

NEURAL NETWORKS: 1. DEEP LEARNING - 2. CONVOLUTIONAL NN - 3. RECURRENT NN - 4. TRANSFER LEARNING

BINARY CLASSIFICATION



LOGISTIC REGRESSION AS A NEURAL NET



THE TASK IS TO LEARN w & b BUT HOW?

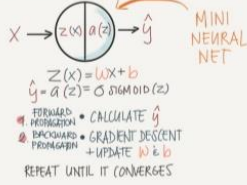
A. OPTIMIZE HOW GOOD THE GUESS IS BY MINIMIZING THE DIFF. BETWEEN GUESS (\hat{y}) AND TRUTH (y)
 $LOSS = \sum (\hat{y}_i - y_i)^2$
 $COST = J(w, b) = \frac{1}{n} \sum_{i=1}^n L(\hat{y}_i, y_i)$
 $COST = LOSS$ FOR THE ENTIRE DATASET



FINDING THE MINIMUM WITH GRADIENT DESCENT

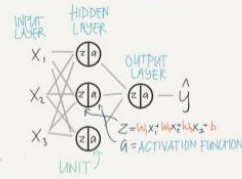
- 1. FIND THE DIRECTION (USING DERIVATIVES)
- 2. WALK (UPDATE w & b) AT A LEARNING RATE
- REPEAT UNTIL YOU REACH BOTTOM (CONVERGES)

PUTTING IT ALL TOGETHER

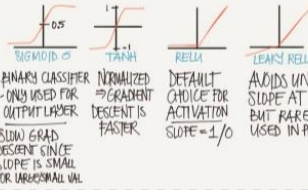


© Testenundz

2 LAYER NEURAL NET



ACTIVATION FUNCTIONS



SHALLOW NEURAL NETS

WHY ACTIVATION FUNCTIONS?
 EX. WITH NO ACTIVATION - $a = z$

$$a^{(1)} = z^{(1)} = w^{(0)}x + b^{(0)} \quad \text{LAYER 1}$$

$$a^{(2)} = z^{(2)} = w^{(1)}a^{(1)} + b^{(1)} \quad \text{LAYER 2}$$

$$a^{(2)} = w^{(0)}(w^{(1)}x + b^{(1)}) + b^{(2)}$$

$$= w^{(0)}w^{(1)}x + w^{(0)}b^{(1)} + b^{(2)}$$

WE COULD JUST AS WELL HAVE SKIPPED THE WHOLE NEURAL NET & USED LIN. REG.
 INITIALIZING w & b
 WHAT IF: INIT TO 0
 THIS WILL MAKE ALL THE UNITS TO BE THE SAME AND LEARN EXACTLY THE SAME FEATURES
 SOLUTION: RANDOM INIT BUT ALSO WANT THEM SMALL SO RAND * 0.01

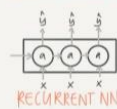
INTRO TO DEEP LEARNING

SUPERVISED LEARNING

INPUT: X	OUTPUT: y	NN TYPE
HOME FEATURES	PRICE	STANDARD NN
AD+USER INFO	WILL CLICK ON AD (y/n)	NN
IMAGE	OBJECT (1...1000)	CONV. NN (CNN)
AUDIO	TEXT TRANSCRIPT CHINESE	RECURRENT NN (RNN)
ENGLISH	POS OF OTHER CARS	CUSTOM/HYBRID
IMAGE/RADAR		



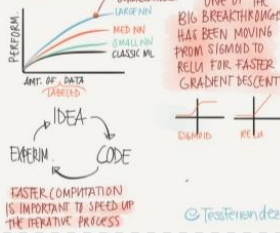
NETWORK ARCHITECTURES



NNs CAN DEAL WITH BOTH STRUCTURED & UNSTRUCTURED DATA



WHY NOW?



SpiderNet

сверточная нейронная сеть для выявления мошенничества

Афанасьев Сергей
 КБ «Ренессанс Кредит»

16 ноября 2021 г.
 Москва

Itsy Bitsy SpiderNet: Fully Connected Residual Network for Fraud Detection

Sergey Afanasiev
National Research University HSE
Moscow, Russia

Anastasiya Smirnova
National Research University HSE
Moscow, Russia

Diana Kotereva
National Research University HSE
Moscow, Russia

ABSTRACT

With the development of high technology, the scope of fraud is increasing, resulting in annual losses of billions of dollars worldwide. The preventive protection measures become obsolete and vulnerable over time, so effective detective tools are needed. In this paper, we propose a convolutional neural network architecture SpiderNet designed to solve fraud detection problems. We noticed that the principles of pooling and convolutional layers in neural networks are very similar to the way anti-fraud analysts work when conducting investigations. Moreover, the skip-connections used in neural networks make the usage of features of various period in anti-fraud models possible. Our experiments have shown that SpiderNet provides better quality compared to Random Forest and adapted for anti-fraud modeling problems 1D-CNN, 1D-DenseNet, F-DenseNet neural networks. We also propose new approaches for fraud feature engineering called B-tests and W-tests, which generalize the concepts of Beaudot's Law for fraud anomalies detection. Our results showed that B-tests and W-tests give a significant increase to the quality of our anti-fraud models. The SpiderNet code is available at <https://github.com/asmirnova24/SpiderNet>

CCS CONCEPTS

• Security and privacy → Usability in security and privacy.

KEYWORDS

neural networks, fraud detection, CNN, feature engineering

1 INTRODUCTION

The development of high technologies contributes not only to the growth of corporations and world economies but also to the development of fraud, which leads to losses of billions of dollars every year around the world.

In 2018, eight Indian banks incurred \$1.3 billion in losses in a fraud case involving Kingfisher Airlines founder Vijay Mallya¹. In another case, the Agricultural Bank of China faced losses of \$497 million after being defrauded by employees of billionaire Guo Wengui².

Hacker attacks are another global problem. In 2019, the FBI issued an official announcement that global losses from fraudulent Business Email Compromise (BEC) reached \$26 billion during the period from June 2016 to July 2019³.

¹<https://www.theguardian.com/world/2020/apr/28/kingfisher-airlines-vijay-mallya-fraud-appeal-conviction-india>
²<https://www.reuters.com/article/us-china-corruption/tycoons-skin-in-fraud>
³<https://www.fbi.gov/media/72019/72419010>

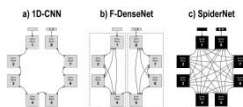


Figure 1: Convolutional neural network architectures designed for fraud detection: a) 1D-CNN, b) F-DenseNet, c) SpiderNet

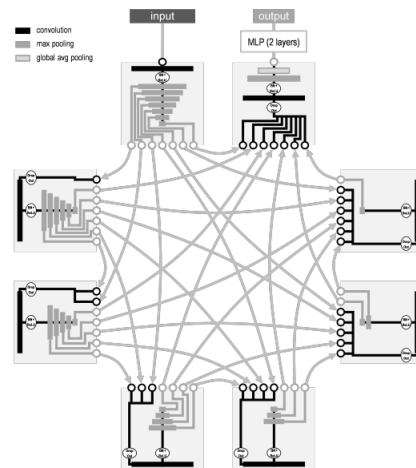
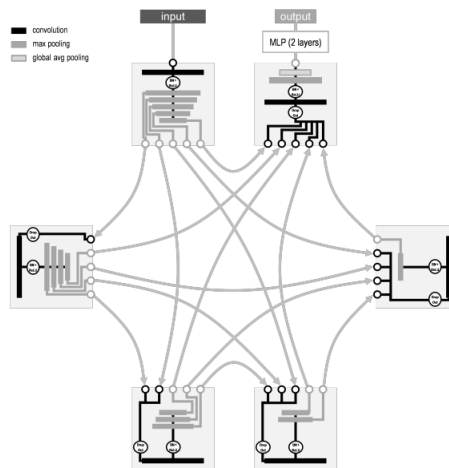
Another growing threat is social engineering, which has hit Russian bank customers seriously. According to the official data of the Bank of Russia, losses of Russian banks' clients from card fraud reached \$130 million in 2020, which is 10 times higher than similar losses in 2017⁴.

