May-June 2020
ISSN: 0193-4120 Page No. 3876-3880

Feature Construction by Using Autoencoder's Fusion for Credit Card Fraud Detection

[1]Deepika.S, [2]S.Senthil
[1]Research Scholar, Dept. of Computer Science Engineering, REVA University
[2]Professor and Director, School of Computer Science and Applications, REVA University
[1]deepikajaiswal9963@gmail.com, [2]dir.csa@reva.edu.in

Article Info
Volume 83
Page Number: 3876-3880
Publication Issue:
May-June 2020

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *12 May 2020*

Abstract
From past few years fraud transactions in credit card transaction is drastically increased in banking and e-commerce organizations. Hence need an automatic fraud detection model which can address all issues of customer. Machine Learning is one of the solutions to design model to find credit card fraud detection through the use supervised binary classification approach. In machine learning, the accuracy is depends on feature sets. In this paper we derived more number of feature sets from original feature set using different normalizations strategies. By using auto-encoders fusion, derived most optimal feature set and then used in Generative Adversarial Network (GAN) for training and to identify fraud transaction. These normalized optimal feature vectors with auto encoder fusion and GAN model given good results when compared with other state-of-art methods.

Keywords: *Fusion, auto-encoder, machine learning, GAN*

1. Introduction

Credit Card fraud is once somebody uses your credit your MasterCard or open-end credit to form purchase you didn't authorize. Credit card fraud is basically of two types is card present fraud and card not present fraud. According to Robertson[1],,the world wide fraud losses multiplied from $7.6 billion in 2010 to $21.81 billion in 2015, By 2020 MasterCard fraud losses are expected to succeed in to $31.67 billion. Robertson also mentioned that card present fraud in US in 2016 decreased to the one third when compared to its previous years where as the card not present fraud has increased dramatically in few years because of online ecommerce business and fraudsters legitimate steps of fraud.

Card not present fraud loss is anticipated to grow from $2.8 billion in 2014 to $7.2 billion in 2020.The card not present fraud presently calculates for over 70% of card fraud [2].It is crucial to note that banks usually undergo the losses for card present fraud and merchants endure the losses for card not present fraud. Thus, the main focus of merchants should always on to reduction of frauds in card not present which is the main aim of this paper. A remarkable amount of research has been conducted by both industry and educational institution to improvise the machine learning models for the fraud detection it's been always a challenge to improvise the accuracy of fraud detection. Machine learning models are one of the most important aspects for the identification of frauds.

The feature selection and feature construction are two important pre-processing techniques in the data mining. Both of the strategies not only allow dimensionality reduction however also offer class accuracy and improvement in efficiency. Feature construction offers with generation of new excessive level capabilities called constructed functions whereas characteristic selection selects the subset of relevant function from the original dataset. The constructed features have been not unusual practice in Credit card fraud detection from a chain of transaction facts to assemble a prototype to expect the accuracy of the fraud. However, the standard quality of the features is always vital to improvise the performance of the model [3].In data mining the feature construction has been the second major stream of analysis to include domain data and experience [4].Constructed features are outlined in terms of original features in order that no new inherently informed data is added in the

May-June 2020
ISSN: 0193-4120 Page No. 3876-3880

process of feature construction. It commonly aims to convert the original representation space to new one that can help to achieve improved accuracy and disclose hidden patterns.

In this paper we endorse an unsupervised approach for detecting fraudulent transactions. One of the effective class of neural networks is GAN(General Adversarial Network).It is made up of a system of two neural networks models which compete with each other making itself to analyse, capture and identify the variations in dataset. The data mining techniques are the conclusion of a prediction model supported a group of examples. This paper goal to endorse an efficient method that automatically detects fraud the usage of a method called Auto encoders.

The main contribution of this paper is to adopt a brand new model for sleuthing the fraud exploitation deep learning algorithmic model called auto encoders and the propose model are able to achieve the high performance rate when put next to alternative models. An auto encoder is a unsupervised learning that learns to map from the input to output with try of encoding and decoding phases. The mapping from the input to hidden layer is finished in encoder part, and mapping from the hidden layers to the output layer is finished by decoder part that helps in reconstructing the inputs. The hidden layer of auto encoder compromises of low dimensional and nonlinear representation of the input data. The issue with auto encoder is it constrains the quantity of information that can traverse a full network exerting a learned compression of input data[5].Auto encoder can transform the data into lower dimensions because of input vectors, the efficiency will be increased in unsupervised learning[6].

