Proceeding of the 3rd International Conference of International Conference on Business and Economics
Faculty of Economy and Business, Universitas Pattimura,
December 11, 2025
PATTIMURA PROCEEDING: Conference of Science and Technology
e-ISSN: 2829-3770 | February 2026 | pp.267-280

Digital Forensic Accounting in the Era of Cybercrime : A Global Bibliometric Review

Nurul Maghfirah Surianto[1*], Ricky Setiawan[2]

[1]*Universitas Negeri Makassar, nurul.maghfirah@unm.ac.id, Makassar, South Sulawesi, Indonesia*
[2]*Universitas Negeri Makassar, rickysetiawan@unm.ac.id, Makassar, South Sulawesi, Indonesia*

[*]Corresponding author's email: nurul.maghfirah@unm.ac.id

ABSTRACT

This study uses bibliometric analysis to examine developments and research trends in the field of forensic accounting from 2005 to 2025. Publication data extracted from the Scopus database is analyzed using VOSviewer software to map statistical patterns, visualize academic networks, and identify key research topics in this field. The results reveal dynamic shifts in publication volume caused by factors such as the increasing complexity of financial crime, advances in the integration of digital technologies, heightened expectations for transparency, evolving regulatory frameworks, increased interdisciplinary collaboration, and improved internal control mechanisms. The high volume of journal articles indicates strong global academic interest. In addition, the analysis highlighted significant contributions from both developed and emerging economies, including the United States, India, United Kingdom, Indonesia, South Korea and Australia. Key research topics include risk management, fraud detection, digital forensics, fraud analysis, digital compliance, and financial governance. This study underscores the ongoing need for research to improve fraud detection and prevention strategies, promote global academic collaboration, and strengthen efforts to maintain financial integrity and transparency.

Keywords: *Digital Forensic Accounting, Cyber Crime, Bibliometric Analys, Vosviewer*

Introduction

Digital forensic accounting has grown rapidly in response to the increasing complexity of cybercrime, requiring the integration of advanced technology, proactive investigation strategies, and a robust legal framework to ensure effective examination of digital evidence. Recent studies emphasize that technological innovations including artificial intelligence

DOI: https://doi.org/10.30598/pcst.2026.iconbe.p267-280

(AI), machine learning (ML), blockchain, and Internet of Things (IoT) systems play a central role in automating evidence collection and analysis, enabling faster and more accurate detection of anomalies and fraud patterns (Tyagi et al., 2024); (Balusamy et al., 2025); (Shamoo, 2024); (Zangana et al., 2025). Modern forensic processes increasingly rely on disk, memory, and network forensics to address the rapid expansion and complexity of digital artifacts generated in cyber environments. However, these advances also pose significant legal and ethical challenges, particularly regarding the admissibility, integrity, and proper handling of digital evidence, which requires investigators to adhere to strict procedural standards to ensure acceptance in the judicial process ((Sharma, 2024); (Aleke & Trigui, 2024); (Allah Rakha, 2024). Consequently, contemporary research highlights the need for stronger interdisciplinary collaboration between forensic accountants, cybersecurity specialists, and law enforcement agencies to improve the quality of investigations, support threat intelligence sharing, and adopt dynamic forensic investigation models such as DFIFM that strengthen institutional capacity in responding to evolving digital threats (Nelufule et al., 2025); (Trivedi & Kumar, 2024). Overall, these developments highlight that the effectiveness of digital forensic accounting in the era of cybercrime is highly dependent on the integration of advanced technology, compliance with legal standards, and adaptive multidisciplinary practices. Digital forensic accounting has emerged as a critical discipline in response to the increasing complexity of cybercrime, financial fraud, and technology-enabled illegal activities.

Although existing studies have extensively discussed digital forensic accounting (DFA) in relation to technological advancements, cybercrime investigation, and legal–ethical considerations, much of the literature remains fragmented and primarily focused on technical or case-based perspectives. There is limited research that systematically maps the intellectual structure, thematic evolution, and global research patterns of DFA over time, particularly across diverse regional contexts, including developing and archipelagic countries with varying levels of digital readiness. This gap highlights the need for a comprehensive, longitudinal, and data-driven overview of the field. Accordingly, this study offers novelty by conducting a global bibliometric analysis of DFA research published between 2005 and 2025 using Scopus data and VOSviewer, identifying publication trends, influential contributors, collaborative networks, and emerging themes such as big data analytics, public sector governance, and fraud disclosure. By integrating technological, governance, and regional perspectives, this study advances the literature by positioning DFA not only as an investigative tool, but also as a strategic mechanism for strengthening financial transparency, institutional resilience, and sustainable digital governance in the era of cybercrime.(Aleke & Trigui, 2024).

