PROBABILISTIC CREDIT CARD FRAUD DETECTION SYSTEM IN ONLINE TRANSACTIONS

[1]ISMAILA W.O., [2]ALESE B. K., [3]ISMAILA F. M.

[1]Department of Computer Science & Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
[2]Department of Computer Science, Federal University of Technology, Akure, Nigeria.
[3]Department of Information and Communication Technology, National Open University, Lagos, Nigeria.
E-mail: woismaila@lautech.edu.ng

Abstract- This paper discussed the past works on fraud detection system and highlights their deficiencies. A probabilistic based model was proposed to serve as a basis for mathematical derivation for adaptive threshold algorithm for detecting anomaly transactions. The model was optimized with Baum-Welsh and hybrid posterior-Viterbi algorithms. A credit card transactional data was simulated, trained and predicted for fraud. Four profiles are considered viz; (55 35 10), (70 20 10), (95 3 2) and (34 33 33). And finally, the proposed model was evaluated with different metrics namely; True-positive, false-positive, accuracy and ROC curve. The results showed that with the optimization of parameters, posterior-Viterbi cum new detection model performed better than Viterbi cum old detection model.

Keywords- Probabilistic, Baum-Welsh, HMM, posterior-Viterbi, fraud detection, Optimization

I. INTRODUCTION

In today's increasingly electronic society and with the rapid advances of electronic commerce on the Internet the use of credit cards for purchases has become convenient and necessary. It was reported that there are approximately 322 million credit and debit cards in circulation across the UK, Spain and France and around 92 million in Germany [1].

Credit-card-based purchases can be categorized into two types: physical card and virtual card. 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. In the second kind of purchase, only some important information about a card; card number, expiration date, and secure code is required to make the payment. Such purchases are normally done on the Internet or over the telephone. As the number of credit card users rises world-wide, the thought toward its usage from various business activities is on the increase and so does is the desperation of fraudsters perpetually frauds through the use of credit card.

In e-commerce, credit card fraud is an evolving problem. The growing number of credit card transactions provides more opportunity for thieves to steal credit card numbers and subsequently commit fraud. This can be perpetrated by individuals, merchants and also lack of security that can lead to the compromise of credit card numbers stored in online databases (computer intrusion) [2].

Credit card fraud detection system (CCFDS) is a computer program that attempts to perform fraud detection by identifying fraud or anomaly transaction as quickly as possible once it has been perpetrated. Credit card fraud detection has drawn a lot of research interest and a number of techniques, with special emphasis on data mining and neural networks, have been suggested and their problems are highlighted in the Table 1.

The most recent and closest work to the one done in this thesis is that of [3] who described a method for fraud detection in credit card on-line transactions using HMMs.

The results obtained were quite encouraging. Nevertheless, there are some areas where there are needs for improvement which are: optimization of model parameters; application of hybrid posterior-Viterbi algorithm to generate optimized states; and a better approach to detection algorithm with an adaptive threshold [3] based on account-level of individual card owner.

Hidden Markov Model

A Hidden Markov Model (HMM) has a finite set of states governed by a set of transition probabilities. The sequence of states, which is the quantity of interest pattern recognition problems, can be observed only through the stochastic processes defined into each state (i.e. the parameters of the pdfs of each state must be known) before being able to associate a sequence of states $Q= \{q_1,\ldots q_k\}$ to a sequence of observations $x = \{x_1,..., x_k\}$.

The true sequence of states is therefore hidden by a first layer of stochastic processes. In order to define an HMM completely, following elements are needed;

(i) The set of states $S = \{s_1, s_2,\ldots,s_N\}$, where S_i , $i =1,2,\ldots N$ is an individual state.

(ii). The set of observation symbols $V = \{v_1, v_2,\ldots,v_M\}$, where v_i, $i =1,2,\ldots M$ is an individual observation symbol.

"Table 1: List of Fraud Detection Systems "

fraud detection system-	Authors	Problems
Neural network based	[7], [8]; [13]; [16]; [18]	-Supervised in nature and -Imbalance /skewness of data -fraud alarm rate is still relatively high.
Fuzzy expert system.	[11]	-it is expert based -can only detect known fraud scenarios.
Self-organizing maps	[15]	The detection system performance was not evaluated.
PCA and Imbalance Class Weighted Support Vector Machine (ICW-SVM).	[14];[17]	-model performed well with only small class samples -inadequate performance metrics.
Efficient Scalable Multi-Level Classification Scheme *k*-NN	[12]	-fraud alarm rate is still relatively high.
HMM and specific/general threshold	[3]	-parameters lack optimization -specific threshold .

