Artificial Neural Network and Location Coordinates based Security in Credit Cards

[1]Hakam Singh,[2]Vandna Thakur
Department of Computer Science
Career Point University Hamirpur
Himachal Pradesh ,India

***Abstract* - Credit cards frauds become more popular hence enhancement in security to avoid these is important. This research work discusses the development and research for the detection of fraud in physical credit card environments by using artificial intelligence applications and location coordinate comparing technology. The current research deals with selected authenticated modes based fraud detection, which will identify and avoids frauds. Through this proposed model we identify theft or frauds before it actually happen such that no loss will occurs in credit card platforms. It includes two steps authentication process to begin a transaction.**

I. INTRODUCTION

Artificial Neural Networks

Artificial Neural Networks are relatively crude electronic models based on the neural structure of the brain. The brain basically learns from experience. It is natural proof that some problems that are beyond the scope of current computers are indeed solvable by small energy efficient packages. This brain modeling also promises a less technical way to develop machine solutions. These biologically inspired methods of computing are thought to be the next major advancement in the computing industry. Different networks structured with different methods e.g. back propagation network consisting of three layers input layer, hidden layer and output layer each layer has different values to perform operation as shown in Figure1. Back propagation network result are used for bank transaction to either begin or abort.[1-3]

Applications of neural network

- Language Processing.
- Character Recognition.
- Image (data) Compression.
- Pattern Recognition.

Location Coordinates

Location coordinates consists of longitude and latitude values which will specify particular communicating device position. Global Positioning System is a satellite based navigation system that can be used to locate positions anywhere on earth. it consists of satellites, control and monitor stations, and receivers. GPS receivers take information transmitted from the satellites and uses triangulation to calculate a user's exact location. GPS is used on incidents in a variety of ways, such as:

- To determine position locations; for example, you need to radio a helicopter pilot the coordinates of your position location so the pilot can pick you up.

Credit Card Frauds

Credit-card-based purchases can be categorized into two types:

a) Physical Card(card physically used)
b) Virtual Card. (cards properties such as numbers, expire data, secure code are used)

In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Several techniques for the detection of smart card fraud have been proposed in the last few years.[4]

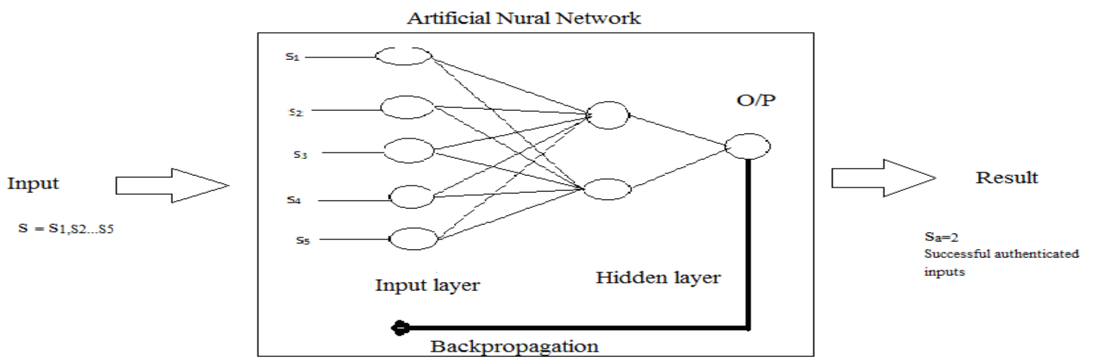


Figure 1

II. Objectives

To Provide Secure Physical credit card Access.

- To study several techniques for the detection of credit card frauds.
- To select a secure credit card authentication model to reduce the credit card frauds. as financial frauds is the major problem of Banks and current security system.

III. Research Methodologies

Two Step Authentication Model Algorithm.

1. Let N is the number of input states(authenticated modes) in the proposed model. We denote the set of input states $S = \{S_1, S_2,\ldots.S_n\}$, $S_{i,}$ i= 1,2… to N is individual states as shown Figure2,3.

