Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multi-Model Biometrics system for Person Identity Verification

Shekhar Singh
Assistant Professor
Department of Computer Science & Engineering
Panipat Institute of Engineering and Technology, Samalkha, Panipat, India

ABSTRACT: ***Multi-model Biometrics system for person identity verification have mainly two authentication process, face identification and signature verification. A set of Fisher scores is calculated for face image through partial derivative analysis of the parameters estimated in each HMM. These Fisher scores are further combined with some traditional features such as log-likelihood, 2-D DCT and appearance based features to form feature vectors that exploit the strengths of both local and holistic features of human face. Neural Network is then applied to analyze these feature vectors for face recognition. Experimental results on a public available face database are provided to demonstrate the viability of this method. The signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. Handwritten signatures are considered as the most natural method of authenticating a person's identity. The method presented in this paper consists of image prepossessing, geometric feature extraction, neural network training with extracted features and verification. A verification stage includes applying the extracted features of test signature to a trained neural network which will classify it as a genuine or forged. In this paper, off-line signature recognition & verification using neural network is proposed, where the signature is captured and presented to the user in an image format. Signatures are verified based on parameters extracted from the signature using various image processing techniques. This work has been tested and found suitable for its purpose.***

Keywords: ***Face recognition, HMM, Fisher scores, 2-D DCT, Facial Expression, Biometrics, BPN algorithm, Neural Networks, Off-line Signature Recognition and Verification.***

I. INTRODUCTION

A problem of personal verification and identification is an actively growing area of research. The methods are numerous and are based on different personal characteristics; voice, lip movement, hand geometry, face, odor, gait, iris, retina and fingerprint are the most commonly used authentication methods. All these psychological and behavioral characteristics are called biometrics. The driving force of the progress in this field is above all, the growing role of the internet and electronic transfers in modern society. Therefore considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems [9]. The biometrics have a significant advantage over traditional authentication techniques due to the fact that biometric characteristics of the individual are not easily transferable are unique of every person and cannot be lost, stolen or broken.

One of the most popular appearance based methods [1–3] for face recognition developed in recent years is the Fisher face method. The Fisher face method performs LDA of feature vectors obtained as one-dimensional representation of a face image and retrieves the identity of person based on the nearest-neighbor classification criterion in the LDA space. This method is insensitive to large variation in lighting direction and facial expression [2]. Meanwhile, statistical model based methods such as hidden Markov model have also been proposed for face recognition problems [4–8]. This method uses HMM to describe the statistical distribution of observation vector sequences which are generated from small sub-image blocks of face image. Classification is usually based on Bayesian decision rule, e.g., maximum a posteriori criterion. Comparing with appearance based methods; HMM methods focus mainly on local characteristics of human faces. These methods have the flexibility to incorporate information from different instances of faces at different scales and orientations [5]. However, in these existing statistical model based methods, only the calculated likelihood of a particular observation on each established model is used as the measure of closeness of the observation towards the corresponding class. In this work, we present a new feature vector generation scheme from HMMs. The scheme generates feature vectors which represent the influence of the model parameters of several competing HMMs on the generation of a particular observation vector sequence. Similar methods were proposed and used in biosequence analysis, speech recognition and speaker identification [9, 14, and 15]. Unlike previous schemes which are inherently two-class problem oriented, the proposed scheme in this work is multi-class problem oriented and the resulting feature vectors appear to be more effective. We also explore the strengths of both Fisher face method, 2-D DCT and HMM method by combining

appearance based features and statistical model based features together to form new feature vectors, which may have greater discriminative power over those used separately.

The hand written signature is regarded as the primary means of identifying the signer of a written document based on the implicit assumption that a person's normal signature changes slowly and is very difficult to erase, alter or forge without detection. The handwritten signature is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning, face recognition and retinal vascular pattern screening. It is easier for people to migrate from using the popular pen-and-paper signature to one where the handwritten signature is captured and verified electronically. The signature of a person is an important biometric attribute of a human being and is used for authorization purpose. Various approaches are possible for signature recognition with a lot of scope of research. Here, we deal with an off-line signature recognition technique. Signatures are composed of special characters and flourishes and therefore most of the time they can be unreadable. Also intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together [6]. Signature recognition is the process of verifying the writer's identity by checking the signature against samples kept in the database. The result of this process is usually between 0 and 1 which represents a fit ratio (1 for match and 0 for mismatch).

II. FACE RECOGNITION

The new technique uses a neural network for face recognition. The proposed recognition technique consists of two phases: training and testing, which are described separately below.

