Enhancement to Training of Bidirectional GAN: An Approach to Demystify Tax Fraud

1st Priya Mehta
Welingkar Institute of Management Development and Research
Mumbai, India
priya.mehta@welingkar.org

2nd Sandeep Kumar
Department of Computer Science and Engineering
Indian Institute of Technology Hyderabad
Sangareddy, India
sandeep@iith.ac.in

3rd Ravi Kumar
Department of Computer Science and Engineering
Indian Institute of Technology Hyderabad
Sangareddy, India
CS18MTECH11028@iith.ac.in

4th Ch. Sobhan Babu
Department of Computer Science and Engineering
Indian Institute of Technology Hyderabad
Sangareddy, India
sobhan@cse.iith.ac.in

Abstract—Outlier detection is a challenging activity. Several machine learning techniques are proposed in the literature for outlier detection. In this article, we propose a new training approach for bidirectional GAN (BiGAN) to detect outliers. To validate the proposed approach, we train a BiGAN with the proposed training approach to detect taxpayers, who are manipulating their tax returns. For each taxpayer, we derive six correlation parameters and three ratio parameters from tax returns submitted by him/her. We train a BiGAN with the proposed training approach on this nine-dimensional derived ground-truth data set. Next, we generate the latent representation of this data set provided by the Commercial Taxes Department, Government of Telangana, India.

Index Terms—outlier detection, tax fraud detection, bidirectional GAN, goods and services tax

I. INTRODUCTION

A. Outlier Detection

Outliers are data points that are far from other data points. In other words, they are unusual values in a data set. Detecting outliers is essentially identifying unexpected elements in data sets [1]. Outlier identification has several real world applications such as fraud detection and intrusion detection. Outlier detection is a challenging activity. Several machine learning techniques are proposed in the literature for outlier detection. Several methods derived from neural networks have been applied to outlier detection. Generative Adversarial Networks have emerged as a leading technique. Goodfellow et al. proposed a new approach for training generative models via an adversarial process [2]. This method simultaneously trains two neural network modules: a generator module that captures the probability distribution of the training data and a discriminator module that estimates the probability that a sample came from the training data set rather than generated by the generator. In this way, the two modules are competing against each other, they are adversarial in the game theory sense, and are playing a zero-sum game. In their existing form, GANs have no means of learning the inverse mapping (projecting training data back into the latent space). Jeff Donahue et al. proposed Biogenic Generative Adversarial Networks (BiGANs) as a method of learning this inverse mapping [3]. Kaplan et al. implemented anomaly detection using BiGAN, considering it as a one-class anomaly detection algorithm [4]. Since generator and discriminator are highly dependent on each other in the training phase, to minimize this dependency, they proposed two different training approaches for BiGAN by adding extra training steps to it. They also demonstrated that the proposed approaches increased the performance of BiGAN on the anomaly detection tasks.

B. Indirect Tax

Indirect tax is collected by an intermediary (such as a retailer and manufacturer) from the consumer of goods or services [5]. The intermediary submits the tax he/she collected to the government by filing tax return forms at regular time intervals. In reality, the intermediary acts as a conduit for the flow of tax from the consumer of the goods or services to the government.

1) Goods and Services tax: Goods and Services Tax (GST) is a destination-based, multi-stage, comprehensive taxation system. In GST, the tax is levied in an incremental manner at each stage of the supply chain based on the value added to goods/services at that stage. This tax is levied at each stage of the supply chain in such a way that the tax paid on purchases...
(Input tax or input tax credit) is given as a set-off for the tax levied on sales (output tax or liability).

Figure 1 shows how tax is collected incrementally at each stage of the supply chain. In this example, the manufacturer purchases goods from the supplier for a value of $200 and pays $20 as tax at a tax rate of 10%. The supplier then pays the tax he/she collected to the government. In the next stage of the supply chain, the retailer purchases finished goods from the manufacturer for a value of $240 and pays $24 as tax at a tax rate of 10%. The manufacturer pays ($24 – $20 = $4) to the government, which is the difference between the tax he paid to the supplier and the tax he collected from the retailer. Finally, the consumer buys it from the retailer for a value of $300 and pays $30 as tax at a tax rate of 10%. So the retailer will pay ($30 – $24 = $6) to the government. In essence, for every dealer in GST, the tax payable is the difference between output tax and input tax.

