IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8676

Swindling of Bank Transaction Detection Based on Biometric Key Generation

Mini S[1], Dr. R. Kavitha Jaba Malar[2]

"[1]Post Graduate Scholar in Computer Science, St. John's College of Arts and Science, Ammandivilai

"[2]Associate Professor, Department of Computer Science, St. John's College of Arts and Science, Ammandivilai

Abstract: The banking sector is a very relevant zone in our modern generation. Almost each and every person has to deal with bank either manually or online. Due to a rapid amelioration in the electronic commerce technology, the exploit of credit cards and debit cards has increased. Nowadays most of the banking transactions are done through credit card, debit card and online net banking. These methods are endangered with new attacks. Swindling detection in banking area is one of the essential concepts nowadays because money is substantial part in our life. Data mining is popularly used to detect swindling effectively. It is an established process that acquires data as input and obtains models or patterns as output. Associative rule mining is used in this work. In this research the whole banking operations are concentrated and observed the performance on dataset to detect swindling by giving low risk and high customer satisfaction.

Keywords: Pixel, Ridges, Swindling, Transaction.

I. INTRODUCTION

Banking fraud occurs when someone attempts to take assets from a financial institution or from customers of that institution by posing as a bank official. Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. In many instances, bank fraud is a criminal offence. While the specific elements of particular banking fraud laws vary depending on jurisdictions, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft. For this reason, bank fraud is sometimes considered a white-collar crime. Lapses in system make easy the job of offenders to dupe banks. Fraud is any dishonest act and behavior by which one person gains or intends to gain advantage over another person. Fraud causes loss to the victim directly or indirectly. Unlike ordinary thefts and robberies, the amount misappropriated in these crimes runs into lakhs and crores of rupees. Bank fraud is a federal crime in many countries, defined as planning to obtain property or money from any federally insured financial institution. The number of bank frauds in India is substantial. It is increasing with the passage of time. Bank fraud is a big business in today's world. With more educational qualifications, banking becoming impersonal and increase in banking sector have gave rise to this white collar crime. In order to hide serious financial problems, some businesses have been known to use fraudulent bookkeeping to overstate sales and income, inflate the worth of the company's assets or state a profit when the company is operating at a loss. These tampered records are then used to seek investment in the company's bond or security issues or to make fraudulent loan applications in a final attempt to obtain more money to delay the inevitable collapse of an unprofitable or mismanaged firm. Information security is one of the cornerstones of Information Society. Integrity and privacy of financial transactions, personal information and critical infrastructure data, all depend on the availability of strong and trustworthy security mechanisms. Network and Internet connectivity has provided great benefits to the modern society in terms of sharing and accessing information, one mechanism of information security that has been the subject of much attention in recent years is the security management of the assets of important information crucial challenge. Organizations also provide clients with access everywhere for information systems and the frequency and the evolution of security threats are growing, and the need to provide security assume greater importance. Effective information security management requires security resources, including the prevention of the attack, and reducing vulnerability and threat deterrence. User authentication is performed in various ways. The focus is on PIN authentication because of its simplicity and maturity. Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. In many instances, bank fraud is a criminal offence. While the specific elements of particular banking fraud laws vary depending on jurisdictions, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft. For this reason, bank fraud is sometimes considered a white-collar crime.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8676

