Credit Card Fraud Detection Using Neural Network

Raghavendra Patidar, Lokesh Sharma

***Abstract*- The payment card industry has grown rapidly the last few years. Companies and institutions move parts of their business, or the entire business, towards online services providing e-commerce, information and communication services for the purpose of allowing their customers better efficiency and accessibility. Regardless of location, consumers can make the same purchases as they previously did "over the desk". The evolution is a big step forward for the efficiency, accessibility and profitability point of view but it also has some drawbacks. The evolution is accompanied with a greater vulnerability to threats. The problem with making business through the Internet lies in the fact that neither the card nor the cardholder needs to be present at the point-of-sale. It is therefore impossible for the merchant to check whether the customer is the genuine cardholder or not. Payment card fraud has become a serious problem throughout the world. Companies and institutions loose huge amounts annually due to fraud and fraudsters continuously seek new ways to commit illegal actions. The good news is that fraud tends to be perpetrated to certain patterns and that it is possible to detect such patterns, and hence fraud.**

In this paper we will try to detect fraudulent transaction through the neural network along with the genetic algorithm. As we will see that artificial neural network when trained properly can work as a human brain, though it is impossible for the artificial neural network to imitate the human brain to the extent at which brain work, yet neural network and brain, depend for there working on the neurons, which is the small functional unit in brain as well as ANN. Genetic algorithm are used for making the decision about the network topology, number of hidden layers, number of nodes that will be used in the design of neural network for our problem of credit card fraud detection. For the learning purpose of artificial neural network we will use supervised learning feed forward back propagation algorithm. Finally we will see what future work can be done in making fraud detection.

I. INTRODUCTION

Credit card fraud

Credit card fraud can be defined as "Unauthorized account activity by a person for which the account was not intended. Operationally, this is an event for which action can be taken to stop the abuse in progress and incorporate risk management practices to protect against similar actions in the future". In simple terms, Credit Card Fraud is defined as when an individual uses another individual s credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. And the persons using the card has not at all having the connection with the cardholder or the issuer and has no intention of making the repayments for the purchase they done.

Manuscript received May 19, 2011.

Raghavendra Patidar. Electronics & Communication Engineering. RCEW, jaipur. India. +919414552184 (raghav_sec@rediffmail.com).
LokeshSharma. Electronics&CommunicationEngineering. MAIET. Jaipur .India. +919413839550. (lokeshsharma_25@rediffmail.com).

II. DIFFERENT TYPE OF FRAUD TECHNIQUES

There are many ways in which fraudsters execute a credit card fraud. As technology changes, so does the technology of fraudsters, and thus the way in which they go about carrying out fraudulent activities. Frauds can be broadly classified into three categories, i.e., traditional card related frauds, merchant related frauds and Internet frauds. The different types of methods for committing credit card frauds are described below.

A.Merchant Related Frauds

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:

i. *Merchant Collusion*: This type of fraud occurs when merchant owners or their employees conspire to commit fraud using the cardholder accounts or by using the personal information. They pass on the information about cardholders to fraudsters.

ii. *Triangulation:* Triangulation is a type of fraud which is done and operates from a web site. The products or goods are offered at heavily discounted rates and are also shipped before payment. The customer while browse the site and if he likes the product he place the online information such as name, address and valid credit card details to the site. When the fraudsters receive these details, they order goods from a legitimate site using stolen credit card details. The fraudsters then by using the credit card information purchase the products.

B. Internet Related Frauds

The internet is the base for the fraudsters to make the frauds in the simply and the easiest way. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border, economic and political spaces, the internet has become a new worlds market, capturing consumers from most countries around the world. The below described are most commonly used techniques in Internet fraud:

i. *Site cloning*: Site cloning is where fraudsters close an entire site or just the pages from which the customer made a purchase. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services from because the pages that they

are viewing are identical to those of the real site. The cloned site will receive these details and send the customer a receipt of the transaction through the email just as the real company would do. The consumer suspects nothing, while the fraudsters have all the details they need to commit credit card fraud.

