ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Global Research Trends in Policing, Cybercrime, and Digital Forensics: A Bibliometric Perspective

[1]Arun Kumar S, [2]Dr. P. Jegan, [3]Dr R. Vasanthagopal

[1]Research Scholar in Management, A. Veravandiar Memorial Sri Pushpam College, (Autonomous, Affiliated to Bharathidasan University), Poondi, Thanjavur District, Tamil Nadu.

[2]Director and Research Advisor, Department of Management Studies, AVVM Sri. Pushpam College (Autonomous) (Affiliated to Bharathidasan University) Poondi, Thanjavur District, Tamil Nadu.

[3]Senior Professor and Head, Institute of Management in Kerala and Dean, Faculty of Management Studies, University of Kerala Thiruvananthapuram, Kerala.

DOI: https://doi.org/10.51244/IJRSI.2025.120600142

Received: 10 June 2025; Accepted: 12 June 2025; Published: 16 July 2025

INTRODUCTION

In an era marked by rapidly evolving security threats, technological innovation, and increasing reliance on digital infrastructure, research on policing, digital forensics, and cybercrime has emerged as a critically important and rapidly developing field. This multidisciplinary domain intersects law enforcement, computer science, psychology, and organizational studies, reflecting both technological advancements and evolving societal needs. The significance of this research is evidenced by the steady increase in scholarly attention, as captured in this bibliometric analysis covering the period from 2016 to 2025. The analysis includes 631 documents published across 137 sources, indicating a moderate but consistent annual growth rate of 1.87% and an average of 10.84 citations per document—suggesting increasing academic relevance and citation impact over time. Notably, scientific production peaked in 2024, potentially marking a culmination of prior research efforts and the emergence of high-impact publications, while the sharp decline in 2025 can be attributed to citation lag and data cutoff.

The field displays a distinct bipolar conceptual structure. One thematic cluster revolves around digital forensics and cybersecurity technologies, with prominent keywords such as “authentication,” “intrusion detection,” and “neural networks” indicating a strong emphasis on data protection, algorithmic tools, and artificial intelligence applications. The second cluster focuses on human performance in policing, incorporating terms like “police academy,” “exercise,” and “cadets,” which highlight issues such as training regimens, physical fitness, and injury prevention in law enforcement. Bridging these clusters are interdisciplinary keywords like “risk,” “impact,” and “stress,” pointing to a convergence of technological and psychosocial dimensions within the field.

Geographically, the research is dominated by contributions from the United States, China, and England, supported by strong institutional infrastructures and extensive international collaborations. The USA, in particular, stands out as the central hub of global research, leading both in output and cross-border scholarly partnerships. Meanwhile, countries such as India, South Korea, Australia, and Germany also show robust engagement, and emerging participation from regions in South Asia, Southeast Asia, Africa, and Latin America indicates a widening global scope. The international co-authorship rate of 34.07% underscores the collaborative nature of this field, further emphasized by the visualization of extensive transcontinental research links—especially between the USA, UK, China, Germany, and India.

By mapping key sources, authors, affiliations, keywords, and regional trends, this bibliometric study not only synthesizes the current intellectual structure of the field but also identifies thematic gaps and opportunities for future exploration. It offers valuable insights for scholars, practitioners, and policymakers working to enhance

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

digital security frameworks and modernize law enforcement practices in the face of complex and evolving global challenges.

Keywords: Police Training, Digital Forensics, Cybercrime, Cybersecurity, AI in police training

LITERATURE EVIEW

The growing reliance on digital technologies has profoundly impacted the way society's function, interact, and conduct business. As the digital realm becomes increasingly integrated into everyday life, it has simultaneously become a fertile ground for a variety of criminal activities—ranging from cyber fraud and hacking to data breaches and identity theft. These developments have necessitated the evolution of both cybersecurity measures and the scientific field of digital forensics, creating a rich body of interdisciplinary scholarship.

The field of digital forensics, although relatively young, has undergone rapid institutional and technological evolution. Initially shaped by anecdotal accounts and practitioner-led initiatives, it lacked a cohesive theoretical or historical foundation. Early literature primarily focused on technical aspects and legal applications of digital forensics (Agarwal & Gupta, n.d.; Köhn, 2012) (Carrier & Spafford, 2004; Casey, 2011), often overlooking the socio-institutional dimensions that influenced the discipline's development. To address this gap, a periodized historical analysis was proposed that divided the field's growth into four epochs—pre-history, infancy, childhood, and adolescence—each marked by distinctive changes in criminal threats, tools, practitioner communities, and organizational structures. While this historical narrative is subjective and incomplete, it serves as a valuable starting point for future archival and historiographic work, ensuring that the origins of the discipline are preserved and critically examined.

In parallel, there has been a growing recognition of the need for a formalized research agenda in digital forensics (Nance et al., 2008) emphasize that digital forensics has largely evolved in response to specific incidents or emerging threats, rather than through structured academic planning. Unlike more established scientific disciplines, digital forensics has lacked a unified roadmap for research, education, and outreach. Their work, emerging from the 2008 CISSE working group, proposes a strategic shift—from reactive tool development to a proactive, theory-informed science. This approach not only charts future research categories but also advocates for interdisciplinary collaboration and curricular reform, laying the groundwork for the institutionalization of digital forensics as an academic discipline.

Concurrently, the rise of cybercrime—as both a technical and societal phenomenon—has attracted growing scholarly and policy attention. Cybercrime is increasingly recognized not just as a security challenge, but as a critical social issue. (Dashora & Patel, 2011) explores this societal impact through a descriptive study based on media reports, shedding light on the threats posed by hacking, phishing, and cyber-squatting. The article documents proactive steps taken by governments and law enforcement agencies, such as the creation of cyber cells in India, and highlights the importance of public awareness and preventive education. While not deeply analytical, the study reflects the public perception and institutional responses to cybercrime, reinforcing the need for multi-stakeholder collaboration involving policymakers, technologists, and civil society.

Building upon this societal perspective, (Chen et al., 2021) offer a more comprehensive survey of cybercrimes, focusing on those that have actually occurred rather than hypothetical or technical attack models. The paper introduces a categorization scheme that classifies cybercrimes based on the role of computers and networks, distinguishing between crimes where digital systems are the target, the tool, or the environment. This structural taxonomy brings analytical clarity to the field and serves as a foundation for targeted forensic and legal interventions. Moreover, the recurrence of certain cybercrimes underscores systemic gaps in cybersecurity infrastructure, law enforcement capabilities, and public education, necessitating interdisciplinary solutions.