![Figure 1: Tax Flow in GST](image)

2) Tax evasion: Taxation and tax evasion go hand in hand. It is a never-ending cat and mouse game. Business dealers manipulate their tax returns to avoid tax and maximize their profits. Tax enforcement officers formulate new rules and regulations to control tax evasion after studying the behavior of known tax evaders who exploit the loopholes in the existing taxation laws. In this game tax evaders always try their best to stay a few steps ahead of the enforcement officers. Hence, it is necessary for the officials to identify the evasion as early as possible and close the loopholes before the techniques become a widespread practice. In this manner, the taxation officers will be able to limit the loss of government revenue due to tax evasion. The following are prominent ways of tax evasion:

1) The dealer will collect tax at a higher rate from the customer and pays it to the government at a lower rate.
2) The dealer does not report all the sales transactions made by her/him (sales suppression).
3) The dealer will show a lower taxable turnover by wrongly applying the prescribed calculations.
4) The dealer creates fictitious sales transactions where there is no movement of goods but only the invoices are circulated in order to claim an Input Tax Credit (ITC) and evade tax payment. This method is called bill trading.

C. Our Contribution

In this article, we propose a new training approach for bidirectional GAN (BiGAN) to detect outliers. This is an enhancement to the BiGAN training approach given in [4]. To validate the proposed approach, we train a BiGAN with the proposed training approach to detect taxpayers, who are manipulating their tax returns in the Goods and Services Taxation system, which came into operation in India in July 2017.

The Goods and Services Taxation system unified the taxation laws in India. As per this system, dealers are supposed to file tax return statements every month by providing the complete details of sales and purchases that happened in the corresponding month. The objective of this work is to identify dealers who manipulate their tax return statements to minimize their tax liability. We train BiDirectional GAN (BiGAN) using the proposed approach on nine-dimensional ground-truth data derived from tax returns submitted by taxpayers (six correlation parameters and three ratio parameters). Next, we encode the ground-truth data set using the encoder (generate latent representation) and decode it back using the generator (regenerate the ground-truth data) by giving the latent representation as input. For each taxpayer, compute the cosine similarity between his/her ground-truth data and regenerated data. Taxpayers with lower cosine similarity measures are potential return manipulators. This idea can be applied in other nations where multi-stage indirect taxation is followed.

The rest of the paper is organized as follows. In Section II, we discuss the previous relevant works. In Section III, we will explain the data set used. In Section IV, we explain our proposed enhancement for BiGAN. In Section V, we give a detailed description of the methodology used in this paper. The results obtained are discussed in Section VI.

II. RELATED WORK

Chandola et al. presented several data mining techniques for anomaly detection [1]. Daniel de Roux et al. presented a very interesting approach for the detection of fraudulent taxpayers using only unsupervised learning methods [6]. Yusuf Sahin et al. worked on credit card fraud detection [7]. They developed some classification models based on Artificial Neural Networks (ANN) and Logistic Regression (LR). This study is one of the first in credit card fraud detection with a real data set to compare the performance of ANN and LR. Zhenisbek Assylbekov et al. presented statistical techniques for detecting VAT evasion by Kazakhstani business firms [8]. Starting from features selection they performed an initial exploratory data analysis using Kohonen self-organizing maps. Hussein et al. described classification-based and clustering-based anomaly detection techniques [9]. They applied K-Means to a refund transaction data set from a telecommunication company, with the intent of identifying fraudulent refunds. Gonzlez et al. described methods to detect potential false invoice issuers/users based on the information in their tax return statements using different types of data mining techniques [10]. First, clustering algorithms like SOM and neural gas are used to cluster
similar taxpayers. Then decision trees, neural networks, and Bayesian networks are used to identify those features that are related to the conducting of fraud and/or no fraud. Song Wang et al. introduced the challenges of anomaly detection in the traditional network, as well as in the next generation network, and reviewed the implementation of machine learning in the anomaly detection under different network contexts [11].

