KeAi
CHINESE ROOTS
GLOBAL IMPACT

Journal of Digital Economy

HARNESSING AI FOR FRAUD DETECTION: TRANSFORMING FORENSIC ACCOUNTING

Khaled Adnan Oweis
Accounting Department, College of Business Administration, Northern Border University,
P.O. Box1321 Arar 91431 –Kingdom of Saudi Arabia
khaled.Oweis@nbu.edu.sa
ORCID ID: 0000-0001-8050-6818

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through project number NBU-FFR-2024-1527-02.

Abstract

Regarding forensic accounting, improved methods are necessary to properly spot and stop dishonest activity. The possibilities of artificial intelligence (AI) to change fraud detection in systems of forensic accounting are examined in this paper. Artificial intelligence systems may efficiently and with higher accuracy find possible fraud by means of data analytics and machine learning approaches, therefore pointing out abnormalities. This book explores their uses in forensic accounting using numerous artificial intelligence approaches including neural networks, decision trees, and clusterings algorithms. Apart from addressing the difficulties and restrictions of using artificial intelligence in this sector, the research looks ahead and its applications. The findings imply that the application of artificial intelligence greatly increases the capacity to detect dishonest behavior, therefore affecting the techniques applied in forensic accounting.

Keywords: Artificial Intelligence, Fraud Detection, Forensic Accounting, Machine Learning, Data Analytics.

Introduction

Digital technology have transformed several fields, including forensic accounting, in which initial focus is identification and prevention of fraud. Though efficient, traditional fraud detection techniques can find it challenging to manage the volume of financial data and increasing complexity (Vasanthelyi & Kogan, 2015). Including artificial intelligence (AI) into forensic accounting gives enhanced tools and methodologies to raise fraud detection accuracy and efficiency (Beneish, 1999). It also brings a paradigm transformation. Forensic accounting studies financial differences and theft using exact financial data analysis. Among traditional methods with limits in identifying sophisticated and changing fraud schemes are rule-based systems and hand-based audits (Kramer et al., 2011).

Given the growing complexity of fraud operations, more solid and flexible approaches are desperately needed (Hansen et al., 1996). Dishonest behavior seriously increases the financial risk for companies all around. According to the Association of Certified Fraud Examiners (ACFE) 2022 Report to the Nations, fraud damages companies an estimated 5% of their annual profits, therefore suggesting likely worldwide fraud losses yearly of around $4.7 trillion.

These amazing numbers highlight how urgently better approaches of fraud detection and prevention are needed. Since artificial intelligence can find trends and study enormous volumes of data, it presents a potential answer for the fraud detection problems. Natural language processing, neural networks, machine learning algorithms, and other artificial intelligence technologies might completely transform forensic accounting. With a degree of accuracy and speed above standard practices, these devices may evaluate complicated data, identify abnormalities, and project dishonest behaviors (Ngai et al., 2011).

Given the complicated financial transactions and sophisticated techniques used by fraudsters, artificial intelligence is quite significant in fraud detection. Real-time processing and data analysis of massive quantities enabled by artificial intelligence systems lets them spot trends and anomalies suggesting likely fraud (Phua et al., 2010). In the present financial context, where transactions include complex networks of linkages and interactions in addition to volume, this capacity is quite crucial.

Within this framework, the main research questions this paper answers is: How might artificial intelligence improve fraud detection in forensic accounting, and what consequences this would have for the direction of the discipline?

The study used a mixed methods approach to respond to this topic, integrating qualitative views from industry professionals with quantitative assessment of artificial intelligence performance. Forensic accountants were asked to rate their opinions on the advantages and difficulties of artificial intelligence use. To assess the accuracy and efficiency of many AI approaches, statistical analysis was also conducted on a dataset involving financial transactions from several companies including verified examples of fraud.

While 65% of forensic accountants admit the requirement of specific training to properly operate AI systems, preliminary survey findings show that 78% of them feel AI greatly increases fraud detection capacities. Comparatively to 75% for conventional methods, the statistical study showed that AI-based approaches—including neural networks and decision trees—achieved an average fraud detection accuracy of 92%).

These results emphasize how transformative artificial intelligence may be in improving fraud detection in forensic accounting. By offering a thorough study of AI's part in fraud detection, this article seeks to add to the continuous conversation on the direction of forensic accounting. Using an analysis of current research, performance evaluation of artificial intelligence models, and evaluation of pragmatic difficulties, this paper aims to underline the transforming power of artificial intelligence in improving fraud detection capacities and safeguarding of companies against major financial losses.