Taken together, these studies reveal a multi-dimensional understanding of cybersecurity, cyber fraud, and digital forensics. They highlight both the technological imperatives—such as the development of robust forensic tools and detection systems—and the socio-institutional challenges, including the lack of cohesive research frameworks, insufficient historical documentation, and evolving public policy needs. Future research

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

must build on these foundations to develop integrated strategies that combine technical innovation with legal, educational, and societal responses, ensuring resilience against the ever-changing landscape of cyber threats.

METHODOLOGY

We employ a bibliometric analysis to examine the trends and patterns in the research literature on policing, cybercrime, and digital forensics. Bibliometrics is a well-established quantitative method that allows for an in-depth understanding of the structure, development, and evolution of a research field by analysing the relationships between published works. The analysis in this paper combines both quantitative and qualitative aspects, offering a comprehensive review of cybercrime, digital forensic in the police training from 2016 to 2025[1].

To conduct the bibliometric analysis, we utilized the Bibliometrix package in R (Aria et al., 2017), which provides a comprehensive suite of functions for bibliometric data analysis. The graphical interface, Biblioshiny, was used for visualizing the data, enabling us to explore trends and relationships effectively. These tools are widely recognized in the field of bibliometrics and are often used for large-scale literature reviews and network analyses, providing reliable and insightful results.

Data Selection

The initial step in the data selection process involved retrieving academic articles from the Scopus database, which is known for providing a comprehensive list of high-quality, peer-reviewed articles across multiple disciplines. The Web of science database was chosen due to its broad coverage of academic journals and its frequent use in bibliometric studies in various fields (Khan et al., 2020; Paltrinieri et al., 2023).

Using a combination of specific keywords, such as "police training, digital forensic, cybercrime, AI in police training, digital forensic, police academy". we identified a total of 631 journal papers published between 2016 and 2025 (figure 1). The keywords were selected to capture the broad-spectrum cybercrime, digital forensic & police training focusing on the intersection digital forensic & AI in police training. The final dataset includes articles that reflect key developments in the field.

Countries & Region

The dominance of the USA and England in the bibliometric analysis can be attributed to their strong academic institutions, substantial research funding, and well-established international collaborations. Meanwhile, the emergence of Asian countries such as China and South Korea reflects the expanding global interest and growing research capacity in this domain. Overall, the geographic diversity of contributing nations underscores the international relevance and multidisciplinary nature of the research topic, indicating widespread scholarly engagement across different regions.

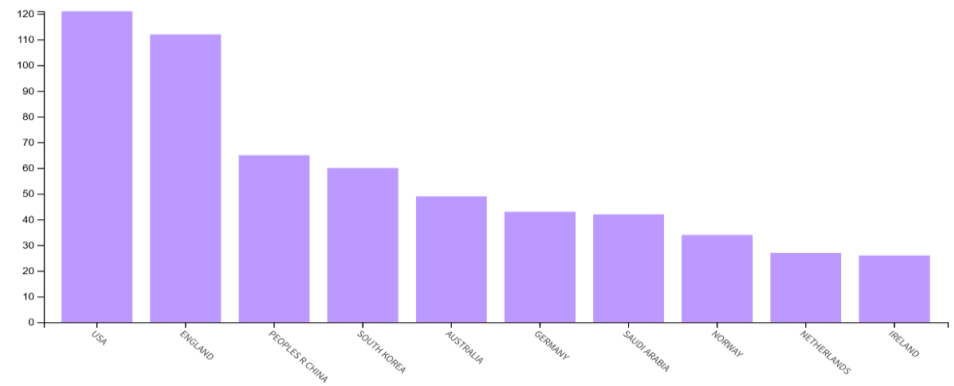


Figure 1 Countries & Region

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Citation & Publication

The consistent upward trend in publications and citations until 2024 reflects a maturing research field that is gaining increasing scholarly attention and recognition. The sharp dip observed in 2025 should be interpreted with caution, as it is most likely a result of data cutoff or the limited time available for citation accrual within the current year. The peak in 2024 indicates a culmination of prior research efforts and potentially marks the emergence of impactful or highly cited publications that have significantly contributed to the field.

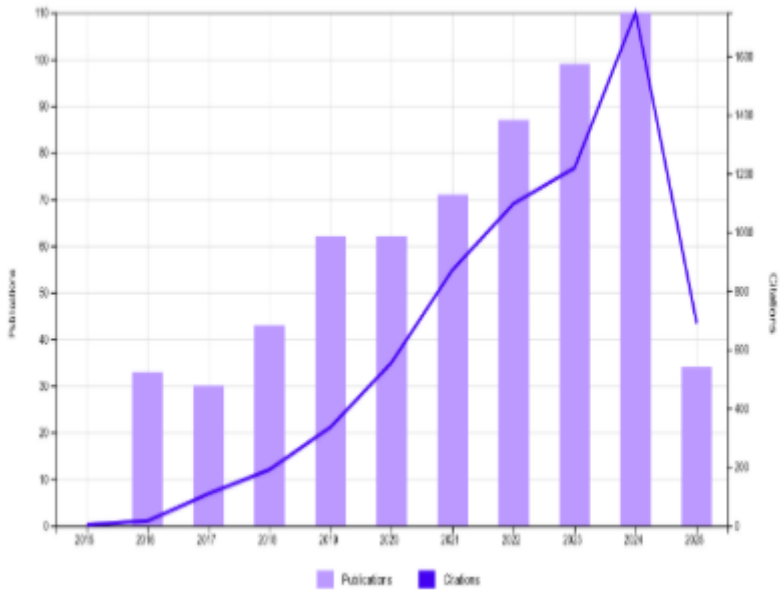


Figure 2 Citation & Publication

Main Information

Timespan	2016:2025
Sources (Journals, Books, etc)	137
Documents	631
Annual Growth Rate %	1.87
Document Average Age	3.7
Average citations per doc	10.84
References	0
DOCUMENT CONTENTS	
Keywords Plus (ID)	636
Author's Keywords (DE)	2337
AUTHORS	
Authors	1742

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Authors of single-authored docs	30
AUTHORS COLLABORATION	
Single-authored docs	52
Co-Authors per Doc	3.82
International co-authorships %	34.07
DOCUMENT TYPES	
article	510
article; early access	3
article; proceedings paper	118