II. LITERATURE SURVEY

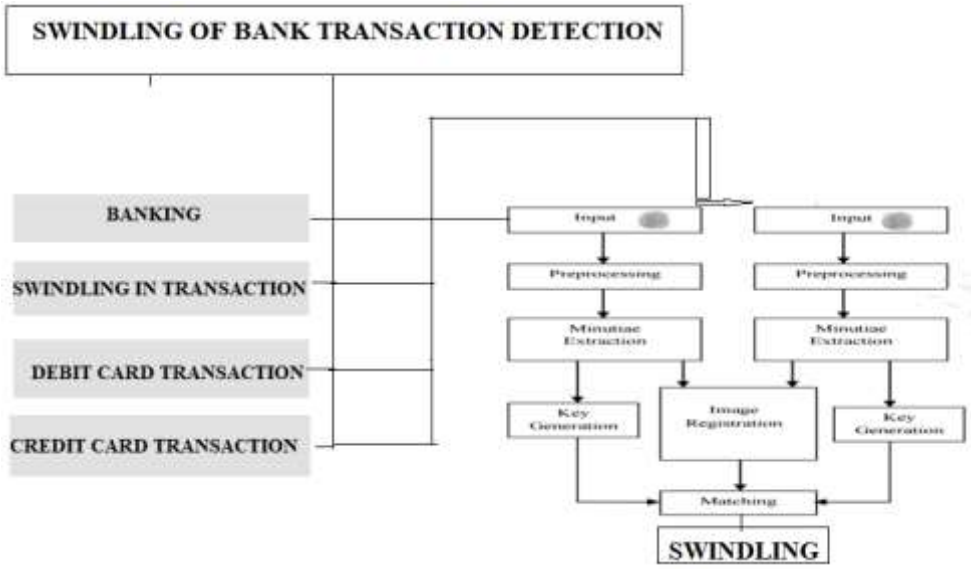
Ghosh and Reilly [1] proposed a credit card fraud detection with a neural network. They have built a detection system, which is trained on a large sample of labeled credit card account transactions. These transactions contain example fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and no received issue (NRI) fraud. The initial population is selected randomly from the sample space which has many populations. The fitness value is calculated in each population and is sorted out. In selection process is selected through tournament method. The Crossover is calculated using single point probability. Mutation mutates the new offspring using uniform probability measure. In elitism selection the best solution are passed to the further generation. Syeda et al. [2] have used parallel granular neural networks (PGNNs) for improving the speed of data mining and knowledge discovery process in credit card fraud detection. A complete system has been implemented for this purpose. Stolfo et al. [3] suggest a credit card fraud detection system (FDS) using meta learning techniques to learn models of fraudulent credit card transactions. Meta learning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models. A meta classifier is thus trained on the correlation of the predictions of the base classifiers. The same group has also worked on a cost-based model for fraud and intrusion detection. They use Java agents for Meta learning (JAM), which is a distributed data mining system for credit card fraud detection. Alekerov et al. [4] present CARDWATCH, a database mining system used for credit card fraud detection. The system, based on a neural learning module, provides an interface to a variety of commercial databases. Kim and Kim[5] have identified skewed distribution of data and mix of legitimate and fraudulent transactions as the two main reasons for the complexity of credit card fraud detection. Based on this observation, they use fraud density of real transaction data as a confidence value and generate the weighted fraud score to reduce the number of misdetections. Fan et al. [6] suggest the application of distributed data mining in credit card fraud detection. Brauset al. [7] developed an approach that involves advanced data mining techniques and neural network algorithms to obtain high fraud coverage. Chiu and Tsai [8] have proposed Web services and data mining techniques to establish a collaborative scheme for fraud detection in the banking industry. With this scheme, participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment.

III. PROPOSED METHODOLOGY

The research combines few techniques in order to get accurate and robust detection results. The system consist of four main modules

1. Banking
2. Swindling in Transaction
3. Debit Card Transaction
4. Credit Card Transaction

In banking customer account is created with the fingerprint image. For all transactions the fingerprint image is analysed for the detection of swindling. As the pre-processing step, the histogram equalization and Binarization process is done. Then minutias are extracted using cross numbering technique. Biometrics based key generation technique is used for the security of the fingerprint image. Finally, Matching is done for swindling detection.



IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8676

Figure 1: Proposed Architecture

The quality of the ridge structures in a fingerprint image is an important characteristic, as the ridges carry the information of characteristic features required for minutiae extraction. In practice, a fingerprint image may not be well defined due to the noise that corrupt the clarity of the ridge structures. Thus image enhancements are often employed to reduce the noise and enhance the definition of ridges against valleys. The mean and variance of a gray level fingerprint image, I, are defined as,

$$M(I) = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j)$$

$$VAR(I) = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} (I(i,j) - M(I))^2$$

Let I(i;j) represent the grey-level value at pixel (i;j), and N(i;j) represent the normalized gray level value at pixel (i;j). The normalized image is defined as

$$N(i,j) = \begin{cases} M_0 + \sqrt{\frac{V_0(I(i,j)-M)^2}{V}} & \text{if } I(i,j) > M, \\ M_0 - \sqrt{\frac{V_0(I(i,j)-M)^2}{V}} & \text{otherwise,} \end{cases}$$

