International Journal of Engineering & Technology, 7 (2.33) (2018) 484-490

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Two- way authentication system for ATM

Emad Afaq Khan [1] *, Dr. Sumaira Muhmmad Hayat Khan [2]

[1] Asia Pacific University, Malaysia
[2] Department of computer science,Asia Pacific University, Malaysia
**Corresponding author E-mail: Sumaira@apu.edu.my*

Abstract

This electronic document is research-based project that involves the use facial recognition in ATMs. This idea is not quite popular as in some points the facial recognition still lacks in credibility. This paper involves the research and the implementation phase of the facial recognition for ATM banking.

Keywords: *Facial Recognition; Eigen Faces; Image Attributes*

1. Introduction

The face recognition will be a useful and safe way for the ATM transactions as it will eliminate all the tools of security and authentication and will be more secure and time saving. It can be seen on a much larger scale too like law and enforcement, entertainment and personal security etc.
But overall, the face recognition system and its problems with algorithms will be stated with the literature review as a part of the problem statement.
Security Experts says that Automatic Teller Machine (ATM) in future will have biometric authentication systems to confirm characters of customer amid transaction. In South America, companies have presented fingerprint innovation as an embedded part of ATM frameworks, where subjects have already started utilizing fingerprint as a part of place of PIN or Password for general identification with their ID cards. Rowley [1] said, "Banks will move to smart cards and biometric will be next step after that ". Bank has already been moved to smart cards and this is the ideal opportunity to execute biometric authentication approach in ATM frameworks. Nowadays, there are gadgets to perform biometric identification and authentication of taking after: fingerprint, hand, retina, iris, face, and voice. Rowley [1] also mentioned that most insecure is a magnetic stripe with a PIN, more secure is a smart card with a PIN, and even more secure is a smart card with biometrics. India is also lacking in executing biometric with smart card as a safety approach.
Various ideas are given by researchers for biometric authentication including fingerprint, iris and retina, voice, and so on. Fingerprint approach for identification given by Oko S. and Oruh J. [2] was not demonstrated effective as when resident will move to ATM framework, fingers may become messy from natural environment and will not be able to access his account with ATM framework, since fingerprints will not match from the case that was traced amid identification.
Furthermore, an iris and retina approach proposed by Bhosale S. and Sawant B. [3] as an identification technique, however subjects may not want a laser beamed into their eyes for retina scan at each time he wants to access account through ATM. Along these lines, iris and retina as identification authentication demonstrated wasteful. Ajaykumar M also proposed vibration detector sensor as a security framework for ATM machines. and Bharath Kumar. Voice was also proposed for security in ATM frameworks as a biometric with smart card. The cons arrived at the same time as two residents can have same voice and one can easily hack and can fraud with another's account. Along these lines, this paper came with an idea of face acknowledgment system with 3 unique angles as a biometric authentication that cannot be lost, stolen, harmful, grimy, duplicated, forgotten and is always available. Subsequently, biometric gadget is ultimate attempt in attempting to demonstrate who you are.
The conclusion driven from the above-mentioned research is that the face recognition will play an important role for the ATM banking and will make it safer. The flexibility within the system will be an option to whether use face recognition as standalone or with the combination of the security tool like the card and its pin. Both functions will consider in the proposed system that will provide ease to the users depending upon their situation and priority.

2. Related work

In this section, some of the similar system and some of the approaches made by different organizations will be mentioned for the readers to have a clear idea on where this project is going and what similarities are there among these systems. The basic technology found in the all these similar systems is the use of facial recognition technology.
According to Department of Social Services, in US, the policing for the welfare benefits is being tested through facial recognition where the newly registered applicants are compared to the existing database to find out if they are not claiming under more than one identity.
But it has been observed that the facial recognition is not working well among the millions of people stored in the database therefore they have performed some demographics to narrow down the search and make it more reliable. In this area, an iris or fingerprint technology will be more suitable but to make the system more acceptable and intrusive, facial recognition technology is used. States like Illinois, have implemented facial recognition to minimize the people from obtaining multiple driving licenses.

