Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Two Step Verification for Withdraw the Amount from ATM Machine

M. Hemamalini
Student,
Dept.of Computer Science and Engineering,
Adhiparasakthi College of Engineering, Kalavai,
Vellore Dist., Tamil Nadu, India

D. Jagadeesan
Assistant Professor,
Dept. of Computer Science and Engineering,
Adhiparasakthi College of Engineering, Kalavai,
Vellore Dist., Tamil Nadu, India

Abstract - Two step verification of ATM card is required to prevent the illegal access of an account. This paper describes the two step verification of account by matching the distance of the top, left, right, bottom of the human skull image. The skull of the human is captured by the pseudo 3D image capture at the ATM terminal. The feature points are calculated and encrypted and sent to the server via a secure channel. The encryption is based on bio keys. If the value matches with the encoded value in the database, it allows for withdraw of amount. If not it declines to withdraw.

Keywords: ATM, PIN, biometrics, security, skull, encryption, decryption.

I. INTRODUCTION

Now-a-days people withdraw money from the ATM centers by using the ATM card and PIN number provided for the unique users. A personal identification number (PIN) [6] is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. The user is granted access only when the number entered matches with the number stored in the system [1].

Though the pin number is used for security purpose, it is not much secure. Because it can be cracked by the crackers by trying all possible combinations of values or account takeover will take place [2]. Hence two step verification is required to protect against withdraw of money by the crackers.

The following are the same characteristics that the customers have [3],

- Something only the user knows (e.g., password, PIN, pattern)
- Something only the user has (e.g., ATM card, smart card, mobile phone)
- Something only the user is (e.g., biometric characteristic).

The success of skull matching technique depends on matching with the results stored in the database. Hence this method helps to identify the authorized user accurately. For this requirement of

- A front-end subsystem (pseudo-3D image capture) used to capture an image using sensor and converting to some digital format.
- A back-end system (database) to compare the values.
- A template to store the values.

II. REVIEW OF RELATED WORKS

Biometrics allows a customer (account holder) to be validated or authenticate using physical, behavioral attributes or their characteristics. These characteristics must be verifiable automatic [4]. There are several BM techniques available for security purpose. They are,

A. Fingerprints Recognitions

Fingerprints are used for identification of unique persons by using the pattern of a friction ridge. It is the oldest techniques that are used for authentication.

V. Padmapriya and S. Prakasam has says that the fingerprints reduce the rate of fraudulent activities on the ATM machines. But the drawback is that it can be easily duplicated. It can be obtained in tapes and can be easily breakable [7].

Fig. 1: Example of fingerprints

B. Irish Recognition

Jonas Nyasulu and Tierry Fomene has discussed Iris recognition is suited for verification and comparisons is made in seconds. Irish is an efficient authentication method since it is located in the eye. But it has a drawback that, it rejects the correct user due to the lens, Blind persons and persons affected by eye disease [8].

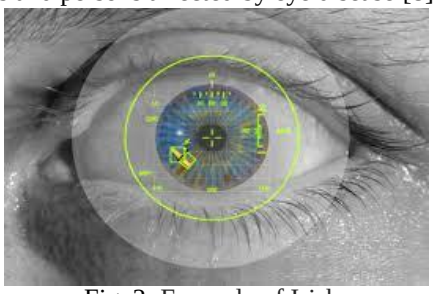

Fig. 2: Example of Irish

C. Face Recognition

Sneha P. Wandale, Prof. P.A. Tijare and Prof. S.N. Sawalkar has discussed the facial recognition is cost effective, reliable and high accuracy. But it is not more efficient because face change over time and hinders the accurate identification [9].

Fig. 3: Example of Image processing

D. Palm Veins

Ishani Sarkar, Farkhod Alisherov, Tai-hoon Kim , Debnath Bhattacharya has discussed palm vein technology is contactless authentication and effective. The veins in the palm are unique and it cannot be spoofed able because it is present in the human hand. Hence it is not more efficient than the retina [10].

Fig. 4: Example of palm vein technology

E. Retina

Shouvik Biswas,Anamitra Bardhan Roy, Kishore Ghosh Nilanjan Dey, has discussed the retina can be used for authentication purpose, since it provides self manipulative, simple, fast and much more secure for ATM and reduces the size of database drastically as no image is stored. But the drawback is that fear to scan and it is more expensive [ ].

