Artificial Intelligence in Forensic Accounting: A Literature Review

Hongtao Guo
Salem State University

Zaiyong Tang
Salem State University

This literature review examines the transformative impact of artificial intelligence (AI) on forensic accounting. Drawing from recent academic research, industry reports, and global case studies, the review traces the historical evolution of AI applications—from early expert systems to modern machine learning and natural language processing techniques. Key challenges, such as data quality, model explainability, ethical concerns, and regulatory gaps, are examined alongside the opportunities that AI presents, including improved detection accuracy, real-time monitoring, and the ability to analyze unstructured data. The review emphasizes the synergistic relationship between human expertise and AI, advocating for hybrid approaches that enhance investigative efficiency and objectivity. It also identifies future research directions, including explainable AI, blockchain analytics, continuous auditing, and the integration of advanced techniques such as federated learning. This review offers scholars and practitioners a comprehensive and up-to-date understanding of how AI is transforming forensic accounting practices globally.

Keywords: artificial intelligence, forensic accounting, fraud detection, machine learning

INTRODUCTION

Financial fraud and white-collar crime continue to inflict enormous costs on organizations worldwide, with recent estimates suggesting over $4.7 trillion lost annually to occupational fraud (Association of Certified Fraud Examiners (ACFE), 2022). This pervasive risk has fueled the growth of forensic accounting, a specialized field dedicated to detecting, investigating, and preventing financial misconduct. In recent years, the advent of artificial intelligence (AI) has introduced new tools to this domain (Ellili et al., 2024), promising to augment the capabilities of forensic accountants in unprecedented ways. AI technologies, such as machine learning (ML), natural language processing (NLP), robotic process automation (RPA), and large language models (LLMs), empower forensic accountants to conduct more precise, efficient, and proactive fraud investigations (Dong et al., 2024; Street and Wilck, 2023; Mulyadi and Anwar, 2025; Paul and Celestin, 2025). As a result, forensic accounting is undergoing a technological transformation: tasks that once required teams of investigators poring over documents for weeks can now be accelerated and enhanced by AI-driven automation (Brunner, 2023; Paul & Celestin, 2025). Indeed, an estimated 60% of forensic accounting firms globally are already utilizing AI-powered tools for fraud detection and investigation (Valid8, 2025), thereby moving the field toward more proactive and data-driven fraud risk management.

This literature review provides a comprehensive examination of the application of AI in forensic accounting, with a focus on developments over the last five years, alongside a foundational background. Given the rapid advancement pf AI, an updated review is warranted. In addition, our approach is both narrative and analytical, encompassing qualitative insights and practical implications that a bibliometric analysis may not capture. We synthesize findings from academic research, industry reports, and case studies around the world to highlight how AI techniques have been integrated into fraud detection and forensic investigations. The review is organized as follows: Next, we provide a historical overview of AI in forensic accounting. We then discuss key research issues, challenges, and opportunities that emerge when applying AI to forensic accounting. We identify trends and opportunities for future research and practice and conclude with reflections on the trajectory of AI in forensic accounting. By compiling insights from a global perspective, this review aims to provide scholars and practitioners with a clear and up-to-date understanding of how AI is reshaping forensic accounting and what lies ahead in this rapidly evolving intersection of technology and financial fraud examination.

HISTORICAL OVERVIEW OF AI IN FORENSIC ACCOUNTING

Early Foundations (20th Century)

Forensic accounting in its modern form dates back to the mid-20th century, well before the era of advanced analytics. Although techniques were mostly manual at the time, foundational concepts were established. Through the mid-20th century, forensic accounting largely relied on labor-intensive scrutiny of books and records to detect irregularities. By the 1980s, textbooks and guides (e.g., Albrecht et al., 1984) began cataloging red flags and techniques for fraud detection, and simple computer programs were used for tasks such as searching for duplicate payments or validating sequences of invoices. Overall, this period established the scope of forensic accounting (investigating fraud, corruption, money laundering, etc.) but used traditional accounting audits and rudimentary data checks.

Emergence of Computer-Aided Analysis (1980s–1990s)

The advent of personal computers and database technology in the 1980s ushered in the first wave of computer-assisted auditing tools in forensic accounting. Firms began using Computer-Assisted Audit Techniques (CAATs) to extract and analyze large volumes of financial data – an early step toward automation. Forensic accountants could apply spreadsheet programs and specialized software (like ACL and IDEA) to sort transactions, filter out anomalies, and perform calculations much faster than manual methods. During the late 1980s, AI primarily referred to expert systems – rule-based programs that encoded human expertise. Auditing researchers have experimented with expert systems to evaluate internal controls or flag audit risks, effectively creating decision rules that mimic those of an experienced auditor. These were forerunners of AI in forensic work, albeit limited by the computing power and data limitations of the time. Nonetheless, the 1990s firmly established two important tools in the fraud examiner's toolkit: Benford's Law for anomaly detection in numerical data (Gorenc, 2024) and the Fraud Triangle Theory (Cressey, 1953) for understanding the conditions that lead to fraud.

Rise of Data Analytics and Early Machine Learning (2000s)

The early 2000s saw an eruption of major accounting scandals (Enron, WorldCom, Tyco, Parmalat, Satyam, etc.), which in turn spurred significant regulatory and technological responses. In the wake of the Sarbanes–Oxley Act (2002) and increased scrutiny on corporate financial reporting, there was a heightened demand for robust fraud detection mechanisms. More financial data was stored electronically; data mining techniques began to be applied to forensic datasets. Traditional statistical methods (regression, ratio analysis) were augmented by machine learning algorithms that could handle more variables and nonlinear patterns. By the late 2000s, research had demonstrated the use of decision trees, Bayesian classifiers, and neural networks to detect financial statement fraud with accuracy often exceeding that of classic models (see, for example, Kirkos et al. (2007). Similarly, support vector machines (SVMs) and clustering methods were explored for identifying anomalies in transaction datasets that might indicate embezzlement or

suspicious expenditures (Kotsiantis and Pintelas, 2007). In practice, Big Four accounting firms also started investing in proprietary analytics platforms during this era. For instance, PricewaterhouseCoopers (PwC) began incorporating anomaly detection routines in its fraud risk assessment services (Heye, 2021). By the end of the decade, forensic data analytics – referring to the use of quantitative analysis and AI to comb through transactional data, emails, and other evidence in investigations - had emerged. However, challenges such as limited computing power, relatively sparse data on known fraud cases, and skepticism from practitioners kept AI as a complement rather than a core in most forensic engagements at this time.