(iii). A set of state transition probabilities, that is, $A=[a_{ij}]$, Where $a_{ij}=p\{q_{t+1}=S_j \backslash q_t=S_i\}$, $1\leq i,j\leq N$; t=1, 2…… (1) Where q_t denotes the current state.
(iv). The observation symbol probability distribution in each of the states, $B = \{b_j(k)\}$, where $b_j(k)=P(O_k \backslash S_j)$, $1\leq j\leq N$, $1\leq k\leq M$ ……. (2) (v). The initial state distribution, $\pi = [\pi_i]$, where $\pi_i = P\{q_1 = S_i\}, 1\leq i \leq N$, …….(3)
Therefore the compact notation $\lambda = (A, B, \pi)$…….(4) can be used to denote an HMM with discrete probability distributions [4]. Supposing $Q = q_1, q_2,\ldots\ldots,q_T$is a state sequence that generate an observation sequence O. Then according to the assumption for an HMM, λ, the probability that O is generated from this sequence is given by:

$P(O \backslash q_1, q_2,\ldots\ldots,q_T, \lambda) = \Pi^T_{t+1}\, p(o_t \backslash q_t, \pi)$ …….. (5)

$P(O \backslash q_1, q_2,\ldots\ldots,q_T, \lambda) = b_{q1}(O_1).\, b_{q2}(O_2)\ldots\, b_{qT}(O_T)$ ….. (6)

The probability of the state sequence $q_1, q_2,\ldots\ldots,q_T$ is

$P(q_1, q_2,\ldots\ldots,q_T \backslash \lambda) = \pi_{q1}\, a_{q1q2}\, a_{q2q3} \ldots a_{qT\text{-}1qT}$ ..... (7)

The probability of generation of the observation sequence O by the HMM specified by λ is; $P(O \backslash \lambda) = \Sigma_{allq}$ …….. (8)

The structure of HMM adopted in this work is a full ergodical, 10th-order HMM (where 10^{th}-order represents the number of states, that is, merchant category). A sample digram is shown in figure 1. The transition matrix is a multi-dimensional matrix, stating that the probability of transitioning to a new state depends not only on the current state according to the traditional HMM but also on the previous states [6, [7].

Posterior-Viterbi Decoding

This model consisting of values for the transition and emission probabilities matrices along side with the sequence of symbols derived from each of the cardholder's transactions price range from the testing data sets will be passed into the posterior-Viterbi algorithm, (a combined algorithms proposed

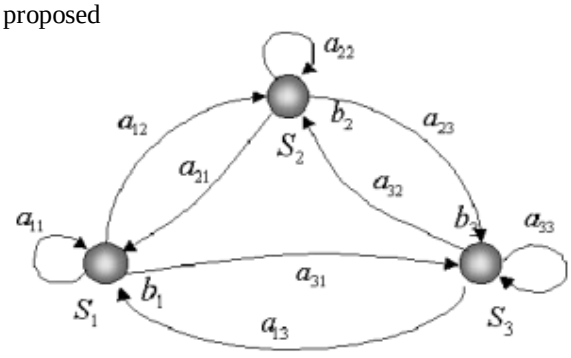


Figure 1. Fully Ergodic three-state HMM

by [8] which will produce a sequence of states ($q_1, q_2,\ldots..q_n$) most likely to have produced the symbol sequence which represent the price range ($o_1,o_2,\ldots o_n$). The specific problem to be solved by the Posterior-Viterbi algorithm is to use posterior decoding to find the path which maximizes the product of the posterior probability of the states and after having computed the posterior probabilities, Viterbi algorithm is used to find the best allowed posterior path through the model. In the PV algorithm, the basic idea is to compute the path π^{PV}

$$\pi^{PV} = argmax_{\{\pi \in A_p\}} \prod_{i=1}^{L} P(\pi_i \mid O, M) \quad \ldots\ldots\ldots (9)$$

Where A_p is the set of the allowed paths through the model, and $P(\pi_i \mid O,M)$ is the posterior probability of the state assigned by the path πat position i (as computed in 9).

