Secure Transaction using Face Recognition Technique

L.Saranya[1] S.Srimonika[2] L.K.Shoba[3]
[1,2]Student [3]Assistant Professor
[1,2,3]Department of Information Technology
[1,2,3]Jeppiaar Engineering College, Chennai

Abstract— *Automated Teller Machine (ATM) is one of the convenient approaches for doing transactions. It is easy to carry a single card with multi-account rather than carrying different individual cards. In order to authenticate the multi-account, face recognition technique is used with the help of biometrics. The real time image will be captured by the webcam and it will be compared with the database. If the captured image gets matched with the database image, then it will allow for further process. Authentication is more important for any secret operations and it provides high security and safety to the account.*

Keywords— ATM, Face Recognition, Biometrics, Webcam

I. INTRODUCTION

ATM is one of the automatic systems being used since 1967 by many of us. ATM was invented by John Shepphardbaren on June 1967 at United Kingdom. It first came in India in 1968. The process is, when the user swipes the card, the bar code will be read by the card reader and then asking for PIN.

In modern days, it is very important to integrate multi-account into one card. It is more convenient to use and easy to remember the single passwords for multi-account. But using PIN is not enough for providing security. In order to provide authentication, face recognition using biometrics is used and it is more reliable, non-intrusive, and extremely accurate and in-expensive. It is more secure.

II. BIOMETRICS

sBio(life) & metrics(to measure) is used for measuring and analyzing biological data. It is rapidly evolving technology widely used in forensics security, preventing unauthorized access in bank. It is used to identify individuals by their physical characteristics or personal behavior. Biometrics has three steps:

- Acquiring data
- Encryption
- Analysis of data

It has two modules:

- Database Preparation
- Verification Module

III. LITERATURE SURVEY

Security Experts says that Automatic Teller Machine (ATM) in future will have biometric authentication techniques, in order to verify identities of customer during transaction. In South America, there are companies that have introduced fingerprint technology as a embedded part of ATM systems, where citizens have already started using fingerprint in place of PIN or Password for general identification with their ID cards. India is still lacking in implementing biometric with smart card as a safety approach. Various ideas are given by researchers for biometric authentication including fingerprint, retina, iris, voice, etc. Fingerprint approach for identification given by Oko S. and Oruh J. (2012) not prove efficient as when citizen will move to ATM system, fingers may become dirty fromnaturalne can easily hack and can fraud with another's account. And one more is Signature; sometimes this may be a chance to do forgery. So, this paper came up with an idea called face recognition to calculate the distance between the eyes, nose and mouth, using biometrics.

IV. FACE RECOGNITION

Face recognition specifies specific facial features and it can be measured. Eigen faces categorizing faces according to the degree of fit with a fixed set of 150 master eigenfaces. It is very useful in using active identification. Facial part detection detects the positions of parts like centre of eyes, tip of nose, corner of jaws. Functions of face recognitions are:

A. Acquiring the Image of an Individuals Face; 2 Ways to Acquire Image:

- Digitally scan an existing photograph; acquire a live picture of a subject.

B. LOCATE IMAGE OF FACE:

Software is used to locate the faces in the image that has been obtained.

C. ANALYSIS OF FACIAL IMAGE:

Software measures face according to its peaks and valleys; focuses on the inner area of the face identified as the "golden triangle", valleys are used to create a face print with their nodal points.

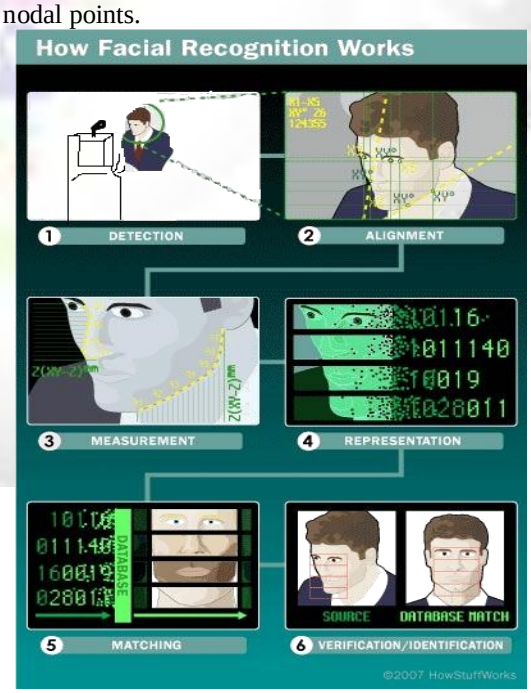

Fig. 1: Face Recognition

D. Comparison:

The face print created by the software is compared to all face prints the system has stored in its database.

E. Match or No Match:

The software decides that whether the image matches or not.

