ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Performance Analysis of Security and Accuracy on Palmprint Based Biometric Authentication System

D. Vinod Kumar[1], A. Nagappan[2]

Professor, Department of ECE, VMKV Engineering College, Vinayaka Missions University, Salem, Tamilnadu, India[1]

Principal, VMKV Engineering College, Vinayaka Missions University, Salem, Tamilnadu, India[2]

ABSTRACT: Biometrics is the science of measuring human characteristics for the purpose of authenticating or identifying the identity of an individual. Palmprint one of the human physiological characteristics is gaining attention among researchers as the mean of security. This is because palmprint is rich in unique features. It is universal, unique, permanent, collectible, consistent, comparable, inimitable and tamper-resistant. Palmprint is universal because every individual has palmprint. In this paper, Palmprint biometric is used for personal authentication.

KEYWORDS: Palmprint, Biometrics, Preprocessing, Feature extraction, Matching

I. INTRODUCTION

Authentication, also known as Verification, refers to the problem of confirming or denying a person's claimed identity [5]. In another word, authentication is the verification of the user's identity using the identification items or passwords that the user provided. Authentication involves one-to-one matching with the database or the information stored in the identification items. The result from the authentication matching is either "Yes" or "No", where "Yes" means the individual is the claimed identity and "No" means the individual's claim cannot be verified. Authentication is usually used for logical access or physical access to specific building area.

Identification, also known as Recognition, refers to the problem of establishing a subject's identity either from a set of already known identities (closed identification problem) or otherwise (open identification system) [5]. In another word, identification recognizes the individual by searching the individual's templates with the templates stored in database. Identification involves one-to-many database search. The result from the identification searching is a set of possible matches that either have the highest similarities or exceeded the predefined threshold. Identification is usually used for physical access or law enforcement application.

Human tendency is to use "what they know", for example passwords or pin numbers, for authentication and identification. Passwords can be stolen, shared or guessed by other individual. Thus, password should have a minimum character length, in alphanumeric format, limited access in a time period, different in each application and should frequently be changed. All of these policies make passwords hard to remember. Some people even write their passwords on their keyboards or monitors.

Moreover, human use "what they have", for example identification items, to authenticate and identify an individual's identity. Examples of the identification items are identification card, credits card, smart card and signature stamp. Unauthorized individual can steal and use the identification items for illegal operations. Thus, biometric, "what you are", is introduced to overcome these shortcomings.

Biometrics is the word derived from Greek words "Bio" means life and "Metrics" means to measure. Biometrics is the science of measuring human characteristics for the purpose of authenticating or identifying the identity of an individual. Biometrics System is used for automated recognition of an individual. In information system, in particular,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance [12, 13].

II. PALMPRINT AS BIOMETRICS

Palmprint is one of the human physiological characteristics. It is universal, unique, permanent, collectible, consistent, comparable, inimitable and tamper-resistant. Palmprint is universal because every individual has palmprint. It is unique because every palmprint is different from others. Kong et al. [6] proved that palmprint contains rich genetically unrelated features for classifying identical twins. Palmprint is permanent or inseparable from the individual compared to identification items. Palmprint is easy to collect and consistent because it does not change significantly over time. It can be used to compare digitally with other individuals. Palmprint is hard to imitate due to its size and features rich. Palmprint is tamper resistant because it cannot be changed and hiding it is difficult.

Palmprint biometric system is more acceptable by public than face recognition system. This is because users can gain access anytime they want without being monitored by a surveillance camera. Palmprint is harder to imitate compared to fingerprint due to its size and curvature. It is easier to obtain latent fingerprint, or fingerprint left after touching a surface, than the latent palmprint. Palmprint can achieve higher accuracy than hand geometry biometric system. This is because palmprint features are more distinctive and unique than the hand geometry features. Palmprint biometric system requires cheaper acquisition device than iris biometric system.

III. PALMPRINT BASED BIOMETRIC SYSTEMS

A palmprint authentication system consists of four parts: palmprint image acquisition device, palmprint image pre-processing, feature extraction and feature matching. Palmprint scanner is used to collect palmprint images for enrolment and real time processing. Preprocessing is to find the region of interest from hand image. Feature extraction is to obtain required and effective features from the palmprints. Feature matching is to compare two palmprint features.

