MULTI-LEVEL ACCESS CONTROL SYSTEM IN AUTOMATED TELLER MACHINES

[*]ISMAILA W. OLADIMEJI, [**]OMIDIORA E. OLUSAYO, [***]ISMAILA FOLASADE M. [****]OLAJIDE A. TAIWO

[,**]Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria [***]Department of Computer Science, Osun State Polytechnic, Iree, Nigeria. [****]Department of Computer Science, Kwara State Polytehnic, Ilorin, Nigeria*

ABSTRACT

E-commerce theft involves using lost/stolen debit/credit cards, forging checks, misleading accounting practices, etc. Due to carelessness of cardholders and criminality activities of fraudsters, the personal identification number (PIN) and using account level based fraud detection techniques methods are inadequate to cub the activities of fraudsters. In recent times, researchers have made efforts of improving cyber-security by employing biometrics traits based security system for authentication. This paper proposed a multi-level fraud detection system in automated teller machine (ATM) operations. The system included PIN level, account-level and biometric level. Acquired RealScan-F scanner was used to capture liveness fingers. Transactional data were generated for each individual fingerprint with unique PIN. The results of the simulation showed that (i) the classification at account level only yielded 94.5% accuracy and 5.25% false alarm rate; (ii) matching at biometric level only yielded 100% accuracy and 0% false alarm rate; (iii) combine matching at the three levels produced 84.7% accuracy and 2.65% false alarm rate; (iv) while the classification using voting technique yielded 97.35% accuracy and 0.47% false alarm.

Keyword: *E-commerce, personal identification number, automated teller machine, account level, fraud* detection, liveness fingers, RealScan-F

INTRODUCTION

An ATM was created by City Bank of New York in 1960, the idea was for customers, without a teller, to pay utility bills and get a receipt. In the last few years, there have been many reports of hacking into the electronic ATM system and caused billion dollars of losses in the banking company itself. Some popular ATM frauds includes: skimming attack, card trapping, PIN cracking, phishing attack, ATM malware, ATM hacking, physical attack, etc. In e-commerce, credit card fraud is an emerging problem. The danger of these fraudulent activities prompted the researchers to innovate different fraud detection/prevention techniques with emphasis on machine learning algorithms [1,29]. Some of the supervised and unsupervised machine learning algorithms used include Hidden Markov Model [2,3]*;* Neural Network [4,5]; Decision Trees [6]; Genetic Algorithm [7,8]; Artificial Immune System [9]; hybridized algorithms [10,11,12]; Meta-learning techniques [13-16]; evolution-fuzzy [28] Dempster-Shafer theory and Bayesian learning [17]; Lago in 2008 [18] used five methods of classification for fraud detection: Naive Bayes, Bayesian Network, Artificial Immune System and Decision Tree. In [19] work, Communal detection and Counter Propagation Neural Network were employed to identity theft detection in online transactions.

However, those software based fraud detection systems still showed some level of false alarm rate hence there is need for improvement to produce robust security system that will greatly reduce the activities of fraudsters.

Biometric identification is utilized to verify a person's identity by measuring digitally certain human characteristics and comparing those measurements with those that have been stored in a template for that same person. Biometric techniques include fingerprint, iris, hand geometry-vein, ear, sweat pores, handwritten signature, keystroke and speech. With biometrics, such fraudulent incidents can be minimized, as an added layer of authentication is now introduced that ensures that even with the correct PIN information and in possession of another person's ATM card, the user's biometric features cannot easily be faked [20]. To discourage potential attackers from presenting a fake finger or, even worse, to force a legitimate user of the system to present his finger, or even to halt a person to gain access, the system must be augmented by a liveness detection system. To prevent false acceptance there is need to recognize whether the finger on the plate of the fingerprint sensor is alive or

not. Liveness detection methods have properties which include, non-invasive, reliable, user friendly, fast and low cost. Fingerprint liveness detection methods have been developed as an attempt to overcome the vulnerability of fingerprint biometric systems to spoofing attacks. [21,22,23]. In the literature, several works have been done which include [24, 25,27,28,29,30,31,32,33,34]. Thus, this research is based on employing liveness biometrics cum transactional based fraud detection system in addition to improve the security aspect of ATM transactions from fraudulent activities.

Materials

A. Hardware Specifications

The devices used for this research are

(i) Intel-based Laptop computer equipped with the Intel AtomTMN270 3.0 GHz CPU, 5 GB of RAM and 8 Windows XP Embedded.

(ii) RealScan-F, is a single finger/palm-print live scanner, featuring Suprema's cutting-edge optical, it is capable of capturing highest quality images regardless the physical condition of fingers.

Figure 1: Fingerprint Scanner LF10

B. Software Requirements

The software employed are MatLabverion17, Microsoft Office package, Java package and SQL package.