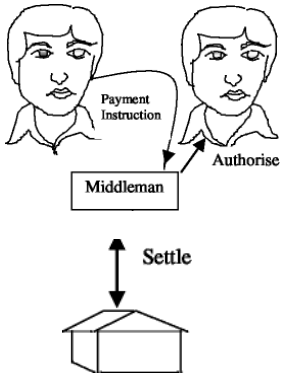


Fig.1: General Model of Internet Transaction

ii. *False merchant sites***:** Some sites often offer a cheap service for the customers. That site requests the customer to fill his complete details such as name and address to access the webpage where the customer gets his required products. Many of these sites claim to be free, but require a valid credit card number to verify an individual s age. These kinds of sites in this way collect as many as credit card details. The sites themselves never charge individuals for the services they provide. The sites are usually part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudsters.

iii. *Credit card generators***:** These are the computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. This makes the user to allow to illegally generating as many numbers as he desires, in the form of any of the credit card formats.

III. OTHER FRAUD TECHNIQUES

A.*Lost/ Stolen Cards***:** When one person loses his card or a card is stolen by someone or when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. This the easiest way for the fraudsters where he gets the information of the cardholders without investing any on the modern technology. It is perhaps the hardest form of traditional credit card fraud to tackle.

B.*Account Takeover***:** This type of fraud occurs when the valid customer's personal information is taken by the fraudsters. The fraudster takes control of a legitimate account by either providing the customer's account number or the card number. The fraudster then contacts the card issuer, as the genuine cardholder, to ask the mail to redirect to a new address. The fraudster reports card lost and asks for a replacement to be sent.

C.*Cardholder-Not-Present (CNP)***:** CNP transactions are performed only on the internet that is remotely, in such kind of frauds neither the card nor the cardholder is present at the point-of-sale. This take many types of transactions such as orders made over the phone or Internet, by mail order or fax. In such transactions, retailers are unable to physically check the card or the identity of the cardholder, which makes the user unknown and able to disguise their true identity. The details of the credit card are normally copied without the cardholder's knowledge, collected from the receipts thrown by the customer or obtained by skimming process. Fraudulently obtained card details are generally used with fabricated personal details to make fraudulent CNP purchases. This means that while the three or four digit Card Security Code on the back of cards can help prevent fraud where card details have been obtained, but when the card is stolen it won't be helpful.

D.*Fake and Counterfeit Cards***:** This is another type of fraud where the creation of counterfeit cards, together with lost or stolen cards poses highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. The below mentioned are some of the techniques used for creating false and counterfeit cards.

E.*Erasing the magnetic strip***:** This is the type of the fraud where the fraudsters erase the magnetic stripe by using the powerful electro-magnet. The fraudster then tampers with the details on the card so that they match the details of a valid card, which they may have attained, for example, when the fraudster begins to use the card, the cashier will swipe the card through the terminal several times, before realizing that the metallic strip does not work. The cashier will then proceed to manually input the card details into the terminal. This kind of fraud is having high risk because the cashier will be looking at the card closely to read the numbers.

F. *Creating a fake card***:** Today we have sophisticated machines where one can create a fake card from using the scratch. This is the common fraud though fake cards require a lot of effort and skill to produce it. Modern cards are having many security features, all designed to make it difficult for fraudsters to make good quality fraudulent. After introducing the Holograms in the credit cards it makes very difficult to forge them effectively.

*G.Skimming***:** Skimming is fast emerging as the most popular form of credit card fraud. Most cases of Counterfeit fraud involve skimming. It is a process where the actual data on a card's magnetic stripe is electronically copied onto another. Fraudsters have been found to carry pocket skimming devices, a battery-operated electronic magnetic stripe reader, with which they swipe customer's cards to get hold of customer s card details. The fraudster does this whilst the customer is waiting for the transaction to be validated through the card terminal. The card holder doesn't t know about this and it is very difficult for him to identify. In other cases, the details obtained by skimming are used to carry out fraudulent card not-present transactions by fraudsters. Until the cardholder gets the bill to he don't understand what s the thing happened.

H.*Phishing***:** Phishing is a type of fraud designed to steal a

person's identity. It is usually committed via spam e-mail or pop-up windows. Phishing works by a malicious person sending lots of false e-mails. The e - mails looks like they come from a website or company you trust, for example your bank. The message tells you to provide the company with your personal details including your payment card details. They can claim that the reason for this is a database crash or the like. To make the e- mails look even more authentic, the fraudster might put a link to a website that look exactly like the real one but is in fact a scam site. These copies are often called "spoofed websites". When you are on the spoofed site they can ask you for even more personal details that will be directly transmitted to the person who made the site.