1.1 Processing of face image

The features of facial images used in recognition must not be influenced by the appearance of any individual human. Therefore, pre-processing of the face images is needed in order to extract some information that is required by the recognition task and shared by all the face images of the same category. Therefore, the recognition task will become easier due to the use of difference images. The images are incorporated into the computer where they are converted into gray images of size M×N. Then, horizontal and vertical projections for the top two sub blocks are performed. The minimum points of the projection curves will be the candidates for the eye positions. To get stable results, DFT is used to smooth the curves. Clearly, the eye positions are correctly detected and determined. Next, the mouth is detected using similar projections applied to the bottom block. To obtain reliable mouth positions, compensation of white teeth is introduced before the projections are performed, by setting a proper empirical threshold such that the white teeth are detected and blackened. Based on the eye and mouth positions detected, the image is rotated and scaled if needed, and finally an image of size 256×256 is produced.

1.2 Face image compression using 2-D DCT

To facilitate the recognition, we need to compress the difference image to reduce data in a proper way, without losing the key features that play important role in the recognition task. The 2-D DCT used frequently in image compression is a powerful tool for this purpose. The 2-D DCT can reduce the number of data significantly by transforming an image into the frequency domain where the lower frequencies present relatively large magnitudes while the higher frequencies indicate much smaller magnitudes. That is to say, the higher frequency components can be ignored without damaging the key characteristics of the original difference image, as far as the face recognition is concerned. The size of the face images is M×N. The 2-D DCT coefficients of a square block with size L1×L2 of the lower frequencies hold much of the information on the face and are arranged as an input vector to the neural network for training or testing purposes.

1.3 Neural Network Training for Face Identification

The dimension of the input vector of the neural network is M ×N. One-hidden-layer neural network are considered in this work, which are trained by the program provided in the MATLAB toolbox. There is only one output "logsig" node in the neural network and the threshold for expression classification is set to 0.6. "logsig" is also the activation function for all the hidden units. The training parameters, such as the learning rate, number of epochs, etc. are properly selected. The input vector dimension, the number of hidden units, the initial weights, and the training parameters are systematically changed each time neural network is trained in order to achieve higher mean recognition rate of the face.

Neural network are constructed for specified pair of 2-D DCT block. NN trained present fast convergence and the training process terminated within 500 epochs, with the summed square error (SSE) reaching the pre-specified goal or occasionally saturated. Extensive simulations revealed that the SSE goal does not affect the performance of the neural network obtained in terms of training recognition rate if set lower than 0.6. To achieve good performance, one needs to set the block size of 2-D DCT larger than 16 and the number of hidden units larger than 8. The mean testing recognition rate for database is as high as 98.5%, which presents the highest record among all the previous techniques for the same database. Obviously, the proposed technique presents, on the whole, improved recognition capabilities in comparison with those previous techniques.

III. EXPERIMENT RESULTS OF FACE RECOGNITION

The proposed network was trained with feature vector data cases. When the training process is completed for the training data, the last weights of the network were saved to be ready for the testing procedure. The time needed to train the

training datasets was approximately 8.60 minutes. The testing process is done for 400 cases. These 400 cases are fed to the proposed network and their output is recorded.

Performance plot: Performance plot show the training errors, validation errors, and test errors appears, as shown in the training process. Training errors, validation errors, and test errors appears, as shown in the following figure 1.

