International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Credit Card Fraud Analysis using Robust Space Invariant Artificial Neural Networks (RSIANN)

S. Deepika, S.Senthil

Abstract*: One of the impact factor for any organizations or banks revenue and service quality is credit card fraud activities. Hence, need of efficient approach for detect early potential fraud and/or prevent them. In this paper, we considered pre-processing and used deep convolution neural network called as Space Invariant Artificial Neural Networks for classifying fraudsters. Available Credit card fraud dataset may not have sufficient information hence need pre-processing. The proposed approach has pre-processing phrase to make as robust. This approach used leverage layers and suitable tuning parameters for getting good classification accuracy. In neural network applications, choosing of tuning parameters and model selection has great role in solving the problems. We have done careful analysis and selected leverage layers and corresponding parameter values. The proposed architecture tested with all possible tuning parameters to evaluate the performance on pre-processed credit card fraud records. We found the proposed robust SIANN (RSIANN) is outperformed other state-of-art machine learning (ML) algorithms (Support vector machine (SVM), random forest (RF), Navie bayes and deep convolution neural network (DCNN) in terms of accuracy (85%). Thus, this model analyses the transaction and decide it fraud or not.

***Index Terms*: credit card fraud, CNN, pre-processing, machine learning.**

I. INTRODUCTION

Online transactions especially credit card contain a big portion of online transactions. These transactions have rapid growth in the digital economic system. A major problem in this area is fraud .In 2018 southeast countries surveyed, the fraud revenue loss rate averaged about 1.6% of annual ecommerce revenue. The loss was heaviest in Indonesia (3.2%), moderate in Thailand (1.9%), Vietnam (1.3%), and Malaysia (1.2%), and smallest in Singapore (1.0%) [2].Most of the financial organizations provides complex security solutions to the fraudsters that change their strategies over time. Optimizing the fraud is one of the featured solution in FMS. It always require constant balance between revenue maximization, fraud minimal loss and reduced operational cost .This paper propose the framework with convolution neural network (CNN) implementing with Space Invariant Artificial Neural Networks (SIANN) which makes the data images convert into samples with help of the kernel and preprocess them to the SIANN With appropriate machine learning technique like Bayesian algorithm [3],AIS(Artificial Immune system)[4-5], hidden Markov [5] and support vector machines [6] are used for the detection of frauds in different aspects in fraud detection system. RSIANN is based on image fraud identification system which has pre-processing phase which gathered all fraudulent transactions in one location and normal transaction in another place. It is used for detecting fraud with greater accuracy and automation.

A textual analysis of the data has obtained the accuracy of 67.3% with the measures of linguistic characteristics by Humpherys et al [8].S.Goel et.al [9] has performed sentiments analysis to obtain the positive and negative sentiments used in fraudulent. The unstructured data can be transformed into variables that will be quantities to the classification model. Logistic regression[11] is statistical classifier which is used as benchmark classifier in the system. Different types of NN(neural networks) have been proposed including MLP(multilayer perceptron)[12],GMDH(Group method,datahandling[13],PNN[14],,RBF[15],self-organizati onal maps[16] to optimize the problem of nonlinearity in the characteristics of the fraud detection problems.

This paper discussion as follows: Section 2 describes characteristics of data set. Sections 3 describe about proposed framework for analyzing credit card frauds. The section 4 and 5 gives the results and discussion and conclusions respectively.

II. DATASET CHARACTERISTICS

Many datasets are available for credit card fraud detection including fraud records and normal records. There should be more memory cells needed in case of many varieties of fraud types in dataset. The dataset can divide into two regions i. fraudulent ii. Normal records. All fraudulent records are formed in one sub space and remaining will be gathered in another place. The number of fraudulent and normal records is different in different datasets. This is the why banks or organizations use different protocols for providing security. Preprocessing of dataset is very useful for finding important fields and remove useless fields from fraud point of view. In order to address this issue, this paper has preprocessing phase.

III. STRUCTURE OF PROPOSED RSIANN MODEL

Recently convolution neural network (CNN) has lot focus for different applications and yielded optimal results. Another version of CNN is SIANN based on their shared-weights architecture and translation invariance characteristics.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author
S. Deepika*, Research scholar (Rg. No: R16PCS09), REVA University, Asst. Professor, Anurag group of Institutions (Autonomous), Hyderabad.
S.Senthil, Professor & Director- School of Computer Science and Applications, Reva University, Bangalure.

The basic input of CNN is 2D image. This paper considered artificial images which are describing the profile of customer as input. Totally 500 users profiles converted into 25000 images during period of 120 days. The basic CNN architecture is given Fig. 1.

