Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 45 (2015) 390 – 396

Procedia Computer Science

International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

Enhanced security for ATM machine with OTP and Facial recognition features

Mohsin Karovaliya[a], Saifali Karedia[b], Sharad Oza[c], Dr.D.R.Kalbande[d]

[a]*Computer Engineering Department, Sardar Patel Institute of Technology, Mumbai 400058, India*
[b]*Computer Engineering Department, Sardar Patel Institute of Technology, Mumbai 400058, India*
[c]*Computer Engineering Department, Sardar Patel Institute of Technology, Mumbai 400058, India*
[d]*Professor,Computer Engineering Department, Sardar Patel Institute of Technology, Mumbai 400058, India*

Abstract

The purpose of this paper is to reinforce security of the conventional ATM model. We have posited a new concept that enhances the overall experience, usability and convenience of the transaction at the ATM. Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This completely eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

Keywords: PCA; OTP; eigenfaces; ATM; security; fraud; face recognition;

1. Introduction

Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, but various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats[8]. To overcome, hybrid model which consists of conventional features along with additional features like face

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).
doi:10.1016/j.procs.2015.03.166

recognition and one-time password (OTP) is used. Database holds information about a user's account details, images of his/her face and a mobile number which will improve security to a large extent.

First, the user will swipe the ATM card. A live image is captured automatically through a webcam installed on the ATM, which is compared with the images stored in the database. If it matches, an OTP will be sent to the corresponding registered mobile number. This randomly generated code has to be entered by the user in the text box. If the user correctly enters the OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm and an OTP drastically reduces the chances of fraud plus frees a user from an extra burden of remembering complex passwords.

2. Purpose and benefits of using face recognition and OTP in ATM:

Face recognition finds its application in a variety of fields such as homeland security, criminal identification, human-computer interaction, privacy security, etc. The face recognition feature inhibits access of account through stolen or fake cards. The card itself is not enough to access account as it requires the person as well for the transaction to proceed. Eigenface based method is used for the face recognition. However, the drawback of using eigenface based method is that it can sometimes be spoofed by the means of fake masks or photos of an account holder. To overcome this problem 3D face recognition methods can be used. However, its computation cost is high and requires large storage space which makes it very difficult to store information about a large number of users and 3D masks can also be used to spoof the 3D facial recognition based model. 3D printing is mostly used for such attacks. These drawbacks can be easily overcome by using One-Time passwords (OTP). OTP ensures that the user is authentic by sending the randomly generated 6-digit code to the registered mobile number of the corresponding account holder. In addition, the user will not have to remember PIN. It prevents the fraudulent attacks like:

2.1. Eavesdropping

The ATM card or PIN of a user can be spied upon and can be accessed easily by obtaining the card by faulty means. This can lead to some serious consequences.

2.2. Spoofing

There is a possibility that, when a user enters the PIN during the transaction process, a hacker fakes as the authorized site and prompts the user to re-enter PIN due to a system error. When a user complies with the instruction the hacker stores the data and uses it for his future peccadilloes intentions. This man-in-the-middle (hacker) attack is futile because new password is temporarily assigned in every new transaction.

2.3. Brute-force attack

Using the brute force, if we try to crack the current static four digit PIN it can be done in 9999 attempts, thus weakening the security. In our model a 6-digit code is sent to a registered number, thus increasing the security and reducing the chances of cracking the code using brute force.

3. Biometrics Comparison

Table 1.Comparison of biometric technologies

Biometrics	Cost	Accuracy	Performance	Flaws	Stability
Iris	High	High	High	Lighting	High
Retina	High	High	High	Glasses	High
Face	Medium	Medium	Medium	Beard, glasses, age	Medium
Fingerprint	Low	Medium	Medium	Dirt, dryness	High

4. Face detection and recognition

At this stage a user simply needs to look into the camera installed on ATM. If the user is recognized, then OTP is sent to user's mobile phone. We have seen thefts in ATM like the criminal entering into the room and forcing the user to access his or her account. To overcome this problem we have found a simple solution; if more than one faces are detected by the machine then the account gets temporarily locked. This additional feature is simple yet effective. Therefore, this system ensures that transaction is proceeded only when user alone is accessing the machine.

In general, face recognition techniques can be divided into two groups based on the face representation they use[6]:

1. Appearance-based:
It uses holistic texture features and is applied to either entire face or only to the specific regions in face image. Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminate Analysis (LDA) fall under this category.
2. Feature-based:
It uses geometric facial features (mouth, eyes, nose, etc.) and geometric relationships between them.