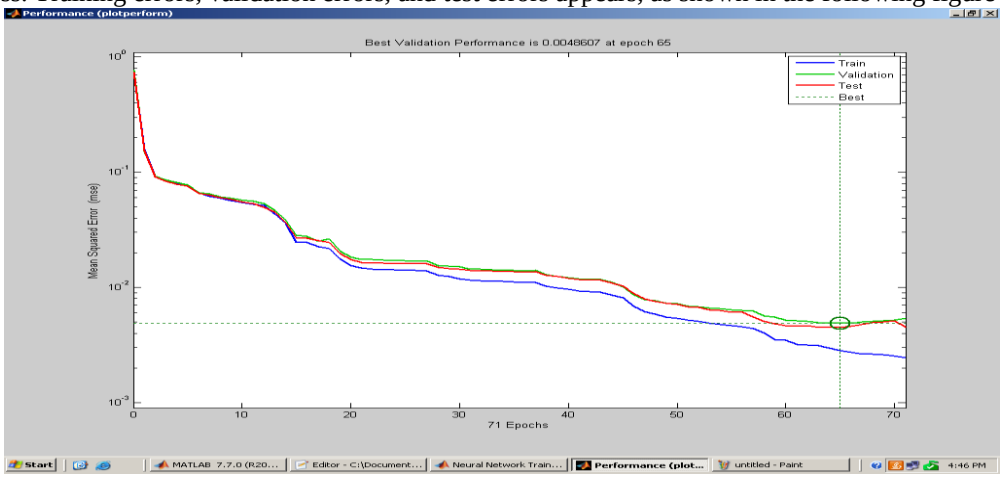

Figure 1: Performance plot

Receiver Operator Characteristic Measure (ROC) Plot: The colored lines in each axis represent the ROC curves. The *ROC curve* is a plot of the true positive rate (sensitivity) versus the false positive rate (1 -specificity) as the threshold is varied. A perfect test would show points in the upper-left corner, with 100% sensitivity and 100% specificity. For this problem, the network performs very well. The results show very good quality in the following figure 2.

Figure 2: ROC Plot

Regression plots: This is used to validate the network performance. The following regression plots display the network outputs with respect to targets for training, validation, and test sets. For a perfect fit, the data should fall along a 45 degree line, where the network outputs are equal to the targets. For this problem the fit is reasonably good for all data sets, with R values in each case of 0.93 or above. The results show in the following figure 3.

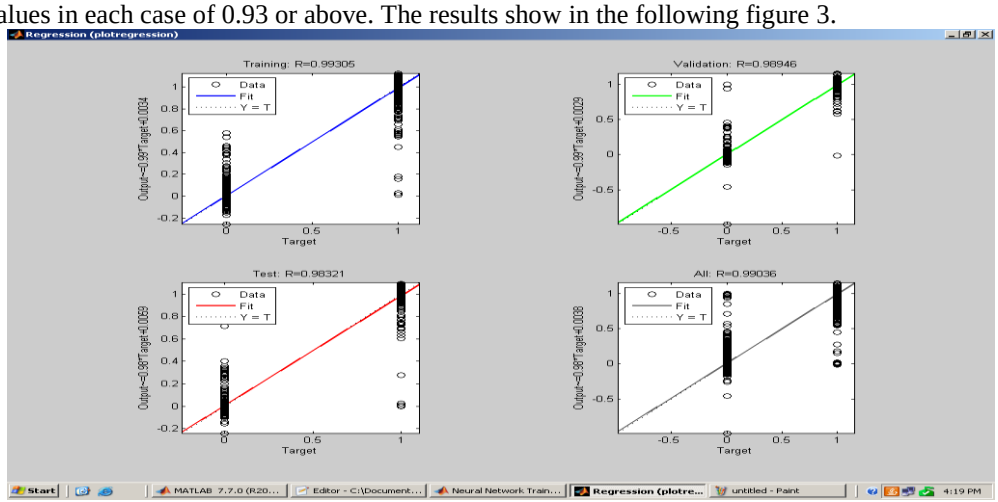

Figure 3: Regression Plots

Training State Plot: Training state plot show the deferent training state in training process and validation check graph. These plots also show the momentum and gradient graph and state in training process. The results show in the following figure 4.

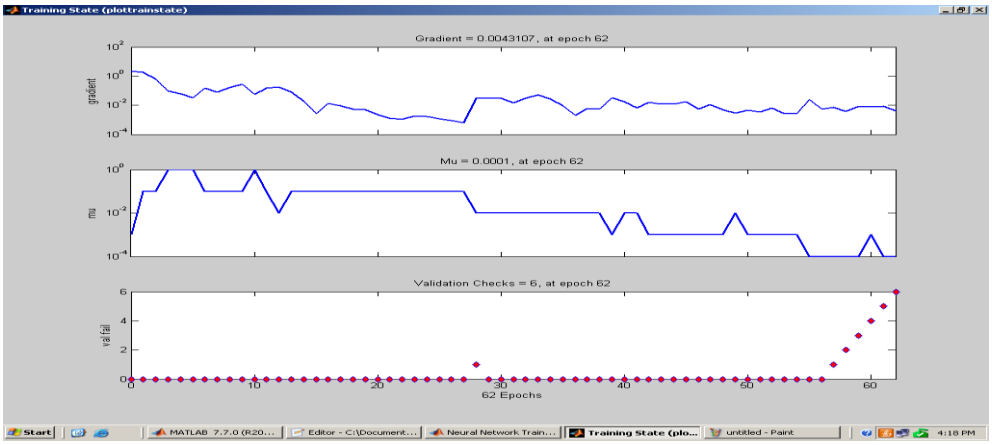

Figure 4: Training State Plot

Confusion Matrix: This figure shows the confusion matrices for training, testing, and validation, and the three kinds of data combined. The network outputs are very accurate, as you can see by the high numbers of correct responses in the green squares and the low numbers of incorrect responses in the red squares. The lower right blue squares illustrate the overall accuracies. The diagonal cells show the number of cases that were correctly classified, and the off-diagonal cells show the misclassified cases. The blue cell in the bottom right shows the total percent of correctly classified cases (in green) and the total percent of misclassified cases (in red). The results show very good recognition.

