ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

JOURNAL OF CURRENT SCIENCE

HEALTH INSURANCE FRAUD DETECTION USING DEEP LEARNING.

Mr.Francis Vijaykumar Anna Reddy[1] ,k.sai satwika[2],Rajeshwari[3], Gayatri[4]

[1]Assistant Professor, Department of CSE, MallaReddy Engineering College for Women, Hyderabad, fannareddy@yahoo.com

[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, TS, India.

ABSTRACT

Collusive fraud, in which multiple fraudsters collude to defraud health insurance funds, threatens the operation of the healthcare system. However, existing statistical and machine learning-based methods have limited ability to detect fraud in the scenario of health insurance due to the high similarity of fraudulent behaviors to normal medical visits and the lack of labeled data. To ensure the accuracy of the detection results, expert knowledge needs to be integrated with the fraud detection process. By working closely with health insurance audit experts, we propose FraudAuditor, a three-stage visual analytics approach to collusive fraud detection in health insurance. Specifically, we first allow users to interactively construct a co-visit network to holistically model the visit relationships of different patients. Second, an improved community detection algorithm that considers the strength of fraud likelihood is designed to detect suspicious fraudulent groups. Finally, through our visual interface, users can compare, investigate, and verify suspicious patient behavior with tailored visualizations that support different time scales. We conducted case studies in a real-world healthcare scenario, i.e., to help locate the actual fraud group and exclude the false positive group. The results and expert feedback proved the effectiveness and usability of the approach.

I. INTRODUCTION

AN effective health insurance system plays a significant role in managing healthcare resources, enhancing life quality for people, and maintaining social stability. More than 1.3 billion people have enrolled in theNational Basic Medical Insurance in China1. However, increasing health insurance fraud events have become a severe social problem. According to the inspection conducted by the National Healthcare Security Administration and the Ministry of Public Security in China, nearly half of 815,000

ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

health institutes have improper or even illegal funds costs in 2020, leading to an economic loss of more than 22.3 billion yuan ($3.4 billion)2. The emerging collusive fraud is the most serious and urgent among these events [1]. Fraudsters collude to purchase drugs with insurance reimbursement and cash the drugs out. The massive amount of fraud brings serious consequences. There is an urgent need for efficient and effective detection methods to quickly identify collusive fraud and prevent further loss.

Detecting collusive fraud in health insurance faces two challenges. First, it is difficult to distinguish the medical visits behavior of fraudsters from those of normal patients. Typically, fraudsters frequently buy large quantities of easily marketable drugs. However, due to the need to maintain long-term medication, patients with chronic diseases and those requiring Traditional Chinese medicine (TCM) treatment have similar purchasing behaviors to fraudsters'. Second, manual auditing is necessary but laborious. Misidentification is unacceptable for fraud detection because a patient has to bear legal responsibility after being recognized as a fraudster. Verifying fraud requires auditors to synthesize a large amount of contextual information, such as the amount of reimbursement, the degree to which the patient's disease and drugs match, and the time of visits.

Existing collusive fraud detection methods can hardly handle these challenges. Existing methods focus on modeling the relationships between fraudsters by graphs and detecting fraudulent groups through statistical or machine learning (ML) methods. Statistical approaches use structural and attribute features [2], [3], [4], or spectral analysis [5] to detect anomalous substructures (i.e., fraud groups/events). However, audit experts told us that these methods are prone to false positives, due to the ambiguous nature of collusive fraud in health insurance. Excluding false positives is time-consuming for auditors and can significantly reduce detection efficiency. ML methods mainly use graph neural network (GNN) models to detect collusive fraud [6], [7], [8]. Fraudsters and their associations are constructed as homogeneous or heterogeneous graphs. GNNs trained on labeled data can yield the representation of fraudsters and be further applied to judge unlabeled individuals. Unfortunately, large amounts of labeled data are indispensable for high-performance GNNs. Without sufficient labeled fraud, GNN models are not applicable in our scenario.

ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

To address these challenges, we propose a novel visual analytics approach to help health insurance audit experts identify suspicious groups, investigate the visit behavior of suspicious patients, and validate collusive fraud results. We propose a co-visit network to represent the relationship among patients. The weights of the edges are calculated by extracting the characteristics of collusive fraudsters, such as the time gap and number of visits. Suspicious groups with multiple simultaneous visits to the same location can then be identified by a weighted community detection algorithm. The algorithm is integrated into a prototype system, Fraud Auditor, that supports experts in interactively browsing and improving model detection results. Fraud Auditor can help experts quickly locate and examine fraud by observing co-visit links in visualizations of patient medical behavior. Combined with contextual information such as disease, drug, and fee information, false positive groups can be verified and excluded. We provide case studies and expert interviews in real health insurance scenarios to validate the effectiveness of the proposed approach.

The contributions in this work include:

_ A problem characterization that summarizes the requirements of collusive fraud detection in the scenario of health insurance.

_ A novel three-stage visual analytics approach to detect collusive fraud in health insurance that considers the visit pattern of fraud groups and expert knowledge.

_ An interactive prototype system, Fraud Auditor, to facilitate the identification, examination, and validation of suspicious collusive fraud groups.

II. LITERATURE REVIEW

A Machine Learning-based Approach for Medical Insurance Anomaly Detection by Predicting Indirect Outpatients' Claim Price, Mahdi Sharifi Garmdareh; Behzad Soleimani Neysiani; Mohammad Zahiri Nogorani; Mehdi Bahramizadegan, About 10% of insurance claims are fraudulent according to published reports. Insurance companies can take a very robust approach to detect anomalies using machine learning techniques. This study proposes a new model based on regression-based machine learning algorithms to predict the Total Price of a patient's claim based on the history of other patients, and then compare the estimated amount with the actual amount to obtain their price difference. The abnormal or fraud costs will be predicted in claims based on a threshold for the absolute price difference. A dataset of 99,440 records of RASA web portal is gathered for evaluation. Deep learning has the best mean absolute error (MAE)

ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

in the training phase, but the decision tree has the best MAE in the testing phase. So, the decision tree is used for anomaly detection, which can detect about 17% of records as abnormal with at least a 30% deviation. Expert human assessors check the results and approve more than 50% of reported anomalies.

Fraud Detection System for Effective Healthcare Administration in Nigeria using Apache Hive and Big Data Analytics: Reflection on the National Health Insurance Scheme,Justin Onyarin Ogala; Ese Sophia Mughele; Stella Chinnye Chiemeke, Nigerian researchers have shown that the lack of adequate mechanisms for fraud detection has impaired both providers and beneficiaries of this scheme. This work develops a fraud detection program for Nigeria's National Health Insurance Scheme (NHIS). Nigeria's National Health Insurance Scheme (NHIS) and Health Maintenance Organizations (HMOs) are the subjects of this study. The study was conducted using available data from NHIS-registered healthcare facilities and HMOs. Unified Modeling Language (UML) tools were used to create the framework. The framework was built with Apache Derby DB, Hadoop Distributed File System (HDFS), and Apache MapReduce as the big data processing platform. Using Apache Hive and Big Data Analytics, a system for detecting healthcare fraud is developed. This system used data from the Nigerian National Health Insurance Scheme (NHIS), which was broken down into three categories: enrolment, referral, and claim data. The analysis of current healthcare investigative methods is conducted, and a new framework is proposed.

III. EXISTING SYSTEM :

Akoglu et al. [2] extracted structural features, such as node degree or centrality, from the graph to find egonets. SpamCom [3] identified spammer communities on Twitter by using structure and attribute features such as Twitter content similarity, user topology, and user profile. In healthcare scenarios, Chen et al. [5] applied a spectrum analysis-based community detection method to detect patient referral fraud cases from a bipartite graph of physicians and specialists. Zhao et al. [13] generated a dynamic heterogeneous information network containing patients, hospitals, and diseases. Then, they identified anomalies that fit predefined fraud patterns (e.g., the high-cost single treatment) over fixedor variable periods. Statistics-based methods can produceinitial fraud candidates but may have erroneous results,requiring further validation by experts.

