INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

FPR a Safe and Secured Biometric in Internet Banking

[1]N.Subbarao, [2]S.M.Riyazoddin, [3]M.Janga Reddy
CMR Institute of Technology, Hyderabad, Andhra Pradesh

Abstract-In this paper, we present an enhanced approach for fingerprint segmentation based on canny edge detection technique and Principal Component Analysis (PCA). The performance of the algorithm has been evaluated in terms of decision error trade-off curves of an overall verification system. Experimental results demonstrate the robustness of the system
.

Keywords: - FPR; Canny Edge detection; PCA; NN.

I. Introduction

Human beings use physical characteristics such as finger, voice, gait, etc. to recognize each other from their birth itself. With new advances in technology, biometrics has become an emerging technology for recognizing individuals using their biological traits. This technology makes use of the fact that each person has specific unique physical traits that are one's characteristics which can't be lost, borrowed or stolen. By using biometrics it is possible to confirm or establish identity based on "who the individual is", rather than by "what the individual possesses" (e.g., an ID card) or "what the individual remembers" (e.g., a password). Passwords determine identity through user knowledge, if someone knows the password, then that person can get access to some restricted areas or resources of a certain system. The drawback is that a password has nothing to do with the actual person using it. Passwords can be stolen, and users can give their passwords to others, resulting in systems that are vulnerable to unauthorized people. There is no foolproof way to make password-protected systems safe from unauthorized users. There is no way for password-based systems to determine user identity beyond doubt. The initial intent of such schemes is, however, to ensure that the provided services are accessed only by an authorized user, and not anyone else. Several systems require authenticating a person before giving access to their resources.

Biometrics has been long known to recognize persons based on their physical and behavioral characteristics. Examples of different biometric systems include fingerprint recognition, finger recognition, iris recognition, retina recognition, hand geometry, voice recognition, signature recognition, etc. Finger recognition in particular, has received a considerable attention in recent years both from the industry and the research communities. The real-life challenge here is the identification of individuals in everyday settings, such as offices or living-rooms. The dynamic, noisy data involved in this type of task is very different to that used in typical computer vision research, where specific constraints are used to limit variations. Historically, such limitations have been essential in order to limit the computational burden required to process, store and analyze visual data. However, enormous improvements in computers in terms of speed of processing and size of storage media, accompanied by progress in statistical techniques, is making it possible to realize such complex systems.

Applications

1. **Commercial** applications such as computer network login, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning, etc.,
2. **Government** applications such as national ID card, correctional facilities, driver's license, social security, welfare-disbursement, border control, passport control, etc., and
3. **Forensic applications** such as corpse identification, criminal investigation, terrorist identification, parenthood determination, missing children, etc.

Finger recognition has received considerable interest as a widely accepted biometric, because of the ease in collecting finger images of persons. Finger recognition is being used in various applications like crowd surveillance, criminal identification, and criminal record, access to entry etc. Finger recognition developers, however, have to consider a number of major issues before finger recognition systems become standard systems. The requirements for a useful, commercial finger recognition and identity logging system, for small groups of known individuals in busy unconstrained environments, (such as domestic living rooms or offices) can be split into several groups:

1. General requirements that need to be satisfied by all components of the system,
2. Acquisitions requirements concerned with monitoring and extraction,
3. Finger recognition requirements for the recognition stage, and
4. Identity requirements which are concerned with how the recognition output is used.

II. Literature Survey

Neeta et.al.(2010) proposed alignment-based elastic matching algorithm is capable of finding the correspondences between minutiae without resorting to exhaustive research. In this work is based on the concept of segmentation using Morphological operations, minutia marking by especially considering the triple branch counting, minutia unification by decomposing a branch into three terminations and matching in the unified x-y coordinate system. After a 2-step transformation in order to increase the precision of the minutia localization process and elimination of spurious minutia with higher accuracy. There is a scope of further improvement in terms of efficiency and accuracy which can be achieved by improving the hardware to capture the image or by improving the image enhancement techniques. So that the input image to the thinning stage could be made better this could improve the future stages and the final outcome.

