2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI)
Dec. 22nd, 2017
(Iran University of Science and Technology) – Tehran, Iran

Using deep networks for fraud detection in the credit card transactions

Zahra Kazemi
Science and Research
Islamic Azad University
Tehran, Iran
Email: zk3911@gmail.com

Houman Zarrabi
Science and Research
Iran ICT Research Center
Tehran, Iran
Email: h.zarrabi@itrc.ac.ir

***Abstract*— Deep learning is a very noteworthy technic that is take into consideration in the several fields. One of the most attractive subjects that need more attention in the prediction accuracy is fraud detection. As the deep network can gradually learn the concepts of any complicated problem, using this technic in this realm is very beneficial. To do so, we propose a deep autoencoder to extract best features from the information of the credit card transactions and then append a softmax network to determine the class labels. Regarding the effect of features in such data employing an overcomplete autoencoder can map data to a high dimensional space and using the sparse models leads to be in a discriminative space that is useful for classification aims.**

The benefit of this method is the generality virtues that we can use such networks in several realms e.g. national intelligence, cyber security, marketing, medical informatics and so on. Another advantage is the ability to facing big datasets. As the learning phase is offline we can use it for a huge amount of data and generalize that is earned. Results can reveal the advantages of proposed method comparing to the state of the arts.

Keywords— Credit card transactions; fraud detection; deep networks; autoencoder

I. Introduction

Fraud in the credit card transactions leads to a huge amount of losses each year. In the recent years by the improvement of machine learning methods it is beneficial to utilize these technics to prevent such difficulties and decide about the upcoming events [1].

As the banking transactions and the behavior of customers are in a high variance patterns, selecting the robust method with the high accuracy is a serious problem. To do so, many methods are suggested and there are several implementations. One of the most applicable suggestions, look forward the prediction of customer behaviors for the next confidences. When a person requests for a loan, it is very important to determine the level of risk according to the agreement.

Recently, several methods of data mining seek to find the best way for this prediction. One of the most popular methods that has been very useful in the recent decade is employing deep learning. There are several methods of deep learning that can extract most applicable and abstract features form raw data. As autoencoders are so simple and they can be used regardless of class labels, they are so useful for our purpose [2].

There are several variants of autoencoders that each one has pros and cons. Regarding the aim of our problem we have used two of them in this research and compare the results with the state of the arts [3]. Another advantage of employing deep autoencoders in this realm is according to big data maintenance. As these methods are eager and by considering huge amount of data can take the advantages of generalization they can be very useful [4].

In the rest of this paper, at first we discuss about some needed background around fraud detection and deep autoencoders. Then the proposed method is explained and the results are demonstrated. Finally, the discussion and future works are presented.

II. Background

In this section we discuss about some required concepts.

A. Fraud detection regarding credit card transactions

Credit cards are playing a deniable role in the banking systems, and there are several information extraction and data mining methods to extract various concepts from the corresponding transactions [5]. As the best way is to prevent the fraudulent activities, the most useful applications of such methods is to make decision about the reliability of a customer [6]. Maybe this decision is to grant him a loan or some other facilities like increasing his credit.

There are several proposed methods to detect the fraudulent activities [5]. In an efficient method in this realm, Khodabakhshi and Fartash proposed to use k-nearest neighbor (kNN) with association rules to detect outliers among the transactions which is used in credit card in electronic banking system. [7].

978-1-5386-2640-5/17/$31.00 ©2017 IEEE

Another enhanced method in this realm uses Genetic Programming to evolve decision trees for data classification and prevent the search spaces to become extremely large [8]. They study the problem of mining changes of classification characteristics as the data changes. For example "members with a large family no longer shop frequently, but they used to". Finding this kind of changes holds the key for the organization to adopt to the changed environment and stay ahead of competitors. The challenge is that it is difficult to see what has really changed from comparing the old and new classifiers that could be very large and different [8].

One of the most popular methods, uses a self-organization map (SOM) algorithm to map data in a discriminative space and use some simple method to discern the class label [9]. Dominik proposed a fraud detection method based on the user accounts visualization and threshold-type detection.

B. Autoencoders

The autoencoder is similar to a simple multilayer perceptron (MLP). Its learning method is the same too, but there is a major difference that is unsupervised learning [10]. In such networks the input is the available features of data, like MLP, but instead of reaching a target the goal is to reach to the input again. Then we are using a network to map data from the original space to a low dimensional space provided that, we do not miss the initial concepts [11]. The procedure of converting raw data to a low dimension space named encoding and the reverse operation that reconstruct the original data is decoding. Fig. 1 shows the structure of such a simple network.

The results in such network is very similar to the results of linear feature extractions like PCA. The only difference is the constraint of the orthogonality, while the final results show the same conditions [12]. To improve the results a nonlinear function can be added to the neurons that leads to regarding the nonlinearity conditions. Then autoencoder can be used in several applications and the main advantage is to extract best features for data analysis.