Our model uses Principal Component Analysis. To build eigenfaces, good data is required for component matching. The eigen faces are ordered from largest to lowest, where the eigenfaces having larger eigenvalue finds greater variance as compared to those having less eigenvalue. From this set of eigenfaces only first K of them are selected which exhibits most of the unique properties. An advantage of PCA to other methods is that the 90% of the total variance is contained in 5-10% of the dimensions[7,8].

4.1. The purpose of using PCA

1. Time taken for computation is very less as it considers only the essential components from images.
2. Based on multiple face images as input, i.e. it considers multiple input images of each person with different expressions and under different lightening conditions.
3. Demands less storage space for storing dataset.
4. Smaller database representation since only the trainee images are stored in the form of their projections on a reduced basis.
5. Reduced dimensions increase the efficiency of the process.

4.2. Working of face recognition technique

4.2.1. Eigenfaces Initialization

This process can only be performed by the authorized people in the bank. When a customer creates an account he/she needs to provide images. This can be done by capturing his/her image from webcam in the bank. The accountant captures some images and stores them to the database which has label as account number associated to each of them.

For training of images in the database, each image in a data set is resized such that each of them has the same dimensions for example N×N. Each image is converted into face vector forms. The face vectors have dimensions of $N^2 \times 1$. Each face vector is normalized i.e. common features from all the face vectors are removed. This is done by calculating the average face which contains features of all the face vectors and subtracting it from each of the face vectors. The matrix A is formed which contains these face vectors and is represented as:

$A = [\phi_1, \phi_2, \phi_3, ..., \phi_M]$ and has dimensions of $N^2 \times M$.

where,
ϕ_k - Face vector obtained after subtracting average face.
M - Total number of face vectors used for training.

Eigenfaces are calculated from the covariance matrix by dimensionality reduction technique (wherein the eigenfaces

are calculated by covariance matrix with reduced dimensionality) which is given by the formula:

$$C = A^T A \quad (1)$$

It has dimensions of M×M. Therefore M eigenfaces, each of size M are calculated by simple matrix multiplication. From these M eigenfaces only K of them (the principal components) are selected heuristically (by artificial intelligence) which contain the most unique and vital information and discards the remaining which contain redundant or noisy information without much loss of the valuable information. The original eigenfaces are calculated from these K eigenfaces by the pre multiplying matrix A with each of the K eigenfaces. This method reduces the computation time and noise from input images. These eigenfaces contribute to the formation of images in the data set. The original image is calculated by multiplying weights(w_1, w_2, w_3...) with the corresponding eigenface and adding them, then the average face is added to it which was subtracted earlier. Therefore, each image in a dataset is represented by a weight vector Ω, which is the eigen face representation of the i^{th} face.

4.2.2 Eigenfaces Recognition

Once the card is swiped, then following process takes place:
1. Capture the image from the webcam and detect face from it. If more than one face us captured in an image, then temporary block the access of account for security and privacy reasons. If only one face is captured, then continue the process (step 2).
2. Resize the face to the standard dimensions of N×N.
3. Convert the input face into face vector.
4. Normalize the face vector.
5. Project the normalized face vector onto the eigen space.
6. Calculate the weight vector of input image.
7. Calculate the distance between the input weight vector and all the weight vectors of the training set.
8. If the distance is less than the threshold value, the person is identified and the transaction can proceed or else the transaction cannot proceed.

5. OTP working

For implementing OTP, we will make use of GSM modem to send SMS (an OTP) to user's mobile number. The idea to use mobile phones is preferred over e-mail because the people in rural areas have simple phones which can receive text messages but have no internet connections and e-mail facilities. Since mobile phones are ubiquitous, we intend to use mobile phones so that everyone can take the benefit of the new proposed system. The user will receive OTP immediately after passing the face recognition test. Once OTP is received user has to enter the code which is of 6-digit. User gets three chances to enter the code. If the code is entered incorrectly in three consecutive attempts account gets temporarily blocked and notification is sent to registered mobile number. This feature is added in order to restrict the fraudulent means of attacking the account of a user by wearing masks or in rare cases, if unauthorized user's face mistakenly matches authorized user's face.

5.1 Random Number Generation

Generation of sequence of Pseudo-Random Numbers, (Y_n):

$$Y_{n+1} = (a \times Y_n + C) \bmod (m) \quad (2)$$

Choices of a (multiplier), C (increment) and m (modulus) are important because random numbers generated will be in sequence if not handled properly.

5.2 Proposed Random Number Generation formula

The drawback of the above random number generator is that the sequence has a finite number of integers and the

sequence gets repeated over a period of time[11]. Therefore, we have modified the formula by applying the same random number generator formula to 'C' and this value is substituted in the random number generator's increment. So the new random number generator formula will be:

$$\begin{aligned} C &= (b \times X_n + d) \bmod (m) \\ X_{n+1} &= C \\ Y_{n+1} &= (a \times Y_n + C) \bmod (m) \end{aligned} \tag{3}$$

The random number(Y_{n+1}) generated will be the OTP. The value of 'm' should be a large prime number in order to distinct unrelated numbers. Though the overhead is increased due to computation, but the repetition of a sequence is completely eliminated.