Shashi et.al.(2010) proposed Fingerprint Verification based on fusion of Minutiae and Ridges using Strength Factors in which the minutiae and ridge methods are combined. In FVMRSF method in the pre-processing stage the Fingerprint is Binarized and Thinned. The Minutiae Matching Score is determined using Block Filter and Ridge matching score is estimated using Hough Transform. The strength factors *Alpha (α)* and *Beta (β)* are used to generate Hybrid matching score for matching of fingerprints. Then the minutiae and the ridge parameters are fused using the Strength Factors to improve the performance. But the performance could have been improved by adding the wavelet transform as it helps in compact fingerprint recognition.

Kazuya et.al.(2010) proposed a method to select pixels used for camera identification according to the texture complexity to improve the accuracy of camera identification. In this method camera identification accuracy is reduced by the image processing engine such as motion blur correction, contrast enhancement, and noise reduction. Also suggested a method for improving the identification accuracy by the image restoration method. In this paper, we have shown the improved camera identification method. The identification accuracy is improved by selecting pixels used for correlation calculation according to the texture complexity. And the identification accuracy is also improved by the image restoration which restores the PNU noise varied by the image processing engine. But still there is big concern to have a systematic method to correctly estimate the restoration function. is left to the future work.

Miroslav et.al.(2010) developed a fast algorithm for finding if a given fingerprint already resides in the database and for determining whether a given image was taken by a camera whose fingerprint is in the database. Here they realized that in worst-case complexity is still proportional to the database size but does not depend on the sensor resolution. The algorithm works by extracting a digest of the query fingerprint formed by the most extreme 10,000 fingerprint values and then approximately matches their positions with the positions of pixels in the digests of all database fingerprints. The algorithm requires a sparse data structure that needs to be updated with every new fingerprint included in the database. The algorithm is designed to make sure that the probability of a match and false alarm for the fast search is identical to the corresponding error probabilities of the direct brute-force search. After that they also claim that the fast algorithm does not rely on any structure or special properties of the fingerprints in the database. Hence it can be utilized in any application where a database contains *n*-dimensional elements and *n* is a fixed large number. The only requirement is that the elements consist of real numbers or integers from a large range. But integers from a small range would lead to ill-defined ranks. An extreme case when the rank correlation and consequently, the fast search algorithm cannot be used, are binary vectors.

Sara et.al. (2010) suggested a reliable authentication mechanism which is not dependent on a series of characters, but rather on a technology that is unique and only possessed by the individual called Finger ID. This technique is aims to promote the convenience for the internet user since he/she will not have to remember multiple passwords for a multiple number of accounts. The accessibility, usability and security guidelines have been tested on the Fingered website and browser by means of numerous activities and found that the web accounts a more secure, accessible and usable one. But this increases the cost of the system.

Chandra et.al. (2011) proposed a method how to get a noise-free fingerprint image they proposed the finger print classifications, characteristics and pre-processing techniques. Where they applied the histogram on 256 gray scale finger print image with the default threshold value; then the histogram-equalized image is obtained. Next, histogram-equalized image is given under the binarization process. Finally the binarized fingerprint image is filtered with the implementation of the Median filtering technique in order to produce the noise free image. The comparison of the median filtered image with the original noisy image shows the depth of the noise spread in the original image. Their experimental result shows the noise rate which was eliminated in the input fingerprint image and quality of the filtered image using the Statistical – Correlation tool.

Bay ram et.al. (2012) proposed a method to represent sensor fingerprints in binary-quantized form as the large size and random nature of sensor fingerprints makes them inconvenient to store. In their work they analyzed the change in the performance caused due to loss of information due to binarization. Hence, binarization of sensor fingerprints is an effective method that offers considerable storage gain and complexity reduction without a significant reduction in fingerprint matching accuracy. But this will not be effective for noisy or information lost fingerprints leading to the misclassification.