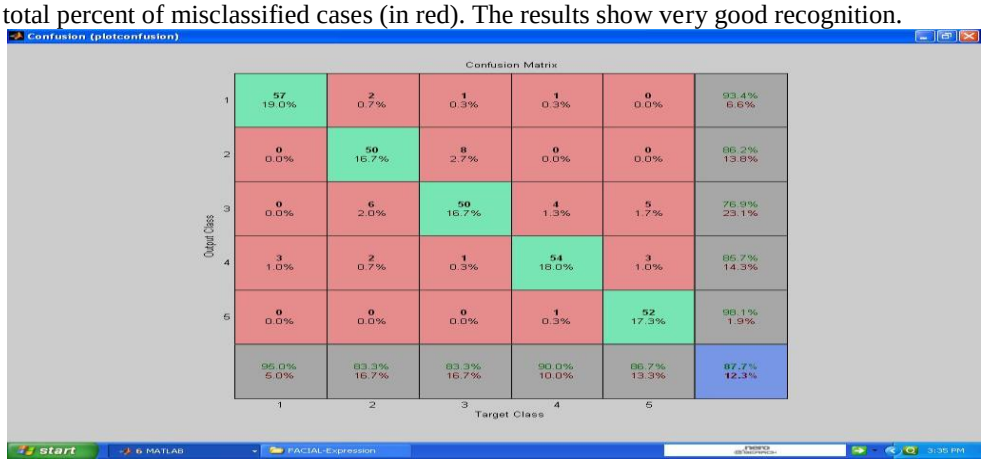

Figure 5: Confusion Matrix

IV. SIGNATURE RECOGNITION

The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf. Thus the users are more likely to approve this kind of computerized authentication method [30, 32]. Signature verification systems differ in both their feature selection and their decision methodologies. More than 40 different feature types have been used for signature verification [27, 28]. Features can be classified into two major types: local and global [34, 35]. Global features are features related to the signature as a whole, for instance the average signing speed, the signature bounding box and Fourier descriptors of the signatures trajectory. Local features correspond to a specific sample point along the trajectory of the signature. Examples of local features include distance and curvature change between successive points on the signature trajectory [36, 37]. The pressure information at each point along the signature trajectory is another example of commonly used local feature. Some of these features are compared in order to find the more robust ones for signature verification purposes.

There are many ways to structure the NN training, but a very simple approach is to firstly extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. The second step is for the NN to learn the relationship between a signature and its class (either "genuine" or "forgery"). Once this relationship has been learned, the network can be presented with test signatures that can be classified as belonging to a particular signer. NNs therefore are highly suited to modeling global aspects of handwritten signatures.

4.1 METHODOLOGY FOR SIGNATURE RECOGNITION

The design of a system is divided into two stages:

1. Training stage
2. Testing stage

A training stage consist of four major steps

1) Retrieval of a signature image from a database
2) Image pre-processing
3) Feature extraction
4) Neural network training

A testing stage consists of five major steps

1) Retrieval of a signature to be tested from a database
2) Image pre-processing
3) Feature extraction
4) Application of extracted features to a trained neural network
5) Checking output generated from a neural network.

Fig. 6 shows one of the original signature image taken from a database and all the subsequent figures show the resultant signature image obtained after performing the steps mentioned in an algorithm.

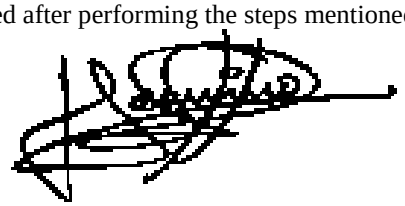

Figure 6: Signature Image

4.1.1 Pre-processing

The pre processing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signature standard and ready for feature extraction. The pre-processing stage improves quality of the image and makes it suitable for feature extraction [31, 35]. The prepossessing stage includes

4.1.2 Converting image to binary

A gray scale signature image is converted to binary to make feature extraction simpler.

