Comparative Study Using Neural Networks Techniques for Credit Card Fraud Detection

Imane Sadgali(✉), Nawal Sael, and Faouzia Benabbou

Laboratory of Modelling and Information Technology,
Faculty of Sciences Ben M'SIK, University Hassan II, Casablanca, Morocco
sadgali.imane@gmail.com, saelnawal@hotmail.com,
faouzia.benabbou@univh2c.ma

Abstract. Credit cards have become a necessity in the virtual world for digitized and paperless transactions. Every day, millions of credit card transactions occur, but these transactions are subject to various types of fraud. Numerous works have proposed techniques developed to analyze, detect and prevent credit card fraud. In recent years, several studies have used machine-learning techniques to find solutions to this problem. In this article, we conducting a comparative study of techniques based on neural networks, applied to the same data set. Our goal is to offer a complete analysis to choose the best credit card fraud detection techniques.

Keywords: Fraud detection · Machine learning · Credit card · Neural network · Deep learning

1 Introduction

Fraud affects public and private organizations, and covers a wide range of illegal practices and acts involving deception or intentional misrepresentation. This is a costly problem for many financial institutions, so they use a variety of fraud prevention models to address this problem. Over the years, along with the evolution of fraud detection methods, fraud perpetrators have also changed their fraud practices to avoid detection [24]. Therefore, credit card fraud detection methods require constant innovation.

Machine learning techniques are actively involved in finding a solution to this problem of credit card fraud detection. They are often used to extract and discover the truths hidden behind very large amounts of data. In addition, many recent works use modern detection techniques in many areas, with the increase in the number of frauds affecting the financial sector each year.

In our previous state of art [1], where we stand out the best techniques of machine learning for credit card fraud detection. Here, we use the same dataset to confirm our previous finding. This study aims to evaluate different machine Learning techniques with regard to their efficacy in detecting credit card fraud, over the same dataset.

The rest of the document is structured as follows. Section 2 presents related works. Section 3 gives a description of used dataset. Section 4 will details the method of our comparative study. Section 5 analyses results and Sect. 5 ends the paper with the conclusions and future work.

M. Ben Ahmed et al. (Eds.): SCA 2019, LNITI, pp. 287–296, 2020.
https://doi.org/10.1007/978-3-030-37629-1_22

2 Related Works

From our previous work [1], we have observed that, practically, almost all of techniques focus on online frauds, because it considered as the most critical and spreader one. However, most of them give a result based on a particular dataset, which is itself characterized by unbalanced data. In this paragraph, we will present a different works, related to neural network techniques, implemented for credit card fraud detection.

In 2008, Quah proposed, for real-time fraud detection, a new and innovative approach. He uses self-organization map (SOM), Neural Networks (NN) and rules induction (RI). The filtering of transactions for further review reduces the overall cost as well as processing time [4]. In 2014, Olszewski have proposed fraud detection system visualizing the user activities with SOM, which is a method of mapping a high dimensional data into a 2-dimensional map of neurons and classifying based on threshold value, which works for multiple frauds [5].

In 2017, Mubalaik proposed an ANN-MPL Algorithm (Artificial Neural Network-ltechniques, it helps to anticipate and quickly detect fraud. Zanin proposed hybrid data mining/complex network; Parenclitic Network (PN), classification algorithm, able to detect illegal instances in a real card transaction dataset [10]. It can be observed that, fraud detection using neural network is based on Pattern Recognition, when a fraudulent transaction is detected; the weights of the inputs related to that transaction pattern are updated. The disadvantage of this approach is that every time a new pattern of fraud occurs the entire network has to be re-trained.

Deep Learning (DL) presents a promising solution to the problem of credit card fraud detection by enabling institutions to make optimal use of their historic customer data as well as real-time transaction [9]. In a comparative study between DL, LR and Gradient Boosted Tree [10], the authors found that deep learning has the largest value for the majority of the feature sets, such as: frequency of transaction, number of transactions, transaction amount,… In [11] the authors evaluated different DL algorithms and shown that, the Long Short-term Memory (LSTM) and Gated Recurrent Units (GRUs) model significantly outperformed the baseline ANN. This indicates that order of transactions for an account contains useful information in differentiating between fraud and non-fraudulent transactions.

Most of these proposed work, present results based on specific dataset, from one financial institution. That why we choose to applied this techniques to one and unique generic dataset, to have a reliable result, and a trusted comparison.