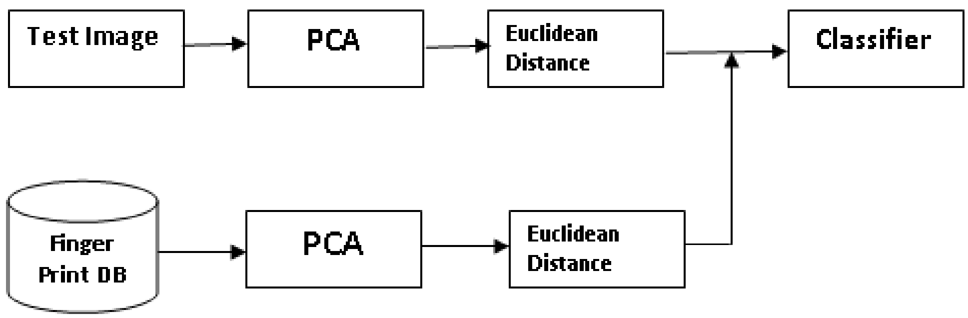
Yoon et.al.(2012) proposed an algorithm based on the features extracted from the orientation field and minutiae satisfies the three essential requirements for alteration detection algorithm:1) fast operational time, 2) high true positive rate at low false positive rate, and 3) ease of integration into AFIS. The proposed algorithm and the NFIQ criterion were tested on a large public domain fingerprint database (NIST SD14) as natural fingerprints and an altered fingerprint database provided by a law enforcement agency.

Romany et.al.(2012) proposed a new technique to fingerprint recognition based a window that contain core point this window will be input ANN system to be model. This method is adaptive singular point detection method that increases the accuracy of the algorithm. This robust method for locating the core point of a fingerprint. The global threshold reduces chances of falsely locating a core point due to presence of discontinuities like scars or wrinkles, which may occur in the existing processes. Since the detection is based on a global threshold, the method only gives us an approximate location of the core point. For exact detection of the core point, we use the geometry of region technique over a smaller search window using ANN. They show that as image size window that contain core point in center decreases the system performance also decrease but not the size but also the number of minutiae.

III .Fingerprint Classification Algorithm

In this section, we introduce a basic version of the algorithm for fingerprint classifying (FPC), which has as preliminary input a database of fingerprint images (Train Database).A test fingerprint image (Test Database) is then entered, and the algorithm returns whether or not the test image is in the stored fingerprint bank. The steps followed in this process of classification are

a. Store previously the fingerprint database denoted by
b. Build the image space by using the PCA technique;
c: Acquire and project the fingerprint testing image into image space;
d. Define a criterion for classifying the (*IX*);
e. Decide whether *the test image belongs* or not to the stored base.



1. Building Image Space Using PCA

Principal Component Analysis (PCA) [3] is a statistical technique used to transform dimensions of the space from a higher one to a lower. It helps to find patterns in data. It uses standard deviation, mean value, variance, covariance and matrix algebra concepts from statistics and mathematics. As image is a high dimension data. Work with images is high source demanding and complex. All the image data is represented in the form of long vectors. It has two methods covariance and correlation.

Let we have a data set S= {s1, s2, s3, Sn} then mean denoted by SM will be.

$$SM = \sum S_i / n \qquad i = 1,2,3,.....n \qquad (2.1)$$

Standard deviation SD will be as

$$SD = \sqrt{(S_i - SM)^2 / n - 1} \qquad i = 1,2,3,.....n \; (2.2)$$

Variance is very similar to the standard deviation and the formula for the data set S can be calculated as

$$Var(S) = \Sigma (S_i - SM)^2 / n - 1 \; i = 1,2,3,.....n \qquad (2.3)$$

Covariance another term is used in statistics. Standard Deviation and Variance deal with one dimensional data where as the Covariance is similar measures between 2 dimensional data. Let consider S and L two data sets then the covariance will be as.

$$Cov(S) = \sum (S_i - SM)(L - LM) / n - 1 \; i = 1,2,3.....n \qquad (2.4)$$

If covariance is calculated for one dimensional data then it will be equal to the variance [27].

