Journal of the Nigerian Association of Mathematical Physics
Volume27, (*July, 2014*), pp 451 – 456

Credit Card Fraud Detection Using Hidden Markov Model And Fuzzy Logic

F. A. U. Imouokhome and C. O. Jibunoh

Department of Computer Science, University of Benin, Benin City. Nigeria

Abstract

Commercial activities all over the world today is governed by the electronic banking (e-banking) systems. Payments for goods and services are made through the use of smart cards, credit cards, money transfers, etc. However, the systems are fraut with fraudulent practices. One of the techniques developed to arrest this is the credit card fraud detection systems using the Hidden Markov Model (HMM). This is not very effective due to its weakness in handling uncertainty resulting from insufficient and corrupted data.This paper presents a model that extends the use of the HMM by integrating it with Fuzzy Logic to take care of uncertainties in data presented to the HMM at the training phase. The Fuzzy Logic extension to the HMM is meant to accommodate some purchases that are above the normal limit of the card holder's spending profile or value.

Keywords: e-banking, Fraud Detection, Hidden Markov Model (HMM), Fuzzy Logic, Membership function

1.0 Introduction

As world electronic-based commercial activities increases by the day, so are the activities of fraudsters in swindling business people who depend daily on the use of e-commerce to make online payments for their transactions. Reports of these fraudulent practices are everywhere in the banking industry. One of the techniques that have been deviced to forestall this evil practices is the Credit Card Fraud Detection System. The use of this technique generally involves verifying the amount or value of a current transaction by comparing it with previous ones for any possible match before the online payment is allowed; otherwise, the transaction is rejected. Credit Card Fraud Detection System using the Hidden Markov Model (HMM) has been proposed by many researchers in this direction. The weakness of this model is that it is usually associated with uncertainty because of insufficient and corrupted data it is presented with at its training phase, and the model is not able to accommodate transactions that are not within those in the card holder's normal transaction profile. This paper therefore presents a model that extends the use of the HMM by integrating it with Fuzzy Logic to take care of uncertainties in data presented to the HMM at the training phase, and to accommodate some purchases that are above the normal limit of the card holder's spending profile or value.

2.0 Background

The proposed system is a model that combines the strengths of the HMM and Fuzzy Logic (FL). This is aimed atdecreasing the number of False Positive transactions recognised by credit card fraud detection systems as malicious eventhough such transactions are truly genuine, as well as accommodating some purchases that are above the normal limit of the card holder's spending profile or value.

2.1 The Hidden Markov Model

A Hidden Markov Model (HMM) is a double-layered finite state process with a hidden Markov process that controls the selection of the states of an observable process. In Markovian process, the next state of the process is dependent on the present state; i.e., it is a sequential (history-based) model. HMM has all the parameters of a Markov model with the addition of the stochastic emission function; which means that given the state S_t, the symbol O_t is observed.

According to[1] an HMM can be defined mathematicallyto consist of the following.

1. **S** = set of states in the process;
   $S_i = \{S_1, \ldots, S_N\}$; i.e.,$1 \leq i \leq N$ . . . . . (1)
   N = number of states.

Corresponding author: F. A. U. Imouokhome E-mail: franmokome@yahoo.com, Tel.: +2347062289738

2. M observation symbols per state, $V = \{v_1, \ldots, v_M\}$
   where v_i, is an individual observation symbol for a finite value of M; and i = 1,…,M.
3. A = State transition distribution (function or probability) matrix;
4. B = Emission distribution, or observation symbol probability function (or matrix).
5. Initial state probability, $\pi = \{\pi_i\}$, where π_i is the probability that the model is in state S_i at the time t = 0 with

A complete specification of an HMM requires the estimation of two model parameters (N and M), specification of observation symbols, and the specification of the three probability distributions A, B, and π[2]. The notation $\lambda = \{\pi, A, B\}$is used to indicate the complete set of parameters of the HMM model, where A, B implicitly include N and M. [3].The use of the HMM model (λ) involves training it with a set of data to estimate its parameters (π, A, B) using the Baum-Welch. The algorithm is an iterative likelihood maximization method based on forward-backward probabilities.According to [1], given a model $\lambda = (A, B, \pi)$,

'A' is defined as the state transition probability distribution (or matrix).

$A = a_{i,j} = P\{q_{t+1} = S_j | q_t = S_i\}$, $1 \leq i, j \leq N$; t = 1, 2, ... (2)

where P{.} denotes the probability;

q_t denotes the current state.