2.S_a is set of selected successful inputs S_a>2 i.e at least two inputs selected from N.

```
3. if  $S_a$>2,
              begin T (transaction) ;
              …………………….
else
               abort T (transaction) ;
```

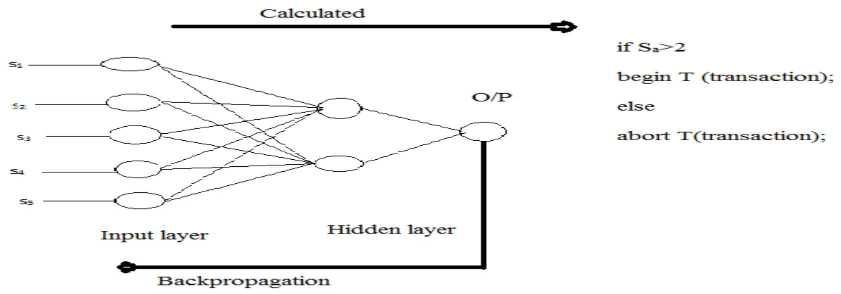


Figure 2

Different input parameters combination possible in this model to provide more flexibility.

Let S_1 we 1st input taken as ATM PIN password common in all steps. Now select the 2nd input from list e.g face recognition S_2, voice recognition S_3 and Registered mobile no location S_4.

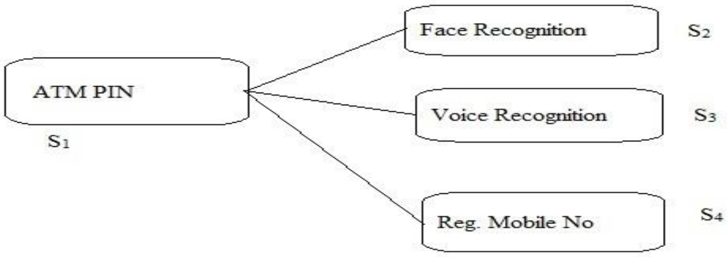


Figure 3

IV. Implementation

Two Step Authentication Access Model

Purposed Authenticated modes to Securely Access Bank Accounts through credit cards in ATM.Figure4

1. Access through secure ATM PIN.

2. Access through Face Recognition.
3. Access through Voice Recognition.
4. Access through Reg. Mobile No based location.