IV. FRAUD DETECTION USING NEURAL NETWORK

Although there are several fraud detection technology exist based on Data mining, Knowledge Discovery and Expert System etc. but all these are not capable enough to detect the fraud at the time when fraudulent transaction are in progress due to very less chance of a transaction being fraudulent .It has been seen that Credit card fraud detection has two highly peculiar characteristics.

The first one is obviously the very limited time span in which the acceptance or rejection decision has to be made.

The second one is the huge amount of credit card operations that have to be processed at a given time. To just give a medium size example, millions of Visa card operations take place in a given day, 98% of them being handled on line. Of course, just very few will be fraudulent (otherwise, the entire industry would have soon ended up being out of businesses), but this just means that the haystack where these needles are to be found is simply enormous.

A. Working principal (Pattern Recognition)

Neural network based fraud detection is based totally on the human brain working principal. Neural network technology has made a computer capable of think. As human brain learn through past experience and use its knowledge or experience in making the decision in daily life problem the same technique is applied with the credit card fraud detection technology. When a particular consumer uses its credit card , there is a fix pattern of credit card use , made by the way consumer uses its credit card.

Using the last one or two year data neural network is train about the particular pattern of using a credit card by a particular consumer. As shown in the figure the neural network are train on information regarding to various categories about the card holder such as occupation of the card holder, income, occupation may fall in one category, while in another category information about the large amount of purchased are placed, these information include the number of large purchase, frequencies of large purchase, location where these kind of purchase are take place etc. within a fixed time period.

In spite of pattern of credit card use neural network are also trained about the various credit card fraud face by a particular bank previously. Based on the pattern of uses of credit card , neural network make use of prediction algorithm on these pattern data to classify that weather a particular transaction is fraudulent or genuine.

When credit card is being used by unauthorized user the neural network based fraud detection system check for the pattern used by the fraudster and matches with the pattern of the original card holder on which the neural network has been trained, if the pattern matches the neural network declare the transaction ok.

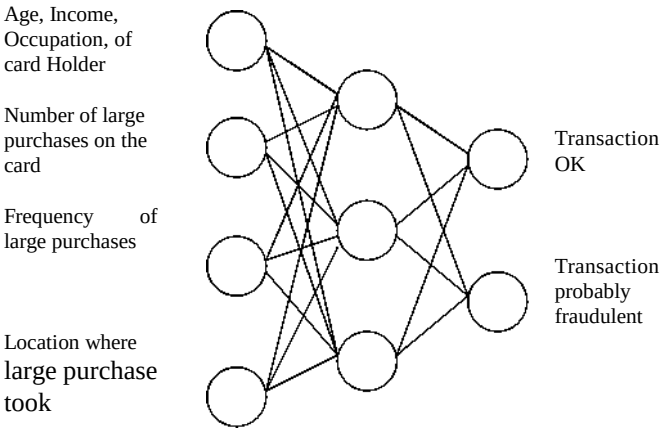


Fig. 2: Layer of Neural Network in Credit Card

When a transaction arrives for authorization, it is characterized by a stream of authorization data fields that carry information identifying the cardholder (account number) and characteristics of the transaction (e.g., amount, merchant code). There are additional data fields that can be taken in a feed from the authorization system (e.g., time of day). In most cases, banks do not archive logs of their authorization files. Only transactions that are forwarded by the merchant for settlement are archived by the bank's credit card processing system. Thus, a data set of transactions was composed from an extract of data stored in Bank's settlement file. In this extract, only that authorization information that was archived to the settlement file was available for model development.

B. Fraud Detection

Matching the pattern does not mean that the transaction should exactly match with the pattern rather the neural network see to what extent there exist difference if the transaction is near by the pattern then the transaction is ok otherwise if there is a big difference then the chance of being a transaction illegal increase and the neural network declare the transaction a fault transaction.

The neural network is design to produce output in real value between 0 and 1 .If the neural network produce output that is below .6 or .7 then the transaction is ok and if the output is above .7 then the chance of being a transaction illegal increase.

There are some occasion when the transaction made by a legal user is of a quite different and there are also possibilities that the illegal person made use of card that fit into the pattern for what the neural network is trained. Although it is rare, yet

If the legal user can't complete a transaction due to these limitation then it is not much about to worry But what about the illegal person who is making use of card , hare also work human tendency to some extent when a illegal person gets a credit card he is not going to make use of this card again and again by making number of small transaction rather he will try to made as large purchase as possible and as quickly that may totally mismatch with the pattern for what the neural network is trained.