Xu et al. [7] propose GRC, a novel GNN model, that learns representations of different types of individuals and detects loan fraud by using attention mechanisms and

imposing conditional random fields. However, these ML methods are supervised or semi-supervised and thus require fraud-labeled data, which is lacking in our health insurance scenario.

Niu et al. [4] use a node-link diagram to demonstrate the loan guarantee network, where each node belongs to a community defined by a random walk algorithm and is encoded with the corresponding color. In order to identify collective anomalies, Tao et al. [25] proposed a high-order correlation graph to support analysis processes starting with an abnormal node.Corresponding nodes that contribute to the anomaly can be easily identified through the high-order correlation graph. Our system incorporates graph and sequence visualization. To focus on collusive fraud in health insurance scenarios, our system provides richer contextual information, such as disease, drugs, and visit frequency.

Disadvantages

- ✓ In the existing work, the system did not implement suspicious groups identification.
- ✓ This system is less performance due to lack of Graph Neural Network.

IV. PROPOSED SYSTEM

The system proposes a novel visual analytics approach to help health insurance audit experts identify suspicious groups, investigate the visit behavior of suspicious patients, and validate collusive fraud results. We propose a co-visit network to represent the relationship among patients. The weights of the edges are calculated by extracting the characteristics of collusive fraudsters, such as the time gap and number of visits. Suspicious groups with multiple simultaneous visits to the same location can then be identified by a weighted community detection algorithm. The algorithm is integrated into a prototype system, Fraud Auditor, that supports experts in interactively browsing and improving model detection results. FraudAuditor can help experts quickly locate and examine fraud by observing co-visit links in visualizations of patient medical behavior.

Combined with contextual information such as disease, drug, and fee information, false positive groups can be verified and excluded. We provide case studies and expert interviews in real health insurance scenarios to validate the effectiveness of the proposed approach.

Advantages

ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

1. A problem characterization that summarizes the requirements of collusive fraud detection in the scenario of health insurance.
2. A novel three-stage visual analytics approach to detect collusive fraud in health insurance that considers the visit pattern of fraud groups and expert knowledge.
3. An interactive prototype system, FraudAuditor, to facilitate the identification, examination, and validation of suspicious collusive fraud groups.

V.MODULES

Service provider

In this module, the service provider has to login by using valid user name and password. After login successful he can do some operations such as

Browse insurance claim datasets and train & test data sets, view trained and tested accuracy in bar chart, view trained and tested accuracy results, view prediction of fraud in health insurance, view fraud in health insurance ratio, download predicted data sets, view fraud in health insurance ratio results, view all remote users,

View and authorize users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote user

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once login is successful user will do some operations like register and login, predict fraud in health insurance status, view your profile.

Decision tree classifiers

Decision tree classifiers are used successfully in many diverse areas. Their most important feature is the capability of capturing descriptive decision making knowledge from the supplied data. Decision tree can be generated from training sets. The procedure for such generation based on the set of objects (S), each belonging to one of the classes C1, C2, …, Ck is as follows:

ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

Step 1. If all the objects in S belong to the same class, for example Ci, the decision tree for S consists of a leaf labeled with this class

Step 2. Otherwise, let T be some test with possible outcomes O1, O2,…, On. Each object in S has one outcome for T so the test partitions S into subsets S1, S2,… Sn where each object in Si has outcome Oi for T. T becomes the root of the decision tree and for each outcome Oi we build a subsidiary decision tree by invoking the same procedure recursively on the set Si.

Gradient boosting

Gradient boosting is a machine learning technique used in regression and classification tasks, among others. It gives a prediction model in the form of an ensemble of weak prediction models, which are typically decision trees.[1][2] When a decision tree is the weak learner, the resulting algorithm is called gradient-boosted trees; it usually outperforms random forest.A gradient-boosted trees model is built in a stage-wise fashion as in other boosting methods, but it generalizes the other methods by allowing optimization of an arbitrary differentiable loss function.