Fig. 5: Example of retina

F. Comparisons of different Biometrics

Table 1: Comparisons of different Biometrics [5]

Technology	Advantages vs. Hand Geometry	Disadvantages vs. Hand Geometry
Fingerprint	• False accept rate can be lower (depends on product) • Pricing may be lower (depends on application)	• Larger template, fewer users per reader, requires more readers • Higher false reject rate (depends on product) • Privacy issues/law enforcement association with fingerprints • One in 50 people have unreadable fingerprints • Sensitive to dirt, dry skin, etc.
Iris scanning	• Low false accept rate (probably lowest of all biometrics)	• Higher false reject rate • Larger template, fewer users per reader • Problems with lighting, eyeglasses and contact lenses • Sometimes perceived as more intrusive
Facial	• Pricing may be lower (depending on number of employees) • Touch-free	• Larger template, fewer users per reader • Higher false reject rate • Perceived as more intrusive • Problems with lighting, eyeglasses, hats, hair styles, weight gain and facial hair
Vein	• Smaller in size • Runs in ID mode (one-to-many comparison)	• Difficult to enroll without guidance • Slightly higher false reject rate • Slightly higher false accept rate

III. PROBLEM IDENTIFICATION

To overcome the drawbacks of the above biometric techniques, the skull of the human can be used. Skull of human vary by each person, hence it can be used for authentication purpose.

- Used for secure banking applications.
- Difficult to break.
- Cannot be spoofed.

IV. PROPOSED WORKS

The image of the skull is taken by the pseudo-3D Image capture at the ATM terminal and is encrypted using the bio key and translate the encrypted value to the database. If the value in the template of the database matched with the current encrypted value, it allows for withdraw else its decline.

4.1 Architecture for Encrypt and Comparison

Encryption process is used to convert the PIN number and feature points to unreadable form (cipher text). Initially the customer (card holder) opens an account in the require bank and gets the PIN number to access it. The image of the customer's skull is taken and feature points are calculated. The feature point value is encrypted using the bio key and stored in the database along with the PIN number. It does not require the separate database to store the feature point values. Comparisons of skull feature values are made while withdraw. If an account has the co-applicant, then the image of the skull of co-applicant is also taken and stored along with the PIN. If co-applicant is using the ATM card, first it checks for main applicant, if the value does not match it checks for the co-applicant value. And allow for withdraw.

4.2 Architecture for Decryption

Decryption is the reverse of encryption. The values are decrypted and then compared. Decryption process is carried out using the same bio key. It compares the values and allow for withdraw only when the values are matched. Else it decline to withdraw.

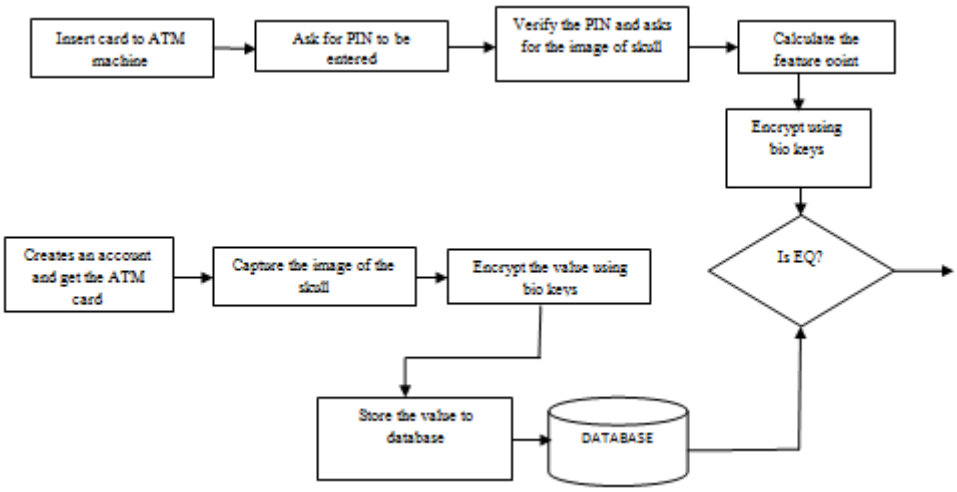

Fig. 6: Architecture for Encrypt and Comparison

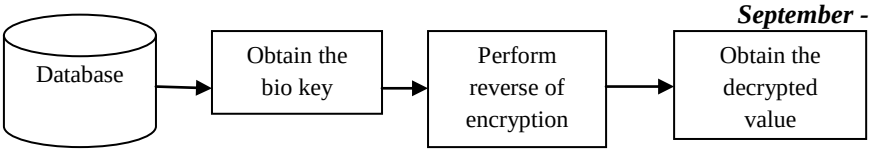

Fig. 7: Architecture for Decryption

4.3 Algorithm

Step 1 : Get the ATM card and PIN number from the respective bank by creating an account.

