

실시간 리샘플링 기법을 활용한 LSTM 기반의 사기 거래 탐지 시스템

김서이¹, 이연지², 이일구³

¹성신여자대학교 미래융합기술공학과 석사과정

²성신여자대학교 융합보안공학과 박사과정

³성신여자대학교 융합보안공학과, 미래융합기술공학과 부교수

cheonrang01@gmail.com, cselab.lyj@gmail.com, iglee@sungshin.ac.kr

LSTM-based fraud detection system framework using real-time data resampling techniques

Seo-Yi Kim¹, Yeon-Ji Lee², Il-Gu Lee^{1,2}

¹Dept. of Future Convergence Technology Engineering, Sungshin Women's University

²Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

금융산업의 디지털 전환은 사용자에게 편리함을 제공하지만 기존에 존재하지 않던 보안상 취약점을 유발했다. 이러한 문제를 해결하기 위해 기계학습 기술을 적용한 사기 거래 탐지 시스템에 대한 연구가 활발하게 이루어지고 있다. 하지만 모델 학습 과정에서 발생하는 데이터 불균형 문제로 인해 오랜 시간이 소요되고 탐지 성능이 저하되는 문제가 있다. 본 논문에서는 실시간 데이터 오버샘플링을 통해 이상 거래 탐지 시 데이터 불균형 문제를 해결하고 모델 학습 시간을 개선한 새로운 이상 거래 탐지 시스템(Fraud Detection System, FDS)을 제안한다. 본 논문에서 제안하는 SMOTE(Synthetic Minority Oversampling Technique)를 적용한 LSTM(Long-Short Term Memory) 알고리즘 기반의 FDS 프레임워크는 종래의 LSTM 알고리즘 기반의 FDS 모델과 비교했을 때, 데이터 사이즈가 96.5% 감소했으며, 정밀도, 재현율, F1-Score가 34.81%, 11.14%, 22.51% 개선되었다.

1. 서론

금융 산업의 디지털 전환은 금융 서비스의 편리한 이용을 촉진했지만, 동시에 새로운 문제를 야기하였다. 기존에 대면 방식으로 진행되던 금융 업무 서비스를 비대면으로 이용하게 되면서 발생한 전자 금융 거래 방식의 비대면 인증 방식 취약점을 이용한 신종 사기 수법이 등장하면서, 지능적인 금융 사기에 의한 피해가 증가하고 있다. 이 문제를 해결하기 위해 기계학습 기반의 이상 거래 탐지 시스템(Fraud Detection System, FDS)을 구축하는 연구들이 활발하게 이루어지고 있다[1]. 그러나 정확한 사기 거래 예측과 탐지를 위해 해결해야 할 다양한 과제들이 남아있다.

국가통계포털(KOSIS)에 따르면 2024년 2월을 기준으로 금융 공동망에 집계된 데이터는 약 10억 7천만건으로 수집되는 데이터의 양이 방대하다[2]. 그러나 이 중 사기 거래 데이터는 전체의 극히 일부를 차지하기 때문에 이 데이터를 그대로 학습에 사용할 경우에 데이터 불균형으로

인한 탐지성능 저하 문제가 발생할 수 있다. 데이터 불균형 문제는 데이터 샘플링을 통해 완화 가능하며, 그중 데이터 과적합 방지 및 성능 향상을 위해 오버샘플링(Oversampling) 방식이 선호된다. 하지만 오버샘플링의 경우 데이터셋의 크기가 커지기 때문에 학습 시간 측면에서 비효율적이다.

본 논문에서는 앞서 언급한 문제를 해결하기 위해 부족한 사기 거래 데이터를 오버샘플링하는 동시에 정상 데이터를 다운샘플링(Downsampling)하여 실시간 데이터 샘플링 기법 제안하고, 이를 적용한 LSTM(Long-Short Term Memory) 기반의 FDS 프레임워크를 제안한다. 제안 방법은 최소한의 사기 거래 데이터가 수집되면 실시간 오버샘플링 혹은 다운샘플링하고, 이를 통해 데이터 불균형을 해소한다. 이후 LSTM 알고리즘을 이용하여 긴 시계열 데이터를 효과적으로 처리한다. 이를 통해 최소한의 사기 거래 데이터를 이용하여 빠르고 효과적인 사기 거래 탐지가 가

능하다.