K-Nearest Neighbors (KNN)

- Simple, but a very powerful classification algorithm

- Classifies based on a similarity measure
- Non-parametric
- Lazy learning
- Does not “learn” until the test example is given

- Whenever we have a new data to classify, we find its K-nearest neighbors from the training data

Example

- Training dataset consists of k-closest examples in feature space
- Feature space means, space with categorization variables (non-metric variables)
- Learning based on instances, and thus also works lazily because instance close to the input vector for test or prediction may take time to occur in the training dataset

Logistic regression Classifiers

ISSN NO: 9726-001X
Volume 12 Issue 01 Jan 2024

Logistic regression analysis studies the association between a categorical dependent variable and a set of independent (explanatory) variables. The name *logistic regression* is used when the dependent variable has only two values, such as 0 and 1 or Yes and No. The name *multinomial logistic regression* is usually reserved for the case when the dependent variable has three or more unique values, such as Married, Single, Divorced, or Widowed. Although the type of data used for the dependent variable is different from that of multiple regression, the practical use of the procedure is similar.

Logistic regression competes with discriminant analysis as a method for analyzing categorical-response variables. Many statisticians feel that logistic regression is more versatile and better suited for modeling most situations than is discriminant analysis. This is because logistic regression does not assume that the independent variables are normally distributed, as discriminant analysis does.

This program computes binary logistic regression and multinomial logistic regression on both numeric and categorical independent variables. It reports on the regression equation as well as the goodness of fit, odds ratios, confidence limits, likelihood, and deviance. It performs a comprehensive residual analysis including diagnostic residual reports and plots. It can perform an independent variable subset selection search, looking for the best regression model with the fewest independent variables. It provides confidence intervals on predicted values and provides ROC curves to help determine the best cutoff point for classification. It allows you to validate your results by automatically classifying rows that are not used during the analysis.

Naïve Bayes

The naive bayes approach is a supervised learning method which is based on a simplistic hypothesis: it assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature .
Yet, despite this, it appears robust and efficient. Its performance is comparable to other supervised learning techniques. Various reasons have been advanced in the literature. In this tutorial, we highlight an explanation based on the representation bias. The naive bayes classifier is a linear classifier, as well as linear discriminant analysis, logistic

regression or linear SVM (support vector machine). The difference lies on the method of estimating the parameters of the classifier (the learning bias).

While the Naive Bayes classifier is widely used in the research world, it is not widespread among practitioners which want to obtain usable results. On the one hand, the researchers found especially it is very easy to program and implement it, its parameters are easy to estimate, learning is very fast even on very large databases, its accuracy is reasonably good in comparison to the other approaches. On the other hand, the final users do not obtain a model easy to interpret and deploy, they does not understand the interest of such a technique.

Thus, we introduce in a new presentation of the results of the learning process. The classifier is easier to understand, and its deployment is also made easier. In the first part of this tutorial, we present some theoretical aspects of the naive bayes classifier. Then, we implement the approach on a dataset with Tanagra. We compare the obtained results (the parameters of the model) to those obtained with other linear approaches such as the logistic regression, the linear discriminant analysis and the linear SVM. We note that the results are highly consistent. This largely explains the good performance of the method in comparison to others. In the second part, we use various tools on the same dataset (Weka 3.6.0, R 2.9.2, Knime 2.1.1, Orange 2.0b and RapidMiner 4.6.0). We try above all to understand the obtained results.

Random Forest

Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that operates by constructing a multitude of decision trees at training time. For classification tasks, the output of the random forest is the class selected by most trees. For regression tasks, the mean or average prediction of the individual trees is returned. Random decision forests correct for decision trees' habit of overfitting to their training set. Random forests generally outperform decision trees, but their accuracy is lower than gradient boosted trees. However, data characteristics can affect their performance.

The first algorithm for random decision forests was created in 1995 by Tin Kam Ho[1] using the random subspace method, which, in Ho's formulation, is a way to implement

the "stochastic discrimination" approach to classification proposed by Eugene Kleinberg.

An extension of the algorithm was developed by Leo Breiman and Adele Cutler, who registered "Random Forests" as a trademark in 2006 (as of 2019, owned by Minitab, Inc.).The extension combines Breiman's "bagging" idea and random selection of features, introduced first by Ho[1] and later independently by Amit and Geman[13] in order to construct a collection of decision trees with controlled variance.

Random forests are frequently used as "blackbox" models in businesses, as they generate reasonable predictions across a wide range of data while requiring little configuration.