In the design of neural network-based pattern recognition systems, there is always a process of business (e.g., jewelry store, consumer electronics, restaurant, hotel, etc.) History descriptors contain features characterizing the use of the card for transact-ions and the payments made to the account over some immediately prior time interval. Other descriptors can include such factors as the date of issue (or most recent reissue) of the card. This can be important for the detection of NRI (non-receipt of issue) fraud.

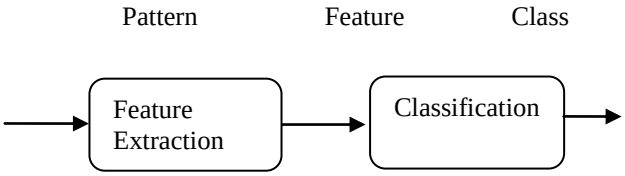


Fig. 3: Pattern Recognition

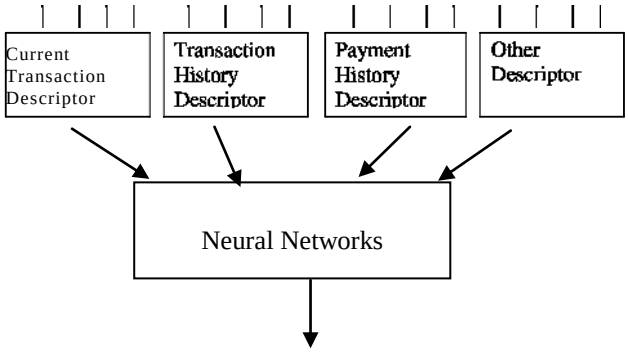


Fig.4: Group of input features characterizing each transaction to the network.

V. TRANSACTION FRAUD SCORER

.The neural network used in this fraud detection a three-layer, feed-forward network that use two training passes through the data set. The fust training pass involves a process of prototype cell commitment in which exemplars from the training set are stored in the weights between the first and second (middle) layer cells of the network. A final training pass determines local a posteriori probabilities associated with each of these prototype cells. P-RCE training is not subject to problems of convergence that can afflict gradient-descent training algorithms. The P-RCE network and networks like it have been applied to a variety of pattern recognition problems both within and beyond the field of financial services, from character recognition to mortgage underwriting and risk assessment layer consisted of a single cell that outputs a numeric response that can be considered as a "fraud score". This is analogous to credit scoring systems that produce a score, as opposed to a strict probability. The objective of the neural network training process is to arrive at a trained network that produces a fraud score that gives the best ranking of the credit card transactions. If the ranking were perfect, all of the high scoring transactions down to some threshold would be fraud; below this threshold, only good transactions would be ranked. However, perfect separation of frauds from goods is not possible due to the inherently non-separable nature of the fraud and good distributions in the selected pattern recognition Space.

Final evaluation of the trained network can be done on the Blind Test data set. The Blind Test data represented an unsampled set of all Banks' transactions during last few months.

A. Learning Algorithm (Feed Forward Back Propagation)

The back propagation learning rule is a standard learning technique. It performs a gradient descent in the error/ weights space. To improve the efficiency, a momentum term is introduced, which moves the correction of the weights in the direction compliant with the last weight correction.

It is a multi-layer feed forward network that is trained by supervised learning. A standard back propagation network consists of 3 layers, an input, an output and a hidden layer. The processing elements of both input and output layer are fully connected with the processing elements of the hidden layer, as shown in figure. The fact that it is feed forward means that there are no recurrent loops in the network. The output of a node never returns at the same node, because cycles are not allowed in the network. In standard back propagation this can never happen because the input for each processing element always comes from the previous layer (except the input layer, of course). This, again, is a large simplification compared with the real brain because the brain itself appears to contain many recurrent loops.

