International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

Securing ATM by Facial Recognition Authentication

P. Muniasamy[1], S. Joney Babayal[2]

[1,2]Assistant Professor in Computer Science, Ayya Nadar Janaki Ammal College, Sivakasi

Abstract: ***With the support of ATM, though banking becomes easier, it also became feeble. There has been countless gear of abuse that have in use in banking transactions. Thus there is a essential need to provide high security. This paper proposes the amalgamation of Face Recognition System in the identity verification process engaged in ATMs to enhance the security system.***

Keywords: ATM System, Face Recognition Software (FRS), Security

1. Introduction

The rise of technology bring into force loads of types of tools that aspire at more customer pleasure. ATM is a machine which made money transactions effortless for customers. But it has both advantages and disadvantages. Current ATMs make use of naught more than an access card and PIN for uniqueness confirmation. This has ATM Using Face Recognition System demonstrate the way to a lot of fake attempt and mistreatment through card theft, PIN theft, stealing and hacking of customer's account details and other part of security.

2. What Are Face Recognition Systems?

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

3. When Did They Develop?

The pioneer of robotic Face Recognition includes Helen Chan Wolf, Woody Bledsoe and Charles Bisson. During 1964 and 1965, Bledsoe, all along with Helen Chan Wolf and Bisson, 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, slight work was published. Given a large database of photos and images, the trouble occurred 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 first and foremost by Peter Hart. Peter's experiment done on a database contains over 2000 images, the computer eternally outperformed humans when presented with the same detection tasks. The enlargement period for facial recognition started in the delayed 1980s and they were existing systems was made accessible in the 1990s.

4. How do they Work?

A database of people's face is maintained by the system that handles face detection. When a face needs to be predictable a snap of the one's look is taken and evaluated to the appearance present in the database to observe if a match is found. There are typically 3 parts related to a face recognition system

- Face detector,
- Eye localizer and
- Face recognizer

1) The face detector
The face detector spot the face, eliminating any other detail, not related to the face (like the backdrop). It identifies the facial region and leaves the non-facial region in the photo of the person to be identified.

2) The eye-localizer:
It finds the spot of the eyes, so that the position of the face can be identified better.

3) The recognizer:
It will check the database to find a match.

5. Algorithm for Face Recognition Systems

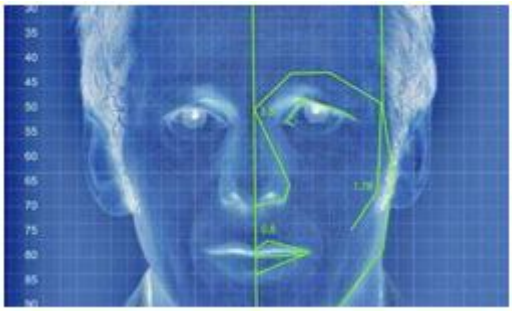
Various facial recognition algorithms be familiar with faces by extracting features, from a snap of the subject's face. For example, an algorithm may examine the size, relative position, in addition to/or outline of the nose, eyes, cheekbone and jaw. These facial appearances are then used to search for other imagery across matching features. Other algorithm manages a balcony of face images and then compresses the image's face information and it saves only the data in the image that is used for face detection. A searched image is then compared with the face record.

Face Recognition Systems algorithms is alienated into two main approaches namely

- Geometric based
- Image-template based.

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 self-governing of lighting environment and facial expressions.

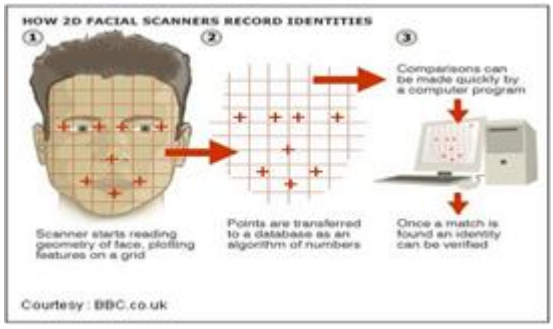


Surface Texture Analysis
The most superior method is Surface Texture Analysis (STA). STA does not examine the entire face but a patch of membrane on it. This patch is divided into separate blocks. The skin surface, the pore on the skin and other face characteristics are converted to a code. This code is used for comparison.

