defined as

$$GAR = 1 - FRR$$

The GAR is found to be 81.25% in case of geometrical features and 4.20% in texture feature as shown in table 4.1. For a good security system, the GAR should be high.

Half Total Error Rate (HTER) is a possible way to measure the performance of the biometric system by combining both types of system errors i.e. false accept and false reject. Therefore HTER is a biometric measure which combines the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) and is defined by following formula:

$$HTER = \frac{1}{2}\ (FAR + FRR)$$

HTER obtained in this case is 21.875% in case of geometrical features and 7.70% in texture feature as shown in table 4.1.

Accuracy is defined as the percentage efficiency of a system in terms of its ability of authentication. The accuracy is calculate as,

$$Acuracy = 100 - \frac{FAR + FRR}{2}$$

Accuracy of the system calculated is 78.12% in case of geometrical features and 92.30% in texture feature as shown in table 4.1.

TABLE 4.1
PERFORMANCE PARAMETERS (IN %)

Features	FAR	FRR	GAR	HTER	Acc.
Geometrical Feature (Finge Length)	25.00	18.75	81.25	21.87	78.12
Texture Featu (Principal lines	10.20	5.20	4.20	7.70	92.30

V. CONCLUSION

Biometrics is being used all over the globe and is undergoing constant development. Human palmprint and hand geometry has proved to be a reliable biometric. In this work an algorithm is proposed to extract geometrical and textural feature of a palmprint for authentication of an individual using human palmprint. Biometrics for a single feature used alone may prove to be a weak authentication tool as the human palmprint can be sensed by some false means without making individual aware of it. Thus, the integration of geometrical and texture feature for the biometric technology makes a powerful tool with least chances of getting forged or attacked. This study aims to provide a biometric security to the security systems which can be applied for highly secure areas like nuclear plants, banks, military base, airports, parliaments, secretariats etc. Most of the security system studies have used fingerprint recognition, facial recognition, iris recognition & voice recognition as their biometric modality means whereas fewer studies have been reported using human palmprints as an input for security system. The performance of the proposed algorithm in case of texture feature is suitable for real time applications.

As a future work, feature extraction techniques either in palmprint feature or hand geometry can be enhanced and can be fused with other biometric traits for enhancing the performance of biometric security in the security systems.

VI. ACKNOWLEDGMENT

The authors gratefully acknowledge the management of Vidya College of Engineering for providing us all facility and support needed for this work.

REFERENCES

[1] Liang Wang and Xin Geng, “Behavioral Biometrics for Human Identification”, Medical Information Science Reference, 2010.
[2] N.V. Boulgouris, Konstantinos N. Plataniotis and E. M. Tzanakou, “Biometrics: Theory, Methods and Applications”, Wiley-IEEE Press, 2009.
[3] Arun A. Ross, Karthik Nandakumar and Anil K. Jain, “Handbook of Multibiometrics”, International Series on Biometrics, Springer, 2006.
[4] James Wayman and Anil Jain, “Biometric Systems: Technology, Design and Performance Evaluation”, Springer, 2004.
[5] Samir Nanavati, Michael Thieme and Raj Nanavati , “Biometrics: Identity verification in a networked world”**,** John Wiley & Sons, 2002.
[6] Anil Jain, Ruud Bolle and Sharath Pankanti, “Biometrics: personal identification in networked society”**,** Boston: Kluwer Academic, 1999.
[7] Kasturika B.Ray and Rachita Mishra, “Palmprint as a Biometric Identifier”, International Journal of Electronics and Communication Technology, 2011
[8] D. Zhang, Wai-Kin Kong, J. You and M. Wong, “Online Palmprint Identification”, IEEE Transaction on Pattern Analysis and Machine Intelligence, 25th ed, vol-9, 2003.
[9] N. Duta, A.K. Jain, K.V. Mardia, “Matching of Palmprints”, Pattern Recognition Letters, 23rd ed, 2002, pp. 477-485.
[10]W.X. Li, D. Zhang, S.Q. Xu, “Palmprint Recognition Based on Fourier Transform”, Journal of Software, 13(5), 2002.
[11]X.Q. Wu, K.Q. Wang, and D. Zhang, “An Approach to Line Feature Representation and Matching for Palmprint Recognition”, http://www.jos.org.cn/10010-9828/15/869.htm, 2004.
[12]A.K. Jain, N. Duta, “Deformable Matching Of Hand Shapes For User Verification”, International Conference on Image Processing, Vol. 4, 1999, pp. 24-28.
[13]N. Otsu, “A threshold selection method from gray-scale histogram”, IEEE Trans. Syst., Man, Cybernetics,vol. 8, 1978, pp. 62-66.
[14]C. C. Han, H. L. Chen, C. L. Lin, K. C. Fan, “Personal authentication using palm-print features” , Pattern Recognition, 36(2) (2003), 2003, 371-381.
[15]D. S. Huang, W. Jia, D. Zhang, “Palmprint verification based principal lines”, Pattern Recognition 41, 2008, 1316-1328. http://dx.doi.org/10.1016/j.patcog.2007.08.016
[16]Y. F. Yao, X. Y. Jing, H. S. Wong, “Face and palmprint feature level fusion for single sample biometrics recognition”, Neurocomputing, 70, 2007, 1582-1586. http://dx.doi.org/10.1016/j.neucom.2006.08.009
[17]College of Engineering, Pune-411005 (An Autonomous Institute of Government of Maharashtra),http://www.coep.org.in/index.php?pid=367.
[18]http://en.wikipedia.org/wiki/Edge_detection
[19]M. Vatsa, R. Singh, A. Noore, “Reducing the False Rejection Rate of Iris Recognition using Textural and Topological Features”, International Journal of Signal Processing, 2006.
[20]R. Wang, B. Bhanu, “Performance prediction for multimodal biometrics”, in Proceedings of the IEEE International Conference on Pattern Recognition, 2006.
[21]L. Hong, Y. Wan and A. I. Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998.