2.1 Artificial Neural Network (ANN)

An artificial neuron network (ANN) is a computational model based on the structure and functions of biological neural networks. … ANNs are considered nonlinear statistical data modeling tools where the complex relationships between inputs and outputs are modeled or patterns are found.

2.2 Multilayer Preceptron (MPL)

"Perceptrons" is a term coined by Rosenblatt (1958) while studying the basic idea behind the mammalian visual system. A perceptron is an artificial neuron having n input signals with different weights, an activation (processing) function, and a threshold function. A perceptron can efficiently solve the linearly separable problems. However, to solve more realistic problems, there is a need to have complex architecture using multiple neurons [36].

2.3 Long Short-Term Memory (LSTM)

Long short-term memory (LSTM) is an artificial recurrent neural network (RNN) architecture used in the field of deep learning…. LSTM networks are well-suited to classifying, processing and making predictions based on time series data, since there can be lags of unknown duration between important events in a time series.

2.4 Recurrent Neural Network (RNN)

A recurrent neural network (RNN) is a class of artificial neural networks where connections between nodes form a directed graph along a temporal sequence. This allows it to exhibit temporal dynamic behavior. Unlike feedforward neural networks, RNNs can use their internal state (memory) to process sequences of inputs.

2.5 Gated Recurrent Unit (GRU)

A gated recurrent unit (GRU) is part of a specific model of recurrent neural network that intends to use connections through a sequence of nodes to perform machine-learning tasks associated with memory and clustering, for instance, in speech recognition.

2.6 Self-organization Map (SOM)

A self-organizing map (SOM) is a type of artificial neural network (ANN) that is trained using unsupervised learning to produce a low-dimensional (typically two-dimensional), discretized representation of the input space of the training samples, called a map, and is therefore a method to do dimensionality reduction.

Table 1 below, gives result of previous works, each paper has his own particular dataset.

Table 1. Previous works results

Technique	Accuracy (%)	Reference
ANN + MPL	99.4	[9]
LSTM	91.2	[31]
RNN	90.4	[31]
GRU	91.6	[31]
ANN	88.2	[31]
SOM	100	[35]

As we can see, some works achieve a high accuracy, but it does not mean is the best technique for credit card fraud detection. That why we decide to make this comparison with the same dataset, to have a detached and objective result.

3 Method of Comparison

In our analysis, we applied neural network techniques on the dataset, on which we have added transaction label.

The following are neural network algorithms, which are employed to build a classifier for the given dataset. The classifier model classifies the credit card transactions as either fraudulent or not.

3.1 NN

Neural Networks (NN) is a mature technology with an established theory and recognized application areas. A NN consists of a number of neurons, i.e., interconnected processing units. Associated with each connection is a numerical value, called "weight". Each neuron receives signals from connected neurons and the combined input signal is calculated. The total input signal for neuron j is: $U_j = \sum w_{ij} * x_i$, where x_i is the input signal from neuron i and w_{ij} is the weight of the connection between neuron i and neuron j. If the combined input signal strength exceeds a threshold, then the input value is transformed by the transfer function of the neuron and finally the neuron fires [31]. The neurons are arranged into layers. A layered network consists of at least an input (first) and an output (last) layer. Between the input and output layer there may exist one or more hidden layers [32].

3.2 MPL

Multilayer Preceptron Layer (MPL) is an artificial neural network structure and is a nonparametric estimator that can be used for classifying and detecting intrusions [8]. Multilayer Perceptron (MLP-ANNs) are the simplest and therefore the most commonly used NN architectures [28]. The structure of an MLP-ANN consists of one input layer, one intermediate or hidden layer, and one output layer. Each layer can have a number of neurons, which are connected linearly by weights to the neurons in the neighboring layers.

In multilayer preceptron model, such many neurons are arranged in three layers. The multilayer perceptron here has n input nodes, h hidden nodes in its (one or more) hidden layers, and m output nodes in its output layer.

There may be multiple input and output layers if required. W_{ij} is the weight associated with *i*th node of the input layer to *j*th node of the next layer. In a similar way, each node of a given layer is connected to every node in its adjacent layer. All connections are in a forward direction only. That is why such a structure is known as fully connected, feed-forward, multilayer network.