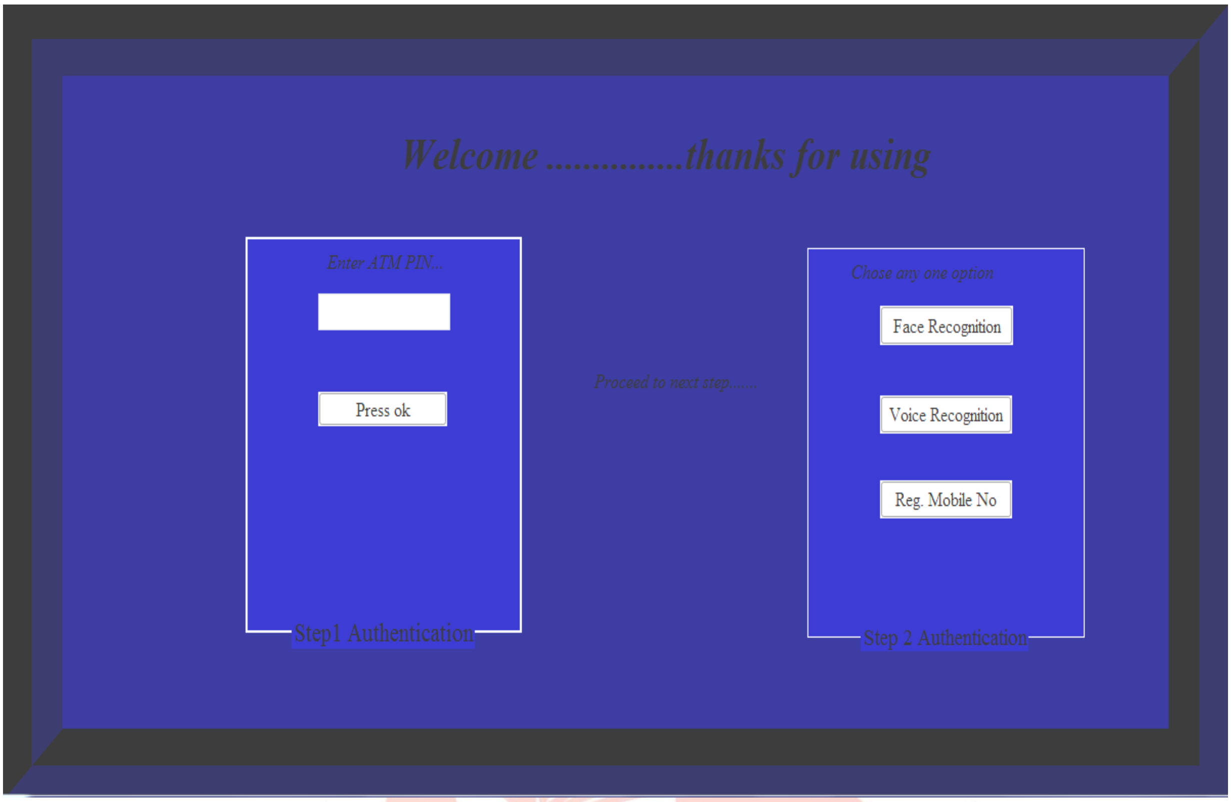


Figure 4

Step 1. Authentication

Access through secure ATM PIN.

Different Steps are performed

1. Enter ATM PIN and Press Ok .
2. Comparison algorithm can find difference between run time input atm pin with stored atm pin in babk database.
   a) If ATM PIN is Correct it will proceed to next step2. Figure5(a)

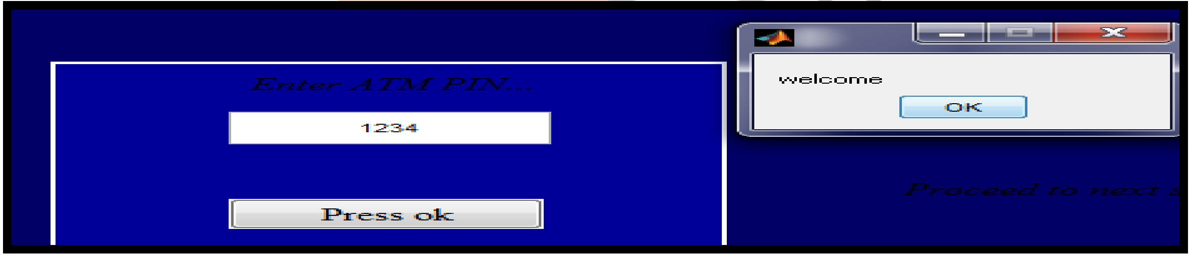


Figure 5(a)

b) Else ‘Access is denied’ and transaction ‘aborted’. Figure 5(b)

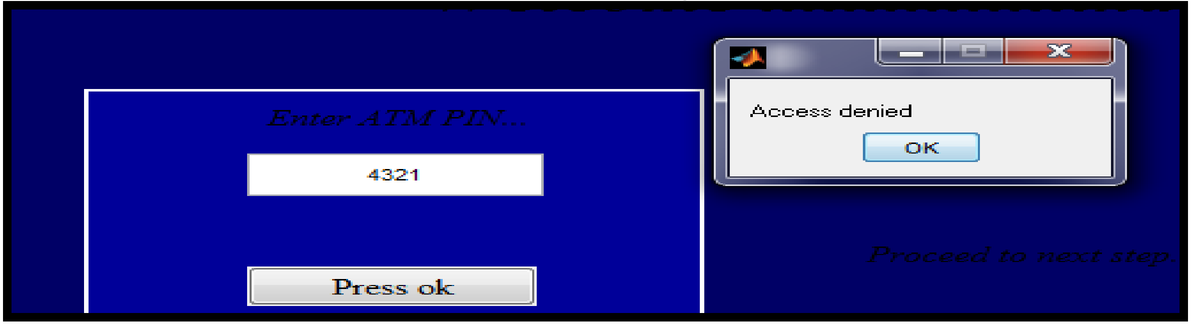


Figure 5(b)

After verifying step 1 proceed to step2.

