JNNCE Journal of Engineering & Management – A Peer Reviewed Bi-annual Journal
Available online @ https://jjem.jnnce.ac.in
ISSN: 2582-0079 (O)
Indexed in International Scientific Indexing (ISI)
Impact Factor Value: 1.025 for 2018-19
Volume: 3, Number: 1
January - June 2019

A Novel Technique for ATM Security by Image Processing

Pranesh Kulkarni
4th Semester MCA,
JNNCE,
Shimoga
alandikarpranesh@gmail.com

Dr. Raghavendra S.P
Assistant Prof,
Dept. of MCA JNNCE,
Shimoga
raghusp@jnnce.ac.in

Abstract Face recognition presents a challenging problem in the field of image analysis and computer vision. The security of information is becoming very significant and difficult. Security cameras are presently common with a security system in airports, offices, schools & colleges, ATM, banks and in many other locations. Face recognition is a biometric system used to identify or verify a person from a digital image. Face Recognition system is widely used in security. Face recognition system should be able to automatically detect a face in an image. This involves extracting the features from the image and then recognize the face, regardless of lighting, expression, illumination, ageing, transformations (translate, rotate and scale image) and posture, which is a difficult task.
Though banking becomes easier today with the support of ATMs, it also became feeble and vulnerable. There have been countless cases of abuse that have occurred in banking transactions. Thus, there is an essential need to provide high security for banking transactions. This paper proposes the amalgamation of Face Recognition System in the identity verification process engaged in ATMs to enhance their security system.

KEYWORDS: *ATM System, Face Recognition Software (FRS), Security.*

1. Introduction

The rise of technology has brought into force several types of tools that aspire at more customer pleasure. ATM is a machine which has made money transactions effortless for customers. But it has both advantages and disadvantages. Current ATMs make use of not more than an access card and PIN for uniqueness confirmation. This exposes ATMs to a lot of fake attempts to use them by means of card theft, PIN theft, stealing and hacking of customer's account details. Using Face Recognition System in ATMs can show the way to deal with such cases.

Face recognition is becoming an active research area spanning several disciplines such as image processing, pattern recognition, computer vision, neural networks, cognitive science, neuroscience, psychology and physiology. It is a dedicated process and not merely an application of the general object recognition process. It is also the representation of the most splendid capacities of human vision.

In order to develop a useful and applicable face recognition system several factors need to be take in hand.
1. The overall speed of the system from detection to recognition should be acceptable.
2. The accuracy should be high.

3. The system should be easily updated and enlarged, that is easy to increase the number of subjects that can be recognized.

1.1What Are Face Recognition Systems (FRS)?

FRS is an application that mechanically identifies a person from a digital image or a video outline from a video source. One of the processes to do this method is by matching chosen facial features from a facial database and the image.

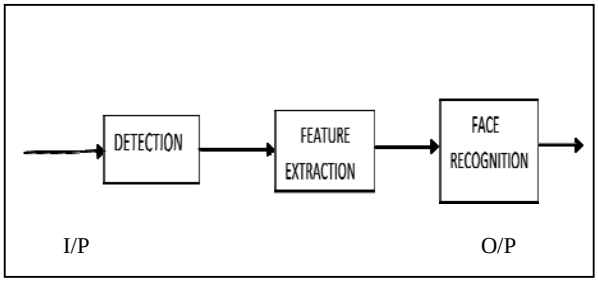

Fig 1: Basic flowchart of FRS

1.2When Did They Develop?

The pioneers of robotic Face Recognition include Helen Chan Wolf, Woody Bledsoe and Charles Bison. During 1964 and 1965, Bledsoe, along with Helen Chan Wolf and Bison, worked on using the computer to be familiar with human faces. He was pompous of his work, but because the support was provided by an unknown intelligence group that did not allow more publicity, little work was published. Given a large database of photos and images, the problem encountered was to select from the database a tiny set of records such that one of the image records coordinated the photograph. The achievement of the performance could be well thought-out in terms of the relation of the respond list to the quantity of report in the database. Still the recognition problem was made hard by the great discrepancy in lean and head rotation, lighting intensity and angle, facial expression, etc. In 1966, the work was continued by Peter Hart. Peter's experiment was done on a database contains over 2000 images; the computer outperformed humans when presented with the same detection tasks. The growth period for facial recognition started in late 1980s and they were existing systems was made accessible in the 1990s.

2. Literature Survey

Arunkumar, Vasanth Kumar, Naveenly King, Aravindan[1] have observed that the growth in the electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Users have been largely depending on and trusting the Automatic Teller Machine (ATM) to conveniently meeting their banking needs. The ATM fraud has recently become more widespread. This system is used to avoid the ATM robberies and wrong person misuses the ATM...