Leung et al. proposed various machine learning technique to address the issues of anomaly detection and imbalance categorization [12]. Shuhan Yuan et al. used a deep learning approach for fraud detection [13]. This method will work only for the labeled data set. Jian Chen et al. applied deep learning techniques to credit card fraud detection. They first used sparse autoencoder to obtain representations of normal transactions and then trained a generative adversarial network (GAN) with these representations. Finally, they combined the SAE and the discriminator of GAN and applied them to detect whether a transaction is genuine or fraud [14]. Shenggang Zhang et al. proposed an anomaly detection model based on BiGAN for software defect prediction. The model proposed by them not only does not need to consider the class imbalance problem but also uses a semi-supervised method to train the model [15]. Raghavendra Chalapathy et al. presented a structured and comprehensive overview of research methods in deep learning-based anomaly detection. Furthermore, they reviewed the adoption of these methods for anomaly detection across various application domains and assess their effectiveness [16].

III. DESCRIPTION OF THE DATA SET

GSTR-3B is a monthly return that has to be filed by the dealer. It is a simple return in which a summary of Input Tax Credit along with outward supplies are declared, and payment of tax is affected by the taxpayer. Table I is a sample of GST returns data. Each row in this table corresponds to a monthly return by a dealer. ITC (Input tax credit) is the amount of tax paid during purchases of services/goods by the dealer. The output tax is the amount of tax collected by the dealer during the sales of services/goods. The dealer has to pay the Government the gap between the output tax and ITC, i.e., output tax - ITC. The actual database consists of much more information, like, return filing data, tax payment method, exempted sales, international exports, and sales on RCM (reverse charge mechanism). Figures 2, 3, 4, and 5 show the distribution of turnover, liability, input tax credit, and cash payments.

| S.No. | Firm | Month | Purchases | Sales | ITC  | Output Tax |
|-------|------|-------|-----------|-------|------|------------|
| 1     | BC   | Jan 2019 | 190000    | 210000 | 20200 | 24000      |
| 2     | BE   | Sep 2021 | 202000    | 270000 | 5200  | 9200       |
| 3     | BD   | Oct 2021 | 400200    | 420000 | 41000 | 43000      |

Table I: GST Returns Data (GSTR-3B)

IV. ENHANCED BiGAN

A. Generative Adversarial Network

A generative adversarial network (GAN) is a recent invention in deep learning designed by Ian Goodfellow and
his colleagues [2]. Two neural network modules (generator, discriminator) compete with each other in a simultaneous game. Given a training data set (ground-truth data set), the generator learns to generate new data with the same statistics as the training data set and the discriminator learns to estimate the probability that the given input came from the training data set rather than generated by the generator.

The discriminator’s parameters are optimized to minimize the loss function in Equation 1. Here $D_I$ is the estimated probability by the discriminator that input came from the ground-truth data set rather than generated by the generator given the ground-truth data set as input, and $D_G$ is the estimated probability by the discriminator that input came from the ground-truth data set rather than generated by the generator given the generated data set as input. The generator’s parameters are optimized to minimize the loss function in Equation 2.

$$-1 \times (\log(D_I) + \log(1 - D_G)) \quad (1)$$
$$-1 \times (\log(D_G)) \quad (2)$$

B. Bidirectional GAN

Bidirectional GAN (BiGAN) is a representation learning method. BiGAN adds an encoder to the standard GAN architecture. The encoder takes ground-truth data set $X$ and outputs a latent representation $E(X)$ of this data set. The generator takes a random sample $z$ and generates a data set $G(z)$. The BiGAN discriminator discriminates not only $X$ versus $G(z)$, but jointly in data and latent space (discriminates tuple $(X, E(X))$ versus tuple $(G(z), z)$).