The paper is organised as follows as. Section 2 describes the proposed methodology of the model. Section 3 describes the results and discusses the methodology and section 4 describes the conclusions of the paper.

2. Proposed Methodology

By considering local and global behaviour of features fairly straightforward, the K means cluster [7] approach is used to construct effective features set.k-means clustering approach is very simple and runs quickly on large dataset. It offers the ability to decide effectiveness of arbitrary number of clusters. Let C_1, C_2, C_3, C_4 are clusters obtained from k-means algorithm. The ouput of k-means cluster n this paper, we constructed four clusters namely C_1= {VV_i, VV_{i+1}, VV_{i+2}…..}, C_2= {VV_i, VV_{i+1}, VV_{i+2}…..},, C_3= {VV_i, VV_{i+1}, V_{i+2}…..}, and C_4= {VV_i, VV_{i+1}, VV_{i+2}…..}. The proposed algorithm for deriving features is given below.

Algorithm for features extraction
Input:
Transaction clusters; C= { c_1,c_2.. c_n};
Output:
Final Feature set; FF= { F, F′ , F″, F‴ }
Begin:

1. Identify the amount of transaction record ci based on time stamp ;
2. Apply k-means cluster approach and form 4 clusters of features namely $f_1(x_i…x_n)$,$f_2(x_i…x_n)$,$f_3(x_i…x_n)$and $f_4(x_i…x_n)$ where x_i represents corresponding individual feature
3. Calculate the z-score normalization ofthe set F={f_1,f_2,f_3,f_4} and obtain new vector for each set F′ = {f_1′, f_2′, f_3′, f_4′}. Here f_1′ is z-score normalized values of f_1, f_2′ is z-score normalized values of f_2, f_3′ is z-score normalized values of f_3 and f_4′ is z-score normalized values of f_4.
4. Calculate the min-max normalization of the set F={f_1,f_2,f_3,f_4} and obtain new vector for each set F″ = { f_1″, f_2″, f_3″, f_4″}. Here f_1″ is min-max normalization normalized values of f_1, f_2″ is min-max normalization normalized values of f_2, f_3″ is z-score normalized values of f_3 and f_4″ is min-max normalized values of f_4.
5. Calculate Box-cox normalization of the set F = {f_1,f_2,f_3,f_4} and obtain new vector for each set F‴ = { f_1‴, f_2‴, f_3‴, f_4‴ }. Here f_1‴ is box-cox normalized values of f_1, f_2‴ is box-cox normalized values of f_2, f_3‴ is box-cox normalized values of f_3 and f_4‴ is min-max normalized values of f_4.
6. Form final feature set FF= { F, F′ , F″, F‴ }

Here FF indicates the real data and corresponding augmented data.

The Fig.1 and Fig.2 will gives, graphical description of auto-encoder. Auto-encoders are simple neural networks consisting of three layers namely input layer, hidden layer and output layer. Here the number of inputs at input layer is equal to number of outputs

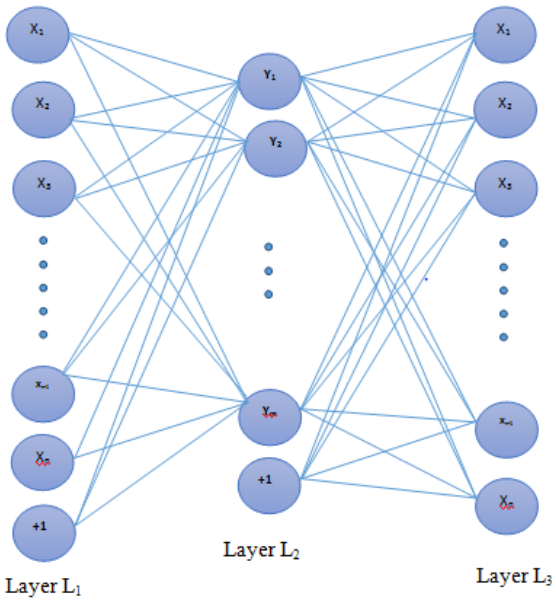

Figure 1: Auto-encoder visualization.

