Sequence-wise credit card fraud detection with a novel resampling method based on outlier data

Mehdi Ghatee*, Behnam Yousefimehr

Department of Mathematics and Computer Science, Amirkabir University of Technology

No. 424, Hafez Avenue, Tehran 15875-4413, Iran

Abstract

One of the crucial difficulties in organizations like insurance companies and banks is detecting electronic fraud. One of the most significant areas of electronic banking is credit cards. Today, most banking transactions are done online using credit cards. As a result, as the use of credit cards has expanded, so too have the financial losses brought on by credit card fraud. Numerous studies have been conducted in the past to detect and prevent credit card fraud. However, most of them lose their usefulness over time due to concept drift. This article presents models resistant to concept drift, sequentially and non-sequentially, on two real-world data sets. It also tries to improve the results of the state-of-the-art papers.

Additionally, it provided a resampling technique based on outlier data that offers better resampling than previous approaches and shows promising results in the detection stage. Our experimental results on two real-world data sets show that our proposed models outperform advanced models in every evaluation criterion. The F1 score for non-sequential fraud detection in the European and Brazilian credit card datasets was 89% and 99%, respectively, and for sequential fraud detection, it was 83% and 99%.

Keywords: Fraud detection, Resampling, Sequential modeling, Machine learning, Deep learning.

* Corresponding author: Mehdi Ghatee, Associate Professor of Computer Science, Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran.

Email address: ghatee@aut.ac.ir(M. Ghatee), behnam.y2010@aut.ac.ir (B. Yousefimehr),

1. Introduction

Credit card fraud is critical since even a single instance of fraud can have severe financial consequences. Since fraud detection is such a crucial subject, many studies have previously been done in this field. On the other hand, criminals are gradually modifying their behavior and devising new fraudulent tactics to avoid detection by fraud detection systems, and therefore the proposed models suffer concept drift. Credit card fraud detection is a process that determines if a transaction is normal or fraudulent. This problem detection faces numerous challenges, including a lack of data, scalability, unbalanced class sizes, and concept drift.[1].

Much research has been done on this topic using machine learning models and traditional techniques such as decision trees [2], support vector machines [3], hidden markov model [4], neural network [5], deep learning [6], k-nearest neighbor [7] and discriminant analysis [8]. In addition, algorithms such as LightGBM [9] in non-sequential models for their high speed and Accuracy, and RNNs [10], [11], and [12] in sequential models for their ability to maintain the sequence, have made significant advances in recent years. Considering the promising results of these two approaches and good opportunities for improvement, in this paper, in addition to using our new balancing method, we use the LightGBM algorithm in the non-sequential part and the LSTM network in the sequential part. The models we offer can work more accurately than the previous models.

The rest of the paper is structured as follows. Section 2 discusses previous work on credit card fraud detection. Section 3 describes our methodology and the structure of the proposed system. Section 4 discusses the experiments, presents the results, and evaluates model performance. In the last part of the paper, Section 5, we summarize what we have done and discuss what else needs to be done.

2. Related works

This section reviews the previous work in credit card fraud detection. Much research has been conducted to study the issues of credit card fraud detection. Save, Prajal et al. [2] and Gaikwad, Jyoti R., et al. [13] presented a decision tree-based fraud detection method for credit cards. Instead of just spending a profile, Singh, Gajendra, et al. [3] propose an SVM-based technique with multiple kernel involvement and several user profile fields. Duman, Ekrem, et al. [14] proposed a new way to use the well-known meta-heuristic methods of genetic algorithms and scatter search together. Carcillo, Fabrizio, et al. [15] suggest a hybrid strategy for improving fraud detection accuracy by combining supervised and unsupervised techniques. Unsupervised outlier scores were computed and tested on a real, labeled credit card fraud dataset. The experimental results suggest that the combination is effective and improves detection accuracy. For the first time, Mahmoudi, Nader, et al. [16] investigated a linear discriminant called the Fisher Discriminant Function in the credit card fraud detection problem, making the standard function more sensitive to crucial examples. This way, the profit that can be obtained from a fraud classifier is maximized. According to experimental data, the Modified Fisher Discriminant could provide more profit. Srivastava, Abhinav, et al. [4] use a Hidden Markov model (HMM) to model the sequence of operations in credit card transaction processing and show that an HMM is trained using regular cardholder behavior. It is considered fraudulent if the HMM does not accept an incoming credit card transaction with a high enough probability. Tingfei, Huang, Cheng Guangquan, et al. [17] presented the VAE technique, which creates many cases from minority groups and uses them to train the classification network.