본 논문은 다음과 같이 구성되어 있다. 2장에서 종래의 LSTM 기반의 사기 거래 탐지 기술을 소개하고 한계점을 분석한 후, 이를 개선하기 위한 제안 기술을 3장에서 소개한다. 4장에서 제안 기술의 성능을 입증하기 위한 시뮬레이션 결과를 분석한 후, 5장에서 결론을 맺는다.

2. LSTM 알고리즘을 이용한 사기거래 탐지

Ibtissam Benchaji 의 연구[3]에서는 Attention 메커니즘과 LSTM 알고리즘을 결합하여 모델 학습 시 관련성이 높은 데이터에 가중치를 적용한 이상 거래 탐지 모델을 제안했다. 적합한 피쳐 선택을 위해 균일 매니폴드 근사 및 투영 (Uniform Manifold Approximation and Projection, UMAP) 방식을 이용했고, 데이터 불균형 문제를 해결하기 위해서 SMOTE(Synthetic Minority Oversampling Technique) 오버샘플링 방식을 이용했다. 제안한 방식을 LSTM, SVM(Support Vector Machine) 및 ANN(Artificial Neural Network) 과 비교했으며, Recall 값이 약 13% 향상된 결과를 보였다. 하지만 해당 모델은 예측 성능을 향상시키기 위해 여러 단계가 추가되었으며 계산 오버헤드 및 지연시간 측면을 고려하지 못했다.

Mohmad, Yanash Azwin 의 연구[4]에서는 신용 거래 채무 이행 여부에 대한 예측 모델을 제안했다. LSTM 알고리즘을 이용하여 고객의 신용 거래 데이터로 신용 점수 계산을 자동화하고, 이를 기반으로 추후 채무 불이행에 대한 조기 경보를 발생시켰다. 분류 정확도를 개선하기 위해 K-겹 교차 검증(K-fold cross validation) 기법(K=5)을 이용하여 데이터 셋을 분할했으며, 시계열 데이터 처리를 위해 LSTM 알고리즘을 이용하여 모델을 학습했다. 기존 단일 모델과의 성능 비교를 위해 정규성 검정(Kolmogorov-Smirnov test), Brier score, 검량선 제어(Calibration curves control) 등을 수행했으며, 대부분의 지표에서 약 1% 내외의 성능을 개선했지만, 제안 모델의 복잡도에 비해 성능 개선이 크지 않았고 지연시간 측면에 대한 고려가 부족했다.

기존 LSTM 알고리즘을 이용한 사기 거래 탐지에 관한 연구에서는 성능 개선을 위해 데이터 샘플링, 피쳐 선택 등 다양한 기법 등을 이용하였지만 그 과정에서 발생하는 오버헤드 및 지연시간을 고려하지 않았다. 본 논문에서는 이상 거래 탐지 시 발생하는 데이터 불균형 문제를 해결하기 위해 최소한의 사기 데이터만을 이용한 실시간 데이터 오버샘플링 기법과 효과적인 시계열 데이터 처리를 위한 LSTM 알고리즘을 결합하여 빠르고 정확한 FDS 프레임워크를 제안했다.