Literature Review and Conceptual Background

Digital Forensic Accounting

Digital forensic accounting (DFA) has evolved as an interdisciplinary field that integrates forensic accounting, digital forensics, and cybersecurity to address the growing complexity of cyber-enabled financial crimes. Prior studies have emphasized the role of advanced technologies such as artificial intelligence, big data analytics, and blockchain in enhancing fraud detection, evidence collection, and investigative efficiency. In parallel, the literature also highlights legal, ethical, and governance challenges related to the admissibility, integrity, and privacy of digital evidence, underscoring the need for robust regulatory frameworks and professional standards in digital investigations.

Digital forensic accounting is an emerging field that combines traditional forensic accounting with digital forensics to investigate financial crimes in the digital age. It involves the identification, collection, analysis, and presentation of digital evidence to support legal proceedings and uncover fraudulent activities. Here's a breakdown of its key components, methodologies, and the impact of technology on the field, along with legal and ethical considerations, current trends, and challenges. Digital forensic accounting marks a significant advancement over conventional forensic accounting, largely influenced by rapid technological advances and the unique complexities introduced by cybercrime. The following sections outline the key differences, technological impact, required competencies, legal considerations, and challenges that distinguish digital forensic accounting from traditional approaches (Dkhar et al., 2025).

The Era of Cyber Crime

Research on cybercrime increasingly shows that the rapid digitisation of financial systems and organisations has expanded the scope and sophistication of fraudulent activities, requiring adaptive investigation models and cross-sector collaboration. Although many studies analyse DFA from a technical, legal, or organisational perspective, most of them use qualitative, conceptual, or case-based approaches. Only a few studies have attempted to systematically synthesise the overall development, intellectual structure, and thematic evolution of DFA research at the global level.

The era of cybercrime is marked by rapid evolution, driven by advancements in technology and societal changes. Here's a comprehensive overview of emerging trends, legal frameworks, psychological factors, and organizational responses to cybercrime. The landscape of cybercrime continues to evolve, influenced by technological advances and social changes. Addressing this complex issue requires a multifaceted approach that includes a robust legal framework, international cooperation, an understanding of psychological motivations, and proactive organizational strategies. Ongoing research and collaboration are essential to keep pace with the dynamic nature of cyber threats and develop effective preventive measures (Cotrina et al., 2024). Different countries have developed distinct legal frameworks to combat cybercrime. For instance, the Saudi Anti-Cybercrime Law outlines

specific penalties for cyber fraud, while the Budapest Convention serves as a pivotal international agreement aimed at harmonizing laws across nations (Buçaj & Idrizaj, 2024).

Bibliometric Analysis

Bibliometrix is a comprehensive tool that utilizes the R programming language to perform bibliometric analyses. It integrates a web-based interface called Biblioshiny, allowing researchers to conduct detailed analyses of literature, including science mapping and performance analysis (Aria & Cuccurullo, 2017). Bibliometrix stands out as a powerful tool for bibliometric analysis, offering a range of features that enhance its functionality and accessibility for researchers. Its evolution reflects the growing need for effective tools to navigate the expanding body of academic literature, making it an invaluable resource for understanding research trends and patterns across disciplines.

In this context, bibliometric analysis provides an appropriate methodological framework to address these limitations by mapping publication trends, research networks, and dominant themes within the literature. Rather than testing hypotheses, bibliometric research aims to identify patterns, research gaps, and emerging directions in a field. Accordingly, this study adopts a bibliometric approach to integrate fragmented research streams in digital forensic accounting, clarify its conceptual development, and highlight underexplored areas particularly those related to governance, public sector applications, and developing or archipelagic contexts thereby establishing a structured foundation for future empirical and theoretical research.