The discriminator is trained to minimize Equation 3, where $D_E$ is the estimated probability by the discriminator that input came from $(X, E(X))$ rather than $(G(z), z)$ given $(X, E(X))$ as the input, and $D_G$ is the estimated probability by the discriminator that input came from $(X, E(X))$ rather than $(G(z), z)$ given $(G(z), z)$ as the input. The generator is trained to minimize Equation 4. The encoder is trained to minimize Equation 5

$$-1 \times (\log(D_E) + \log(1 - D_G)) \quad (3)$$
$$-1 \times (\log(D_G)) \quad (4)$$
$$-1 \times \log(1 - D_E) \quad (5)$$

C. Enhanced Bidirectional GAN

Kaplan et al. suggested one more cost function to optimize generator and encoder parameters of BiGAN [4]. Let $X$ be the current batch of input data set and $E(X)$ be the output of encoder with $X$ as input. Let $G(E(X))$ be the output of generator with $E(X)$ as input. They suggested to update encoder’s and generator’s parameters together to minimize the mean of euclidean distance between $X$ and $G(E(X))$ as in Equation 6.
Cosine similarity is a measure used to find similarity between two vectors. Mathematically, it measures the cosine of the angle between two vectors projected in a multidimensional space. We propose that increasing the cosine similarity between \( X \) and \( G(E(X)) \) is a better approach than minimizing the euclidean distance between them. We update encoder's and generator's parameters together to increase the cosine similarity between \( X \) and \( G(E(X)) \).

\[
\text{mean of cosine similarity}(X, G(E(X)))
\]

\[
\text{mean of euclidean distance}(X, G(E(X)))
\]

**V. Methodology**

The objective of this work is to train Bidirectional GAN (BiGAN) using the proposed training approach on nine-dimensional ground-truth data derived from tax returns submitted by taxpayers (six correlation parameters and three ratio parameters) to identify malicious dealers who manipulate their tax return statements. We had taken the data sets explained in Section III from July 2017 to March 2022 and derived nine features (parameters) from these data sets.

- Six are sensitive correlation parameters.
- Three are ratio parameters.

In Subsection V-A, we explain the six correlation parameters that are used. In Subsection V-B, we describe the three ratio parameters that are used. In Subsection V-C, we give a detailed algorithm.

**A. Correlation parameters**

In the Indian GST system, three types of taxes are collected, viz., CGST, SGST, and IGST.

- **CGST:** Central Goods and Services Tax is levied on intrastate transactions and collected by the Central Government of India.
The Six Correlation Parameters

| S. No. | The Six Correlation Parameters |
|--------|-------------------------------|
| 1      | Total GST Liability VS Total Sales Amount |
| 2      | SGST Liability VS Total GST Liability |
| 3      | SGST paid in cash VS SGST Liability |
| 4      | SGST paid in cash VS Total Sales Amount |
| 5      | Total ITC VS Total Tax Liability |
| 6      | IGST ITC VS Total Tax Liability |

Table II: correlation parameters

- **SGST**: State/Union Territory Goods and Services Tax, which is also levied on intrastate transactions and collected by the state or union territory Government.
- **IGST**: Integrated Goods and Services Tax is levied on interstate sales. Central Government takes half of this amount and passes the rest of the amount to the state, where corresponding goods or services are consumed.

The six correlation parameters are mentioned in Table II. Total GST liability is the sum of CGST liability, SGST liability, and IGST liability. Total ITC is equal to the sum of SGST ITC, CGST ITC, and IGST ITC.

### B. Ratio parameters

1) The ratio of **Total Sales VS. Total Purchases**: This ratio captures the value addition.

2) The ratio of **IGST ITC VS. Total ITC**: This ratio captures how much purchase is shown as interstate or imports compared to total purchases.

3) The ratio of **Total Tax Liability VS. IGST ITC**.

