ISSN:0975-9646

Image Based Fraud Prevention

D. Madhu Babu[1], M. Bhagyasri[2], K. Lahari[3], CH. Madhuri[4], G. Pushpa Kumari[5].

[1]Assosiate Professor, [2,3,4,5]Student,
Department of CSE,
Lendi Institute of Engineering and Technology, Vizianagaram,India.

***Abstract*— In this paper, by using hidden markov model and svd coefficient. we proposed image based fraud prevention. Based on priority here we are taking seven state HMM. As another novel point, we used a small number of quantized Singular Values Decomposition (SVD) coefficients as features describing blocks of face images. Fraud prevention describes measures to avoid frauds that occur in the first place. Instead of outlier we are taking image as an input that input is human face. A wide variety of techniques have been proposed for feature extraction by using HMM and SVD coefficient. Based on priority here we are taking seven states HMM. When the card is inserted to ATM then it asks the pin number and captures the image. The image features are extracted then compared the image with the image stored in the training data base. If the image is matched then the transaction will proceed. If the image is not matched with the images in database then the transaction will not proceed. Image may be finger print or face. So by using image we can prevent the frauds.**

Keywords— **Face Recognition, Hidden Markov Models, Singular Value Decomposition.**

I. INTRODUCTION

Now a day's the frauds are increased in various fields such as online transactions, ATM's. Fraud detection involves identifying fraud quickly as possible once it has been committed. Generally frauds are detected by using outlier analysis. This has made it easier for fraudsters to indulge in a new and abstruse ways of committing credit card fraud over online transaction. Outlier detection refers to the problem of finding patterns in data that do not conform to expected normal behaviour. In outlier the frauds are detected by comparing the current and previous transactions. It takes more time to detect the fraud. So outlier has become inefficient. By using Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money).

Face recognition is the recognizing a special face from set of different faces. Face has a significant role in human beings communications where, each person along with his/her feelings mainly is distinguished by his/her face Image. One can easily find out that one of the main problems in machine-human being interactions is the face recognition problem. A human face is a complex object with features varying over time. So a robust face recognition system must operate under a variety of conditions. Face recognition has been undoubtedly one of the major topics in the image processing and pattern recognition in the last decade due to the new interests in, security, smart environments, video indexing and access control. Existing and future applications of face recognition are many. We divide these applications into two main categories of governmental and commercial uses. Rapid progression through customs by using face as a live passport in immigration, comparison of surveillance images against an image database of known terrorists and other unwanted people in security/counterterrorism, and verifying identity of people found unconscious, dead or individuals refusing to identify themselves in hospital are examples of governmental uses. Withdrawing cash from an automated teller machine (ATM) without cards or pin numbers in banking and access control of home and office in premises access control are some examples of commercial uses of face recognition systems which demonstrate the importance of these systems. There have been a several faces recognition methods, common face recognition methods are Geometrical Feature Matching, Eigen faces method, Bunch Graph Matching, Neural Networks, Support Vector Machines, Elastic Matching and Hidden Markov Models.

Instead of outlier we are taking image as an input. Image is nothing but a face. A wide variety of techniques have been proposed for feature extraction by using HMM and SVD coefficient.

II. MAIN TITLE

Image Based Fraud Prevention we justify this title based on the Image we are going to make the transactions. Image is taken as input and by using 7-state HMM and SVD coefficient the features of that image i.e., face is extracted and then compared with the database Image if that Image is recognized then the transactions are made this is how we are going to prevent the frauds in the initial stage itself.

III. HIDDEN MARKOV MODELS

HMMs are usually used to model one dimensional data but in recent years,they have been used in vision texture segmentation, face finding, object recognition and face recognition. Every Hmm is associated with non-observable (hidden) states and an observable sequence generated by the hidden states individually. The elements of HMM are as below:

- N= |S| is the number of states in the model, where S={s1,s2, ... ,sN} is the set of all possible States. The state of model at time t is given by qtS.

- M= |V| is the number of different observation symbols, where V = {v1, v2, ..., vM} is the set of all possible observations symbols vi (also called the code book of the model.) the observation symbol at time t is given by otV. As the reader is expected to know, observation vector is another concept that frequently used in HMM model. Indeed the training and test process of HMM models are performed in the observation vectors space.

