Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 26 (2023), No. 8, pp. 1837–1854
DOI : 10.47974/JIM-1761

Utilizing mathematical concepts of heat map for an intelligent and secure approach to efficiently detect credit card fraud

Amit Gupta *
M. C. Lohani †
Mahesh Manchanda §
Department of Computer Science and Engineering
Graphic Era Hill University
Dehradun
Uttarakhand
India

Abstract

In the current scenario of digital world, every year the financial institutions have to face billions of dollars losses due to fraudulent transactions. Out of different categories of financial frauds credit card transaction fraud is the most common. To reduce the effect of these fraud transactions there is a need for a well-designed and secured fraud detection system with a state of art fraud detection model. Our work's primary contribution is the creation of a fraud detection system that makes use of some mathematical usage of creating heat maps which is then enhanced with the use of a deep learning architecture and a sophisticated feature engineering method based on HCNN- Heat Map Convolutional Neural Network. HCNN is a model which create the heat maps for the imbalance data set without replicating the minor class records and without discarding major class records. The experimental findings show that our suggested technique is a practical and successful mechanism for detecting credit card fraud. The main objective of our model is to develop such a technique that can be used to detect and correctly classify more numbers of fraud transactions thus, our suggested technique, may detect considerably more fraudulent transactions than the benchmark methods with the accuracy of 91.7%.

Subject Classification: *68T07.*

Keywords: *Machine learning, Credit card fraud, Heat map, Financial fraud, Mathematical foundations for heat maps.*

* *E-mail:* **amitgupta7920@gmail.com (Corrsponding Author)**
† *E-mail:* **getmlohani@gmail.com**
§ *E-mail:* **manchandamahesh@gmail.com**

1. Introduction

Fraudulent actions have been on the rise in a variety of businesses around the world, particularly in the field of financial sector. Financial fraud is something when someone harms your financial health. The method that is applied to give you financial loss can be deceptive, misleading or any other illegal practices. For any type of financial fraud, it is very essential to detect the financial fraud in early stages so that loss can be minimized. Along with the detection of any financial fraud it is also advisable to report the fraud to required and appropriate agencies. We can observe various types of Financial Frauds such as Identity Theft, Investment Fraud, Mortgage and Lending Frauds, Mass Marketing Frauds and Credit Card Frauds. By understanding the types of fraud, implementing security measures, and promoting awareness, individuals, businesses, and financial institutions can collectively work to mitigate the risks associated with credit card fraud and create a safer financial environment for everyone. Credit card fraud [11] is the most serious and popular in financial institutions, and it must be prevented or detected as quickly as possible. Fraud detection approaches must investigate and strictly handle credit card fraud [15] in order to drastically limit the effects. Credit card fraud detection relies heavily on mathematical and statistical techniques to analyse transaction data, identify anomalies, and protect against fraudulent activities. For the detection and prevention of fraud transactions the usage of various Machine Learning [10] and Artificial Intelligence approaches gives remarkable good results. Using these mathematically based machine learning approaches previous transactions are used to train fraud detection systems in order to predict future fraud transactions. The major issue in developing an efficient model for the detection of fraud transaction is the datasets, as the available datasets are highly imbalanced in nature [16]. The number of fraudulent cases is substantially lower than in normal circumstances when it comes to fraud detection. In a skewed dataset, one class of dataset contains a very large number of instances, while the other class has a very small number of them. Machine learning algorithms, on the other hand, operate best when there is a balanced distribution of classes. In the past years different techniques are used to address the issue of skewed datasets [18]. The techniques which are used to generate balanced datasets are Synthetic Minority Oversampling Technique (SMOTE) or Adaptive Synthetic (ADASYN). The model proposed in this study tries to overcome the challenges of these techniques and able to propose new method to convert the imbalanced dataset to balanced dataset[21].

The work in this paper has been categorized into the following sections: **Related Work / Literature Survey** which specifies work done in the detection and prevention of financial frauds using various techniques specified by Machine Learning. Next section is **Background Work** that gives the brief description of Machine Learning and its working. It also describes the Data Preprocessing, Imbalanced Datasets and tradition methods to deal with highly imbalanced datasets. Next section is **Contribution** which specifies the description of Heatmaps and Convolutional Neural Networks, these two techniques are used in our proposed model. Next section of the paper is **Proposed Model** which describe our model and algorithm HCNN for the detection of fraudulent transactions in highly imbalanced datasets. Then, the most important section of the paper, **Result and Discussion** that contains the results, graphs, etc. of our proposed algorithm. Lastly it specifies **Conclusion and Future Scope** which specifies the future scope of this study.