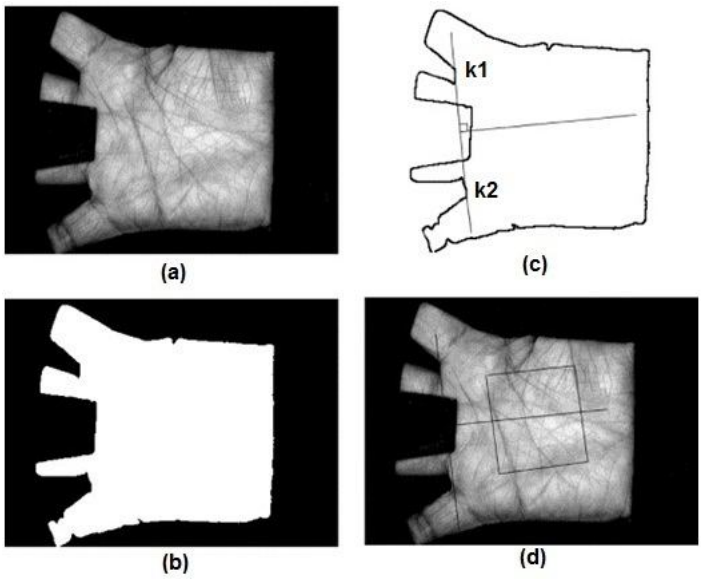


Figure 1: Preprocessing steps (a) Original Image, (b) Binarized image, (c) Key points determination, (d) Region of Interest/Palmprint.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

A. HAND IMAGE ACQUISITION

The first stage of palmprint based biometric system is hand image acquisition. Hand image acquisition is capturing of user's hand images using an image acquisition device. The image acquisition devices can be a scanner, a Charge-Coupled Device camera (CCD camera) or a digital camera. All image acquisition devices take different amount of time in capturing hand image. The digital camera takes less time as compared to scanner in capturing hand image.

B. IMAGE PREPROCESSING STAGE

After the palmprint image is captured, the palmprint region is located from the image. In the image preprocessing stage, three major operations are performed. They are image segmentation, image alignment, palmprint selection and extraction. Image segmentation separates the user palmprint from its background. Image alignment arranges the palmprint image according to a predefined orientation. Palmprint selection and extraction crops out the Region of Interest from palmprint image. The preprocessing includes binarization, detection of key points from the image, rotation of image and image enhancement.

C. PALMPRINT FEATURE EXTRACTION STAGE

Palmprint consists of four types of features. They are geometry features, line features, point features and texture features. After the palm area is extracted, one or several types of features are extracted from the palmprint image. Each of the feature types and some of the palmprint feature extraction methods are explained in the following sub sections.

1. Geometry Features

Palmprint geometry features for adults are relatively similar. Thus, it is incorporated with finger geometry features to form hand geometry biometric system. Figure 2 shows the geometry features of the hand. In Ajay et al., [1] sixteen hand geometry features are extracted. They are four finger-length (from four fingers except thumb), eight finger-width (two finger width readings from four fingers except thumb), palm width, palm length, hand area and hand length are computed.

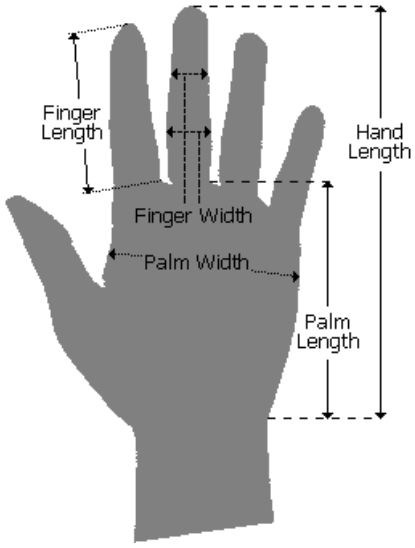


Figure 2: Hand Geometry Features

The hand geometry features [1] have false acceptance rate (FAR) of 5.29 percents and false rejection rate (FRR) of 8.34 percents. It is relatively high because most adult have similar hand geometry features. The palmprint features extracted

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

[1] have FAR of 4.49 percents and 2.04 percents of FRR. Since the palmprint features performed better than the hand geometry features, the palmprint line features decision score are fused with the hand geometry features decision score at the decision level fusion scheme with max rule to achieve better performance than representation level fusion scheme.