Principal Component Analysis is defined as a dimensionality reduction technique which transforms a random vector say x, say of size *n*, to a random vector of y, say of size *k* where *k* is chosen smaller than *n*. This transformation is defined below:

2. Calculating the Eigen Values and Eigen Vectors

Let e_i and $\lambda_i = 1,2,......n$ be the eigenvectors and corresponding Eigen values of the covariance matrix C_X of the random vector x (where λ1, λ2 ……λn). Since we know that x takes real values (e.g. image data). The covariance matrix C_X is real and symmetric. It follows that the Eigen values of C_X are real. A transformation matrix is formed whose columns are the eigenvectors of C_X which is given by:

$$[e_1, e_2, ...e_n] \quad (2.5)$$

Principal Component Analysis is defined by a transformation obtained as follows:

$$y = W^T (x - mx) \quad (2.6)$$

The transformation given by equation 2.6 has several important properties.

The first property we examine here is the covariance matrix of the random vector y. This is defined as

$$C_y = E[(y - my)(y - my)^T] \quad (2.7)$$

Where m*y* is equal to zero vector 0, since:

$$my = E[y]$$

$$= E[W^T (x - mx)]$$

$$= W^T E[x] - W^T m$$

$$= 0 \quad (2.8)$$

By substituting 2.6 and 2.8 into 2.7 gives the following expression for C_Y in terms of C_X

$$C_y = E(W^T x - W^T mx)(W^T x - W^T mx)^T$$

$$= E[W^T (x - mx)(x - mx)^T]W$$

$$= W^T E[(x - mx)(x - mx)^T]W$$

$$= W^T C_X W \quad (2.9)$$

It is shown by Lawley and Maxwell [30] that C_Y is a diagonal matrix with elements equal to the Eigen values of C_X that is λ

$$C_y = \begin{bmatrix} \lambda_1 & & & & 0 \\ & \lambda_2 & & & \\ & & \cdots & & \\ & & & \ddots & \\ 0 & & & & \lambda_n \end{bmatrix}$$

This is an important property, since the terms other than the main diagonal are 0; the elements of y are uncorrelated. In addition, each Eigen value λ_i is equal to the variance of the i^{th} element of y.

The second important property deals with reconstruction of random vector x from random vector y. Since we consider x whose observations are real, the covariance matrix C_X is real. It follows that the set of eigenvectors of C_X form an orthonormal basis $W^{-1} = W^T$ Using this property, x can be reconstructed from y by using the relation:

$$x = W_y + m_x \tag{2.10}$$

Suppose, however, that instead of using all eigenvectors of C_X, we construct W from the first k eigenvectors corresponding to the largest Eigen values. The y vector will then be k dimensional and the reconstruction giving by equation follows:

$$\hat{X} = W_k y + mx \tag{2.11}$$

$\hat{X}$ Represents an approximation of x obtained from the transformation matrix W composed of first k eigenvectors of C_X.

3. Euclidean Distance for FPC

The mean square error between x and $\hat{X}$ is given by the expression [30]:

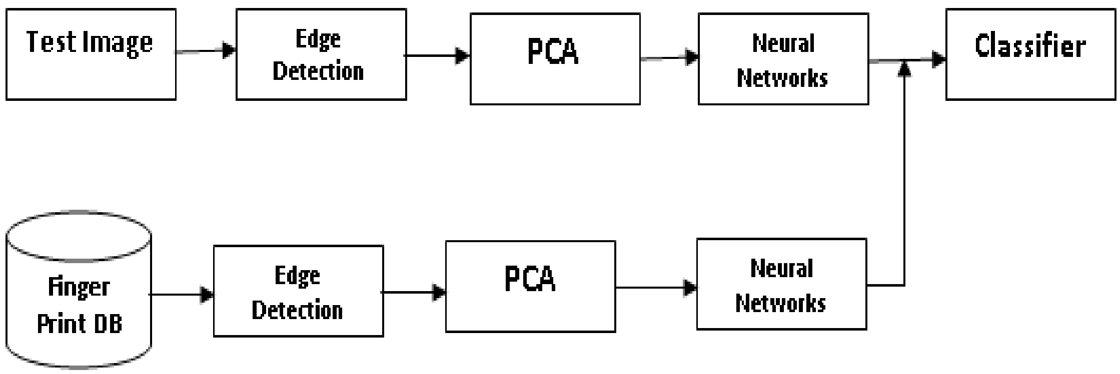
$$e_{ms} = \sum_{j=1}^{n} \lambda_j - \sum_{j=1}^{k} \lambda_i$$