.

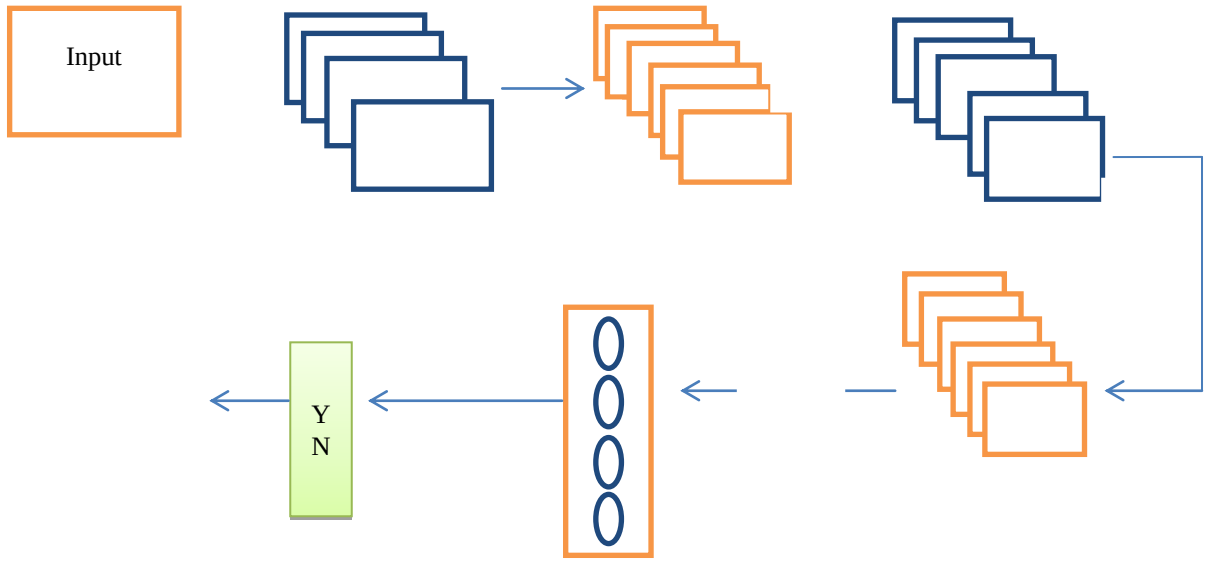

Fig. 1: Basic frame work of CNN.

This data is passed to proposed RSIANN. One of the main advantages of CNN is it considered direct 2D image as input. The proposed RSIANN consists of 5 layers as shown in Fig. 1. By using several adjustable kernels the input is convolved to generate feature map to form a first layer. The basic pooling size is 2x2. This process is repeated for remaining layers. After getting one dimensional layer feature, passed to final classifier to classify fraud or not. Generally softmax can used as final multiple classifiers. In major layers total feature map is divided into lots of local regions and convolved with basic kernels. After completion of this convolution process by activation functions, we will get final feature map. Now, the kk-th layer is convolution layer and m-th output in this layer can be denoted as:

$$Y_j^k = g(\sum_{i \in M_m} Y_i^{kk-1} * K_{im}^{kk} + b_m^{kk} \quad (1)$$

Wherein, M_m presents the local area, m –th kernel, K_{im}^{kk} is a restriction of convolutional kernel m , b_m^{kk} is basic bias, g (.) is the Sigmoid function.

The 2x2 area is used for subsampling layer, that is max of 4 sample points in area generate new weight value.

The residual error raster layer l_r can written as :

$$l_r = [l_{111}, l_{222}, l_{333}, l_{444} \ldots\ldots l_{jmn}]^T \quad (1)$$

The equation 2 indicates organization 1D- 2D and 2D to 1D feature vector in subsampling layers.

In max pooling, try to find maximum residual error using units of major layer. The error in layer S layer is q Δ . After updating the parameters, the error is forwarded to C layer, and it is expressed in Eqn. (3)

$$\Delta_t = upsampling(\Delta_t) \quad (3)$$

In convolution layer two tasks can be done. Fist one residual error and update the parameters. Generally gradient method is used update the parameters. As per forward propagation updated parameter ϵ_l in convolution layer is :

$$\frac{\partial y}{\partial x} = rot_{180}\ ((\sum Y_q\ ) * rot_{180}\ (\Delta l)) \quad (4)$$

Where rot_{180} indicates rotation of 180 ^{o} degree rotation of feature vector.