Anti-fraud tools can be roughly divided into directive, preventive, and detective. Directive tools such as instructions and warnings work like a scarecrow and only affect untrained fraudsters. Preventive tools help prevent fraud, but over time, fraudsters adapt and find ways to get around them. Detective tools are essential to detect fraud and minimize losses if fraud has not been prevented. Statistical approaches and machine learning methods are used to develop detective tools. However, there are unresolved problems in this area, such as instability and low generalizing ability of anti-fraud models, as well as high privacy of domain expertise(s).

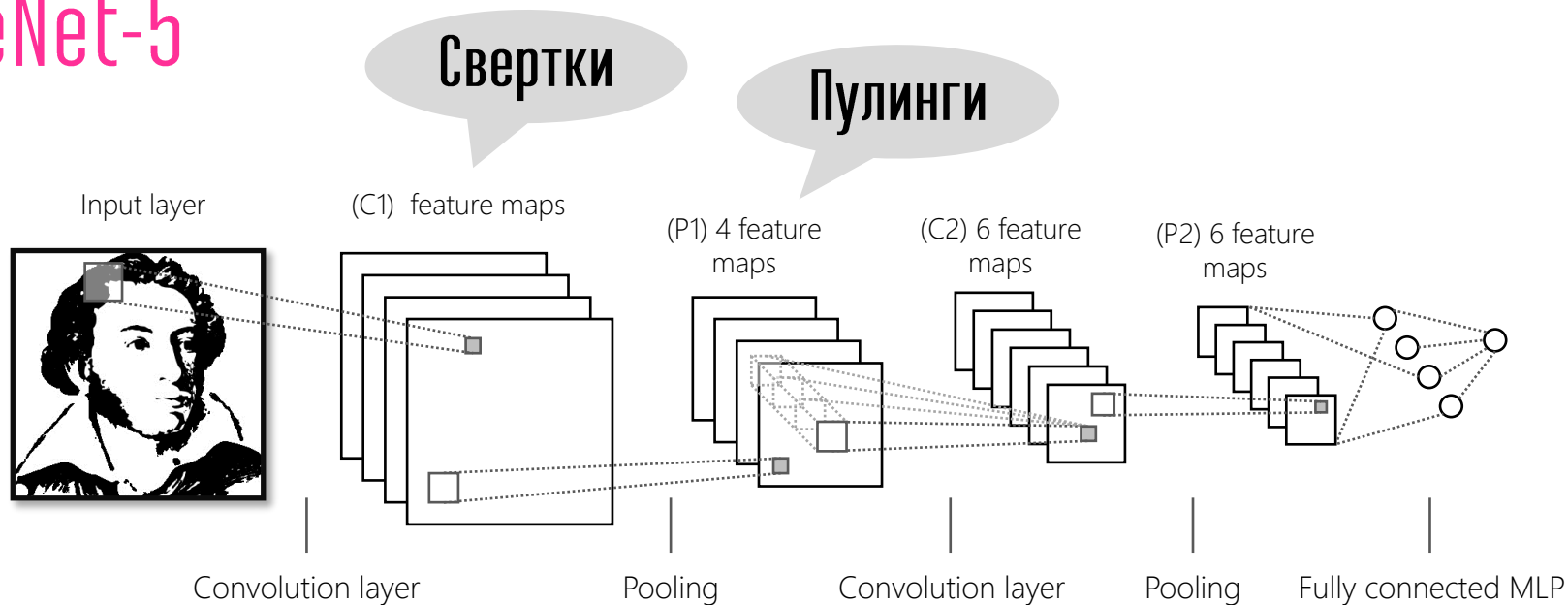
On the other hand, in recent years, we have seen outstanding advances in deep learning and the successful application of neural networks to practical tasks such as computer vision [21, 22, 34, 46] and natural language processing [19, 49, 51, 57, 58]. This gives us hope that innovative ideas proposed in deep learning will help to remove some of the issues in fraud detection modeling.

In this paper, we propose a convolutional neural network architecture SpiderNet designed to solve fraud detection problems. We noticed that convolutional and pooling layers principles are very similar to the methods of manual processing of information by anti-fraud analysts during investigations. In addition, skip-connections used in convolutional networks [22] make it possible to use features of various period, including fraud scores from external providers.

⁴https://cbr.ru/analytic/cif/losses/04_19487

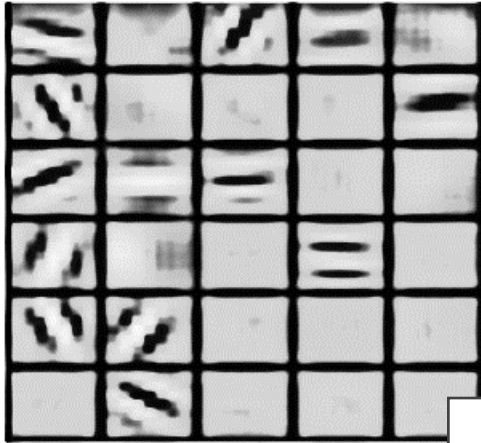


LeNet-5



Признаки выделяются нейронной сетью!

Feature Map1



Feature Map2



Feature Map3



CNN выделяют разные признаки

Высоко
частотные



Шумы, пиксели

Средне
частотные



Черточки, узоры

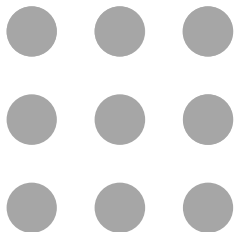
Низко
частотные



Цвета, текстуры

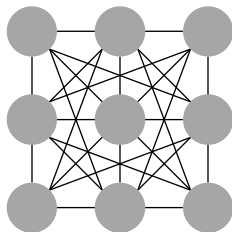
Ручная разработка fraud-правил

Признаки



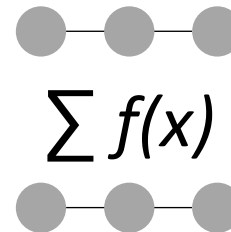
Analysts develop features for fraud detection based on the results of investigations (applications, behavior, anomalies, velocity, etc.)

Правила



Analysts build rules from features using machine learning methods: Decision Trees, Branch & Bound, Association Analysis etc.

Триггеры



Strong rules are selected from the rules using the iterative method to be included in fraud detection system

CNN в системах моделирования

2015 Credit-CNN, 2016 LSTM-CNN, 2018 DenseNet, 2020 Attention-CNN

Credit Card Fraud Detection Using Convolutional Neural Networks

Kang Fu, David Cheng, Yi Tu, and Lijiang Zhang^(*)

Key Laboratory of Shanghai Education Commission for Intelligent Information and Cognitive Engineering, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
{fukang1993,dawei_cheng_yi,tu1993,ljzhang}@sjtu.edu.cn

Abstract. Credit card is becoming more and more popular in financial transactions, at the same time frauds are also increasing. Conventional methods use rule-based expert systems to detect fraud behaviors, neglecting diverse situations, extreme imbalances of positive and negative samples. In this paper, we propose a CNN-based fraud detection framework, to capture the intrinsic patterns of fraud behaviors learned from labeled data. Abundant transaction data is represented by a feature matrix, on which a convolutional neural network is applied to identify a set of latent patterns for each sample. Experiments on real-world massive transactions of a major commercial bank demonstrate its superior performance compared with some state-of-the-art methods.