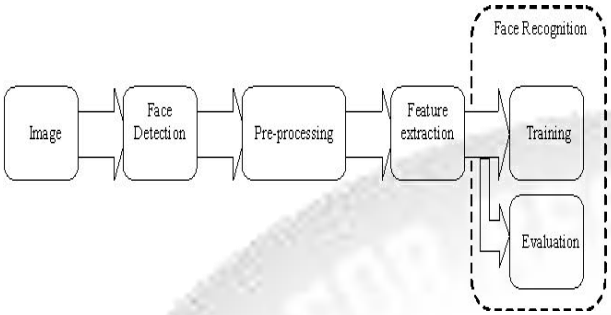

Fig. 2: Block Diagram

V. FUNCTIONS

The functions are:

A. Face Detection:

Face detection and indication of any facial zones that are opposite in various guidelines in complex scene

B. Facial Pose Estimation:

Estimation of the angle to which a face is twisted Facial part detection: The identification of the positions of face parts for example the centre of eyes, tip of nose, and corners of the jaws.

C. Facial trait Classification:

The classification of faces by color, gender, civilization, age, appearance and other character. Face identification: The identification of persons by comparisons with registered people B.

D. Statistical face Recognition:

The face recognition that is most commonly used in commercial applications. The first step is to define a facial pattern of a specific size. Human vision can judge whether or not a face is present even in a low-resolution image made up of 16x16 pixels. This ability does not rely on color, and human eyes will find faces even in a monochrome image, computer process facial patterns using image of about the same size.

1) Detection of Face to Be Scanned:

The system scans the image from top left to bottom right until it finds this pattern.

2) Facial Pattern Classification:

Facial patterns are not easy to define. They vary from person to person, and they also change according to the angle of the face and differences in lighting conditions or facial expressions. To overcome this, it is necessary to formulate functions that allow discrimination between facial and non-facial images by applying statistical methods to large numbers of facial and non-facial images. It is possible to achieve powerful pattern classification performance despite the simplicity of the operation involved.

VI. EXISTING SYSTEM:

In the existing system, finger prints used. It consists of ridges (raised skin) and furrows (lowered skin) that twist to form the distinct pattern. This pattern is different from person to person the fingers may become dirty or oily due to natural environment. Voice recognition, recognizes voice, two persons may have same voices, sometimes illness or cold.

VII. PROPOSED SYSTEM

The system proposes face recognition using biometrics. When the user swipes the multi-account card, the real time image will be captured by using the capture button.

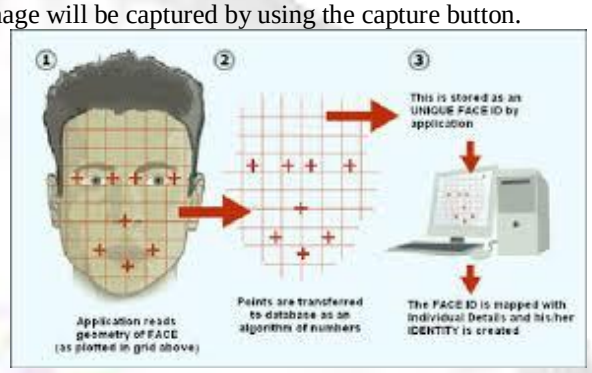

Fig. 3: Process Matching

Then the image is extracted ,then it calculate the distance between the eye, nose and jaws and matched with the stored image by using face recognition algorithm, template based algorithm, current complex algorithm and pattern recognition algorithm .If both the image matches, it will allow for further transaction ,otherwise it will be discarded. After that, it will display a multi-account on the monitor .The users can select the account, meanwhile entering the pin after finishing the face recognition process. Then the user can do the transaction in safe mode. This is more reliable, non-intrusive, extremely accurate, inexpensive.

VIII. CONCLUSION

The paper concludes that face recognition using biometrics, it provides more authenticity. It has a great scope in the future. Authentication with smart cards is a stronger method of authentication and verification as it is uniquely bound to individuals. It is a viable approach, as it is easy to maintain and operate with lower cost. Hence by this method only the authorized person can alone tale the money, strangers or unknown persons cannot access it. In future the same can be enhanced with 3D camera and motion capturing technologies for achieving best results. No one other than the users can use the card.

REFERENCES

[1] Shouvik Biswas , Anamitra Bardhan Roy, Kishore Ghosh, Nilanjan Dey, "A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 4, April 2012.

[2] Renu Bhatia,"Biometrics and face recognition Technique", Department of Computer Science and

Applications, Kurukshetra University, Kurukshethra, Haryana, India.
[3] Adini (2010). Nigerian banks look to biometric ATM machines to reduce fraud.
[4] George Webster (2010). Biometric ATM gives cash via facial recognition scan. Http://edition.cnn.com. accessed October 10, 2012.
[5] Ladislav Lenc, Pavel Král: Two-step supervised confidence measure for automatic face recognition. MLSP 2014: 1-6
[6] Ladislav Lenc, Pavel Král: Automatic Face Recognition - Methods Improvement and Evaluation. ICAART (1) 2011: 604-608
[7] Blackburn, Duane M. Face Recognition 101: A Brief Primer. Department of Defense Counterdrug Technology Development Program Office. 07 April 2003. Available: http://www.frvt.org/DLs/FR101.pdf.
[8] Jenkins, R. and A. M. Burton. "100% Accuracy in Automatic Face Recognition." Science. 319.5862: 435-435.
[9] "German casinos secured with facial recognition." Biometric Technology Today. 14.11/12: 12.