4.1.3 Image resizing

The signatures obtained from signatory are in different sizes so, to bring them in standard size, resizing is performed, which will bring the signatures to standard size 256*256 as shown in Fig. 7.

4.1.4 Thinning

Thinning makes the extracted features invariant to image characteristics like quality of pen and paper. Thinning means reducing binary objects or shapes to strokes that are single pixel wide.

4.1.5 Bounding box of the signature:

In the signature image, construct a rectangle encompassing the signature. This reduces the area of the signature to be used for further processing and saves time.

4.1.6 Feature Extraction

The choice of a powerful set of features is crucial in signature verification systems. The features that are extracted in this phase are used to create a feature vector. A feature vector of dimension 24 has been used to uniquely characterize a candidate signature. These features are extracted as follows:

Maximum horizontal and vertical histogram:

Horizontal histogram is calculated by going through each row of the signature image and counting number of black pixels. A row with maximum number of black pixels is recorded as maximum horizontal histogram. Similarly, a vertical histogram is calculated by going through each column of the signature image and finding a column with maximum number of black pixels.

Center of mass:

Split the signature image in two equal parts and find center of mass for individual parts.

Normalized area of signature:

It is the ratio of area of signature image to the area of signature enclosed in a bounding box. Area of a signature is the number of pixels comprising it.

Aspect Ratio:

It is the ratio of width of signature image to the height of the image. This is done because width or height of person's signature may vary but its ratio remains approximately equal.

Tri surface feature:

Two different signatures may have same area .so; to increase the accuracy of the features three surface feature has been used. In this, a signature is divided into three equal parts and area for each part is calculated. Eq. (1) is then used to calculate normalized area of each part. Figure (6) shows tri surface feature

The six fold surface feature:

Divide a signature in three equal parts and find bounding box for each part. Then calculate centre of mass for each part. Draw a horizontal line passing through centre of mass of each part and calculate area of signature above and below centre of mass within a bounding box. This provides six features.

Transition feature:

Traverse a signature image in left to right direction and each time there is a transition from 1 to 0 or 0 to 1, calculate a ratio between the position of transition and the width of image traversed and record it as a feature. Repeat a same process in right to left, top to bottom and bottom to top direction. Also calculate total number of 0 to 1 and 1 to 0 transitions. This provides ten features.

4.1.7 Training a neural network

Extracted 24 feature points are normalized to bring them in the range of 0 to 1.These normalized features are applied as input to the neural network.

4.1.8 Verification.

In the verification stage, a signature to be tested is pre-processed and feature extraction is performed on pre processed test signature image as explained in section 2.2 to obtain feature vector of size 24. After normalizing a feature vector it is fed to the trained neural network which will classify a signature as a genuine or forged.

4.2 NEURAL NETWORK FOR SIGNATURE RECOGNITION

The objective of this study is to classifying hand written signature using feed forward back propagation neural network and Levenberg-Marquardt (LM) as the training algorithm. LM algorithm has been used in this study due to the reason that the training process converges quickly as the solution is approached. For this study, sigmoid, hyperbolic tangent functions are applied in the learning process. Feed forward back propagation neural network use to classify signature according to feature vector characteristic. Feed forward back propagation neural network is created by generalizing the gradient descent with momentum weight and bias learning rule to multiple layer networks and nonlinear differentiable transfer functions. Input vectors and the corresponding target vectors are used to train feed forward back propagation neural network. Neural network train until it can classify the defined pattern. The training algorithms use the gradient of the performance function to determine how to adjust the weights. The gradient is determined using a technique called back propagation, which involves performing computations backwards through the network. The back propagation computation is derived using the chain rule of calculus. In addition, the transfer functions of hidden and output layers are tan-sigmoid and tan-sigmoid, respectively.

4.2.1 Training and Testing Result

The proposed network was trained with feature vector data cases. When the training process is completed for the training data, the last weights of the network were saved to be ready for the testing procedure. The time needed to train the training datasets was approximately 7.60 minutes. The testing process is done for 200 cases. These 200 cases are fed to the proposed network and their output is recorded.

Performance plot: Performance plot show the training errors, validation errors, and test errors appears, as shown in the training process. Training errors, validation errors, and test errors appears, as shown in the following figure 7.