Since this paper aims to solve the problem using resampling along with LightGBM or LSTM deep neural networks, in the rest of this section, we will focus on the literature on these two perspectives. Ileberi, Emmanuel, Yanxia Sun, et al. [18] showed that using AdaBoost positively affects credit card fraud detection. Additionally, the results obtained by the boosted models were superior to those achieved by existing methods. Taha, Altyeb Altaher, et al. [19] provided an optimized light gradient boosting machine (OLightGBM) for fraud detection in credit card transactions, where a Bayesian-based hyperparameter optimization algorithm is used to optimize the parameters of the light gradient boosting machine (LightGBM). Roy et al. [20] found that the LSTM and GRU models outperformed the baseline ANN, indicating that transaction sequence is essential in detecting fraudulent and normal transactions. Forough, Javad et al. [22] [23] developed a rapid ensemble model based on sequential data modeling using deep recurrent neural networks like LSTM and GRU and a new voting mechanism based on artificial neural networks to detect fraudulent cases. They later introduced a novel credit card fraud detection model based on deep neural networks and probabilistic graphical models (PGM). They investigated how considering hidden sequential dependencies among transactions and predicted labels could improve the results. Also, they came up with a new undersampling method that helps keep the sequential patterns of the data during the random undersampling process.

3. Methodology

As previously stated, fraudulent people try to deceive the model by repeatedly changing their behavior, and thus the presented models suffer concept drift over time. As a result, in the non-sequential part, the focus is on ensemble learners, making it more difficult to deceive the model. In the sequential part, the problem of concept drift is solved mainly due to forgetting the past behavior. The data used in this work and the implementation of all models are available on GitHub[1].

[1] https://github.com/behnamy2010/fruaddetection

3.1. Feature selection

In the feature selection section, we have used a collective approach so that we have used six different methods:

1. Information Value using Weight of evidence
2. Variable Importance using Random Forest
3. Recursive Feature Elimination
4. Variable Importance using Extra trees classifier
5. Chi-Square best variables
6. L1-based feature selection

If at least 2 out of 6 methods vote the feature to be necessary, that feature is selected.

3.2. non-sequential credit card fraud detection

3.2.1. *Resampling*

We employ the oversampling approach in this part. Because we consider that the inclusion of outliers in the linear combination of approaches results in an improper effect, we do not include them in the sampling.

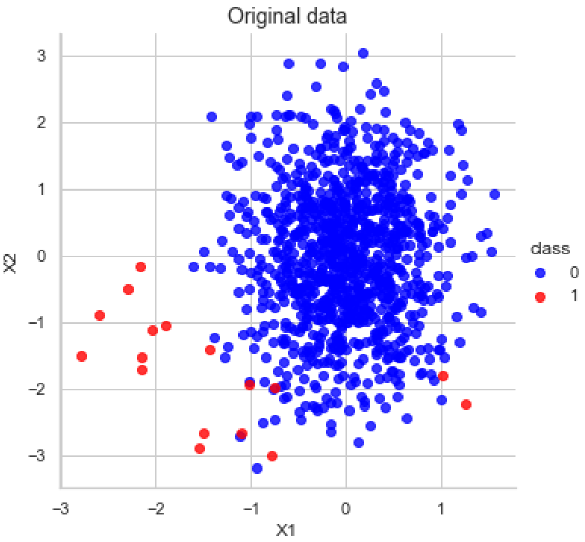

Fig.1. Imbalanced small dataset with outliers in the minority class

In Fig.1, we illustrate a small data set showing the outlier data problem and how to solve it.

3.2.1.1. SMOTE

SMOTE begins by randomly selecting a minority class instance and locating its k nearest minority class neighbors. The synthetic instance is then constructed by selecting one of the k nearest neighbors b at random and connecting a and b in the feature space to form a line segment. convex combination of the two selected instances, a and b, generates the synthetic instances. [24].