6. Techniques and Methods

They are of three types
- 2-D,
- 3-D
- Surface Texture Analysis.

a) 2-D Technique
The 2-D recognition method was individual 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 precise. Change in facial expression or difference in ambient lighting on a appearance that is not directly looking into the camera did not produce expected results.



b) 3-D Technique
Progression in face recognition gave origin to the 3-D recognition system. This stepped up technique, used facial

7. ATM (Automatic Teller Machine)

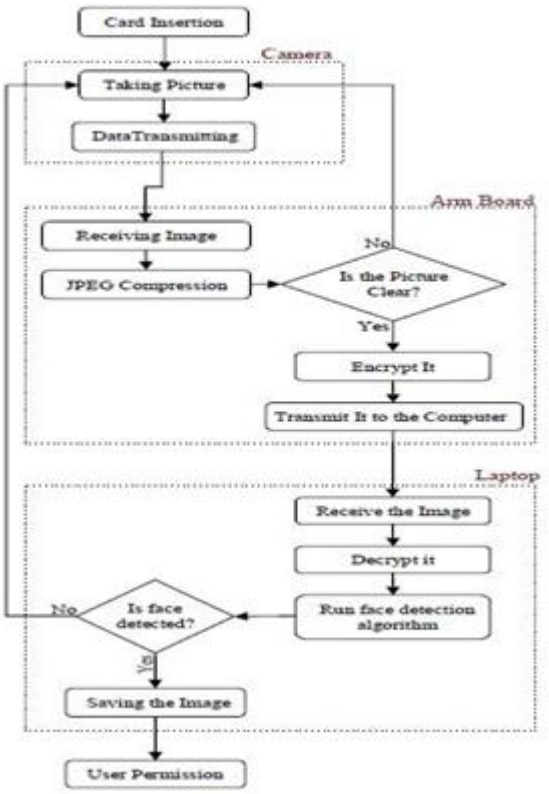
For the past ten years, the bulk of ATMs used worldwide ran under IBM‟s now out-of-date OS/2. Movement in the banking world is now going on using Windows and Linux. A leading world-wide ATM manufacturer, NCR currently announced an harmony to employ Windows XP Embedded in its next generation of personalized ATMs. For fewer influential ATMs, KAL, a software development company based in Scotland, gives Kalignite CE, which is a modified version of Windows CE platform. This platform allows developers that target older machines to more easily build up multifaceted user-interactive systems. Many financial institutions are having a third choice, Windows NT. It is because of its maturity and stability as a platform. On an alternative, the largest bank in the south of Brazil, Banrisul, had installed a custom version of Linux in its put of two thousand ATMs, replaces legacy MS-DOS systems. In these types of ATMs, it sends database requests to bank servers which do the bulk of transaction processing.

8. Working of FRS in ATM

Face Recognition Systems (FRS) labor in ATMs in the following way

- Initially the customer's picture is taken when the account is open and the user is allowed to set non-verified transaction limits.
- At ATM, access card and PIN are used to pre-verify 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 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 granted upon by the user when the account was opened, and could store the photograph of the user for later examination by bank official. In the case of using credit card at ATMs, confirmation system would not presently be feasible without creating a repair for the entire credit card issuing industry.



Working of FRS in ATM

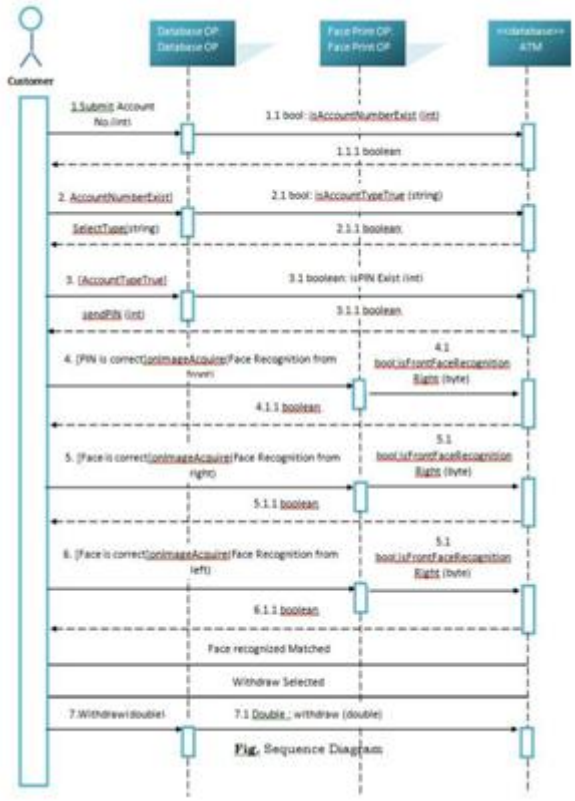


Fig. Sequence Diagram

9. 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 allowing 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 are functioning properly, they will be tweaked as much as potential to increase performance (decreasing the time used up matching) and to decrease memory footstep.