Performance Metrics

In general, the objective of fraud detection is to maximize correct predictions and maintain incorrect predictions at an acceptable level. The typical fraud detection techniques attempt to maximize accuracy rate and minimize false alarm rate. A high correct

diagnostic probability can be implied by minimizing probability of undetected fraud and false alarms. The evaluation on the proposed method was carried out with these standard metrics— true positive rate, false positive rate, accuracy, precision and receiver operating characteristics (ROC) curve metrics.

II. ARCHITECTURE OF THE CCFDS

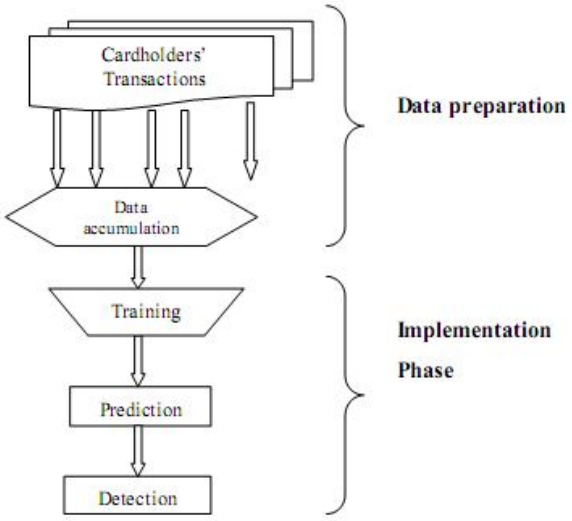
Several research papers developed on fraud detection systems were not based on any architectural design but their approaches could be divided into three stages; data accumulation, system model and detection engine [9], [10]. Also in [11], the authors employed a block diagram containing three phases viz; data entry phase, rule generator phase and committee decision to decide on appropriate rule to detect fraud. However, in 2010, [12] employed a multistage approach to an Overall Architecture of Distributed Fraud Detection System. The architecture consists of data sites stage (data accumulation), classification engine stage, (acts as a re-combination agent to build a unified global classifier) and the detection engine, which has local fraud detection agents. And lastly, [3] showed the process flow of the proposed fraud detection system with two stages (training and detection stages).

This work employed a combined architecture of both [3] and [6] approaches to the proposed Fraud Detection System as shown in figure 2. The architecture consists of two stages viz; data preparation and implementation. The data preparation stage includes the collection of transactions of individual cardholder and the data preparation for training while implementation stage includes the training phase, prediction phase and detection engine. The cardholders' data are stored at transactional levels and account level in different banks. The data mapping phase has to do with matching the parameters of HMM to selected variables of cardholder's transaction data. The training phase involves the processes that are required in preparing the created HMM model for prediction purpose. The prediction phase is used to predict the type of goods/purchase the cardholder bought from the merchant giving a price range (observation symbol). The detection phase employed the parameters from trained HMM model to identify the new transactions as fraudulent or not.

Cardholder's Transactions Details

The cardholder's transactions details consist of demographic and transaction variables. The demographic variables include cardholder's name, address, sex, marital status, country, city, educational background, telephone number, etc, being provided during registration of a new card. The transaction variables provide information about the transaction details of the cardholder. Specific attributes in credit transaction data are often not revealed but they should comprise of transaction value, transaction time and date, transaction category or payment channels (payment, refund, ATM, mobile top-up, etc), ATM/POS indicator, Merchant code, card reader response codes, shipping address, account balance, card number, expiration date, etc. [13]. This transaction data contains two categories viz; transaction amount or actual price and merchants' category or types of goods category.

Figure2. Architecture of the Proposed model



Data Preparation

A cardholder makes different kinds of purchases of different amounts over a period of time. Each individual transaction amount usually depends on the corresponding type of goods purchased. Hence, the transition in the type of purchase is considered as state transition in this model. The type of each purchase is linked to the line of business of the corresponding merchant. The set of all possible types of purchase and equivalently, the set of all possible lines of business of merchants forms the set of hidden states of the HMM [3].

The purchase values x is being quantize into M price ranges $V_1, V_2, \ldots V_M$, forming the observation symbols at the issuing bank. The actual price range for each symbol is configurable based on the spending habit of individual cardholders. These price ranges can be determined dynamically by applying a clustering algorithm on the values of each cardholder's transactions. In this work, only three price ranges, namely, low (l), medium (m), and high (h) are considered. The set of observation symbols is, therefore, V = {l, m, h} making M=3. Thus, the observation sequence of the above transaction amounts of a particular cardholder is Observations / emissions sequence (O) = l, m, m, l, l, h, h, h, l, m.