A S Tolba [2] et al have proposed an overview of face recognition and its applications**.**

Divyarajsinh N. Parmar [3] remarks that, Face recognition presents a challenging problem in the field of image analysis and computer vision. The security of information is becoming very significant and difficult. Face recognition is a biometric system used to identify or verify a person from a digital image.

Kresimir Delac, Sonja Grgic and Mislav Grgic [4] observe that, Face recognition has repeatedly shown its importance over the last ten years or so. Not only is it a vividly researched area of image analysis, pattern recognition and more precisely biometrics (Zhao et al., 2003; Delac et al., 2004; Li & Jain, 2005; Delac & Grgic, 2007), but also it has become an important part of our everyday lives since it was introduced as one of the identification methods to be used in e-passports.

Mourad Moussa, Maha Hmila, Ali Douik [5] find that, in the field of image processing and recognition, discrete cosine transform (DCT) and principal component analysis (PCA) are two widely used techniques. In their paper a novel technique is demonstrated for face recognition approach based on them. Feature selection (FS) is a global optimization problem in machine learning, which reduces the number of features, removes irrelevant, noisy and

redundant data, and results in acceptable recognition accuracy.

Priyanka [6] has explored in this paper, some of the common and reliable approaches for facial recognition. These approaches include PCA, LDA, KDA, Neural Network etc. The paper has also discussed the basic model of facial recognition and explained each stage of this model.

T.Suganya, T.Nithya, C.Sunita, [7] propose the amalgamation of Face Recognition System in the identity verification process engaged in ATMs to enhance the security system.

Yongzhong Lu [8] has presented a critical survey of existing literature on human face recognition over the last 4–5 years and has observed that interest and research activities in face recognition have increased significantly over the past few years, especially after the American airliner tragedy on September 11, 2001.

3. Proposed Methodology

The important step is to locate a dominant open-source appearance identification program that uses local feature analysis and that is based on facial verification. This plan must be compliable on multiple systems, involving Windows and Linux variants, and also be customizable to the degree of allowance for variations in processing power of the machines onto which it would be deployed. Once a final program is done, a simple ATM black box program is developed. This program will serve as the hypothetical ATM with which the facial recognition software will work together. It will take a name and password, and then look into a folder for a photograph that is associated with that name. It will then take an image from a separate folder of "live" images and use the facial recognition program to produce a match level between the two images.

At last it will use the match level to decide whether "access" or not to allow "access", at which point it will terminate. Both pieces of software will be checked for errors and run on a Windows XP and a Linux system. If both function properly, they will be tweaked as much as possiblel to increase performance (decreasing the time used up matching) and to decrease memory footstep.

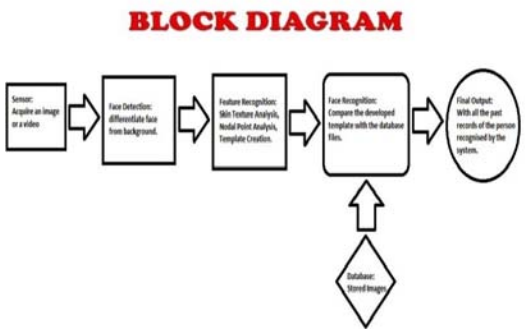

Fig 2: Block Diagram of face recognition

3.1 Techniques and Methods

They are of three types:

- 2-D
- 3-D
- Surface Texture Analysis.

3.1.1 2-D Technique: The 2-D recognition method was one of the original techniques employed. It maintained details of people's faces as seen two dimensionally. Details like width of the nose, width of the eyes, distance between the eyes, jaw line, cheek bone figure were used for contrast. This type of face recognition was not too accurate. Change in facial expression or difference in ambient lighting on an appearance that is not directly looking into the camera did not produce expected results.

3.1.2 3-D Technique: Progress in face recognition gave rise to the 3-D recognition system. This stepped up technique used facial appearance like contours of the eye sockets, chin, nose, peaks and valley on the visage for identification. The database will store details of faces also. The advantage of 3-D technique over 2-D method is that 3-D face identification works fine even if the face is turned at 90 degree to the camera. It is independent of lighting environment and facial expressions.

3.1.3 Surface Texture Analysis: The most advanced method is Surface Texture Analysis (STA). STA does not examine the entire face

but a patch of membrane on it. This patch is divided into separate blocks. The skin surface, the pore on the skin and other face characteristics are converted to a code. This code is used for comparison.