$$= \sum_{j=k+1}^{n} \lambda_j \tag{2.12}$$

The first line of equation 12 indicated that the error is zero, if k = n. additionally since the ¸j's decrease monotonically, equation 12 also shows that the error can be minimized by selecting the k eigenvectors associated with the largest Eigen values. Thus PCA is optimal in the sense that it minimizes the mean square error between the vector x and its approximation $\hat{x}$.

Thus Recognition of images using PCA takes three basic steps. The transformation matrix is first created using the training images. Next, the training images are projected onto the matrix columns. Finally, the test images are identified by projecting these into the subspace and comparing them to the trained images in the subspace domain. But finding the finger discriminating features like minutia, valleys or ridges is very difficult task using PCA whose basic task is dimension reduction and also used as a classifier. To mitigate this problem a new method is proposed where the finger features are located first with help of canny edge detection technique and then classification is done using PCA.

Iv. Proposed Method



Depending on the noise level, no clear separation can be found, thereby restricting the use of the Euclidean distance. In this section we show that the use of type canny edge or Sobel edge detection [10] can help mitigating the influence of noise. The edge detection is applied at the moment that the image is inserted into the base and when the test image is acquired. With the inclusion of edge detection component the complete sequence of the algorithm is:
Step 1: Store previously the fingerprint database
Step2: Apply Edge Detections:
Step3: Build the image space by using the PCA
Step4: Define the criteria for classification using neural networks.
Step5: Acquire, apply edge detection and project the fingerprint testing image into image space
Step6: Decide whether Test Image belongs or not to the stored base.
We apply "Canny" edge detection component of the

Canny edge detection algorithm

The purpose of edge detection in general is to significantly reduce the amount of data in an image, while preserving the structural properties to be used for further image processing. The aim of John F. Canny [ref1, ref2] was to develop an algorithm that is optimal with regards to the following criteria:
1. **Detection**: The probability of detecting real edge points should be maximized while the Probability of falsely detecting non-edge points should be minimized. This corresponds to Maximizing the signal-to-noise ratio.
2. **Localization**: The detected edges should be as close as possible to the real edges.

3. **Number of responses**: One real edge should not result in more than one detected edge
Canny's Edge Detector is optimal for a certain class of edges (known as step edges).

STEP I: Noise reduction by smoothing

Noise contained in image is smoothed by convolving the input image I (i, j) with Gaussian filter G. Mathematically, the smooth resultant image is given by

$$F(i, j) = G * I(i, j)$$

Prewitt operators are simpler to operator as compared to sobel operator but more sensitive to noise in comparison with sobel operator.

STEP II: Finding gradients

In this step we detect the edges where the change in greyscale intensity is maximum. Required areas are determined with the help of gradient of images. Sobel operator is used to determine the gradient at each pixel of smoothened image. Sobel operators in i and j directions are given as

$$D_i = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} \text{ And } D_j = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

These sobel masks are convolved with smoothed image and giving gradients in i and j directions.

$$G_i = D_i * F(i, j) \text{ And } G_j = D_j * F(i, j)$$

Therefore edge strength or magnitude of gradient of a pixel is given by

$$G = \sqrt{G_i^2 + G_j^2}$$

The direction of gradient is given by

$$\theta = \arctan\left(\frac{G_j}{G_i}\right)$$

G_i And G_j are the gradients in the i- and j-directions respectively.