Prediction Phase

The new sequence and the trained model are used by posterior-viterbi algorithm to estimate new probability of acceptance and to generate the most likely sequence

of states that could have generated the observed emissions. After the HMM parameters are learnt, the symbols (i.e. l, m, h) from a cardholder's training data are taking to form an initial sequence of symbols. Let $O_1, O_2,\ldots,O_R$ be one such sequence of length R. This recorded sequence is formed from the cardholder's transactions up to time t. This sequence is being input into the HMM to compute the probability of acceptance by the HMM. Let the probability be Φ_{old}, which can be written as follows:

$\Phi_{old}= P(O_1, O_2,\ldots\ldots O_R \backslash r)$ …… (10)

Let O_{R+1} be the symbol generated by a new transaction at time t+1 from simulation engine. To form another sequence of length R, $O_1$is dropped and O_{R+1} is added in that sequence, generating $O_2, O_3\ldots\ldots O_R, O_{R+1}$ as the new sequence. The new sequence and the trained model are inputted to the PV-HMM and the probability of acceptance by the HMM is estimated. Let the new probability be $\Phi_{new.}$

$\Phi_{new}= P (O_2, O_3,\ldots\ldots O_{R+1} \backslash r)$ …… (11)

Let the quantity $\Delta\Phi = /\Phi_{old} - \Phi_{new}/$. If $\Delta\Phi \leq 0$, it means that the new sequence is accepted (although it could be a fraud) [1].

Detection Stage

The architecture of the detection stage is shown in figure 3. Once the HMMs have been employed to predict the new hidden credit card transactions states in a given observation sequence. Then, there is need to compute the quantity (Θ) of the new accepted transaction.

$$\Theta = \Delta\Phi / \Phi_{new} \quad \ldots\ldots\ldots\ldots (12)$$

In this work, a credit card fraud detection system based on cardholders' account-specific thresholds is implemented as against universal threshold that was applied to all cardholders' transactions by [1]. The newly added transaction is determined to be fraudulent if the quantity probability ( ) is above a threshold computed in equ. (13). In this paper an initial threshold of 50% is selected.

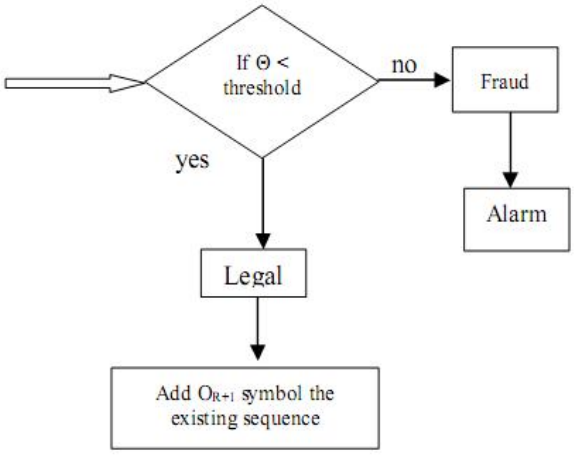


Figure 3 The Architecture of Detection phase

$$threshold = (\Theta_{new} + IT)/2 \quad \ldots\ldots\ldots\ldots (13)$$

If O_{R+1} is malicious, the issuing bank does not approve the transaction, and the CCFDS discards the symbol. Otherwise, $O_{R+1}$is added in the sequence permanently, and the new sequence is used as the base sequence for determining the validity of the next transaction. However, if the new transaction to be generated is more than one, the extended detection algorithm is designed in appendix A.

III. EXPERIMENTAL SETUP

Testing the proposed method using real data set is a difficult task. Banks do not, in general, agree to share their data with researchers. Though some banks granted researchers access to their credit card database but with an agreement of no disclosure [12], [11]. Therefore, it is necessary to perform simulation studies to test the efficiency of the system.

A simulator is used to generate a mix of genuine and fraudulent transactions (Parameters settings of [3] is employed). In a typical scenario, an issuing bank, and hence, its Fraud Detection System receives a large number of genuine transactions sparingly intermixed with fraudulent transactions. The model was trained and tested using 60% of simulated data for training and 40% for prediction.