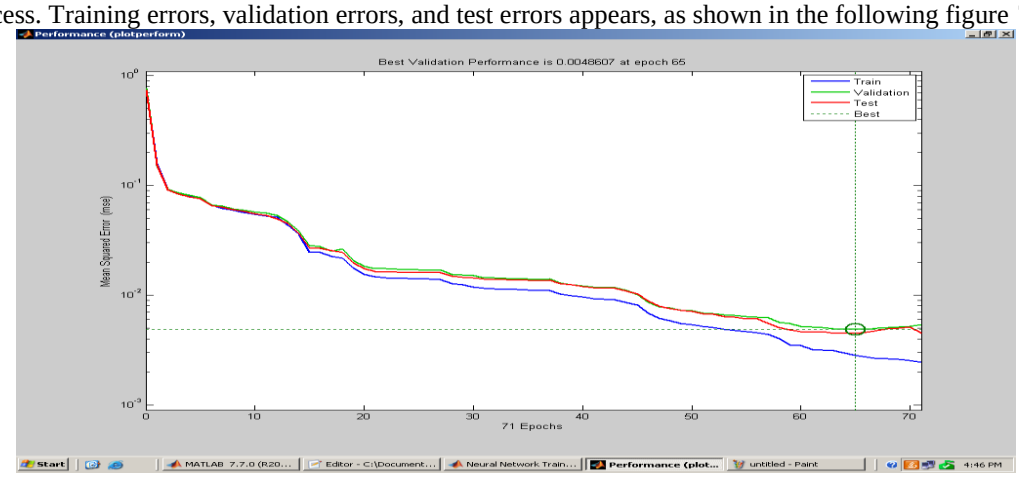

Figure 7: Performance plot

Receiver Operator Characteristic Measure (ROC) Plot: The colored lines in each axis represent the ROC curves. The *ROC curve* is a plot of the true positive rate (sensitivity) versus the false positive rate (1 -specificity) as the threshold is varied. A perfect test would show points in the upper-left corner, with 100% sensitivity and 100% specificity. For this problem, the network performs very well. The results show very good quality in the following figure 8.

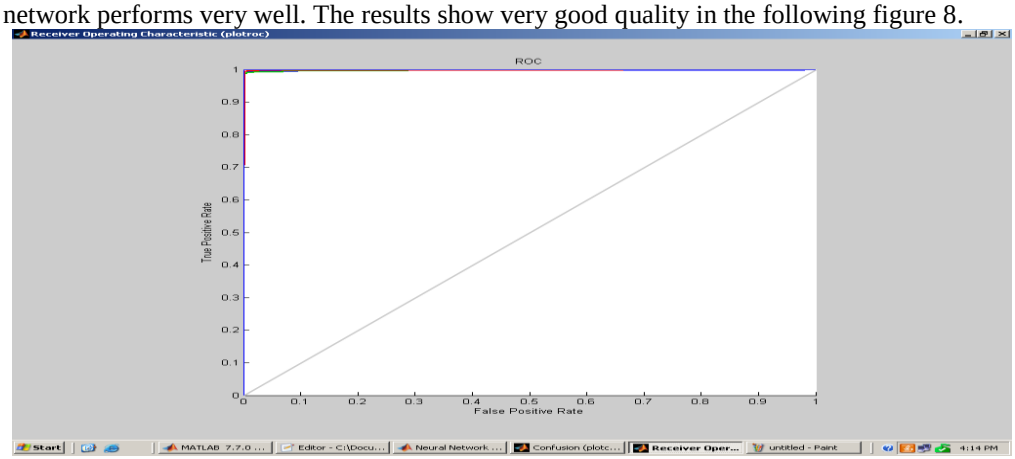

Figure 8: ROC Plot

Regression plots: This is used to validate the network performance. The following regression plots display the network outputs with respect to targets for training, validation, and test sets. For a perfect fit, the data should fall along a 45

degree line, where the network outputs are equal to the targets. For this problem the fit is reasonably good for all data sets, with R values in each case of 0.93 or above. The results show in the following figure 9.

