Adversarial Learning for Credit Card Fraud Detection

Tung-Tu Wu  
 Department of Electrical Engineering  
 National Taiwan University  
 Taipei, Taiwan  
 [b08901133@ntu.edu.tw](mailto:b08901133@ntu.edu.twm)

ABSTRACT

With the advance of technology, e-commerce and online payment platforms develop rapidly, while the establishment of credit card fraud detection system (DFS) lags behind, which consequently leads to the continuous increase in fraud cases and financial losses. Though Machine Learning (ML), especially Deep Learning (DL) has emerged as a promising solution, there are two characteristics of credit card fraud data that might hinder neural networks’ performance: (1. Fraud and non-fraud cases are highly imbalanced. (2. Types of credit card fraud vary throughout the time as fraudsters would learn to cheat the currently deployed DFS. To deal with these two difficulties, we present an adversarial neural network (GAN) for one-class unsupervised learning. During the training process, scarce fraud cases are dismissed, and the remaining normal transaction cases would be utilized to train our model. Unsupervised learning means that the model would treat the problem as anomaly detection instead of traditional binary classification. Experimental results demonstrate that our proposed method outperforms other state-of-the-art anomaly detection models on either balanced or imbalanced testing data.

∗Article Title Footnote needs to be captured as Title Note

†Author Footnote to be captured as Author Note

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

*WOODSTOCK’18, June, 2018, El Paso, Texas USA*

© 2018 Copyright held by the owner/author(s). 978-1-4503-0000-0/18/06...$15.00

https://doi.org/10.1145/1234567890

CCS CONCEPTS

**• Computing methodologies → Machine learning → Machine learning approaches → Neural networks**

**• Computing methodologies → Machine learning → Learning paradigms → Unsupervised learning → Anomaly detection**

KEYWORDS

Credit card fraud detection, Adversarial learning, One-class classification, Anomaly detection

ACM Reference format:

FirstName Surname, FirstName Surname and FirstName Surname. 2018. Insert Your Title Here: Insert Subtitle Here. In *Proceedings of ACM Woodstock conference (WOODSTOCK’18). ACM, New York, NY, USA, 2 pages.* https://doi.org/10.1145/1234567890

1 INTRODUCTION

In recent years, credit card had become an indispensable thing in people’s daily life. More and more customers form the habit of online purchase, bringing huge profits to e-commerce companies [21]. However, as a lot of transactions are made online, credit card fraud comes out to be increasingly rampant. We can see that financial losses caused by credit card fraud are on a constant rise [21]. Though there might have been DFS designed and utilized by financial institutions and enterprises, customers are still facing threat of their personal properties since the various and keep changing means of fraud [22].

In the realm of ML, there are mainly two techniques to design a fraud detection system: supervised learning and unsupervised learning [22]. The former regards the credit card fraud detection problem as a two-class (i.e. binary) classification problem and requires a labeled dataset for the training process. This is undoubtedly a more straightforward method compared with unsupervised learning algorithms. Nevertheless, based on the fact that the fraud cases merely possess a very small portion among all the online credit card transactions, the dataset collected by bank sectors is also highly imbalanced. To be specific, the dataset is skewed towards the ordinary transactions conducted by genuine cardholders rather than fraudsters such as [kaggle].

Although some measures, such as SMOTE[??], could be applied to deal with the data imbalance, a more preferred way is to design an unsupervised learning process and transform the binary classification problem to the outlier detection or the anomaly detection task. This holds an advantage that the system could discover the potential new types of credit card fraud that do not exist in the training dataset. Specifically, a normal binary classifier simply learns the rules to differentiate the two given groups of data, which might suffer concept drift problem []. On the other hand, anomaly detection encourages neural networks or support vector machine (SVM) to focus only on the characteristics of normal cases, and cases which do not fit the normal conditions are automatically fall into the abnormal class. Therefore, when a novel credit card fraud case happens, the system would be able to classify it as an abnormal transaction if it does not perfectly satisfy the characteristics of expected normal cases. As a result, in view of the consensus that unsupervised learning could probably lead to a preferable result, this paper would focus more on the unsupervised learning models.

Generative adversarial networks (GANs) [], which have strong potential for unsupervised learning and semi-supervised learning tasks, appear to be a favorable choose for anomaly detection problem. A series of GAN-based image anomaly detection models have been studied [] [] [], while none of them present the version for numerical data such as credit card fraud detection. For instance, [] conduct the anomaly detection with the discriminator in the latent space x, while it is meaningless to project the numerical data to low-dimensional latent space if the raw features have been low enough. In other words, though GAN-based credit card fraud detection models give the impression of bringing promising results, few studies have been conducted.

This paper follows the work of \  
?



Figure 1: Figure Caption and Image above the caption [In draft mode, Image will not appear on the screen]

**Theorem/Proof/Lemma.** Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement.

....Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract.

1.1 Heading Level 2

In the below paragraph, it is explained how alt-txt value is placed in **MS Word 2010**. To add alternative text to a picture in Word 2010, follow these steps:

1. In a Word 2010 document, insert a picture.
2. Right click on the inserted picture and select the **Format Picture** option.
3. Select the **Alt Txt** option from the left-side panel options.
4. In the "Title:" and "Description:" text boxes, type the text you want to represent the picture, and then click "Close".

Below are steps to place alt-txt value in **MS Word 2013/2016**. To add alternative text to a picture in Word 2013/2016, follow these steps:

1. In a Word 2013/2016 document, insert a picture.
2. Right click on the inserted picture and select the **Format Picture** option.
3. In the settings at the right side of the window, click on the "Layout & Properties" icon (3rd option).
4. Expand **Alt Txt** option.
5. In the "Title:" and "Description:" text boxes, type the text you want to represent the picture, and then click "Close".

*1.1.1 Heading Level 3.* Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here.

*1.1.1.1 Heading Level 4.*Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here.

ACKNOWLEDGMENTS

Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here.

REFERENCES

[1] Patricia S. Abril and Robert Plant, 2007. The patent holder's dilemma: Buy, sell, or troll? *Commun. ACM* 50, 1 (Jan, 2007), 36-44. DOI: <https://doi.org/>10.1145/1188913.1188915.

[2] Sten Andler. 1979. Predicate path expressions. In *Proceedings of the 6th. ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL '79)*. ACM Press, New York, NY, 226-236. DOI:https://doi.org/10.1145/567752.567774

[3] Ian Editor (Ed.). 2007. *The title of book one* (1st. ed.). The name of the series one, Vol. 9. University of Chicago Press, Chicago. DOI:https://doi.org/10.1007/3-540-09237-4.

[4] David Kosiur. 2001. *Understanding Policy-Based Networking* (2nd. ed.). Wiley, New York, NY..

Conference Name:ACM Woodstock conference

Conference Short Name:WOODSTOCK’18

Conference Location:El Paso, Texas USA

ISBN:978-1-4503-0000-0/18/06

Year:2018

Date:June

Copyright Year:2018

Copyright Statement:rightsretained

DOI:10.1145/1234567890

RRH: F. Surname et al.

Price:$15.00