Each observation vector is a vector of observation symbols of length T. T is defined by user based on the in hand problem.

• $A = \{a_{ij}\}$ is the state transition probability matrix, Where:

$$a_{ij} = p[q_{t+1} = s_j | q_t = s_i], 1 \le i, j \le N, a_{ij} \quad (1)$$

$$\sum_{j=1}^{N} a_{ij} = 1,\ 1 \le i \le N \quad (2)$$

• $B = \{b_j(k)\}$ is the observation symbol probability Matrix, Where:

$$b_j(k) = p[o_t = v_k | q_t = s_j], 1 \le j \le N, 1 \le k \le M \quad (3)$$

$\pi = \{\pi_1, \pi_2, \pi_3, \ldots \pi_N\}$ is the initial state distribution, where:

$$i = p[q_1 = s_i], 1 \le i \le N \quad (4)$$

Using shorthand notation HMM is defined as following triple:

$$\lambda = (A, B, \pi) \quad (5)$$

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

SINGULAR VALUE DECOMPOSITION:

The Singular Value Decomposition (SVD) has been an important tool in signal processing and statistical data analysis. Singular values of given data matrix contain information about the noise level, the energy, the rank of the matrix, etc. As Singular vectors of a matrix are the span bases of the matrix, and orthonormal, they can exhibit some features of the patterns embedded in the signal. SVD provides a new way for extracting algebraic features from an image. A singular Value Decomposition of an m×n matrix X in any function of the form:

$$X = U \sum V^T \quad (6)$$

Where U(m×m) and V(m×m) are orthogonal matrix, and Σ is and m×n diagonal matrix of singular values with components $\sigma_{ij} = 0, i \ne j$ and $ij > 0$.

Further more, it can be shown that there exist non-unique matrices U and V such that $\sigma_1 \ge \sigma_2 \ge \ldots\ldots\ldots\ldots \ge 0$

The columns of the orthogonal matrices U and V are called the left and right singular vectors respectively; an important property of U and V is that they are mutually orthogonal. The main theoretical property of SVD relevant to face image recognition is its stability on face image.

IV. PROPOSED METHOD:

We have proposed image based fraud prevention in this we are taking image as an input if the image is matched with the database image then transaction will proceed. so, by using 7-state HMM and SVD coefficients we are extracting the features of the image i.e., face based on priority i.e. first priority for eyes, mouth and second priority for hair, forehead, eyebrows, nose, chin then based on priority the input image is compared with database image if matched or face is recognized then the transactions are made this is how we are providing the security.

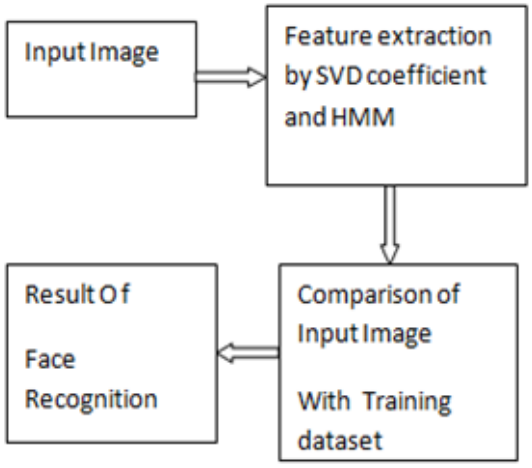

Fig.1: Face recognition process

Face recognition using Singular Value Decomposition and HMM consist of steps in which it captures the information content in an image of a face which are further useful for face recognition efficiently. In processing flow of face recognition using SVD and HMM approach, it includes extraction of face features by SVD coefficient , Seven state HMM divides face image in seven states then by using classifier ,there is comparison of input image with training dataset. If input image matches with training dataset image then face is said to be recognized otherwise face is unrecognized.