5.3 Cryptographic hash functions

Various Cryptographic hash functions are used to improve the security level. We have chosen MD5 also known as Message Digest because it is widely used hash function. Since, it is the fastest cryptographic hash function, it is convenient to use MD5 and is mostly accepted by a wide variety of platforms[3].

5.4 Steps

1. A 6-bit OTP is generated using the random number generator technique.
2. This OTP generated is texted to a user's mobile phone number.
3. This OTP undergoes MD5 hashing technique thus converting it into encrypted form and is temporarily stored in the database which will be erased after one minute.
4. The user will have to enter the OTP within one minute time limit.
5. The user's entered OTP again undergoes similar hashing technique and is compared with the stored temporary encrypted OTP value in database.
6. If it matches, then the transaction can be proceeded.
7. Steps 1-5 are repeated for every new transaction.

6. How will the model help to prevent the theft

Our proposed system's linear dependency of three phases, i.e card requirement, face recognition and OTP plays a crucial role in preventing theft as explained below:

1. If a thief creates a duplicate card to access a user account, the thief's face will not match with user's face.
2. In rare cases, if the thief manages to match the user's face by using masks, then OTP will be sent to the user's registered number, which in turn will alert the user that someone is trying to access the account.
3. Suppose if a user's mobile phone is stolen, the user can deactivate the phone number by contacting the service provider which will prevent OTP to reach the stolen phone which will help to prevent unauthorized access to the account.

To break through these three phases, a thief needs to steal/duplicate cards, then match a user's face and then steal user's phone. Thus passing through this system is only possible if the user is careless to report a stolen/misplaced phone or stolen/misplaced ATM card to deactivate account.