If subsampling layer is connected to convolution layer, the residual error spread p~ is:

$$\Delta_t = (\sum_{t \in C} \Delta_p * rot_{180}\ (\theta_t))\ Y_p \quad (5)$$

after all parameters are updated, then we considered as one iteration. This process is conceded for all training samples and testing samples until we meet required training requirements. After completion of this process, data is given to multiple classifiers to classify a particular transaction is fraudulent transaction or not as shown in Fig. 2.

Subsequently configure the infrastructure and initialize the parameters, for input the training set, training labels testing set and testing labels. After comparing output to testing labels, we can get final classification accuracy.

This paper recommended different hyper parameters for CNN training. Here, this paper tested many epochs using entropy loss function [15] which is given in Eqn. 6 that we try to minimize.

$$\nabla = \frac{1}{2}\sum_i (r_i - q_i)^2 \quad (6)$$

Where r_i is the output of the i^{th} output layer and q_i is the i^{th} value of the predicted output. The final framework is summarized in Table 1.

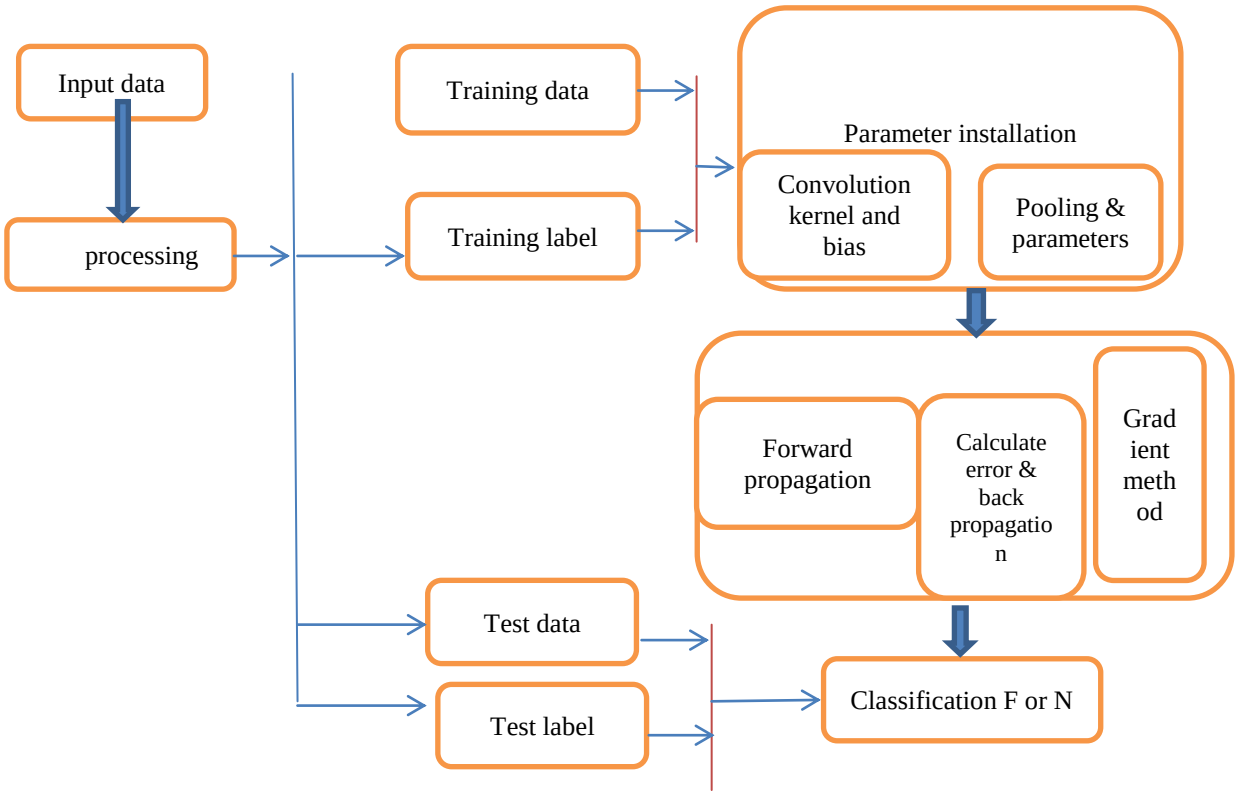

Fig. 2: Space Invariant Artificial Neural Networks (SIANN) for credit card fraud detection.

Table 1: Considered Parameters of frame work.

Factor	Used Value
Epoch	52
LR	0.1
Momentum	0.7
WD	0.049
MBS	300

*LR- Learning rate, WD- weight decay, MBS- Mini batch size.