2. Related Work

[1] In 2011 Joachim D. Pleil et. Al. utilized the "Heat maps" as a visualization tool for the visualization of complexity of genomic and proteomic data of system biology. Heat map is the matrix of different colors where the dependent variable has different intensity. Particular hypotheses can be explored at either X-axis or Y-axis because of the flexibility of the heat maps. The different colors of the third quantitative dimension help to rapid overview of data. So the authors use this map to measure the environmental exposure and the biomarkers like breath, urine and blood etc.

[2] in 2013 Leland Wilkinsona et. al. describes the history of cluster heat maps. They stated that heat maps are the data matrix in which hierarchical cluster structure of rows and columns are displayed. This data matrix is composed of rectangular tiles of different color shades which represents the dependent variable's value. Actually, heat maps are agglutination of various visualization graphics developed by statisticians over more than a century. The authors claim that heat maps were first published in the late 19th century and then in the 20th century, literature surveys are published about this. After this heat map is widely used for bioinformatics.

[3] In 2014 Shilin Zhao et. al. developed a package "heatmap3" in R which has some advanced features. Actually, the authors improve the Heat map function of R in terms of customization so that it can generate the advance heat maps and dendrograms. This new heatmap3 allows to create customized state of art heat maps and dendrograms as well as it includes a wide range of color combinations, legends and side annotations, latest labelling features etc. this can also measure the distance between two samples by using agglomeration method for clustering.

[4] In this paper the authors use the heat map to visualize the Geographical Information System. They apply the heat map on the accidental data of Olomouc city, Czech Republic. The data were visualized many times by changing the different parameters like color, kernel size, radius and transparency. In this paper the author experiments with various different exploratory methods for evaluation and analysis of heat maps. The authors find many strengths and weaknesses of the Heat maps.

[5] in 2014 Hang Chu et. al. recognized human group activities by a new Heat-map-based (HMB) algorithm. This algo works in two phases, in the first phase the path followed by the human is modelled and in the second phase the heat map is generated by the thermal diffusion process for showing the group activities. At the end the Surface fitting method is also used for the identification of the human group activities. The temporal motion information is kept by the heat map and the surface fitting find out the characteristics of the heat map for the identification of human activity.

[6] N. Shcheglova et. al. developed a mathematical model for dynamics of fire propagation based on the satellite images and then calculated the damage caused by the fire. The author developed a new algorithm, Navier-Stokes equations for the indication of state timberland in the region. Then they compiled a schematic Heat map and its three-dimensional prototype for the two areas. This 3D model helps for making the understanding of fire in these particular regions and as well as it helps for the evaluation of the risk of the phenomenon and the extent of the fire.

3. Background Work

3.1 *Machine Learning*

Machine Learning is a branch of Artificial Intelligence and Computer Science that mainly focus on the effective use of datasets and different algorithms in the way as human learns various things [22]. Now-a-days machine learning is an essential part of Data Science which itself is

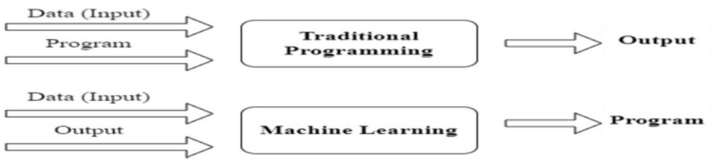

Figure 1.0

Machine learning and Tradition learning

growing drastically. Simply, we can say that machine learning is an important application of Artificial Intelligence that facilitates the development of such systems which has ability to learn themselves [24]. It mainly provides mechanism for the development of such computer programs which can use data for learning. The main objective of any machine learning techniques is to provides an ability to any computer system to learn automatically without human interference. Machine Learning is different from traditional programming in the following way which is shown in Figure 1.0

3.2 *Machine Learning Methods*

Machine Learning algorithms can be classified as following:

3.2.1 Supervised Machine Learning Algorithms:

It can be used to apply the learning from past values to some new values or data with the use of some labelled examples for the predictions of future events [19].