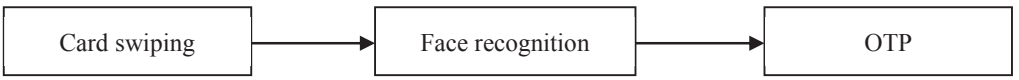

Fig. 1. Flow of the model

7. Flowchart

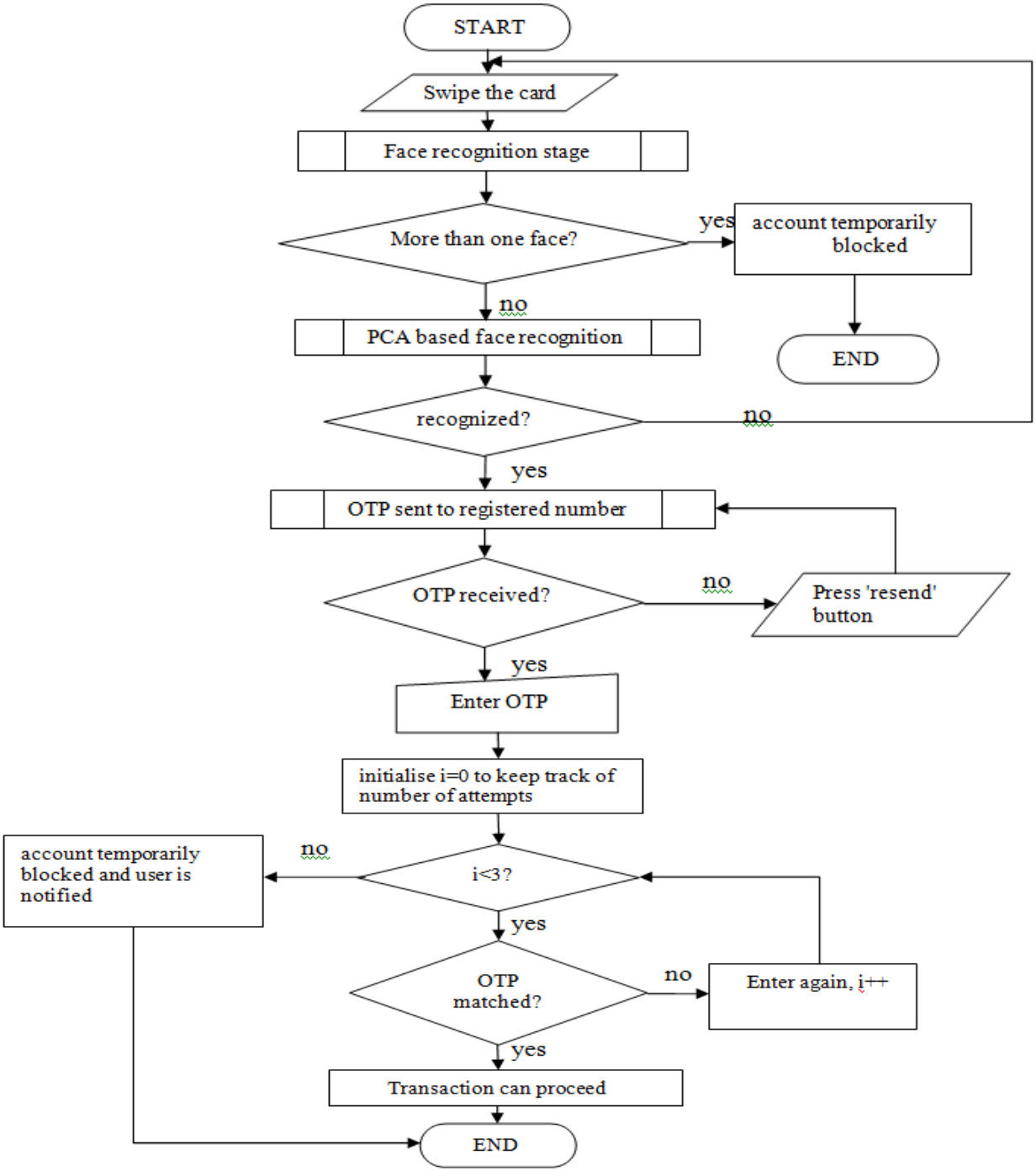

Fig. 2. Proposed model of ATM

8. Drawbacks of the model and how to overcome them

1. One of the major setbacks of this model is when the camera does not work properly or is damaged. Due to such technical abnormalities the transaction is hindered. However, to solve this problem, we have introduced a 'report' button on the screen during the face recognition phase. This notifies the authority of a bank and the problem can be resolved as soon as possible. In order to prevent unnecessary use of report button, detail of user is provided to the authority to identify the user who has reported the problem.
2. If the user does not receive OTP in short time after the face recognition phase, it can delay the transaction which in turn makes user impatient. To overcome this situation a 'resend OTP' button will be provided which will resend OTP.
3. The major drawback of this system is that if a particular network service is down, then it becomes impossible for the user to receive OTP.

9. Future Scope

As we mentioned in the table 1, facial recognition technique seems more challenging as compared to other biometrics, thus more efficient algorithm can be developed. The flaws in face recognition technique like the inability to detect face when beard, aging, glasses and caps can be rectified and eliminated or reduced. If the cost of retina or iris recognition reduces, it can be used instead of face recognition.

10. Conclusion

This project is still under development. The model shows the qualitative analysis of algorithms used based on the metrics of existing algorithms. According to the statistics PCA based face recognition is very accurate, requires less computation time and less storage space as trainee images are stored in the form of their projections on a reduced basis. After the completion of the project we will collect the quantitative aspects of the model and compare it with the qualitative results for further proof.

Acknowledgements

As the authors of this paper we would like to acknowledge the Head of Computer Department D.R. Kalbande, Sardar Patel Institute of Technology for lending his support and help for the research and development of this paper. We would also like to thank the IEEE society for providing reference papers and resources as well as to the resources provided by the websites and books mentioned in the reference section of this paper. We would also thank our family and friends for lending their support and co-operation in the work.

References

1. Rupinder Saini, Narinder Rana,Rayat 'Comparison of various biometric methods', Institute of Engineering and IT, International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue I (March 2014)
2. Devinaga, R. (2010). ATM risk management and controls. European journal of economic, finance and administrative sciences. ISSN 1450-2275 issue 21.
3. A.Forouzan, Cryptography and Network Security, Tata McGraw Hill
4. Anil K. Jain and Arun Ross. Introduction to Biometrics. In Anil K. Jain, Patrick Flynn, and Arun. A. Ross, editors, Handbook of Biometrics. Springer US, 2008.
5. Rafael C. Gonzalez and Richard E.Woods, Addison Wesley, Digital Image Processing.
6. Ekenel HK, Stallkamp J, Gao H, Fischer M, Stiefelhagen R, Face Recognition For Smart Interacations, interact Research, Computer Science Department, University at Karlsruhe.
7. Sezin Kaymak , “Enhanced Principal Component Analysis Recognition Performance”.
8. Vinay Hiremath and Ashwini Mayakar, Face recognition using Eigenface approach.
9. Aru, Okereke Eze, Ihekweaba Gozie, Facial Verification Technology for Use In Atm Transactions
10. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013),PP 22-29
11. http://www.ics.uci.edu/~smyth/courses/ics178/random_number_generators article.pdf