Advanced AI and Big Data Era (2010s–Present)

Over the last decade, the confluence of Big Data, cloud computing, and advanced AI algorithms has propelled forensic accounting into a new era. As digital transactions multiplied and storage became inexpensive, organizations accumulated massive datasets (e.g. detailed accounting records, communications, log files) ripe for analysis. Unsupervised learning gained prominence for fraud detection – algorithms that could sift through large pools of unlabeled data to spot outliers and suspicious patterns. Techniques such as clustering (to group similar transactions and flag unusual ones), anomaly detection models, and association rule mining (to identify unusual combinations of events) became feasible to run at large scale (Malladhi, 2023). Deep learning architectures emerged, capable of finding intricate patterns in complex data. Forensic accounting has begun to incorporate tools like neural networks, not only for numeric data but also for unstructured data sources. A notable advancement in the 2010s was applying natural language processing (NLP) and text mining to forensic investigations – for example, analyzing the linguistic tone of emails or the narratives in annual reports for signs of deception. Research demonstrated that certain keywords, writing styles, or emotional tones in communications could correlate with fraudulent behavior by management (Craja et al., 2020; Bhattacharya and Mickovic, 2024). AI models were trained to flag potentially incriminating documents among millions (a task impossible to do manually in a reasonable time) (Brunner, 2023). By the late 2010s, the industry's use of AI had accelerated, with many large accounting firms and investigative agencies deploying AI-driven forensic platforms. These systems could automatically ingest a client's entire general ledger and highlight irregular journal entries (e.g. weekends entries, round-dollar amounts, backdated entries, etc.), cross-correlate vendor data to detect conflicts of interest, or even use image recognition to verify the authenticity of invoices and receipts. By 2020, surveys indicated a clear shift: forensic accounting was transitioning from reactive investigation to proactive prevention through the use of AI and analytics (Valid8, 2025). The COVID-19 pandemic further accelerated digital audits and remote investigations, making AI tools even more indispensable in analyzing electronic evidence when face-to-face interviews or on-site inspections were curtailed.

In the last five years, AI in forensic accounting has truly gone global. There is robust research and implementation happening across continents. For example, emerging economies are leveraging AI to strengthen their fraud detection capabilities – a 2025 study in Rwanda showed that introducing AI/ML techniques improved fraud detection rates dramatically (from ~23% in 2020 to ~67% in 2024) and reduced detection time from months to mere weeks (Paul and Celestin, 2025). Such results underline the potency of AI when adopted, even in regions without a long history of forensic analytics. Meanwhile, advanced economies are experimenting with cutting-edge AI, with ensemble models that combine multiple algorithms proving particularly effective, outperforming single methods in accuracy (Malladhi, 2023). Large language models and AI assistants are also entering the scene – for instance, AI chatbots have been tested in fraud investigations to interactively query databases or assist investigators with summarizing case evidence (Paul and Celestin, 2025). These developments point to a trend of AI becoming deeply embedded in forensic accounting workflows. Table 1 summarizes key milestones in this historical evolution of AI in forensic accounting:

TABLE 1
KEY MILESTONES IN THE HISTORICAL EVOLUTION OF AI IN FORENSIC ACCOUNTING

Period	Key Developments in Forensic Accounting and AI
Mid-20th century	*Forensic accounting* emerges as a field. Largely manual methods; foundational concepts like Fraud Triangle Theory introduced.
1980s	First use of computers in fraud detection. CAATs and simple analytics (e.g. applying Benford's Law to datasets) assist auditors. Early expert systems developed for audit risk assessment.
1990s	Growth of digital records leads to data-driven audits. Academic experiments with AI (neural nets, decision trees) for detecting fraud begin. Notable fraud cases (ZZZZ Best, Enron preparation) highlight a need for better tools.
Early 2000s	Wave of corporate scandals (Enron, WorldCom, etc.) prompted Sarbanes–Oxley and major investments in fraud detection. Data mining and machine learning techniques (SVMs, clustering) applied in research and practice for forensic analytics. Big Four firms establish forensic data analysis teams.
2010s	Big Data era: Massive volumes of transactions and communications are analyzable. Unsupervised anomaly detection and deep learning gain traction. NLP is used for e-discovery and analyzing textual evidence. AI aids major investigations globally (Olympus, Petrobras, etc.).
2020s (last 5 years)	Widespread adoption of AI tools in forensic accounting (an estimated 60% of firms use them). Ensemble models and advanced AI significantly improve accuracy. Focus on real-time fraud prevention, blockchain analytics for cryptocurrency fraud, and Explainable AI due to regulatory/ethical concerns. Global usage expands to developing markets with notable success stories.

This historical trajectory shows a clear trend: as data and technology capabilities have grown, forensic accounting has progressively incorporated more sophisticated AI techniques. What began as manual detective work has evolved into a high-tech discipline where algorithms and accountants work hand-in-hand. In the next sections, we delve into the current research that addresses how to best leverage AI for forensic accounting, the challenges that remain, and the opportunities on the horizon.

RESEARCH ISSUES, CHALLENGES, AND OPPORTUNITIES

Applying AI to forensic accounting brings both significant challenges that must be addressed and exciting opportunities to enhance fraud detection and investigation. This section discusses the major issues identified in recent research as well as the potential benefits and improvements AI offers to forensic accounting practice. We organize the discussion into two key areas: challenges (the hurdles and risks associated with adopting AI) and opportunities (the positive impact and capabilities unlocked by AI).

Challenges in Implementing AI for Forensic Accounting

Integrating AI techniques into forensic accounting is not without difficulties. Researchers and professionals have highlighted several recurring challenges that need careful consideration:

- Data Quality and Availability: AI algorithms are only as good as the data they learn from, and in fraud detection, obtaining quality data is a perennial issue. Fraud cases (especially material ones) are relatively rare, which means labelled datasets of fraud vs. non-fraud cases are limited (Bao et al., 2020). This scarcity can hinder supervised learning models from generalizing well. Moreover, the data that does exist is often sensitive and siloed (e.g. confidential financial

records), making it hard to share for research or aggregate for better models. Companies may be reluctant to divulge fraud incidents, leading to a lack of public data. Additionally, real-world accounting data can be messy – with errors, missing entries, and noise – which can confuse AI models. Ensuring data integrity and preprocessing data (for example, merging data from different sources like bank records, invoices, and emails) is a major preparatory effort. If data is incomplete or biased (e.g. containing mostly certain types of fraud and not others), the AI will likewise be biased (Valid8, 2025). In short, feeding AI with high-quality, representative data remains a challenge, and poor data can lead to inaccurate or misleading results (Brunner, 2023).