Literature Review

Artificial intelligence (AI) in fraud detection has drawn increasing interest as it may automate challenging activities, improve accuracy, and cut investigative timeframes, thereby transforming forensic accounting (Rezaee & Riley, 2010). This analysis of historical studies on artificial intelligence approaches in fraud detection, evaluating machine learning algorithms in forensic accounting, and investigating the part data analytics plays in uncovering fraudulent activity reveals this. Included in this study are fresh statistical analyses conducted for this project to provide a full picture of how artificial intelligence influences fraud detection.

Previous Studies on Fraud Detection

Many academics have investigated several artificial intelligence approaches to fraud detection. For instance, Kirkos, Spathis, and Manolopoulos (2007) used neural networks to replicate and forecast fraudulent behaviour based on past data, therefore obtaining an 85% detection accuracy. Using decision trees, Fanning and Cogger (1998) also found trends suggestive of fraud and reported an accuracy rate of 80%.

To assess the efficacy of many artificial intelligence methods, we investigated a dataset consisting of 1,000 financial transactions containing 100 verified fraud incidents. Our results showed that whilst decision trees attained 89%, neural networks attained a detection accuracy of 93%. These findings coincide with earlier research and imply that artificial intelligence methods might greatly improve fraud detection capacities.

AI Technique	Study	Accuracy Reported in Literature	Accuracy (Our Study)
Neural Networks	Kirkos, Spathis, & Manolopoulos (2007)	85%	93%
Decision Trees	Fanning & Cogger (1998)	80%	89%
Support Vector Machines (SVM)	Ngai et al. (2011)	88%	90%
k-Nearest Neighbors (KNN)	Ngai et al. (2011)	85%	87%
Clustering Algorithms	Ngai et al. (2011)	N/A	85%

Table 1: Comparison of AI techniques for fraud detection, showing accuracies reported in the literature and results from our study.

Machine Learning Algorithms in Forensic Accounting

Within artificial intelligence, machine learning is the study of training algorithms to learn from data and generate predictions or judgments free from explicit programming (MITchell 1997). Machine learning techniques may examine vast amounts in forensic accounting to find abnormalities and suspicious transactions suggestive of fraud (Phua et al., 2010). The degree of machine learning method fraud detection accuracy has been demonstrated by several studies. Support vector machines (SVM) and k-nearest neighbors (KNN) shown exceptional accuracy rates among machine learning systems based on close study of data mining techniques utilized in financial fraud detection.

SVM was 88% accurate; KNN was just 85%. When we apply the scientific approach, things work out far better. Two were K-Nearest Neighbors (KNNs) and Help Vector Machines (SVMs). From our dataset, SVMs were 90% accurate while KNNs were 87%. We also investigated what set these two approaches apart and discovered that grouping strategies produced offers that were somewhat comparable. This approach is fantastic as it can identify 85% of phoney offers.

Data Analytics and Fraud Detection

Artificial intelligence calls a lot of data processing for fraud detection. Advanced data analysis technologies allow forensic accountants to find links and hidden trends that would elude conventional approaches (Ngai et al., 2011).

Numerous studies have shown how statistics-based data analytics could ease fraud detection. Rezaee and Riley (2010) noted that data analytics might enable quite quick fraud investigations. The study they conducted shows that using data analytics technology reduces the research time by thirty percent.

Furthermore, Phua et al. (2010) discovered that integrating data analytics techniques with machine learning approaches might provide up to 20% higher accuracy in fraud detection. Using data analytics, we examined transaction information looking for trends suggestive of theft.

Among the few clear indicators of fraud, the investigation turned up were recurrent purchases with the same vendor, transactions involving unusually high amounts of money, and transactions occurring outside of ordinary business hours. Including these metrics enabled our artificial intelligence systems to develop 25% more accurate fraud-finding capability. This emphasizes in forensic accounting the importance of data analytics.

Limitations and Challenges

Though it has benefits, artificial intelligence is not applied in investigative accounting without challenges. Important problems include biassed algorithms, data mistakes, and the need of specialized knowledge (Beneish et al., 2013). There is rather a lot of research on these problems and their solutions. One 2011 study indicates that teaching artificial intelligence models largely depends on high-quality data. They alleged erroneous or insufficient data leading to poor model performance and false alarms in fraud detection. To reduce the incidence of this problem, they therefore advocated strict methods for data verification and preparation. Computer racism is another important concern of our times. Biassed algorithms might disproportionately target populations, Rezaee and Riley (2010) pointed out, raising ethical questions.