Method

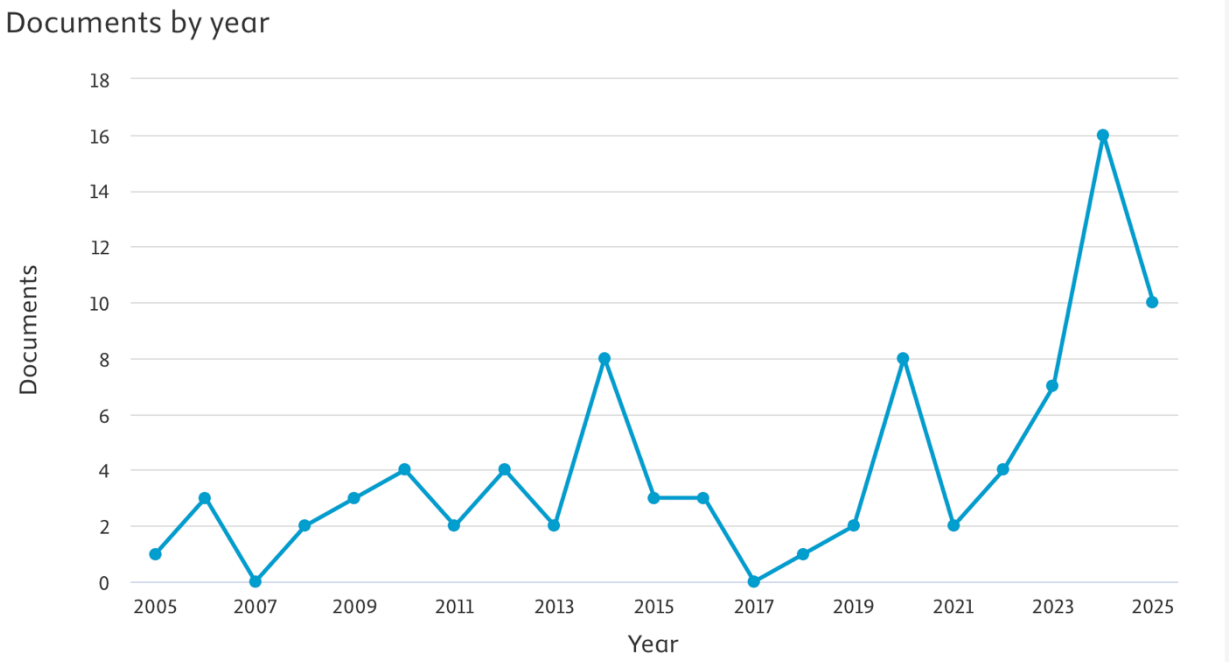
This study applies the bibliometric analysis method, which is an approach that aims to assess and map scientific literature in a particular field. Through this analysis, researchers can identify research development patterns, collaborative relationships, and the level of influence of authors and related publications. The document search was conducted using Publish or Perish software connected to the Scopus database. The search query was formulated using the keywords ‘digital forensic accounting’, which were applied to article titles, abstracts, and keywords to ensure relevance. The publication time frame was set from 2005 to 2025, reflecting the period in which digital forensic accounting emerged and developed in line with the growth of cybercrime and digital technology. Only journal articles and conference proceedings written in English were included to maintain academic consistency and comparability. The initial search yielded 86 documents. A relevance screening process was then conducted by reviewing the titles, abstracts, and keywords to ensure that each document explicitly discussed digital forensic accounting in the context of fraud detection, cybercrime investigation, governance, or digital evidence analysis. Publications focusing on general accounting, conventional forensic accounting without digital components, or unrelated cybersecurity topics were excluded. This screening process ensured that the final dataset accurately represented the core of the DFA research.

Bibliometric analysis was conducted in two main stages. First, descriptive performance analysis was carried out to examine publication growth, document types, country contributions, and citation patterns. Second, knowledge mapping analysis was conducted using VOSviewer software to visualise the relationships between keywords, authors, and countries. Keyword co-occurrence analysis was applied to identify dominant research themes and emerging topics, while network visualisation, overlay, and density were used to analyse thematic evolution over time and the intensity of research focus in the field. VOSviewer was chosen for its ability to effectively map large bibliographic datasets and produce interpretable visual representations of research structures. This bibliometric analysis not only presents a comprehensive mapping of the direction of research development, but also reveals the specific contributions of various stakeholders, including the government, the business sector, and civil society in the context of sustainability.

