International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

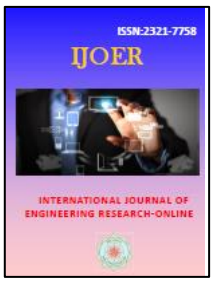
Vol.5., Issue.3, 2017
May-June

RESEARCH ARTICLE

ISSN: 2321-7758

ATM Security Using Face recognition and OTP

Prof. S.A.DHOLE, CHAITALI JADHAV, CHAITALI BHOSALE, POOJA DERE
Department of Electronics and Telecommunications
Bharati Vidyapeeth's College of Engineering For Women, Katraj Dhankawadi, Pune
Savitribai Phule Pune University
Chaitalijadhav08@gmail.com , chaitalibhosale28@gmail.com , poojapdere@gmail.com



ABSTRACT
The purpose of this project is provide security to the conventional ATM model. This paper posited a new concept that enhances the overall experience, usability and convenience of transaction at the ATM. Features like face recognition and one time password (OTP) are used for the enhancement of security of accounts the privacy users. Face as 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. There is no worry of losing ATM card and no need to carry ATM card in your wallet.
Keywords: PCA, OTP, 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 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. To overcome, hybrid model consist of conventional features along with additional features like face recognition and one time password (OTP) is used. Database holds information about a user's account details, images of his/her face and mobile number which will improve security to a large extent.

Face recognition finds its variety of such as homeland security, criminal identification, human-computer interaction, privacy security etc. Face recognition has been attracting intense research efforts due to its importance both as one of the main building blocks of natural human computer interfaces and as a biometric trait. Face recognition has the advantage of ubiquity and of being universal over other major biometrics, in that everyone has a face and everyone readily displays the face.

First, user will enter user id and password. After that a live image is captured automatically though a webcam install on the ATM, which is compared with the images stored in the database. If it matches, then the person is authorized. And then an OTP will be send 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 enter the OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm, and an OTP drastically reduces the chances of frauds plus frees a user from an extra burden of remembering a complex password.

2. METHODOLOGY

In ATM security system, firstly user will enter user id and password which is provided by

bank. After that a live image is captured automatically though a webcam install on the ATM, at this stage a user simply needs to look at camera installed on ATM, the user is authorized When this image matches with the image stored in database. When a customer creates an account he/she needs to provide image, this can be done by capturing his/her image from webcam in the bank. The accountant capture some images and stores them to the database which has label as account number associates to each of them.

If person is authorized then an OTP will be send to the corresponding registered mobile number. The idea to use mobile phones is preferred over email because the people in rural area have simple phones which can receive a 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. Once OTP is received user has to enter the code, User gets three chances to enter the code.

Initially we store the face of user and that will be verified with the face that we are giving, when the time of authentication. If both the face OTP are matched then account will open. As it is based on the face authentication there is no chance of disclosing of password or pin to the third parties.

3. BLOCK DIAGRAM

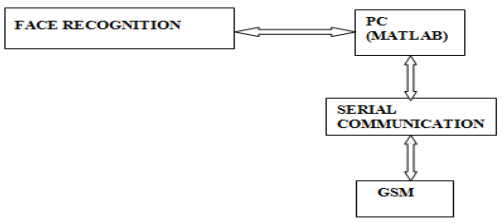


Fig 3.1. Block diagram of ATM security system using fingerprint and face recognition system

3.1. BLOCK DIAGRAM DESCRIPTION

3.1.1.Web Camera: Webcam is used for taking the live image of person face we are using "ROBO 351 i-boll" Web Cam after observing its specification it capture the image and sent it to PC through USB data cable. It require +5v , 0.35 amp (max) voltage and current for its operation.

Fig.3.3 Webcam

Specifications:

1.Camera :1.3 mp..

2.Video Resolution : 640 x 480 sensor resolution.

3.USB certification : USB 2.0 high speed certified.

3.1.3. Serial interface:RS232 is the most known serial port used in transmitting the data in communication and interface. Even though serial port is harder to program than the parallel port, this is the most effective method in which the data transmission requires less wires that yields to the less cost. The RS232 is the communication line which enables the data transmission by only using three wire links. The three links provides 'transmit', 'receive' and common ground.