Copyright © 2018 Emad Afaq Khan, Dr. Sumaira Muhmmad Hayat Khan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2.1. Facial surveillance

The domain where most enthusiasm for face recognition is being indicated is likely surveillance. Video is the medium of decision for surveillance considering the extravagance and kind of data that it contains normally, for applications that require recognizable proof, face recognition is the best bio-metric for surveillance. Although gait or lip movement recognition have some potential.
One of the greater advantages for the use facial recognition technology in this domain is that the user participation is not required. And the recognitions can be made for the organizations to achieve a positive goal. [5]
This system is already deployed in the United States but there is one drawback, that is the accuracy of the system is not consistent. The technology in this domain is being improved day by day and involves steerable cameras, invisible wavelengths and ASP (advance signal processing) for the collection of valid information through surveillance systems. [6]

a) NeoFace Reveal

NeoFace Reveal is an Advanced Criminal Investigative Solution Using Face Recognition Technology. NEC came up with a NeoFace Reveal is a workstation that helps reduce the investigation time. It deals with the facial video evidence and makes the investigator spend less time. Another favorable position of NeoFace Reveal is its fast preparing of facial confirmation combined with its capacity to produce persons of premium rundown examination quickly after the crime has occurred. This point of interest permits investigators recognizes a suspect before the suspect leaving the community, state or nation. NeoFace Reveal demonstrates a prompt quantifiable profit for clients. It lessens examination time and examiner workload. The arrangement transforms the already unusable pictures into hard proof to unravel crimes. [7]

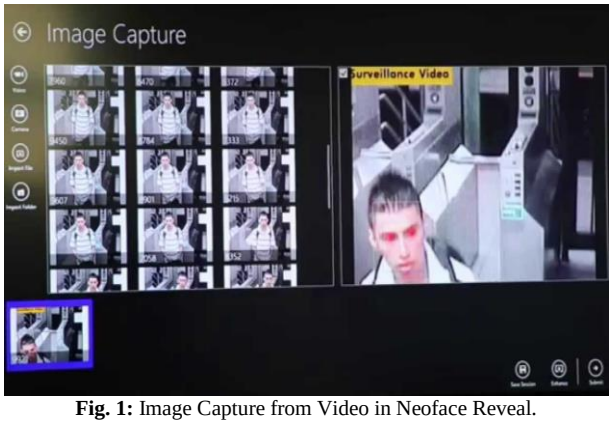


Fig. 1: Image Capture from Video in Neoface Reveal.

b) SekuFace

SekuFace is a product designed and created by Eurotech. It is a high-end IP based system that recognizes face with submissive privacy constraints that matches the performance levels present in the current market of facial recognition. [8]
The product is applicable in many fields that are mentioned below but still lacks some of the departments where there is a need for facial security.

- Residential areas
- Private and public buildings
- Security and Surveillance Systems

This software also allows the users to cross check the identities and their related info that has been stored. The records of the users are deleted once the operation is completed thus keeping the privacy policy alive.

Fig. 2: Seku Face System (Similar to Atms).

c) ATM with Facial Recognition in China

Facial recognition use in ATMs has been tried for some time now, however China appears to have won the race to reveal the first completely functional system to the overall population. A group of college and innovation organization analysts in China presented an ATM with implicit facial recognition technology, which will in a perfect world diminish the danger of unlawful withdrawals.
This ATM has built in cameras for capturing the user's identity and later match with the existing database. [9]
But this facial technology is an added layer over the normal ATM and basically is not implemented in whole of china but rather is a prototype on a small scale. To improve more security, it will be linked to nearby police stations for higher security.

Fig. 3: Shows the Facial Recognition System in ATM created in China with A Small Section Showing the Camera View.

3. Proposed technique

The system will involve the integration of Facial Recognition along with the ATM. Thus, the breakdown of the domain research

is the advancement in the Facial Recognition and the application of this field with the ATM.
Recognition of faces is something that individuals as a rule do easily and without much familiar thought, yet it has remained a troublesome issue in the zone of AI and IT, where nearly 20 years of exploration is simply starting to yield helpful mechanical arrangements. As a biometric technology, automated face recognition has various attractive properties that are driving examination into useful procedures. The issue of face recognition can be expressed as 'recognizing a person from images of the face' and includes various varieties other than the most commonplace use of mug shot ID. One striking part of face acknowledgment is the expansive interdisciplinary nature of the enthusiasm for it: Every data medium that is utilized for face recognition conveys power to specific conditionsAll paragraphs must be justified alignment. With justified alignment, both sides of the paragraph are straight.
One of the disadvantages of the facial recognition is a low accuracy rate and especially when it is compared to another biometrics performance of fingerprint and iris.
Last but not the least, the variability of the image. Different attributes of the face add up the complexity of the image and causes failure in the process of recognition and this problem cannot be avoided even after a careful design of the system. Inadequate constraint or handling of such variability inevitably leads to failures in recognition (IBM Watson Research Center). Following is the elaboration of the attributes causing failure:

3.1. Physical attributes

Facial Expressions, facial expression change; aging; personal appearance like make-up, glasses, facial hair, hairstyle, disguise. This sums up that the physical attributes are dependent on many attributes.

3.2. Attainment geometry attributes

This involves the changes in scale, location and the in-plane rotation of the face that will be facing the camera and the depth involved like facing the camera indirectly or maybe half frontal face.

3.3. Imaging changes

Depends on the variable illumination, camera instability or different characteristics channel (especially in broadcast, or compressed images).

Fig. 4: Illustration of Image Changes.

There is a great assorted quality in the way facial appearance is translated for recognition by an automatic framework. Right now, various diverse frameworks are being worked on, and which is most appropriate and may rely on upon the application domain. A major contrast in approaches is whether to speak to the appearance of the face, or the geometry. Brunelli and Poggio [10], have compared these two approaches, at the end of the day most frameworks today utilize a combination of both appearance and geometry. Geometry is hard to measure with any accuracy, particularly from a solitary still image, however gives more robustness against disguises and aging. Appearance information is readily obtained from a face image, however is more subject to superficial variation, particularly from posture and demeanor changes. In practice for most purposes, even appearance-based frameworks must estimate some geometrical parameters with a specific end goal to infer a "shape free" representation that is free of expression and posture artifacts. [11] This is achieved by discovering facial landmarks and warping the face to a canonical neutral posture and expressions. Facial features are also important for geometric approaches and for anchoring local representations.
Face appearance representation plans can be partitioned into local and global, contingent upon whether the face is spoken to in general, or as a progression of small areas. Most global approaches are based on a principal components representation of the face image intensities. This representation plan was contrived first for face image pressure purposes and along these lines utilized for acknowledgment purposes. [12]
The latter instituted the term Eigen faces for this sort of representation. A face image is spoken to as a vector of intensities and this vector is then approximated as a total of basis vectors (Eigen faces) registered by principal component analysis from a database of face images. These principal components speak to the typical variations seen in the middle of faces and give a compact encapsulation of the appearance of a sample face image, and a basis for its comparison with other face images. This principal component representation is like, for example, the Fourier transform, a decorrelation transforms to an alternative basis where great representation of the salient characteristics of an image can be created from just a couple low-arrange coefficients in spite of discarding many of the higher-request terms.

3.4. Eigen faces

One of the methods for the recognition is the Eigen face method. Turk and Pentland [12] started using the PCA technique that acted as the feature vectors for the solving problem related to facial recognition. The used the Euclidean distance for the similarity function. This was later derived as the Eigen Face.
It is adequate and productive technique to be utilized as a part of face recognition because of its straightforwardness, speed and learning capability. Eigen faces are a set of Eigen vectors utilized as a part of the Computer Vision issue of human face recognition. They allude to an appearance-based approach to face recognition that looks to capture the variation in a gathering of face images and utilize this information to encode and compare images of individual faces in a holistic manner. [13]
The Eigen faces are Principal Components of a distribution of faces, or equivalently, the Eigen vectors of the covariance matrix of the set of the face images, where an image with N by N pixels is considered a point in N 2-dimensional space. Past work on face recognition overlooked the issue of face boost, if predefined measurement was relevant and adequate. This proposes that coding and decoding of face images may give information of face images emphasizing the significance of features. These features may or may not be related to facial features, for example, eyes, nose, lips and hairs. We want to extract the relevant information in a face image, encode it proficiently and compare one face encoding with a database of faces encoded similarly. [12]
A basic approach to extracting the information content in an image of a face is to by one means or another capture the variation in an accumulation of face images. We wish to find Principal Components of the distribution of faces, or the Eigen vectors of the covariance matrix of the set of face images. Each image location adds to each Eigen vector, with the goal that we can display the Eigen vector as a sort of face. Each face image can be spoken to exactly as far as linear combination of the Eigen faces. According to Pankaj and Majhi [14], the quantity of conceivable Eigen faces is equal to the quantity of face image in the training set. The faces can also be approximated by using best Eigen face, those that have the largest Eigen values, and which therefore account for most variance between the set of face images. The primary reason for using less Eigen faces is computational productivity.