Result And Discussion

In this study, the keyword used in Scopus was “digital forensic accounting” with a research period from 2005 to 2025, with a total of 86 articles and the following details on the number of articles published per year

Figure 1

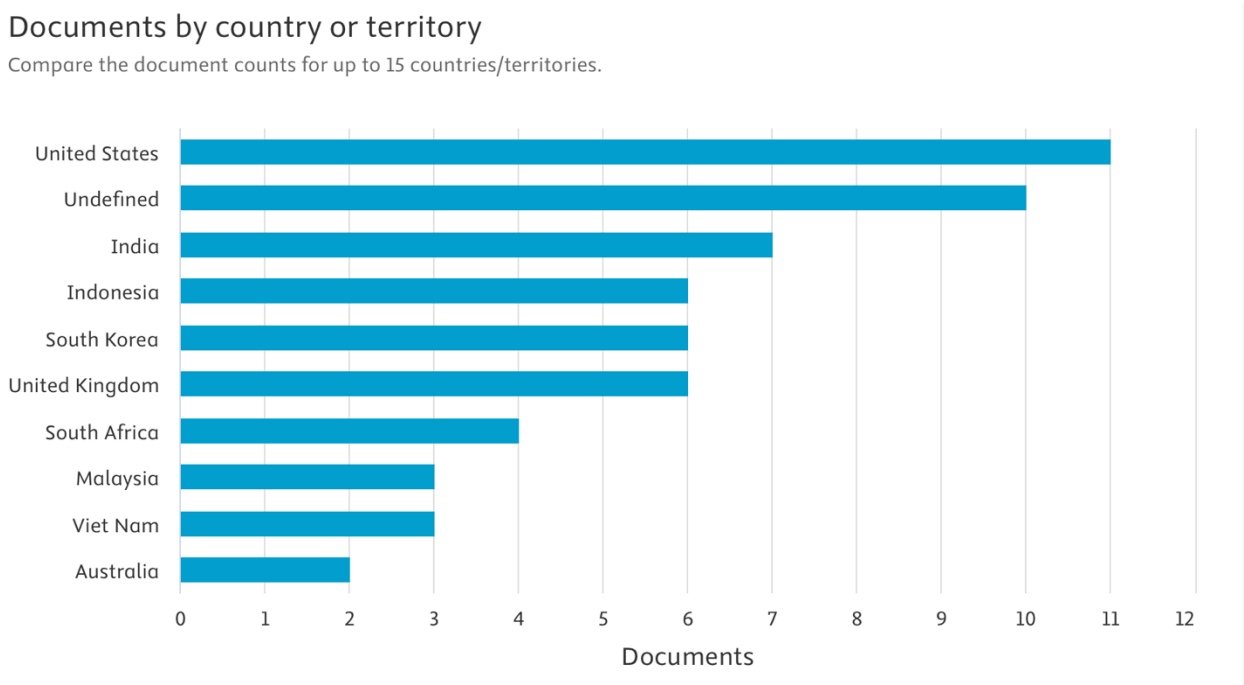


Source : Vosviewer, 2025

Based on Figure 1, it can be seen that the number of articles published on digital forensic accounting in the Scopus database has increased rapidly from 2020 to 2024. At the beginning of the period, the number of publications was still relatively low. In fact, in 2005,

only one article was published. This shows that this topic was still new and had not attracted much attention from researchers at that time. In 2019, an increase began to be seen, although the number was still relatively small. A bigger jump occurred in 2020, when the number of articles published reached 8 articles. This increase was driven by growing global awareness of cybercrime threats and the need for stronger digital detection and investigation mechanisms to support the integrity of financial systems. This upward trend continued, with the number of publications rising steadily until it peaked in 2024 with 16 articles published. The increase in the number of publications shows that the issue of digital forensic accounting is gaining attention from researchers and professionals, especially in efforts to strengthen oversight, detect fraud, and combat cybercrime in accounting and financial systems. This year, more and more people are realizing that digital forensic accounting does not only focus on the analysis of electronic evidence, but is also related to improving the long-term resilience of financial systems by integrating investigative technology into control practices and risk management strategies. Although in 2021 the number of publications decreased slightly to 2 articles. This decline is most likely due to incomplete data, considering that publications usually take time to be published. This decline does not indicate a decrease in interest in the topic but rather a delay in the journal publication process. Additionally, the graph illustrating the active involvement of countries in digital forensic accounting research is visualized in the following image:

Figure 2



Source : Vosviewer, 2025

The results of mapping based on country of origin show that publications related to digital forensic accounting are dominated by the United States with the highest number of documents. This finding indicates that the country plays a major role in the development of research in this field, mainly due to its strong technological infrastructure, research capacity, and the urgency of handling increasingly complex cybercrimes. In addition, a number of publications categorized as "undefined" indicate limitations in metadata recording in some databases, which may affect the accuracy of geographical distribution analysis. India, Indonesia, South Korea, and the United Kingdom also made significant contributions, indicating these countries' growing interest in digital security and forensic investigation. Meanwhile, countries such as South Africa, Malaysia, Vietnam, and Australia have a lower number of publications, but still reflect a growing interest in strengthening digital-based forensic approaches. Overall, this distribution pattern shows that digital forensic accounting research has become a global focus, with the involvement of various countries at varying levels of readiness and need in facing cybercrime threats.