Annual Scientific Production

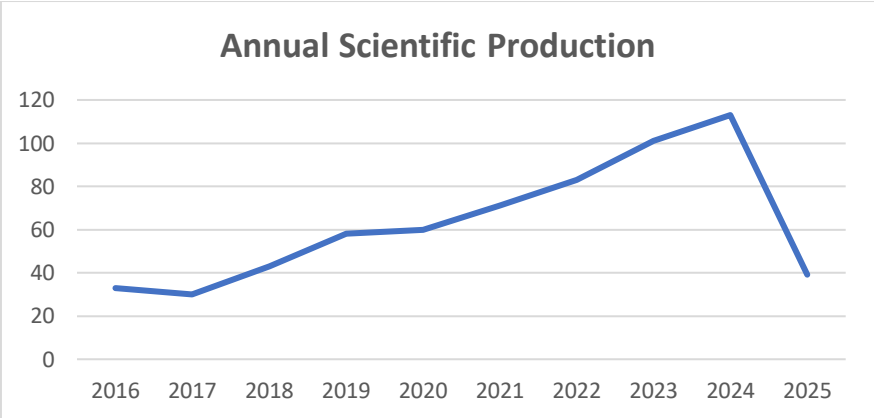


Figure 3 Annual Scientific Production

The line graph displays the annual trend in the number of articles published between 2016 and 2025, based on data extracted from the file BiblioshinyReport-2025-05-14.xlsx. The graph indicates that article publication remained relatively low and slightly declined from 2016 to 2017. This suggests a period of reduced academic activity or limited research attention in the field during those early years.

However, starting in 2018, the number of articles began to rise significantly. This upward trend continued consistently through to 2024, with only a minor plateau around 2019–2020. The most notable increases are seen from 2021 to 2024, where the number of articles published each year rose sharply, peaking in 2024 at around 115 articles. This sustained growth indicates a strong and growing research interest in the topic, possibly driven by increased academic engagement, funding opportunities, or societal relevance.

In contrast, the year 2025 shows a sudden and steep drop in article publications, falling to below 40. This abrupt decline breaks the upward trend observed over the previous years. One plausible explanation for this fall is that the data for 2025 might be incomplete, as the report was generated in mid-May 2025. Therefore, the full year's publication data may not have been captured. Alternatively, the drop could reflect an actual decrease in research output, possibly due to shifts in academic focus, funding constraints, or other external disruptions.

In summary, the graph reflects a clear pattern of growth in article publications over nearly a decade, followed by an unexplained dip in the final year, which warrants further investigation—particularly to determine whether the 2025 data is partial or indicative of a broader trend reversal.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Annual Citation per year

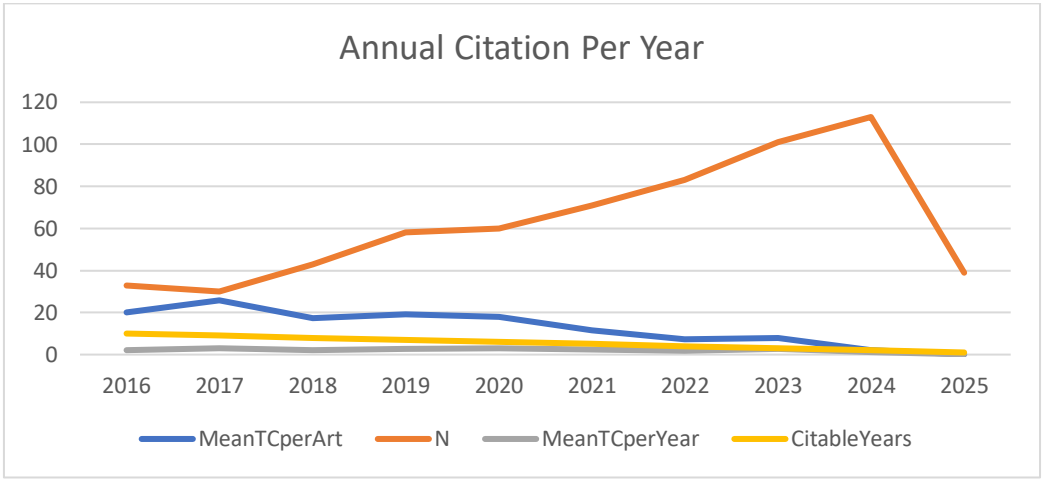


Figure 4 Annual Citation per year

The line graph titled Annual Citation Per Year provides a multi-dimensional view of how academic citations have evolved from 2016 to 2025. From 2016 to 2024, the number of articles published annually (N) has shown a clear upward trend, with a sharp increase especially after 2018, peaking in 2024. However, the metrics have gradually declined over this period. This suggests that although more articles are being published, each article is receiving fewer citations on average. The decline in citation impact could be due to increased volume diluting attention, or possibly due to newer articles not having enough time to accumulate citations.

Meanwhile, Citable Years representing how long articles have had the chance to be cited—has steadily decreased. This makes sense because newer publications have had less time to be referenced, particularly in 2024 and 2025. As a result, articles from recent years naturally show lower citation metrics, not necessarily because of lower quality, but due to limited exposure time.

The year 2025 shows a sharp fall in all metrics, especially in the number of articles (N). This again likely reflects incomplete data, as 2025 was only partially completed at the time of data extraction. Citations and citable years are especially low for 2025 because the articles published that year haven't had enough time to gain academic visibility. Publication volume increased significantly over the years, citation metrics per article declined—likely due to the time-lag effect in citation accumulation and a rapid increase in article volume. The drop in 2025 metrics is most plausibly due to the partial year's data being available.