Where M and V are the estimated mean and variance of I(i;j), respectively, and M_0 and V_0 are the desired mean and variance values, respectively. The local orientation at pixel (i;j) can then be estimated using the equation

$$V_x(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} 2\partial_x(u,v)\partial_y(u,v),$$

$$V_y(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} \partial_x^2(u,v)\partial_y^2(u,v),$$

$$\theta(i,j) = \frac{1}{2}tan^{-1}\frac{V_y(i,j)}{V_x(i,j)},$$

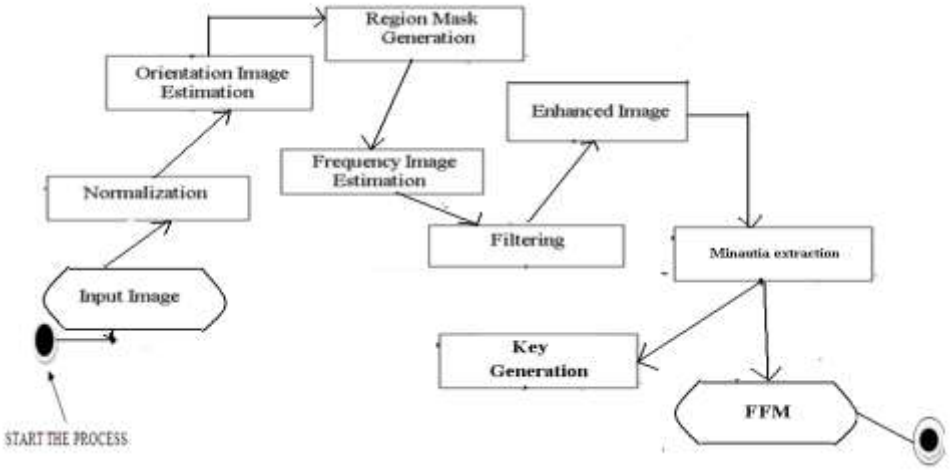


Figure 2: Activity Diagram of the system

The minutiae are extracted by scanning the local neighbourhood of each ridge pixel in the image using a 3×3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighbourhood.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8676

$$CN = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i-1}|, \quad P_9 = P_1$$

Where Pi is referred as the pixel value related to the neighbourhood P. For a pixel P, its eight neighbouring pixels are scanned in an anti-clockwise direction as follows:

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Table 1: 3×3 window for searching minutiae

The pixel can then be classified according to the property of its CN value. Using the properties of the CN as

CN	Property
0	Isolated Point
1	Ridge Ending Point
2	Continuing Ridge Point
3	Bifurcation Point
4	Crossing Point

Table 2: CN property

A pixel is thus classified as a ridge ending if it has only one neighbouring ridge pixel in the window, and classified as a bifurcation if it has three neighbouring pixel and continuing ridge point if it has two neighbouring pixels etc. The 64-bit key generator block is further divided into sub-blocks portraying in details the inner working of the block. The input JPEG/JPG is converted to binary image. The black pixels that denote ridges and the white pixels that denote valleys are employed by almost all minutiae extraction algorithms. A grey level image is translated into a binary image in the process of binarization, by which the contrast. For each 3X3 window, If the central pixel is 1 and has exactly 3 one-value neighbours, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 One-value neighbour, then the central pixel is a ridge ending.

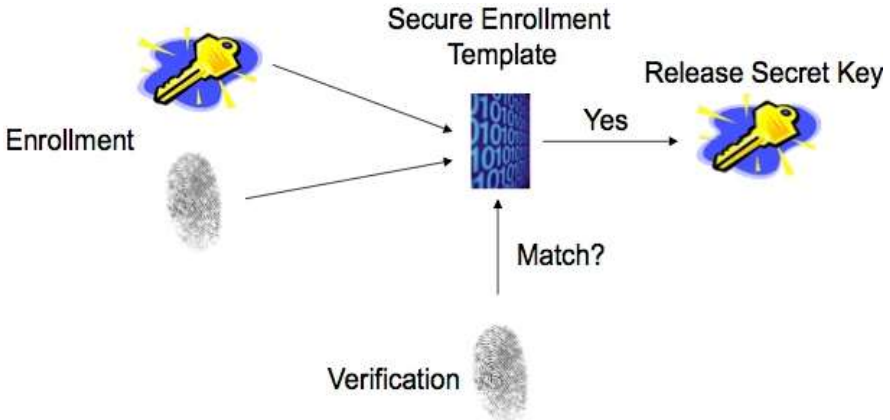


Figure 4: Secure Banking

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8676

IV. RESULT AND DISCUSSION

During FAR determination, a fraud attempt is an attack using the characteristics of non-authorized persons. This, however, pretends a high security which may not be present since there are a lot of further possibilities for promising attacks. A fraud attempt is successful if the user interface of the application provides a successful message or if the desired access is granted. A fraud attempt counts as rejected if the user interface of the application provides an unsuccessful message. In cases where no unsuccessful message is available, a verification time interval has to be given to ensure comparability. If the verification time interval has expired the fraud attempt is counted unsuccessful.