Figure 3
VOSViewer Network Visualization Results

Source : Vosviewer, 2025

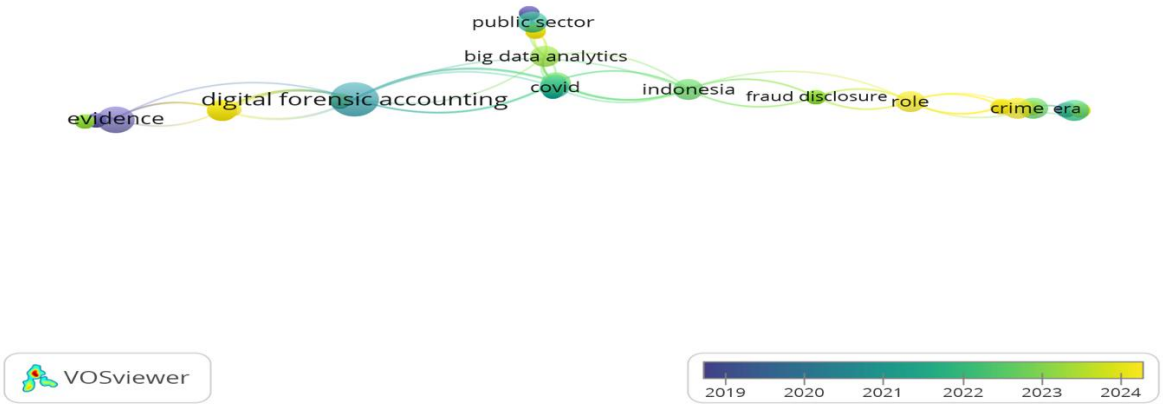
Visualization of keyword networks with different color clusters shows a maturing thematic structure in digital forensic accounting research. The diverse color distribution reflects the differences in research focus that are developing in parallel, each representing complementary scientific domains. The blue cluster, centered on the keyword evidence, describes the epistemological basis that emphasizes the importance of the validity, integrity, and reliability of digital evidence as the foundation of forensic investigation. This confirms that early studies in this field were still very oriented towards procedural and methodological aspects related to the collection and analysis of electronic evidence. The shift to the orange and brown clusters, dominated by the keyword "digital forensic accounting," indicates a shift

in focus from evidence to strengthening the concepts, roles, and functions of digital forensic accounting. This cluster illustrates the theoretical consolidation that forms the basis for the development of technology-based investigation frameworks. The strong interconnection between nodes in this cluster reflects the synergy between accounting, investigation, and information technology perspectives. Meanwhile, the red cluster, which contains keywords such as public sector, big data analysis, and COVID, shows that current research is moving towards multidisciplinary integration. The presence of big data analysis as an important node indicates the use of advanced analytical techniques to detect anomaly patterns, identify digital traces, and process data on a large scale. The red domain illustrates a strong thematic urgency, particularly in the context of the COVID-19 pandemic, which has accelerated the digitization of public services. As a result, the public sector has become a strategic research domain due to increased exposure to fraud and cybercrime risks.

In addition, the purple cluster, which includes keywords such as Indonesia, fraud disclosure, and function, indicates a more contextual and applied research orientation. The focus on fraud disclosure indicates concern about the effectiveness of fraud reporting supported by digital forensics technology. The presence of the word “Indonesia” indicates the contribution of research from developing countries, which offers an important perspective on the challenges of implementing digital forensics policies in environments with varying levels of technological readiness.On the right side of the network, the green and light blue clusters, which contain keywords such as crime and era, indicate the emergence of a new discourse related to the characteristics of modern digital crime and the demands for forensic expertise that must adapt to the ever-evolving conditions of the digital era. The position of these clusters indicates the direction of research evolution towards the discussion of more complex and multi-platform crime phenomena involving the global digital ecosystem. Overall, the cluster structure seen in this visualization shows that digital forensic accounting research is shifting from an evidence-based approach to a broader and more comprehensive approach, which includes big data analysis, public sector governance, fraud dynamics, and socio-technological developments. The pattern reflects the maturity of the research agenda, in which this field is increasingly positioned as an interdisciplinary discipline that plays a strategic role in risk mitigation, strengthening transparency, and developing digital security policies.