4.FACE DETECTION AND RECOGNITION

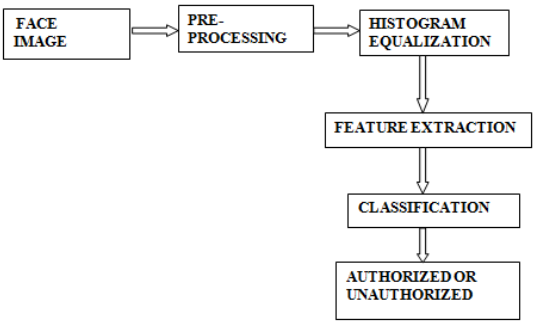
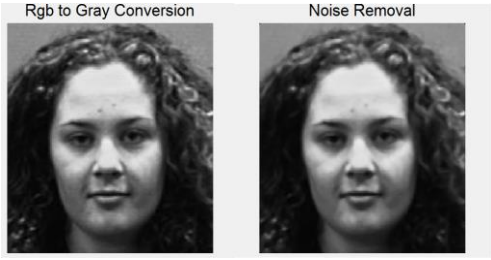


Fig.4.1 Block diagram of face image processing

4.1.1.Pre-processing

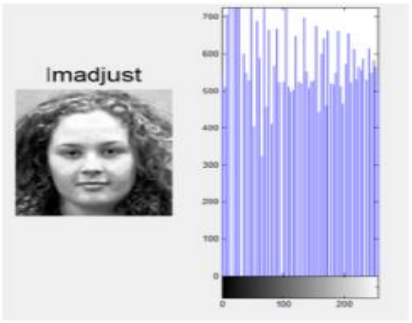
1. Face Image Reading In this step, the face image is loaded by using the Matlab built-in function imread.
2. RGB to Gray Image Raw data of face image obtained is in the RGB format. The face image in the RGB format is then changed into gray scale image so that image processing can be executed on the image. Matlab built-in function „rgb2gray is used to convert RGB image to gray scale image.

   I=rgb2gray(RGB);



4.1.2. Histogram Equalization: Histogram equalization is a technique of improving the global contrast of an image by adjusting the intensity distribution on a histogram. This allows areas of lower local contrast to gain a higher contrast without affecting the global contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values.

- Histogram :It is discrete function h(rk)=nk, where rk is kth grey level in the range of [0,L-1] and nk is number of pixels having grey level rk.



4.1.3.Feature Extraction: For feature Extraction PCA algorithm is used.

Purpose of using PCA algorithm:

- Demands less storage space for storing data set.
- Reduced dimensions increase the efficiency of process.
- Uses to build eigenfaces, good data is required for component matching.
- Time taken for computation is very less as it considers only essential components from images.

Steps for PCA algorithm: Let a face image Γ(x, y) be a two dimensional M by N array of intensity values. In this thesis, I used a set of image by 200 × 149 pixels. An image may also be considered as a vector of dimension M × N, so that a typical image of size 200 × 149becomes a vector of dimension 29,800 or equivalently a point in a 29,800 dimensional space.

Step1: prepare the training faces.

Obtain face images I1, I2, I3, I4 , ... IM (training faces). The face images must be centred and of the same size.

Step 2: Prepare the data set.

Each face image Ii in the database is transformed into a vector and placed into a training set S.

$S=\{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4 \ldots\ldots\ldots\ldots \Gamma_M\}$ ...(1)

In My example M = 34. Each image is transformed into a vector of size MN × 1 and placed into the set. For simplicity, the face images are assumed to be of size N × N resulting in a point in N^2 dimensional space. An ensemble of images, then, maps to a collection of points in this huge space.

Step 3: compute the average face vector

The average face vector (Ψ) has to be calculated by using the following formula:

$$\psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n \quad \ldots(2)$$

Step 4: Subtract the average face vector .

The average face vector ψ is subtracted from the original faces Γ_i and the result stored in the variable$\Phi_{i,}$

$$\Phi_i = \Gamma_i - \psi \quad \ldots(3)$$

Step 5: Calculate the covariance matrix.

We obtain the covariance matrix C in the following manner,

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n \Phi_n^T = AA^T \quad \ldots(4)$$

$$(N^2 \times N^2 \; matrix)$$

Where

$$A = [\Phi_1, \Phi_2, \Phi_3, \Phi_4, \ldots\ldots\ldots\ldots \Phi_M]$$

$$(N^2 \times M \; matrix)$$

Step 6: Calculate the eigenvectors and eigenvalues of the covariance matrix.