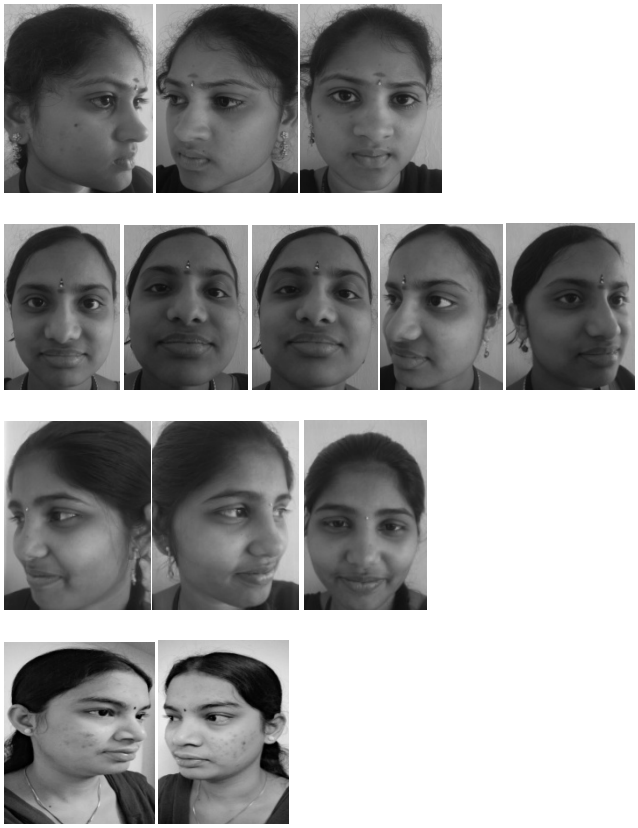

Fig.2 Four examples of images in database

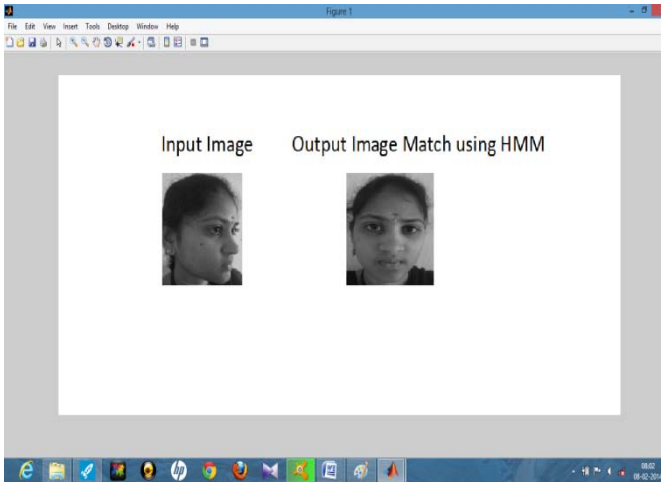

Fig. 3 Input image and recognized image from the training data base

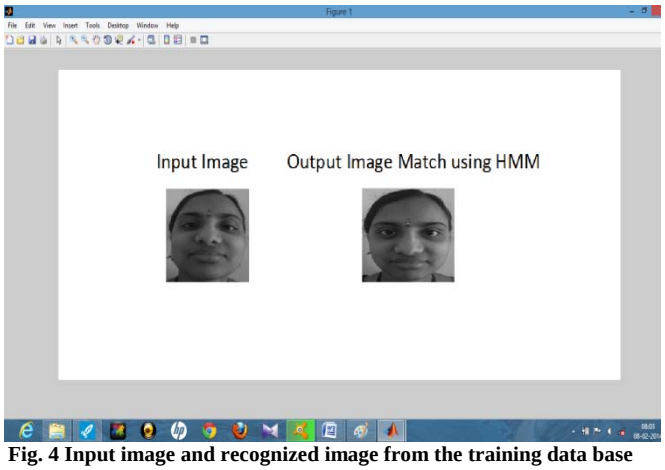

Fig. 4 Input image and recognized image from the training data base

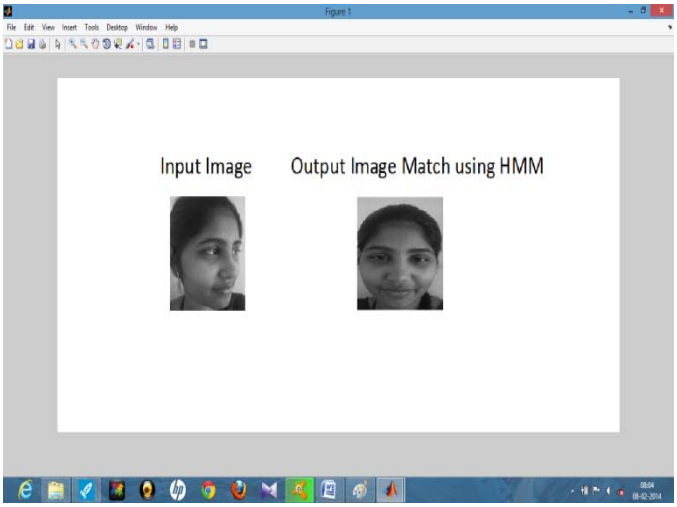

Fig. 5 Input images and recognized image from the training data base

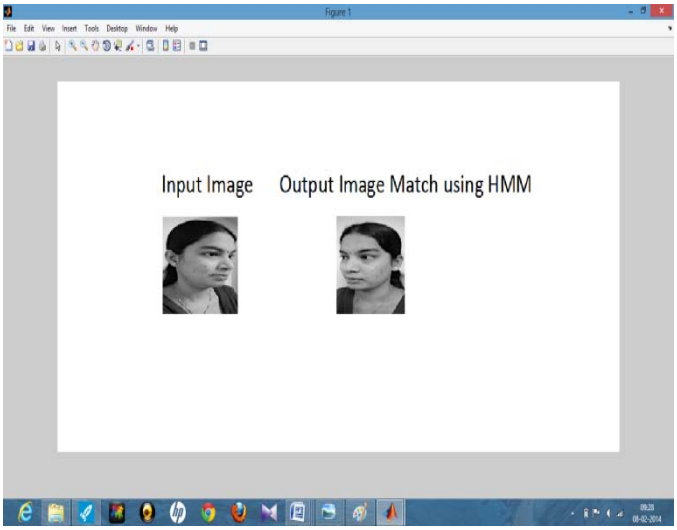

Fig. 6 Input image and recognized image from the training data base

V. CONCLUSIONS

We are going to provide security for the online transactions based on image. By using Image we are going to provide transactions. Images of each face were converted to a sequence of blocks. Each block was featured by a few number of its SVD parameters. Each class has been associated to Hidden Markov Model as its classifier. The evaluations and comparisons were performed on the two well known face image databases. So that Fraud is prevented in the initial stage itself. This can be used in companies in order to provide security by allowing authorized persons.

Future work: In the future, focus on the use large and more complicated databases to test the system. For this complicated database it is simply expected that all the previous methods will not repeat such efficiency reported in the paper. Try to improve the feature extraction