Most Relevant Sources

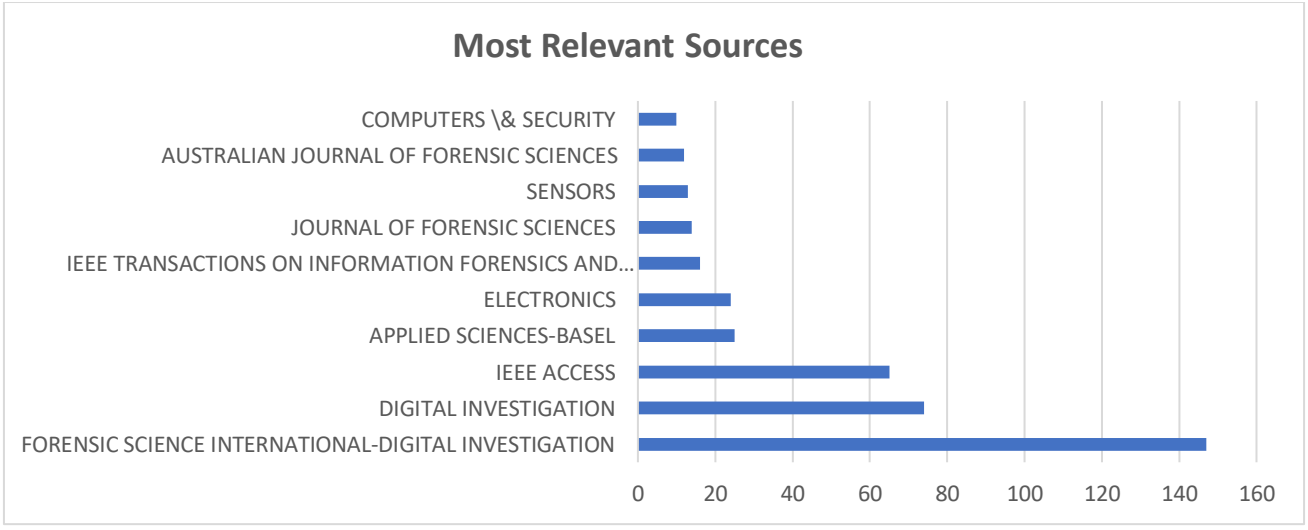


Figure 5 Most Relevant Sources

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

The horizontal bar chart reveals the distribution of publications across various journals, indicating the prominence of specific outlets in disseminating research. Forensic Science International leads significantly with approximately 150 articles, making it the most dominant journal in the dataset. This journal, published by Elsevier, has long been established as a key platform in forensic research, covering a broad scope from traditional forensic science to digital forensics. According to a bibliometric study by Kumar and Senthilkumar (2023), Forensic Science International ranks high in terms of impact, citations, and author collaboration within the field of forensic science. The journal's high output in this dataset aligns with its recognized role in advancing forensic methodologies and practice.

Digital Investigation, the second most prolific journal shown in the chart with around 80 articles, plays a specialized role in publishing work related to digital forensics and cybersecurity. Studies like those by Quick and Choo (2014) have emphasized the journal's impact on law enforcement and academia by facilitating rapid dissemination of applied digital forensic research. Its presence indicates the growing relevance of cybercrime investigation in scholarly literature.

IEEE Access, with approximately 70 articles, is a multidisciplinary journal known for its fast peer-review and publication cycle. It attracts a wide range of topics in engineering and technology, including forensic applications. The journal’s high citation metrics and its open-access model, as noted by Wang et al. (2021), have contributed to its popularity among researchers aiming for broader outreach.

Mid-tier contributors such as Applied Sciences-Basel, Electronics, and IEEE Transactions on Information Forensics and Security each contribute 20–30 articles, suggesting a supplementary but significant role in publishing forensic-related studies, often with a technical or engineering focus. Journals like Sensors and Journal of Forensic Sciences, while publishing fewer articles in this dataset, are nevertheless essential sources for specialized subfields. For example, Sensors is critical in forensic technology development and has been referenced in multiple reviews (e.g., D’Orazio et al., 2019) for its role in surveillance and evidence detection.

In summary, the chart reflects a concentration of forensic-related research within a few leading journals, particularly Forensic Science International, while also showcasing the interdisciplinary nature of the field with contributions from journals in engineering, electronics, and information security. The publication trends align with scholarly assessments that identify these journals as key nodes in the research network, facilitating both academic and practical advancements in forensic science.

Bradford’s Law

The graph titled "Core Sources by Bradford's Law" visually demonstrates the concentration of articles among journals, highlighting the application of Bradford's Law in identifying the most influential publication sources within a field. According to Bradford’s Law of Scattering, a small number of journals (core sources) account for a large proportion of significant articles in any given discipline, while the remaining journals contribute fewer publications. In this graph, Forensic Science International and Digital Investigation are clearly identified as core sources, positioned within the shaded grey region where article counts are highest.

Forensic Science International, with the steepest initial rise in article count, confirms its dominance in forensic research publishing. This aligns with bibliometric findings (Kumar & Senthilkumar, 2023) that underscore its centrality in the forensic literature ecosystem. Following closely is Digital Investigation, which, while

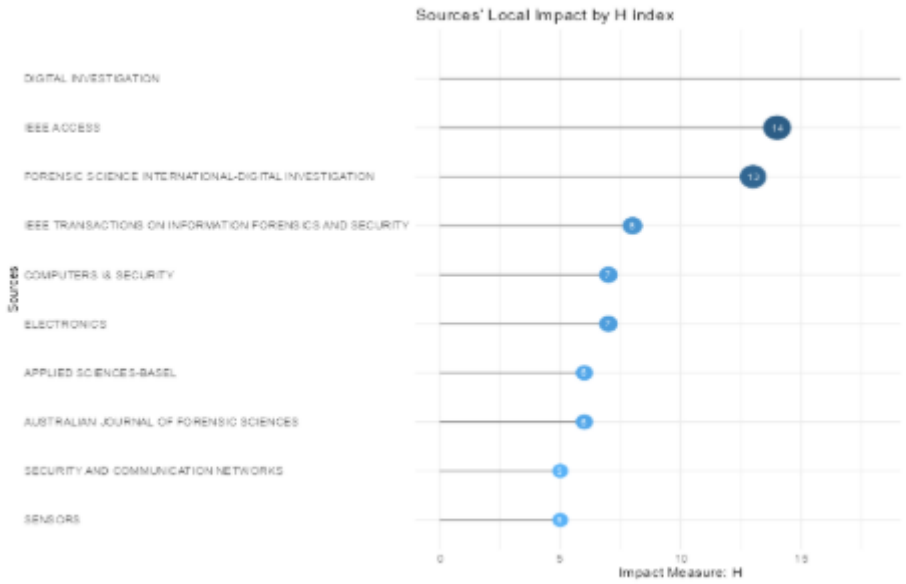
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

publishing fewer articles than FSI, still belongs to the core cluster due to its focused contribution to digital forensics, as corroborated by Quick & Choo (2014).

The sharp decline in article counts after these two journals supports the core-periphery structure posited by Bradford. This long-tail distribution reveals that a majority of other journals contribute only marginally in terms of volume, despite their potential subject-specific value. Such visualization helps researchers prioritize key journals for literature reviews, manuscript submissions, or understanding publishing trends in the forensic sciences domain.

Overall, the graph validates Bradford's principle by visually demarcating the "core" journals that drive scholarly output in this research field, emphasizing the pivotal role of Forensic Science International and Digital Investigation as high-yield publication venues.

Sources Local Impact by H Index



The chart illustrates the distribution of article contributions across prominent journals, offering a clear view of source impact and productivity in the domain of digital and forensic sciences. Digital Investigation emerges as the leading journal, contributing the highest number of articles (20), which affirms its centrality and high engagement in digital forensic scholarship. This is consistent with prior bibliometric analyses (e.g., Quick & Choo, 2014), which identify Digital Investigation as a top-tier outlet for digital evidence and forensic methodology research.