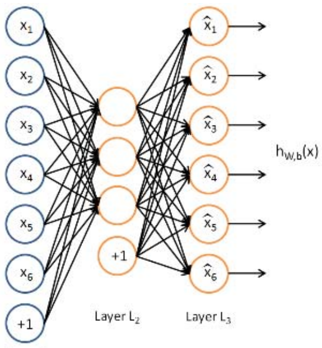

Fig. 1. Encoding and decoding stages of a simple autoencoder

In the task of classification, when the dimension of input data is not large or when the data is not discriminative, we can take the advantages of sparse autoencoders. In this case the number of neurons in the hidden layer are more that the input neurons and the problem has a trivial solution. Then by exerting sparsity on the hidden layer we can reach to the data like sparse coding technique.

Sparsity may be achieved by additional terms in the loss function during training (by comparing the probability distribution of the hidden unit activations with some low desired value) [13], or by manually zeroing all but the few strongest hidden unit activations [14]. Fig. 2 demonstrates the overall view of overcomplete and sparse autoencoders.

C. Deep networks

The most important thing in data analysis is accessing to proper data representation [15]. Deep learning is one of the most powerful and popular methods. In deep network, motivated from the decision making in the brain of humans, the learning and feature representation is a multi-stage procedure. Then any complex problem can be represented in a simple manner and the data representation is more manageable.

One of the most popular deep networks, emerge in autoencoders [3]. In such networks, in the first layer, data is encode to a low dimensional space, such that by decoding the initial data is reachable. The second layer uses the encoded data and map it to a lower dimensional space that is reversible, so the encoded data can decode to the output of first layer and so on, it can decode to the original space and so on.

In the simple MLP, traditionally, to apply nonlinearity some activation functions are employed e.g. sigmoid and hyperbolic tangent function. But in the deep networks, using such functions leads to vanishing gradient difficulty. As backpropagation computes gradients by the chain rule, the gradient decreases exponentially and the front layers train very slowly [16].

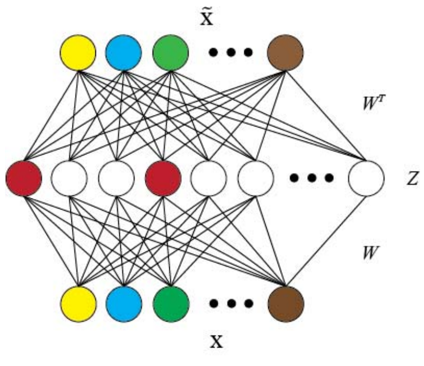

Fig. 2. Structure of sparse autoencoders. The hidden layer has more neurons than the others and as there is a trivial solution that make some neuron the same as input and leave the other ones zero, we need the term of sparsity.

To solve this difficulty, another activation function named rectifier is exerted [17]. A unit employing the rectifier is also called a rectified linear unit (ReLU) [18]. The activation function considers as below:

$$F(x) = \max(0,x) \qquad (1)$$

where x is the input to a neuron. By this function the update of consequent neurons is possible and leads to faster learning. After extracting the final features a powerful classifier can discriminate the classes. A useful classifier that often is added to such networks is softmax [19]. As we only need two classes for discrimination, a logistic function is enough. Then by appending a simple classifier at the end of final encoded layer the recognition process is fulfilled.

Finally, the encoded output of final layer can be regarded as the final intended feature representation and moreover containing the original data information, the noise and other redundant features are eliminated.

III. PROPOSED METHOD

As there are several behaviors of customers in the banking transactions, extracting the appropriate pattern to detect fraudulent ones is very complex. To do so, employing deep networks is a beneficial idea and can be very useful to employ deep autoencoders.

We can pass the initial features of each transaction to the network and by training a deep autoencoder, extract the appropriate features. The structure of such network depends on the number of available features in the dataset. After that we can use a softmax layer to decide about the class label. Table I shows the algorithm according to the implementation of this idea.

As in such datasets we have less features in the input, we can raise the number of features gradually and extract some features in a sparse manner. Olshausen states that when the number of code elements are more than the dimensions of the input space, the bases would be non-orthogonal and thus exerting the constraint of sparsity will only deploy the necessary bases to represent the given input [16]. So similar to human brain employing sparse autoencoder leads to map data in a high level space that each sample can be reconstructed with only some of the features.

TABLE I. THE ALGORITHM OF DATA DISCRIMINATION

Input: raw features **Output: class labels**
1. Pass input features to the initial layer of autoencoder 2. Train autoencoder in 3 layers to extract best features of data 3. Use a softmax classifier to determine class labels in the output

IV. EXPERIMENTAL RESULTS

In this section at first we introduce the employed dataset and then, the results of the proposed method are compared to the state of the arts in this realm.

A. Dataset

As the information of credit cards are private, there are few public datasets in this field and most of papers in this realm have gathered their own dataset for evaluation.

German Credit Data is one of the most famous datasets in the realm of fraud detection and is employed in the several papers. It is available in two formats. The original dataset contains categorical attributes, but as in some of methods only numerical data are supported, another version is provided with only the numerical features. In this dataset, people are described by a set of attributes as good or bad credit risks. Table II shows the characteristics of the mentioned dataset.

For the learning of the network, at first 900 transactions are used as training and then, the remained 100 samples regarded as test data.