Supervised learning means that the network is repeatedly presented with input/output pairs (I,O) provided by a supervisor, where O is the output the network should produce when presented with input I. These input/output pairs specify the activation patterns of the input and output layer. The network has to find an internal representation that results in the wanted input/output behavior. To achieve this, back propagation uses a two-phase propagate-adapt cycle.

i. First Phase: In the first phase the input is presented to the network and the activation of each of the nodes (processing elements) of the input layer is propagated to the hidden layer, where each node sums its input and propagates its calculated output to the next layer. The nodes in the output layer calculate their activations in the same way as the nodes in the hidden layer.

ii. Second Phase: In the second phase, the output of the network is compared with the desired output given by the supervisor and for each output node the error is calculated. Then the error signals are transmitted to the hidden layer where for each node its contribution to the total error is calculated. Based on the error signals received, connection weights are then *adapted* by each node to cause the network to

converge toward a state that allows all the training patterns (input/output pairs) to be encoded.

VI. PROBLEM WITH THE TRAINING OF NEURAL NETWORK

Problem with neural networks is that a number of parameter have to be set before any training can begin. However, there are no clear rules how to set these parameters. Yet these parameters determine the success of the training. In the most general case, neural networks consist of an (often very high) number of neurons, each of which has a number of inputs which are mapped via a relatively simple function to its output. Networks differ in the way their neurons are interconnected (topology), in the way the output of a neuron determined out of its inputs (propagation function) and in their temporal behavior (synchronous, asynchronous or continuous).

The topology of a network has a large influence on the performance of that network but, so far, no method exists to determine the optimal topology for a given problem because of the high complexity of large networks. the choice of the basic parameter (network topology, learning rate, initial weights) often already determines the success of the training process. The selection of these parameters follow in practical use rules of thumb, but their value is at most arguable.

Genetic Algorithms Overview

The biological metaphor for genetic algorithms is the evolution of the species by survival of the fittest, as described by Charles Darwin. In a population of animals or plants, a new individual is generated by the crossover of the genetic information of two parents.

The genetic information for the construction of the individual is stored in the DNA. The human DNA genome consists of 46 chromosomes, which are strings of four different bases, abbreviated A, T, G and C. A triple of bases is translated into one of 20 amino acids or a "start protein building" or "stop protein building" signal. In total, there are about three billion nucleotides. These can be structured in genes, which carry one or more pieces information about the construction of the individual. However, it is estimated that only 3% of the genes carry meaningful information, the vast majority of genes - the "junk" genes - is not used.

The genetic information itself, the genome, is called the *genotype* of the individual. The result, the individual, is called *phenotype***.** The same genotype may result in different phenotypes. Twins illustrate this quite well.

Genetic algorithms are algorithms for optimization and machine learning based loosely on several features of biological evolution. They require five components:

i. A way of encoding solutions to the problem on chromosomes.

ii. An evaluation function which returns a rating for each chromosome given to it

iii. A way of initializing the population of chromosomes.

iv. Operators that may be applied to parents when they reproduce to alter their genetic composition. Standard operators are mutation and crossover Parameter settings for the algorithm, the operators, and so forth.

v. Given these five components, a genetic algorithm operates according to the following steps:

- Initialize the population using the initialization procedure, and evaluate each member of the initial population.
- Reproduce until a stopping criterion is met. Reproduction consists of iterations of the following steps:

➢ Choose one or more parents to reproduce. Selection is stochastic, but the individuals with the highest evaluations are favored in the selection.

➢ Choose a genetic operator and apply it to the parents.

➢ Evaluate the children and accumulate them into a generation. After accumulating enough individuals, insert them into the population, replacing the worst current members of the population.

The genetic information is encoded in a bit string of fixed length, called the parameter string or individual. A possible value of a bit is called an allele.

Each parameter string represents a possible solution to the examined problem. For the GANN problem, it contains information about the construction of a neural network. The quality of the solution is stored in the fitness value.

The basic GA operators are crossover, selection and mutation.

i. *Selection*—or survival of the fittest. The key to selection is to give preference to better outcomes.

ii. *Mutation*—or randomly trying combinations and evaluating the success (or failure) of the outcome.

iii. *Crossover*—or combining portions of good outcomes in the hope of creating an even better outcome.

Crossover is performed by taking parts of the bit-string of one of the parents and the other parts from the other parent and combining both in the child. There are three basic kinds of crossover: one point, two-point and uniform.

One-point crossover is illustrated in Figure . Both parent bit-strings are cut at the same point. So, the child can be generated by taken one part from each parent.