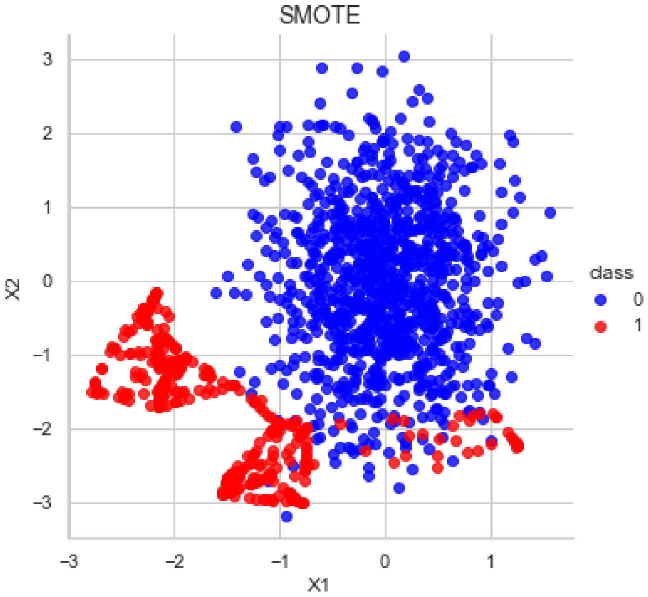

Fig.2. Illustration of oversampling with SMOTE

As seen in Fig 2, SMOTE has also generated data in the majority class distribution due to outlier data and their participation in the linear combination.

3.2.1.2. OCSVM

One-class support vector machine (SVM) is an unsupervised model for anomaly or outlier detection. One-class support vector machine is training to learn the boundary of normal data and recognize data outside the boundary as outliers.[25]

3.2.1.3. OCSVM - SMOTE

The method we propose for resampling is detecting outlier data using OCSVM and not participating in resampling. Of course, we do not remove outlier data because they are significant; rather, by identifying them, we simply prevent them from participating in resampling.

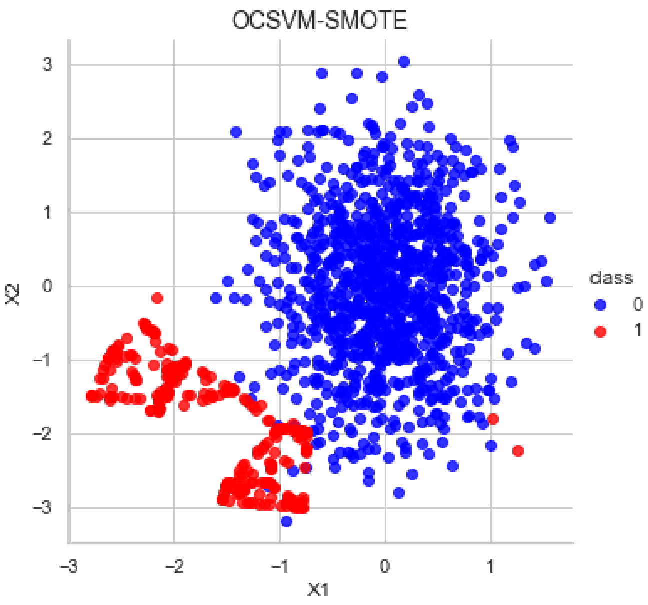

Fig.3. Illustration of resampling with our proposed method: OCSVM – SMOTE

As shown in Fig 3, resampling occurred mainly in the minority class distribution and did not affect the majority class distribution in addition to retaining the outlier data.

3.2.2. *LightGBM*

LightGBM is an ensemble learning and gradient boosting framework that employs tree-based learning techniques, and "light" refers to its speed. LightGBM Unlike other tree-based approaches that grow level-wise grows leaf-wise by selecting the leaf with the greatest loss [26].