'B' is defined as the observation symbolprobability (or matrix) in each state.

$B = \{b_j(k)\}$ . . . . . (3)

where $\{b_j(k)\}$ is theprobability that symbol v_k is emitted in state S_j.

$b_j(k) = P\{o_t = v_k | q_t = j\}$, $1 \leq j \leq N$, $1 \leq k \leq N$ . . (4)

where $b_j(k)$ = the probability that the symbol v_k is emitted in state S_j;

$v_k = k^{th}$ observation symbol in the alphabet (observation space);

o_t = current observation vector.

$b_j(k) \geq 0$, $1 \leq j \leq N$,$1 \leq k \leq M$, and $\sum_{k=1}^{M} bj(k) = 1, 1 \leq j \leq N$

π is defined as the initial state initial state probability vector.

$\pi_i = P\{q_i = i\}$ and $1 \leq i \leq N$, ...(5)

Having obtained the HMM parameters (π, A, B),the next step is to use the Viterbiforwardalgorithm to estimate the most the likelihood probability ($P\{O|\lambda\}$) of the HMM, given an input observation sequence ($O = o_1, o_2, ..., o_T$)of the model parameters. The algorithm, which is a solution for the problem of maximization, considers only acceptable sequences as follows.

i. Initialisation: $\delta_t(i) = p\{o_1, o_2, ..., o_T, q_t = i|\lambda\}$

where δ_1 = forward variable,

$o_1, o_2, ..., o_T$ = partial observation sequence.

$b_i(o_1)$, $1 \leq i \leq N$

ii. Recursive calculation of the Maximum Likelihood (ML) state sequences and their probabilities: $\delta_1(i) = \max_{1 \leq i \leq N}[\delta_{t-1}(i)a_{ij}]b_j(o_t)$, $2 \leq t \leq T$, $1 \leq j \leq N$

iii. Termination: $P\{O|\lambda\} = \sum_{i=1}^{N} \delta_T(i)$

2.2 Fuzzy Logic Systems

Fuzzy logic is a logic that is based on fuzzy sets; i.e., sets of elements or objects characterised by truth-values in the [0, 1] interval as opposed to 0 and 1 crisp values in the conventional set theory. The function that assigns a number in [0, 1] to each element of the universe of discourse of a fuzzy set is called a membership function. If the value of the membership functionequals one, x belongs completely to the fuzzy set. If the membership function equals zero, x does not belong to the set at all. x partially belongs to it if the membership degree is between 0 and 1 as expressed in equation. These are expressed mathematically in equation (5) as

$$\mu_F(x)\begin{cases} = 1 & x \text{ is a full member of } F \\ \in (0,1) & x \text{ is a partial member of } F \\ = 0 & x \text{ is a not member of } F \end{cases} \quad . \quad . \quad . \quad (6)$$

where $\mu_F(x)$ is called the membership function of x in F. It represents theextent (degree or grade) to which x belogs to the fuzzy set F.

If U denotes the universe of discourse of a fuzzy set F, then F is completely characterised by

$\mu_F(x) : U \rightarrow [0, 1]$. . . . . (7)

Equation (7) represents a mapping from U into the unit interval [0, 1]. "Fuzzy systems, or fuzzy models, are actually mathematical models that describe relations between variables, using membership functions of fuzzy sets. These mathematical models are flexible, but they are not "fuzzy" in layman terms. The membership functions themselves are precise mathematical functions" [4].

In a fuzzy logic system, fuzzy sets can be involved in system description, specification of system parameters, and in representation of input, output and system state. When involved in system description, fuzzy sets appear as linguistic terms or labels to represent the state of the linguistic variable in the fuzzy rule in the form of IF-THEN linguistic rules.

Any system can be described by a collection of such types of IF-THEN linguistic rules, also known as fuzzy rules. The general form of such an IF-THEN rule is: IF antecedent propositions THEN consequent propositions.When involved in specification of system parameters, fuzzy sets may appear as fuzzy numbers in which the parameters used are approximate (fuzzy) numbers instead of exact real numbers.Lastly, fuzzy sets may appear as the only means to express human perceptions or even noisy or uncertain data or information that have to be used as system input, output, and system state.