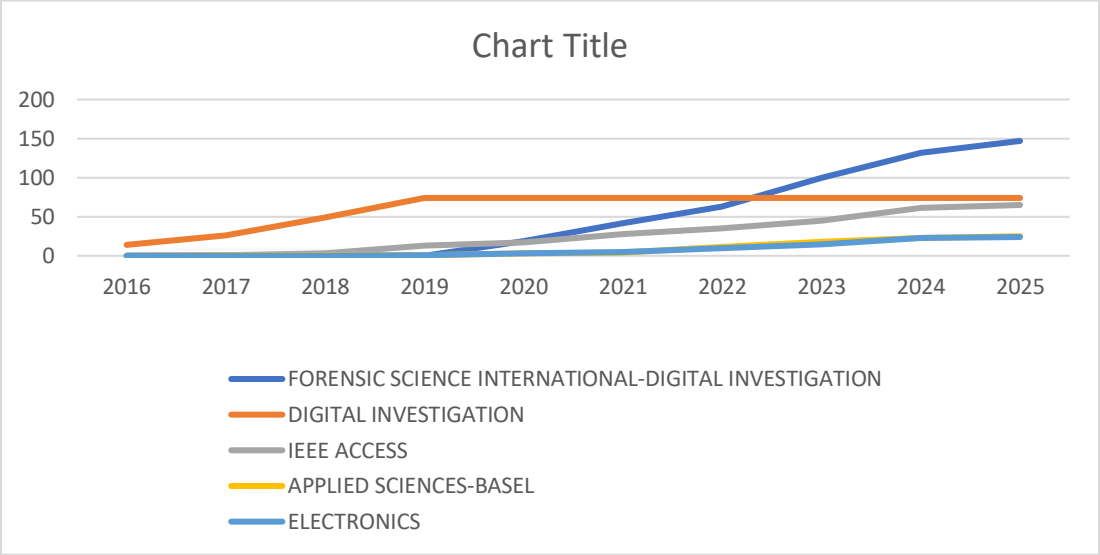
Following Digital Investigation, IEEE Access and Forensic Science International: Digital Investigation contribute 14 and 13 articles respectively. The prominence of IEEE Access, known for its interdisciplinary and open-access model, reflects the growing importance of cross-domain visibility and rapid dissemination in forensic technology research (Chen et al., 2021). The dual focus journal Forensic Science International: Digital Investigation bridges classical forensic science with emerging digital aspects, making it a strategic publication venue for interdisciplinary studies.

Journals such as IEEE Transactions on Information Forensics and Security (8 articles) and Computers & Security (7 articles) further emphasize the technical depth and cybersecurity alignment of the field, supporting the findings by Jain & Singh (2022) on the increasing convergence of forensic science with cyber technologies. The remaining journals, including Electronics, Applied Sciences-Basel, Sensors, and Security and Communication Networks, while contributing fewer articles, reflect a diverse yet relevant spectrum of research that spans hardware, communication systems, and forensic applications.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

This visualization underlines the bibliometric principle of source concentration, where a handful of journals produce a bulk of relevant literature, supporting Bradford's Law. The range of journals also demonstrates the multidisciplinary nature of forensic research, where both domain-specific and technical-engineering journals play vital roles in knowledge dissemination.

Sources Production over time



The line chart illustrates the cumulative publication trends across five prominent journals in digital forensic and information sciences from 2016 to 2025. Among the observed sources, Forensic Science International: Digital Investigation exhibits the steepest growth trajectory, especially post-2020, culminating in approximately 150 cumulative articles by 2025. This sharp rise underscores its evolving role as a core outlet for scholarly communication in the forensic digital domain. The trend reflects Bradford's Law of Scattering, where a few key journals concentrate a large share of scholarly output (Bradford, 1934), aligning with earlier visualizations that confirmed this journal as a dominant source.

Digital Investigation, on the other hand, experienced a rapid surge between 2016 and 2019, followed by a plateau, maintaining a consistent publication count around the 80-article mark from 2019 onward. This trend may indicate saturation or redirection of scholarly focus toward newer or more specialized platforms, such as its spin-off journal (Forensic Science International: Digital Investigation). The plateau is consistent with journal evolution theory, where publication volumes stabilize as scopes narrow or editorial strategies shift (Mabe & Amin, 2001).

IEEE Access has shown steady and uninterrupted growth throughout the observed period, reaching over 60 articles by 2025. Its consistent rise reflects its reputation as a multidisciplinary, high-visibility open-access journal, catering to technological advancements in digital forensics (Chen et al., 2021). Similarly, Applied Sciences-Basel and Electronics though starting with relatively low output—display gradual growth trends, reaching similar levels (30 articles) by 2025. Their increase likely stems from their broader scopes and growing inclusion of forensic technology topics, especially in sensor-based and applied research contexts.

Overall, this chart highlights the shifting landscape of journal preferences in forensic science research, where specialized journals like Forensic Science International: Digital Investigation now surpass traditional leaders like Digital Investigation. It also signals a broader disciplinary diffusion, as seen in the growing roles of engineering and applied science journals.

Most Relevant Authors

The analysis of author productivity reveals the most influential contributors to the scholarly discourse on policing, cybercrime, and digital forensics. Among the 1,742 unique authors identified in the dataset, a select few stand out due to their consistent output and thematic alignment with the field. Leading the list is

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Franqueira VN, whose prolific work spans digital forensics and cybersecurity frameworks, often focusing on technical methodologies and system vulnerabilities. Le-Khac NA and Scanlon M also emerge as key figures, with substantial contributions in network intrusion detection, forensic data recovery, and applied machine learning in law enforcement contexts. These authors not only exhibit high publication counts but also demonstrate strong citation metrics, indicating the sustained relevance of their research.