May-June 2020
ISSN: 0193-4120 Page No. 3876-3880

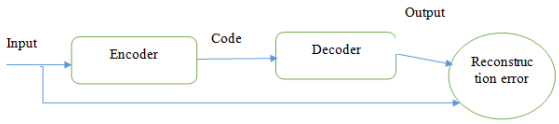

Figure 2: Auto-Encoder visual description

At the output layer. The dimensionality of input F is m space, new form of feature FF has n dimension space. The three layered neural network auto-encoder consider both F and FF which has same.This strategy uses back propagation algorithm for training.

$FF_{w,b}(x) = g(f(x)) \approx F(x)$ (1)

$E(w,b;x,y) = \frac{1}{2}\left\|FF_{w,b} - y\right\|^2$ (2)

Here FF is final feature vector and E is reconstruction error.

As shown in Fig.1, the input feature set values forwarded in the forward direction ie. Second layer to third layer (Decoder (H)) after calculating error E by adjusting feature values in FF in the encoder and get the output at output layer. In hidden layer we restrict the number of hidden units less the input original nodes, and then we can get a compressed representation of input feature vector. For dimension reduction purpose there are many methods like principle component analysis (PCA) which gives the most variability of data. In dimensional reduction, discarding some features may leads to loss of information. Here, getting important features from original features is most important task.

In our experimental setup, we use four auto encoders for extracting optimal features which gives more accuracy. For encoder, we will give real data i.e.F, for second encoder F′, for third encoder F″ and fourth encoder F‴. From these four encoders and using of PCA, we get most optimal feature set which will identify the transaction is genuine or false. After getting these optimal features, use these features as input for GAN.

Generative Adversarial Network (GAN)

In GAN there are two feed-forward neural networks, first one is Generator G and second one is Discriminator D where both are competitor for each other and usually a deep neural network [8].

In this, GAN there are layers where one layer output is input for immediately next layer. The strength of features will depend on number of layers and layer size [9]. Obviously first layer takes input features and last layer gives optimal features consists of highest abstraction. The high level features are derived from low level features.

The basic idea of GAN[10] is refine generative model, and discriminative model can separate real ones from generative examples. The generator takes noise z and using probability distribution, it generates artificial examples. On the other hand discriminate can differentiate real data from artificial examples. The overall abstraction of GAN is, generative model can create more and more instances over the time and discriminator improves its capability of distinguishing real instance from artificial instances. Minimizing its prediction error by training is aim of discriminator and maximizing the prediction error by the discriminator aim of generator. This computation is represented in mathematical way as follows.

$\min\max(E_{x\sim pD}[\log D(x)] + E_{z\sim pz}[\log(1 - D(G(z)))$ (3)

Where pD is the data distribution, pz is prior distribution of G.

The goal of generator is keep minimum difference in between real and generated data and goal of discriminator is maximizes the probability between real and generated ones. One of the most critical issues to GAN training is stability i.e. balancing between its layers. Sometimes discriminator gets very quickly show better performance and generator cannot match speed of discriminator. In case more unbalancing, the components will get fails then GAN also completely fail. The Fig.3 clearly describes the proposed framework.

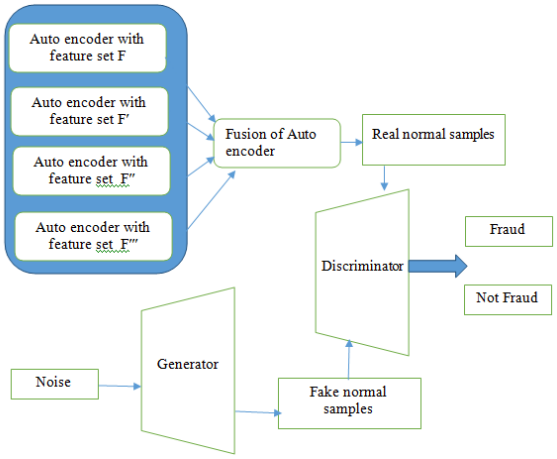

Figure 3: Framework of proposed method.