2. Line Features

Palmprint line features can be categorized into three types, namely, principal lines, wrinkles and ridges. The principal lines are the major lines that are available in more than 50 percents of the total human population. The three major principal lines are the heart line, the life line and the head line. The coarse lines on the palmprint are called as wrinkles while the fine lines on the palmprint are called as ridges. Figure 3 shows the palmprint line features. Several line based feature extraction methods exist to extract the lines from Palmprint image like Sobel [15], Phase congruency [7, 10], Canny [2]. The challenge in line based feature extraction is to accurately extract the line features, as lines on a Palmprint are unique but are not in specific direction. It is difficult to predict the direction of lines on Palmprint.

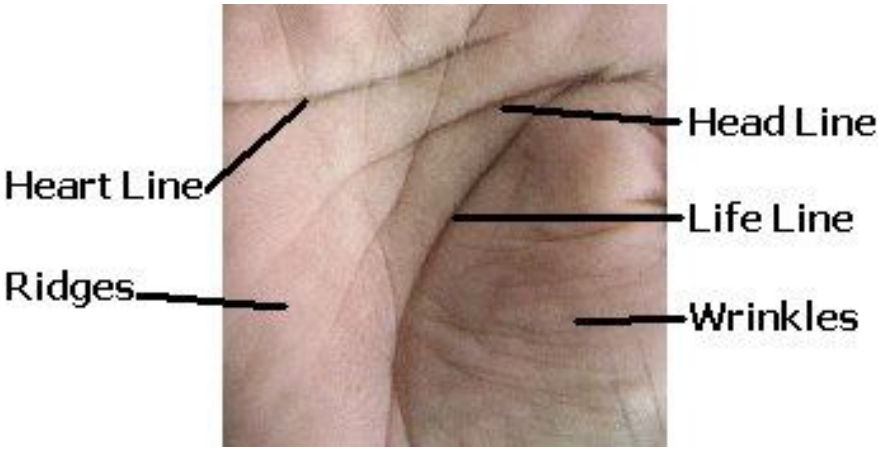
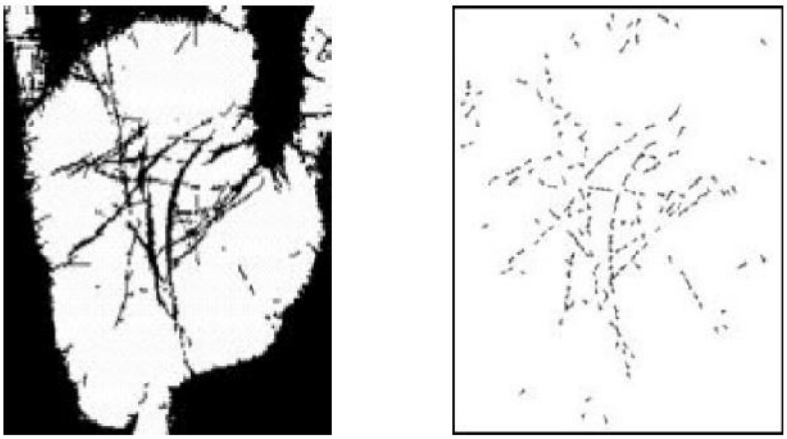


Figure 3: Palmprint Line Features



(a) Binarized hand Image (b) Palmprint Point Features

Figure 4: Extraction of Feature Points [14].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

3. Point Features

The palmprint point features includes datum points, delta points, minutiae points, etc. The palmprint point features can be captured using high-resolution acquisition devices or offline-based palmprint images. In Duta et al. [3], points are extracted that lie on the prominent palm lines. The palmprint image with point features are as shown in Figure 4. Duta et al. [3] method is applicable for use in both online and offline palmprint images.