The network receives inputs from neurons in the input layer, and the output of the network is given by the neurons in an output layer. In such a network, artificial neurons, which are organized in layers, send their signals “forward” and then the errors are propagated backward. The idea of such backpropagation is to reduce this error until the ANN learns the training data in a supervised manner. While learning, input data from the training set are passed to the input layer of the network. The network calculates and then compares with the actual output from the training set. This phase is known as forward pass. Depending on the distance observed between the calculated output and actual output, weights are adjusted. This phase is known as backward pass. Such many forward and backward passes are experimented on a network to train the network for a set of data. Such multiple sets are used to train the network. At the end, when real input values are fed to the network, it gives the output based on its learning.

This algorithm is known as backpropagation learning algorithm in a supervised manner because of two reasons: (i) the error (difference calculated between the correct output and calculated output) is propagated back and the solution (from input to output) is propagated in forward direction and (ii) the training set is a must. The backpropagation algorithm has become the most popular one for training of the multilayer perceptron [36].

3.3 CNN

Convolutional Neural Network (CNN) is a part of deep learning. Mapping of input into hidden layer represents one feature map. Each feature map represents one characteristic. Process of compressing neurons into feature map is called convolution. Subsampling reduces parameters of feature map. Fully connected layer is same as neural network [26]. CNN is successfully applied in face recognition, character recognition, image classification … etc. Kang Fu, Dawei Cheng, Yi Tu, and Liqing Zhang at [27] proposed a convolutional neural network based approach to find fraudulent transactions in credit card. To relieve the problem of the imbalanced dataset, they used cost based sampling method to generate different number of synthetic frauds to train the model.

They applied CNN model because it is suitable for training large size of data and CNN has mechanism to avoid over-fitting [25].

The convolution layer is the core building block of the CNN. It carries the main portion of the network’s computational load.

This layer performs a dot product between two matrices, where one matrix is the set of learnable parameters otherwise known as a kernel, and the other matrix is the restricted portion of the receptive field. The kernel is spatially smaller than an image, but is more in-depth. This means that, if the image is composed of three (RGB) channels, the kernel height and width will be spatially small, but the depth extends up to all three channels.

During the forward pass, the kernel slides across the height and width of the image producing the image representation of that receptive region. This produces a two-dimensional representation of the image known as an activation map that gives the response of the kernel at each spatial position of the image. The sliding size of the kernel is called a stride [37].

If we have an input of size W x W x D and D_{out} number of kernels with a spatial size of F with stride S and amount of padding P, then the size of output volume can be determined by the following formula:

$$W_{out} = (W - F + 2P)/S + 1 \quad (1)$$

4 Data Description

4.1 Dataset Generation

This study is based on a dataset, generated, containing approximately 60.000 transactions in across 12 attributes. These attributes include transaction and client information.

The chosen features, from financial institution database, for our experience are:

- Transaction amount: the amount of transaction adjusted in bank currency
- Transaction type: national, international or e-commerce.
- Transaction date and time: date and time of transaction in YYMMDDHHMMSS format.
- Transaction channel: the channel of incoming transaction (Automatic terminal machine (ATM), Terminal of payment electronic, merchant application or)
- Billing address: address of billing for the customer and Shipping address: address of merchant or point of service for the purchase, address of ATM for withdrawal.
- Merchant type: hotels, healthcare, transport, food …

The rest of features are providing using features engineer.

Table 2 displays the distribution of legitimate and fraudulent transactions.

Table 2. Distribution of dataset

Type of transactions	Number of transactions	Percentage of transactions
Genuine	59832	99.72%
Fraudulent	168	0.28%

To construct this dataset, we try hard to have a randomly 200 transactions with two transactions status, and data susceptible to be fraudulent transactions. The rest of dataset was generated with only the legitimate status.

There is a significant class imbalance in the classifier, where 99.72% of transactions are of the non-fraudulent. To be as close as possible to a real financial dataset.

4.2 Feature Engineer

The creation of domain expertise functions participate significantly in the construction of predictive models of credit card fraud detection; since financial systems manage a huge flow of information about card accounts, customers and transactions [3]. However, not all of these data reveal important predictors such as consumer consumption patterns over time, or a client's travel abroad, etc. Many of these predictors can be derived from all of the original data. This research identifies and creates some important and commonly used predictors.

For this study, the following predictors were created and added to the data:

- Inter transaction gap time: time between the current transaction and the last one.
- Number of transaction per day.
- Number of transactions per week.
- Number of transactions per month.
- Frequency of transaction type.
- Time range purchase: weekend, evening, holiday, other. Results

To compare these algorithms, the following measures are considered. There are many factors used to measure the performance of classifiers or predictors.

For our analysis we choose the accuracy factor: Accuracy = (TP + TN)/(TP + FP + TN + FN).