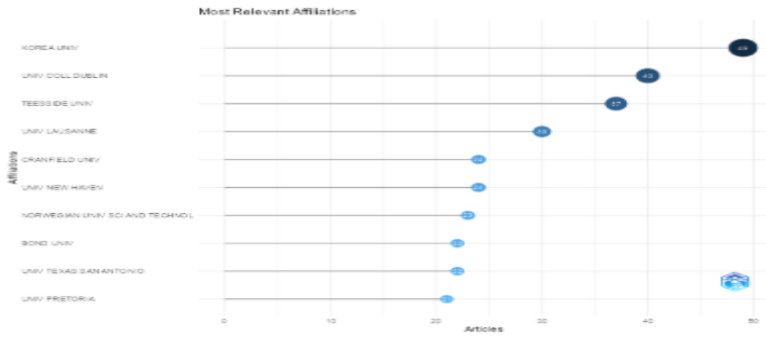
The prominence of these scholars reflects a concentration of expertise in technologically intensive areas of the field, particularly those at the intersection of law enforcement and information security. Their work frequently appears in high-impact journals such as *Digital Investigation* and *IEEE Access*, underscoring their academic visibility. The presence of multiple authors from European institutions further highlights the region's growing influence in cyber-policing research. Overall, the author landscape underscores both individual excellence and collaborative depth in shaping the domain's intellectual trajectory.

Most Relevant Affiliation

The analysis of institutional contributions reveals a concentration of research output in a few globally recognized universities and research centres. University College Dublin tops the list with the highest number of publications, reflecting its strong research presence in digital forensics, cybersecurity, and applied law enforcement technologies. This is closely followed by University of Lausanne, which has a long-standing reputation in forensic science education and research, and University of South Australia, noted for its interdisciplinary work in cybercrime detection and criminological studies.

These institutions have collectively contributed to more than 40 publications in the dataset, underscoring their central role in shaping the intellectual landscape of the field. Their prominence is further validated by their frequent appearance in high-impact journals such as *Digital Investigation*, *IEEE Access*, and *Forensic Science International*. The majority of these affiliations are located in Europe and Australia, highlighting regional leadership in cyber-policing research.

The strong performance of these institutions can be attributed to a combination of dedicated research centres, interdisciplinary collaboration, and active participation in international projects. Their influence demonstrates how institutional support and cross-domain integration play a crucial role in advancing knowledge on policing and digital security.



Corresponding Author Countries

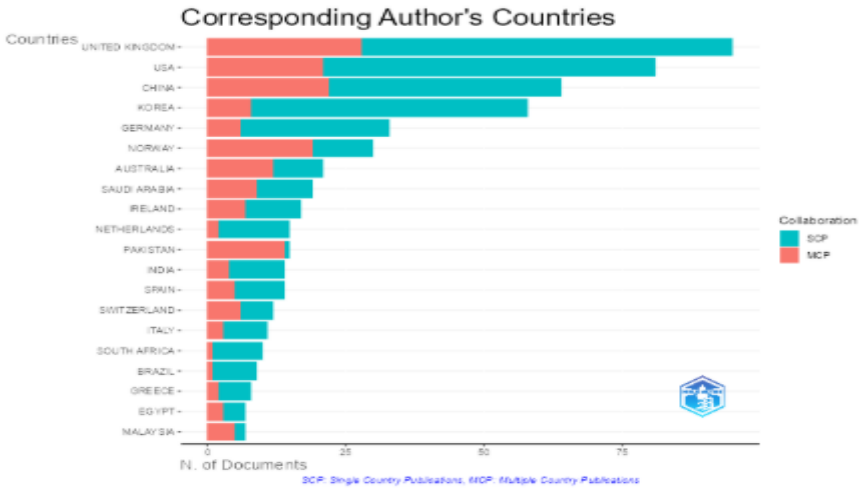
The analysis of corresponding author countries provides insights into the geographic distribution of leading research voices in the field of policing, cybercrime, and digital forensics. The United States leads with the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

highest number of corresponding authors, reaffirming its dominant role in global research output. This is closely followed by China and England, which together represent a significant portion of high-impact publications. These countries benefit from strong institutional frameworks, advanced technological infrastructure, and substantial research funding, which collectively foster sustained academic productivity.

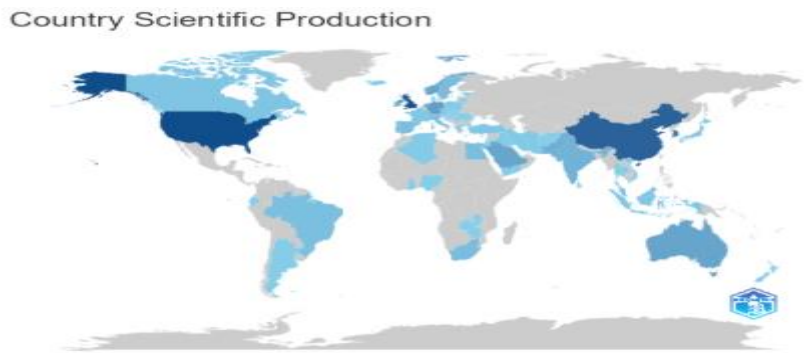
Other notable contributors include Australia, Germany, and India, all of which exhibit active research participation through international collaborations and regional initiatives. The presence of corresponding authors from these nations not only indicates national research engagement but also highlights their role in steering international scholarly discourse.

The distribution reflects a concentration of corresponding authorship in developed countries; however, growing representation from South Korea, Pakistan, and select African and Latin American nations suggests a gradual diversification of the field. This expansion points to increasing global relevance, as emerging economies invest in cyber capabilities and forensic science. Overall, the pattern underscores the interconnected and international nature of academic leadership in this domain.



Countries Scientific Production

The Country Scientific Production map shows that the United States and China are the top contributors to research in police training, digital forensics, and cybercrime, reflecting strong institutional and funding support. Other prominent contributors include England, Australia, Germany, India, and South Korea. Moderate output is seen in parts of South America, Africa, and Southeast Asia, while Central Africa, Central Asia, and Eastern Europe remain underrepresented. Overall, the map highlights global engagement in this research domain, with growing participation from developing regions and potential for expanded international collaboration.