Fig. 8: Example of ATM cards

Step 2 : If he/she is a new customer the front end system asks for the image of the skull and calculates the feature points.
Step 3 : Encrypt the values using the bio key else go to step 4
Step 4 : Insert the ATM card to the ATM machine.
Step 5 : It asks for a PIN number to be entered.
Step 6 : Then checks the PIN number with the encoded value stored in the database.
Step 7 : If a match occurs, then it asks for the image of the skull and goto Step 9.
Step 8 : Else it asks the customer to re-enter the password. Maximum it allows three times to re-enter the password. If no match occurs the account will get blocked and go to step 12.
Step 9 : Takes the image of the skull using the pseudo 3D image capture and encrypts the value.

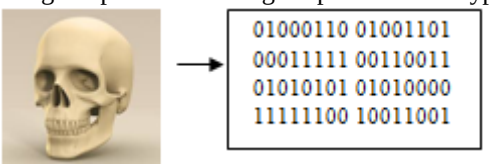

Fig. 9: Example of skull

Step 10 : Then compares this value with the encoded value in the database.
Step 11 : If a match occurs, then allows for withdrawal of money.
Step 12 : Else it goes to the home page.

4.3 Flowchart

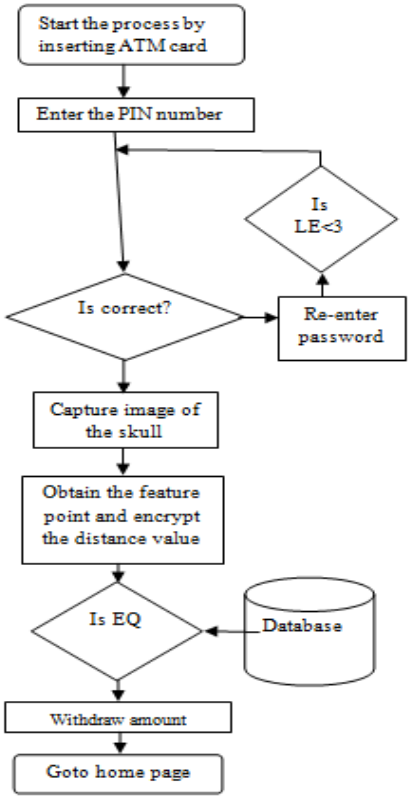

Fig. 10: Flowchart

V. RESULTS AND DISCUSSION

Since skull is unique to each person's this technique is accurate, reliable and achieves approximately 75% security over the frauds happening in the ATM.

VI. CONCLUSIONS

Since the PIN number can be easily identified and cracked the two-step verification is used for the ATM card. Hence the account is much more secure towards the illegal access of account by getting the image of the skull and obtaining the feature point. Encrypt uses the bio authentication and compared with the database. System has allowed the customer to withdraw only when the image is matched. The success of this technique based on rate of accuracy by comparing the result.

REFERENCES

[1] Prithika. M, P. Rajalakshmi (2013), "Credit card duplication and crime prevention using Biometrics", Vol. 10, Issue 1, pp. 01-07.

[2] V.Dheepa1 , Dr. R.Dhanapal (2009), "Analysis of Credit Card Fraud Detection Methods", International Journal of Recent Trends in Engineering, Vol 2, No. 3, pp. 126-128.

[3] "Characteristics of customer", http:// www.wikipedia.org

[4] Navneet Sharma, Vijay Singh Rathore (2012), "Role of Biometric Technology over Advanced Security and Protection in Auto Teller Machine Transaction", International Journal of Engineering and Advanced Technology (IJEAT), Vol. 1, Issue 6, pp. 249-251.

[5] Comparison of bio-metrics", www.allegion.ca"

[6] "Personal Identification Number (PIN)", http://en.wikipedia.org/wiki?curid=337220

[7] S. Padhmapriya and N. Prakasam,(2013), "Enhancing ATM Security using Fingerprint and GSM Technology", International Journal of Computer Application", International Journal of Computer Applications, Vol. 80, No. 16, pp. 43-46.

[8] Jonas Nyasulu, Tierry Fomene,(2008), "Report on the literature Study of Iris Biometric Recognition", https://www.ida. liu.se/~TDDD17/oldprojects/2008/projects/6.pdf

[9] Sneha .P, Wandale, Prof. P.A. Tijare and Prof. S.N. Sawalkar (2013), "Principal component Analysis (PCA) with Back Propagation Neural Network (BPNN) for face Recognition System", International Journal of Application or Innovation in Engineering and Management, Vol. 2, Issue 4.

[10] Ishani Sarkar, Farkhod Alisheror, Tai-hoon. Kim and Debnath Bhattacharya (2010), "Palm Vein authentication system: A Review", International Journal of control and Automation, Vol. 3, No.1, pp. 27-34.

[11] Shouvik Biswas, Anamitra Bardhan Roy, Kishore Ghosh Nilanjan Dey,(2012), "A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 4, pp. 178-182.