and the modeling of the faces. The use of 2D HMM more complicated models may improve the system performance. Our future work will be focus on the extension of this paper. Try to improvise the system by recognizing derived stereoscopic 3D JPEG Images.

ACKNOWLEDGMENT

We would like to say thanks to our Management Members for providing us good infrastructure and Principal for encouraging us and Head Of our Department for motivation and Continuous encouragement.

REFERENCES

[1] "Feature Extraction and Representation for Face Recognition", 1M. Saquib Sarfraz, 2Olaf Hellwich and 3Zahid Riaz.

[2] "Image-based Fraud Detection in Automatic Teller Machine" IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.11, November 2006.

[3] W.Y. Zhao, R. Chellappa, A. Rosenfeld and J.P.Phillips, "Face Recognition: A Literature Survey", ACM Computing Surveys, December Issue, pp. 399-458, 2003.

[4] Nes A. and Bo. K. "Face Recognition," Image Processing Specialization Project, Norwegian University of Science and Technology, November 2002.

[5] Nefian A. V. and Hayes M. H. "Hidden Markov Models for Face Recognition," In Proceedings IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.2721–2724, Seattle, May 1998.

[6] Extraction of Facial Regions and Features using Color and Shape Information .Karin Sobottka Ioannis Pitas Department of Informatics University of Thessaloniki Greece.