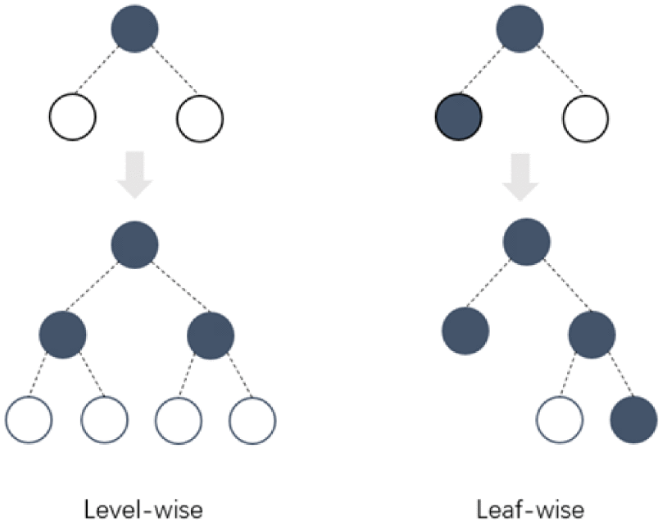

Fig.4. Tree generation approach in LightGBM [27].

3.2.3. *LightGBM with OCSVM - SMOTE for fraud detection*

In the proposed method, we first separate the train and test data using the K-Fold method, select the features from the training data using a combination of feature selection algorithms and then oversample the reduced dimensionality dataset using the proposed OCSVM-SMOTE method. Moreover, finally, train the LightGBM algorithm using the obtained data.

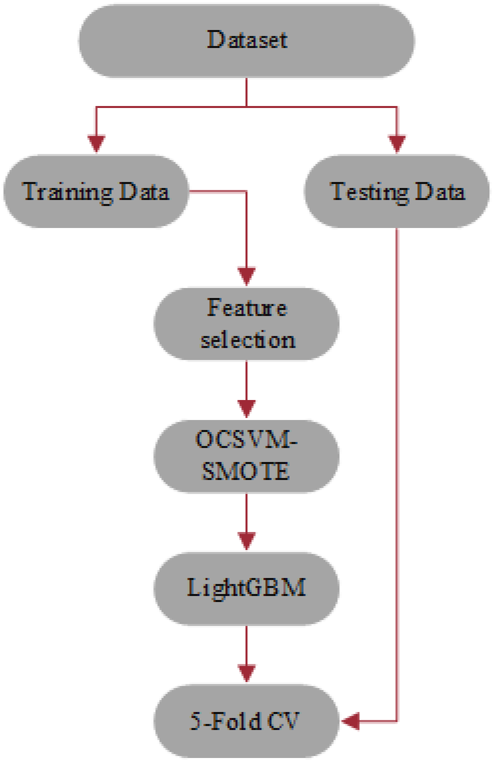

Fig.5. Schematic of our non-sequential credit card fraud detection approach

3.3. Sequential credit card fraud detection

3.3.1. *Resampling*

Because the sequence of fraud data is critical in this part, we use random undersampling in the majority class. Furthermore, in order to execute undersampling from the most frequent section of the data, we first detect poorly distributed data with OCSVM and exclude it from undersampling.

3.3.2. Random undersampling

Random undersampling is randomly selecting instances from the majority class and removing them from the training dataset.

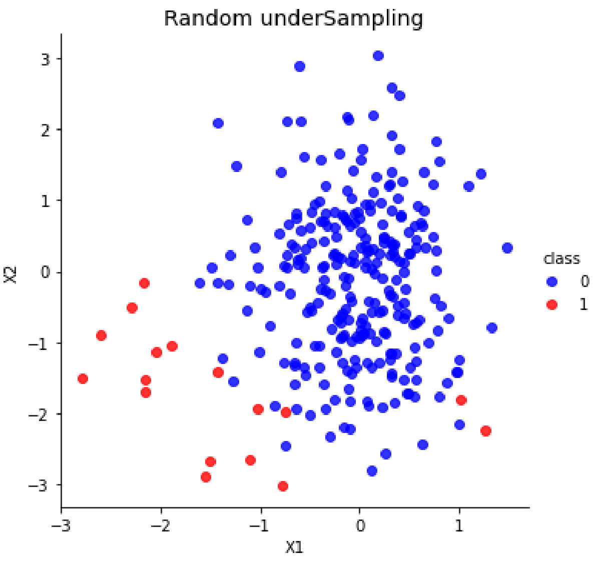

Fig.6. Illustration of undersampling with Random undersampling

As shown in Figure 6, a considerable portion of the poorly distributed normal data is lost.

3.3.3. OCSVM – Random undersampling

The strategy we propose for resampling is to use OCSVM to detect sparsely distributed data and avoid resampling. It should be noted that we do not remove these data but rather identify them to prevent them from engaging in undersampling.