- True Positives (TP) are the data tuples that are correctly identified as «not fraudulent» data
- False Positives (FP) are the data tuples that are mistakenly identified as «not fraudulent» data.
- True Negatives (TN) are the data tuples that are correctly identified as fraud data.
- False Negatives (FN) are the data tuples that are mistakenly identified as fraud data.

Batch size: is a term used in machine learning and refers to the number of training examples utilized in one iteration.

After applying the machine learning techniques discussed in the paper, the accuracy of each supervised learning technique used has been calculated and listed in Table 3.

Table 3. Accuracy of neural network

Techniques	Hidden layer size	Batch size	Accuracy
Simple neural network	100	50	58.06%
	100	20	**67.58%**
	50	50	49.85%
	50	20	49.07%
	20	50	49.65%
Multilayer preceptron layer	100	50	51.52%
	100	20	87.88%
	50	50	68.57%
	50	20	82.86%
	20	50	54.29%
Convolutional neural network	100	50	80.00%
	100	20	**82.86%**
	50	50	71.43%
	50	20	77.14%
	20	50	68.57%

For the test conditions, we fixed the learning rate to 0.001, and we choose to use Relu and Softmax as an activation functions.

The Softmax activation transforms a bunch of arbitrarily large or small numbers into a valid probability distribution. While other activation functions get an input value and transform it, regardless of the other elements, the Softmax considers the information about the whole set of numbers we have The values that Softmax outputs are in the range from 0 to 1 and their sum is exactly 1 (like probabilities) [33].

For our dataset, we balanced data using under-sampling method. When we have an imbalanced data, the accuracy is higher but does not insure a good prediction. A simple example, if we have a model that give one result for all our data: not fraudulent transaction, the accuracy of this model will be equal to the rate of non-fraudulent transactions: 99.72%, and of course that totally unaccepted.

From Table 3 we conclude that the best accuracy we can reach with the combination of hidden layer size = 100 and batch size = 20, and the higher result was with simple neural network applied on our dataset was. Following by convolutional neural network.

5 Conclusion

This paper examined the performance of three advanced data mining techniques, NN and MPL, together with CNN, for credit card fraud detection. A unique generic dataset on credit card transactions was used in our evaluation. The performance of each technique was analyzed and compared. Multilayer preceptron proved to be the best among the others for credit card fraud detection applied to our unique and generic dataset.

Our main objective is to identify techniques that gives the best result, in order to integrate it in our adaptive model for credit card fraud detection. In our future work, we will present a complete architecture of an adaptive model for credit card fraud detection, using our finding in this comparison.

References

1. Sadgali, I., Sael, N., Benabbou, F.: Detection of credit card fraud: state of art. Int. J. Comput. Sci. Netw. Secur. **18**(11), 76–83 (2018)
2. ACFE Association of Fraud Examiners Certificates. http://www.acfe.com/uploadedfiles/acfewebsite/content/documents/rttn-2010.pdf. Accessed 15 July 2014
3. Barker, K.J., D'amato, J., Sheridon, P.: Credit card fraud: awareness and prevention. J. Financ. Crime **15**(4), 398–410 (2008)
4. Quah, J., Sriganesh, M.: Real-time credit card fraud detection using computational intelligence. Expert Syst. Appl. **35**(4), 1721–1732 (2008)
5. Olszewski, D.: Fraud detection using self-organizing map visualizing the user profiles. Knowl. Based Syst. **70**, 324–333 (2014)
6. Sanchez, D., Vila, M.A., Cerda, L., Serrano, J.M.: Association rules applied to credit card fraud detection. Expert Syst. Appl. **36**(2), 3630–3640 (2009)