- Model Transparency and Explainability: Many AI and machine learning models, particularly complex ones like neural networks or ensemble methods, operate as "black boxes," making decisions without providing easily interpretable reasons (Malladhi, 2023). In forensic accounting, this lack of transparency is problematic. Investigations often lead to legal proceedings, where an expert may need to explain how a fraud was detected. If an AI flags a transaction as fraudulent but cannot explain that it was because, say, the transaction deviated from expected patterns in multiple variables, a judge or jury may not lend it weight. Moreover, forensic accountants themselves need to trust and understand the AI's output to act on it. Interpretability is therefore another issue – how to design AI systems whose work can be audited and justified. Recent literature emphasizes the development of Explainable AI (XAI) for accounting, aiming to provide reasons or highlight the factors contributing to a risk score (ACFE, 2022; Malladhi, 2023). Without interpretability, there is risk that important fraud indicators are dismissed or, conversely, that false positives waste investigators' time. As of now, AI's limited contextual understanding, inability to articulate the "intent" behind a fraudulent transaction or a legitimate anomaly, and opaque decision-making process (ACFE, 2022; Mehta et al., 2021) remain critical issues.
- False Positives and Need for Context: Fraud detection inherently deals with imbalanced data – most transactions are legitimate, with only a tiny fraction being fraudulent. An aggressive AI detector may cast a wide net and flag many anomalies, but most could be false alarms. Sifting through these false positives can impose a burden on investigators, potentially eroding confidence in the tool. One reason AI may over-flag is the lack of business context. Contextual understanding is something humans excel at, and AI struggles with: an outlier transaction might be perfectly normal given seasonal business fluctuations or a one-time event, but an AI focusing only on historical patterns could mark it as suspicious (Valid8, 2025). Current AI systems often focus on individual data points and may miss the bigger picture relationships that clarify those transactions (Valid8, 2025). This challenge requires AI to be carefully tuned to strike a balance between sensitivity and specificity. It also reinforces that human judgment remains essential – investigators must review AI alerts and utilize domain knowledge to distinguish genuine issues from noise (Valid8, 2025).
- Ethical and Legal Considerations: The use of AI in any field raises ethical issues, and forensic accounting is no exception. Key concerns include bias, privacy, and accountability. Bias can enter AI models if the training data is skewed or if the algorithms inadvertently learn discriminatory patterns. For instance, if historically more fraud has been detected in certain industries or regions, a model might disproportionately scrutinize transactions associated with those areas, leading to bias against specific groups or companies. Ensuring fairness requires careful feature selection and possibly bias mitigation techniques (such as re-balancing training data (Valid8, 2025). Privacy is another critical issue: forensic AI often needs to process sensitive personal and financial information. Data protection laws, such as the General Data Protection Regulation (GDPR), impose strict requirements on how data can be used. Using AI might entail consolidating data from multiple sources (bank records, emails, HR files), potentially stepping over privacy boundaries if not controlled. There are also questions about employees' privacy – for example, if an AI monitors communications to detect collusion, how

to balance that with privacy rights. Legally, the introduction of AI analysis into investigations raises the issue of evidentiary acceptance (Metallo, 2020). Will courts accept insights generated by an algorithm? Traditionally, courts prefer established methodologies and expert testimonies; an AI's output might be challenged if it's seen as novel or not widely accepted. Furthermore, who is accountable if the AI makes an error? Suppose an innocent employee is falsely accused because of an algorithm's mistake. In that case, the legal liability for that error is a grey area – is it the organization's fault or the software vendor's fault? Due to these concerns, research emphasizes establishing ethical guidelines and AI governance in accounting. One study identifies key considerations, such as maintaining objectivity, ensuring data privacy, and upholding transparency, when deploying AI in forensic accounting (Pham and Vu, 2025). Professional bodies have also begun addressing this issue: for example, the International Federation of Accountants (IFAC) has discussed AI ethics and the need for accountants to understand the limitations of AI tools so that they can use them responsibly.

- Integration with Existing Systems and Skills Gap: Practical challenges arise in integrating AI tools into the traditional workflow of audits and investigations. Many organizations' accounting systems were not designed with AI in mind, so extracting data in real-time and feeding it to AI platforms can require significant IT overhauls. There is also the matter of cost – advanced AI solutions and the infrastructure to handle big data (servers, cloud services) can be expensive. Small firms or public sector agencies with limited budgets may struggle to invest in these technologies, potentially widening the gap between those who can afford cutting-edge tools and those who cannot. Alongside the issue of technology integration is the skills gap: forensic accountants historically come from accounting backgrounds, rather than computer science. Implementing AI means firms need professionals who understand data science and machine learning, or they must train their existing staff. Currently, there is a shortage of accounting professionals well-versed in AI techniques, which can slow adoption. Continuous training is necessary for practitioners to effectively utilize these tools and interpret their output (Akomolafe, 2024; Brunner, 2023). Change management is another aspect – some auditors and investigators may be resistant to relying on AI, either from fear of being replaced or skepticism about the technology (Mehta et al. 2021). Overcoming this requires demonstrating the reliability of AI and showing how it can make their jobs easier, not redundant. In essence, the challenge is socio-technical: merging advanced technology with human expertise in an organizational context that may not yet be fully prepared. Research in this area often calls for interdisciplinary education (blending accounting with data analytics curricula) and for management to champion a "human + AI" approach rather than seeing it as human vs. AI (Valid8, 2025).
- Regulatory and Compliance Hurdles: The regulatory environment surrounding the use of AI in audit and forensic services is still evolving. Audit standards and guidelines (from bodies such as the PCAOB and IAASB) are only beginning to incorporate guidance on the use of automated tools and AI. In fraud investigations, there are few formal standards for documenting or presenting AI findings as evidence. Without clear standards, firms may be hesitant to rely too heavily on AI in high-stakes investigations. Additionally, regulators themselves (like securities commissions, financial intelligence units, etc.) are experimenting with AI for detecting fraud and may impose certain requirements on data and model validation when firms use AI in regulatory compliance reporting. For example, if a bank uses an AI system for anti-money laundering detection, regulators might ask for proof that the system meets certain detection thresholds or doesn't discriminate. The lack of standardized evaluation frameworks for AI in forensic accounting is thus a challenge – each firm might be validating and using AI in its own way. The literature suggests a need for standardized testing datasets or benchmarks so that different fraud detection models can be objectively compared (Paul and Celestin, 2025). The absence of such standards currently means uncertainty about how effective a given AI tool truly is relative to another. Finally, compliance also intersects with data location – using AI often

means centralizing data (possibly in the cloud), which can conflict with data residency laws or client confidentiality agreements if not managed properly.

Despite these challenges, it is important to note that none are insurmountable. They represent active areas of research and development. For instance, significant work is ongoing to create more explainable AI models for accounting and to devise methods to reduce false positives by incorporating business context. Ethical frameworks and best practices are being proposed to tackle bias and privacy concerns (Valid8, 2025; Pham and Vu, 2025). The accounting profession is increasingly recognizing the need to upskill; many accounting programs and certifications now include data analytics components to bridge the skills gap. The challenges outlined above define the requirements for successfully leveraging AI in forensic accounting: high-quality data, explainable and fair algorithms, skilled human oversight, and supportive governance structures. Meeting these requirements is an ongoing process.

Opportunities and Benefits of AI in Forensic Accounting

Balanced against these challenges are the substantial opportunities that AI presents in the fight against financial fraud. When thoughtfully implemented, AI technologies can greatly enhance the effectiveness and efficiency of forensic accounting. Key opportunities identified in the literature and practice include:

- Enhanced Fraud Detection Accuracy: Perhaps the most celebrated benefit of AI is its ability to detect complex patterns and subtle anomalies that traditional methods might miss. Machine learning models can consider dozens or hundreds of variables simultaneously – far beyond the mental capacity of a human auditor – and identify non-obvious relationships indicative of fraud (Kirkos et al. 2024; Mulyadi and Anwar, 2025). For example, AI can correlate transactional data with employee data, market news, and communications to flag an unusual convergence of risk factors. Ensemble models, which combine multiple algorithms, have demonstrated particularly high accuracy in fraud detection by leveraging their collective strengths (Malladhi, 2023). The net effect is a reduction in false negatives (frauds that would have slipped through). Research consistently finds AI-based models outperform classic statistical techniques in identifying known fraud cases (Bao et al., 2020; Ikumapayi and Ayankoya 2025). In one comparative study, modern AI methods (neural networks and SVMs) correctly identified significantly more instances of fraudulent financial reporting than traditional ratio analysis (Islam and Rahman, 2025). Field evidence mirrors this. As noted earlier, a Rwandan bank implementing AI saw its detection accuracy increase from ~23% to ~66% over a four-year period (Paul and Celestin, 2025). In sum, AI offers the opportunity for more reliable fraud detection, catching a higher proportion of frauds (and catching them sooner) than was previously possible.
- Efficiency and Speed – "Faster Investigations": Time is critical in fraud investigations – the sooner an issue is identified and stopped, the lower the losses. AI can dramatically speed up forensic accounting processes by automating the ingestion and analysis of data. Tasks such as reviewing transactions, reconciling figures, or reading through emails that could take an audit team weeks or months to complete may be done in hours with machine assistance (Paul and Celestin, 2025). One white paper emphasizes that AI helps "compress the time to insight" in investigations (Valid8, 2025). For example, AI-powered e-discovery tools can quickly scan and categorize vast collections of documents, contracts, and communications, highlighting those with potential red flags (such as the presence of certain keywords or abnormal language patterns) (Brunner, 2023). This was previously a laborious task requiring many staff hours. The opportunity here is twofold: cost savings (since fewer hours are spent on manual work) and speed to action (fraud can be intervened upon earlier). Quicker investigations also mean less disruption to business operations and preservation of evidence before it is destroyed. Overall, AI allows forensic engagements to be conducted with unprecedented efficiency, which is especially helpful given the ever-growing volumes of digital data that must be examined in modern cases.

- Real-Time and Continuous Monitoring: By embedding AI algorithms into live financial systems, organizations can receive real-time alerts for suspicious activities (Brunner, 2023; Valid8, 2025). For instance, an AI system can monitor all journal entries being made in an ERP system and immediately flag any that violate certain rules. Banks already employ such techniques for credit card fraud: transactions are scored in milliseconds and potentially declined if deemed very high risk. The same concept is being expanded to general ledger and accounting data. This continuous auditing means issues are caught as they occur, potentially preventing fraudulent disbursements before the money actually leaves the company. It also serves as a deterrent – if employees know that intelligent systems are constantly watching for irregularities, the risk of attempting fraud increases. Predictive analytics enabled by AI can even anticipate fraud risks by analyzing trends. For example, AI might detect that an employee is exhibiting behaviors similar to those of past fraud perpetrators and alert management to conduct a closer review. As experts note, AI is transforming fraud investigation from "reactive research to proactive prevention", helping organizations stay a step ahead of fraudsters (Valid8, 2025).
- Ability to Analyze Unstructured Data: A major leap that AI provides is the ability to incorporate unstructured and semi-structured data into forensic analysis. Traditional accounting analytics focused almost exclusively on numerical data (e.g. journal entries, transaction amounts). However, vital evidence of fraud often lies in textual and other unstructured forms – emails discussing side deals, documents with altered figures, voice recordings, images (like receipts or invoices), etc. AI technologies such as NLP and computer vision allow these sources to be analyzed systematically. NLP can analyze communications to identify inconsistencies between what is stated in emails and what the accounting records indicate. It can also analyze the narrative portions of financial statements (MD&As, footnotes) for linguistic cues of deception. An illustrative example is using NLP to identify all instances where an email correspondence mentions words like "override," "backdate," or "delete records" – clear signals to flag for an investigator. Meanwhile, image recognition AI can verify the authenticity of documents – for example, identifying if a PDF invoice has been digitally altered or if a scanned signature is forged. These capabilities vastly extend the reach of forensic accounting beyond spreadsheets. One recent development is the introduction of AI assistants that can help summarize and search PDFs intelligently (Brunner, 2023). This means a forensic accountant can quickly summarize key themes in thousands of pages of contracts or identify all instances of a particular clause that may indicate fraudulent intent. The opportunity here is that no piece of data is off-limits to analysis now – AI can derive insights from the full spectrum of corporate data, structured or unstructured, giving a more holistic view of fraud schemes.
- Improved Consistency and Objectivity: Human investigators, no matter how experienced, can have off days or cognitive biases. AI systems, in contrast, apply the same criteria consistently across all data. This can improve the objectivity of fraud detection. For instance, an AI model will impartially flag anomalies based on learned patterns, whereas a human might subconsciously ignore red flags due to trust in a colleague or an expectation bias. Moreover, AI algorithms can be tuned to a desired false-positive/false-negative tradeoff and will adhere to that threshold consistently, ensuring the unwavering application of fraud detection rules. This consistency is valuable in large organizations or across global audits where you want the same level of scrutiny regardless of who the auditor is. It also helps in compliance – demonstrating that you have an AI systematically monitoring transactions can show regulators you have uniform controls in place. By reducing human error and oversight, AI can catch issues that a person might overlook when fatigued or rushed (Brunner, 2023). Consistency also plays a crucial role in document review during litigation support, as AI can ensure that every document is coded or logged using the same criteria, thereby reducing variability in how evidence is handled (Brunner, 2023). Overall, AI provides a more reliable and repeatable process, which strengthens the rigor of forensic investigations.

- Resource Optimization and Cost Savings: From a business perspective, one of the biggest opportunities of AI is doing more with less. Automated analysis means fewer staff hours are needed for routine tasks, allowing forensic accounting teams to cover more ground without proportional cost increases. This can make fraud risk management more affordable and scalable, even for smaller organizations. For forensic accounting firms offering services, these efficiency gains enable them to handle more cases simultaneously and provide faster turnarounds for clients (Brunner, 2023). Cost savings also accrue from preventing fraud losses in the first place and from reducing the length of investigations. Additionally, AI can help target investigative efforts where they matter most, thereby optimizing resource allocation. For example, rather than spending time randomly sampling transactions, an AI risk-scoring model can direct investigators to the top 1% highest-risk entries. This focused approach means less wasted effort on checking clean records and more on suspicious ones. One study highlighted that by automating data analysis, organizations free up auditors to focus on complex, value-added work rather than tedious tasks, which not only enhances efficiency but also improves job satisfaction and expert utilization (Brunner, 2023). In sum, AI can significantly lower the marginal cost of fraud detection – an important consideration as data volumes explode. Without AI, an ever-increasing volume of transactions would require ever-increasing audit manpower; AI breaks that linear relationship by handling large volumes cheaply.
- Augmenting Human Expertise (Hybrid Intelligence): Rather than replacing forensic accountants, AI in practice augments their expertise. The combination of human and machine can be more powerful than either alone. Humans bring domain knowledge, professional skepticism, and legal judgement; AI brings speed, pattern recognition, and breadth of analysis. This synergy presents a key opportunity: hybrid models, where AI handles data crunching and humans handle interpretation and decision-making, tend to yield the best outcomes. Moreover, AI can serve as a second pair of eyes, providing a form of quality assurance on human work. It might catch something an investigator missed, or vice versa, an investigator might catch something the AI missed. As technology improves, AI can elevate the forensic accounting profession by taking over the mundane tasks and enabling accountants to be strategic "fraud analysts" and advisors. In practical terms, we are already seeing this with large firms equipping their teams with AI platforms – the accountants who know how to utilize these tools can deliver deeper insights and demonstrate more value to clients.
- Detection of Complex and Emerging Fraud Schemes: Finally, AI offers the opportunity to detect types of fraud that were exceedingly difficult to uncover in the past. Complex schemes involving numerous transactions, off-book entities, or collusion across departments can generate subtle signals across disparate data sources – signals that a human might not piece together. AI is well-suited to integrating multi-source data and finding cross-correlations that indicate a sophisticated fraud. For example, AI can identify an unusual pattern of inventory write-offs in conjunction with concurrent spikes in certain expense accounts and external news of a supplier facing financial troubles – together, these might indicate a concealed related-party transaction or kickback scheme. Another area is network analysis: AI graph algorithms can map relationships between entities (employees, customers, vendors) to detect rings of collusion or repeated links common to fraudulent cases (like the same address or bank account used by multiple shell companies). These are fraud patterns that only become apparent when viewing the "big picture" – something AI excels at assembling from lots of micro-data. Additionally, AI can adapt to new fraud patterns faster. When fraudsters change tactics, AI models (especially those using online learning or regular retraining) can learn the new patterns from fresh data, whereas traditional rule-based controls might fail until manually updated. This adaptability is crucial, as fraud is not a static threat; for instance, the rise of cryptocurrency fraud and COVID-19 relief fund scams in recent years has required the quick development of new detection algorithms. AI-based systems, for example, caught suspicious disbursements in pandemic aid by recognizing patterns of applications that a human might not have had time to