Keywords: Credit card fraud · Convolutional neural network · Imbalanced data

1 Introduction

With the rapid development of economy globalization in recent decades, credit cards are much more popular in commercial transactions. The corresponding problem of the credit card fraud emerges accordingly. Machine learning approaches have been proposed to overcome these challenges. Kakkimani [6] proposed the decision tree and boolean logic functions to characterize the normal transaction flows so as to detect fraudulent transactions. However, some of the fraudulent transactions similar to the legitimate trading patterns can not be identified. So neural networks and Bayesian networks have been employed. Ghosh [2] used a neural network to detect credit card frauds. Bayesian belief networks and artificial neural networks have been also introduced to tackle the problem [9]. These models have been criticized for being overly complex to detect frauds and there has been a high probability of being over-fitting. In order to reveal the latent patterns of fraudulent transactions and avoid the model over-fitting, we use a convolutional neural network to reduce the feature redundancy effectively.

How to generate features of credit card transactions successfully is one of the major challenges to machine learning approaches. Some aggregation strategies

© Springer International Publishing AG 2018.
A. Hesse et al. (Eds.): ECNP 2018, Part III, LNCS 10944, pp. 485–496, 2018.
DOI: 10.1007/978-3-319-60751-3_42

Spectrum-based deep neural networks for fraud detection

Shuhan Yuan
Tongji University
yuanshuhan@tongji.edu.cn

Jun Li
University of Oregon
lijun@uoregon.edu

Xintao Xu
University of Arkansas
xintaoxu@uark.edu

Aiding Lu
University of North Carolina at Charlotte
aiding.lu@uncc.edu

ABSTRACT. In this paper, we focus on fraud detection on a signed graph with only a small set of labeled training data. We propose a novel framework that combines deep neural networks and spectral graph analysis. In particular, we use the node projection (called as spectral coordinates) in the low-dimensional spectral space of the graph's adjacency matrix as input of deep neural networks. Spectral coordinates in the spectral space utilize the joint spatial-temporal information of the network. Due to the small dimensions of spectral coordinates compared with the dimensions of the adjacency matrix derived from a graph, training deep neural networks becomes feasible. We develop and evaluate two neural networks, deep autoencoder and convolutional neural network, in our fraud detection framework. Experimental results on a real signed graph show that our spectrum-based deep neural networks are effective in fraud detection.

Keywords: Node projection, spectrum, deep neural networks

1 INTRODUCTION

Online social networks (OSNs) have become popular social services for taking people together. Unfortunately, due to the openness of OSNs, fraudsters can also easily register themselves, inject fake contents, or take fraudulent activities, imposing severe security threats to OSNs and their legitimate participants. Many fraud detection techniques have been developed in recent years [1, 4, 5, 6], including content-based approaches and graph-based approaches. Different from content-based methods, graph-based methods (e.g., graph-based approaches like identifying frauds based on network topologies. Often based on supervised learning, the graph-based approaches consider that nodes and edges are labeled as either benign graphs associated with nodes, edges, user-id, or communities from the graph [2, 10].

In practice, a small set of labeled users are often available and hence supervised learning-based detection approaches could be developed. In this paper, we introduce deep neural network models for detecting frauds in signed graphs. These neural networks have achieved remarkable results in computer vision, natural language processing, and speech recognition [3, 7, 8, 12]. A deep neural network can learn different levels of representations on different layers of neural networks [1]. However, one challenge of applying deep neural networks for fraud detection is lack of sufficient labeled data. When deep neural networks with a high-dimensional input

have a large number of parameters, the deep neural networks need to be trained with a large training dataset [12]. Hence it is often infeasible to use the adjacency matrix of the underlying graph as input of deep neural networks because of the high dimensions of the adjacency matrix and the small number of labeled users. To propose a novel framework that combines spectral graph analysis with the deep neural networks. In particular, we first project a graph with its spectral space by the principal eigenvectors of its adjacency matrix. The spectral space captures the most topological information of the graph. Each node is then mapped to a low-dimensional point (called spectral coordinates) in the spectral space. We then use each node's spectral coordinates together with the aggregate information of its neighbor nodes' spectral coordinates as the input of the deep neural network models. Deep autoencoder and convolutional neural networks are as follows. First, using both spectral graph analysis and deep neural networks, we can avoid labeling graph nodes themselves to identify the difference between fraudulent and regular users. Second, the low-dimensional spectral space contains the most useful topology information of a graph. Compared with the adjacency matrix, the dimension of spectral coordinates of nodes is much lower. Thus, using the node spectral coordinates as inputs to deep neural networks, we can avoid labeling graph nodes themselves to identify the difference between fraudulent and regular users. While our framework covers signed graphs in order to capture both positive and negative relationships between nodes in the signed graph, inputs of the two deep neural networks are composed of combination spectral coordinates of the node and its positive/negative connected neighbors.

2 MODELS

2.1 Framework. Given a signed undirected graph G , each node i indicates either a regular user or a fraudster. The signed graph G can be represented as a symmetric adjacency matrix A_{ij} , where i is the index of nodes. In A_{ij} , $A_{ij} = 1$ ($A_{ij} = -1$) indicates that i is positive (negative) edge between nodes i and j , and $A_{ij} = 0$ indicates no edge. Also, i is a real eigenvalue. Let $\{u_i\}$ be the i -th largest eigenvalue of A with eigenvalue λ_i , $i = 1, 2, \dots, n$. The spectral decomposition of A is $A = U \Lambda U^T$, where U is Figure 1. There usually exist k leading eigenvalues that are significantly greater than the rest ones of the network. The row vector $u_i = [u_{i1}, u_{i2}, \dots, u_{in}]$

Multi-Scale DenseNet-Based Electricity Theft Detection

Bo Li¹, Kele Xu^{1,2}, Xianyan Cui^{1*}, Yihang Wang², Xinbo Ai¹, Yimbo Wang²

1. Beijing University of Posts and Telecommunications,
Beijing, 100876, China

deephui_126@mails.bnu.edu.cn

2. School of Computer, National University of Defense Technology,
Changsha, 410073, China

cxieie_sdu@ali.com

3. School of Information Communication, National University of Defense Technology,
Wuhan, 430015, China

4. The University of Melbourne, Parkville, 3010, Australia

yihang@itdcs.unimelb.edu.au, austin

3. Jilin Mining Bank,
Beijing 100013, China

wangyibo@cnbc.com.cn

Electricity theft detection issue has drawn lots of attention during last decades. Timely identification of the electricity theft in the power system is crucial for the safety and availability of the system. Although sustainable efforts have been made, the detection task remains challenging and falls short of accuracy and efficiency, especially with the increase of the data size. Recently, convolutional neural network-based methods have achieved better performance in comparison with traditional methods, which employ handcrafted features and shallow-architecture classifiers. In this paper, we present a novel approach for automatic detection of electricity theft in the multi-scale dense connected convolution neural network (multi-scale DenseNet) in order to capture the long-term and short-term periodic features within the sequential data. We compare the proposed approaches with the classical algorithms, and the experimental results demonstrate that the multi-scale DenseNet approach can significantly improve the accuracy of the detection. However, our method is scalable, enabling larger data processing while no handcrafted feature engineering is needed.