### C. Identifying Fraudulent Taxpayers using BiGAN

**Algorithm 2**: Identifying Fraudulent Taxpayers

**Data**: Nine Dimensional Ground-Truth Data (GT)

**Result**: Fraudulent Taxpayers

1. Train a BiGAN with the ground-truth data set $GT$ using Algorithm 1
2. $LR$ $\leftarrow$ latent representation of the ground-truth data set $GT$ computed using the encoder
3. $RG$ $\leftarrow$ output of the generator with $LR$ as the input
4. $CS$ $\leftarrow$ Cosine similarity between corresponding rows of $GT$ and $RG$
5. $Fraudset$ $\leftarrow$ taxpayers whose similarity score is less than $first\ quantile - 1.5 * IQR$

### VI. Experimentation and Results Obtained

We had taken returns data of 1184 iron and steel dealers. We computed correlation and ratio parameters defined in subsections V-A and V-B for each dealer. Table III gives a snapshot of the parameters created for each dealer. Figure 10 and Figure 11 show the distribution of correlation and ratio parameters respectively. Figures 7, 8, and 9 give the PyTorch code of discriminator, generator, and encoder respectively.

After experimentation, we opted for four-dimensional latent space. Note that input to the discriminator is thirteen dimensions (four-dimensional latent space data and nine-dimensional training/ground-truth data set).

Figure 12 shows the discriminator’s error at different epochs. Figure 13 shows the average cosine similarity measure between corresponding rows in the training data set and regenerated data set at different epochs. The boxplot in Figure 14 shows the distribution of cosine similarities between corresponding rows in the training data set and regenerated set at the final epoch. The third quantile value is 0.8992, first quantile value is 0.6827. There are nineteen taxpayers whose cosine similarity values are less than the first quantile $− 1.5 * IQR$.

Tax returns of these taxpayers need further investigation by tax officers. Expected evasion by these taxpayers is more than a few hundred million Indian rupees.

### VII. Conclusion

In this paper, we enhanced the BiGAN training approach given in [4]. This training approach significantly improved the performance/stability of BiGAN.

We analyzed the tax returns data set of a set of business dealers in the state of Telangana, India, to identify dealers.
who perform extensive tax evasion. We had taken data of 1184 iron and steel dealers and derived ground-truth data set based on their monthly returns. The ground-truth data contains nine parameters (six are correlation parameters and three are ratio parameters). We used the proposed method of BiGAN training to identify fraudulent dealers. First, we trained a BiGAN using the ground-truth data set. Next, we encoded the ground-truth data set using the encoder and decoded it back using the generator by giving the latent representation as input. For each taxpayer, we computed the cosine similarity between his/her ground-truth data and regenerated data. Taxpayers with lower cosine similarity measures are potential return manipulators. We identified nineteen dealers whose cosine similarity score is less than the first quantile \(-1.5 \ast IQR\). Expected

```python
class Discriminator(nn.Module):
    def __init__(self):
        super().__init__()
        self.model = nn.Sequential(
            nn.Linear(43, 32),
            nn.ReLU(),
            nn.Linear(32, 64),
            nn.ReLU(),
            nn.Linear(128, 64),
            nn.ReLU(),
            nn.Linear(64, 32),
            nn.ReLU(),
            nn.Linear(16, 1),
            nn.Sigmoid(),
        )

    def forward(self, x):
        return self.model(x)

class Generator(nn.Module):
    def __init__(self):
        super().__init__()
        self.model = nn.Sequential(
            nn.Linear(64, 32),
            nn.ReLU(),
            nn.Linear(16, 1),
            nn.Sigmoid(),
        )

    def forward(self, latent):
        return self.model(latent)

class Encoder(nn.Module):
    def __init__(self):
        super().__init__()
        self.model = nn.Sequential(
            nn.Linear(9, 32),
            nn.ReLU(),
            nn.Linear(32, 64),
            nn.ReLU(),
            nn.Linear(128, 64),
            nn.ReLU(),
            nn.Linear(64, 32),
            nn.ReLU(),
            nn.Linear(32, 4),
        )
```

Figure 7: Discriminator

Figure 8: Generator

Figure 9: Encoder

Figure 10: Correlation Parameters

Figure 11: Ratio Parameters

Figure 12: Discriminator Error
evasion by these taxpayers is more than a few hundred million Indian rupees.