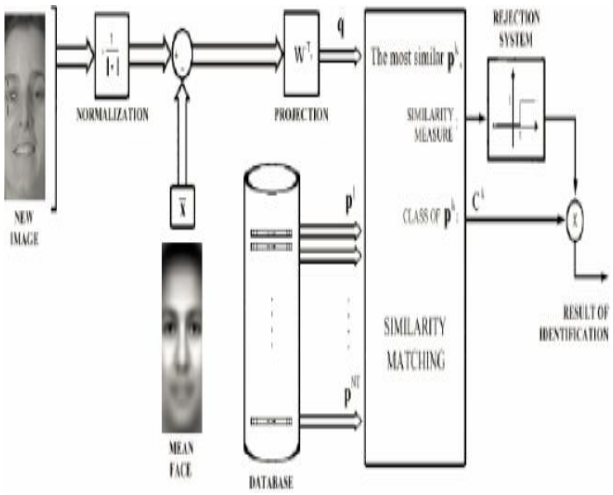


Fig. 5: Eigen Face Technique Flow of Detection.

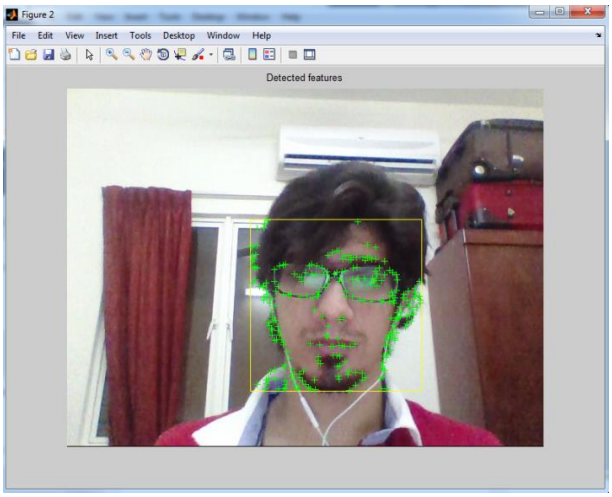


Fig. 7:.Facial Features Detection.

3.5. Matching

Having prepared a face and extracted the features, these are put away or transmitted as a facial code (face template), which can be as small as 84 bytes. [15] For each representation sort, a distance or similarity measure is characterized that allows "similar" faces to be resolved.

A significant part of the art in biometrics is in the configuration of a model of the biometric data and, given a plan for extracting the model parameters as a representation of the data, in creating a similarity measure that effectively discriminates between samples from the same individual and samples from diverse individuals. As with any biometric framework, some limit on similarity must be picked above which two face images are regarded to be of the same individual. Altering the limit gives diverse False Accept and False Rejection Rates — trading the coincidental against the other relying upon the security level required. This is a trade-off between comfort and security is easy to use for matchers to have a low false reject rate, while secure matchers have a low false accept rate. Based on the above-mentioned analysis an example for the matching process is illustrated in the given picture below:

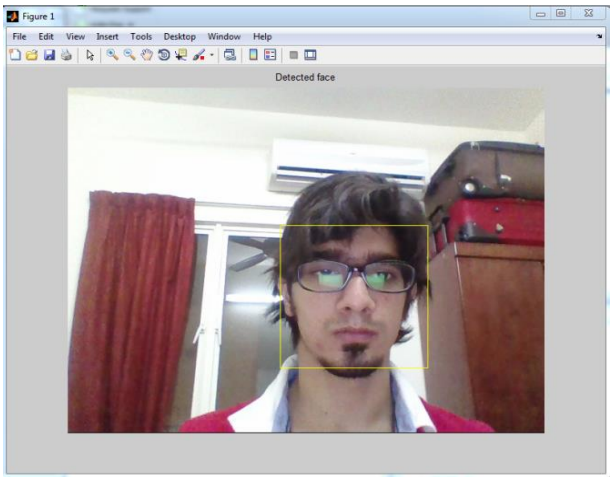


Fig. 6: Facial Detection.