3.2.2 Unsupervised Machine Learning Algorithms:

These methods can be applied in such situations when the data used for training is not classified or not labelled. It mainly tries to develop a function that can be used to describe the hidden structure from unlabelled data [20]

3.2.3 Semi – Supervised Machine Learning Algorithms

It is basically the usage of both labelled and unlabelled data for the purpose of training of data. It mainly uses considerably small amount of labelled data and large amount of unlabelled data.

3.2.4 Reinforcement Machine Learning Algorithms

This is the advanced form of machine learning algorithms which provides the capability to interact with its environment. In this the model in not trained on any sample data rather it follows the concept of trial, error or rewards for learning.

The function of any machine learning system can be "Descriptive" in which the data is mainly used to specify what had happened, "Predictive" which is used to predict some future values or events after analyzing the data, "Prescriptive" is the machine learning model which is mainly used to give suggestion about any action to take place.

3.3 *Data Pre-processing*

As the datasets that is collected from wide variety of data sources and due to the large amount of data and heterogeneity of data sources, data is not uniform. Due to the fact that the model accuracy and predictions is directly dependent on the quality of data that is high quality data is the essential part for prediction, thus data pre-processing becomes important and mandatory step in data analytics or model building using machine learning [23]

Main factors that lead to quality of Data:

1. Accuracy: Erroneous data can lead to degrade in the results. It includes human / computer typing errors, missing values, duplication of training examples
2. Completeness: Data should be complete in each manner. It might be incomplete due to following: Unavailability of Data, Deleting of inconsistent data
3. Consistency: Data should always be inconsistent

3.4 *Imbalanced Datasets*

Imbalanced Datasets or imbalanced class distribution is the scenario in data analysis [16] in which the number of observations of one class is very low or less in comparison of other class. This results in the decrease in the efficiency of any predictive model. This problem is not only faced with binary class data but also in multiclass data. The efficiency due to imbalanced datasets may be upto 95% which seems to be very good but the problem is that most of the records belong to majority class but if the model is executed with minority class or combination of both, then efficiency is not very good. Class imbalance appears in many domains like – Fraud Detection [17], Spam Filtering, Disease Screening etc. The accuracy generated for imbalanced datasets may be misleading in following manner:

1. As for non-fraud transactions you can have 100% accuracy
2. For transaction which are fraudulent the accuracy can be 0%
3. Overall accuracy can be very high not because your model is good but because of the larger number of non-fraudulent observations.

3.5 *Traditional Methods that can be used with Imbalanced Datasets*

3.5.1 Choose Proper Evaluation Matric

The accuracy of any model or classifier is defined as total number of correct predictions divided by total number of predictions. For imbalanced datasets F1 score is more appropriate metric. It can be defined as harmonic mean of precision and recall.

$$F1 = 2*((precision * recall)/(precision + recall))$$

3.5.2 Resampling (Oversampling and Undersampling)

This method or technique is used to either Upsample or Downsample the minority or majority class. Oversampling is used to oversample the minority class by increasing or replicating the number of records of the minority class, whereas undersampling is done by decreasing the records of majority class. Using these techniques both the classes have same number of records and the dataset becomes balanced which is shown in Figure 2.0

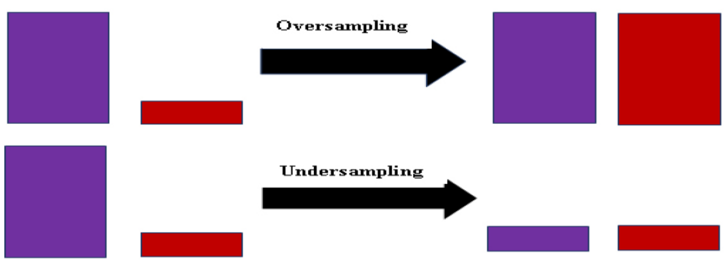

Figure 2.0

Data sampling Techniques

3.5.3 Synthetic Minority Oversampling Technique (SMOTE):

Just adding duplicate records to the dataset does not add any new information or record to the dataset, thus, the performance of the model is not enhanced too much. SMOTE works in the following manner that it observes into various minority class instance and then use K-nearest neighbor to select a random nearest neighbor, and a synthetic instance is created randomly in feature space.