manually identify. In summary, AI broadens the scope of frauds that can be caught – from simple ledger manipulations to sprawling conspiracies – and can evolve as fraudsters evolve.

The opportunities outlined above demonstrate why there is intense interest in applying AI to forensic accounting. Many of these above benefits have already been realized to various degrees by early adopters, and ongoing research continues to push the frontier (Paul and Celestin, 2025). Table 2 below summarizes some of the key challenges versus opportunities of AI in forensic accounting for clarity:

TABLE 2
CHALLENGES AND OPPORTUNITIES OF AI IN FORENSIC ACCOUNTING

Key Challenges (Issues to Overcome)	Key Opportunities (Benefits to Leverage)
Data limitations: Scarcity of labeled fraud data; data quality and silos can hinder model training (Bao et al. 2020).	*Greater accuracy:* AI detects subtle patterns and complex fraud schemes that humans might miss, improving fraud catch rates (Malladhi, 2023).
Black box models: Many AI models lack interpretability, making it hard to explain findings to stakeholders (Malladhi, 2023).	*Speed and efficiency:* Automated analysis of massive datasets dramatically reduces investigation time and costs (Paul and Celestin, 2025; Brunner, 2023).
False positives: AI can over-flag anomalies without context, requiring human review to filter noise (Valid8, 2025).	*Real-time monitoring:* AI enables continuous auditing and immediate alerts for suspicious transactions, catching fraud in real-time (Brunner, 2023; Valid8, 2025).
Ethical concerns: Risks of bias in algorithms; privacy and data protection challenges when analyzing sensitive information (Valid8, 2025).	*Unstructured data analysis:* AI (e.g. NLP) can analyze emails, documents, and images for fraud evidence, extending forensic capabilities beyond numbers (Brunner, 2023).
Skills gap: Need for forensic accountants to have data science knowledge; change management in adopting new technology (Brunner, 2023).	*Augmented expertise:* AI handles routine tasks, freeing human experts to focus on complex judgment areas – a productive human–AI collaboration (Valid8, 2025; Brunner, 2023).
Lack of standards: Few guidelines on validating AI tools or using AI outputs as evidence, creating uncertainty in adoption.	*Scalability:* AI allows coverage of entire datasets (100% testing) and the ability to investigate more cases simultaneously without proportional increases in staff (Brunner, 2023).

As this table suggests, the challenges and opportunities are two sides of the same coin – addressing the challenges will unlock even more of AI's potential benefits. The current state of research is primarily focused on finding ways to mitigate these challenges (through improved data practices, XAI techniques, ethical frameworks, and training programs, among others) in order to fully realize the opportunities for faster, smarter, and more effective fraud detection. We next turn to the literature's key findings so far: what do we know about AI's impact in forensic accounting? What has prior research discovered about its performance, best practices, and limitations?

KEY RESEARCH FINDINGS

The body of research on AI in forensic accounting has grown substantially in recent years, this section highlights several key findings that have emerged from the literature:

1. AI Outperforms Traditional Methods in Many Fraud Detection Tasks: A consistent finding across numerous studies is that AI-based models (machine learning and data mining techniques) tend to outperform traditional statistical or rule-based approaches in detecting fraud

(Bao et al. 2020; Bertomeu, 2020; Bertomeu et al., 2021; Islam and Rahman, 2025; Ikumapayi and Ayankoya 2025). Traditional methods, such as linear ratio analysis and heuristics (e.g., flagging all transactions over a certain amount), or manual sampling, have been the baseline in audits. Research by Ikumapayi and Ayankoya (2025) compared regression and other conventional models with AI models, such as neural networks and SVMs, for detecting accounting fraud. The AI models achieved higher detection rates and better predictive power. Similarly, Talukder et al. (2024) noted that ensemble and machine learning approaches could identify complex fraud patterns that simple outlier tests missed, thus reducing false negatives. The advantage of AI is most pronounced in situations involving large, high-dimensional data, where patterns are non-linear or involve interactions among multiple variables. For instance, decision trees and random forests can capture combinatorial red flags that a single-ratio threshold test would not. However, studies also caution that this outperformance is contingent on having sufficient quality data for training – when data is extremely limited, advanced models might overfit, in which case simpler models could rival them. Overall, the literature clearly indicates that when properly trained, AI models provide higher accuracy in identifying known instances of fraud than legacy methods, often by a substantial margin.

2. Significant Improvements in Efficiency and Scope Documented: Beyond accuracy, a few case studies and empirical assessments have documented how AI improves the efficiency of forensic work. A key finding is that AI tools can process full populations of data rather than samples. For example, Perols (2011) found that machine learning techniques could analyze entire sets of financial statements to detect fraudulent ones with higher precision than sample-based audit methods. In Rwanda, as cited earlier, organizational metrics showed fraud detection time dropped from ~6 months to ~2.5 months after adopting AI/ML systems, and detection rates nearly tripled (Paul and Celestin, 2025). These quantitative improvements align with anecdotal reports from industry: forensic accounting teams augmented with AI have been able to tackle far larger datasets and identify issues that were previously impractical to find. Such results are compelling evidence of the efficiency gains and have been a driving force for further AI adoption in practice.
3. Need for Human Expertise Remains a Prominent Conclusion: A nearly universal finding in the literature is that AI is most effective in forensic accounting when combined with human expertise, rather than as a standalone tool (Brunner, 2023; Farber, 2025). Studies often conclude with the caveat that human judgment is irreplaceable for certain aspects of fraud investigation. AI may flag anomalies, but human investigators must contextualize them, establish intent, and construct the narrative required in legal settings. Multiple sources highlight that AI cannot determine intent or the qualitative aspects of fraud (Valid8, 2025). For example, an AI might spot that an invoice was paid twice, but it takes a person to investigate whether that was a mistake, a control failure, or an employee diverting funds. Research also notes that AI can sometimes produce spurious correlations (finding patterns that are statistically unusual but not actually related to fraud) – human oversight is needed to vet these. As one practitioner insight put it, "AI can identify suspicious patterns for fraud, but often can't establish intent – that component is critical and still up to professionals to determine" (Valid8, 2025). This message is important, as it has guided the design of AI tools (with analyst-in-the-loop features) and the development of training programs (to enhance accountants' ability to work with AI).
4. Effectiveness of Specific AI Techniques – Ensemble Models and Hybrid Approaches: A notable finding is the high performance of ensemble models (combinations of classifiers) compared to individual algorithms for forensic purposes. As mentioned in Tageldin and Venter (2023), empirical tests show that ensembles (such as voting or stacked models blending a neural network, decision tree, and SVM) often yield better accuracy and robustness. This is likely because fraud signals can manifest in diverse ways; one algorithm might catch linear patterns while another catches nonlinear ones, and together they cover more ground. Studies have found, for example, that combining an outlier detection model with a supervised classifier can