* Corresponding author

The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI 2020)

Spatio-Temporal Attention-Based Neural Network for Credit Card Fraud Detection

Dawei Cheng, Sheng Xiang, Chengcheng Zhang,

Yili Zhang, Fangzhou Yang, Lijiang Zhang^{*}

Mid-Ji Lab of Artificial Intelligence, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
{dawei_cheng, yili_zhang, lijiang_zhang, yfzhang}@sjtu.edu.cn

Abstract

Credit card fraud is an important issue and incurs a considerable cost for both cardholders and issuing institutions. Contemporary methods apply machine learning based approaches to detect fraudulent behavior from transaction records. But manually generating features needs domain knowledge and may be behind the massive growth of data, which means we need to automatically focus on the most relevant patterns in fraudulent behavior. Therefore, in this work, we propose a spatio-temporal attention-based neural network to model the fraud behaviors. In particular, transaction records are modeled by the graph structure and analyzed by integrating the comprehending information, including spatial and temporal behaviors. Attention weights are jointly learned in an end-to-end transaction flows, the result shows that STAN performs better than other state-of-the-art baselines in both AUC and precision-recall curves. Moreover, we conduct empirical studies with domain experts on the proposed method for fraud pattern analysis, the result demonstrates the effectiveness of our proposed method in both detecting suspicious transactions and mining fraud patterns.



Figure 1: The framework of credit card fraud detection.

and feedback the analysis results to the predictive model for model updating.

An attacking strategies from potential fraudsters change, it is essential that a well-balanced system can adapt to the evolving patterns of fraud behaviors [4, 2018, Tang et al. 2018]. We summarize the following five major observations from the fraud patterns in transaction records. 1) *Temporal aggregation*: fraudulent transactions are subject to the limited time of the activities. As the cardholder will freeze the card as soon as possible once suspicious transactions have been detected, fraudsters are required to reach the credit limit in a short time. That means the behaviors of the fraud transactions would be exposed in a limited time. 2) *Spatial aggregation*: fraudsters are subject to use the device and mechanics of transactions. That is, due to the economic constraints, fraudsters will use the card frequently with only a small number of merchants, which are spatially different from normal transactions.

Many existing models to deal with fraud transactions have been extensively studied (Pardalos, Sharda, and others 2011; Bahmani et al. 2016; Carmona, Figueira, and Costa 2017). They mainly split into one of two distinct types. 1) *Rule-based methods* directly generate sophisticated rules by domain experts for identification, for example, (Sejic and Zarempski 2014) proposed an association rules method for mining credit fraud rules. 2) *Machine learning based methods* learn static models by exploring large amounts of historical data. For example, (Frost et al. 2017) explored features based on neural networks and built supervised classifiers for detecting

Credit Card Fraud Detection Using Convolutional Neural Networks

Kang Fu, Dawei Cheng, Yi Tu, and Liqing Zhang^(✉)

Key Laboratory of Shanghai Education Commission for Intelligent Interaction and Cognitive Engineering, Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai, China
{fukang1993,dawei.cheng,tuyi1991,lqzhang}@sjtu.edu.cn

Abstract. Credit card is becoming more and more popular in financial transactions, at the same time frauds are also increasing. Conventional methods use rule-based expert systems to detect fraud behaviors, neglecting diverse situations, extreme imbalance of positive and negative samples. In this paper, we propose a CNN-based fraud detection framework, to capture the intrinsic patterns of fraud behaviors learned from labeled data. Abundant transaction data is represented by a feature matrix, on which a convolutional neural network is applied to identify a set of latent patterns for each sample. Experiments on real-world massive transactions of a major commercial bank demonstrate its superior performance compared with some state-of-the-art methods.

Keywords: Credit card fraud · Convolutional neural network · Imbalanced data

1 Introduction

With the rapid development of economy globalization in recent decades, credit cards are much more popular in commercial transactions. The corresponding problem of the credit card fraud emerges accordingly. Machine learning approaches have been proposed to overcome these challenges. Kokkinaki [4] proposed the decision tree and boolean logic functions to characterize the normal transaction modes so as to detect fraudulent transactions. However, some of the fraudulent transactions similar to the legitimate trading patterns can not be identified. So neural networks and Bayesian networks have been employed. Ghosh [2] used a neural network to detect credit card frauds. Bayesian belief networks and artificial neural networks have been also introduced to tackle the problem [6]. These models have been criticized for being overly complex to detect frauds and there has been a high probability of being over-fitting. In order to reveal the latent patterns of fraudulent transactions and avoid the model over-fitting, we use a convolutional neural network to reduce the feature redundancy effectively.

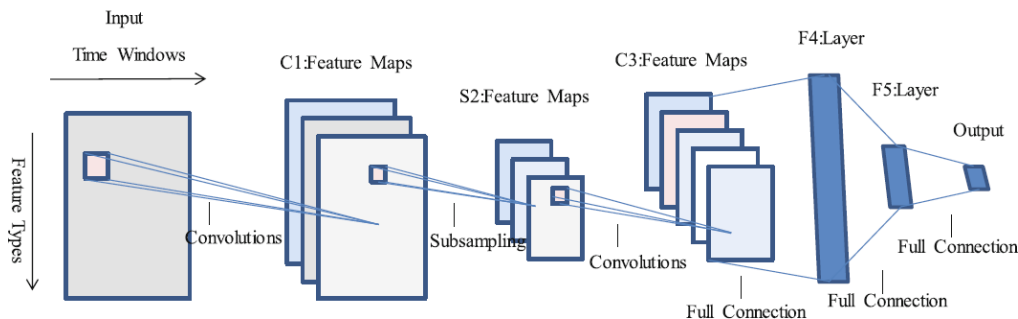
How to generate features of credit card transactions successfully is one of the major challenges to machine learning approaches. Some aggregation strategies

© Springer International Publishing AG 2016
A. Hesse et al. (Eds.): ICONIP 2016, Part III, LNCS 9949, pp. 483–490, 2016.
DOI: 10.1007/978-3-319-46675-0_23

Kang Fu
Dawei Cheng & ko

2016

Convolutional Neural Networks



2017

Learning Temporal Representation of Transaction Amount for Fraudulent Transaction Recognition using CNN, Stacked LSTM, and CNN-LSTM

Yaya Heryadi¹, Harco Leslie Hendric Spits Warnars²

Computer Science Department, BNUIS Graduate Program – Doctor of Computer Science

Bina Nusantara University

Jakarta, Indonesia 11480

yayaheryadi@bnuis.edu.id¹, spits.hendric@bnuis.ac.id²

Abstract—This paper aims to explore deep learning model to learn short-term and long-term patterns from imbalanced input dataset. Data for this study are imbalanced card transactions from an Indonesia bank in period 2016-2017 with binary labels (nonfraud or fraud). From 50 features of the dataset, 30 principal components of data contribute to 97.4% of the cumulative Eigenvalues. This study explores the effect of fraud in fraud sample ratio from 1 to 4 and three models: Convolutional Neural Network (CNN), Stacked Long Short-term Memory (LSTM), and Hybrid of CNN-LSTM. Using Area Under the ROC Curve (AUC) as model performance, CNN achieved the highest AUC for R-L2.4 followed by St-LSTM and CNN-LSTM.

Keywords—fraudulent recognition, imbalanced data classification, CNN, LSTM, CNN-LSTM.

I. INTRODUCTION

The issue of fraudulent card financial transaction, such as credit card and debit card transaction, continues to gain wide attention from various research communities due to its negative impact to financial loss and reputation damage to the banks as card issuers. Despite many technologies have been proposed to prevent and detect fraudulent transaction using cards, fraudulent transactions are still prevalent due to its popularity and ubiquitous of financial transaction facilities.

Fraudulent transaction recognition problem is an interesting but challenging computer vision problem due to its imbalanced data in nature. In the past ten years, many studies to address fraudulent transaction recognition have been reported resulted in a plethora of methods to develop a robust classifier that maximize classification accuracy and minimize two aspects: (1) false positive which disrupt customers or merchants or banks, and (2) false negative which ruined prudent image of bank can be minimized.