C. Radial Basis Function Networks

The radial basis function (RBF) network has its foundation in the conventional approximation theory. It has the capability of universal approximation. The RBF network is a popular alternative to the well-known multilayer perceptron, since it has a simpler structure and a much faster training process.

The RBF network is a three-layer $(J_1\text{-}J_2\text{-}J_3)$ feedforward neural network, as shown in Figure 2. Each node in the hidden layer uses a RBF, denoted $\phi(r)$, as its nonlinear activation function. The hidden layer performs a nonlinear transform of the input, and the output layer is a linear combiner mapping the nonlinearity into a new space. Usually, the same RBF is applied on all nodes;

that is, the RBF nodes have the nonlinearity $\phi_i(\vec{x}) = \phi(\vec{x} - \vec{c}_i), i = 1, \ldots, J_2$, where $\vec{c}_i$ is the prototype or center of the *i*th node and $\phi(\vec{x})$ is an RBF.

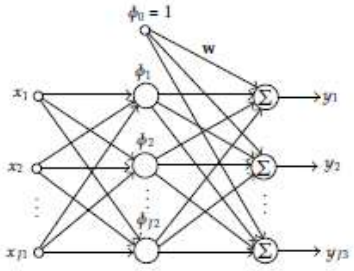

Figure 2: Architecture of the RBF network. [35]

For input $\vec{x}$, the output of the RBF network is given by

$$y_i(\vec{x}) = \sum_{k=1}^{J_2} w_{ki}\phi(\|\vec{x} - \vec{c}_k\|), \quad i = 1, \ldots, J_3, \tag{1}$$

where $y_i(\vec{x})$ is the *i*th output, w_{ki} is the connection weight from the *k*th hidden unit to the *i*th output unit, and $\|\cdot\|$ denotes the Euclidean norm. The RBF $\phi(\cdot)$ is typically selected as the Gaussian function, and such an RBF network is usually termed the Gaussian RBF network.

RBF network learning can be formulated as the minimization of the MSE function

$$E = \frac{1}{N}\sum_{i=1}^{N}\left\|\vec{y}_p - \mathbf{W}^T\vec{\phi}_p\right\|^2 = \frac{1}{N}\left\|\mathbf{Y} - \mathbf{W}^T\mathbf{\Phi}\right\|_F^2 \tag{2}$$

RBF networks have now used in a vast variety of applications, such as face tracking and face recognition , robotic control antenna design, channel equalizations, computer vision and graphics [35].

D. Particle swarm optimization (PSO)

PSO is a stochastically global optimization method that belongs to the family of Swarm Intelligence and Artificial Life. It is based on the principles that flock of birds, school of fish, or swarm of bees searches for food sources where at the beginning the perfect location is not known. However, they eventually reach the best location of food source by means of communicating with each other.

In the PSO, particles are evolved by cooperation among the individuals themselves; hence it can be classified as a population-based technique, where the entire population is called swarm. Each particle represents a possible solution to the optimization problem, and these particles adjust its flying

trajectory according to its own flying experience and other particles' flying experience [37,38]. The PSO algorithm is in figure 3.

1. Initialize all particles in the swarm to random positions within the search space.
2. Initialize velocity vectors.
3. Initialize particle personal best positions to be equal to the current positions of the particles.
4. Repeat until converged:
   (a) Update the fitness of each particle i using the fitness function f and the particle's current position.
   (b) Update each particle's personal best position
   (c) Update the global best particle position
   (d) Update each particle's velocity.
   (e) Update each particle's position.

Figure 3: The general PSO Algorithm [38]

E. Support Vector Machines

Support Vector Machines (SVM) algorithms was introduced by [39] and makes use of unlabelled data in order to perform unsupervised novelty detection in high-dimensional data. As for SVM, this algorithm is based on the use of a kernel (linear, polynomial, sigmoid or RBF) and uses the kernel trick in order to compute the dot product between data points represented in a high-dimensional space to find a separating hyperplane.

SVM which is developed by Vapnik (1995) is based on the idea of structural risk management (SRM). SVM is a relatively new computational learning method constructed based on the statistical learning theory classifier (Chiu and Guao, 2008). SVM is based on the concept of decision planes that define decision boundaries. A decision plane is one that separates between a set of objects having different class memberships. SVM creates a hyperplane by using a linear model to implement nonlinear class boundaries through some nonlinear mapping input vectors into a high-dimensional
feature space.