Step2. Authentication

ATM PIN password can be considered as mandatory part then different combination can occurs.

- ATM PIN and Face Recognition.
- ATM PIN and Voice Recognition.

- ATM PIN and Reg. Mobile No Location.

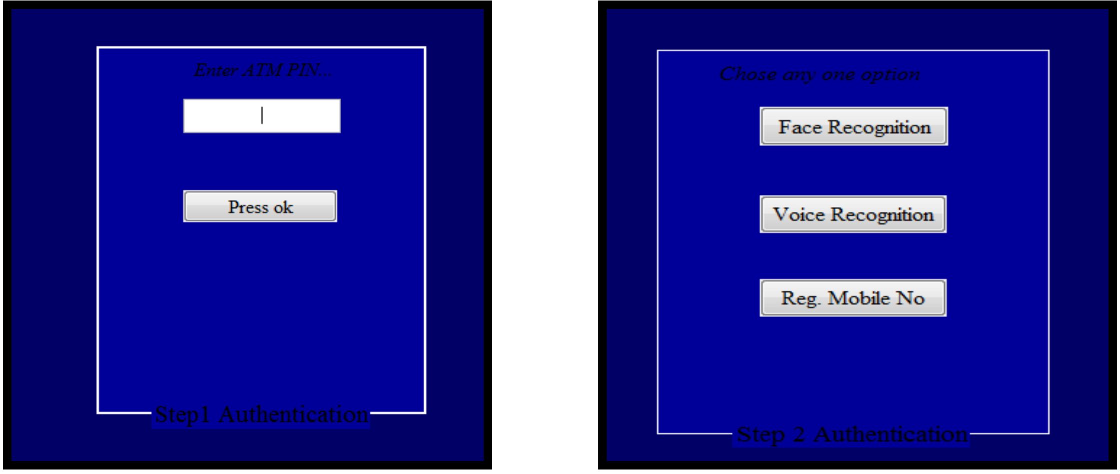
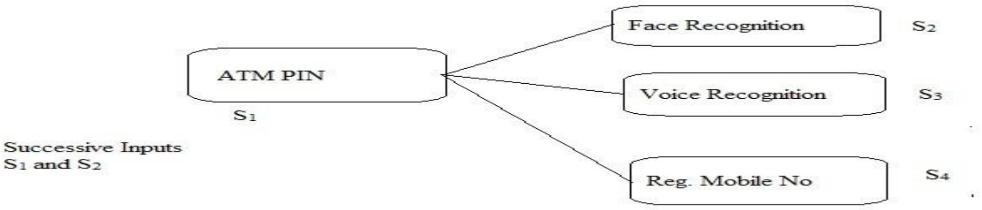


Figure6 (a) (b)