B. Results

According to the complexity of such data and the user's behaviors diversity, this realm of data mining suffers from the low accuracy comparing with the other subjects. In the pioneer methods, the accuracy was about %76 and in the recent ones it reaches about %82.

As deep learning considers some complexity of data distribution and handle the shape of data gradually, it can improve the detection rate and outperform the rival methods. In the first attempt we employ an autoencoder with 20 neurons in the input layer and 15, 10 and 5 neurons in the next layers respectively. Then this is an underfit deep autoencoder (UDAE). In the second proposed method we use 20 neurons in the input layer and 30, 50 and 100 neurons in the next layers respectively and exert a %20, %10 and %5 sparsity limitation for them.

Table III compares the accuracy of the proposed methods regarding the rivals. In the first method, the application of kNN with association rules are employed [7] and in the second one to confine the search space of decision tree GP method is utilized [8]. In the 3rd one, mapping data in a topological space is regarded [9]. The experiments have repeated 10 times in 10 folds cross validation and the variances have determined.

TABLE II. THE CHARACTERISTICS OF GERMAN CREDIT DATA

GERMAN CREDIT DATA	
Number of Instances	1000
Number of Attributes	20
Area	Financial

TABLE III. COMPARING THE PROPOSED METHODS WITH THE STATE OF THE ATRS. THE ACCURACY AND THE VARIANCE OF ALL METHODS ARE CORRESPONDING TO 10 FOLD CROSS VALIDATION

Method	Accuracy	Variance
kNN [7]	76.1	± 2.08
GP [8]	78.3	± 3.22
SOM [9]	82.4	± 1.83
UDAE	81.6	±2.09
ODAE	84.1	± 1.81

Finally, a softmax layer to apply classification is appended to our networks and leads to the best accuracy of all. We can see that the variance in the networks are the bests.

V. CONCLUSION AND FUTURE WORK

Fraud detection is a very hot topic in the financial realms and the loss of Non-creditworthy customers have a huge amount of loss for the banks and other corporations. But the diversity of applicant behaviors make the detections and predictions very difficult.

One of the most useful technics that has motivated the human brains is deep learning. In such networks any complicated distribution of data can be recognized in some stages. So we utilize a deep autoencoder in some layers to extract best features of the data and then classify the instances. In such networks, moreover gaining the high accuracy, the low variance is noticeable.

As the future work we suggest to examine the other variations of deep networks, such as convolutional neural network (CNN). Maybe it will be better to consider the sequence of transactions and use the recurrent convolutional neural network (RCNN) to reach more accurate results.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewersand the Associate Editor for the constructive evaluation of this paper.

REFERENCES

[1] N. Carneiro, G. Figueira, and M. Costa, “A data mining based system for credit-card fraud detection in e-tail,” *Decis. Support Syst.*, 2017.

[2] Q. Feng, Z. Dou, C. Li, and G. Si, “Anomaly Detection of Spectrum in Wireless Communication via Deep Autoencoder,” in *International Conference on Computer Science and its Applications*, 2016, pp. 259–265.

[3] L. Deng and D. Yu, “Deep Learning: Methods and Applications,” *Found. Trends Signal Process.*, vol. 7, no. 3–4, pp. 197–387, Jun. 2014.

[4] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, “Deep learning applications and challenges in big data analytics,” *J. Big Data*, vol. 2, no. 1, p. 1, Feb. 2015.

[5] S. Sorournejad, Z. Zojaji, R. E. Atani, and A. H. Monadjemi, “A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective,” *CoRR*, vol. abs/1611.06439, 2016.

[6] M. Lichman, “{UCI} Machine Learning Repository.” 2013.

[7] M. Khodabakhshi and M. Fartash, “Fraud Detection in Banking Using KNN (K-Nearest Neighbor) Algorithm,” 2016.

[8] K. Wang, S. Zhou, A. W.-C. Fu, and J. X. Yu, “Mining Changes of Classification by Correspondence Tracing,” in *SDM*, 2003.

[9] D. Olszewski, “Fraud detection using self-organizing map visualizing the user profiles,” *Knowledge-Based Syst.*, vol. 70, pp. 324–334, 2014.

[10] Y. Bengio, “Learning deep architectures for AI,” *Found. trends{®} Mach. Learn.*, vol. 2, no. 1, pp. 1–127, 2009.

[11] C.-Y. Liou, W.-C. Cheng, J.-W. Liou, and D.-R. Liou, “Autoencoder for words,” *Neurocomputing*, vol. 139, pp. 84–96, 2014.

[12] H. Abdi and L. J. Williams, “Principal component analysis,” *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 2, no. 4, pp. 433–459, 2010.

[13] A. Ng, “Sparse autoencoder.”

[14] A. Makhzani and B. Frey, “K-sparse autoencoders,” *arXiv Prepr. arXiv1312.5663*, 2013.

[15] Y. Bengio, A. Courville, and P. Vincent, “Representation learning: A review and new perspectives,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 8, pp. 1798–1828, 2013.

[16] B. A. Olshausen and D. J. Field, “Sparse coding with an overcomplete basis set: A strategy employed by V1?,” *Vision Res.*, vol. 37, no. 23, pp. 3311–3325, 1997.