4. Region Feature

It is also called appearance based approach or subspace based approach. Principal Component Analysis (PCA) [11], Linear Discriminant Analysis (LDA) [14], and Independent Component Analysis (ICA) [4] are some of the methods used to extract palmprint features. The features extracted in these methods are not in the form of images but in the form of coefficients or numerical values.

Lu et al. [9], used Wavelet-based Independent Component Analysis methods for palmprint identification. Two-dimensional Wavelet Transform method is applied on palmprint images and later ICA computation is applied. 98.44 percents accuracy is achieved using this method.

PCA are also known as Karhunen Loeve expansion. It is a classical feature extraction and data representation technique widely used in the area of pattern recognition and computer vision [11]. Tao et al. [11], used two-dimensional Principal Component Analysis, 2D-PCA on the palmprint image. In Wang [4], the 2D-PCA and two-dimensional Linear Discriminant Analysis (2D-LDA) are compared with its 1D-PCA and LDA. Wang [4] applies two-dimensional methods directly on the palmprint image rather than transforming it into one-dimensional image vectors. The two-dimensional method can achieve higher recognition rate instead of one-dimensional method.

D. PALMPRINT FEATURE MATCHING STAGE

After obtaining the feature vectors using various types of feature extraction, the feature vectors will be compared with other feature vectors stored in the palmprint database using similarity measurement. Similarity measurement [8,13] is used to measure the resemblance between two feature vectors. The first feature vector is calculated from the acquired hand images while the second feature vector is one of the feature vectors stored in the palmprint database. If both of the feature vectors are similar, the comparison value will tend to be zero, while the comparison value will tend to be a large number if feature vectors are different. Two types of similarity measurement used in this work are the Hamming Distance and the Euclidean Distance.

IV. PERFORMANCE MEASURE

Performance of biometric system is analysed in terms of accuracy. Usually accuracy is observed when False Acceptance Rate and False rejection Rate are equal for deploying in high secured applications False acceptance ratio has to be very minimal.

A. False Accept Rate (FAR)

The FAR is the frequency that a non-authorized person is accepted as authorized. Because a false acceptance often leads to damages, FAR is generally a security relevant measure. FAR is a non-stationary statistical quantity, which does not only show a personal correlation, it is to be determined for each individual feature.

$$FAR(\lambda) = \frac{\text{Number of False Attempts}}{\text{Total No of Attempts}} \quad (1)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

B. False Reject Rate (FRR)

The FRR is the frequency that an authorized person is rejected access. FRR is generally thought of as a comfort criteria, because a false rejection is most of all annoying. FRR is a non stationary statistical quantity, which does not only show a strong personal correlation, it can even be determined for each individual feature.

$$FRR(\lambda) = \frac{\text{Number of False Reject}}{\text{Total No of Attempts}} \quad (2)$$

These two factors are closely related as both depend on the acceptance threshold which is set to achieve the desired security level. If threshold is set to a very high value then false accept rate of the system may decrease but it may increase false reject ratio and a low threshold may result in decrease in false reject ratio but it may increase the false accept rate. So, the threshold is set according the requirement whether a low FAR or a low FRR is needed.

C. Equal Error Rate (EER)

It is the point where False Accept Rate and False Reject Rate are equal. This is the value where both the FAR and FRR are kept as low as possible at the same time. A low EER value indicates a high accuracy of the system. The relation between FAR, FRR and ERR can be seen in the Figure 5. Aim is to reduce the area obtained by these two curves along the x-axis so it is better choice to set the threshold according to the value of EER but this is not always preferred. Depending upon the application of biometric system, value of the threshold is set. For example, in a high security application like access to secret government documents, a few rejection of genuine user can be tolerated but it is not desired to give access to any unauthorized user. Therefore, in this case, the threshold is set to a high value to minimize the value of FRR. For another example in an ATM, it is better to risk few false accepts rather than the annoyance of the customers if the system rejects authorized users.