3. Results and Discussion

The banks are unwilling to make credit card data as public hence it is very difficult to obtain credit card fraud dataset. In this, we considered only publicly available dataset i.e credit card dataset which is consist of 284807 card transactions. In this dataset features are labelled with V1 to V28, which are result of PCA on original features except first feature i.e. Time which is in sec and last two features i.e. amount which is total amount that transfer and class will takes 1 for fraud and 0 for non-fraud. As part of pre-processing, we eliminated duplicates and rescale all features in the interval of [0,1]. After pre-processing, the dataset consists of 446 fraudulent out of 283726. We divide the dataset into two parts as training and testing with ratio of 80% and 20% respectively. Out of total dataset 80% of the data is used for training and calculated fraud probability of each testing record.

May-June 2020
ISSN: 0193-4120 Page No. 3876-3880

By using auto encoders' fusion, we extracted effective features and trained dataset with GAN. In total dataset 20% of the dataset considered as test dataset. Weare calculate the precision for test data with different top percentage like top 5%, 10%, 15%, , 20% and 25%. One of the superior performance indicator of accuracy is precision in an unbalanced data. We repeated 10 tails and calculated average precision and plotted in Fig.4.

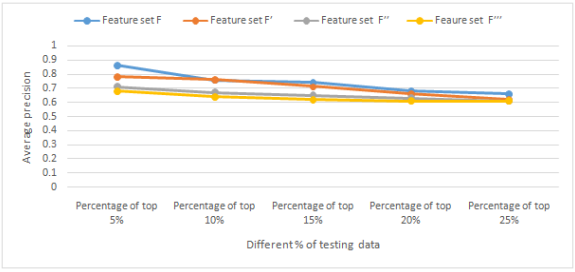

Figure 4: Average precision rate for different feature sets.

For GAN training, we considered individual feature sets namely Feature set F which is original dataset, z-score normalized features set (F′), min-max normalized feature set (F″) and Box-cox normalized feature set (F‴). The original dataset shown high precision rate when compare with normalized feature set.

For increasing performance, we combined original feature set with normalized feature sets. For each feature set, we consider one auto encoder and done fusion of the result of individual auto encoders. By fusion of auto encoders and PCA, the most optimal feature set is generated and these feature set is considered as input for GAN training. In GAN, generator generates different artificial instances by sing probability distribution and discriminator identify the transaction is fault or not. The corresponding model, we calculated precision value and plotted in Fig.5.

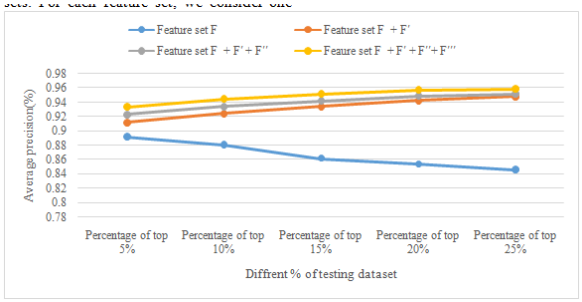

Figure 5: Average precision rate for fusion feature sets

From the Fig.5, the fusion of auto encoder's responses will give new feature sets. These
feature sets given good results in finding the fraud detection.

The proposed AE fusion +GAN method is compared with some state-of-art methods namely Development and Deployment Technique (DDT), k-NN [7], and Deep learning model on terms of popular fraud detection measurement factors i.e. sensitivity, specificity and accuracy. The Fig.6, Fig.7 and Fig.8 shows comparison graphs of proposed and existing methods in terms of sensitivity, specificity and accuracy respectively.

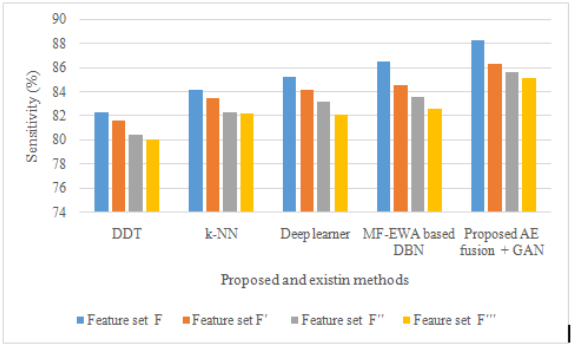

Figure 6: comparison graph of proposed method with existing methods with respect to sensitivity.