VOSViewer Overlay Visualization Results

Figure 4



Source : Vosviewer, 2025

Figure 4 shows the thematic dynamics between periods. This overlay visualization also highlights the occurrence of shifting epistemic focus in digital forensic accounting research. The shift in color from purple (2019) to green and yellow (2022–2024) indicates that this field is transitioning from concept-based studies to a more applied, contextual approach oriented toward solving real problems that arise in the digital ecosystem. In this context, digital forensic accounting is no longer positioned solely as an investigative activity, but has evolved into a strategic analytical tool that supports decision-making and risk mitigation at the institutional level. The strong thematic relationship between big data analytics and the public sector shows that the ability to process, assess, and interpret large-scale data is a key factor that increases the significance of digital forensic accounting. This integration reflects the global trend toward data-driven governance, where digital evidence serves not only as a means of proof but also as a source of strategic insights in public policy and strengthening state financial governance.

The keyword *covid* that appears as a connecting node in the middle of the network confirms the role of the pandemic as an *accelerator of digital vulnerabilities***.** Increased economic and administrative activity through digital platforms during the pandemic has expanded the opportunities for cyber fraud, triggering an urgent need for more comprehensive digital investigation capabilities. Thus, the pandemic is not merely the context of events, but a variable that shapes the direction and urgency of research in this field. Furthermore, the emergence of the terms “fraud disclosure” and “role” in recent years illustrates that research has moved toward evaluating the effectiveness of digital forensic

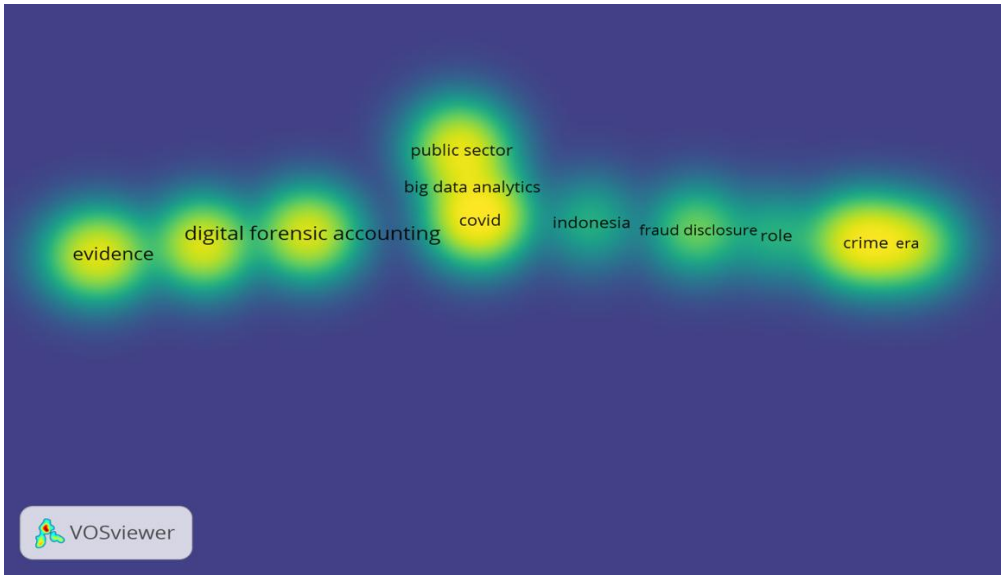
accounting in real-world practice, including its role in improving transparency, strengthening reporting systems, and supporting organizational compliance with accountability standards.

This reflects a shift in focus from merely technical investigations to *institutionalized forensic practices* that are integrated with regulatory frameworks and oversight mechanisms. In addition, the position of the word *Indonesia* in the latest development path indicates an increase in research contributions from developing countries, which generally face unique challenges related to digital literacy, technological readiness, and cybersecurity policy implementation. This national context enriches the global discourse by providing perspectives on capacity gaps, policy adaptation needs, and opportunities for international collaboration in the development of digital forensic accounting.