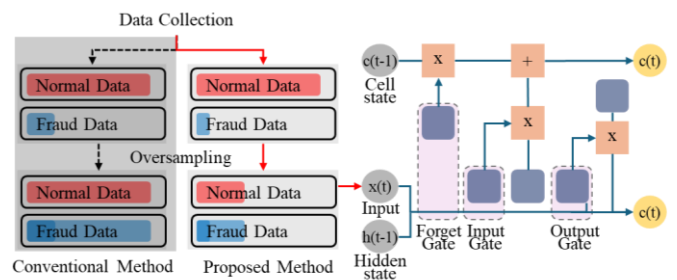
3. SMOTE 기반의 LSTM 을 활용한 사기 거래 탐지

데이터 오버샘플링이란 데이터 클래스의 분포가 불균

형한 상황에서 데이터를 삭제하거나 추가, 합성하는 방식으로 클래스 분포를 균등하게 만드는 기법이다. SMOTE는 데이터 리샘플링 기법 중 오버샘플링의 한 종류로서 개수가 적은 클래스의 표본에 노이즈를 추가하여 새로운 데이터 샘플을 생성해 데이터 불균형 문제를 해소한다[5]. SMOTE는 데이터 클래스의 불균형 정도가 매우 큰 사기 거래 탐지와 관련된 연구에서 가장 활발히 이용되는 리샘플링 기법이며, 노이즈를 추가하여 데이터를 새롭게 합성하는 방식이므로 과적합 문제를 해소할 수 있다.

LSTM 알고리즘은 순환 신경망(Recurrent Neural Network, RNN)기법의 한 종류로서 기존 RNN의 기울기 소멸 문제(Vanishing Gradient Problem)로 인한 한계를 보완했다[6]. RNN 알고리즘은 같은 Cell 을 반복하여 학습하고, Input 에 따라 반복 횟수가 결정되고 Input 시퀀스가 길어질수록 Cell 축이 길어진다. 그러나 신경망의 계층 구조가 복잡해질수록 기억해야 할 데이터가 많기 때문에 기울기 소멸 문제가 발생한다[7]. LSTM 은 Forget, Input, Output Gate 와 Cell state 를 통해 불필요한 데이터를 삭제하고 필요한 데이터를 새롭게 추가하여 긴 시계열 데이터 처리에 탁월하다.

본 논문에서 제안하는 SMOTE 기반의 LSTM 을 활용한 FDS 프레임워크는 금융 데이터가 수집될 때, 사기 거래 데이터가 부족하여 발생하는 데이터 불균형 문제를 해결할 수 있다. 기존의 기계학습 기반 FDS 관련 연구에서는 불균형 데이터에 샘플링 기법을 적용하여 불균형을 해소한다. 본 연구에서는 SMOTE 를 적용했으며, 동시에 데이터가 수집되는 시간을 절약하고자 최소한의 불균형 데이터를 이용하여 탐지 성능 및 지연시간을 개선한다.



(그림 1) SMOTE 기반의 LSTM 을 활용한 FDS 프레임워크

(그림 1)은 SMOTE 기반의 LSTM 을 활용한 FDS 프레임워크를 보여준다. 데이터 수집 과정에서 상대적으로 비율이 적은 사기 거래 데이터가 설정한 최소치에 도달하면 실시간으로 데이터 오버샘플링을 수행한다. 최소치는 LSTM 알고리즘 이용 시, 성능이 저하되지 않는 데이터 셋의 최소량을 의미하며 본 논문에서는 ‘최소 개수’로 표현한다. 정상 거래 데이터와 사기 거래 데이터가 균형을 이루게 되면 LSTM 알고리즘을 이용하여 사기 거래를 탐지한다.

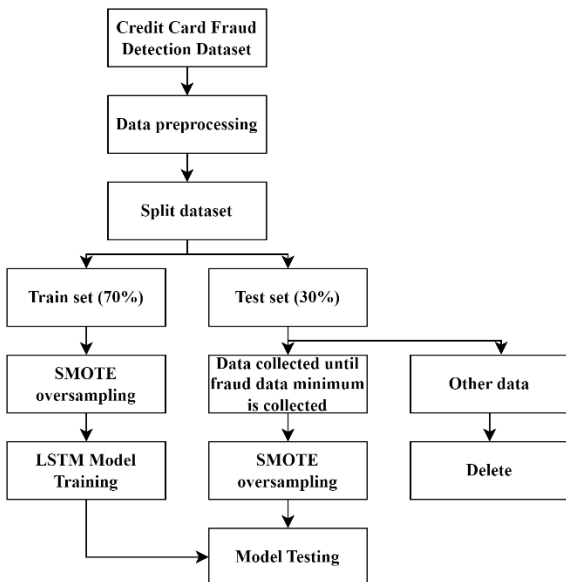
4. 성능 평가 및 결과 분석

본 절에서는 제안 프레임워크의 성능을 평가하기 위한 시뮬레이션 과정 및 결과에 대해 논의한다.