For a binary classification problem where there are only two classes in the training data yi = {−1, 1} a hyper-plane can
be defined as:

$W.x + b = 0$ (3)

Where *W* is the normal to the hyper-plane as shown in equation 6 and offset parameter *b* allows us to increase the margin. |*b*| / |*W*| is the parameter that determines the shortest distance of the plane from the origin. For a good classification model the positive and negative examples of the training data should fulfil the following two conditions:

W x b for y (4)

These inequalities can be combined into one set of inequalities:

yi (*W.xi* + *b*) ³ 1"1"*i* (5)

The SVM finds an optimal hyper-plane responsible for the largest separation of the two classes. In nonlinear SVM, the
training samples are mapped to a higher dimensional space with the help of a kernel function *K(xi ,xj)* instead of the inner
product <*xi* , *xj* > . Some of the famous kernel functions are the polynomial kernels, radial basis function kernels, and
linear kernels (Radhika and Shashi, 2009). The equations for these kernels are shown in equation 6, 7 and 8.

Linear Kernel Function:

$$k(x_i, x_j) = 1 + x_i^T x_j \quad (6)$$

Polynomial Kernel Function:

$$k(x_i, x_j) = (1 + x_i^T x_j)^p \quad (7)$$

Radial Base Function

$$k(x_i, x_j) = exp(-\partial || x_i - x_j ||^p) \quad (8)$$

Where $k(x_i, x_j)$ is the kernel function where each data from set *xi* has an influence on the kernel point of test value *xj*.

Θ is a parameter for RBF kernel and *p* is the number of polynomial degrees for polynomial kernel function. This study considered linear kernel, Polynomial and RBF as a kernel function in SVM model implementation. Choice of kernel functions is the main parameter experimented together with *C* penalty

parameter. For each kernel function experimented, the parameters associated with the kernel function that can also have impact on the results are considered.

Elmi A., Sallehuddin R., Ibrahim S., Zain M. (2014). Classification of SIM Box Fraud Detection Using Support Vector Machine and Artificial Neural Network, International Journal of Innovative Computing 4:2, 19-27

Vapnik, V. (1995). The Nature of Statistical Learning Theory. Springer, New York.

Chiu, N.H., & Guao, Y.Y. (2008). State classification of CBN grinding with support vector machine, Journal of

Material Processing Technology, 201, 601-605

F. Voting Strategy

Every model makes a prediction (votes) for each test instance and the final output prediction is the one that receives more than half of the votes. If none of the predictions get more than half of the votes, we may say that the ensemble method could not make a stable prediction for this instance.

Majority Voting

Voting methods are based on a democratic (weighted) process that combines the predictions provided by the classification models independently calibrated on a number of available analytical sources. The most simple and intuitive approach is based on majority voting rule, which assigns a sample on the basis of the most frequent class assignment ("loose" method), whereas the sample is not classified in case of ties.

Ballabio D., and. Consonni V, (2019). Data Fusion Methodology and Applications, in Data Handling in Science and Technology, https://www.sciencedirect.com/science/article/pii/B9780444639844000053

Chenggang W., Ke L., Zhihong W., and Qijun Z. (2015). A DCNN Based Fingerprint Liveness Detection Algorithm with Voting Strategy, CCBR 2015, LNCS 9428, 241–249.

G. Performance Metrics

i. Performance Metrics employed for fraud detection include

- ***False Positive rate*** (FP_{rate}) is the number of false positives relative to the sum of the number of false positives and true negatives. $FP_{rate} = FP/(FP + TN)$,
- ***True positives rate*** or ***recall*** is the number of true positives relative to the sum of the true positives and the false negatives.

$$recall = \frac{|true\ positives|}{|true\ positives + false\ negatives|}$$

- False Negative Rate is the number of false negatives relative to the sum of the true positives and the false negatives. FN_{rate} = FN/(TP+FN)
- True Negative Rate (TN_{rate}) is the true false detections relative to the sum of the true false detections and the false positive. TN_{rate} = TN/ (TN + FP),
- False Alarm Rate (FA_{rate}) is the number of false positives relative to the sum of the number of true positives and the false positives.
- **Precision** allows us to measure the number of samples that have been correctly classified for a given class divided by the number of samples predicted in this class.

$$precision = \frac{|true\ positives|}{|true\ positives + false\ positives|}$$

- TP_{rate}represents the ratio of positive class that was correctly identified.
- FP_{rate}represents the ratio of the negative cases that was incorrectly identified as positive.
- Accuracy is the quality measurement for classifier, which can be calculated through mathematically finding the ratio of correct classified attempts number according to the total number of all classification attempts.

$$Accuracy = \frac{TP+TN}{TP+FN+TN+FP}\ x\ 100 \qquad (3.8)$$

$$FAR = False\ Acceptance\ Rate = \frac{FP}{(TP + TN + FP + FN)}\ x\ 100$$

$$FRR = False\ Rejection\ Rate = \frac{FN}{TN + FP + TP + FN}\ x\ 100$$

Fan, W., Miller, M., Stolfo, S., Lee, W. & P Chan. 2001. Using Artificial Anomalies to Detect Unknown and Known Network Intrusions, Proc. of ICDM01; 123-248.