7. Askari, S., Hussain, A.: Credit card fraud detection using fuzzy ID3. In: IEEE, Computing, Communication and Automation (ICCCA), pp. 446–452 (2017)
8. Duman, E., Ozcelik, H.: Detecting credit card fraud by genetic algorithm and scatter search. Expert Syst. Appl. **38**(10), 13057–13063 (2011)
9. Mubalik (Mubarek), A., Adali, E.: Multilayer preceptron neural network technique for fraud detection. In: International Conference on Computer Science and Engineering (UBMK), pp. 383–387. IEEE (2017)
10. Zanin, M., Romance, M., Moral, S., Criado, R.: Credit card fraud detection through parenclitic network analysis, arXiv:1706.01953v1, pp. 1–8 (2017)
11. Halvaiee, N.S., Akbari, M.K.: A novel model for credit card fraud detection using artificial immune systems. Appl. Soft Comput. **24**, 40–49 (2014)
12. Dai, Y., Yan, J., Tang, X., Zhao, H., Guo, M.: Online credit card fraud detection: a hybrid framework with big data technologies. In: IEEE Trustcom/BigDataSE/ISPA, pp. 1644–1652 (2016)
13. Malini, N., Pushpa, M.: Analysis on credit card fraud identification techniques based on KNN and outlier detection. In: Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB). IEEE (2017)
14. Chawla, N.V., Bowyer, K.W., Hall, L.O., Kegelmeyer, W.P.: SMOTE: synthetic minority over-sampling technique. J. Artif. Intell. Res. **16**, 321–357 (2002)
15. Zeager, M.F., Sridhar, A., Fogal, N., Adams, S., Brown, D.E., Beling, P.A.: Adversarial learning in credit card fraud detection. In: Systems and Information Engineering Design Symposium (SIEDS), pp. 112–116. IEEE (2017)
16. Shaji, J., Panchal, D.: Improved fraud detection in e-commerce transactions. In: Communication Systems, Computing and IT Applications (CSCITA), pp. 121–126. IEEE (2017)
17. Carcillo, F., Le Borgne, Y., Caelen, O., Bontempi, G.: An assessment of streaming active learning strategies for real-life credit card fraud detection. Int. J. Data Sci. Analytics, 1–16 (2017)
18. Laurens, R., Jusak, J., Zou, C.: Invariant diversity as a proactive fraud detection mechanism for online merchants. In: IEEE Global Communications Conference (2017)
19. Hejazi, M.: One-class support vector machines approach to anomaly detection. Appl. Artif. Intell. J. **27**(5), 351–366 (2013)
20. Vimala Devi, J., Kavitha, K.S.: Fraud detection in credit card transactions by using classification algorithms. In: International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC) (2017)
21. Malini, N., Pushpa, M.: Analysis on credit card fraud identification techniques based on KNN and outlier detection. In: IEEE Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB) (2017)
22. Vapnik, V.: Statistical Learning Theory. Wiley, New York (1998)
23. Cristianini, N., Shawe-Taylor, J.: An Introduction to Support Vector Machines and Other Kernel-based Learning Methods. Cambridge University Press, Cambridge (2000)
24. https://medium.freecodecamp.org/machine-learning-mean-squared-error-regression-line-c7dde9a26b93
25. Bolton, R.J., Hand, D.J.: Unsupervised profiling methods for fraud detection. In: Conference on Credit Scoring and Credit Control, Edinburgh (2001)
26. Modi, K., Dayma, R.: Review on fraud detection methods in credit card transactions. In: IEEE, International Conference on Intelligent Computing and Control (I2C2 2017) (2017)
27. Nielsen, M.: Deep learning, 15 March 2017. http://neuralnetworksanddeeplearning.com/chap6.html
28. Fu, K., Cheng, D., Tu, Y., Zhang, L.: Credit Card Fraud Detection Using Convolutional Neural Networks. Springer, Cham (2016)

29. Prakash, O., Khan, F., Sangwan, R.S., Misra, L.: ANN-QSAR model for virtual screening of androstenedione C-skeleton containing phytomolecules and analogues for cytotoxic activity against human breast cancer cell line MCF-7. Comb. Chem. High Throughput Screen **16**, 57–72 (2013)
30. Bengio, Y., Boulanger-Lewandowski, N., Pascanu, R.: Advances in optimizing recurrent networks. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 8624–8628, May 2013
31. Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., Beling, P.: Deep learning detecting fraud in credit card transactions. In: Proceedings of International Conference Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, pp. 129–134 (2018)
32. Han, J., Camber, M.: Data Mining Concepts and Techniques. Morgan Kaufman, San Diego (2000)
33. Kirkos, E., Spathis, C., Manolopoulos, Y.: Data mining techniques for the detection of fraudulent financial statements. Expert Syst. Appl. **32**(4), p995–1003 (2007)
34. https://www.udemy.com/machine-learning-with-tensorflow-for-business-intelligence/learn/lecture/8447970#overview
35. Olszewski, D.: Fraud detection using self-organizing map visualizing the user profiles. Knowl.-Based Syst. **70**, 324–333 (2014)
36. Sajja, P.S., Akerkar, R.: Swarm Intelligence and Bio-Inspired Computation (2013)
37. Bengio, Y., Goodfellow, I.J., Courville, A.: Deep Learning, 11 January 2015