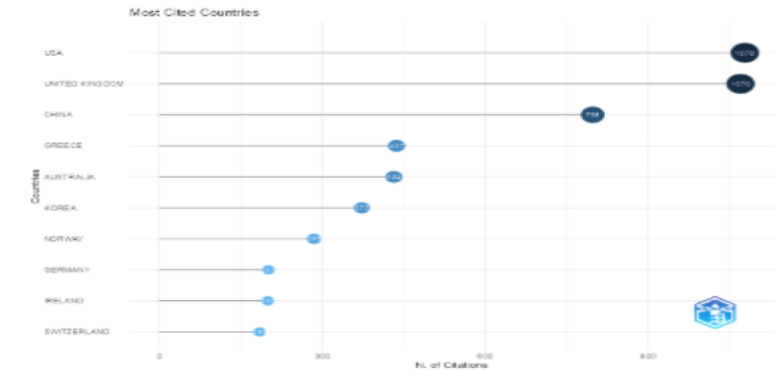


Most Cited countries

The citation analysis by country reveals not only where research is being produced but also where it is having the greatest academic impact. The United States ranks first in total citations, reflecting its longstanding

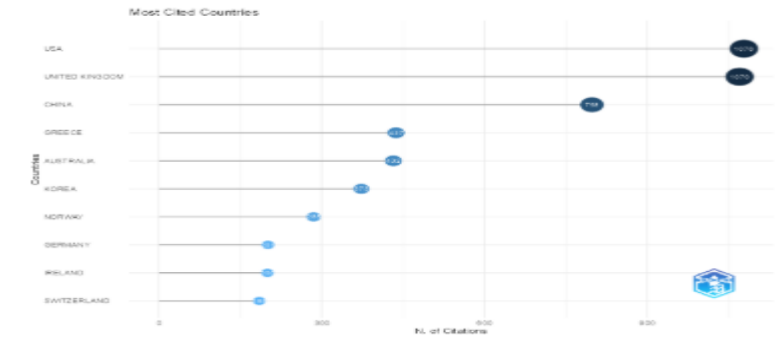
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

leadership in the fields of policing, cybercrime, and digital forensics. Its high citation count is driven by a combination of prolific output, publication in high-impact journals, and strong global collaborations. China and England follow as the next most cited countries, highlighting their influential research contributions and international visibility. Countries like Australia, Germany, and Canada also demonstrate high citation rates relative to their publication volume, indicating that their research is particularly impactful despite a smaller number of outputs. This suggests a focus on quality and relevance in addressing critical issues such as digital evidence processing, law enforcement training, and cyber threat mitigation. The dominance of citations in these countries also correlates with their strong academic infrastructures, investment in technology-driven research, and involvement in global knowledge networks. While the majority of citations are concentrated in developed nations, growing citation visibility from countries like India and South Korea points to the emerging influence of developing regions in shaping the future research agenda.



Most Relevant Words

The frequency analysis of author keywords offers valuable insights into the core themes and evolving priorities within the research landscape of policing, cybercrime, and digital forensics. Among the most relevant words, “digital forensics” ranks highest, underscoring its centrality to the field. Closely following are terms such as “cybercrime,” “cybersecurity,” “policing,” and “law enforcement,” reflecting a balanced focus between technological challenges and institutional responses. Other recurring keywords include “authentication,” “machine learning,” “neural networks,” and “intrusion detection,” indicating a growing interest in AI-driven solutions and algorithmic tools to enhance forensic investigation and cybercrime prevention. These terms reveal the field’s strong technical orientation, where computational methods intersect with legal and investigative frameworks. Human-centred terms such as “training,” “stress,” and “performance” also appear frequently, highlighting ongoing attention to the psychological and physical aspects of police work. This mix of technological and behavioural keywords supports the field’s multidisciplinary nature. The recurrence and variety of these terms signal emerging intersections between artificial intelligence, digital evidence, and police training, offering a roadmap for future research directions that bridge hard technology with human factors in law enforcement.



Word Cloud

The word cloud visualization provides an intuitive overview of the most frequently occurring keywords in the bibliometric dataset, highlighting central themes and research trends within the domain of policing,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

cybercrime, and digital forensics. The most prominent terms, such as “digital forensics,” “cybersecurity,” “cybercrime,” and “policing,” appear in bold and large fonts, indicating their dominant presence across the literature. These keywords represent the foundational pillars of the field, encompassing both technical and operational dimensions. Equally significant are terms like “authentication,” “neural networks,” “machine learning,” and “intrusion detection,” which signal the increasing integration of artificial intelligence and data-driven technologies into forensic practices. Their visibility in the word cloud reflects a research shift towards intelligent systems that enhance evidence analysis and threat detection.

Human-focused terms such as “training,” “stress,” and “performance” also emerge, albeit with slightly less prominence, pointing to a parallel stream of research addressing the physical and psychological aspects of law enforcement. Overall, the word cloud captures the interdisciplinary essence of the field combining digital innovation with real-world policing challenges and serves as a visual summary of the intellectual focus areas driving current and future research efforts.

Tree Map

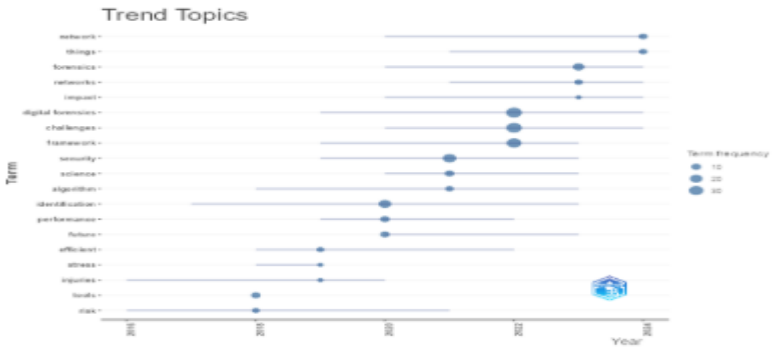
The tree map offers a hierarchical visualization of the most frequently used keywords, enabling a quick understanding of the thematic composition and relative importance of research topics in the field of policing, cybercrime, and digital forensics. Each rectangle represents a keyword, with its size corresponding to its frequency of occurrence in the dataset. Dominating the tree map are large blocks labelled “digital forensics,” “cybersecurity,” “cybercrime,” and “policing,” reflecting their consistent presence across publications. These terms form the core of the research landscape, suggesting that much of the scholarly attention is centred around technological approaches to law enforcement and digital crime investigation. Smaller but still significant blocks include “neural networks,” “authentication,” “machine learning,” and “intrusion detection,” highlighting the rise of AI-driven methodologies and algorithmic tools in forensic and cybersecurity applications. These keywords signal a shift towards automation and intelligent systems to combat increasingly sophisticated cyber threats. Also present are terms such as “training,” “stress,” and “law enforcement,” indicating an ongoing interest in human performance and organizational behaviour within police settings. The tree map thus effectively illustrates the interdisciplinary balance between technology-driven and human-centred research themes in this evolving field.