Kokkinaki, A. 1997. On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling, Proc. of IEEE Knowledge and Data Engineering Exchange Workshop; 107-113

ii. Performance measures for biometric systems are classified into verification systems in which a biometric matcher makes a 1:1 match decision and identification systems which makes a 1:m match decision. Some of the metrics used include:

- True positive (TP): number of users that have been correctly authenticated;
- False positive (FP): number of impostors that have been authenticated;
- **Genuine attempt** A single attempt by a user to match his/her own stored template.
- **Impostor attempt** The opposite – a user's template is matched against someone else's template.
- *False Match / False Acceptance*
  Proportion of impostor attempts that are falsely declared to match a template of another object. That is Number of false acceptance / Number of impostor attempts
- *False NonMatch / False rejection*
  Proportion of genuine attempts that are falsely declared not to match a template of the same object. That is Number of False rejection / Number of genuine user attempt
- **Receiver Operating Characteristics (ROC):** A graphical representation giving a relationship between FAR and FRR.
- **Equal Error Rate** is a threshold set to evaluate the performance of the recognition, which is a midpoint region between False accept and false reject in ROC plot
- **Normal Presentation Classification Error Rate** (NPCER) is given by the proportion of normal (live) presentations incorrectly classified as attack (non-live) presentations and
- **Attack Presentation Classification Error Rate** (APCER) is given by the proportion of attack (non-live) presentations incorrectly classified as normal (live) presentations.

[33] Ghiani L., Yambay D. A., Mura V., Marcialis G. L., Roli F., and Schuckers S. (2017), "Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015," Image and Vision Computing, vol. 58, pp. 110–128.

METHODOLOGY

The system architecture, as shown in figure 4, include bank headquarter that has a central database, bank branches and their ATM outlets being connected by internet facilities. The central database is equipped with fraud detection system to screen cardholder new transactions. The ATM machines are equipped with biometric scanning system to capture the cardholder traits for authentication.

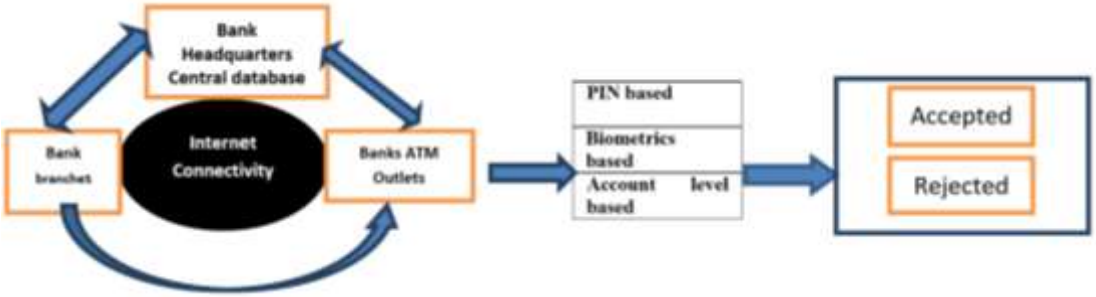

Figure 4: The Proposed System Architecture

i. Liveness Biometric level

This section entailed the steps involved in executing this proposed liveness fingerprint system viz; Sample dataset, Image pre-processing, feature extraction, and image matching as shown in figure 5.