On the right side of the network, the words *crime* and *era* **,** which are highlighted in the brightest color (2023–2024), indicate a strengthening of studies on contemporary digital crime phenomena. Research focus is shifting toward understanding the characteristics of modern crime, the operational mechanisms of perpetrators, and the new competencies that forensic professionals must master. This shows that digital forensic accounting is entering a new phase as a field increasingly influenced by rapidly changing socio-technological dynamics. Overall, this overlay pattern provides strong evidence that digital forensic accounting research is undergoing an evolutionary development, moving from a conceptual approach towards *interdisciplinary, technology-embedded, and policy-relevant frameworks*. This visualization also indicates that future research will increasingly depend on the integration of advanced technology, cross-border collaboration, and a deep understanding of the ever-evolving characteristics of digital crime.

VOSViewer Density Visualization Results

Figure 5



Source : Vosviewer, 2025

The VOSviewer density visualization image shows the intensity of occurrence and interconnections of key concepts in digital forensic accounting investigations. Areas with

brighter colors indicate topics that appear most frequently and have a high level of significance in the research network. The first prominent cluster, marked by the keyword "evidence," reflects that the aspect of digital evidence is a key foundation in digital forensic accounting investigations. The dominance of hotspots around this word indicates that issues related to reliability, authentication, and the process of collecting electronic evidence remain topics of academic interest. This shows that the validity of digital evidence is still the center of discussion in the development of forensic accounting methodologies. In addition, the dense area around the keyword digital forensic accounting shows that this central concept serves as a connecting point between several other research topics. The color density indicates that the literature still focuses on defining, determining the scope, and strengthening the digital forensic framework in the context of accounting. It also shows that research is in a phase of conceptual consolidation, where academics are trying to combine the perspectives of accounting, technology, and criminal investigation. The brightest spots appear in the keyword groups COVID, big data analytics, and public sector. The high density indicates that these three topics are the focus of recent research in digital forensic accounting. The COVID-19 pandemic has accelerated the use of digital technology in public services and financial systems, increasing the risk of fraud and cybercrime. In this context, big data analysis has emerged as a strategic solution used to detect anomalous patterns and improve the effectiveness of investigations. Meanwhile, the intensity of the public sector keyword reflects the increased attention to issues of transparency, accountability, and strengthening the capacity of the public sector in dealing with the threat of digital crime.

On the other hand, the very bright color distribution on keywords such as fraud disclosure, function, and Indonesia indicates more applied and contextual research developments. The emergence of the word "Indonesia" shows the contribution of research from developing countries that are beginning to position digital forensic accounting as an important tool to strengthen fraud reporting and governance in environments with varying levels of technological readiness. The highly prominent theme of fraud disclosure confirms that the ability of entities to uncover fraud based on digital evidence is an increasingly relevant topic, especially in the context of rising public expectations for transparency. Finally, the color density on the keywords crime and era indicates an expansion of the research focus to discussions of the characteristics of the modern digital crime era. This shows that the literature not only discusses forensic techniques, but also the social dynamics, technology, and evolving crime patterns that influence the need for new skills in digital forensic accounting.Overall, the interpretation of this density map shows that research in digital forensic accounting is evolving towards a multidisciplinary approach, with a strong focus on issues of digital evidence, big data integration, fraud risk in the public sector, and the implications of the pandemic on the digital crime landscape. This pattern reinforces that this field is increasingly important, not only in financial investigations, but also in strengthening governance and technology risk mitigation across various sectors.

Conclusion, Implications, Suggestions, And Limitations

The results of bibliometric analysis provide a number of important implications for the development of literature and professional practice in the field of digital forensic accounting. Findings regarding the high intensity of keywords such as evidence, big data analysis, and fraud disclosure indicate that analytical technology and the use of large-scale data have become essential components in modern financial investigations. This reinforces that digital competence is no longer just an additional skill, but a basic requirement for forensic accountants in the era of cybercrime. In addition, the emergence of interconnections between the public sector and developing countries, including Indonesia, highlights the urgency of increasing the capacity of government agencies to apply digital forensic techniques to detect and prevent increasingly complex financial crimes. The visualization of the density map also shows the concentration of themes in covid and era of crime, which illustrates how the Covid-19 pandemic has contributed to an increased risk of financial abuse and expanded the modus operandi of cybercrime. This situation has implications for regulators and organizations, which must adjust internal control policies, strengthen data security systems, and adopt technology-based approaches to risk mitigation. Therefore, this study not only maps the development of the literature but also provides important insights into the transformation of the accounting investigation landscape in the digital age.