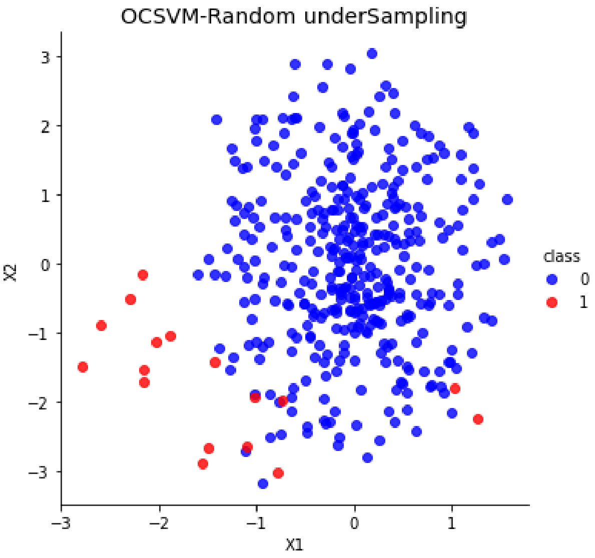

Fig.7. Illustration of resampling with our proposed method: OCSVM – Random undersampling

As illustrated in Figure 3, the proposed technique can better retain the data distribution after undersampling.

3.3.4. *LSTM*

Long short-term memory networks (LSTM) are a type of recurrent neural network (RNN) that can learn long-term dependencies, particularly in sequence prediction problems [28].

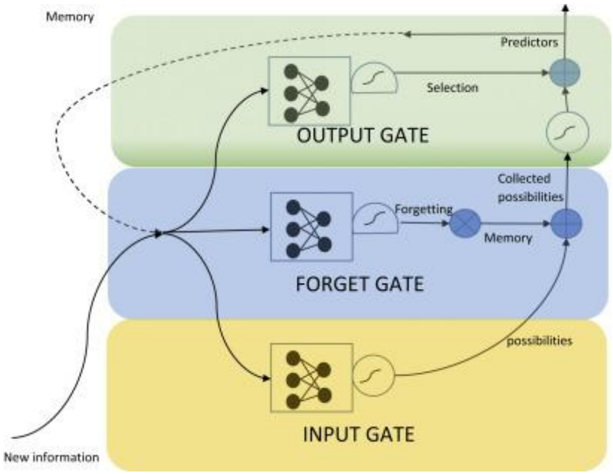

Fig.8 A typical LSTM cell structure [29].

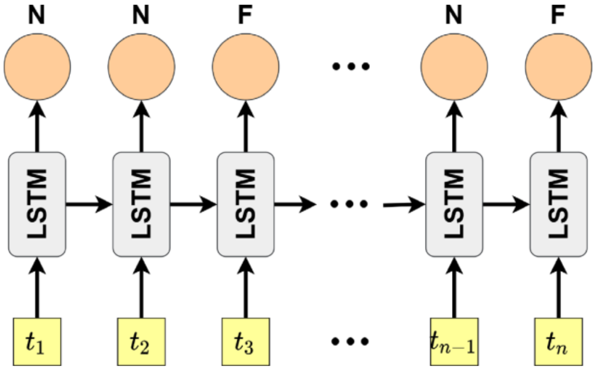

Fig.9 A layer of LSTM. The ith transaction is indicated by t$_i$. N and F represent normal and fraudulent labels, respectively [10].

3.3.5. LSTM *with OCSVM - random undersampling for fraud detection*

In the proposed method, we first separate the train and test data and select features from the training data using a combination of feature selection algorithms and then undersample the reduced dimensionality dataset using the proposed OCSVM - random undersampling method. Moreover, finally, train the LSTM algorithm using the obtained data.

4. Experiments and Results

4.1. Datasets

In our studies, we used two real data sets presented by Pozzolo et al. [30] and Gadi et al. [31].

The first dataset pertains to credit card transactions performed by European users in September 2013 for two days. This dataset includes 284,807 transactions, with fraudulent samples constituting 0.172 percent of the total.[30]

The second data set was obtained from a Brazilian bank from April 2004 to September 2004. There are 374,823 transactions in this dataset, and 3.74 percent are fraudulent samples.[31]

A summary of the two datasets is provided in Table 1.