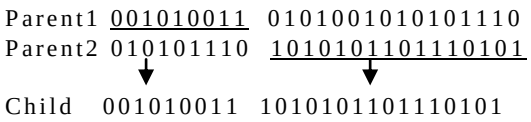


Figure5: One Point Crossover

Two-point crossover differs from the previous version merely in the point that two random cuts are made, so three pieces have to be put together in order to produce an offspring.

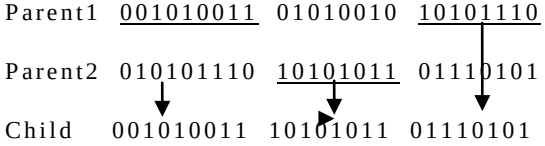


Figure6: Two-point crossover

The third one, uniform crossover is suggested in. It is illustrated in figure 1.6. Here, for each bit, it is randomly decided, if it is copied from parent one or two. During a generation a fixed number of crossovers and mutations are performed.

Figure8 illustrates the principle structure of a genetic algorithm. It starts with the random generation of an initial set of individuals, the initial population.

The individuals are evaluated and ranked. Since the number of individuals in each population is kept constant, for each new individual an old one has to be discarded, in general the one with the worst fitness value.

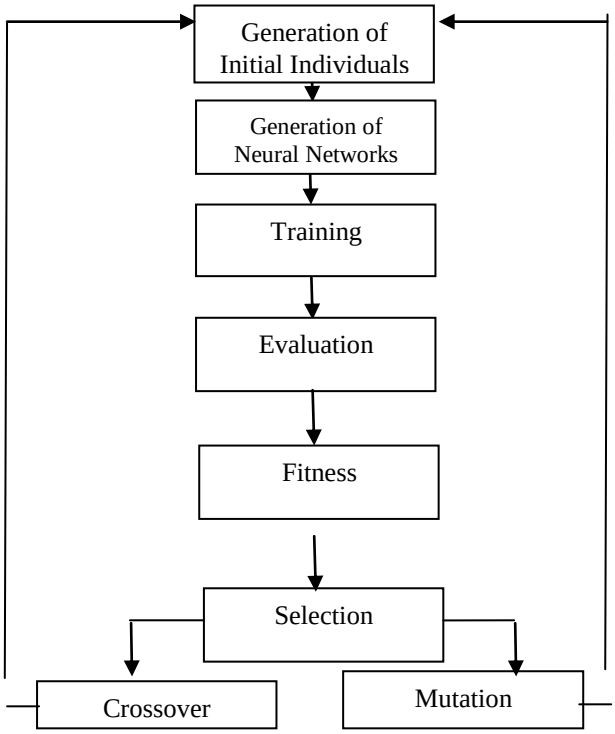
VII. GENETIC ALGORITHM ALONG WITH NEURAL NETWORK

(GANN) By combining genetic algorithms with neural networks (GANN), the genetic algorithm is used to find these parameters. The inspiration for this idea comes from nature: In real life, the success of an individual is not only determined by his knowledge and skills, which he gained through experience (the neural network training), it also depends on his genetic heritage (set by the genetic algorithm). One might say, GANN applies a natural algorithm that proved to be very successful on this planet: It created human intelligence from scratch. The main question is how exactly GA and NN can be combined, i.e. especially how the neural network should be represented to get good results from the genetic algorithm. The general idea of combining GA and NN is illustrated in figure.

Information about the neural network is encoded in the genome of the genetic algorithm. At the beginning, a number of random individuals are generated. The parameter strings have to be evaluated, which means a neural network has to be designed according to the genome information. Its performance can be determined after training with back-propagation. Some GANN strategies rely only on the GA to find an optimal network; in these, no training. takes place. Then, they are evaluated and ranked. The fitness evaluation may take more into consideration than only the performance of the individual.

Some approaches take the network size into account in order to generate small networks. Finally, crossover and mutation create new individuals that replace the worst or all members of the population This general procedure is quite straight-forward. The problem of combining GA and NN, however, lies in the encoding of the network The new ideas and concepts of GA and NN bring new life into Artificial Intelligence research. But still, we encounter again an old problem: the problem of representation. Initializing the Population The initial population is not generated by randomizing the chromosome strings but by randomizing weight matrices which are then encoded as strings. This allows the initial weights to be distributed in a smaller range than the used encoding interval and reduces the Probability of starting back propagation in a very flat region of the error function which would lead to very small gradients. Encoding Neuronal Networks Information about the neural network is encoded in the genome of the genetic algorithm. At the beginning, a number of random individuals are generated. The parameter strings have to be evaluated, which means a neural network has to be designed according to the genome information. Its performance can be determined after training with back-propagation. Direct Encoding In this paper, the term "direct encoding" refers to encoding strategies that directly encode parameters of the neural net such as weight values, connection information, etc. into the genome.