STEP III: Non maximum suppressions:

Non maximum suppression is carried out to reserves all local maxima in the gradient image, and deleting everything else this results in thin edges. For a pixel M (i, j):

Firstly round the gradient direction θ nearest45°, then compare the gradient magnitude of the pixels in positive and negative gradient directions i.e. If gradient direction is east then compare with gradient of the pixels in east and west directions say E (i, j) and W (i, j)respectively.

 If the edge strength of pixel M (i, j) is largest than that of E (i, j) and W (i, j), then preserve the value of gradient and mark M (i, j) as edge pixel, if not then suppress or remove.

STEP IV: Hysteresis thresholding:

The output of non-maxima suppression still contains the local maxima created by noise. Instead choosing a single threshold, for avoiding the problem of streaking two thresholds t_{high} and t_{low} are used.

For a pixel M (i, j) having gradient magnitude G following conditions exists to detect pixel as Edge:

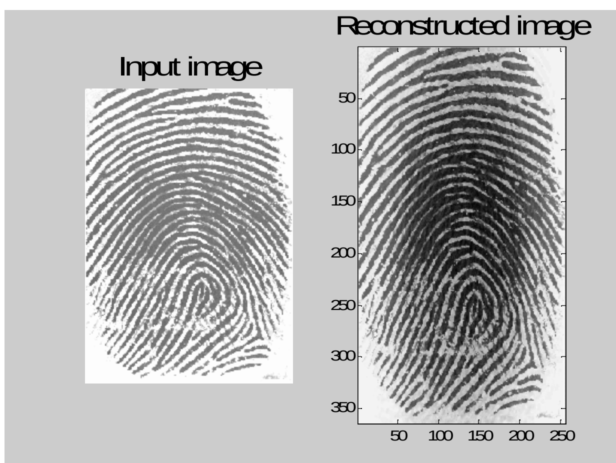
- If G $< t_{low}$ than discard the edge.
- If G > than t_{high} keep the edge.
- If t_{low} < G < and t_{high} and any of its neighbors in a 3 ×3 region around it have gradient magnitudes greater than t_{high} keep the edge.
- If none of pixel (x, y)'s neighbors have high gradient magnitudes but at least one falls between t_{low} and t_{high} search the 5 × 5 region to see if any of these pixels have a

Magnitude greater than thigh. If so, keep the edge.

- Else, discard the edge.

Result Analysis

The proposed system is analyzed using sample Caltech fingerprint database. In this method the total number of 21Train Database and 5 Test Database images are used.



Method	Training Samples	Test Samples	True Classification	False Classification	Accuracy (%)

	s				
PCA	**50**	**31**	**25**	**6**	**80.64**
PCA+canny	**50**	**31**	**28**	**3**	**90.32**

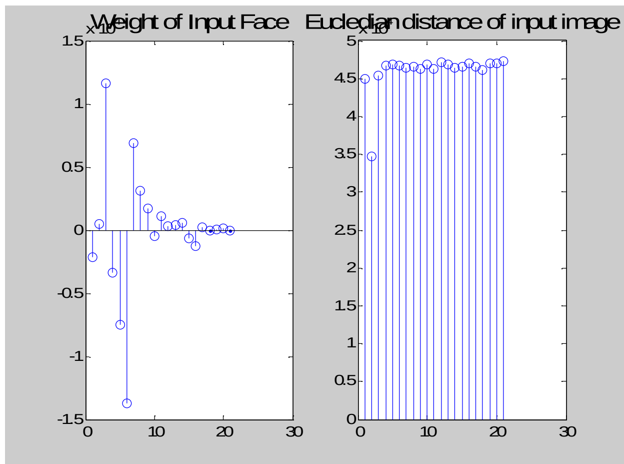


Fig.4. Histogram Analysis of Reconstruction

Further this method is extended to improve the recognition accuracy by using multilayer perceptron neural network.

a. RBF Neural Network – Classifier

An RBF neural network as shown in figure 2 with a mapping $\Re^T \rightarrow \Re^S$ .Let $P \in \Re^T$ be the input vector and $C_i \in \Re^T$ $(1 \le i \le u)$ be the prototype of the input vector. The output of each RBF unit is as follows: [3].