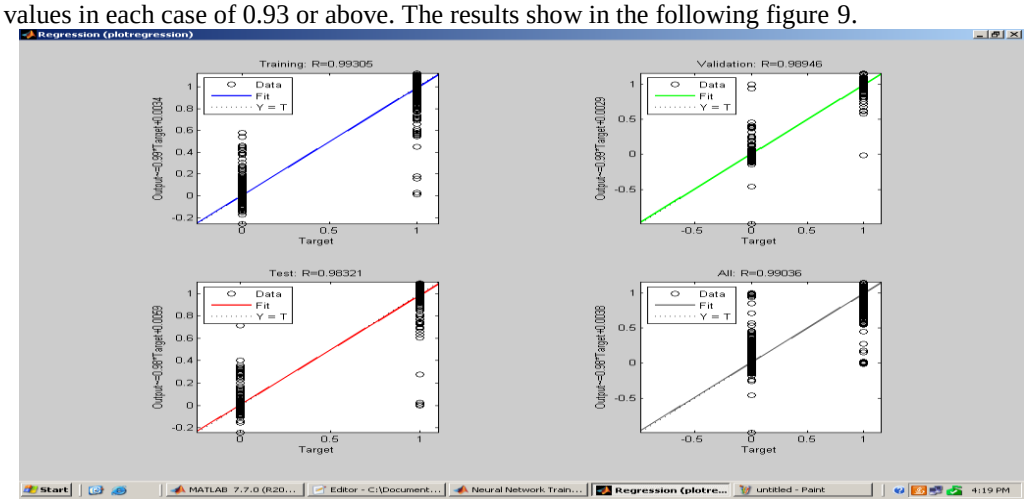

Figure 10: Regression Plots

Training State Plot: Training state plot show the deferent training state in training process and validation check graph. These plots also show the momentum and gradient graph and state in training process. The results show in the following figure 10.

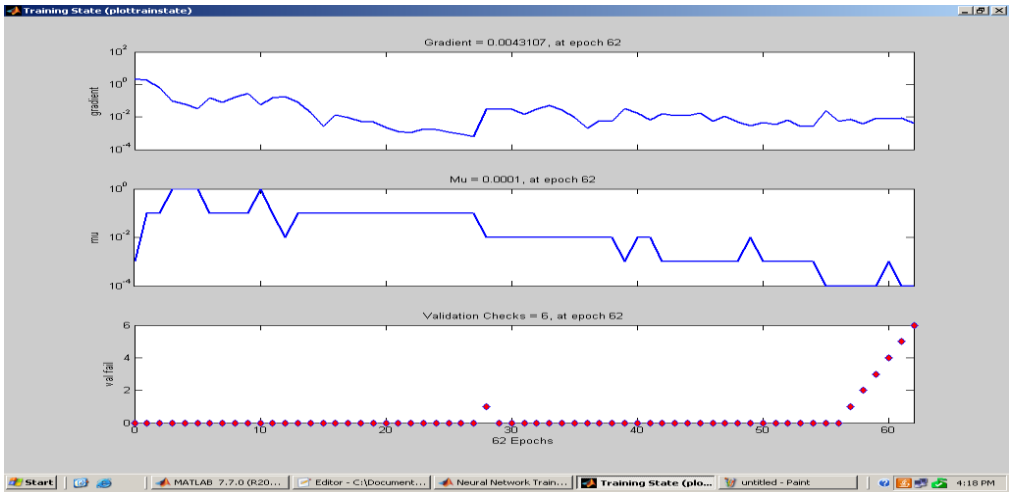

Figure 10: Training State Plot

V. RESULTS AND DISCUSSION

For training and testing of the system many signatures are used. The results provided in this research used a total of 2500 signatures. Those 2500 signatures are comprised of 50 sets (i.e. from 50 different people) and, for each person there are 25 samples of genuine signatures and 25 samples of forgeries. To train the system, a subset of this database was taken comprising of 25 genuine samples taken from each of the 50 different individuals and 25 forgeries made by different person for one signature. The features extracted from 25 genuine signatures and 25 forged signatures for each person were used to train a neural network.

After applying a feature vector of test signature if the output neuron generates value close to +1 test signature is declared as genuine or if it generates value close to -1 it is declared as forged.Fig.7 shows performance graph of the training a two layer feed forward neural network. The correct classification rate of the system is 98.66% in generalization. Our recognition system exhibited 100% success rate by identifying correctly all the signatures that it was trained for. However, it exhibited poor performance when it was presented with signatures that it was not trained for earlier. We did not consider this a "high risk" case because recognition step is always followed by verification step and these kinds of false positives can be easily caught by the verification system. Generally the failure to recognize/verify a signature was due to poor image quality and high similarity between two signatures. Recognition and verification ability of the system can be increased by using additional features in the input data set.

VI. CONCLUSION

This paper presents a method of off line handwritten signature verification using neural network approach. The method uses features extracted from preprocessed signature images. The extracted features are used to train a neural network using error back propagation training algorithm. The network could classify all genuine and forged signatures correctly. In this paper, a new face recognition technique is proposed which uses 2-D DCT, HMM, Fisher Scores and neural network to separate the face systematically. The 2-D DCT and fisher scores are applied to the difference images to

compress and refine the features useful for the recognition task. The new technique has been applied to face image. Experimental results have demonstrated the superior effectiveness of the new method.