The picture above is a sample screenshot of a facial detection on a camera. A rectangular box shows the confirmation of the face detected. This is a sample that has been taken from the past project of the researcher which will also be used in the system architecture chapter for further elaboration of the project.

Based on different algorithms, the features of the face like ears, nose, eyes and chin etc. are traced and the correctness of the algorithms and the mathematical functions will define the efficiency and accuracy of the program. All these features will be put in the form of datasets and later used for matching process in the database.

Fig. 8: Conversion of the Trained Face in Grayscale.

Pictures captured will be later saved in grayscale formats hence taking one step closer for the matching process.

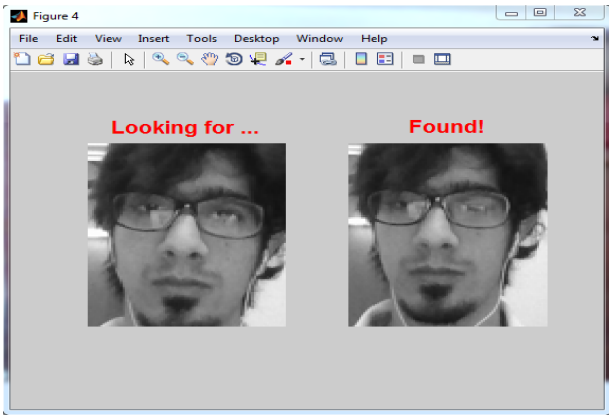


Fig. 9: Matching Process.

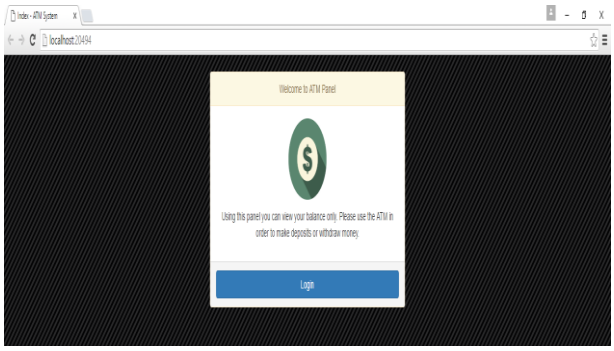
The subject is captured by the system and all its extracted features are later calculated and passed through the matching process where it is compared to the existing database of the users.

4. Experimental results

The proposed system has been developed using a variety of technologies including C#.Net, WPF, SQL Server, Entity Framework, and ASP.Net MVC. The major justification behind selection of all these technologies is since all of them are from Microsoft and for that purpose the best matches each other. In other words, the compatibility between these technologies are very high which can be regarded as the main justification behind their selection. As previously stated earlier in this paper, the major purpose of the system is to allow for facial authentication in ATM machines. This function can be regarded as a very challenging function to create with respect to the fact that it involves extreme artificial intelligence concepts. To effectively implement the facial recognition, a framework known as Luxand has been used which provides the basic tool for implementing facial authentication. In this process, the images of customers are maintained in the system's database in a way that a customer can have various images in order to maximize the precision of the system based on various lighting, angles, or white balance. Through buffering all images belonging to a specific customer, the facial scanning tries to match the images and it will stop upon encountering the first successful match. Accordingly, the system has been provided with two sections of which one of them is the ATM machines simulator and the other is a web application that allows systems admins to administer the system, and customers to do basic tasks such as monitoring their balance. The following sections of this chapter will provide more information in respect of the implementation of the system.