Actually every input artificial image is has different size. Consequently, in orders to feed them into proposed framework model, all artificially images are resized to 28x28 for 2 classes' i.e. (Fraudulent, Normal). The details of proposed model are given in Table 2.

Table 2: Our proposed RSIANN Framework.

.

Layer	Layer specification
1	CL 1
2	CL 2 +ReLU
3	Max pooling
4	CL 3 +ReLU
5	Max pooling
6	CL 4 +ReLU
7	Max pooling
8	Fully connected layer(FCL)
9	Soft max

*CL-Convolution layer

For completing training process as early as possible used rectified linear unit (RELU) over other methods (Sigmoid, Tanh-function). Max pooling used to preserve most essential feature while disposal irrelevant details [20] and this is very important in analyzing our artificial images. The last layer of our proposed model is FCL ending with soft max function with 2 predicted units for binary classification i.e. fraud or not.

IV. EXPERIMENTAL RESULTS

To test the efficacy of the proposed model, we have calculated the accuracy during different epochs. Each epoch is considered parameter updating with relu, maxpooling and gradient descent. The experimental results given in Fig. 3 shows that maximum accuracy is gained in 50 epoch, means network converged at 50th epoch.

Fig. 3: Accuracy of our proposed model using different epochs.

Epoch	Accuracy
1	0.08
5	0.10
15	0.68
20	0.70
25	0.74
35	0.74
40	0.76
45	0.80
48	0.80
50	0.85
52	0.85

Our proposed method is explored four old-style ML algorithms: SVM, RF, naive bayes , linear regression and Deep convolution neural network (DCNN). In SVM implementation, we used RBF kernel function, for avoiding, over fitting, used k-fold cross validation approach. More details, we used 45 persons profiles artificial images used for training and remaining used as testing. The final results are given in Table 3. This table is clearly showing the proposed RSIANN high accuracy when compared with state-of-art methods.

Table 3: Comparison of proposed and existing models in terms of accuracy.

.

Model	Accuracy
SVM	0.77
RF	0.72
Naive bayes	0.70
Linear regression	0.71
DCNN	0.82
Proposed RSIANN	0.85

Identifying the fraudulent transaction on time will avoid huge damage of economic status of organization or bank. For experiment purpose, for getting high speed computations used GPU for evaluating performance of proposed model. In general CPU gives low results while handling huge datasets. The parallel processing is strength of GPU is when compared to CPU.

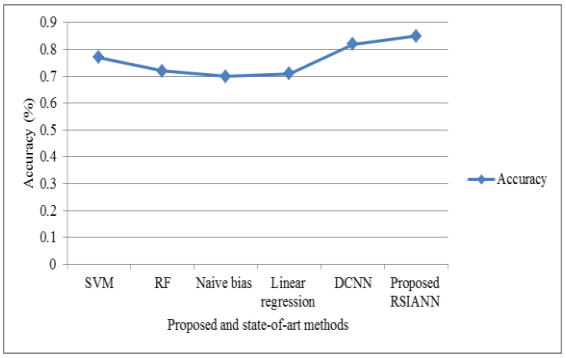

Fig.4: Comparison of proposed RSAINN with state-of-art approaches.

The Fig.4 clearly shows the efficacy of proposed model over state-of-art methods.

The main contribution of this paper

1. The proposed model has pre-processing phase which gathered all fraudulent transactions in one location and normal transaction in another place. This one make proposed model as robust.
2. By using of deep neural network, there is chance of optimal weights should be derived for different hyper parameters.
3. Considering of customer profiles as artificial images is strong point of this paper. This consideration makes a possibility to use of deep neural networks. ‘
4. Initializing model and training module used optimized hyper parameters to increase the accuracy.

V. CONCLUSION

In this paper we have examined performance of RSIANN against the old-style ML algorithms to classify the fraudulent transaction. The results show that the proposed RSIAN outperformed over the old-style machine learning algorithms i.e. SVM, RF, Naive bayes, linear regression and DCNN with an accuracy 85%. This work is good attempt to analyze the credit card frauds in different organizations and banks. May be this method does not contain benchmark CNN model, in future we can use pre-trained CNN and optimized activation functions with different kernels.