3.0 Literature Review

Reports in some journal papers have revealed that a lot of researches have been carried out on the use of HMM for the design of credit card fraud detection systems. For example, [5] proposed a HMM-based system for credit card fraud detection with multiple involvements of several fields of user profile instead of the spending profile only. According to these authors, simulation results from the proposed system showed an improvement in True positive (TP), True Negative (TN) rates, a decrease in the False Positive (FP) and False Negative (FN) rates. Sableet al [6] proposed a model for fraudulent transaction detection using HMM. The work shows the sequence of operations in credit card transaction processing using HMM, and proved that the system can be used effectively to detect fraud. Patil et al [7] proposed a HMM-based credit card fraud detection system. To authenticate a user (i.e., card holder), the system uses an Implicit Password Authentication System (IPAS). This is meant to ensure that genuine transactions are not rejected. Cho and Park [8] proposed an efficient anomaly based Intrusion Detection System by demonstrating privilege transition flow of data by using HMM. Srivastava et al. [9] used HMM for identifying credit card fraud by showing that the credit card transactions with high probability is deemed by proficient HMM as abnormal behaviour or fraudulent. Prasad [10] introduced a three-level security system in which a user is prompted to supply his user password for his authentification in the first level. The second level of security uses the HMM to reject a transaction with sufficiently high probability. The third level sends some questions to be answered by the user to prove genuiness of transaction. Ingol and Thool [3] modelled the sequence of operations in credit card transaction processing by using HMM. An empirical method of Anomaly detection system that analyses the spending habit of a card holder was proposed by Jadhav and Bhandari [11]. The system models the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and shows how it can be used for the detection of frauds.

One of the flaws identified with existingcredit card fraud detection is thedetection offraud only after completion oftransaction — i.e.,when the card holder complains. Another flaw weakness associated with the system is that it uses labelled data to detect fraud and hence cannot detect fraud of other scenarios.A third flaw is the excessive restriction it imposes on card holders making online purchases stressful for them. These detractive features of existing systems motivated thepresent study, which proposes a model that combines the Hidden Markov model and Fuzzy Logic, as a methodology to eradicate the restrictions in the existing systems.

4.0 Methodology

Two methodologies are employed in the proposed model to assure the security of card holder's money when he transacts business through e-payment. First, that of an existing system is descibed, and then that of the proposed.

4.1 Existing Credit Card Fraud Detection System

Architecture of an existing credit card fraud detection system is as shown in Figure 1.

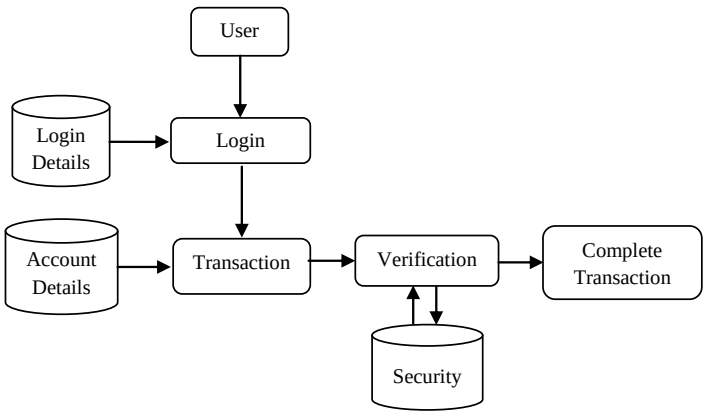

Figure 1: System Model for Credit Card Fraud Detection Using HMM (Jadhav and Bhandari

The system has a database that contains the account details (i.e., the spending profile) of the card holder. The spending profile is categorised into low (l), medium (m) and high (h). These are regarded as the states in the HMM,where
V = {l, m, h} and M = 3

The next step is to determine the probability matrices (A, B, π) at the training phase of the HMM using forward-backward algorithm. Determination of these parameters leads to the formation of an initial sequence of the existing spending behaviour or profile of the card holder.

Let $O_1, O_2, \ldots, O_R | \lambda$ consist of R symbols to form a sequence determined from the card holder's transaction up to time t. The Hidden Markov Model uses this sequence of symbols to compute the probability of acceptance (δ_1). Thus

$$\delta_1 = P(O_1, O_2, \ldots, O_R | \lambda) \quad . \quad . \quad . \quad . \quad (8)$$

When a new transaction is processed at time (t+1), a new sequence O_{R+1} is generated raising the total number of sequences to R+1. For R sequences to be considered, O_1 sequence is dropped and R sequences are taken from O_2 to O_{R+1}. The probability of the new R sequences (δ_2) now becomes

$$\delta_2 = P(O_1, O_2, \ldots, O_{R+1} | \lambda) \quad . \quad . \quad . \quad . \quad (9)$$