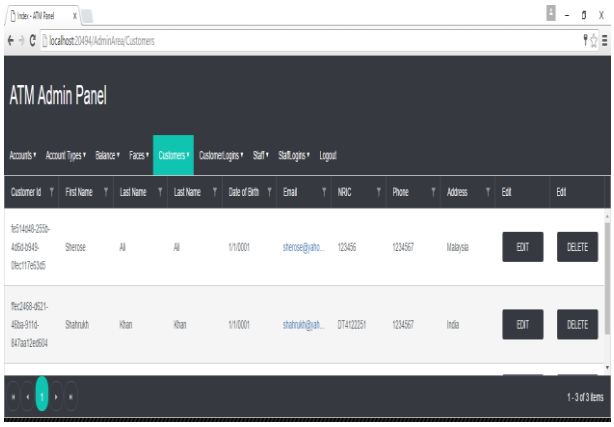
4.1. Web-end

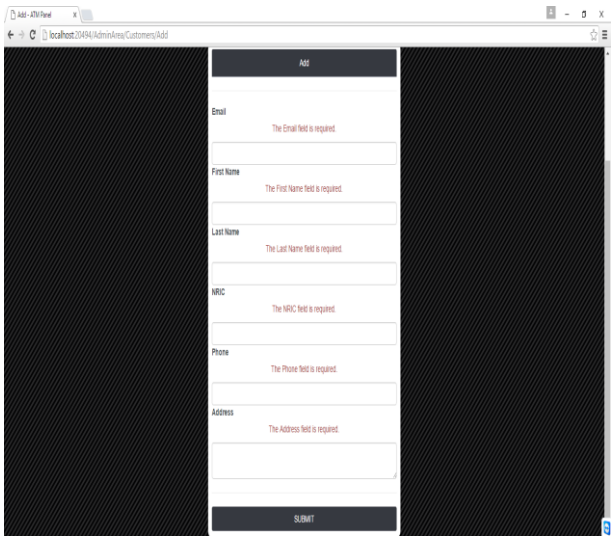
This end of the system consists of two different sections which are respectively the Admin and Customer panel. These two panels respectively allow system admins to control the flow of data into the system as well as being able to view and query all data, and the customer panels allows customer to view their transactions and deposits.

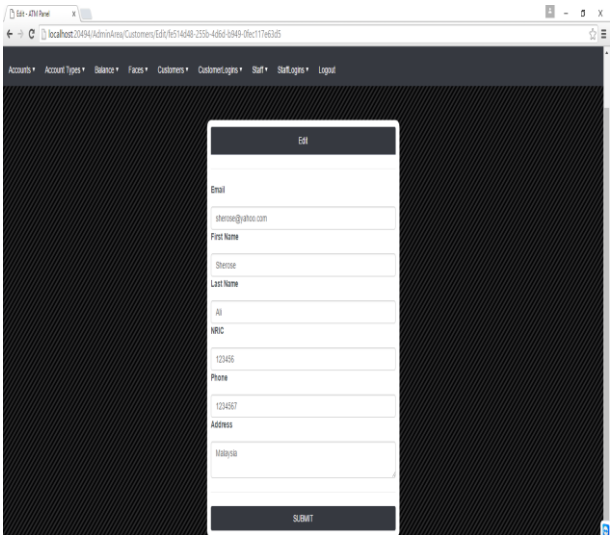


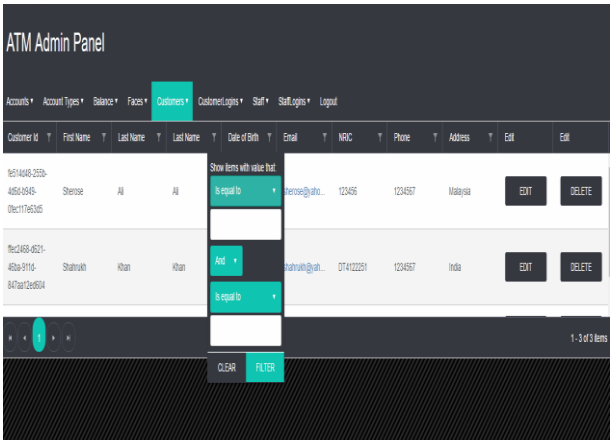
4.2. Admin panel

As previously explained earlier, using this area of the system, admins can add, remove, edit, view, and search all data in the system. The forms provided in this panel are fully validated in the client side to prevent any inconsistencies in the system. Furthermore, the grid views have been provided with advanced filtering functions allowing for fine searching in the system. The following provide an example of the implemented admin panel