both identify unknown frauds and accurately classify known ones, thereby balancing precision and recall. Unsupervised methods have been found useful for exploratory analysis – e.g., clustering to find groups of transactions that behave differently from others, which then become candidates for investigation. Kirkos et al. (2007) demonstrated that cluster analysis could effectively separate companies into distinct groups, one of which had a high concentration of fraud firms, thereby profiling a risk cluster. However, unsupervised techniques alone do not provide a definitive yes/no fraud indication, so research often suggests a hybrid approach: using unsupervised methods to generate features or narrow down candidates and then employing supervised methods to make the final classification. Another insight is related to NLP models: studies applying text mining (Throckmorton et al., 2015; Fissette, 2017; Li et al., 2023) suggest that textual cues can significantly enhance fraud prediction models when combined with numerical data. One practical example of the effectiveness of this technique is Benford's Law integrated with machine learning – researchers have embedded Benford's Law analysis as a feature in ML models to detect accounting fabrications. The finding is that this integration improves the detection of certain manipulations (such as faked invoices) better than either approach alone. In summary, the literature indicates that no single algorithm is perfect, but intelligent combinations (ensembles, hybrid human-AI systems) yield the best results in forensic detection.

5. Common Fraud Indicators Identified by AI Studies: Through the application of AI on numerous fraud datasets, research has surfaced some common indicators or red flags that AI models frequently rely on. For instance, decision tree models frequently identify features such as abnormal fluctuations in revenue relative to cash flows, a high frequency of round-dollar transactions, or an unusual ratio of certain expenses to sales as top splitters when distinguishing between fraud and non-fraud firms. These machine-derived indicators align with known red flags (e.g. the classic Beneish M-score components or ACFE red flag checklists) but also bring new ones to light. One study by Zhou and Kapoor (2011), which used neural networks on financial statement data, found that off-balance sheet items and complex related-party transactions were significant in fraud prediction – highlighting that AI can handle these complexity indicators better than naive checks. In forensic audits of disbursements, AI models have identified patterns such as repeated small invoices just under approval thresholds and high variance in unit prices among similar purchases as strong indicators of potential fraud. These findings are valuable because they inform practice: auditors refine their rule-based controls by incorporating these AI-generated indicators (e.g., adding a control to review all vendor payments just under authorization limits). In essence, AI research not only validates many traditional fraud risk factors but also helps quantify their importance and discover new combinations of signals. It has also been noted that AI can detect "benign anomalies" – irregularities that are not fraudulent but rather procedural issues (such as data entry errors or control deficiencies). Overall, a key takeaway is that AI-driven analysis has enriched the understanding of what fraud looks like in data, providing a more evidence-based set of red flags for the profession.
6. Adoption is Uneven – Organizational and Geographic Trends: Another finding, more from surveys and meta-analyses, is that the adoption and impact of AI in forensic accounting is not uniform across the board. Larger firms and financial institutions have been early adopters, showing strong results, whereas many smaller practices and organizations are lagging behind. A bibliometric analysis by Hossain (2023) noted a "notable dearth" of forensic accounting research in certain regions. This hints that in some countries, either awareness or resources for AI in forensic accounting are lacking. Conversely, regions with high financial activity and effective fraud enforcement (North America, Europe, parts of Asia) exhibit a greater uptake. For example, banks in developed countries are extensively using AI for anti-money laundering, whereas some developing countries are currently piloting these tools. Within organizations, research has found that support from top management and a culture that values innovation are

crucial for successful AI integration in audits (common findings in technology adoption literature applied to accounting).

TRENDS AND FUTURE DIRECTIONS FOR RESEARCH

The literature and industry commentary point to a range of developments that are likely to drive the next generation of tools and research projects. Here we outline key future directions and emerging trends:

- Emphasis on Explainable and Ethical AI: As highlighted, one of the foremost trends is developing explainable AI (XAI) specifically for forensic use. Future research is focused on creating models that can output human-readable explanations (for example, pinpointing which factors led to an anomaly score) so that auditors and courts can trust and understand the results. This aligns with an emphasis on ethical AI, ensuring that algorithms are transparent, fair, and accountable. In the next few years, we can expect to see frameworks and possibly regulations that require AI tools used in financial reporting or investigations to be auditable themselves. Scholars are already calling for standardized ethical guidelines and governance procedures for AI in accounting (Schweitzer, 2024). For instance, developing AI audit trails (records of how an AI model processed data) and bias testing protocols will be active areas. The trend is toward AI systems that not only detect fraud but do so in a manner aligned with legal and ethical norms, thereby increasing stakeholder confidence in these technologies.
- Integration with Blockchain and Cryptocurrency Forensics: The rise of cryptocurrencies and blockchain technology presents new challenges and opportunities for forensic accounting. A growing trend is the integration of AI with blockchain analytics to handle fraud and compliance in crypto assets. Blockchain's public, immutable ledger provides vast data but analyzing it for illicit activity is complex – a task suited to AI pattern recognition. Future forensic tools are likely to utilize AI to trace transactions through blockchain networks and link them to real-world entities, thereby augmenting traditional financial fraud investigations. Similarly, smart contract auditing may employ AI to flag suspicious or anomalous code that could be designed to defraud. As digital assets become more mainstream, forensic accountants will need AI to monitor and investigate blockchain-based transactions at a large scale. This reflects a trend in which AI will be used to analyze new data sources, including data from payment systems, cryptocurrency exchanges, social media (for sentiment analysis or clues), and beyond. Forensic accounting is expanding its scope, and AI is the tool enabling analysis of these unconventional data pools.
- Advanced Analytics and AI Techniques: On the technical frontier, future research is exploring ever more advanced AI techniques for fraud detection. Deep learning will continue to play a role, particularly as more labeled data becomes available to train complex models. Techniques like graph neural networks are an emerging trend, especially apt for modeling networks of transactions or relationships. These models can learn patterns on transaction graphs, potentially improving detection of collusion, money laundering rings, or procurement fraud networks. Another promising avenue is the use of anomaly explanation systems. Research is aiming to have AI suggest possible reasons for the anomaly, drawing on case libraries or expert knowledge. We also anticipate more use of transfer learning and federated learning: transfer learning could allow models trained on one company's fraud data to be adapted to another, and federated learning would enable multiple organizations to collaboratively train fraud detection models without sharing raw data (addressing privacy concerns). Additionally, there's interest in how Generative AI might assist forensic accounting – for example, using large language models (like GPT-style AI) to quickly summarize evidence or generate insights from case documents. While generative AI must be used cautiously, it could become a powerful aid for forensic accountants sifting through complex cases, essentially acting as an AI research assistant under human supervision.