Based on these findings, there are several suggestions that can be used as a reference for future research. Subsequent studies should explore thematic analysis through a systematic literature review approach so that the theoretical contributions of each study can be analyzed more comprehensively. Researchers can also combine qualitative methods, such as interviews or case studies, to enrich their understanding of the implementation of digital forensic accounting in the field. In addition, expanding bibliometric data sources to other databases, such as Web of Science, IEEE, or ACM, can increase the representativeness of research results. Special attention should be given to the context of developing countries, which face different challenges in terms of digital infrastructure and technological readiness. Despite providing a comprehensive mapping, this study has several limitations. First, the analysis relies on only one or a few databases, so it does not fully reflect all global publications related to digital forensic accounting. Second, the keyword-based approach in VOSviewer tends to be descriptive, so it does not capture the depth of methodology or the quality of each article's scientific contribution. Third, reliance on publication metadata can lead to terminological bias, where important topics not included in the keywords may be overlooked. In addition, this study has not analyzed the dynamics of thematic change in depth in a longitudinal approach, so that the conceptual evolution of this field has not been fully described. Given these implications and limitations, future research should develop fraud detection models based on technologies such as machine learning or artificial intelligence and evaluate their effectiveness in a digital forensics context. These efforts will contribute to strengthening the literature and improving investigative capacity to address the growing threat of financial crime in the digital age.

Bibliography

Aleke, N. T., & Trigui, M. (2024). Legal and ethical challenges in digital forensics investigations. In Cybercrime and digital forensics (pp. 147–176). IGI Global. https://doi.org/10.4018/979-8-3373-0857-9.ch006

Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. Mexican Law Review, 16(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Balusamy, S., Rengasamy, R., & J, A. (2025). Cybercrime investigations in the era of artificial intelligence: Automated evidence collection and analysis through the use of machine learning. In Proceedings of the 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1–6). IEEE. https://doi.org/10.1109/GINOTECH63460.2025.11076712

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by international law and cyber conventions. Multidisciplinary Reviews, 8(1), Article 2025024. https://doi.org/10.31893/multirev.2025024

Cotrina, L. K. C., León, P. M. S., Reyes Reyes, C. A., Ballesteros, M. A. A., Guzmán Valle, M. D. L. Á., Castillo, J. C. A., Acosta, R. M., & Morales, A. E. P. (2024). Cyber crimes: A systematic review of evolution, trends, and research approaches. Journal of Educational and Social Research, 14(5), 96. https://doi.org/10.36941/jesr-2024-0124

Dkhar, W., Lyngdoh, B. F., & Kumar, P. (2025). Forensic accounting: A strategy for preventing and detecting financial fraud in the digital era. International Journal of Accounting and Economics Studies, 12(2), 282–291. https://doi.org/10.14419/z7g9we35

Nelufule, N., Senamela, P., & Moloi, P. (2025). Digital forensics investigations on evolving digital ecosystems and big data sharing: A survey of challenges and potential opportunities. In Proceedings of the 2025 IST-Africa Conference (IST-Africa) (pp. 1–12). IEEE. https://doi.org/10.23919/IST-Africa67297.2025.11060495

Shamoo, Y. (2024). Cybercrime investigation and fraud detection with AI. In Cybercrime and digital forensics (pp. 83–114). IGI Global. https://doi.org/10.4018/979-8-3373-0857-9.ch004

Sharma, S. (2024). Digital forensics: Legal standards and practices in cybercrime investigation. In Proceedings of the 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) (pp. 1–6). IEEE. https://doi.org/10.1109/ICIPTM59628.2024.10563327

Trivedi, C., & Kumar, S. (2024). The forensic investigation model to empower investigation agencies in the era of digital technology. In Proceedings of the First International Conference on Pioneering Developments in Computer Science and Digital

Technologies (IC2SDT) (pp. 58–63). IEEE. https://doi.org/10.1109/IC2SDT62152.2024.10696006

Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial intelligence-based cybersecurity and digital forensics. In Artificial intelligence-enabled digital twin for smart manufacturing (pp. 391–419). Wiley. https://doi.org/10.1002/9781394303601.ch18

Zangana, H. M., Suryawati, R. F., Mustafa, F. M., & Vitianingsih, A. V. (2025). AI in forensic accounting. In Advances in forensic accounting (pp. 125–162). IGI Global. https://doi.org/10.4018/979-8-3373-6536-7.ch005