SVM

In classification tasks a discriminant machine learning technique aims at finding, based on an *independent and identically distributed* (*iid*) training dataset, a discriminant function that can correctly predict labels for newly acquired instances. Unlike generative machine learning approaches, which require computations of conditional probability distributions, a discriminant classification function takes a data point *x* and assigns it to one of the different classes that are a part of the classification task. Less powerful than generative approaches, which are mostly used when prediction involves outlier detection, discriminant approaches require fewer computational resources and less training data, especially for a multidimensional feature space and when only posterior probabilities are needed. From a geometric perspective, learning a classifier is equivalent to finding the equation for a multidimensional surface that best separates the different classes in the feature space.

SVM is a discriminant technique, and, because it solves the convex optimization problem analytically, it always returns the same optimal hyperplane parameter—in contrast to *genetic algorithms* (*GAs*) or *perceptrons*, both of which are widely used for classification in machine learning. For perceptrons, solutions are highly dependent on the initialization and termination criteria. For a specific kernel that transforms the data from the input space to the feature space, training returns uniquely defined SVM model parameters for a given training set, whereas the perceptron and GA classifier models are different each time training is initialized. The aim of GAs and perceptrons is only

to minimize error during training, which will translate into several hyperplanes' meeting this requirement.

CONCLUSION

In this paper, we proposed a visual analytics approach that supports the identification, examination, and annotation of collusive fraud in health insurance. The design and implementation of Fraud Auditor are based on close collaboration with domain experts. By leveraging both automated algorithms and human experience, Fraud Auditor supports a multi-level fraud analysis, including the co-visit network overview, suspicious groups identification, and suspicious patients examination. A suite of visualization designs supports the detection and exploration of fraud groups. The effectiveness of our approach and the usability of the prototype system were recognized through case studies and interviews involving health insurance audit experts.

REFERENCES

[1] J. Li, K.-Y. Huang, J. Jin, and J. Shi, "A survey on statistical methods for health care fraud detection," Health Care Management Science, vol. 11, no. 3, pp. 275–287, 2008.

[2] L. Akoglu, M. McGlohon, and C. Faloutsos, "Oddball: Spotting anomalies in weighted graphs," in Proceedings of Pacific-Asia Conference on Knowledge Discovery and Data Mining, 2010, pp. 410–421.

[3] P. Bindu, R. Mishra, and P. S. Thilagam, "Discovering spammer communities in twitter," Journal of Intelligent Information Systems, vol. 51, no. 3, pp. 503–527, 2018.

[4] Z. Niu, D. Cheng, L. Zhang, and J. Zhang, "Visual analytics for networked-guarantee loans risk management," in Proceedings of Pacific Visualization Symposium, 2018, pp. 160–169.

[5] S. Chen and A. Gangopadhyay, "A novel approach to uncover health care frauds through spectral analysis," in Proceedings of International Conference on Healthcare Informatics, 2013, pp. 499–504.

[6] J.Wang, R.Wen, C.Wu, Y. Huang, and J. Xiong, "Fdgars: Fraudster detection via graph convolutional networks in online app review system," in Companion proceedings of the World Wide Web conference, 2019, pp. 310–316.

[7] B. Xu, H. Shen, B. Sun, R. An, Q. Cao, and X. Cheng, "Towards consumer loan fraud detection: Graph neural networks with roleconstrained conditional random field," in Proceedings of AAAI Conference on Artificial Intelligence, 2021, pp. 4537–4545.

[8] Q. Zhong, Y. Liu, X. Ao, B. Hu, J. Feng, J. Tang, and Q. He, "Financial defaulter detection on online credit payment via multi-view attributed heterogeneous information network," in Proceedings of The Web Conference, 2020, pp. 785–795.

[9] I. Molloy, S. Chari, U. Finkler, M.Wiggerman, C. Jonker, T. Habeck, Y. Park, F. Jordens, and R. v. Schaik, "Graph analytics for realtime scoring of cross-channel transactional fraud," in Proceedings of International Conference on Financial Cryptography and Data Security, 2016, pp. 22–40.