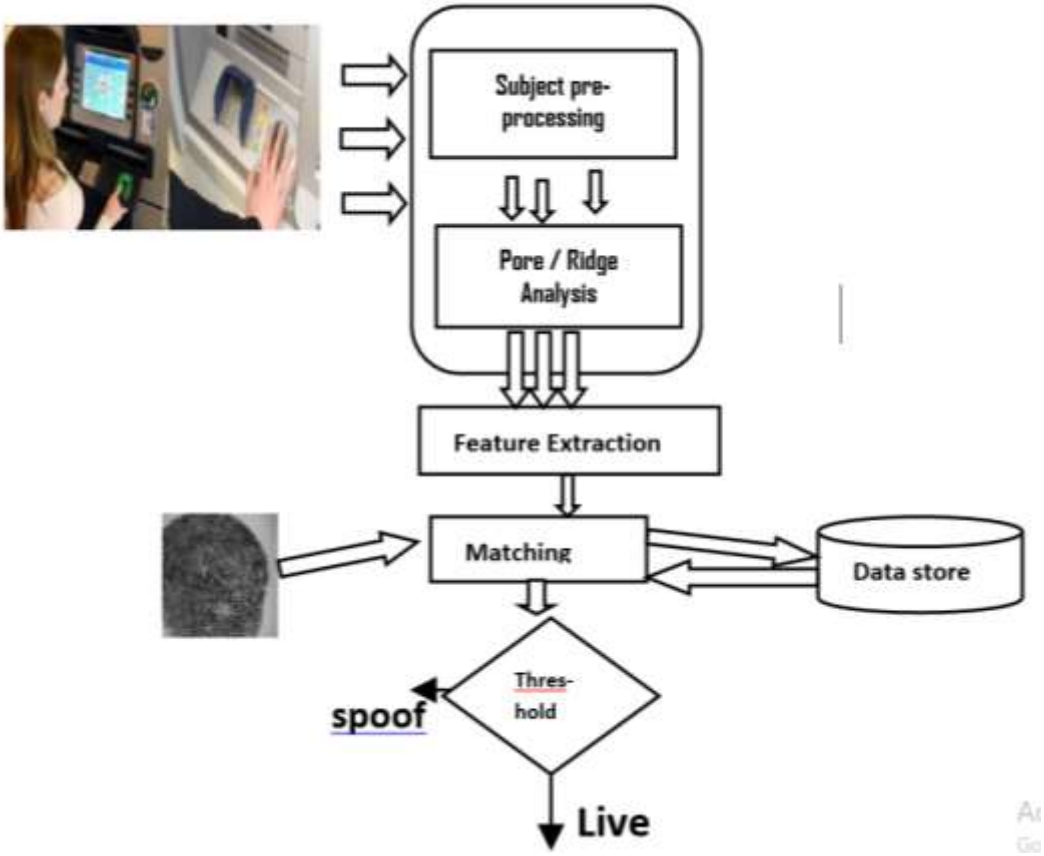

Figure 3: *The work flow of biometric system*

Sample dataset: The sample dataset used for the experimentation consists 200 live finger images captured by RealScan-F samples and 200 ordinary finger images.

Image pre-processing The stage involves enhancement of image by using (i) histogram equalization to adjusting the pixel intensities of image to enhance the contrast, (ii) binarization (the operation that converts the gray scale image into binary image, and (iii) morphological thinning **(**was used to remove selected foreground pixels from binary images**).**

Feature Extraction After the enhancement of the fingerprint image the next step was feature extraction by PSO algorithm. This method extracted the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel. Also, the frequency /number of pores along the ridge segments is extracted. In addition to the pore spacing features, the total number of pores detected relative to the total length of all ridge segments is determined.

Matching A biometric identification system's task is finding a biometric object in a database matching a query biometric object. In this work SVM was used for the classification task.

ii. Transaction/Account level based

.

A simulator was used to generate four thousand transactions sparsely intertwined by malicious transactions. Relevant attributes were selected by PSO and encoded to include several indicator variables to make it suitable for the RBF algorithm and the categorical response variables anticipated, for instance the predicted response class label y, was dichotomously defined as follows:

$$y = W(x) = \begin{cases} 0, & if\ a\ transaction\ is\ genuine \\ 1, & if\ s\ transaction\ is\ malicious \end{cases} \quad (1)$$

The stepwise procedures of the RBF-PSO algorithm are presented below: (population size of 100 is used).

Step 1: Generate random population of N, Set parameter ω_{min}, ω_{max}, c_1 and c_2 of PSO

Step 2: Initialize population of particles having positions x_j and velocities v_j

Step 3: Set iteration k = 1

Step 4: Calculate fitness of particles $F_{ij} = f(\widehat{H}_{LS})$ and find the index of the best particle b

The fitness function for parameters selection is as follow

The length of the particles is determined by the number of input factors, the number of layers, and

the number of nodes in each layer. The total length of the particle L was calculated as

$$\widehat{H}_{LS} = n_{input} * n_1 + \sum_{i=1}^{k-1}(n_j * n_{i+1}) + n_k$$

Where "n" input is the number of input attributes for the RBF, k is the number of internal layers, and

n_i is the number of nodes in layer. The last term in the equation is for the weights between the last internal layer and the output layer, which consists of a single node.