Table 1. The credit card datasets description[11].

Dataset	Normal	Fraudulent	Features	Instances
European cards dataset	284,315	492	30	284,807
The Brazilian dataset	360,792	14,031	17	374,823

4.2. Metrics

This section provides an overview of the performance metrics used to evaluate a classification problem, such as accuracy, precision, recall, and F1.

4.2.1. Accuracy

Accuracy is the total number of predictions divided by the number of correct predictions.

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$

4.2.2. Precision:

Precision is the ratio of positive predictions to the total number of positive classes predicted.

$$Precision = \frac{(TP)}{(TP + FP)}$$

4.2.3. Recall:

Recall is the ratio of positive predictions to the number of positive class values in the test data.

$$Recall = \frac{(TP)}{(TP + FN)}$$

4.2.4. F1-Score:

F1-score depicts the balance between precision and recall.

$$F1 - score = \frac{2 * Precision * Recall}{Precision + Recall}$$

4.3. Results

In this section, we evaluate the suggested approaches' performance on two datasets and in two sequential and non-sequential parts.
Furthermore, our work is only comparable with articles that only performed resampling on training data. We exclude comparisons with articles such as [12] and [18] that performed resampling before separating the train and test data.

4.3.1. resampling in non-sequential credit card fraud detection result

4.3.1.1. OCSVM – SMOTE

In this section, we will compare the proposed method with other famous methods

Table 2. Comparison of different resampling with different percentages

name	Fraud percent	accuracy	precision	recall	f1-score
original	<1	0/999555	0/965812	0/768707	0/856061
feature selected	<1	0/999473	0/925	0/755102	0/831461
ADASYN	5	0/999391	0/846715	0/789116	0/816901
ADASYN	10	0/999345	0/832117	0/77551	0/802817
ADASYN + ocsvm	5	0/999766	0/857143	0/9	0/878049
ADASYN + ocsvm	10	0/999754	0/847059	0/9	0/872727
RandomOverSampler	5	0/999427	0/871212	0/782313	0/824373
RandomOverSampler	10	0/999427	0/876923	0/77551	0/823105
RandomOverSampler + ocsvm	5	0/999777	0/850575	0/925	0/886228
RandomOverSampler + ocsvm	10	0/999777	0/858824	0/9125	0/884848
KMeansSMOTE	5	0/999356	0/870968	0/734694	0/797048
KMeansSMOTE	10	0/999321	0/886957	0/693878	0/778626
SMOTE	5	0/999415	0/859259	0/789116	0/822695
SMOTE	10	0/999391	0/846715	0/789116	0/816901
SMOTE + ocsvm	**5**	**0/999859**	**0/914634**	**0/9375**	**0/925926**
SMOTE + ocsvm	10	0/999801	0/879518	0/9125	0/895706

Table 3. Comparison of the proposed method with previous works

paper	method	Dataset	year	accuracy	precision	recall	f1-score
[32]	CNN	Europe	2022	0.999	0.93	-	0.8571
[33]	ANN	Europe	2021	0.9992	0.8115	0.7619	0.7859
[19]	Optimized LightGBM	Europe	2020	0.9840	0.9734	0.4059	0.5695
Ours	**LightGBM + OCSVM - SMOTE**	**Europe**	**2022**	**0.999824**	0.924654	**0.861427**	**0.891501**
Ours	**LightGBM + OCSVM - SMOTE**	***Brazil***	**2022**	**0.999638**	**0.985101**	**0.995950**	**0.990488**