3.2 Recognition algorithms can be divided into two main approaches:

1. Geometric: Is based on geometrical relationship between facial landmarks, or in other words, the spatial configuration of facial features. This means that the main geometrical features of the face such as the eyes, nose and mouth are first located and then faces are classified on the basis of various geometrical distances and angles between features.

2. Photometric stereo: Used to recover the shape of an object from a number of images taken under different lighting conditions. The shape of the recovered object is defined by a gradient map, which is made up of an array of images (Zhao and Chellappa, 2006).

The Viola-Jones algorithm is a widely used mechanism for object detection. The main property of this algorithm is that preparation is slow, but detection is fast. This algorithm uses Haar basis feature filters; so it does not use multiplications.

The efficiency of the Viola-Jones algorithm can be significantly increased by first generating the integral image.

$$ii(y,x) = \sum_{p=0}^{y} \sum_{q=0}^{x} Y(p,q) \qquad (1)$$

Detection happens inside a detection window. A minimum and maximum window size is chosen, and for each size a sliding step size is chosen. Then the detection window is moved across the image as follows:

1. Set the minimum window size and sliding step corresponding to that size.
2. For the chosen window size, slide the window vertically and horizontally with the same step. At each step, a set of N face recognition filters is applied. If one filter gives a positive answer, the face is detected in the current widow.
3. If the size of the window is the maximum size stop the procedure. Otherwise increase the size of the window and corresponding sliding
4. Step to the next chosen size and go to step 2.

Each face recognition filter (from the set of N filters) contains a set of cascade-connected classifiers. Each classifier looks at a rectangular subset of the detection window and determines if it looks like a face. If it does, the next classifier is applied. If all classifiers give a positive answer, the filter gives a positive answer and the face is recognized. Otherwise the next filter in the set of N filters is run.

Each classifier is composed of Haar feature extractors (weak classifiers). Each Haar feature is the weighted sum of 2-D integrals of small rectangular areas attached to each other. The weights may take values ±1. Fig.2 shows examples of Haar features relative to the enclosing detection window. Gray areas have a positive weight and white areas have a negative weight. Haar feature extractors are scaled with respect to the detection window size.

The classifier decision is defined as:

$$Cm = \int_0^1 t, \sum_{t=0}^{hm-1} Fmt > \theta m \qquad (2)$$

Otherwise

$$\text{Fm, i} = \begin{cases} \alpha \\ \beta \end{cases} m, t \text{ , if } fm, t \geq tm, t \qquad (3)$$

Where $f_{m,i}$ is the weighted sum of the 2-D integrals. It is the decision threshold for the *i*-th feature extractor. $\alpha_{m,i}$ and $\beta_{m,i}$ are constant values associated with the *i*-th feature extractor. θ_m is the decision threshold for the *m*-th classifier. The cascade architecture is very efficient because the classifiers with the fewest features are placed at the beginning of the cascade, minimizing the total required computation. The most popular algorithm for features training is AdaBoost.

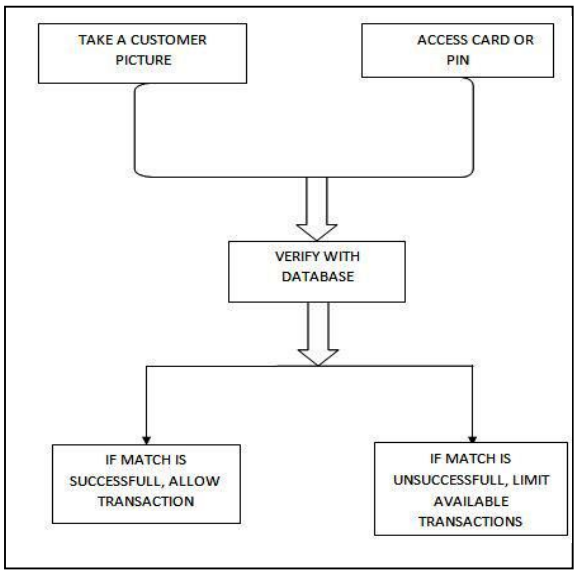

Fig 3: Flowchart of an ATM using ImageProcessing

- Initially the customer's picture is taken when the account is opened and the user is allowed to set non-verified transaction limits.
- At ATM, access card and PIN are used to per verify the user.
- User's snap is taken and an attempt is made to match it to the record image.
- If the match procedure becomes successful, allow the transaction.
- If the match is unsuccessful, limit the available transactions.
- When a match is complete with the PIN but not the imagery, the bank could limit the transactions in a way contracted by the user when the account was opened, and could store the photograph of the user for later examination by the bank official. In the case of using credit card at ATMs, confirmation system would not presently be feasible without revamping the entire credit card issuing industry.