In general, fraudulent transaction recognition methods can be divided broadly into two categories (1) *First*, supervised approach: models are trained to learn patterns from a given labeled samples of fraudulent and non-fraudulent transaction. Second, unsupervised approach: models are trained to detect unusual or anomalous transactions from training dataset. The premise of this approach is that anomalous transaction might be potential cases of fraudulent transactions [2]. Given the trained

models, fraudulent transaction recognition aims to predict probability of fraudulent transaction label.

The successful result of using machine learning to solve classification problems in many domains have concerned many researchers to use these models to recognize fraudulent transactions [3]. Many methods have been proposed such as: Random forest [4] [5], Decision Tree [6], K-Nearest Neighbors [7], SVM [8] [9], HMM [10], neural networks [11], Bayesian learning [11], artificial immune systems [12], association rules [13], hybrid models [14], discriminant analysis [15]. Most of these researches are typically preceded by preliminary studies to extract features from historical financial transaction data that represent the pattern of buying behavior or financial transaction of the customers. Financial transaction is data represented by a set of features as input to machine learning models.

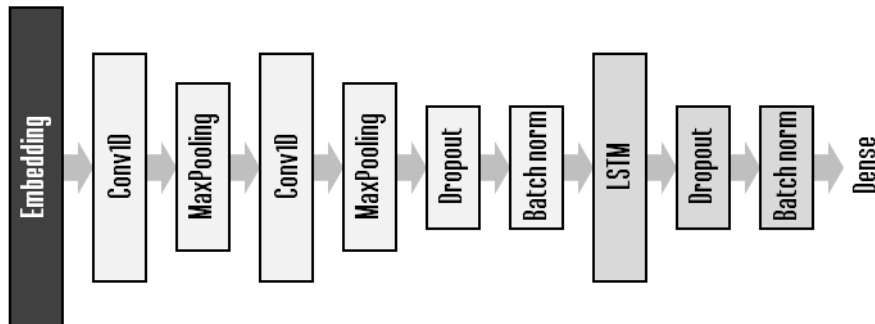
The challenges of fraudulent transaction recognition are mainly: (1) no feature standard to represent financial transaction; (2) the imbalanced data distribution of fraudulent and non-fraudulent transaction. Hence, the number of fraudulent transactions is less than the number of non-fraudulent cases; (3) less availability of dataset to validate models proposed by previous studies due to banking confidential reason; and (4) less separability of fraudulent and non-fraudulent transactions as fraudulent card users is typically mimic their consumer behavior closed to non-fraudulent ones.

This study, therefore, aims to: (1) propose a robust financial transaction features that can separate fraudulent and non-fraudulent class samples and (2) propose a robust classifier by exploring hybrid CNN-LSTM model. Following [16], CNN in the proposed model is used to capture short-term financial transaction features; whilst, LSTM on top of CNNs is used to capture longer-term temporal financial transaction. The models under study are then tested using debit card transaction from a local Indonesia bank under perturbation. The main contribution of this paper is mainly showing empirical results that neither CNN nor LSTM is capable to model financial transaction as each of these models only capable to capture either short-term or long-term temporal transaction patterns.

The remaining paper is structured as follows. Section II will describe several related works. Section III will explain the

Yaya Heryadi Harco Warnars

CNN-LSTM



Multi-Scale DenseNet-Based Electricity Theft Detection

Bo Li¹, Kele Xu^{2,3}, Xiaoyan Cui^{1*}, Yiheng Wang⁴, Xinbo Ai¹, Yanbo Wang⁵

1. Beijing University of Posts and Telecommunications,
Beijing, 100876, China

2. School of Computer, National University of Defense Technology,
Changsha, 410073, China
kelele.xu@gmail.com

3. School of Information Communication, National University of Defense Technology,
Wuhan, 430015, China

4. The University of Melbourne, Parkville, 3010, Australia
yihengw1@student.unimelb.edu.au

5. China Minsheng Bank,
Beijing 100031, China
wangyanbo@cmbc.com.cn

Electricity theft detection issue has drawn lots of attention during last decades. Timely identification of the electricity theft in the power system is crucial for the safety and availability of the system. Although sustainable efforts have been made, the detection task remains challenging and falls short of accuracy and efficiency, especially with the increase of the data size. Recently, convolutional neural network-based methods have achieved better performance in comparison with traditional methods, which employ handcrafted features and shallow-architecture classifiers. In this paper, we present a novel approach for automatic detection by using a multi-scale dense connected convolution neural network (multi-scale DenseNet) in order to capture the long-term and short-term periodic features within the sequential data. We compare the proposed approaches with the classical algorithms, and the experimental results demonstrate that the multi-scale DenseNet approach can significantly improve the accuracy of the detection. Moreover, our method is scalable, enabling larger data processing while no handcrafted feature engineering is needed.

* Corresponding author

Bo Li, K. Xu, X. Cui,
Y. Wang, X. Ai, Y. Wang

2018

Multi-scale DenseNet

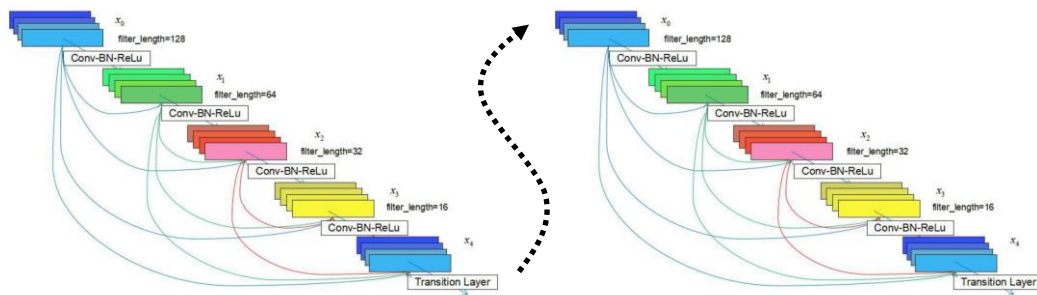


Fig. 1. Multi-scale dense block

Fig. 1. Multi-scale dense block

Spatio-Temporal Attention-Based Neural Network for Credit Card Fraud Detection

Dawei Cheng, Sheng Xiang, Chencheng Shang,
Yi Zhang, Fangzhou Yang, Liqing Zhang*

MoE Key Lab of Artificial Intelligence, Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai, China
{dawei.cheng, y95y1, lake.titica}@sjtu.edu.cn, zhang-lq@cs.sjtu.edu.cn

Abstract

Credit card fraud is an important issue and incurs a considerable cost for both cardholders and issuing institutions. Contemporary methods apply machine learning-based approaches to detect fraudulent behavior from transaction records. But manually generating features needs domain knowledge and may lag behind the needs of fraud, which means we need to automatically focus on the most relevant patterns in fraudulent behavior. Therefore, in this work, we propose a spatio-temporal attention-based neural network (STAN) for fraud detection. In particular, transaction records are modeled by attention and 3D convolution mechanisms by integrating the corresponding information, including spatial and temporal behaviors. Attentional weights are jointly learned in an end-to-end manner with 3D convolution and detection networks. Afterward, we conduct extensive experiments on real-world fraud transaction dataset, the result shows that STAN performs better than other state-of-the-art baselines in both AUC and precision-recall curves. Moreover, we conduct empirical studies with domain experts on the proposed method for fraud post-analysis, the result demonstrates the effectiveness of our proposed method in both detecting suspicious transactions and mining fraud patterns.