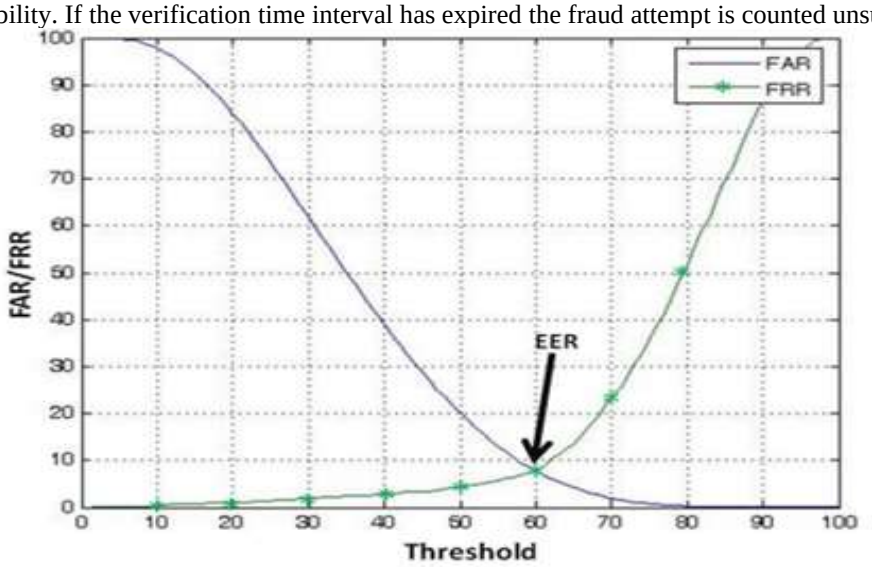


Figure 5: Threshold VS FAR, FRR

V. CONCULSION

Swindling of bank transaction is a serious issue when it comes to payment nowadays seeing how we are in the consumer era and to mitigate that particular problem, we built a model that can distinguish between normal transactions from a fraudulent one. In this research, the model built using Artificial Neural Networks with imaging. We minimized the error function using the algorithm which resulted in a model that correctly predicts 99.48% of the time. We can conclude that this model is a generalized model and very reliable which can be used to detect any type of fraudulent transactions.

REFERENCES

[1]. R. J. Bolton and D. J. Hand. Unsupervised profiling methods for fraud detection. In conference of Credit Scoring and Credit Connol VII, Edinburgh. UK, Sept 5-7,2001.
[2]. Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, ―A review of Fraud Detection Techniques: Credit Card‖, International Journal of Computer Applications (0975 –8887) Volume 45–No.1, May 2012
[3]. K. C. Cox, S. G. Eick, G. J. Wills, andR. J. Brachman.Visual data mining: Recognizing telephone calling fraud.J Data Mining and Knowledge Discover, 1(2):22>231, 1997.
[4]. Hollmn and Jaakko. Pmbabilistic Appmaches to FraudDetecrion,Licentiate's ntesis. Helsinki University of Technology,Department of Computer Science andEngineering, 1999.
[5]. X.D. Hoang, J. Hu, and P. Bertok, ―A Multi-Layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls,‖ Proc. 11th IEEE Int'l Conf. Networks, pp. 531-536, 2003.
[6]. Masoumeh Zareapoor, Seeja.K.R, and M.Afshar.Alam, ―Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criterial‖, International Journal of Computer Applications (0975 –8887) Volume 52–No.3, August 2012
[7]. T. Lane, ―Hidden Markov Models for Human/Computer Interface Modeling,‖ Proc. Int'l Joint Conf. Artificial Intelligence, Workshop Learning about Users, pp. 35-44, 1999.
[8]. Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, ―A review of Fraud Detection Techniques: Credit Card‖, International Journal of Computer Applications(0975 –8887) Volume 45–No.1, May 2012.
[9]. Hidden Markov Model by Jia Li. Department of Statistics ―The Pennsylvaniastate University ‖http://www.stat.psu.edu/~jiali/course/stat597e/notes2/hmm.pdf
[10]. A Revealing Introduction to Hidden Markov Models‖by mark stamp
[11]. Credit card Fraud Detection with a neural network‖ by Ghosh and Reilly. IEEE‖ Proceedings of the Twenty Seventh Annual Hawaii International Conference on System Sciences,1994.