$$R_i(P) = R_i(\|P - C_i\|) \qquad i = 1,2,....u$$

Where (||-||) indicates the Euclidean norm on the input space. Usually, the Gaussian function is preferred among all possible radial basis functions due to the fact that it is factorizable. Hence

$$R_i(P) = \exp\left[-\frac{\|P - C_i\|^2}{\sigma_i^2}\right]$$

Where σ_i^2 is the width of the ith RBF unit.The jth output $y_i(P)$ of an RBF neural network is

$$y_i(P) = \sum_{i=1}^{u} R_j(P) \times W(i, j)$$

(2.19)

where R_o =1, w(j,i) is the weight or strength of the i th receptive field to the j th output and w(j,0) is the bias of the j th output. In order to reduce the network complexity, the bias is not considered in the following analysis. We can see from (2.17) and (2.18) that the outputs of an RBF neural classifier are characterized by a linear discriminant function. They generate linear decision boundaries (hyperplanes) in the output space. Consequently, the performance of an RBF neural classifier strongly depends on the separability of classes in the k-dimensional space generated by the nonlinear transformation carried out by the u RBF units.

Method	**Training Samples**	**Test Samples**	**True Classification**	**False Classification**	**Accuracy (%)**
PCA	**50**	**31**	**25**	**6**	**80.64**
PCA+canny	**50**	**31**	**28**	**3**	**90.32**
PCA+Canny+ NN	**50**	**31**	**29**	**2**	**93.54**

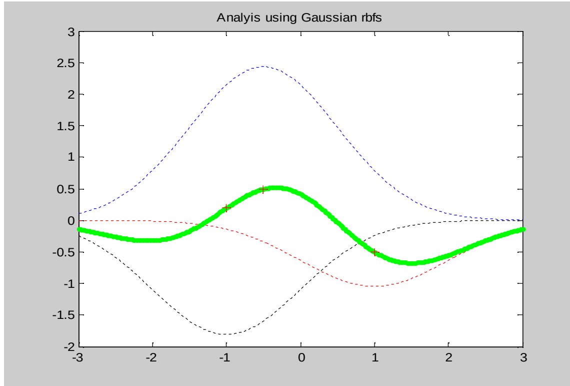


Fig.5. RBF Analysis using Gaussian Function

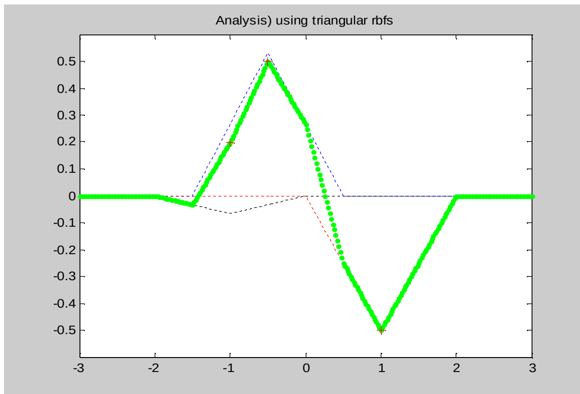


Fig.6. RBF Analysis using Triangular RBF Function

V. Conclusion

We have presented an enhanced Canny edge detection based fingerprint segmentation method and PCA is used for accurate classification and authentication of the individual for safe and secured internet banking. The performances of the proposed and existing algorithms have been evaluated in terms of True classifications using a database with medium-high quality finger print images .Experimental results show that the proposed enhanced algorithm robust than the existing system.

Reference

[1] Ernande F. Melo, H. M. de Oliveira, A Fingerprint-based Access Control using Principal Component Analysis and Edge Detection, vol.30,N.9, 2011.

[2] N. Yager and A. Amin, Fingerprint Classification: a Review, *Pattern AnalApplic*, vol.7: pp.77-93, 2004.