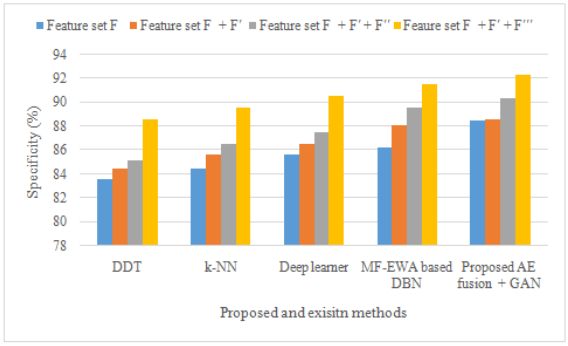

Figure 7: comparison graph of proposed method with existing methods with respect to specificity.

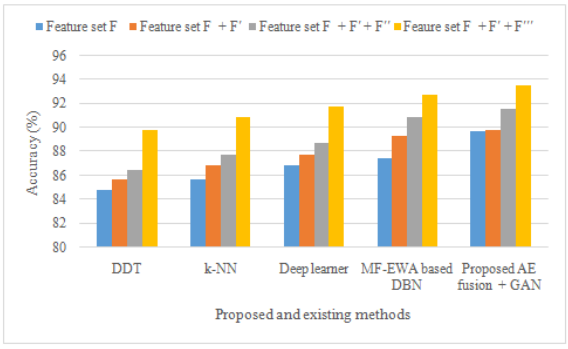

Figure 8: comparison graph of proposed method with existing methods with respect to accuracy.

Forma the graphs it is clearly state that the proposed AE fusion and GAN method shown more efficacy when compared with other existing methods.

Major contribution

1. The available features are clustered by using k-means algorithm

May-June 2020
ISSN: 0193-4120 Page No. 3876-3880

2. For every cluster, derived additional features values by using z-score, min-max and Box-cox normalization.
3. Original and additional features are given to individual auto encoders and then apply fusion on response of all encoders. Here used PCA for dimensionality reduction.
4. The optimal feature set is given as input for GAN for accurate classification of fraud or not.

4. Conclusions

The proposed model is based on fusion of auto encoders and GAN to detect fraud detection of credit card. Finding of optimal feature set is main thought in this paper. The original feature set is combined with normalized ones and derived most optimal features. Here need only normal transactions so our model can handle imbalance also. The experiments are conducted with different combination of feature sets. In all cases the proposed auto encoder fusion with GAN has shown high accuracy when compared to other state-of-art methods. Considered different ratios of test dataset and calculated average precision. This average precision gained high when fusion the feature sets. With respect to sensitivity, specificity, the propose model given good results with accuracy of 93.2.

References

[1] D. Robertson, The Nilson report. 2016. https://www.nilsonreport.com/upload/ content_promo/The_Nilson_Report_10-17-2016.

[2] https://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf- 2017

[3] Lima, Rafael & Pereira, Adriano, "Feature Selection Approaches to Fraud Detection in e-Payment Systems", Lecture Notes in Business Information Processing, 2017

[4] Yue Wu, YunjieXu , Jiaoyang Li, "Feature construction for fraudulent credit card cash-out detection, Elsevier,2019.

[5] Available:https://www.kaggle.com/mlg-ulb/creditcardfraud/data

[6] MohamadZamini; GholamaliMontazer, "Credit Card Fraud Detection using auto encoder based clustering", 2018 9th (IST),978-1-5386-8274-6/18/2018 IEEE,Pg:486-490

[7] A. Hartigan , M.A. Wong , "A k-means clustering algorithm", J. R. Stat. Soc. Ser. C 28 (1) , 1979 ,100–108

[8] LeCun, Y., Bengio, Y., Hinton, G., "Deep learning. Nature" 521 (7553), 436–444, 2015

[9] Bengio, Y., Courville, A., Vincent, P.," Representation learning: A review and new perspectives" IEEE transactions on PAML , 35 (8), 1798–1828, 2013

[10] Akhilesh Kumar Gangwar V Ravi , "WiP: Generative Adversarial Network for Oversampling Data in Credit Card Fraud Detection", ICISS 2019, pp 123-134