- Proactive Fraud Prevention and Continuous Assurance: The future will likely see a stronger shift from reactive investigations to proactive fraud prevention using AI. This means embedding AI not just in forensic departments, but throughout business processes as a continuous assurance mechanism. Continuous auditing powered by AI is a trend already in motion, where transactions are checked in real-time and controls are continuously tested by AI agents. We foresee that internal control systems will increasingly incorporate AI that learns what normal operations look like and provides an "always-on" watch for deviations. In corporate finance, this may extend to predictive analytics that identify units or employees at a higher risk of fraud, allowing for preventative action to be taken. In essence, AI can help create a digital fraud immune system for organizations, constantly monitoring and adapting to new threats. Future research and practice will aim to optimize these systems and assess their effectiveness in reducing fraud incidence.
- Education and Skill Development: A crucial non-technical trend is the push for better education and training to bridge the gap between data science and accounting (Akomolafe, 2024; Paul and Celestin, 2025). Accounting programs around the world are updating curricula to include courses on data analytics, AI, and programming, recognizing that the forensic accountant of the future needs to be as comfortable with algorithms as with ledgers. Professional certifications (like the CFE – Certified Fraud Examiner, or new analytics certifications by accounting bodies) are evolving to test knowledge of data analysis and AI tools. The trend is towards a new breed of forensic accountants who are truly "hybrid" in skill set. Therefore, future research may also investigate pedagogical approaches for teaching AI to accountants, as well as the effectiveness of various training interventions in practice (e.g., whether a workshop on AI for internal auditors leads to measurable improvements in fraud risk detection).
- Regulatory and Standard-Setting Initiatives: As AI becomes integral to auditing and forensic functions, regulators and standard-setters are beginning to formulate responses. We expect future standards or guidelines will directly address the use of AI in audit and forensic engagements. For example, the Auditing Standards Board and PCAOB are examining how audit evidence obtained via automated means (including AI analyses) should be evaluated and documented. In forensic accounting, organizations such as the ACFE or ISACA may issue guidance on the ethical and effective use of AI-based tools in investigations. There is also discussion of having validation standards for AI models used in finance. Governments might impose requirements for explainability or bias testing for AI tools used in areas like credit scoring or insurance fraud detection, which could trickle into forensic accounting expectations. Another possible future development is the certification of specific AI tools to signal reliability. Essentially, the environment around AI is likely to become more regulated, and staying ahead of this by developing industry consensus and best practices is a focus. Researchers are increasingly calling for such standards to ensure consistency and trust in AI-assisted forensic work.
- Collaboration and Data Sharing: Combating fraud is a collective effort, and a forward-looking idea is the creation of shared fraud data exchanges or consortia where companies contribute anonymized data on fraud incidents to help train better AI models for everyone's benefit. We see early signs of this in credit card fraud (banks sharing data to detect cross-institution fraud patterns). In financial statement fraud or occupational fraud, this is trickier due to confidentiality, but future research may explore ways to share insights without sensitive details (again, possibly via federated learning or industry-wide "fraud libraries"). Such collaboration, potentially facilitated by professional associations or government agencies, could greatly enhance AI effectiveness by providing it with more examples of fraud to learn from.

In summary, the future of AI in forensic accounting will be characterized by more intelligent, transparent, and integrated systems. The technology will become more user-friendly and interpretable, enabling non-technical auditors to harness its power with confidence. AI will delve into new domains (like

blockchain) as fraud migrates there, and it will increasingly function in real-time, preventative modes. The role of the forensic accountant will evolve in tandem, becoming more of a strategist and interpreter of AI results as routine analysis becomes increasingly automated. Research will continue to drive these trends, focusing on unresolved challenges to ensure that the next generation of AI tools is robust and trustworthy. If the last five years are any indication, the pace of advancement will remain rapid. The vision for the future is one where AI is a standard part of the forensic accounting toolkit worldwide, improving the profession's ability to protect stakeholders from fraud and financial misconduct.

CONCLUSION

In summary, AI has rapidly evolved from a novel concept to a vital component in forensic accounting. This review highlighted that while AI greatly enhances fraud detection capabilities (with higher accuracy and efficiency), it also introduces new challenges that the profession must address (data quality, explainability, ethics). The overarching finding is that AI works best in tandem with human expertise—a theme consistently echoed across studies. Looking ahead, we anticipate that AI tools will become more standardized, transparent, and integrated into routine forensic practice. By staying attuned to new developments and maintaining a balance between technological prowess and professional skepticism, forensic accountants around the world can harness AI to uphold financial integrity and justice in the years to come.

REFERENCES

Akomolafe, O.C. (2024). *The impact of artificial intelligence on forensic accounting practices in Canada: Examining the adoption and utilization of artificial intelligence technologies in forensic accounting practices and their implications for efficiency and effectiveness* [Research report]. University of Toronto Mississauga. Retrieved from https://mfacc.utoronto.ca/media/1332/download?inline

Albrecht, W.S., Albrecht, C.C., Albrecht, C.O., & Zimbelman, M.F. (2012). *Fraud examination* (4th ed.). Cengage Learning.

Association of Certified Fraud Examiners (ACFE). (2022). *Report to the nations: 2022 global study on occupational fraud and abuse*. Retrieved from https://legacy.acfe.com/report-to-th-nations/2022/

Bao, Y., Ke, B., Li, B., Yu, Y.J., & Zhang, J. (2020). Detecting accounting fraud in publicly traded US firms using a machine learning approach. *Journal of Accounting Research*, *58*(1), 199–235. https://doi.org/10.1111/1475-679X.12292

Bertomeu, J. (2020). Machine learning improves accounting: Discussion, implementation and research opportunities. *Review of Accounting Studies*, *25*(3), 1135–1155. http://dx.doi.org/10.2139/ssrn.3694811

Bertomeu, J., Cheynel, E., Floyd, E., & Pan, W. (2021). Using machine learning to detect misstatements. *Review of Accounting Studies*, *26*(2), 468–519.