3.5.4 Adaptive Synthetic Sampling (ADASYN)

It is an advance version of SMOTE which is used to generate synthetic samples that are inversely proportional to the density of records of minority class. It is designed in such a manner so that the synthetic records in region of future space where the density of minority class is low, less or none as compared to the high-density regions.

4. Contribution

Using Machine Learning or Deep Learning techniques in highly imbalanced datasets does not ensure that the results obtained are efficient. Actually, imbalanced datasets tend to provide biased results due to presence of more records of any one class. To overcome this problem various balancing techniques are used to make dataset balanced. All these traditional data balancing techniques either replicate the minority class records or skip majority class records. In both the cases the results are not appropriate due to absence of uniqueness of the data. In our proposed model we try to overcome this problem, our model mainly focuses on balancing the datasets without replicating the minority class or without skipping any record from the majority class. In our model we first generate the heatmap for group of records (randomly). Each heatmap is different from other and thus there is no replication of the records. Once the heatmaps are generated, these heatmaps images are than passed to CNN for the correct and efficient prediction of fraud and non-fraud transactions.

4.1 *Heatmaps*

Heatmaps (in simpler way) are just the tabulation tables with different color coding (mainly Red, Yellow, Green but any other color combinations can also be used) overlaid within each cell in different high or low shaded patterns. These shading are mainly used to visualize the row column association within the crosstab data. Heatmap is a graphical representation of data where various values are depicted by different shades of colors. The benefit of heat maps is that the complex data can be made easily understandable, and it can be visualized easily. The concept of heat maps originated in 19th Century when manual grey scale shading was used to show data patterns in matrix and tables. The term heatmap was firstly trademarked in early 1990s when software designer Cormor Kinney created a simple tool to graphically display real time financial market information. Heatmaps, now-a-days, are used by data analysts as it gives a more comprehensive way to show the association between variables or attributes in the datasets. Heat maps can be used for various kind of data analysis such as in comparing the various data items with one another, specifying the association and effect of any one attribute on the other. In some cases, heat maps can be used for the detection of human activities. The HMB algorithm was proposed by the researchers to detect the human activity, they use two important concepts of heatmaps, namely converting human as a series of "heat sources" and then applying thermal diffusion process for the creation of heatmaps. Following equation were used for the creation and analysis of heat map.

The authors assumes that if we have x total trajectories in any group than the total thermal energy EN_i can be calculated as [5]

$$EN_i = \sum_x E_{i,x} . e^{-n_t(t_{cur} - t_{id,x})} \tag{1}$$

where $e^{-nt(t_{cur} - t_{id,x})}$ is the time decay term,

n_t is the temporal decay coefficient,

$t_{id,x}$ is the frame no when x-th trajectory leaves patch i.

$E_{i,x}$ is the accumulated thermal energy which can be calculate using following equation 2

$$E_{i,x} = \int_0^{t_{id,x} - t_{is,x}} C . e^{-x_t t} \, dt = \frac{C}{n_t} \left(1 - e^{(-n_t \ (t_{id,x} - t_{id,x})}\right) \tag{2}$$

where $t_{is,x}$ and $t_{id,x}$ are the number of frame when x-th trajectory enter and leave the patch i.

Now the diffusion can be calculated using equation 3.

$$H_i = \frac{\sum_{l=1}^{N} E_l \ . e^{-k_p d \ (i,l)}}{N} \tag{3}$$

where E_l is the thermal energy of any heat souce for patch l,

N represents total count of heat sources

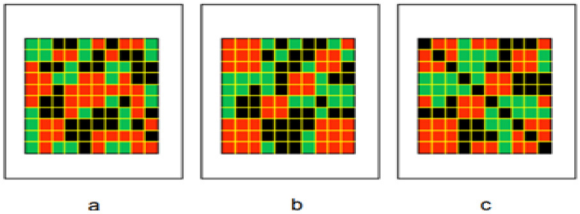

Figure 3.0

Three tri-colored heat maps with the same proportion of red (40%), green (28%) and black (32%) tiles.

Kp spatial diffusion cofficient and
d(i, l) distance between patches

From the past decades to present various kinds of heatmaps came into existence, some of them are: Shading Matrices, Permuting Matrices, Seriation, The Guttman Scalogram, Hierarchical Clustering, Two-way Clustering etc. one of them is illustrated in Figure 3.0.