4.1 데이터 셋

데이터 셋은 Kaggle 에서 제공하는 Credit Card Fraud Detection[8,9]을 이용했다. Credit Card Fraud Detection 은 2013년 9월에 기록된 유럽 신용카드 소지자의 거래 내역을 포함하고 있으며, 총 284,807건의 거래 중 492건의 사기 거래 데이터와 284,315건의 정상 거래 데이터로 이루어져 있다. 사기 거래에 해당되는 데이터는 전체 데이터의 약 0.172% 수준으로 데이터 불균형이 매우 심각하다.

4.2 시뮬레이션 과정



(그림 2) 시뮬레이션 과정

(그림 2)는 제안 프레임워크의 성능 평가를 위한 시뮬레이션 과정을 보여준다. 우선, 데이터 전처리 과정을 통해 클래스 인코딩과 데이터 스케일링한다. 전처리가 완료된 데이터 셋의 70%를 훈련 데이터 셋으로 설정했으며, 나머지 30%는 테스트 데이터 셋으로 설정했다. 각 데이터 셋의 구성은 <표 1>과 같다. 훈련 데이터 셋은 SMOTE를 적용하여 불균형한 데이터를 각 199,020 개로 균등하게 맞추고, LSTM 알고리즘을 이용하여 학습한다. 테스트 데이터 셋이 실제 사기 거래 데이터 수집 상황과 유사하도록 트랜잭션을 하나씩 랜덤하게 읽어오며 사기 거래 데이터 개수가 설정한 최소 개수를 달성하면 더 이상 데이터를 읽어오지 않고, 새로운 테스트 데이터 셋을 구성했다. 새롭게 구성된 테스트 데이터 셋에 SMOTE를 적용하여 데이터를 균등하게 맞추고, 모델을 검증했다.

테스트 데이터 셋의 최소 개수는 아래와 같이 설정했다. 정상 거래 데이터의 사이즈 별 성능을 테스트한 결과에 따

라 성능이 가장 우수한 3,000 개로 고정했다. 사기 거래 데이터의 경우 10 개부터 100 개까지 10 개 단위로 늘려가며 평가했다.

<표 1> 데이터 셋 구성

| | Normal Data | Fraud Data |
|--------------|-------------|------------|
| Training Set | 199,020 | 344 |
| Test Set | 85,295 | 148 |
| Total | 284,315 | 492 |

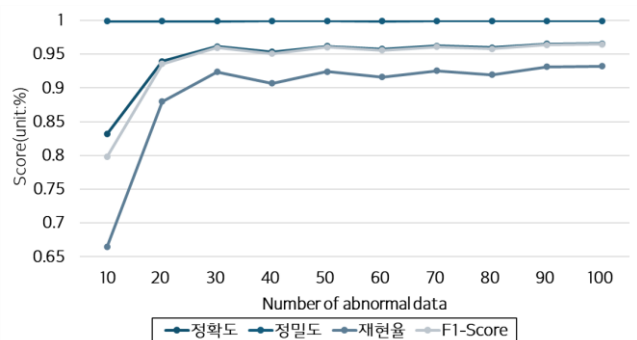
종래 방식 및 제안 방식의 데이터 셋 구성은 <표 2>와 같다. 종래 방식은 테스트 데이터셋을 그대로 이용하며, SMOTE를 적용하면 총 170,590 개의 데이터를 이용한다. 제안 방식은 사기 데이터셋에 SMOTE를 적용한 모델로 사기 거래 및 정상 데이터의 개수와 상관없이 각 3,000 개로 샘플링 하여 총 6,000 개의 데이터를 사용하여 균형을 맞추었다.