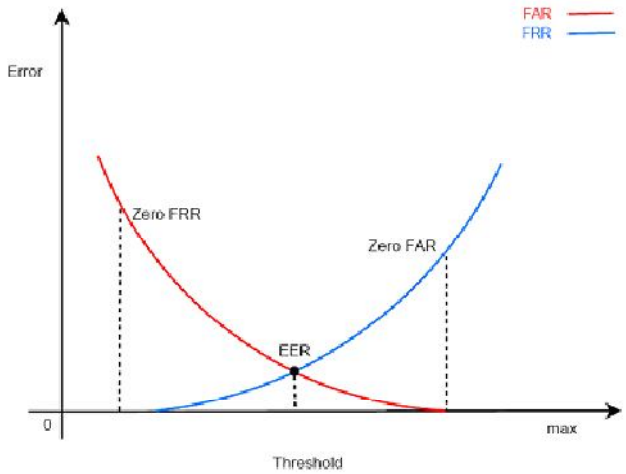


Figure 5: A Typical Performance Curve

E. Receiver Operating Curve (ROC)

For effective comparison of the different biometrics systems, receiver operating characteristics or receiver operating curve (ROC) is used because it is independent of the threshold. In terms of signal theory, ROC is represented by plotting the ratio of true positives Vs true negatives. In context of biometrics, it is the graph of genuine acceptance rate plotted against false acceptance rate as shown in Figure 6. A point in upper left corner in the ROC space represents the ideal ROC curve i.e. 100% genuine acceptance rate and no false acceptance.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

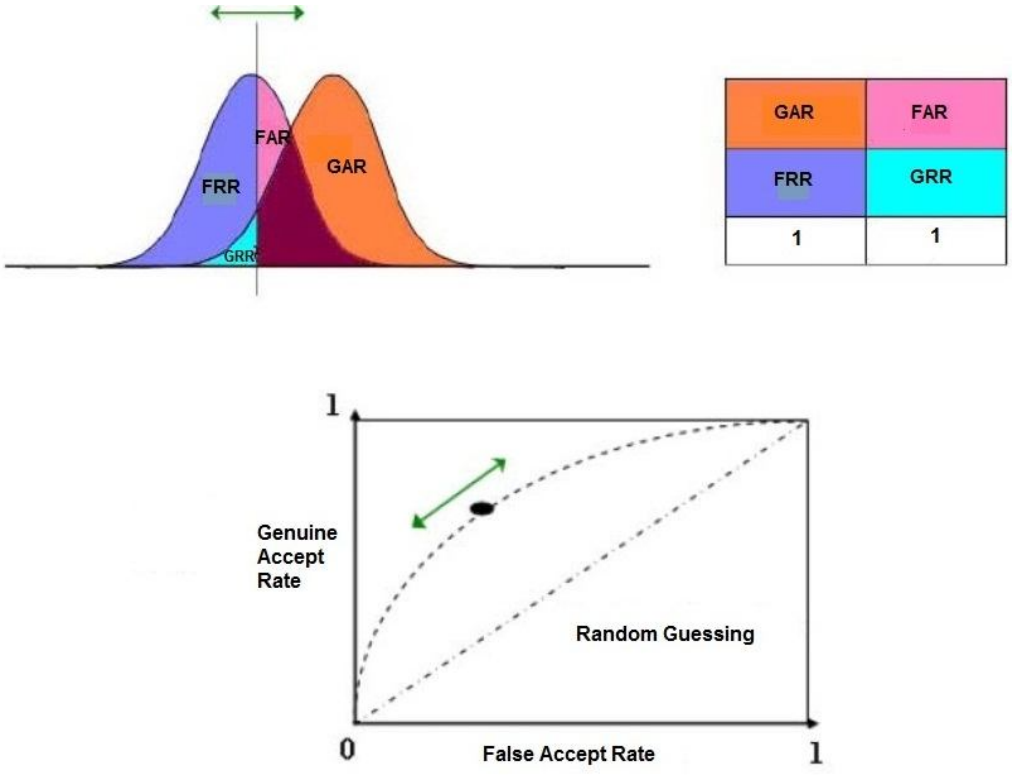


Figure 6: Receiver Operating Characteristics [16].