Introduction

Credit card fraud is a general term for the unauthorized use of funds in a transaction typically through a credit or a debit card (Bhattacharyya et al. 2011). Global card fraud losses amounted to over 25 billion US dollars in 2018 and is forecast to continue to increase (Wang, Chen, and Chen 2019). This huge amount of losses has increased the importance of fraud-fighting. Figure 1 shows a typical fraud detection framework deployed in a commercial system. The card alliance or banks, such as VISA, MasterCard or Citibank, assess each transaction with an online predictive model once it has passed card checking. Unlike a simple card checking system, which focuses on card blacklists, budget checking, etc., the predictive model is designed to detect fraud patterns automatically and produces a fraud risk score. Investigators can thereby focus on the high-risk transactions effectively.

*Corresponding Author
Copyright © 2020, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.

362



Figure 1: The framework of credit card fraud detection.

and feedback the analysis results to the predictive model for model updating.

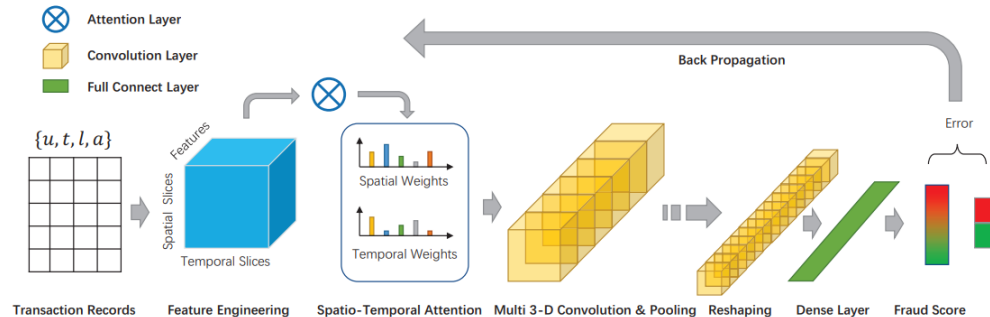
As attacking strategies from potential fraudsters change, it is essential that a well-behaved system can adapt to the evolving strategies (Randhawa et al. 2018; Jiang et al. 2018). We summarize the following two major observations from real-world fraud transactions: 1). *Temporal aggregation*. Fraudsters are subject to the limited time of the activities. As the cardholder will freeze the card as soon as possible once suspicious transactions have been detected, fraudsters are required to reach the credit limit in a short time. That means the behaviors of the fraud transaction would be exposed in a limited time. 2). *Spatial aggregation*. Fraudsters are subjected to cost on the devices and merchants of transactions. That is, due to the economic constraints, fraudsters will use the card frequently with only a small number of merchants, which are spatially different from normal transactions.

Many existing models to deal with fraud transactions have been extensively studied (Putdar, Sharma, and others 2011; Balasen et al. 2016; Carneiro, Figueira, and Costa 2017). They mainly split into one of two directions: 1). *Rule-based methods* directly generate sophisticated rules by domain experts for identification; for example, (Sejra and Zarempoor 2014) proposed an association rules method for mining frequent fraud rules. 2). *Machine learning-based methods* learn static models by exploring large amounts of historical data. For example, (Flore et al. 2017) extracted features based on neural networks and built supervised classifiers for detecting

D. Cheng, S. Xiang, C. Shang,
Y. Zhang, F. Yang, L. Zhang

2020

Attention-CNN



Ключевые идеи для нейросети

1. Нейросеть умеет из слабых признаков создавать сильные
2. Из разных признаков нейросеть умеет выбирать топ-сильных
3. Сильные признаки должны сразу пробрасываться на выходные слои