4.3.2. sequential credit card fraud detection result

Table 4. Comparison of different resampling with different percentages

name	Fraud percent	Accuracy	precision	recall	f1-score
original	<1	0.999649	1	0.722222	0.838710
feature selected	<1	0.999625	0.952381	0.740741	0.833333
RandomUnderSampler	5	0/998010	0/364035	0/768519	0/494047
RandomUnderSampler	10	0/996699	0/251428	0/814815	0/384279
RandomUnderSampler + EllipticEnvelope	5	0/999492	0/922535	0/823899	0/870431
RandomUnderSampler + EllipticEnvelope	10	0/999544	0/984375	0/792453	0/878048
RandomUnderSampler + isf	5	0/999633	1	0/794521	0/885496
RandomUnderSampler + isf	10	0/999596	0/959349	0/808219	0/877323
RandomUnderSampler + lof	5	0/999397	0/892307	0/773333	0/828571
RandomUnderSampler + lof	10	0/999372	0/884615	0/766667	0/821428
RandomUnderSampler + ocsvm	**5**	**0/999718**	**1**	**0/842466**	**0/914498**
RandomUnderSampler + ocsvm	10	0/999252	1	0/788079	0/881481
NearMiss	5	0/775803	0/004009	0/712963	0/007975
NearMiss	10	0/717226	0/003057	0/685185	0/006088
NearMiss + EllipticEnvelope	5	0/993447	0/215815	0/823899	0/342036
NearMiss + EllipticEnvelope	10	0/997555	0/449122	0/805031	0/576576
NearMiss + isf	5	0/999205	1	0/774834	0/873134
NearMiss + isf	10	0/999205	1	0/774834	0/873134
NearMiss + lof	5	0/999410	0/887218	0/786667	0/833922
NearMiss + lof	10	0/999385	0/885496	0/773333	0/825622
NearMiss + ocsvm	5	0/999645	1	0/80137	0/889733
NearMiss + ocsvm	10	0/999158	1	0/761589	0/864661
AllKNN	-	0/999613	0/912087	0/768519	0/834170
AllKNN + EllipticEnvelope	-	0/999544	0/992063	0/786164	0/877192
AllKNN + isf	-	0/999608	1	0/780822	0/876923
AllKNN + lof	-	0/999422	0/90625	0/773333	0/834532
AllKNN + ocsvm	-	0/999275	1	0/794702	0/885608
TomekLinks	-	0/999613	0/931034	0/75	0/830769
TomekLinks + EllipticEnvelope	-	0/999158	1	0/761589	0/864661
TomekLinks + isf	-	0/999633	1	0/794521	0/885496
TomekLinks + lof	-	0/999410	0/972477	0/706667	0/818532
TomekLinks + ocsvm	-	0/999645	1	0/80137	0/889733

Table 5. Comparison of the proposed method with previous works

paper	method	Dataset	year	accuracy	precision	recall	f1-score
[10]	LSTM	Europe	2021	-	0.8575	0.7408	0.7866
[11]	LSTM-CRF	Europe	2022	-	0.8817	0.7569	0.8076

Ours	**LSTM + OCSVM-random undersampling**	**Europe**	**2022**	**0.9996**	**0.9418**	0.7500	**0.8350**
[10]	LSTM	Brazil	2021	-	0.8776	0.7144	0.7874
[11]	LSTM-CRF	Brazil	2022	-	0.9256	0.7955	0.8555
Ours	**LSTM + OCSVM-random undersampling**	**Brazil**	**2022**	**0.9992**	**0.9968**	**0.9839**	**0.9903**

4.4. Discussion

According to the results obtained in the previous sections, it can be seen that the OCSVM outlier detection method has a much better performance than other methods and oversampling or undersampling of more than 5% causes the model to fail. It is also observed that the machine learning and deep learning models presented with the help of the proposed resampling have shown better performance than the previous works.

5. Conclusion and future work

Credit card fraud is a type of identity theft involving the unlawful use of another person's credit card information to charge purchases to the account or withdraw funds from it. Unfortunately, it is on the rise. Credit card fraud detection is difficult because fraudulent people frequently change their behavior to deceive models, and the models undergo concept drift over time. Moreover, another challenge in this field is data imbalance. to solve these problems in this study, in addition to resampling, we have used two sequential and non-sequential fraud detection approaches:

- In the non-sequential part, we combined our suggested OCSVM-SMOTE oversampling method with the LightGBM ensemble learning algorithm. We showed that the combination of OCSVM and SMOTE produces better data and, as a result, model training better.
- In the sequential part, we used the long short-term memory (LSTM) along with our proposed random undersampling method. We showed that the combination of OCSVM improves the undersampling method and, as a result, increases the model's efficiency.

In the future, we plan to employ reinforcement learning approaches to maintain data sequences and evaluate their potential to identify fraud.