<표 2> SMOTE 적용 여부에 따른 데이터 셋 구성 비교 (단위: 개)

| Method | Before SMOTE | Normal | 85,295 |
|---------------------|--------------|--------|------------------|
| | | Fraud | 148 |
| Conventional Method | After SMOTE | Normal | 85,295 |
| | | Fraud | 85,295 |
| | | Total | 170,590 |
| Proposed Method | Before SMOTE | Normal | 3,000 |
| | | Fraud | 10, 20, ..., 100 |
| | After SMOTE | Normal | 3,000 |
| | | Fraud | 3,000 |
| Total | 6,000 | | |

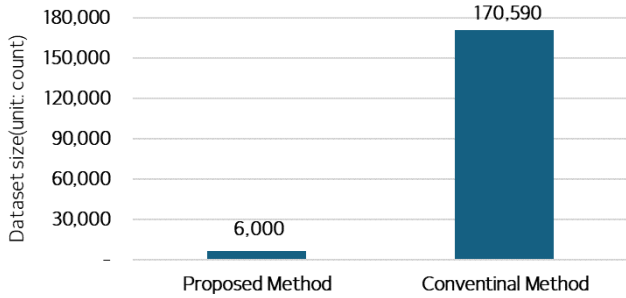
4.3 결과 분석

(그림 3)은 제안 방식의 사기 거래 데이터 최소 개수에 따른 탐지 성능을 비교한 그래프이다. 사기 거래 데이터의 개수를 10으로 설정한 경우와 20으로 설정한 경우를 제외하면 비교적 높은 탐지율을 유지하는 결과를 보였다. 특히 사기 거래 데이터 개수를 30으로 설정한 경우, 적은 양의 사기 거래 데이터만으로도 높은 탐지율을 기록했다.



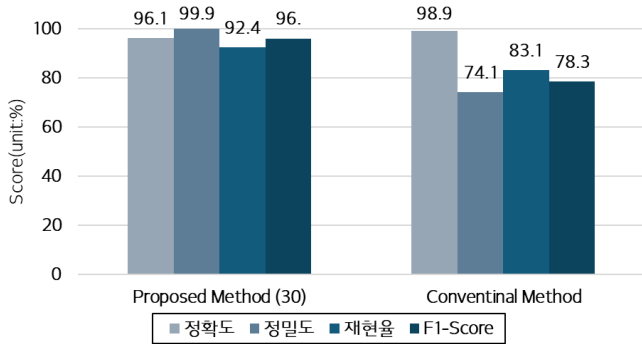
(그림 3) 제안 방식의 사기 거래 데이터 최소 개수 설정에 따른 탐지 성능 비교

(그림 4)는 종래 방식과 제안 방식의 데이터 크기를 비교한 그래프이다. 종래 방식의 경우 170,590 개의 데이터를 이용했으며, 제안 방식의 경우 6,000 개의 데이터를 이용하여 데이터 크기가 96.5% 감소했다.



(그림 4) 종래 방식과 제안 방식의 데이터 셋 크기 비교

(그림 5)는 종래 방식과 제안 방식의 탐지 성능을 비교한 그래프이다. 이 결과는 제안 방식의 사기 거래 데이터를 30으로 설정했을 때 종래의 방식과 데이터 사이즈를 비교한 것이다. 제안 방식은 정확도(Accuracy)를 제외한 모든 지표에서 종래 방식보다 개선된 성능을 보였다. 제안 방식은 종래 방식 대비 정밀도(Precision)가 34.81% 개선되었으며, 재현율(Recall)이 11.14%, F-1 Score 이 22.51% 향상된 결과를 보였다. 정밀도는 양성(사기 거래)이라고 예측한 것 중 올바르게 예측한 것의 비율을 나타내고, 재현율은 올바르게 분류한 것 중, 양성 데이터를 올바르게 분류한 것의 비율을 나타낸다. 사기 거래를 올바르게 판단하는 것이 중요한 이상탐지와 같은 상황에서는 정밀도, 재현율 등을 고려하는 것이 중요하다. 시뮬레이션 결과를 통해 적은 양의 데이터만으로도 종래의 방식 보다 탐지 성능이 우수했다.