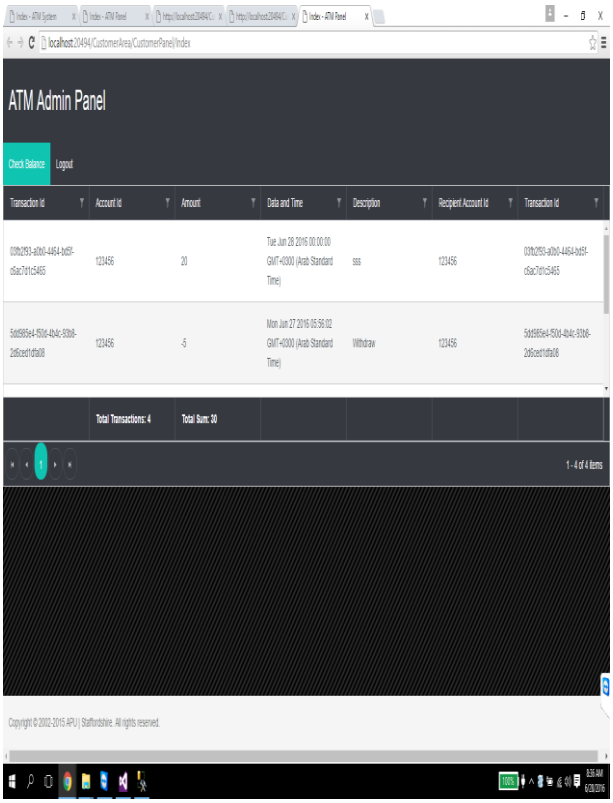






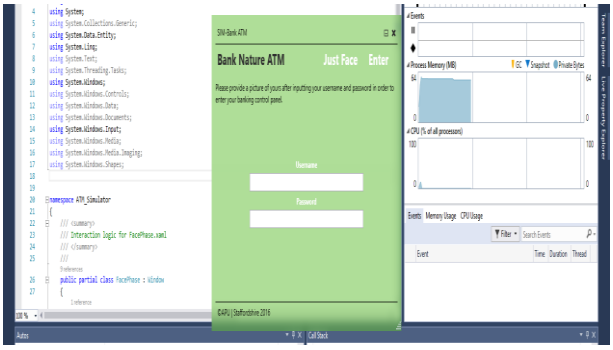
4.3. Customer panel

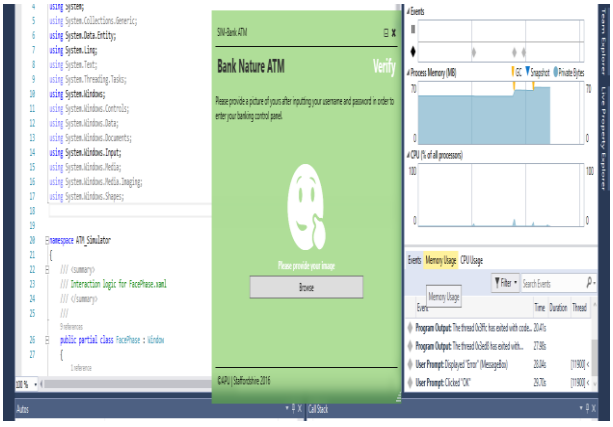
As previously explained, this section of the system allows customers to view their transactions in the system. However, they can refer to the ATM section to make transactions or deposits, pay bills, or chance their password

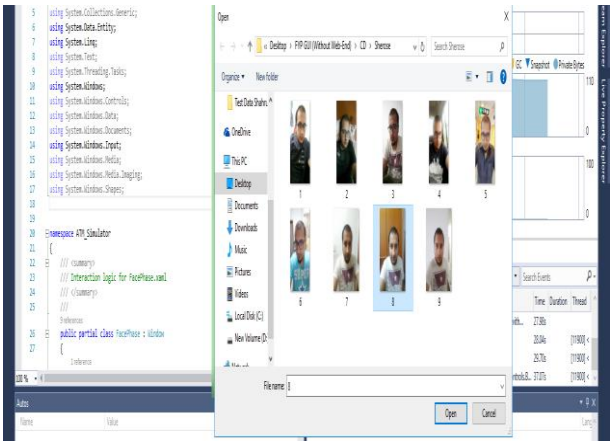


4.4. ATM end

Using this area of the system, customers can login to the system through facial authentication and use their banking accounts. This section of the system allows for two different types of authentication which are respectively two step authentications with both password and facial recognition, and logging in using only facial authentication. In both these processes, the user requires to provide an image of themselves to be authenticated.