References

[1] Mekterović, I., Karan, M., Pintar, D., & Brkić, L. (2021). Credit card fraud detection in card-not-present transactions: Where to invest?. *Applied Sciences*, *11*(15), 6766.

[2] Save, P., Tiwarekar, P., Jain, K. N., & Mahyavanshi, N. (2017). A novel idea for credit card fraud detection using decision tree. *International Journal of Computer Applications*, *161*(13).

[3] Singh, G., Gupta, R., Rastogi, A., Chandel, M. D., & Ahmad, R. (2012). A machine learning approach for detection of fraud based on svm. *International Journal of Scientific Engineering and Technology*, *1*(3), 192-196.

[4] Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). Credit card fraud detection using hidden Markov model. *IEEE Transactions on dependable and secure computing*, *5*(1), 37-48.

[5] Ghosh, S., & Reilly, D. L. (1994, January). Credit card fraud detection with a neural-network. In *System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on* (Vol. 3, pp. 621-630). IEEE.

[6] Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018, April). Deep learning detecting fraud in credit card transactions. In *2018 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 129-134). IEEE.

[7] Malini, N., & Pushpa, M. (2017, February). Analysis on credit card fraud identification techniques based on KNN and outlier detection. In *2017 third international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB)* (pp. 255-258). IEEE.

[8] Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by modified Fisher discriminant analysis. *Expert Systems with Applications*, *42*(5), 2510-2516.

[9] Ge, D., Gu, J., Chang, S., & Cai, J. (2020, April). Credit card fraud detection using LightGBM model. In *2020 international conference on E-commerce and internet technology (ECIT)* (pp. 232-236). IEEE.

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

[11] Forough, J., & Momtazi, S. (2022). Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach. *Expert Systems*, *39*(1), e12795.

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

[13] Gaikwad, J. R., Deshmane, A. B., Somavanshi, H. V., Patil, S. V., & Badgujar, R. A. (2014). Credit card fraud detection using decision tree induction algorithm. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 4(6), 66-69.

[14] Duman, E., & Ozcelik, M. H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications*, *38*(10), 13057-13063.

[15] Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information sciences*, *557*, 317-331.

[16] Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by modified Fisher discriminant analysis. *Expert Systems with Applications*, *42*(5), 2510-2516.

[17] Tingfei, H., Guangquan, C., & Kuihua, H. (2020). Using variational auto encoding in credit card fraud detection. *IEEE Access*, *8*, 149841-149853.

[18] Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. *IEEE Access*, *9*, 165286-165294.

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

[20] Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018, April). Deep learning detecting fraud in credit card transactions. In 2018 Systems and Information Engineering Design Symposium (SIEDS) (pp. 129-134). IEEE. [21]

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

[23] Forough, J., & Momtazi, S. (2022). Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach. *Expert Systems*, *39*(1), e12795.

[24] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: synthetic minority over-sampling technique. *Journal of artificial intelligence research*, *16*, 321-357.

[25] Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the support of a high-dimensional distribution. *Neural computation*, *13*(7), 1443-1471.

[26] Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., ... & Liu, T. Y. (2017). Lightgbm: A highly efficient gradient boosting decision tree. *Advances in neural information processing systems*, *30*.

[27] Ju, Y., Sun, G., Chen, Q., Zhang, M., Zhu, H., & Rehman, M. U. (2019). A model combining convolutional neural network and LightGBM algorithm for ultra-short-term wind power forecasting. *Ieee Access*, *7*, 28309-28318.

[28] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural computation*, *9*(8), 1735-1780.

[29] Al-Jabery, K. K., Obafemi-Ajayi, T., Olbricht, G. R., & Wunsch, D. C. (2020). II. Selected approaches to supervised learning. *Comput. Learn. Approaches Data Anal. Biomed. Appl*, 101-123.

[30] Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015, December). Calibrating probability with undersampling for unbalanced classification. In *2015 IEEE symposium series on computational intelligence* (pp. 159-166). IEEE.

[31] Gadi, M. F. A., Wang, X., & Lago, A. P. D. (2008, August). Credit card fraud detection with artificial immune system. In *International conference on artificial immune systems* (pp. 119-131). Springer, Berlin, Heidelberg.

[32] Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. *IEEE Access*, *10*, 39700-39715.

[33] Asha, R. B., & KR, S. K. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, *2*(1), 35-41.