For any two-colour heat map, it can be represented as

$$H \subset \Re^2$$

Let G represent a board or grid of square with H partitions:

1. Define G any polygon with N number of sides and diameter(g) = G where diameter() = maximum of the length of the N sides of G
2. $G = \{G \subseteq H \mid \cup_g = H \text{ and } g_i \cap \ g_j = \Psi \dashv \text{ for } \xi \text{ i, j } \in Z^+ \text{ and } i \neq j\}$
3. $\text{diameter}(g_i)=\text{diameter}(g_j)\ \forall\ i,j \in Z$

   P can be defined to be a rectangle
4. Define a rectangle, $R \subset G$, to consists of a set of continuous features g, whose union is similar to the polygon G

   The rectangle R, traverses the length of H, beginning from top left corner of H. Define an indication function χ (N)
5. A single score for R across H can be calculated as $\xi\ m= \sum_{(G\subset R)} \chi\ (N)$
6. The lacunarity of H, $\Gamma(K,J)$ may be defined as –

$$\Gamma(N,J) = A_2\ (\xi\ )/\ (A_1\ (\xi\ ))^2$$

   where $M_2 = (\ 1/\ T)\ \sum^{T}_{(A=1)}\ \xi_{\ a}^{\ 2}\ \Psi$ i.e A_1 and A_2 represents the first and second uncentered movements for the scores $\xi_{\ 1}, \xi_2, \xi_3 \ldots\ldots \xi_T$

4.2 *Convolutional Neural Network*

After Machine Learning, Deep Learning[12] is emerged as a most popular and effective technique that is used for analysing big data[14] and complex data. Deep learning uses complex algorithms and artificial neural networks that can be used to train machine which can learn from their past experiences. They are generally used to recognize images as they are been classified by human beings. In deep learning, CNN, which is a type of artificial neural network, can be used for any complex image classification and recognition.

4.2.1 Brain's Architecture Inspired CNN

A simple neural network has the following main layers: Input Layer, Hidden Layer and Output Layer. It is basically inspired by the architecture of the human brain, as neurons are responsible for the processing and transmission of information within the whole human body, in the similar manner the artificial neurons, commonly known as Nodes in CNN, are responsible for taking input – processing them and delivering the results as output. CNN contains many hidden layers, which are mainly responsible for feature extraction from an image after doing some calculations. These layers include Convolution, Pooling, Rectified Linear Units and Fully Connected Layers. Convolution is the very first layer that is responsible for feature extraction from an input image and a fully connected layer is responsible for classification of an object or image. It is always beneficial to represent images and other complex raw data as "Tensors", which are basically higher order matrices. Simply a image can be represented in the form of vector as $v \varepsilon R^P$ which is a column vector with P elements. Matrix for the same can be given as $V \mathcal{E} R^{(M X N)}$ with M rows and N columns.

Now, $V \mathcal{E} R^{(M X N X P)}$ is an 3rd order tensor that contains M,N,P elements and each of them can be indexed by (i, j, d) with $0 \leq i < M$, $0 \leq j < N$ and $0 \leq d < P$

Tensors are very important in CNN as input, intermediate representation and parameter in CNN are all tensors.

4.2.2 The Architecture of CNN

A CNN usually takes a 3rd order tensor as its input image with M rows and N columns. The input is then undergoing a sequential series of processing in which one processing step is termed as "Layer". The abstract description of CNN structure is:

$$v^1 \rightarrow \omega^1 \rightarrow v^2 \rightarrow \omega^2 \ldots\ldots\ldots\ldots v^{(L-1)} \rightarrow \omega^{(L-1)} \rightarrow v^L \rightarrow \omega^{(L)} \rightarrow z$$

This process continues till all the layers are finished. One extra layer, Loss Layer, is added at last which is used for backward error propagation. Let 'o' is the output value for (input), then the cost or loss function can be used to measure the discrepancy between CNN prediction and output 'o'. Loss function can be defined as

$$z = \frac{1}{2} \| (o - v^{L}) \|^{2}$$

5. Proposed Model

Due to imbalanced datasets there are many problems which may lead to inefficiency of any machine learning or deep learning algorithm. Traditional methods which are available to deal with problems related to imbalanced datasets are not efficient enough do work with various machine learning algorithms, thus the proposed model tried to overcome the limitations of the traditional methods and develops an efficient model not only to detect frauds in financial sectors but also to develops a model that works efficiently with imbalanced datasets. The proposed model has 9 steps which are depicts in Figure 4.0. and sample heat map for the dataset is also shown in Figure 5.0(a) and (b).