Bhattacharya, I., & Mickovic, A. (2024). Accounting fraud detection using contextual language learning. *International Journal of Accounting Information Systems*, *53*, 100682. https://doi.org/10.1016/j.accinf.2024.100682

Brunner, P. (2023). *Advancing Forensic Accounting: AI as the New Frontier.* The Brunner Sierra Group. Retrieved from https://brunnersierragroup.com/advancing-forensic-accounting-ai-as-the-new frontier/brunnersierragroup.com+1brunnersierragroup.com+1

Craja, P., Kim, A., & Lessmann, L. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems*, *139*, 113421. https://doi.org/10.1016/j.dss.2020.113421

Cressey, D. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Dong, M.M., Stratopoulos, T.C., & Wang, V.X. (2024). A scoping review of ChatGPT research in accounting and finance. *SSRN*. Retrieved from https://ssrn.com/abstract=4680203

Hossain, M.Z. (2023). *Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention.* ResearchGate. Retrieved from https://www.researchgate.net/publication/370954322_Emerging_Trends_in_Forensic_Accounting_Data_Analytics_Cyber_Forensic_Accounting_Cryptocurrencies_and_Blockchain_Technology_for_Fraud_Investigation_and_Prevention

Farber, S. (2025). AI as a decision support tool in forensic image analysis: A pilot study on integrating large language models into crime scene investigation workflows. *Journal of Forensic Sciences*, *00*, 1–12. https://doi.org/10.1111/1556-4029.70035

Feroz, E.H., Kim, S., & Raab, R.L. (2003). Financial statement analysis: A data envelopment analysis approach. *Journal of the Operational Research Society*, *54*(1), 48–58. https://doi.org/10.1057/palgrave.jors.2601475

Fissette, M.V.M. (2017). *Text mining to detect indications of fraud in annual reports worldwide* [Doctoral dissertation, University of Twente]. https://doi.org/10.3990/1.9789036544207

Gorenc, M. (2024). *Artificial intelligence and Benford's Law as useful tools for detecting accounting fraud.* Working paper, International School for Social and Business Studies, Slovenia.

Heye, B. (2021). *The future of auditing: An analysis of AI implementation in the Big Four accounting firms* [Undergraduate honors thesis, University of New Hampshire].

Holley, B., & Flesher, D. (2020, October/November). Maurice E. Peloubet: A life of impact on accountancy and society. *The CPA Journal*. Retrieved from https://www.cpajournal.com/2020/11/23/maurice-e-peloubet/

Ikumapayi, O., & Ayankoya, B. (2025). AI powered forensic accounting: Leveraging machine learning for real time fraud detection and prevention. *International Journal of Research Publication and Reviews*, *6*(2), 236–250. https://doi.org/10.55248/gengpi.6.0225.0712

Islam, M., & Rahman, G. (2025). AI-driven fraud detection in financial institutions. *Journal of Computer Science and Technology Studies*, *7*(1), 100–112. https://doi.org/10.32996/jcsts.2025.7.1.8

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. https://doi.org/10.1016/j.eswa.2006.02.016

Kirkos, E., Boskou, G., Chatzipetrou, E., Tiakas, E., & Spathis, C. (2024). Exploring the boundaries of financial statement fraud detection with large language models. *SSRN*. Retrieved from https://ssrn.com/abstract=4842962

Knapp, M.C. (1992). *Auditing cases: An interactive learning approach* (3rd ed.). Kansas: South-Western College Publishing.

Knapp, M.C. (1992). ZZZZ Best Company, Inc. *Issues in Accounting Education*, *7*(2), 245–257.

Kotsiantis, S., & Pintelas, P. (2007*). Machine learning applications in accounting*. New York: Springer.

Lee, A., & Ahmed, R. (2023). Ethical and practical challenges in AI implementation for forensic accounting. *Journal of Business Ethics and Technology*, *27*(2), 88–105.

Lee, J., & Ahmed, K. (2023). Fraud risk monitoring using AI-based continuous auditing systems. *Auditing: A Journal of Practice & Theory*, *42*(1), 81–102.

Li, J., Li, N., Xia, T., & Guo, J. (2023). Textual analysis and detection of financial fraud: Evidence from Chinese manufacturing firms. *Economic Modelling*, *126*, 106428. https://doi.org/10.1016/j.econmod.2023.106428

Malladhi, A. (2023). Artificial intelligence and machine learning in forensic accounting. *International Journal of Computer Science and Engineering*, *10*(7), 6–20.

Metallo, V.N.A. (2020). The impact of artificial intelligence on forensic accounting and testimony. *Emory Law Journal Online*, *69*, 2039–2062. Retrieved from https://scholarlycommons.law.emory.edu/eljonline/3

Mehta, K., Mittal, P., Gupta, P.K., & Tandon, J.K. (2021). Analyzing the Impact of Forensic Accounting in the Detection of Financial Fraud: The Mediating Role of Artificial Intelligence. *Advances in Intelligent Systems and Computing*, *1388*, 585–592. https://doi.org/10.1007/978-981-16-25978_50ResearchGate

Mulyadi, M., & Anwar, Y. (2025). Business school teaching case study: taking accountancy from spreadsheets to AI. *Financial Times*. Retrieved from https://www.ft.com/content/bd9c415f-cab5-4ae1-8bf2a17c57f9b5db

Munandar, M., & Honggowati, S. (2025). Bibliometric analysis of forensic accounting research in emerging markets. *Economics and Business Quarterly Reviews*, *8*(1), 47–61. https://doi.org/10.31014/aior.1992.08.01.650

Paul, B.J., & Celestin, M. (2025). The impact of artificial intelligence and machine learning in forensic accounting for fraud detection in Rwanda. *International Journal of Scientific Research and Modern Education*, *10*(1), 39–48.

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory*, *30*(2), 19–50. https://doi.org/10.2308/ajpt-50009

Pham, H., & Vu, P. (2025). Insight into how legal and ethical considerations of artificial intelligence enhance the effectiveness of cyber forensic accounting. *Journal of Global Information Technology Management*. https://doi.org/10.1080/1097198X.2025.2480972

Romero-Carazas, R., et al. (2024). Forensic auditing and the use of artificial intelligence: A bibliometric and systematic review (2000–2024). Working paper.

Schweitzer, M. (2024). Artificial Intelligence (AI) Ethics in Accounting. *Journal of Accounting, Ethics & Public Policy*, *25*(1), 67–85. https://doi.org/10.2139/ssrn.4374567

Street, D., & Wilck, J. (2023). Let's have a chat: Principles for the effective application of ChatGPT and large language models in the practice of forensic accounting. *Journal of Forensic and Investigative Accounting*, *15*(2), 1.

Tageldin, L., & Venter, H. (2023). Machine-Learning Forensics. *Applied Sciences*, *13*(18), 10169. https://doi.org/10.3390/app131810169

Talukder, M.A., Khalid, M., & Uddin, M.A. (2024). An integrated multistage ensemble machine learning model for fraudulent transaction detection. *Journal of Big Data*, *11*, 168. https://doi.org/10.1186/s40537-024-00996-5

Throckmorton, C., Mayew, W., Venkatachalam, M., & Collins, L. (2015). Financial fraud detection using vocal, linguistic and financial cues. *Decision Support Systems*, *74*, 78–87. https://doi.org/10.1016/j.dss.2015.04.006

Valid8s, Inc. (2025). *The impact of AI on fraud investigations. What Forensic Accountants Need to Know.* Retrieved from https://www.valid8financial.com/white-paper/ai-impact-on-fraud-investigations

Vishwakarma, L.A. (2025). Application of artificial intelligence in forensic accounting. *International Research Journal of Modernization in Engineering Technology and Science*, *7*(3).

Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. *Decision Support Systems*, *50*(3), 570–575. https://doi.org/10.1016/j.dss.2010.08.007