Step 5: Select $Gbest_{ij} = \widehat{H}_{LS}$ and $Pbest_{ij} = H$

Step 6: $\omega = \omega_{max} - k \times (\omega_{max} - \omega_{min}) \,/\, Max\_no$

Step 7: Update velocity and position of particles

$$\vec{v}_{ij} = \omega\vec{v}_{ij} + c_1 r_1\left(P_{best} - \widehat{H}_{LS}\right) + c_2 r_2\left(P_{best} - \widehat{H}_{LS}\right) + c_3 r_3\left(G_{best} - \widehat{H}_{LS}\right)$$

$$\vec{x}_{ij} = \vec{x}_{ij} + \vec{v}_{ij}$$

Step 8: Evaluate fitness $F_{bj} = f(\widehat{H}_{LS})$ and find the index of the best particle b_1

Step 9: Update $Pbest$ of population

If $F_{ij} < F_{bj}$ then $Pbest_{bj} = H$ else

$$Pbest_{ij} = Pbest_{bj}$$

Step 10: Update $Gbest$ of population

If $F_{ij} < F_{bj}$ then $Gbest_j = Pbest_{bj}$ and set $b = b_1$ else

$$Gbest_{bj} = Gbest_j$$

Step 11: If $k < Max\_no$ then $k = k + 1$ and goto step f else goto step l

Step 12: Output optimum solution as $Gbest_{bj}$. $Gbest_{bj} = H_{LS}$

EVALUATION METRICS

Discussion of Results

The proposed system was implemented in MATLAB environment. The parameter setting for PSO is 100 population. The scanner captured two hundred liveness fingerprints of cardholders and stored in database. A simulator generated twenty transactions each for cardholders with ten malicious transactions for ten cardholders. Also, a simulator generated four digit valid PINs for one hundred and ninety cardholders and ten invalid for ten cardholders.

Seventy percent of the transactional data were trained and thirty percent were tested. The results of the simulation showed that (i) the classification at account level only yielded 94.5% accuracy and 5.25% false alarm rate; (ii) matching at biometric level only yielded 100% accuracy and 0% false alarm rate; (iii) combine matching at the three levels produced 84.7% accuracy and 2.65% false alarm rate; (iv) while the classification using voting technique yielded 97.35% accuracy and 0.47% false alarm.

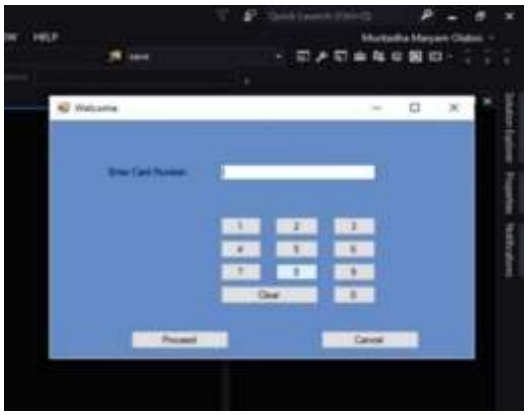

Figure 6. Cardholder PIN Interface system interface

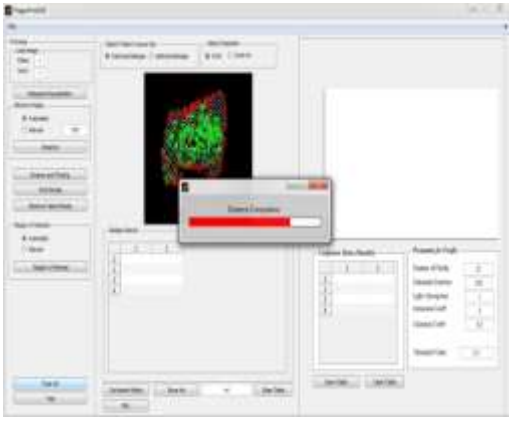

Figure 7: the Biometric

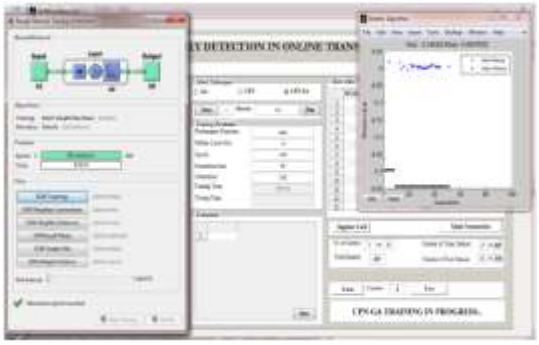

Figure 2: Account level Fraud detection Interface

CONCLUSION

The paper proposed three steps user authentications approach to ATM security system. The proposed system encompassed PIN level, account-level and biometric level. The account level approach was designed with PSO-RBN for attribute selection and classification. The liveness finger-based biometric level approach was designed using PSO for feature selection and SVM for matching.

PIN codes and transactional data were generated for each liveness fingerprint individual. Two hundred was liveness fingers were captured using RealScan-F scanner and four thousand transactions for the cardholders. The system was implemented using MATLAB software.

REFERENCES

[1] Falaki S. O., Alese B. K., Ismaila W. O. (2010): An Update Research on Credit Card On-Line Transactions, International Journal of Economic Development Research and Investment, 1 (2&3), 181- 190. Nigeria.