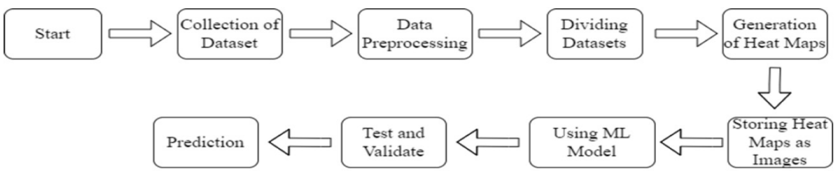

Figure 4.0

Flow of the proposed model

Figure 5.0 (a)

Sample Heat Maps for Fraud Records

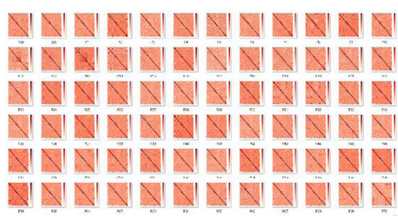

Figure 5.0 (b)

Sample Heat Maps for Non-Frauds Records

5.1 *Pseducode for HCNN*

Begin
Step 1: *Import data from dataset*
Step 2: *Convert the dataset according to the required format*
Step 3: *Divide the Dataset into two parts*
Step 4*: Store all fraud records into fraud.csv file*
Step 5: *Store all non fraud records into nonfraud.csv file*
Step 6: *Repeat the following steps 1000 times*
Loop
Shuffle the fraud records in the group of 1000 record each and store in separate csv file
Name the csv file as p<no of the group>.csv
End Loop
Step 7: *Repeat the following steps 1000 times*
Loop
Shuffle the non-fraud records in the group of 10 record each and store in separate csv file
Name the csv file as p<no of the group>.csv
End Loop
#Creation of Heat Maps
#Generation of Heat Maps for 500 different csv files contains fraud records
Step 8: *Import pandas, matplotlib, seaborn*
Step 9: *Repeat until I is not 500*
Loop
Data.read_csv('p+i.csv') ***# import csv files from Fraud datasets***
Fig.figure(figsize=(25,25)
Data.corr()
Heatmap(Data, cmap= 'Reds')
Show()
Store Heat Map as P<no>.png file within FraudHeatMap Folder
End Loop
#Generation of Heat Maps for 500 different csv files contains non-fraud records
Step 10: *Import pandas, matplotlib, seaborn*
Step 11: *Repeat until I is not 500*
Loop
Data.read_csv('p+i.csv') ***#import csv files from non-Fraud datasets***
Fig.figure(figsize=(25,25)
Data.corr()
Heatmap(Data, cmap= 'Reds')
Show()
Store Heat Map as P<no>.png file within NonFraudHeatMap Folder
End Loop
Step 12: *the Divide Pictures of Heat Maps (Fraud and Non Frauds) into Train, Test, Eval in 70%, 20% and 10% respectively*
Step 13: *Use Machine Learning Algorithm* ***#Used CNN***
Step 14: *Evaluate the model*
End

6. Results and Discussion

The model proposed in this work performs well efficiently for the detection of financial fraud mainly for Credit Card Fraud. This model overcomes the problems related to the tradition methods used to deal with imbalanced datasets as this model neither replicate minor class records nor discard major class records. It just creates a different heat map for the group of records and based on the analysis done on these generated heat map images it classify the transaction for the fraud or normal category. The model is run three times for finding the best results. The final values of results are the average of three runs. In table 1.0 the results for all three executions are illustrated.