A difference (Δ_δ) between the old and the new probabilities is computed from

$$\Delta_\delta = \delta_1 - \delta_2 \quad . \quad . \quad . \quad . \quad . \quad . \quad (10)$$

If $\Delta_\delta > 0$, the new sequence is accepted by the HMM with low probability but the transaction could be a fraud. It is a fraud if the percentage change in probability is above a predefined threshold value;

i.e., $\Delta_\delta | \lambda \geq$ Threshold . . . . (11)

under this condition of suspected fraud, the credit card issuing bank will reject the transaction and the fraud detection system discards the symbol (i.e., O_{R+1}). If the transaction is accepted, O_{R+1} is added to the sequence, and the new sequence is used as the base sequence for determining the validity of the next transaction [9].

4.2 Proposed Credit Card Fraud Detection System

A transaction that is regarded as malicious or fraudulent may not necessarily be one because the spending habit of a card holder may change suddenly on account of a necessity. When this happens, the existing fraud detection system (FDS) would regard such transaction as a fraud. This is a problem of uncertainty in human behaviour, which the system cannot predict. The model of the system proposed in this study, as shown in Figure 2, is embedded with fuzzy logic to overcome this problem of uncertainty.

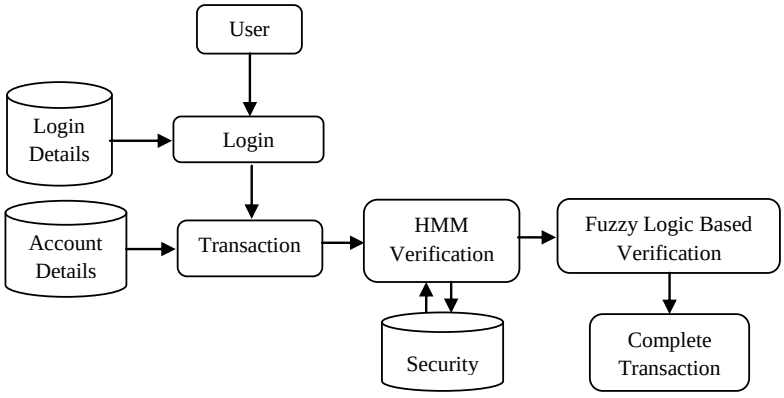

Figure 2: Proposed Model for Credit Card Fraud Detection System, Using HMM-Fuzzy Logic

The proposed system, which is an extension to the HMM,is meant to accommodate some purchases that are above the normal limit of the card holder's spending profile or value. Since this cannot be predicted, it is therefore subjective and vague; but the vagueness can be handled conveniently with fuzzy logic control system. The process of fuzzy logic in the proposed systeminvolves taking the maximum amount or purchase limit (Max) from the HMM of the FDS as the base value (i.e., lower boundary or limit) for the fuzzy logic control system. The upper limit or boundary of the system is taken as 140% of thelower limit (i.e., 1.4*Max).As shown in Figure 3, linguistic labels (very low, low, normal, high, and very high) represented by triangular membership functions are chosen to describe purchasing values that may be allowed for transactions over the interval[Max, 1.4*Max].While values below the upper limit of this interval are allowed by the system, any transactions detected to be very high (i.e., equal to1.4*Max) or higher,are labelled as suspicious and are thereforerejected.

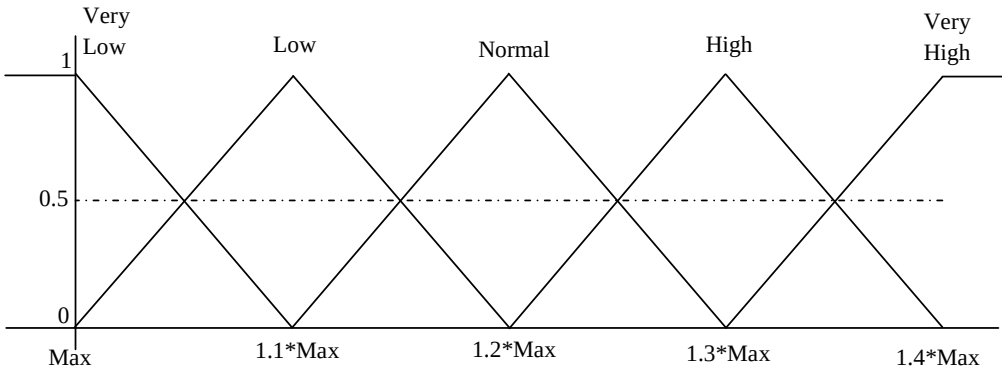

Figure 3:Membership Functions for Transactions Above Upper Limit ofHMM

(i) The triangular membership function depends on three scalar parameters *a*, *b*, and *c* as shown in Figure 4.