This is opposed to "indirect encoding", where rules or alike are encoded which carry information how the network has to be constructed. GENITOR It is the most influential approach of direct encoding that encode the weights of a given (layered) topology in bit-strings .Figure below illustrates this. The index-bit indicates if the connection exists at all, and the weight-encoding bits are a binary representation of the weight value. Whitley reports a 8-bit encoding, "ranging between -127 to +127 with 0 occurring twice". The illustration merges two variation of the GENITOR algorithm: The weight-optimization Generation of initial-



Principle Structure of GA and GANN System

individuals version and the network pruning algorithm. The first uses just the weight-encoding bits, the second merely the index-bit. For the later, the weight values of an already generated optimal network are used, the goal is to find a minimal network with good performance. Of course, the number of weights pruned has to be considered in the fitness function. GENITOR requires that a basic (maximal) architecture has to be designed for each problem. The resulting encoding format is a bit-string of fixed length. The standard GA has no difficulties to deal with this genome. Since crossover can take place at any place of the bit string, a child may have a different weight value than either one of the parents. So, topology and weight values are optimized at the same time. Whitley reports that GENITOR tends to converge to a single solution, the diversity is reduced fast. It seems to be a good "genetic hill-climber". The approach was applied to simple Boolean functions.

VIII. CONCLUSION

In this paper we saw different technique that is being used to execute credit card fraud how credit card fraud impact on the financial institution as well as merchant and customer, fraud detection technique used by VISA and MasterCard. Neural network is a latest technique that is being used in different areas due to its powerful capabilities of learning and predicting. In this thesis we try to use this capability of neural network in the area of credit card fraud detection as we know that Back propagation Network is the most popular learning algorithm to train the neural network so in this paper BPN is used for training purpose and then in order to choose those parameter (weight, network type, number of layer, number of node e.t.c) that play an important role to perform neural network as accurately as possible, we use genetic algorithm, and using this combined Genetic Algorithm and Neural Network (GANN) we try to detect the credit card fraud successfully. The idea of combining Neural Network and genetic Algorithm come from the fact that if a person is inherently very talented and he is trained properly then chances of individual of success is very high.

IX. FUTURE WORK

As we saw in this credit card fraud detection system there is a need of very large amount of previous data related to the pattern the consumer made during credit card use in purchase, as in our GANN, Neural Network is train on this data but the problem arises at the initial stages when very few or not at all initial transaction has been made, how will we train NN when only few or no data is available to train the network because in order to make a Neural Network to predict we must have some pattern through which NN can get train and make prediction. So we must have to design some system that may control credit card fraud before any real transaction is made.

REFERENCES

[1] Jitendra Dara,Laxman Gundemoni, “Credit Card Security And E-Payment.”2006.
[2] The New England Debit Card Task Force “Best Practice Guide for Managing Debit Card Fraud.” IEEE July 2005.
[3] David J. Montana, “Neural Network Weight Selection Using Genetic Algorithms.” Bolt Beranek and Newman Inc. July 2003.
[4] Philip K. Chan, Wei Fan, Andreas L.Prodromidis, and Salvatore J, “Distributed Data Mining in Credit Card Fraud Detection” IEEE December 1999.
[5] Sushmito Ghosh and Douglas L. Reilly, “Credit Card Fraud Detection with a Neural-Network.” Nestor, Inc. IEEE (1994).
[6] Rajesh Parekh,, Jihoon Yang,and VasantHonavar, “Constructive Neural-Network Learning Algorithmsfor Pattern Classification” IEEE 2000.
[7] Mubeena Syeda,Yan-Qing and Yi-Pan,“Parellel Granular Network For Credit Card Fraud Detection”. IEEE 2002.
[8] Erik Bothelius, “Fraud detection in the Internal Account System for Payment Service Providers.” May 8, 2005.
[9] D.WHITLEY,“Genetic Algorithm And Neural Network.”2003.

'