IV. DISCUSSION OF RESULTS

The experiments were carried out by varying both the transaction amount mix, as well as the number of fraudulent transactions intermixed with a sequence of genuine transactions. Transaction amount mix is captured by the cardholder's profile. In this work four profiles are considered. The profiles considered are (55 35 10), (70 20 10), (95 3 2) and (34 33 33). Here, (a, b, c) represents a profile cardholder who has been found to carry out a percent of his transactions in the low, b percent in medium, and c percent in the high range. The performance metrics used are True-positive, false-positive, accuracy and ROC curve.

It can be seen from the results in Table 2 that the positive effect of Posterior-Viterbi algorithm for prediction contribute averagely about 10% to the increase in true-positive and about 6% to the decrease in false-positive. The positive effect of inclusion of new transactions probabilities to determine the acceptability of the new transactions is also notable in Table 3, with a rough estimated average of 13% increment and 11% decrement on true-positive and false-positive respectively.

Table 2. Effect of Posterior-Viterbi

No. of states	5	6	7	8	9	10
True-Positive	+0.14	+0.12	+0.12	+0.21	-0.16	+0.17
False-Positive	-0.07	-0.07	+0.05	-0.08	-0.11	-0.09

Table3. Effect of inclusion of new transactions probabilities

No. of states	5	6	7	8	9	10
True-Positive	+0.15	+0.11	+0.12	+0.12	+0.14	+0.13
False-Positive	-2.15	+0.12	-3.14	-1.10	-2.09	-2.14

Modifying the original fraud detection algorithm by applying account-level threshold also helped to

improve the results as shown in table 4 especially the reduction in false alarm averaged about 12%.

Table 4. Effect of using Account-level Threshold (Note: T-P and F-P are averaged over all the 15 sequence lengths for different number of states)

No. of states	5	6	7	8	9	10
True-Positive	+0.14	+0.25	+0.18	-0.15	+0.20	+0.17
False-Positive	-3.58	+1.03	-4.07	-4.12	-1.10	+0.08

Table 5 summarises the comparison of the two research works stating the improvement of this research in terms of the addition recorded to the values of the average True-positive and Accuracy and the reduction recorded to the values of the average False-positive for individual cardholders' profiles. Figure 4 shows the ROC curve of the proposed model and it can be deduced from the graph that the proposed model falls conservative performance region which implies that classifiers in this region commit few false positive errors.

Table 5. Improvement over Abhinav et al (2008)

Cardholders' Profiles	True-positive %	Accuracy %	False-positive %
95 3 2	+22.9	+1.18	-1.88
70 20 10	+4.01	+5.0	-4.92
55 35 10	+19.04	+1.45	-7.66
34 33 33	+3.46	+3.28	-1.46

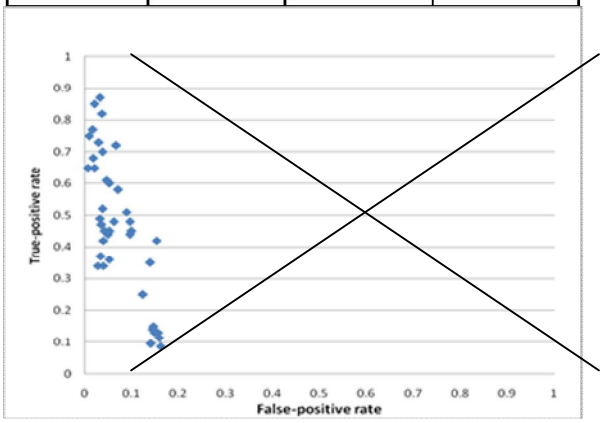


Figure 4. The ROC Curve of the proposed model

CONCLUSION

Credit card fraud has become more and more rampant in recent years. The alarming increase in fraudulent credit card usage has stressed the fraud management systems currently in use at banks and other institutions that process credit card transactions. To improve merchants' risk management level in an automatic and effective way, building an accurate and easy handling credit card risk monitoring system is one of the key tasks for the merchant banks. In this paper, the different steps in credit card transaction processing are represented as the underlying stochastic process of an HMM. A stepwise architecture has been designed to model the new fraud detection system.