REFERENCES

[1] M. Pantic and L. J. M. Rothkrantz, "Automatic analysis of facial expressions: the state of the art," IEEE Trans. Pattern Analysis & Machine Intelligence, vol.22, no.12, pp.1424-1445(Dec. 2000).

[2] Y. S. Gao, M. K. H. Leung, S. C. Hui, and M. W. Tananda, "Facial expression recognition from line-based caricature," IEEE Trans. System, Man, & Cybernetics (Part A), vol.33, no.3, pp.407-412(May, 2003).

[3] A. Nefian, A hidden Markov model-based approach for face detection and recognition, Ph.D. Thesis, Georgia Institute of Technology, 1999.

[4] A. Nefian, Embedded Bayesian networks for face recognition, ICME 2002—IEEE International Conference on Multimedia and Expo, Lausanne, Switzerland, August 2002, pp. 133–136.

[5] H. Othman, T. Aboulnasr, Low-complexity 2-D hidden Markov model face recognition, ISCA 2000—IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, May, 2000, pp. V33–V36.

[6] T. Jaakkola, D. Haussler, Exploiting generative models in discriminative Classifiers, in: S.A. Solla, T.K. Leen, K.R. Müller (Eds.), Advances in Neural Information Processing Systems, vol. 12, MIT Press, Cambridge, MA, 2000.

[7] W. Zhao, R. Chellappa, A. Krishnaswamy, Discriminant analysis of principal components for face recognition, AFGR 1998—IEEE International Conference on Automatic Face and Gesture Recognition, Nara, Japan, April, 1998, pp. 336–341.

[8] Prashanth CR,KB Raja,KR Venugopal, LM Patnaik,"Standard Scores Correlation based Offline signature verification system", International Conference on advances in computing, control and telecommunication Technologies 2009 .

[9] R. Plamondon and S.N. Srihari, "Online and Offline Handwriting Recognition: A Comprehensive Survey", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.22 no.1, pp.63-84, Jan.2000.

[10] J Edson, R. Justino, F. Bortolozzi and R. Sabourin, "An off-line signature verification using HMM for Random,Simple and Skilled Forgeries", Sixth International Conference on Document Analysis and Recognition, pp.1031-1034, Sept.2001. 211-222, Dec.2000.

[11] J Edson, R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, "An off-line Signature Verification System Using HMM and Graphometric features", DAS 2000

[12] B. Herbst. J. Coetzer. and J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," EURASIP.Journal on Applied Signal Processing, vol. 4, pp. 559–571, 2004.

[13] M. Blumenstein. S. Armand. and Muthukkumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification," International Joint Conference on Neural Networks, 2006.

[14] S.Srihari. K. M. Kalera. and A. XU, "Offline Signature Verification and Identification Using Distance Statistics," International Journal of Pattern Recognition And Artificial Intelligence ,vol. 18, no. 7, pp. 1339–1360, 2004.

[15] Martinez, L.E., Travieso, C.M, Alonso, J.B., and Ferrer, M. Parameterization of a forgery Handwritten Signature Verification using SVM. IEEE 38thAnnual 2004 International Carnahan Conference on Security Technology ,2004 PP.193-196.

[16] Aykanat C. et. al ,(Eds). 2004. Proceedings of the 19th International Symposium on Computer and Information Sciences, ISCIS 2004. Springer-Verlag Berlin Heidelberg New York. pp. 373-380.

[17] Sonsone and Vento. "Signature Verification: Increasing Performance by Multi-Stage System", Pattern Analysis & Application, vol.3, no. 2, 2000, pp.169-181

[18] Velez, J.F., Sanchez, A. and Moreno, A.B. 2003. Robust Off-Line Signature Verification using Compression Networks and Position Cuttings.

[19] .Bhattacharyya Debnath, Bandyopadhyay Samir Kumar, Das, Poulami, Ganguly Debashis, Mukherjee Swarnendu, "Statistical approach for offline handwritten signature verification", Journal of Computer Science March 01, 2008.

[20] Edson J. R. Justino, Flávio Bortolozzi and Robert Sabourin , "Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries", in International Conference on Document Analysis and Recognition, vol. 1, pp. 105–110, Seattle, Wash, USA, 2001.

[21] Edson J. R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, "An Off-Line Signature Verification System Using HMM and Graphometric Features", DAS 2000, 4th IAPR International Workshop on Document Analysis Systems, Rio de Janeiro, Brazil, (2000), pp 211--222.