ATM PIN and Face Recognition



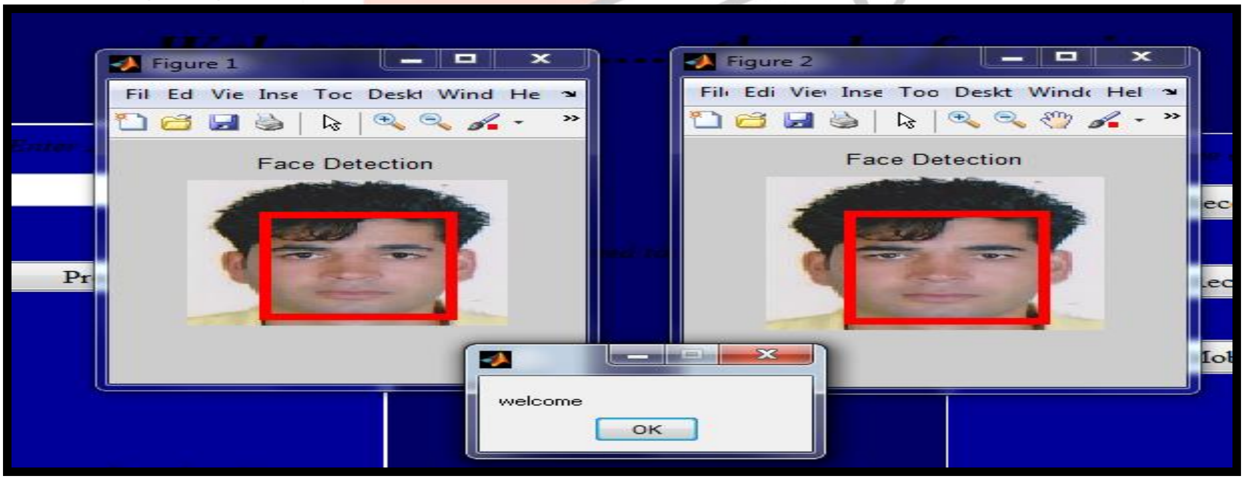
(c)

Sa={$S_{1(\text{ATM PIN})}$ and $S_{2(\text{Face Recognition})}$}

Face Recognition is performed which provides secure identified card access by comparing different runtime images with stored images in bank's database if identified than transaction (T) 'begin' else 'abort'.

Different steps performed

1. At Runtime Credit Card holder image can be taken in consideration.
2. Run time image is compared with already stored image in bank's database of that account holder.
   a) If verified i,e Euclidean Distance value is zero means present card holder is authenticated and transaction begin. Figure6(d)



(d)

b)Else 'Access is denied'.

3. Transaction is 'aborted'.[5,6]

ATM PIN and Voice Recognition

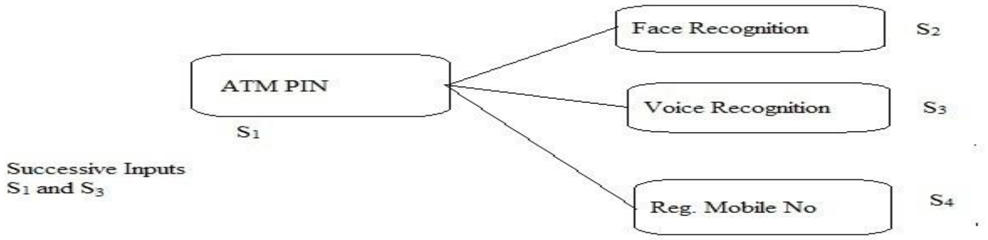
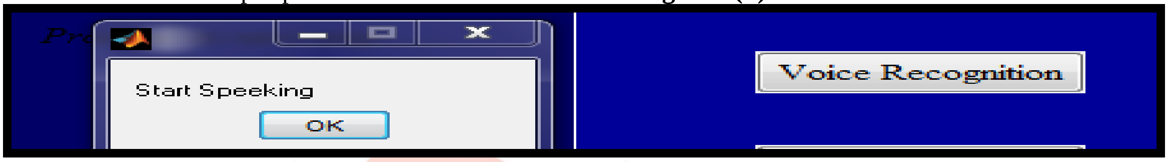


Figure 7(a)

$Sa=\{S_{1(\text{ATM PIN})}$ and $S_{3(\text{Voice Recognition})}\}$
Voice Recognition is performed which provides secure identified card access by comparing different runtime voice patterns with stored voice patterns in bank's database if identified than transaction (T) 'begin' else 'abort'.