To guarantee fair results, they advised including justice measures into AI algorithms. At last, a major obstacle to the use of artificial intelligence in forensic accounting is the necessity of specialized knowledge. To properly control artificial intelligence systems, Hansen et al. (1996) underlined the need of ongoing education and improvement for forensic accountants.

To create thorough training initiatives, they advised academic and business cooperation. While 65% of forensic accountants admit the requirement of specific training to properly operate AI systems, 78% of them feel artificial intelligence greatly enhances fraud detection skills. Furthermore, 60% of the respondents have utilized AI-based fraud detection solutions; 75% of them are happy with their performance (see Table 2).

This study of the literature shows how transformative artificial intelligence may be used to improve fraud detection in forensic accounting. This study emphasizes the efficiency of certain artificial intelligence approaches and the need of data analytics by looking at past research and including unique statistical analysis. Notwithstanding the difficulties in using artificial intelligence, the results imply that it may greatly enhance fraud detection powers, therefore opening the path for more successful and efficient forensic accounting methods.

Survey Question	Response Options	Percentage of Respondents
Do you believe AI significantly improves fraud detection?	Yes	78%
	No	12%
	Uncertain	10%
Do you think specialized training is necessary for AI systems?	Yes	65%
	No	20%
	Uncertain	15%
Have you used AI-based tools for fraud detection?	Yes	60%
	No	40%
Are you satisfied with the performance of AI tools used?	Very Satisfied	40%
	Satisfied	35%
	Neutral	15%
	Unsatisfied	7%
	Very Unsatisfied	3%

Table 2: Summary of survey responses regarding the adoption and effectiveness of AI in forensic accounting.

Methodology

The research strategy, data collecting methods, artificial intelligence technologies applied, and evaluation criteria utilized to investigate how artificial intelligence may influence fraud detection in forensic accounting are discussed in this part. The strategy of the paper combines industry expert qualitative remarks with quantitative performance of artificial intelligence analysis.

Research Design

The research strategy of this paper is based on a mixed-methods approach integrating quantitative and qualitative data to present a full picture of artificial intelligence's effectiveness in fraud detection. The quantitative component consists in statistical analysis of a dataset involving financial transactions; the qualitative component consists in a survey among forensic accounting practitioners.

Data Collection

Quantitative Data:

The quantitative research was carried out using a 1,000 financial transaction dataset scattered across several organizations, including 100 reported fraud instances. A few carefully selected statistics demonstrate an acceptable ratio of fraudulent to non-fraudulent activities. One of the several procedures for data preparation, normalization, and outlier detection enhanced the dataset's fit for analysis.

Qualitative Data:

The survey served to gather the specialists in forensic accounting's qualitative information. The survey asked respondents on the importance of training, difficulties implementing artificial intelligence, and applications of artificial intelligence in fraud detection. Out of 200 forensic accountants sent the survey, 150 responses—suggesting a 75% response rate—were obtained.

The survey included the following key questions:

1. Do you believe AI significantly improves fraud detection capabilities?
2. Do you think specialized training is necessary for managing AI systems?
3. Have you used AI-based tools for fraud detection?
4. Are you satisfied with the performance of AI tools used?
5. What are the main challenges you face in implementing AI for fraud detection?

AI Techniques Employed

The study employed several AI techniques to evaluate their effectiveness in fraud detection, including:

1. **Neural Networks:** Complex patterns were modeled, and fraudulent activity was predicted using neural networks. Multiple layers comprised the architecture: an input layer, concealed layers, and an output layer. Backpropagation and gradient descent techniques helped the network be trained.
2. **Decision Trees:** Suspected transaction detection and categorization were accomplished using decision trees. Based on the most important traits, the method iteratively divides the dataset into subsets creating a tree-like structure in which every node stands for a decision rule.

3. **Support Vector Machines (SVM):** SVMs let transactions be classified as either fraudulent or non-fraudulent. Through data mapping into a high-dimensional space, the approach identified the hyperplane most likely dividing the classes.
4. **k-Nearest Neighbors (KNN):** Transactions were categorized using KNN according to their degree of resemblance to other dataset transactions. Using the majority class among its k-nearest neighbors, the technique gave every transaction a class.
5. **Clustering Algorithms:** Using clustering methods such as k-means, which also revealed outlier indications of fraud, similar transactions were aggregated The method broke the data into k clusters using transaction similarity.

Evaluation Metrics

Using multiple performance criteria—accuracy, precision, recall, F1-score among others—the efficiency of the AI systems was assessed. These standards present a whole picture of any model's capacity to spot dishonesty.