REFERENCES

1. NunoCarneiro, GonçaloFigueira, MiguelCosta, A data mining based system for credit-card fraud detection in e-tail ,2017(0167-9236)
2. https://www.cybersource.com/en-APAC/products/fraud_management
3. Suvasini Panigrahia, Amlan Kundua, Majumdarb, Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning Information Fusion,Volume 10, Issue 4, October 2009, Pages 354-363
4. M.Gadi,X.Wang, A Credit card fraud detection with artificial immune system (2008),119-131
5. A. Brabazon, J. Cahill, P. Keenan, D. Walsh, Identifying online credit card fraud using artificial immune systems, 2010
6. S. Bhattacharyya, S. Jha, K. Tharakunnel, J.C. Westland, Data mining for credit card fraud: a comparative study,Decis.Support.Syst.50(3)(2011)602–613.
7. A. Srivastava, A. Kundu, S. Sural, S. Member, Credit card fraud detection using hidden Markov model, IEEE Trans. Dependable Secure Comput. 5 (1) (2008)
8. S.L. Humpherys, K.C. Moffitt, M.B. Burns, J.K. Burgoon, W.F. Felix, Identification of fraudulent financial statements using linguistic credibility analysis, Decis. Support Syst. 50 (2011) 585–594. doi:10.1016/j.dss.2010.08.009.
9. S. Goel, O. Uzuner, Do sentiments matter in fraud detection? Estimating semantic orientation of annual reports, Intell. Syst. Accounting, Financ. (2016). doi:10.1002/isaf.1392
10. E.F. Zainudin, H.A. Hashim, Detecting fraudulent financial reporting using financial ratio, J. Financ. Report. Account. 14 (2016) 266–278. doi:10.1108/JFRA-05-20150053.
11. W.S. Albrecht, C. Albrecht, C.C. Albrecht, Current trends in fraud and its detection, Inf. Secur. J. A Glob. Perspect. 17 (2008) 2–12. doi:10.1080/19393550801934331.
12. E. Kirkos, C. Spathis, Y. Manolopoulos, Data mining techniques for the detection of fraudulent financial statements (2007) 995–1003. doi:10.1016/j.eswa.2006.02.016.
13. P. Ravisankar, V. Ravi, G. Raghava Rao, I. Bose, Detection of financial statement fraud and feature selection using data mining techniques, Decis. Support Syst. 50 (2011) 491–500. doi:10.1016/j.dss.2010.11.006.
14. C. Gaganis, Classification techniques for the identification of falsified financial statements: a comparative analysis, Intell. Syst. Accounting, Financ. Manag. 16 (2009) 207–229. doi:10.1002/isaf.303.
15. Y.J. Kim, B. Baik, S. Cho, Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning, Expert Syst. Appl. 62 (2016) 32–43. doi:10.1016/j.eswa.2016.06.016.
16. P.F. Pai, M.F. Hsu, M.C. Wang, A support vector machine-based model for detecting top management fraud, Knowledge-Based Syst. 24 (2011) 314–321. doi:10.1016/j.knosys.2010.10.003
17. S.Y. Huang, R.H. Tsaih, F. Yu, Topol S.Y. Huang, R.H. Tsaih, F. Yu, Topological pattern discovery and feature extraction for fraudulent financial reporting, (2014) 4360–4372.

AUTHORS PROFILE

Deepika.S , Assistant Professor, CSE. Completed B.Tech and M.Tech from St. Mary’s Group Of Institutions, JNTUH in the field of Computer Science & Engineering. Pursuing my Ph.D from REVA University,Bengaluru.

Areas of interest are Data mining, Machine Learning, Mobile computing. Published 4 research papers in various reputed National Journals.

Dr. S. Senthil, Professor and Director, School of Computer Application was awarded with Doctoral Degree by Bharathiar University for his dissertation on Lossless Preprocessing Algorithms for effective text compression. He has completed his B.Sc (Applied Sciences – Computer Technology) from P.S.G College of Technology, MCA from Bharathidasan University, M.Phil in Computer Science from Manonmaniam Sundaranar University and Ph.D in Computer Science from Bharathiar University. He has been qualified in State Eligibility Test conducted by Bharathiar University. At present he is guiding 8 Ph.D scholars in the fields of Data mining and Networks. He has 20 years of experience in teaching. His areas of interest include RDBMS, Data Mining, Data Compression, Computer Networks and Data Structures. He has published 30 research papers in various reputed National and International Journals. He has presented a paper entitled "Lossless Preprocessing Algorithms for better Compression" in an IEEE International Conference at Zhangjiajie, China. He was also the recipient of the best paper awards, at an International Conference on “Wisdom Based Computing” at Thiruvananthapuram and at a National Conference on “Transforming India through Digital Innovations” at Guru Shree Shantivijai Jain College for Women, Chennai.