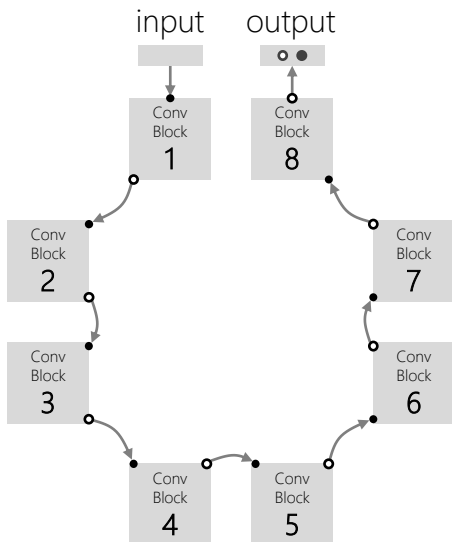
convolutional

pooling

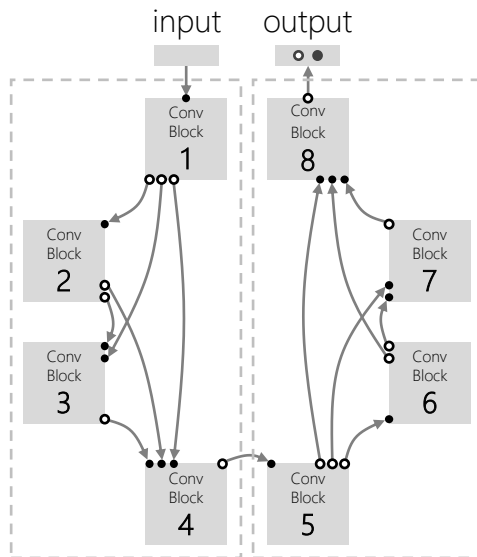
skip-connection

Сравнение CNN-архитектур

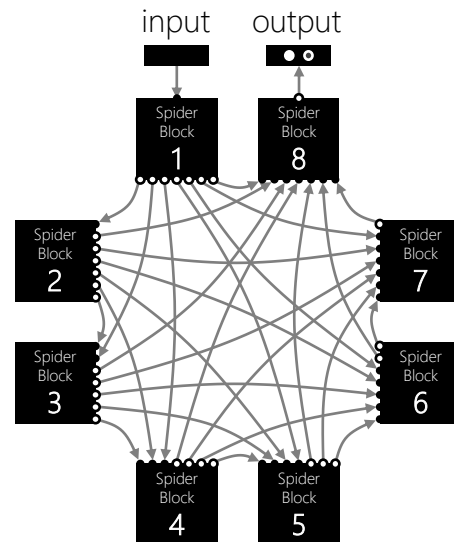
CNN



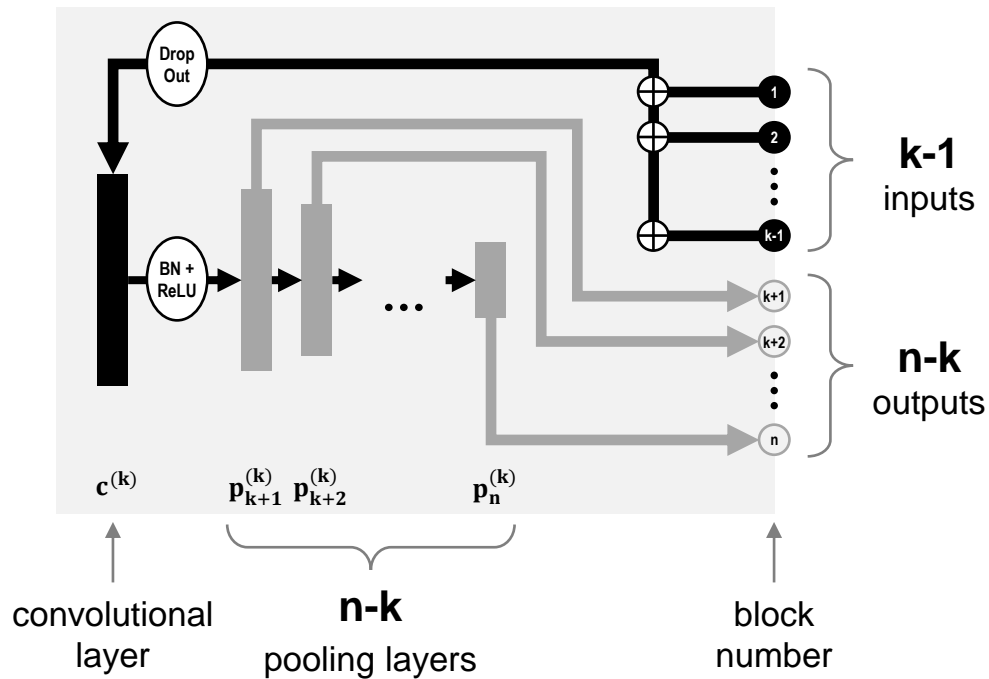
DenseNet



SpiderNet

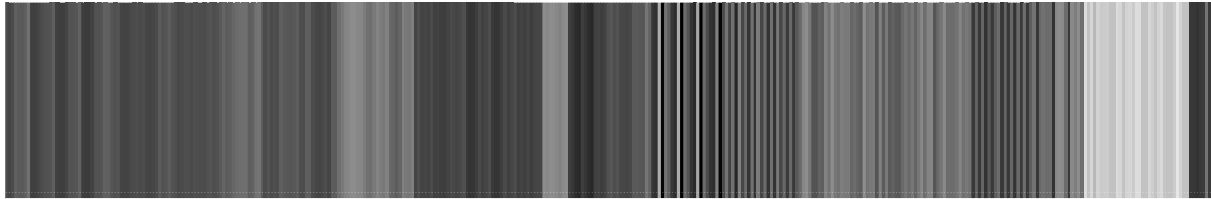


k-тый блок нейронной сети SpiderNet

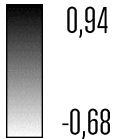
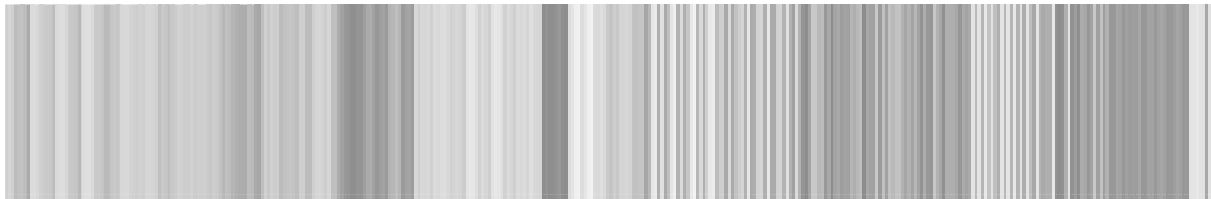


Как CNN видит мошеннические ТТ

a) Top-10 fraudulent POS-partners of the bank

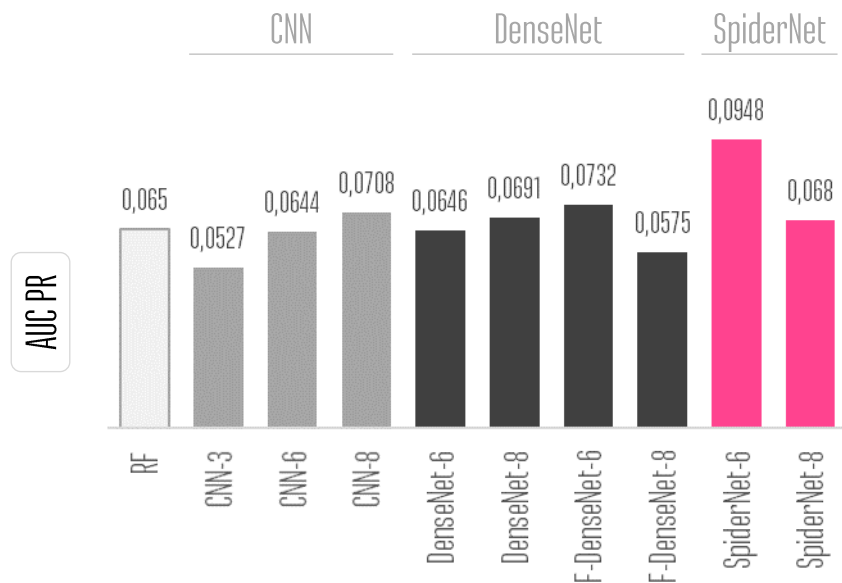


b) Top-10 non-fraudulent POS-partners of the bank

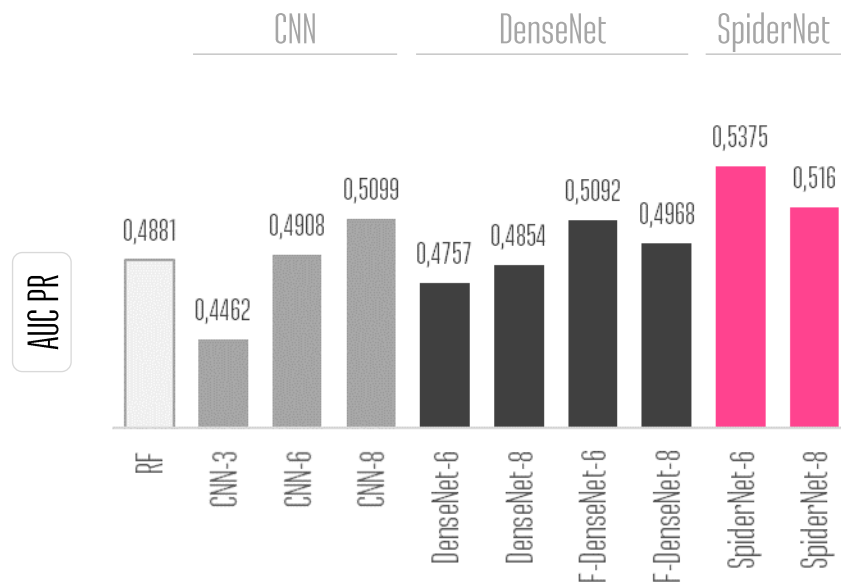


Результаты экспериментов

POS-мошенничество



Онлайн платежи (Alibaba)



Statistical Fraud Detection: A Review

Richard J. Bolton and David J. Hand

Abstract. Fraud is increasing dramatically with the expansion of modern technology and the global superhighways of communication, resulting in the loss of billions of dollars worldwide each year. Although prevention technologies are the best way to reduce fraud, fraudsters are adaptive and, given time, will usually find ways to circumvent such measures. Methodologies for the detection of fraud are essential if we are to catch fraudsters once fraud prevention has failed. Statistics and machine learning provide effective technologies for fraud detection and have been applied successfully to detect activities such as money laundering, e-commerce credit card fraud, telecommunications fraud and computer intrusion, to name but a few. We describe the tools available for statistical fraud detection and the areas in which fraud detection technologies are most used.

Key words and phrases: Fraud detection, fraud prevention, statistics, machine learning, money laundering, computer intrusion, e-commerce, credit cards, telecommunications.

1. INTRODUCTION

The *Concise Oxford Dictionary* defines fraud as "criminal deception, the use of false representations to gain an unjust advantage." Fraud is as old as humanity itself and can take an unlimited variety of different forms. However, in recent years, the development of new technologies (which have made it easier for us to communicate and helped increase our spending power) has also provided yet further ways in which criminals may commit fraud. Traditional forms of fraudulent behavior such as money laundering have become easier to perpetrate and have been joined by new kinds of fraud such as mobile telecommunications fraud and computer intrusion.

We begin by distinguishing between fraud prevention and fraud detection. Fraud prevention describes measures to stop fraud from occurring in the first place. These include elaborate designs, fluorescent fibers, multitone drawings, watermarks, laminated metal strips and holographs on banknotes, personal

identification numbers for bankcards, Internet security systems for credit card transactions, Subscriber Identity Module (SIM) cards for mobile phones, and passwords on computer systems and telephone bank accounts. Of course, none of these methods is perfect and, in general, a compromise has to be struck between expense and inconvenience (e.g., to a customer) on the one hand, and effectiveness on the other.