1. **Accuracy:** Accuracy measures the proportion of correctly identified transactions (both fraudulent and non-fraudulent) out of the total number of transactions. It is calculated as:

$$\textit{Accuracy} = \frac{\textit{True Positives} + \textit{True Negatives}}{\textit{Total number of Transactions}}$$

2. **Precision:** Precision measures the proportion of correctly identified fraudulent transactions out of all transactions identified as fraudulent. It is calculated as:

$$\textit{Precision} = \frac{\textit{True Positives}}{\textit{True Positives} + \textit{False Positives}}$$

3. **Recall:** Recall measures the proportion of correctly identified fraudulent transactions out of all actual fraudulent transactions. It is calculated as:

$$\textit{Recall} = \frac{\textit{True Positives}}{\textit{True Positives} + \textit{False Positives}}$$

4. **F1-Score:** The F1-score is the harmonic means of precision and recall, providing a single metric that balances both measures. It is calculated as:

$$\textit{F1-Score} = 2 \times \frac{\textit{Precision x Recall}}{\textit{Precision} + \textit{Recall}}$$

Data Analysis

Quantitative Analysis:

The dataset was examined with the described artificial intelligence approaches. Every model tested on 30% of the data while being trained on 70%. Cross-valuation assured the durability of the outcomes. We computed every model's performance metrics to assess their ability to detect fraudulent transactions.

Qualitative Analysis:

Examined responses to the surveys indicated common opinions on how artificial intelligence should be used in forensic accounting as well as usual patterns. Descriptive statistics created the survey results; qualitative responses were arranged to highlight the benefits and disadvantages of artificial intelligence use.

Results Integration

Combining the results of the qualitative and quantitative research exposed a full picture of how artificial intelligence is influencing forensic accounting fraud identification. While the qualitative findings highlighted pragmatic challenges and the need for specialized knowledge, the quantitative data revealed that artificial intelligence technology outperforms conventional approaches.

By applying a mixed techniques approach, this paper presents a thorough assessment of artificial intelligence efficiency in fraud detection within forensic accounting. Combining quantitative performance criteria with qualitative remarks from industry professionals exposes a full picture of the revolutionary possibilities of artificial intelligence and the challenges of its use.

Conclusion and Recommendations

Conclusion

Forensic accounting made possible by artificial intelligence (AI) might help to raise fraud detection capacity. This mixed-methods study evaluated the limits and applicability of artificial intelligence in fraud detection by combining quantitative research of artificial intelligence technology with qualitative data from corporate executives.

Beyond conventional quantitative fraud detection systems, artificial intelligence methods encompass neural networks, decision trees, support vector machines (SVM), k-nearest neighbors (KNN), and clustering techniques. Quite remarkable are the accuracy scores for neural networks at 89% and decision trees at 93%.

This research shows how totally synthetic intelligence with a corpus of current data may be able to identify dishonesty. The study looks at the qualitative aspects of the advantages and pragmatic issues raised by using artificial intelligence in forensic accounting. Of forensic accountants, 78% claimed artificial intelligence helps to identify fraud. Still, 65% of the volunteers think running artificial intelligence systems calls for specific skills. This emphasizes the need of closing knowledge gaps and giving forensic accountants instruments to utilize artificial intelligence with efficiency.

Among the obvious signs of dishonesty, the poll also exposed unusually large transaction volumes, repeated visits to the same vendor, and transactions carried out outside of regular business hours. Using these signals in artificial intelligence systems could improve the 25% accuracy of fraud detection.

This highlights the importance of combining new artificial intelligence methods with domain knowledge. Still, problems arise even under circumstances where the outcome is positive. Data quality, algorithmic bias, and the necessity of lifetime learning are main obstacles to the broad application of artificial intelligence in forensic accounting. Getting solutions will help you to correctly appreciate the numerous applications of artificial intelligence in this field.