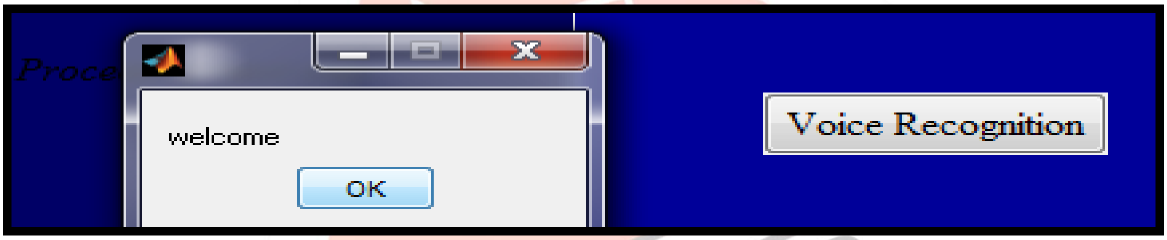
Different Steps are performed

1. Take a run time audio input password of Credit Card Holder. **Figure 7(b)**


Start Speeking

(b)

2. Compare with already stored audio password sample in bank's database.
   a) If their Euclidean Distance value is zero i.e input is authenticated and transaction can 'begin' . Figure 7(c)


welcome

(c)

   b) Else 'Access is denied' .
3. Transaction 'aborted'.[7,8]

.ATM PIN and Reg. Mobile No Location coordinates.

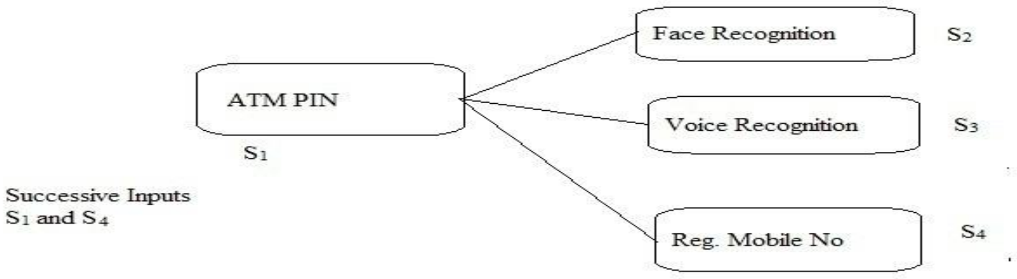


Figure 6(a)

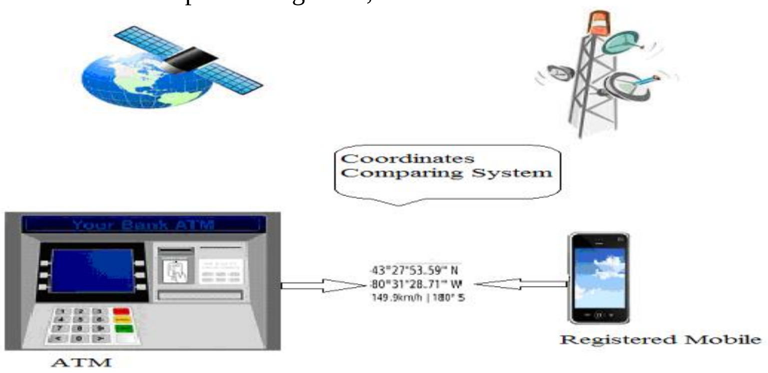
$Sa=\{S_{1(\text{ATM PIN})}$ and $S_{2(\text{Reg. mobile no location})}\}$

Different Step are performed

1. Select Reg. Mobile No option.

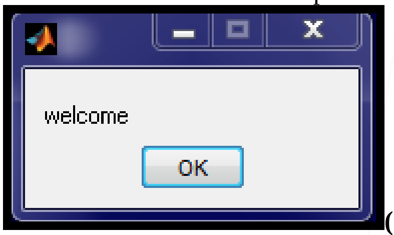
(b)

2. Coordinate Comparing System can find the position coordinates(Longitude and latitude) of current transaction executing machine on which transaction in holding and registered mobile number of transacting account based on different parameters.Figure8(c)
    a) MNC-Mobile Network Code
    b) MCC-Mobile Country Code
    c) LAC-Location Area Code
    d) Network- Network service provide e.g airtel, reliance etc.