Following this, the black boxes will be broken into two parts – a server and a client – It is done to use in a network consist of two-machine. The client code will act as a user interface, which is passing all input data to the server code. It will handle the calls to the facial recognition software (FRS), further reducing the buffer footstep and processor load essential on the customer end. The black box program is used to control a USB camera which is attached to the computer. It is done to avoid the use of the folder of "live" images. At last, it may be possible to add some sort of encryption to the client end to encrypt the input and decrypt the output from the server – knowing that it will boost the processor load, but better allowing us to measure the time it takes for processing.

10. Key Factors To Be Considered

There are certain factors that affect process of support. They are

1. Lighting
2. Extreme facial expressions
3. Angle of view
4. Facial hair
5. Glasses

Other concerns are keeping the time beyond in the verification process to a small amount, allowing for an suitable level of variation in a customer"s face when compared to the database photograph, and the credit cards that can be used at ATMs to withdraw funds are generally provided by institutions, these institutions do not have personally contact with the customer, and hence no chance to acquire a photo. The last concern is that consumers may be wary of the privacy concerns raised by maintaining photographs of customers in a bank record, encrypted orelse, due to possible hacking attempts or employee abuse.

11. Can All ATMs Support FRS?

Most recent generation ATMs support Windows CE, 2000, XP Embedded, or Linux – these machines can also support facial recognition software locally elder ATMs run DOS or OS/2 – these machines can offload the processing to the bank‟s computers. As we have seen before both Local Feature Analysis (LFA) and Principle Feature Analysis (PFA) programs have handle changes in lighting well. This is significant because ATM is active every 24 hours, with or without artificial illumination. Verification rates can be as elevated as 90% when the factors that affect facial recognition systems are taken care of.

12. Advantages and Disadvantages

Advantages

- Verification rates as high as 90% have been attained when face recognition system had used in ATMs.
- It has been used to strengthen security.
- It can be used to reduce fraudulent attempts.
- The procedure used in Face Recognition Systems handle the changes in the light effectively. This is important since ATM use occur day and night, with or without fake light.
- With appropriate lighting and strong learning software, slight variations in the images could be accounted for.
- Positive visual match would cause the existing picture to be stored in the record so that future transactions would have a broader foot from which to compare if the original account photograph fails to provide a match.
- When a match is complete with the PIN but not the imagery, the bank could limit the transactions in a way granted upon by the user when the account was opened, and could store the photograph of the client for later examination by bank official.
- In regards to bank staff gaining access to customer PINs for use in fraudulent transactions, this system will reduce the threat to contact to the low limit forced by the bank and agreed to by the user on visually unverifiable transactions.

Disadvantages

- Not identifying people correctly even if their photo is in the database. Changes in lighting and expressions like scream expressions, squinted eyes, changes in disguise like wearing hats; glasses drop recognition rates significantly even though the user is a genuine account holder.
- Matching profile changes worked reasonably well when the first guidance image(s) were frontal, which allowed 70-80% success rates for up to 45 degrees of profile change however, 70-80% achievement isn‟t amenable to keeping ATM users content with the system.
- Consumers may be cautious of privacy concerns raised by maintaining images of clients in a bank database, encrypted or else, due to feasible hacking attempts or employee abuse.

13. Conclusion

Facial verification software is at present up to the task of provided 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] Penev and Atick, Joseph J. “Local Feature Analysis: A General Statistical Theory for ject Representation.” Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477-500, 1996.
[2] Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. “Quo vadis Face Recognition.” Third Workshop on Empirical Evaluation Methods in Computer Vision. Kauai: December 2001
[3] Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane.
[4] “Evaluating Facial Recognition Technology for Drug Control Applications.” ONDCP International Counterdrug Technology Symposium: Facial Recognition Vendor Test., June 2001.
[5] S. Sruthy. "Literature Survey Automated Person Identifica-tion Techniques." (2013).