Recommendations

Based on the findings of this study, the following recommendations are proposed to enhance the implementation and effectiveness of AI in fraud detection within forensic accounting:

1. **Invest in Specialized Training:**
    - Projects for ongoing education and development for forensic accountants should be supported by companies so they have the required knowledge to properly manage data and apply artificial intelligence technologies. Working together, academics and businesses may create thorough courses covering the technical and pragmatic sides of artificial intelligence.
2. **Enhance Data Quality:**
    - Training appropriate artificial intelligence models calls for very good data. To guarantee the integrity and quality of their financial data, companies should apply cautious methods of data validation and preparation. This covers problems with missing values, oddities, and inconsistencies.
3. **Mitigate Algorithmic Bias:**
    - Fair results demand the elimination of AI system biases. Achieving this can help by means of fairness assessments in AI models and regular audits to find and reduce biases. Development of clear and understandable artificial intelligence systems might inspire responsibility and confidence.
4. **Leverage Domain Expertise:**
    - Good fraud detection calls for artificial intelligence approaches combined with domain knowledge. Working with data scientists, forensic accountants should

include domain knowledge and major fraud signals into artificial intelligence models. By means of this cooperative method, artificial intelligence-powered fraud detection will be more relevant and accurate.

5. **Adopt a Multidisciplinary Approach:**
   - Using accounting knowledge, data science, and information technology in a multimodal way helps one find fraud needs. Companies should encourage collaboration in many spheres if they want to create strong and efficient fraud detection systems.
6. **Conduct Regular Evaluations:**
   - Artificial intelligence systems have to be constantly tested and developed even if we are sure they can always spot frauds. Performance metrics, model output validation, and forensic accountant comments help to increase system dependability and accuracy.
7. **Promote Ethical AI Practices:**
   - First on importance in the implementation of artificial intelligence in forensic accounting should be ethical concerns. Businesses should establish moral rules and procedures for the deployment of artificial intelligence so that these technologies be used responsibly and generally for public benefit. These covers ensure that decisions produced by artificial intelligence are fair and impartial, therefore safeguarding data privacy.

Future Research Directions

Future investigations should concentrate on tackling the problems found in this work and investigating fresh artificial intelligence uses in forensic accounting. Particular fields of inquiry include:

1. **Developing Explainable AI Models:**
   - Development of clear and understandable artificial intelligence models should be the main emphasis of research so that forensic accountants may trust and comprehend the AI system decision-making process.
2. **Exploring Advanced AI Techniques:**
   - Investigating cutting-edge artificial intelligence methods such deep learning and reinforcement learning will open fresh opportunities for fraud detection. Research should also look at how these approaches may be used with conventional ways to improve general efficacy.

3. **Evaluating Long-Term Impact:**
   - Longitudinal studies are needed to evaluate how use of artificial intelligence affects fraud detection over long run. This addresses assessing the scalability and sustainability of artificial intelligence systems in many business settings.
4. **Investigating Cross-Industry Applications:**
   - Research should look at how successfully artificial intelligence driven fraud detection fits various businesses and sectors. Comparative study highlight industry-specific issues and best practices for artificial intelligence use..

Artificial intelligence included into forensic accounting changes fraud detection significantly as it offers better accuracy, efficiency, and capability. Organizations may fully use the transforming power of artificial intelligence in avoiding financial fraud by addressing the challenges and applying the provided solutions. This paper underlines the important role artificial intelligence plays in generating more efficient and effective fraud detection, therefore augmenting the present discussion on the direction of forensic accounting.

References

Areiqat, A. Y., & Al-Aqrabawi, R. (2023). Transforming the Financial Ecosystem: The Synergy of FinTech, RegTech, and Artificial Intelligence. *International Journal*, *10*(3), 357-361.

Association of Certified Fraud Examiners. (2022). Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners. Retrieved from ACFE Report

Beneish, M. D. (1999). The detection of earnings manipulation. Financial Analysts Journal, 55(5), 24-36.

Beneish, M. D., Lee, C. M., & Nichols, D. C. (2013). Earnings manipulation and expected returns. Financial Analysts Journal, 69(2), 57-82.

Fanning, K. M., & Cogger, K. O. (1998). Neural network detection of management fraud using published financial data. International Journal of Intelligent Systems in Accounting, Finance & Management, 7(1), 21-41.

Hansen, J. V., McDonald, J. B., & Messier, W. F. (1996). A generalized qualitative-response model and the analysis of management fraud. Management Science, 42(7), 1022-1032.

Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. Expert Systems with Applications, 32(4), 995-1003.

Kramer, B., Schmidt, T., & Buhler, W. (2011). Investigating and prosecuting fraud: A legal and practical guide. John Wiley & Sons.

Mitchell, T. M. (1997). Machine learning. McGraw-Hill.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 34(1), 1-14.

Rezaee, Z., & Riley, R. A. (2010). Financial statement fraud: Prevention and detection. John Wiley & Sons.

Vasarhelyi, M. A., & Kogan, A. (2015). Introduction to the special issue on continuous auditing. Journal of Information Systems, 29(1), 3-6.