Experimental results show the performance and effectiveness of new approach system and demonstrate the usefulness of learning the spending profile of the cardholders. The results obtained from the evaluation showed the overall average of accuracy and precision are about 84% and about 86% respectively.

Also, The ROC curve revealed that this research falls in conservative performance region which implies that classifiers in this region commit few false positive errors.

ACKNOWLEDGMENT

"The authors thank the "Tertiary Education Trust Fund" for sponsoring the presentation of this paper at the "86th International Conference on Science, Innovation and Management (ICSIM) will be held in Pune, India, during 1st-2nd October, 2016.

REFERENCES

[1] J. David Hand. Statistical techniques for fraud detection, prevention, and evaluation.Imperial College London.2007.

[2]. S. O Falaki, Alese B. K., and Ismaila W. O, "An update research on credit card on-line transactions," International journal of economic development research and investment, 1 (2&3), 181- 190.(2010).

[3]. S. Abhinav, K. Amlan, S. Shamik and K. Arun.." Credit card fraud detection using hidden Markov model" IEEE Transactions on Dependable and Secure Computing.5 (1), 2008, 37.

[4]. D. W. Pierre. "Adaptive thresholding for the digital desk, Technical Report EPC- (1993), pp. 110.

[5] L. Rabiner. A Tutorial on Hidden Markov Models and Selected Application in Speech Recognition.Proc. IEEE, (1989)

[6] Y. Ephraim, A. Dembo and L. R Rabiner, "A minimum discrimination information approach for hidden Markov modeling",. Proc. IEEE Int. Conf. Acoust. (1987)

[7] N. Merhav and Y. Ephraim. "Hidden Markov Processes," IEEE Trans. Information Theory. 48, 1518 (2002).

[8] F. Piero, L. Pier and R. Casadio.BMC Bioinformatics, 6, 1471 (2005).

[9] M. Syeda, Y. Zhang and Y. Pan, ".Parallel Granular Networks for fast Credit Card Fraud Detection," Proceedings IEEE Int'l Conf. (2002).

[10] R. Brause, T. Langsdorf, and M. Hepp. "Credit Card Fraud Detection by Adaptive Neural Data Mining" J. W. Goethe-University, Comp. Sc. Dep., Report 7/99, 1999.

[11] J. B. Peter, K. Jungwon, J. Gil-Ho, C. Jong-Uk. Fuzzy Darwinian Detection of Credit Card Fraud. (2000).

[12] D. D. Patil, M.S. Karad, V. M. Wadhai, J. A. Gokhale, S. H. Prasad, "Efficient Scalable multi-Level classification scheme for credit card fraud Detection, " Computer Science and Network Security. 10, 123-130, (2010)

[13] S. Ghosh and D. L. Reilly. "Credit card fraud detection with a Neural Network." In Proc. of the Twenty-Seventh Hawaii Int. Conf. on System Sciences, (1994).

[14] L. Qibei and J. Chunhua, .Reseach on credit card fraud detection model based on class weighted support vector machine, Journal of Convergence Information Technology, 6(1), 62-68, (2011).

[15]. V. Zaslavsky, A. Strizhak, "Credit card fraud detection using self-organizing maps," Informaion &. Security. 18 (2006)

[16] P. Clifton, A. Damminda, and L. Vincent. Minority Report in Fraud Detection: Classification of Skewed Data, ACM SIGKDD Explorations Newsletter, Vol. 6, pp.50-59. [2004]

[17] R. Chen, M. Chiu, Y. Huang, and L. Chen. Detecting Credit Card Fraud by Using Questionaire-Responded Transaction

Model Based on Support Vector Machines. Proc. of IDEAL(2004), pp.800-806.

[18] J. Dorronsoro, F. Ginel, C. Sánchez, and S. Cruz., Neural Fraud Detection in Credit Card Operations.IEEE Transactions on Neural Networks 8(4): 827-834, (1997).

APPENDIX A

Algorithm for Account Level Threshold of a cardholder

Start
Set Initial threshold to 50%
Enter n (n is number of new transactions to generated)
For i = 1 to n DO
K1: Generate new transaction
Compute $\Theta_{i+1} = \Delta\Phi/\Phi_{i+1}$
Compute threshold = $(\Theta_{i+1} + IT) / 2$
Test for fraud/legal
(if Θ_{i+1} < =threshold then legal else fraud)
Let IT = threshold
GOTO K1
Stop

★★★