(그림 5) 종래 방식과 제안 방식의 탐지 성능 비교

본 시뮬레이션 결과를 통해 데이터의 클래스 불균형이 큰 환경에서 많은 양의 양성 데이터가 수집되지 않더라도 종래의 방식 보다 정확하게 사기 거래를 예측할 수 있음을 보였다. 종래 방식은 SMOTE를 적용하여 데이터 불균형을 해소했지만, 데이터 셋의 크기가 증가하는 문제가 있었다. 제안 방식은 이용하는 데이터 셋의 크기를 크게 줄여 수집 대기 및 모델 검증에 소요되는 시간을 감소시킬 수 있다. 상황에 따라 사기 거래 데이터의 최소 개수를 설정하는 기준이 달라질 수 있으나, 본 논문의 제안 방식을 통해 각 상황에 맞는 최소치의 양성 데이터만 만족하면 일정 수준 이상의 탐지 성능을 달성할 수 있었다.

5. 결론

본 논문에서는 불균형 데이터를 이용하는 상황에서 최소한의 사기 거래 데이터가 수집되면 실시간으로 SMOTE를 적용하고 LSTM 알고리즘으로 모델 학습 및 검증을 수행하는 FDS 프레임워크를 제안했다. 시뮬레이션을 통해 제안하는 FDS 프레임워크는 적은 양의 사기 거래 데이터만으로도 탐지 성능 개선이 가능함을 증명했다.

특히 사기 거래 데이터 개수를 30으로 설정한 경우, 종래 방식과 비교했을 때 데이터 크기를 96.5% 감소시키는 동시에 정밀도, 재현율, F1-Score 측면에서 각각 34.81%, 11.14%, 22.51% 개선된 결과를 보였다.

ACKNOWLEDGEMENTS

본 논문은 2024년도 산업통상자원부 및 한국산업기술진흥원의 산업혁신인재성장지원사업 (RS-2024-00415520)과 과학기술정보통신부 및 정보통신기획평가원의 ICT 혁신인재 4.0 사업의 연구결과로 수행되었음 (No. IITP-2022-RS-2022-00156310)

참고문헌

- [1] Bin Sulaiman, Rejwan, Vitaly Schetinin, and Paul Sant, Review of machine learning approach on credit card fraud detection, Human-Centric Intelligent Systems 2.1, 55-68, 2022
- [2] 금융거래표(2009~), 국가정보포털(KOSIS), <https://kosis.kr/search/search.do>, 2024/4/12
- [3] Benchaji, I., Douzi, S., El Ouahidi, B., Jaafari, J., Enhanced credit card fraud detection based on attention mechanism and LSTM deep model, J Big Data 8, 151, 2021
- [4] Mohmad, Yanash Azwin., Credit Card Fraud Detection Using LSTM Algorithm, Wasit J. Comput. Math. Sci 1, 39-53, 2022
- [5] Dablain, Damien, Bartosz Krawczyk, and Nitesh V. Chawla, DeepSMOTE: Fusing deep learning and SMOTE for imbalanced data, IEEE Transactions on Neural Networks and Learning Systems, 2022
- [6] Bhandari, H. N., Rimal, B., Pokhrel, N. R., Rimal, R., Dahal, K. R., & Khatri, R. K., Predicting stock market index using LSTM, Machine Learning with Applications, 9, 100320, 2022
- [7] Abumohsen, Mobarak, Amani Yousef Owda, and Majdi Owda, Electrical load forecasting using LSTM, GRU, and RNN algorithms, Energies 16.5, 2283, 2023
- [8] Credit Card Fraud Detection, Kaggle, 2021, <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud/data>, 2024/4/12
- [9] Bertrand Lebichot, Gianmarco Paldino, Wissam Siblini, Liyun He, Frederic Oblé, Gianluca Bontempi, Incremental learning strategies for credit cards fraud detection, International Journal of Data Science and Analytics, 12(2), 165-174, 2021