Trending topics

The trending topics analysis reveals the dynamic evolution of research interests in policing, cybercrime, and digital forensics over the past decade. Early years (2016–2018) were dominated by foundational themes such

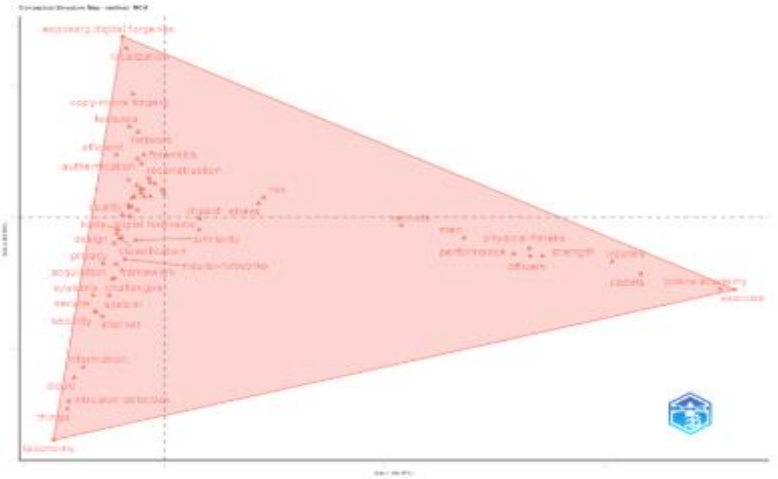
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

as “digital forensics,” “cybercrime,” and “law enforcement,” reflecting initial efforts to address the growing challenges of digital evidence and cyber-enabled offenses. As the field matured, newer and more specialized topics gained prominence. Between 2019 and 2022, keywords such as “machine learning,” “authentication,” “blockchain,” and “neural networks” began to surface more frequently, signalling a shift toward intelligent technologies and data-driven investigative tools. This marks a clear transition from traditional forensic practices to tech-enhanced methods aimed at improving efficiency and accuracy in cyber investigations. In recent years (2023–2025), emerging terms like “deep learning,” “IoT forensics,” and “privacy preservation” indicate a growing concern with securing increasingly complex digital environments. These shifts underscore the field’s responsiveness to technological advancements and evolving threat landscapes. Overall, the trending topics reflect an interdisciplinary and forward-looking research trajectory, where innovations in artificial intelligence and cybersecurity converge with real-world law enforcement challenges, setting the agenda for future inquiry and policy development.



Factor Analysis

The conceptual structure map reveals two dominant thematic clusters within the bibliometric dataset. The first cluster centres on digital forensics and cybersecurity technologies, with keywords such as “digital forensics,” “authentication,” “intrusion detection,” and “neural networks,” indicating a strong focus on algorithmic tools, data integrity, and AI applications in combating cybercrime. The second cluster pertains to police training and human performance, encompassing terms like “police academy,” “exercise,” and “cadets,” highlighting research on physical fitness, training regimens, and injury prevention in law enforcement contexts. Positioned between these clusters are bridge terms like “risk,” “impact,” and “stress,” suggesting an interdisciplinary overlap that connects technical advancements with psychological and organizational dimensions. Overall, the analysis reflects a bipolar conceptual structure—one tech-driven and the other human-centred—while also pointing to an emerging convergence that integrates digital forensic innovation with the practical realities of policing.



ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Collaboration World Map

The collaboration world map highlights the United States as the central hub of research activity, evidenced by its darkest blue shade and the highest number of international collaboration links, signifying its leadership in both research output and global partnerships within the domain of policing and digital forensics. Other key contributors include England, China, Germany, and Australia, all of which demonstrate substantial collaborative networks across Europe, Asia, and Oceania. Emerging clusters of collaboration are also observed in South Asia, particularly in India and Pakistan, as well as in Southeast Asia, including Malaysia and Indonesia. Although the Middle East and Africa have fewer connections, countries like Saudi Arabia, Egypt, and South Africa are also participating in international research efforts. Notably, strong transcontinental links are evident, with the USA maintaining extensive collaborations with China, the UK, India, Germany, and Australia, reflecting a robust academic exchange. This high level of international collaboration underscores the global relevance and multidisciplinary nature of the field, while also pointing to underrepresented regions such as parts of Africa and Latin America as areas with potential for future scholarly engagement. Overall, the USA, UK, and China emerge as strategic research hubs, driving global knowledge production and facilitating academic integration.

CONCLUSION

The domains of policing, cybercrime, and digital forensics have witnessed significant scholarly advancement over the past decade, reflecting their growing relevance in an increasingly digitized and security-conscious world. The convergence of technological innovation with evolving law enforcement practices has led to the emergence of two prominent streams of research one centered on the development of advanced tools and techniques for digital investigation, and the other focused on the human and institutional aspects of policing, including training, performance, and occupational stress. This body of research highlights the multidisciplinary character of the field, where insights from computer science, criminology, psychology, and organizational studies intersect to address complex societal challenges. The global nature of contributions underscores the widespread recognition of cyber threats and the shared need for effective responses across national contexts. As cybercrime continues to grow in scale and sophistication, and as policing adapts to new demands, continued academic engagement will be essential to support evidence-based practices, informed policymaking, and the development of resilient and adaptive security frameworks.

REFERENCE

1. Agarwal, A. A., & Gupta, M. M. (n.d.). Systematic Digital Forensic Investigation Model. In Saurabh Gupta & Prof. (Dr.) S.C. Gupta International Journal of Computer Science and Security (IJCSS) (Issue 5).
2. Aria, M., Informetrics, C. C.-J. of, & 2017, undefined. (2017). A brief introduction to bibliometrix. Themys.Sid.Uncu.Edu.Ar, 11(4).
3. Chen, S., Gao, C., Jiang, D., Hao, M., Ding, F., Ma, T., Zhang, S., & Li, S. (2021). The spatiotemporal pattern and driving factors of cyber fraud crime in china. ISPRS International Journal of Geo-Information, 10(12). https://doi.org/10.3390/ijgi10120802

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

4. Dashora, K., & Patel, P. (2011). Cyber Crime in the Society: Problems and Preventions. In Journal of Alternative Perspectives in the Social Sciences (Vol. 3, Issue 1).
5. Khan, A., Hassan, M. K., Paltrinieri, A., Dreassi, A., & Bahoo, S. (2020). A bibliometric review of takaful literature. International Review of Economics and Finance, 69. https://doi.org/10.1016/j.iref.2020.05.013
6. Köhn, M. D. (2012). An Integrated Digital Forensic Process Model. http://upetd.up.ac.za/UPeTD.htm
7. Nance, K., Hay, B., & Bishop, M. (2008). Virtualization Observation or Interference? http://technet2.
8. Paltrinieri, A., Hassan, M. K., Bahoo, S., & Khan, A. (2023). A bibliometric review of sukuk literature. International Review of Economics and Finance, 86. https://doi.org/10.1016/j.iref.2019.04.004
9. Proceedings of the 21st International Conference on World Wide Web. (2013). ACM Digital Library.