Table 1.0

Proposed Model (HCNN)

HCNN	Precision	Recall	F1	AUC
1	0.9203	0.7458	0.8396	0.8956
2	0.9012	0.7508	0.8284	0.8694
3	0.9108	0.7908	0.8219	0.8837
Average	**0.9107**	**0.7625**	**0.8299**	**0.8829**

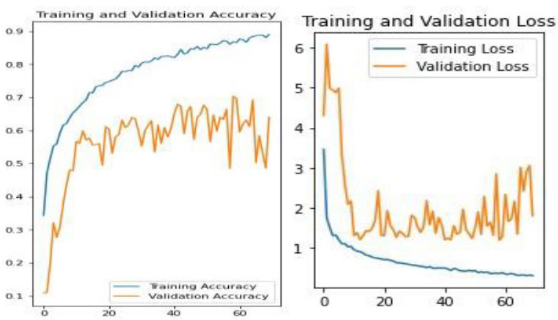

Figure 6.0

ROC curve for the HCNN

The ROC curve for the proposed model is shown in Figure 6.0. In (a) the graph for the validation accuracy is shown and in (b) the graph for validation loss is shown. For validation purposes, three other Deep learning approaches are implemented. The results for all approaches are shown in Table 2.0.

Table 2.0

Comparison for proposed model (HCNN) and LSTM, Naive Bayes

Model	Precision	Recall	F1	AUC
LSTM	0.8575	0.7832	0.7866	0.8702
ResNet	0.8626	0.7289	0.7792	0.8602
EfficientNet	0.8926	0.7756	0.7992	0.8002
HCNN	**0.9107**	**0.7625**	**0.8299**	**0.8829**

When the results of the above models are compared, it is found that the proposed model outperforms in every criteria. However the results of the other models are similar. The proposed model got the precision 91.07, Recall 76.25, F1 score 82.99 and the area under the curve is 88.29. The model is compared with other algorithms, the pictorial representation is shown in figure 7.0. For validation of the proposed model the comparative analysis is performed with the model of J. Forough et al. used the same data set which is used in the proposed model and they applied the Feed Forward Neural network on the data set. In the proposed model CNN is utilized for fraud detection [25]. J. Forough et al. got the precision 85.75, Recall 74.08 and F1 78.66 but the proposed model got the precision 91.07, Recall 76.25 and F1 82.99. J. Forough et al. uses three different techniques for fraud detection like LSTM, GRU and ensemble model as baseline model then they apply FFNN for fraud detection. In contrast the proposed model uses the CNN on the heat map which is generated for different instances.

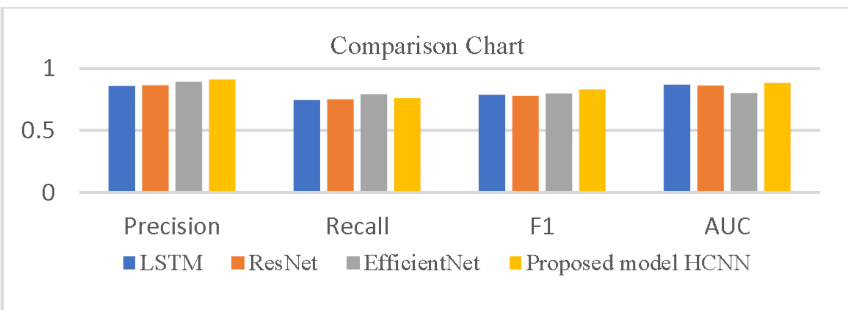

Figure 7.0

Comparison Chart of Proposed Model (HCNN) with other Models

Conclusion

Thousands of methods have been tested on fraud detection datasets in prior research, and some have even produced 100% accurate findings by addressing class imbalance problems. The suggested strategy, however, takes a different track when it comes to detecting credit card fraud. This article suggests a unique method for detecting credit card fraud that makes use of HCNN. With the use of heat map images, this method adds a new dimension to the detection of credit card fraud. It also offers potential future avenues for converting other forms of text data into pictures, allowing the categorization of data with distinctive patterns. In order to find new differentiating characteristics for credit card fraud detection, several feature engineering techniques are used. This study also suggests new features for this field.

As the future work, we like to move one step ahead by taking advantages of significant encoder-decoder models and by changing them for charge card blackmail acknowledgment issues, we need to inspect their ability to act in this environment with basic difficulties

References

[1] Pleil, J. D., Stiegel, M. A., Madden, M. C., & Sobus, J. R., Heat map visualization of complex environmental and biomarker measurements. *Chemosphere*, 84(5), 716-723 (2011).

[2] The History of the Cluster Heat Map Leland Wilkinsona & Michael Friendly.

[3] Zhao, S., Guo, Y., Sheng, Q., & Shyr, Y., Advanced heat map and clustering analysis using heatmap3. *BioMed research international*, (2014).