[2] Falaki S. O., Alese B. K., Adewale O. S., Ayeni J. O., Aderounmu G. A. and Ismaila W. O. (2012). Probabilistic Credit Card Fraud Detection System in Online Transactions" In: *International Journal of Software Engineering and Its Applications*, Vol. 6, No. 4.

[3] Iyer, D., Arti M., Janardhan S., Rathod D., and Sardeshmukh A. "Credit card fraud detection using Hidden Markov Model." In Information and Communication Technologies.

[4] Raghavendra P., Lokesh S. (2011). "Credit Card Fraud Detection Using Neural Network", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-NCAI2011.

[5] Ghosh S. and Reilly D.L., (1994). "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences: Information Systems: Decision Support and Knowledge Based Systems, vol. 3, pp. 621-630.

[6] Dhanapal R., and Gayathiri. P, (2012) "Credit Card Fraud Detection Using Decision Tree for Tracing Email and IP," International Journal of Computer Science Issues (IJCSI) Vol. 9, Issue 5, No 2.

[7] RamaKalyani K.. and UmaDevi D. (2012). "Fraud Detection of Credit Card Payment System by Genetic Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 7.

[8] Rinky D. P., and Dheeraj K. S. (2013). "Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6.

[9] Arunabha M., Mukherjee S. and Mahanti A. (2011) " Artificial Immune System for detecting online credit card frauds," Research Front, www.csi-india.org, CSI Communications.

[10] Ismaila W. O., and Ismaila Folasade. M., (2019). Hybridization of Neural Network-Cum-Evolutionary Algorithm Variants For Fraud Detection In Credit Cards Online Transaction, International Journal Of Innovative Science, Engineering and Technology (IJISET), Vol. 6, Issue 9, pp 524- 529.

[11] Pooja C., A.D. Thakare , Prajakta K. , Madhura G., Priyanka N., (2015). Genetic K-means Algorithm for Credit Card Fraud Detection, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2), 1724-1727.

[12] You D., Jin Y., Xiaoxin T., Han Z. and Minyi G. (2016). Online Credit Card Fraud Detection: A Hybrid Framework with Big Data Technologies, 2016 IEEE TrustCom/BigDataSE/ISPA.

[13] Chan, P., Fan, W., Prodromidis, A. & Stolfo, S. (1999). Distributed Data Mining in Credit Card Fraud Detection. IEEE Intelligent Systems 14: 67-74.

[14] Chen, R., Chiu, M., Huang, Y. & Chen, L. (2004). Detecting Credit Card Fraud by Using Questionaire-Responded Transaction Model Based on Support Vector Machines. *Proc. of IDEAL2004*, 800-806.

[15] Joseph P., Yuri L. (2012). "Improving Credit Card Fraud Detection using a Meta-Classification Strategy", International Journal of Computer Applications (0975 – 8887) Volume 56– No.10.

[16] Gajendra S., Ravindra G., Ashish R., Mahiraj D., S. Chandel, A. Riyaz (2012) "A Machine Learning Approach for Detection of Fraud based on SVM", International Journal of Scientific Engineering and Technology (ISSN: 2277-1581), Volume No.1, Issue No.3, pg : 194-198.

[17] Panigrahi S., Kundu A., Sural S., and Majumdar A. (2009). "Credit card fraud detection: A Fusion Approach using Dempstershafer Theory and Bayesian learning," Information Fusion, vol. 10, no. 4, pp. 354 – 363.

[18] Gadi, Wang, Lago; (2008). Comparison with Parametric Optimization in Credit Card Fraud Detection; IEEE; 2008.

[19] Ismaila W. O., Falohun A. S., Babalola O. R., Ismaila F.. M. Ogunjimi T. O., (2019). Soft Computing: Investigation of Two-Step Approach to Identity Theft Detection in Electronic Payments, Proceedings for Academic Conference of The Sub-Sahara African Academic Research Publications on Unleaching Sub-Sahara African Resources. Vol. 18, No. 2, Nigeria.

[20] Sousedik, C.; Busch, C. (2014). Presentation attack detection methods for fingerprint recognition systems: A Survey. IET Biom. 2014, 3, 219–233.

[21] Sequeira F. and Cardoso S. (2015). Fingerprint Liveness Detection in the Presence of Capable Intruders, Sensors 2015, 15, 14615-14638; doi:10.3390/s150614615, OPENACCESS sensors ISSN1424-8220.

[22] Memon, S.; Manivannan, N.; Boulgouris, A.; Balachandran, W. (...). Fingerprint Sensors: Liveness Detection and Hardware Solutions. In Sensors and Biosensors, MEMS Technologies and its Applications; Yurish, S., Ed.; Volume 2, pp. 121–148.