F. Accuracy

A general term used to describe how accurate a biometric system performs. Biometric accuracy is based on several verifying criteria including the False Accept Rate and False Reject Rate additional biometric system standards.

$$\text{Accuracy (\%)} = 100 - \frac{\text{FAR+FRR}}{100} \quad (3)$$

V. CONCLUSION

The choice of biometric also plays very important role in its application and personal authentication. Biometric to be chosen should possess some basic qualities like, uniqueness, user friendly, easy to adopt, easy to collect, cost involved in acquisition, acquisition devices etc. In this paper, palmprint biometric is analysed for personal authentication. Personal authentication using Palmprint is gaining popularity because of Palmprint being a feature rich and tamper proof biometric. Various characteristics of Palmprint make it better biometric than other biometrics. Performance of biometric system is analysed in terms of accuracy. Usually accuracy is observed when False Acceptance Rate and False rejection Rate are equal for deploying in high secured applications false acceptance ratio has to be very minimal. It is well known fact that increment in FAR leads to less security or not proper authentication because any person can be accepted as genuine. Same applies with FRR, false rejection leads to more time taken for authentication by a genuine person. There has to be a balance between the both FAR and FRR for proper authentication with higher efficiency and better accuracy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

REFERENCES

1. Ajay K., Wong D. C. M., Shen H. C. and Anil K. J., "Personal Verification Using Palmprint and Hand Geometry Biometric", *Proceeding of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Guildford, UK, Pages 668–678, July 2003.
2. Canny J.F., "A computational approach to edge detection", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 8, No. 6, Pages 112–131, April 1986.
3. Duta N., Anil K. J. and Kanti V. M., "Matching of palmprints", Pattern Recognition Letters, Vol. 23, Issue 4, Pages 477-485, February 2002.
4. Guang-Ming Lu, Kuan-Quan Wang and David Zhang, "Wavelet Based Independent Component Analysis for Palmprint Identification", Proceedings of the Third International Conference on Machine Learning and Cybernetics, Vol. 6, Shanghai, Pages 3547-3550, 26-29 August 2004.
5. Jain A., Bolle R. and Pankanti S., "BIOMETRICS: Personal Identification in Networked Society", United States of America: Springer Science+Business Media, Inc., 2006.
6. Kong A. W. K., Zhang D. and Lu G., "A study of identical twins' palmprints for personal verification", Pattern Recognition, Vol. 39, Issue 11, Pages 2149-2156, November 2006.
7. Kovesi P., "Image features from Phase Congruency", Videre J. Comput. Vis. Res., Vol. 1, No. 3, Pages 1–26, Aug 1999.
8. Li W., Zhang D. and Xu Z., "Palmprint Identification by Fourier Transform", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 16, No. 4, Pages 417-432.
9. Lu G. M., Wang K. Q. and Zhang, D. "Wavelet based independent component analysis for palmprint identification", Proceedings of 2004, International Conference on Machine Learning and Cybernetics 2004, Vol. 6, Shanghai, China, Pages 3547-3550, 26-29 August 2004.
10. Struc V. and Pavesic N., "Phase Congruency features for Palmprint verification", IET Signal Processing, Vol. 3, Issue 4, Pages 258-268, July 2008.
11. Tao J. W., Jiang W., Gao Z., Chen S. and Wang C., "Palmprint Recognition Based on 2-Dimension PCA", First International Conference on Innovative Computing, Information and Control 2006, ICICIC'06, Vol. 1, Beijing, China, Pages 326-330, 30-01 August 2006.
12. Vinod Kumar D., Nagappan A., "Study and comparison of various point based feature extraction methods in palmprint authentication system", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 8, Pages 82-89 Dec 2012.
13. Vinod Kumar D, Nagappan A, Jyoti Malik., "Phase Congruency Corner Detection as Biometric Feature", International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 2, No. 1, Pages 179-185, Feb2012
14. Wang M. and Ruan Q. Q., "Palmprint Recognition Based on Two-Dimensional Methods", The 8th International Conference on Signal Processing, Vol. 4, Guilin, China, 16-20 Nov. 2006.
15. Wong K. Y. E., Sainarayanan G. and Ali Chekima, "Palmprint Identification Using Sobel Code", Malaysia-Japan International Symposium on Advanced Technology 2007, Kuala Lumpur, Malaysia, 12-15 November 2007.