The covariance matrix C in step 5 has a dimensionality of $N^2 \times N^2$, so one would have N^2eigenface and eigenvalues. For a 256 × 256 image that means that on must compute a 65, 536 × 65, 536 matrix and calculate 65,536 eigenfaces. Computationally, this is not very efficient as most of those eigenfaces are not useful for our task. In general, PCA is used to describe a large dimensional space with a relative small set of vectors .

Compute the eigenvectors μ_i of AA^T The matrix AA^T is very large ...> not practical!!!

Step 6.1: consider the matrix

$L = A^T A$ (M × M matrix)

Step 6.2: compute eigenvectors v_i of L=A^TA

$$A^TAv_i = \mu_i v_i$$

What is the relationship between μ_i and v_i ?

$$A^TAv_i = \mu_i v_i$$
$$AA^TAv_i = \mu_i Av_i$$
$$CAv_i = \mu_i Av_i$$

[since $C = A\,A^T$]

$$C\mu_i = \mu_i Av_i$$

where,

$$\mu_i = Av_i$$

Thus, $C = AA^T$ and $L = A^TA$ have the same eigenvalues and their eigenvectors are related as follows:

$$\mu_i = Av_i$$

Note 1: $C = AA^T$ can have upto N^2 eigenvalues and eigenvectors.

Note 2: $L = A^TA$ can have upto M eigenvalues and eigenvectors.

Note 3: The M eigenvalues of $C = AA^T$ (along with their corresponding eigenvectors) correspond to the M largest eigenvalues of $L = A^TA$ (along with their corresponding eigenvectors). Where v_i is an eigenvector of $L = A^TA$. From this simple proof we can see that Av_i is an eigenvector of: $C = AA^T$.

The M eigenvectors of $L = A^TA$ are used to find the M eigenvectors μ_i of C that form our eigenface basis:

$$\mu_i = \sum_{i=1}^{M} v_i \Phi_i \qquad ...(5)$$

Where, μ_i are the Eigenvectors i.e. Eigenfaces.

Step 7: keep only K eigenvectors (corresponding to the K largest eigenvalues) Eigenfaces with low eigenvalues can be omitted, as they explain only a small part of Characteristic features of the faces.

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, (Yn):

Y n+1 = (a + Y n + C) mod (m) (2)

Choices of a (multiplier), C (increment) and m (modulus) are important because random numbers generated will bein 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 time11. Therefore, we have modified the formula by applying the samerandom 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:

C= (b X n + d) mod (m)

X n+1 C=

Y n+1 (a Y n + C) mod (m) (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.

5.4 Steps:

i. A 6-bit OTP is generated using the random number generator technique.
ii. This OTP generated is texted to a user's mobile phone number.
iii. 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.

iv. The user will have to enter the OTP within one minute time limit.

v. The user's entered OTP again undergoes similar hashing technique and is compared with the storedtemporary encrypted OTP value in database

vi. If it matches, then the transaction can be preceded.

vii. Steps 1-5 are repeated for every new transaction

6. FUTURE SCOPE

A lot of criminals tamper with the ATM terminal card details by illegal means. Once user's ATM card is lost and password is stolen ,the user's account is vulnerable to attack. Traditional ATM system authenticate generally by using card and a password or PIN which no doubt has some defects. Biometrics authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is non-transferable and unique for every individual. The system can compare scans to record stored in a central or local database or even on a smart card. This technique is very useful in future for avoiding the fraud in ATM system.

7. CONCLUSION

Biometrics, in particular face scanning, continues to gain acceptance as a reliable form of securing access through identification and verification process.

PCA based face recognition is very accurate, requires less computation time and less storage space as a trainee images are stored in the form of their projections on a reduced basis. OTP is used to improve security level.

The system has successfully overcome some of the aspects existing with the present technologies, by the use of face and OTP as the authentication technology.

8. REFERANCE

[1]. MohsinKarovaliya et al., "Enhanced security for ATM machine with OTP and Facial recognition features", International conference on advanced computing technologies and applications. pp.390-396,2015.

[2]. Liton Chandra Paul, "Face recognition using principle component analysis method", International Journal of advance research in computer engineering and technology Volume1.pp.135-139,2012

[3]. Madhuri M. Ghodake, "Face Recognition Using Principal Component Analysis for Security Based System", International Journal of Science and Research .pp.1262-1266,2015.