[4] Netek, R., Pour, T., & Slezakova, R., Implementation of heat maps in geographical information system–exploratory study on traffic accident data. *Open Geosciences*, 10(1), 367-384 (2018).

[5] Chu, H., Lin, W., Wu, J., Zhou, X., Chen, Y., & Li, H., A new heat-map-based algorithm for human group activity recognition. In *Proceedings of the 20th ACM international conference on Multimedia*, pp. 1069-1072 (2012, October).

[6] Shcheglova, S. N., & Shcheglov, B. O. Mathematical Algorithm for Creating 3D Models of Heat Maps as a Biophysical Method for Assessing Environmental and Economic Fire Damage in the Far Eastern Federal District of Russia.

[7] Forough, J., & Momtazi, S., Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing*, 99, 106883 (2021).

[8] Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J., Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, 8, 1-21 (2021).

[9] Gupta, A., Lohani, M. C., & Manchanda, M., Financial fraud detection using naive bayes algorithm in highly imbalance data set. *Journal of Discrete Mathematical Sciences and Cryptography*, 24(5), 1559-1572 (2021).

[10] Itoo, F., Meenakshi, & Singh, S., Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology*, 13, 1503-1511 (2021).

[11] Taha, A. A., & Malebary, S. J., An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. *IEEE Access*, 8, 25579-25587 (2020).

[12] Vats, S., Singh, S., Kala, G., Tarar, R., & Dhawan, S., iDoc-X: An artificial intelligence model for tuberculosis diagnosis and localization. *Journal of Discrete Mathematical Sciences and Cryptography*, 24(5), 1257-1272 (2021).

[13] Vats, S., Sagar, B. B., Singh, K., Ahmadian, A., & Pansera, B. A., Performance evaluation of an independent time optimized infrastructure for big data analytics that maintains symmetry. *Symmetry*, 12(8), 1274 (2020).

[14] Vats, S., & Sagar, B. B., An independent time optimized hybrid infrastructure for big data analytics. *Modern Physics Letters B*, 34(28), 2050311 (2020).

[15] Vats, S. A. T. V. I. K., Dubey, S. K., & Pandey, N. K., Genetic algorithms for credit card fraud detection. In International Conference on Education and Educational Technologies (2013, July).

[16] Lin, C. T., & Lee, I. F., Building decision analysis model by the experts knowledge–applying to management fraud detection. *Journal of Information and Optimization Sciences*, 31(3), 533-542 (2010).

[17] Singh, A., & Jain, A., Cost-sensitive metaheuristic technique for credit card fraud detection. *Journal of Information and Optimization Sciences*, 41(6), 1319-1331 (2020).

[18] Kumar, A., Singh, K., & Khan, T., L-RTAM: Logarithm based reliable trust assessment model for WBSNs. *Journal of Discrete Mathematical Sciences and Cryptography*, 24(6), 1701-1716 (2021).

[19] Khan, T., & Singh, K., Resource management based secure trust model for WSN. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(8), 1453-1462 (2019).

[20] Shariq, M., Singh, K., Lal, C., Conti, M., & Khan, T., ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags. Computer Networks, 217, 109360 (2022).

[21] Kumar, A., Singh, K., Khan, T., Ahmadian, A., Saad, M. H. M., & Manjul, M., ETAS: An efficient trust assessment scheme for BANs. IEEE Access, 9, 83214-83233 (2021).

[22] Khan, T., Singh, K., & Purohit, K. C., ICMA: An efficient integrated congestion control approach. Recent Patents on Engineering, 14(3), 294-309 (2020).

[23] Khan, T., Singh, K., Shariq, M., Ahmad, K., Savita, K. S., Ahmadian, A., ... & Conti, M,. An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach. Computer Communications, 209, 217-229 (2023).

[24] Khan, Tayyab, and Karan Singh. “RTM: Realistic Weight-Based Reliable Trust Model for Large Scale WSNs.” Wireless Personal Communications 129, no. 2 : 953-991 (2023).

[25] Singh, A., & Jain, A., Hybrid bio-inspired model for fraud detection with correlation-based feature selection. *Journal of Discrete Mathematical Sciences and Cryptography*, 24(5), 1365-1374 (2021).

Received September 2023