4.5. Main panel

The main panel of the ATM simulator allows for functions such as making transfers and deposits, viewing balance, withdrawing money, changing passwords and paying bills

5. Conclusion

After all the researches and fact gathering on facial recognition it was time to study the ATMs because it is the place where the researcher wants to implement it. This system idea is not quite popular as in some points the facial recognition still lacks in credibility, but the challenge was accepted and now only the coding stage is left. The has planned to make two sub systems where registering and ATM transactions will take place. This is the biggest challenge in this project. Implementation of these two technologies will later result in a very good outcome for the people/ target market.

The literature review for the project was made with really good care and it was made sure there are no missing links. Overall, to conclude this the researcher is happy in doing this project and it became possible only because of the knowledgeable and kind supervisor. Every stage of this Investigation report was well observed by her and it was made sure by her that the project is going in the right direction. I would like to give her my heartiest thanks for the support.

Last but the not the least, parents played a great role and it is because of their prayers that this investigation report is now completed.

Designing and developing a facial authentication mechanism can be regarded as one of the most difficult and most complex areas of programming which not only mandates advanced knowledge programming, but also requires adequate knowledge of artificial intelligence. Accordingly, the project has been full of puzzles and problems, which have been worked out through contentious investigation about the topic followed by brainstorming the findings in order to determine the best and most efficient approach for discovering a proper solution. Through reviewing and studding the available literature, the fundamental information for concluding the solution has been obtained. Through analyzing the findings comprehensively, the final solution has been determined. The solution underwent implementation and heavy testing, and this can be regarded to which the project owes its success. The final software has been successfully evaluated by the end-users implying that it can enter the release phase to be used in a real-world environment.

References

[1] Rowley, Gregg. 'ATM Security'. The Australian News 2011: n. pag. Print.

[2] Prof. Selina Oko and Jane Oruh, "ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012

[3] S.T. Bhosale and Dr. B.S.Sawant "SECURITY IN E-BANKING VIA CARD LESS BIOMETRIC ATMS", International Journal of Advanced Technology & Engineering Research, Volume 2, Issue 4, July 2012.

[4] Archana et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(10), October - 2013, pp. 261-266

[5] Lee Gomes. Can Facial Recognition Help Snag Terrorists? The Wall Street Journal, September 21 2009.

[6] Defense Advanced Research Projects Agency. Human Identification at a Distance, BAA00-29 edition, Feb 2009. URL: http://www.darpa.mil/iso2/HID/BAA0029

[7] NEC, Necam.com. N.p., 2015. Web. 25 Nov. 2015.

[8] eurotech,. 'Sekuface: Biometric Face Recognition System Eurotech'. Eurotech.com. N.p., 2015. Web. 25 Nov. 2015.

[9] J.-H. Lee and W.-Y. Kim, "Video Summarization and Retrieval System Using Face Recognition and MPEG-7 Descriptors," in Image and Video Retrieval, Vol.3115, Lecture Notes in Computer Science: Springer Berlin / Heidelberg, 2004, pp.179-188.

[10] Roberto Brunelli and Tomaso Poggio. Face Recognition: Features versus Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(10):1042–1052, October 1993.

[11] Ian Craw and Peter Cameron. Face Recognition by Computer. In David Hogg and Roger Boyle, editors, Proceedings of the British Machine Vision Conference, pages 498–507. Springer Verlag, September 1992.

[12] M. A. Turk and A. P. Pentland. Eigenfaces for Recognition. Journal of Cognitive Neuroscience, 3(1):71 – 86, 1991.

[13] Anil K. Jain, Robert P.W. Duin, and Jianchang Mao. Statistical Pattern Recognition: A Review. IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1):4 – 37, January 2000.

[14] Sunita Kumari, Pankaj K. SA, and Banshidhar Majhi. Gender classification by principal component analysis and support vector machine. In ACM International Conference on Communication, Computing & Security, ICCCS 2011, pages 339 – 342, Rourkela, India, February 2011. Privacy:

[15] H. Moon, "Biometrics Person Authentication Using Projection-Based Face Recognition System in Verification Scenario," in International Conference on Bioinformatics and its Applications. Hong Kong, China, 2004, pp.207-213.