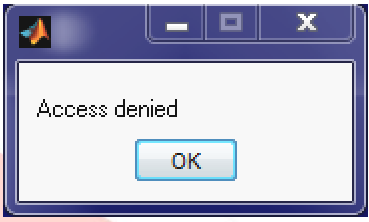


(c)

- If both the position coordinates are same this indicates authenticated or secure transaction.Figure8(e)


welcome

(e) Else'aborted'


Access denied

(f)

3. After verification of user transaction 'begin' or forcefully 'aborted'. [10]

V. Result & Discussion

Result of Two Step Authentication Model

Sr. No	Two Step Authentication Models	Flexibility	Average Execution Time	Average Memory Space
1	ATM PIN with Face Recognition	Medium	7.81166 secs.	8.95kb
2	ATM PIN with Voice Recognition	Low	85.2344 secs.	344kb
3	ATM PIN with Reg. Mobile No	High	0.42416 secs.	6kb

Table1

Length of ATM PIN = 4 bytes
Image Sample Size = 25.6 KB,
Audio Sample Duration=2 seconds
Coordinates values = 28 bytes

Flexibility Rating Scale:
1-5 = Low
5-8 = Medium
8-10 = High

VI. Conclusion

On analyzing the above models it has been concluded that ATM PIN with Reg. Mobile No provides more flexibility, lesser execution time and low memory requirement in credit cards use. Which makes this most user friendly option in credit card use.

VII. Future Scope

Further enhancement in ATM PIN with Reg. Mobile modes are made to increase security and flexibility.

If both the position coordinates are same this indicates authenticated or secure transaction else transaction is under surveillance hence every movement in that account is under consideration.

There are different steps used to verify trusted bank account user

a) OTP (One Time Password) used to verify trusted user through sms facility.
b) ACM(Authentication Conveying Message) similar to OTP but there is no digit value in side message. In this case trusted user has to just convey his permission through 'Accepted' and 'Denied' option on registered mobile screen.

c) Voice Call from bank’s side if non of response given by user this may occur in exceptional case e.g if any kind of disability or ignorance etc.

-OTP sent on registerd mobile number

-Authentication Conveying Message on registerd mobile screen

-Voice call from bank's customer care

VIII. References

[1] Anil K. Jain, Jianchang Mao and K.m. Mohiuddin, ‘Artificial Neural Networks’ IEEE Computer Society Vol. 29 Issue No 03, March 1996 .

[2] Jocelyn Sietsma, Robert J.F.Dow ‘Neural Networks’ vol.4(1);67-79, 1991.

[3] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE Transaction on dependable and secure computing, Vol.5, No. 1, January-March 2008.

[4] Philip K. Chan, Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo, ‘distributed Data Mining in Credit Card Fraud Detection’ Florida Institute of Technology Columbia University, December 1999.

[5] Abhishek Bansal et.al “Face Recognition using PCA & LDA algorithm” Second International Conference on Advanced Computing & Communication Technologies 2012.

[6] Elizabeth B. Varghese, ‘Face Recognition Based On Vector Quantization Using Fuzzy Neuro Clustering’ World Academy of Science, Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering Vol.7 No.11, 2013.

[7] R. Evans, Wayne A. Tjoland, et al. “Achieving a Hands-Free Computer Interface using Voice Recognition and Speech Synthesis”, IEEE AES Systems Magazine, January 2000.

[8] R.Maskeliunas, K.Ratkevicius et.al, “Voice-based Human-Machine Interaction Modeling for Automated Information Services”, ISSN 1392 – 1215, 2011.

[9] Siva kumar T. et al., Design and Implementation of Security Based ATM theft Monitoring system, International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 1 (August 2013) PP: 01-07

[10] Sun Wiijun et al. research of GPS technology in seismic monitoring system senior engineer of costruction an management bejing china.