ACKNOWLEDGMENT

We express our sincere gratitude to the Telangana state Government, India, for sharing the commercial tax data set, which is used in this work.

REFERENCES

[1] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM Comput. Surv., vol. 41, no. 3, pp. 15:1–15:58, 2009. [Online]. Available: https://doi.org/10.1145/1541880.1541882

[2] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets,” in Advances in Neural Information Processing Systems, Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, and K. Weinberger, Eds., vol. 27. Curran Associates, Inc., 2014. [Online]. Available: https://proceedings.neurips.cc/paper/2014/file/5ca3e9b1226f1f80f6949e97b1afcc3-Paper.pdf

[3] J. Donahue, P. Krähenbühl, and T. Darrell, “Adversarial feature learning,” CoRR, vol. abs/1605.09782, 2016. [Online]. Available: http://arxiv.org/abs/1605.09782

[4] M. O. Kaplan and S. E. Alptekin, “An improved bigan based approach for anomaly detection,” in KES, 2020.

[5] S. Dani, “A research paper on an impact of goods and service tax (gst) on indianelawy,” Business and Economics Journal, vol. 7, pp. 1–2, 2016.

[6] D. de Roux, B. Perez, A. Moreno, M. Villamil, and C. Figueroa, “Tax fraud detection for under-reporting declarations using an unsupervised machine learning approach,” in Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, KDD 2018, London, UK, August 19-23, 2018. Y. Guo and F. Farooq, Eds. ACM, 2018, pp. 215–222. [Online]. Available: https://doi.org/10.1145/3219819.3219878

[7] Y. Sahin and E. Duman, “Detecting credit card fraud by ann and logistic regression,” 2011 International Symposium on Innovations in Intelligent Systems and Applications, pp. 315–319, 2011.

[8] Z. Assylbekov, I. Melnykov, R. Bekishev, A. Baltabayeva, D. Bissen-galiyeva, and E. Mamlin, “Detecting value-added tax evasion by business entities of kazakhstan,” in Intelligent Decision Technologies 2016 - Proceedings of the 8th KES International Conference on Intelligent Decision Technologies, KES-IDT 2016, ser. Smart Innovation, Systems and Technologies, L. Jain, R. Howlett, I. Czarnowski, A. Caballero, L. Jain, and L. Jain, Eds. Germany: Springer Science and Business Media Deutschland GmbH, 2016, pp. 37–49, 8th KES International Conference on Intelligent Decision Technologies, KES-IDT 2016 ; Conference date: 15-06-2016 Through 17-06-2016.

[9] H. Issa and M. A. Vasarhelyi, “Application of anomaly detection techniques to identify fraudulent refunds,” Economics of Innovation and Journal, 2011.

[10] P. C. González and J. D. Velásquez, “Characterization and detection of taxpayers with false invoices using data mining techniques,” Expert Syst. Appl., vol. 40, pp. 1427–1436, 2013.

[11] S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez, and B. Rubinstein, “Machine learning in network anomaly detection: A survey,” IEEE Access, vol. 9, pp. 152379–152396, 2021.

[12] Leung, Kingsly, Leckie, and Christopher, “Unsupervised anomaly detection in network intrusion detection using clusters,” in Proceedings of the Twenty-Eighth Australasian Conference on Computer Science - Volume 38, ser. ACSC '05. AU: Australian Computer Society, Inc., 2005, p. 333–342.

[13] S. Yuan, X. Wu, J. Y. Li, and A. Lu, “Spectrum-based deep neural networks for fraud detection,” Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, 2017.

[14] J. Chen, Y. Shen, and R. Ali, “Credit card fraud detection using sparse autoencoder and generative adversarial network,” 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1054–1059, 2018.

[15] S. Zhang, S. Jiang, and Y. Yan, “A software defect prediction approach based on bigan anomaly detection,” Scientific Programming, vol. 2022, 2022.

[16] R. Chalapathy and S. Chawla, “Deep learning for anomaly detection: A survey,” CoRR, vol. abs/1901.03407, 2019. [Online]. Available: http://arxiv.org/abs/1901.03407