[3] M.M.S. Chong, T.H. Ngee, L. Jun and R K. L. Gay, Geometric Framework for Fingerprint Image Classification, *Pattern Recognition*, vol.30,N.9, pp.1475-1488, 1997.

[4]Neeta Murmuand AbhaOtti by “Fingerprint Recognition “in Department of Electrical Engineering National Institute of Technology Rourkela-2010.

[5] Shashi Kumar D. R, R. K. Chhotaray, K.B. Raja, SabyasachiPattanaik by "Fingerprint Verification based on Fusion of Minutiae and Ridges using Strength Factors" in *International Journal of Computer Applications (0975 – 8887) Volume 4 – No.1, July 2010.*

[6] Kazuya Matsushita and Hitoshi Kitazawa by "An Improved Camera Identification Method based on the Texture Complexity and the Image Restoration" in International Journal of Hybrid Information Technology Vol.3, No.1, January, 2010 .

[7] M. Goljan, J. J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints," in *Proc. SPIE-IS&T Conf. Electronic Imaging: Media Forensics and Security XII*, 2010, vol. 7541, p. 754108.

[8] Sara JezaAlotaibi, Mike Wald, David Argles by "Using Fingerprint Recognition in a New Security Model for Accessing Distributed Systems" in International Journal of Intelligent Computing Research (IJICR), Volume 1, Issue 4, December 2010.

[9] Dr. E. Chandra, K.Kanagalakshmi,"Noise Elimination in Fingerprint Image Using Median Filter", Int. J. Advanced Networking and Applications Volume. 02, Issue. 06, pg. 950-955, 2011

[10] Sevinç Bay ram, HüsrevTahaSencar, and NasirMemon by "Efficient Sensor Fingerprint Matching through Fingerprint Binarization" in IEEE Transactions on Information Forensics and Security, Vol. 7, No. 4, August 2012.

[11] Soweon Yoon, JianjiangFeng, Anil K. Jain, "Altered Fingerprints: Analysis and Detection", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.34, NO. 3, March 2012 Pp.451-464

[12] Romany F. Mansour, AbdulSamad, A. Marghilani by "A New Technique to Fingerprint Recognition Based on Partial Window" in Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol 3, No.10, 2012.

[13] Sachin J Katharki, Shashidhara H. R. and A.R.Aswath, Digital Design of Fingerprint Recognition Based on Eigen Vector Transform, ISBN: 978-93-81693-82-7.

[14] Nicolas Morizet, FrédéricAmiel, InsafDrisHamed, Thomas Ea, A Comparative Implementation of PCA Face Recognition Algorithm,ICECS'07.

[15] Lindsay I Smith A tutorial on Principal Components Analysis, February 26, 2002.

[16]. Singh, B. and Malhotra, P. (2004) Adoption of Internet banking: An empirical investigation of Indian banking Sector. Journal of Internet Banking and Commerce, 9 (2).

[17] TerjeKristensen,Two Different Regimes of Fingerprint Identification – a Comparison, American Journal of Computational and Applied Mathematics 2012, 2(2): 1-9 DOI: 10.5923/j.ajcam.20120202.01.

[18] Canny Edge Detection, 09gr820, March 23, 2009.

[19] John Canny. A computational approach to edge detection. Pattern Analysis and Machine Intelligence, IEEE Transactions on, PAMI-8(6):679–698, Nov. 1986.

[20] Fingerprint Recognition Using Minutiae-Based Features by ChiragDadlani, Arun Kumar Passi, Herman Sahota, MitinKrishan Kumar, pattern recognition 2006.

[21]http://www.cs.washington.edu/education/courses/cse576/09sp/projects/project3/artifact/tingyou/proj3/index.html

[22]http://whatevericode.wordpress.com/2008/11/06/principal-component-analysis-matlab-code/

[23]http://www.pages.drexel.edu/~sis26/Eigencode.htm

[24] image.online-convert.com/convert-to-tiff

[25]http://dasl.mem.drexel.edu/alumni/bGreen/www.pages.drexel.edu/_weg22/can_tut.html