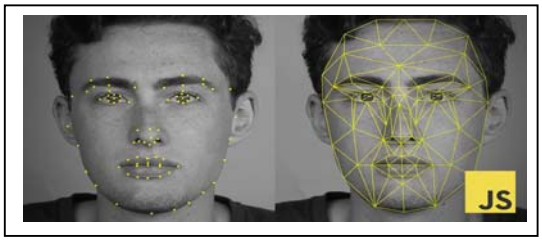

Fig 4: Face Reorganization

4. Experimental Results

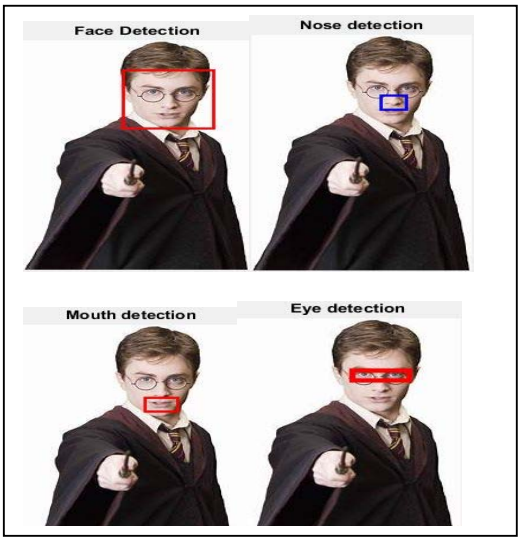

Fig 5: Sample Experimental result for Face, Nose, Mouth and Eyes with Segmentation

The Success rate is evaluated using the following chart. The average value of recognition in terms of face, nose, eyes and mouth is accuracy of each user which is considered for measuring the overall success rate of the proposed methodology. Six sets of supervised classification are demonstrated in the proposed methodology yielding the overall accuracy of around 86.66% which is comparatively better when compared to the state of the art method.

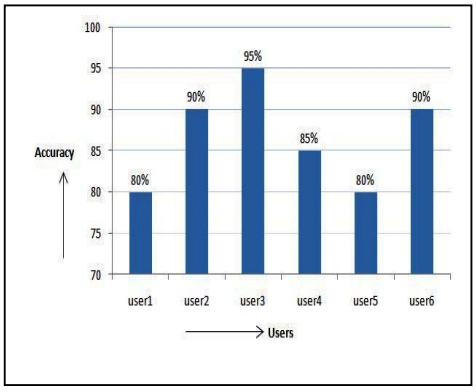

Fig 6: Plot Showing the Success rate

5. Conclusion

Access card / PIN provide insufficient ATM security. Adding facial verification to the process can greatly decrease fraudulent transactions. Current ATM's have the power to perform verification locally, given a software change.

Facial verification software is at present capable up to the task of providing that important match rates for use in ATM transactions. Adding up facial recognition systems to the identity confirmation process used in ATMs can reduce forged transactions to a great extent.

References:

1. Arunkumar, Vasanth Kumar, Naveenly King, Aravindan, "ATM Security using Face Recognition", International Journal of Current Engineering And Scientific Research- Volume-5, Issue-4, 2018.

2. A S Tolba, A.H. El-Baz, and A.A. El-Harby, "Face Recognition: A Literature Review", International Journal of Signal Processing, Volume 2 Number 2, 2014.

3. Divyarajsinh N.Parmar1, Brijesh B. Mehta2, "Face Recognition Methods & Applications", International Journal of Computer Applications in Technology, January 2014.

4. Kresimir Delac, Sonja Grgic & Mislav Grgic, "Image Compression in Face Recognition" - A Literature Survey, October 2008.

5. Mourad Moussa, Maha Hmila & Ali Douik, "A Novel Face Recognition Approach Based on Genetic Algorithm Optimization", https://doi.org/10.24846/v27i1y201813.

6. Priyanka, Research Scholar, Department of Computer Science and Engineering, "A Study on Facial Feature Extraction and Facial Recognition Approaches", International Journal of Computer Science and Mobile Computing, May 2015.

7. T.Suganya, T.Nithya,C.Sunita, B.Meena & Preethi, "Securing ATM by Image Processing"–Facial Recognition Authentication, International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 8, August 2015.

8. Yongzhong Lu, Jingli Zhou, Shengsheng Yu, "A Survey Of Face Detection, Extraction And Recognition", 27 January 2003.

***