In contrast, fraud detection involves identifying fraud as quickly as possible once it has been perpetrated. Fraud detection comes into play once fraud prevention has failed. In practice, of course fraud detection must be used continuously, as one will typically be unaware that fraud prevention has failed. We can try to prevent credit card fraud by guarding our cards assiduously, but if nevertheless the card's details are stolen, then we need to be able to detect, as soon as possible, that fraud is being perpetrated.

Fraud detection is a continuously evolving discipline. Whenever it becomes known that one detection method is in place, criminals will adapt their strategies and try others. Of course, new criminals are also constantly entering the field. Many of them will not be aware of the fraud detection methods which have been successful in the past and will adopt strategies which lead to identifiable frauds. This means that the earlier detection tools need to be applied as well as the latest developments.

Richard J. Bolton is Research Associate in the Statistics Section of the Department of Mathematics at Imperial College. David J. Hand is Professor of Statistics in the Department of Mathematics at Imperial College, London SW7 2BZ, United Kingdom (e-mail: r.bolton, d.j.hand@ic.ac.uk).

Richard J. Bolton David J. Hand

2002

1.

Мошенничество растет с развитием современных технологий

2.

Превентивные меры рано или поздно обходятся => нужны детективные инструменты

3.

Детективные алгоритмы тоже со временем обходят => их надо постоянно развивать

4.

Методики антифрода закрыты – это затрудняет исследование и развитие антифрода

Statistical Fraud Detection: A Review

Richard J. Bolton and David J. Hand



Comment

Foster Provost

The state of research on fraud detection recalls John Godfrey Saxe's 19th-century poem "The Blind Men and the Elephant" (Felleman, 1936, page 521). Based on a Hindu fable, each blind man experiences only a part of the elephant, which shapes his opinion of the nature of the elephant: the leg makes it seem like a tree, the tail a rope, the trunk a snake and so on. In fact, "...though each was partly in the right... all were in the wrong." Saxe's poem was a criticism of theological debates, and I do not intend such a harsh criticism of research on fraud detection. However, because the problem is so complex, each research project takes a particular angle of attack, which often obscures the view of other parts of the problem. So, some researchers see the problem as one of classification, others of temporal pattern discovery; to some it is a problem perfect for a hidden Markov model and so on.

So why is fraud detection not simply classification or a member of some other already well-understood problem class? Bolton and Hand outline several characteristics of fraud detection problems that differentiate them [as did Tom Fawcett and I in our review of the problems and techniques of fraud detection (Faw-



Comment

Leo Breiman

This is an enjoyable and illuminating article. It deals with an area that few statisticians are aware of, but that is of critical importance economically and in terms of security. I am appreciative to the authors for the education in fraud detection this article gave me and to *Statistical Science* for publishing it. There are some interesting aspects that make this class of problems unique and that I comment on, running the risk of repeating points made in the article.

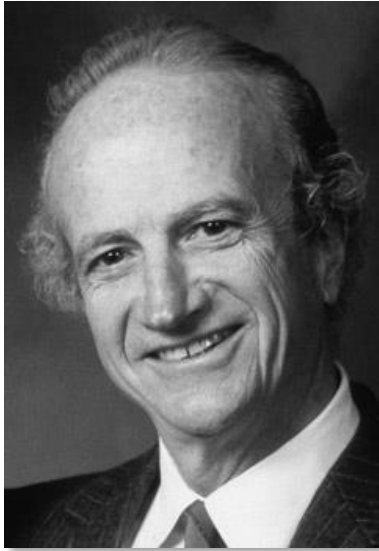
The analysis has to deal with a large number of problems simultaneously. For instance, in credit card fraud, the records of millions of customers have to be analyzed one by one to set up individual alarm settings. It is not a single unsupervised or supervised problem—a multitude of such problems have to be simultaneously addressed and "solved" for diverse data records. Yet the algorithm selected, modulo a few tunable parameters, has to be "one size fits all." Otherwise the on-line computations are not feasible. The alarm bell settings have to be constantly updated. For instance, as customers age and change their economic level and life styles, usage characteristics change. There are also serious database issues—how to structure the large databases so that the incoming streams of data are acces-

Foster Provost Leo Breiman

2002

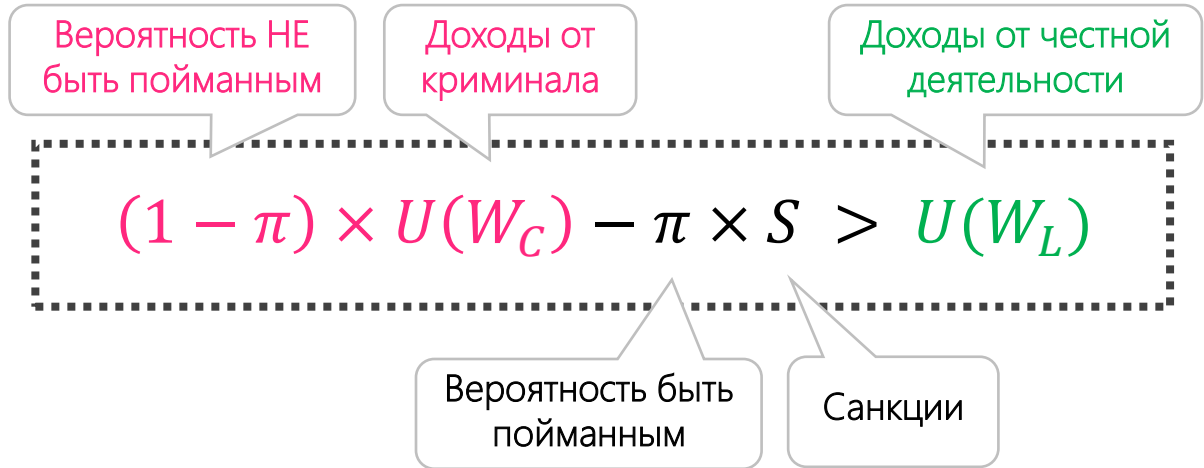
5. Мошенники быстро адаптируются => качество алгоритмов падает после внедрения
6. Часто алгоритм настраивается под конкретную схему, хотя нужно думать о глобальной задаче
7. Для разработки эффективных алгоритмов нужны большие данные
8. Выбор алгоритма не решает проблему, необходимо глубокое изучение данных

Экономика преступления и наказания



Гэри Беккер
(1930–2014)

Преступность можно рассматривать как специфичный рынок, на котором существует спрос и предложение



Формула Беккера для социнженерии

Нужно чтобы вероятность выявления
мошенничества стремилась к 100%!!!

$$(1 - \pi_c) \times U(W_{cr}) - \boxed{\pi_d \times S_f} - \pi_c \times S_c > U(W_L)$$

Diagram illustrating the formula with annotations:

- A pink arrow points from π_c in $(1 - \pi_c)$ to a pink 0 .
- A pink arrow points from π_c in $\pi_c \times S_c$ to a pink 0 .
- A black arrow points upwards from the boxed term $\pi_d \times S_f$.
- A black arrow points downwards from the boxed term $\pi_d \times S_f$.

Сумма фрод-платежей



«Закроешь одну контору –
возникнет ещё пять»

«Телефонное мошенничество и
костюмы на Хэллоуин для
питомцев – единственные
растущие индустрии в Америке»

Спасибо за
внимание!

Афанасьев Сергей

Вице-президент

Начальник управления
статистического анализа

КБ «Ренессанс Кредит»