[23] Babu A., and Paul V. (2016). A Survey on Biometric Liveness Detection Using Various Techniques, International Journal of Innovative Research in Computer and Communication Engineering, *(An ISO 3297: 2007 Certified Organization),* Vol. 4, Issue 11, pp-20055-20061.

[24] Ismaila W. O, Ogunjinmi T.O., Babalola O. R., Ismaila F.. M. (2019). Biometric Automated Teller Machines Based Anti-Spoofing Fingerprint System, International Journal of Embedded and Software Computing. Vol. 9 Issue No.9, pp- 23789- 23792.

[25] Kamble P., and Nikumbh S. (2015) Security System in ATM using Multimodal Biometric System and Steganographic Technique International Journal of Innovative Research in Science, Engineering and Technology. Vol. 4, Issue 4.

[26] Tan B., Schuckers S., (2005). Liveness detection using an intensity based approach in fingerprint scanner, Proceedings of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21.

[27] Tome P., Raghavendra R., Busch C., Tirunagari S., Poh N., Shekar B. H., Gragnaniello D., Sansone C., Verdoliva L., and Marcel S.. (2015). The 1st competition on counter measures to fingervein spoofing attacks. In The 8th IAPR International Conference on Biometrics (ICB), May 2015.

[28] Bentley P. J., Kim J., Jung G.-H. and Choi J.-U., (2000). "Fuzzy Darwinian detection of credit card fraud," in the 14th Annual Fall Symposium of the Korean Information Processing Society, 14th October, 2000.

[29] Delamaire L, Abdou, HAH and Pointon, J, (2009). Credit card fraud and detection techniques: a review, Banks and Bank Systems, Volume 4, Issue 2, 57-68.
[30] Nogueira F., Lotufo R., and. Machado R., (2016). "Fingerprint liveness detection using convolutional neural networks," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1206–1213.
[31] Schuckers S. A., Abhyankar A., (2004). A Wavelet Based Approach to Detecting liveness in Fingerprint Scanners, Proceedings of Biometric Authentication Workshop, ECCV, Prague.
[32] Parthasaradhi S, Derakhshani R, Hornak L, Schuckers S. A. (2005)., Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 35, pp. 335- 343.
[33] Wang C., Li K., Wu Z, and Zhao Q. (2015). A DCNN Based Fingerprint Liveness Detection Algorithm with Voting Strategy, CCBR 2015, LNCS 9428, pp. 241–249.
[34] Dubey R. K., Goh J., and Vrizlynn L. Thing L. (2016). Fingerprint Liveness Detection From Single Image Using Low Level Features and Shape Analysis, IEEE, http://dx.doi.org/10.1109/TIFS.2016.2535899
[35] Wu Y., Wang H., Zhang B., and K. L. Du, (2012). Using Radial Basis Function Networks for Function Approximation and Classification, International Scholarly Research Network ISRN Applied Mathematics, Volume 2012.
[36] Fan S. and Jen C. (2019). An Enhanced Partial Search to Particle Swarm Optimization for Unconstrained Optimization, Mathematics 2019, 7, 357; doi:10.3390/math7040357
[37] Eberhart, R.C.; Dobbins, R.C.; Simpson, P. (1996). Computational Intelligence PC Tools; Academic Press Professional: Boston, MA, USA.
[38] Kennedy, J.; Eberhart, R. (1995). "Particle Swarm Optimization". Proceedings of IEEE International Conference on Neural Networks.
[39] Chiu, N. & Guao, Y. (2008). State classification of CBN grinding with support vector machine, Journal of Material Processing Technology, 201, 601-605
[40] Vapnik, V. (1995). The Nature of Statistical Learning Theory. Springer, New York.
[41] Elmi A. H., Sallehuddin R., Ibrahim S., Zain A. M. (2014). Classification of SIM Box Fraud Detection Using Support Vector Machine and Artificial Neural Network, International Journal of Innovative Computing 4:2, 19-27.
[42] Chenggang W., Ke L., Zhihong W., and Qijun Z. (2015). A DCNN Based Fingerprint Liveness Detection Algorithm with Voting Strategy, CCBR 2015, LNCS 9428, 241–249.
[43] Fan, W., Miller, M., Stolfo, S., Lee, W. & Chan P. (2001). Using Artificial Anomalies to Detect Unknown and Known Network Intrusions, Proc. of ICDM01; 123-248.
[44] Kokkinaki, A. (1997). On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling, Proc. of IEEE Knowledge and Data Engineering Exchange Workshop; 107-113.
[45] Ghiani L., Yambay D. A., Mura V., Marcialis G. L., Roli F. and Schuckers S. A., (2017)."Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015," Image and Vision Computing, vol. 58, pp. 110–128.