[10] Z. Li, H. Xiong, and Y. Liu, "Mining blackhole and volcano patterns in directed graphs: a general approach," Data Mining and Knowledge Discovery, vol. 25, no. 3, pp. 577–602, 2012.

[11] H. Joudaki, A. Rashidian, B. Minaei-Bidgoli, M. Mahmoodi, B. Geraili, M. Nasiri, and M. Arab, "Using data mining to detect health care fraud and abuse: a review of literature," Global Journal of Health Science, vol. 7, no. 1, pp. 194–202, 2015.

[12] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: a survey," Data Mining and Knowledge Discovery, vol. 29, no. 3, pp. 626–688, 2015.

[13] B. Zhao, Y. Shi, K. Zhang, and Z. Yan, "Health insurance anomaly detection based on dynamic heterogeneous information network," in Proceedings of IEEE International Conference on Bioinformatics and Biomedicine, 2019, pp. 1118–1122.

[14] K. Ding, J. Li, R. Bhanushali, and H. Liu, "Deep anomaly detection on attributed networks," in Proceedings of SIAM International Conference on Data Mining. SIAM, 2019, pp. 594–602.

[15] D. Wang, J. Lin, P. Cui, Q. Jia, Z. Wang, Y. Fang, Q. Yu, J. Zhou, S. Yang, and Y. Qi, "A semi-supervised graph attentive network for financial fraud detection," in Proceedings of the International Conference on Data Mining, 2019, pp. 598–607.

[16] S. Ko, S. Afzal, S. Walton, Y. Yang, J. Chae, A. Malik, Y. Jang, M. Chen, and D. Ebert, "Analyzing high-dimensional multivariate network links with integrated anomaly detection, highlighting and exploration," in Proceedings of IEEE Conference on Visual Analytics Science and Technology, 2014, pp. 83–92.

[17] N. Cao, C. Shi, S. Lin, J. Lu, Y.-R. Lin, and C.-Y. Lin, "Targetvue: Visual analysis of anomalous user behaviors in online communication systems," IEEE Transactions on Visualization and Computer Graphics, vol. 22, no. 1, pp. 280–289, 2015.

[18] C. Mac¸ ˜as, E. Polisciuc, and P. Machado, "Vabank: visual analytics for banking transactions," in Proceedings of International Conference Information Visualisation, 2020, pp. 336–343.

[19] C. Mac¸ ˜as, E. Polisciuc, and P. Machado, "Atovis - A visualisation tool for the detection of financial fraud," Information Visualization, vol. 21, no. 4, pp. 371–392, 2022.

[20] J. Zhao, N. Cao, Z. Wen, Y. Song, Y.-R. Lin, and C. Collins, "#fluxflow: Visual analysis of anomalous information spreading on social media," IEEE Transactions on Visualization and Computer Graphics, vol. 20, no. 12, pp. 1773–1782, 2014.

[21] E. Bertini, P. Hertzog, and D. Lalanne, "Spiralview: towards security policies assessment through visual correlation of network resources with evolution of alarms," in Proceedings of IEEE symposium on visual analytics science and technology, 2007, pp. 139–146.

[22] P. Silva, C. Mac¸ ˜as, E. Polisciuc, and P. Machado, "Visualisation tool to support fraud detection," in Proceedings of the International Conference Information Visualisation, 2021, pp. 77–87.

[23] Y. Lin, K.Wong, Y.Wang, R. Zhang, B. Dong, H. Qu, and Q. Zheng, "TaxThemis: Interactive mining and exploration of suspicious tax evasion groups," IEEE Transactions on Visualization and Computer Graphics, vol. 27, no. 2, pp. 849–859, 2021.

[24] W. Didimo, G. Liotta, F. Montecchiani, and P. Palladino, "An advanced network visualization system for financial crime detection," in Proceedings of the Pacific Visualization Symposium, 2011, pp. 203–210.

[25] J. Tao, L. Shi, Z. Zhuang, C. Huang, R. Yu, P. Su, C. Wang, and Y. Chen, "Visual analysis of collective anomalies through highorder correlation graph," in Proceedings of the Pacific Visualization Symposium, 2018, pp. 150–159.