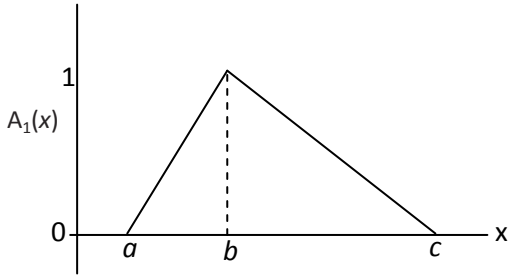

Figure 4: Triangular Membership Function

The parameters *a* and *c*respectively set the left and right "feet," or base points, of the triangle. The parameter *b* sets the location of the triangle peak. Mathematically, the function is given by:

$$\text{Triangle}(x;\, a,b,c) = \begin{cases} 0 & x < a \\ \frac{x-a}{b-a} a \le x \le b \\ \frac{c-x}{c-b} b \le x \le c \\ 0 & x > c \end{cases} \quad . \quad . \quad . \quad . \quad (12)$$

During fuzzy processing, the controller analyzes the input data, as defined by the membership functions, to arrive at a control output. During this stage two actions areperformed; namely, rule evaluation, and the fuzzy outcome calculation, which is based on equation (11). Fuzzy logic is based on the concept that most complicated problems are formed by a collection of simple problems and can, therefore, be easily solved by using a reasoning, or inference, process composed of IF...THEN rules, each providing a response or outcome.

5.0 Conclusion

A model based on two methodologies of: the Hidden Markov Model and Fuzzy Logic is presented in this paper to propose a credit card fraud detection system. It is based on the individual strengths of the two methodologies. When implemented, the system will not only detect fraud, it will also make the use of credit card more comfortable for its users since it is designed to accommodate incidental transactions which are not provided for in previous designs. The authors hope to work on the implementation of the proposed system in their next report.

6.0 References

[1] Dymarski, P. (2011), Hidden Markov Models, Theory And Applications, InTech, Rijeka, Croatia, pages 2 – 26.

[2] Rabiner, L. R. (1989), "A Tutorial on Hidden Markov Model and Selected Applications in Speech Recognition". In Proceedings of the IEEE, 77(2): 257 – 286.

[3] Ingole, A. and Thool, R. C. (2013), "Credit Card Fraud Detection using Hidden Markov Model and its Performance". International Journal Advanced Research in Computer Science and Software Engineering, 3(6): 626 – 632.

[4] Nguyen, H. T., Prasad, N. R., Walker, C. L. and Walker, E. A. (2003),A First Course in Fuzzy and Neural Control, Chapman and Hall/CRC, London.

[5] Kumar, R and Raj, S. (2012), "Design & Analysis of Credit Card Fraud Detection Based On HMM". International Journal of Engineering and Innovative Technology (IJEIT), 2(3): 332 – 335.

[6] Sable, P. N., Mahajan, A. G. and Ugale A. B. (2014), Fraudulent Transaction Detection Using HMM. International Journal of Engineering Development and Research, 2(1): 913 – 916.

[7] Patil, A., Pohare, P., Patil, S., Shelar, P. and Bewoor, L. A. (2014). "Credit Card Fraud Detection Using Implicit Password Authentication". International Journal of Advanced Computational Engineering and Networking, 2(1): 49 – 51.

[8] Cho, B.S. and Park, 1.H. (2003), "Efficient anomaly detection by modeling privilege flows using hidden Markov model", Computers and Security, 22(1): 45 – 55.

[9] Srivastava, A, Kundu, A, Sural, S. and Majumdar, A.K. (2008), 'Credit Card Fraud Detection Using Hidden Markov Model', IEEE Transactions on Dependable and Secure Computing, 5(1), pp. 37-47.

[10] Prasad V. K. (2013), "Method and System for Detecting Fraud in Credit Card Transaction", International Journal of Innovative Research in Computer and Communication Engineering, 1(5): 1132 – 1136.

[11] Jadhav, S. N. and Bhandari, K. (2013), "Anomaly Detection Using Hidden Markov Model", International Journal of Computational Engineering Research, 3(7): 28 – 35.