

The Emerging Threats and Trends in the Landscape of AI-Driven Forgery - A Bibliometric Analysis

Ancaman dan Trend Baharu dalam Landskap Pemalsuan Dipacu AI - Analisis Bibliometrik

¹Almaged Waleed Sadeq Jaaywel
Saadi Ahmad Kamaruddin
Bahtiar Jamili Zaini

Pusat Pengajian Sains Kuantitatif,
Universiti Utara Malaysia,
Malaysia

Correspondence email: ¹almagedwaleed489@gmail.com

Article history:

Received date: 27th January 2026
Revised date: 20th March 2026
Accepted date: 10th April 2026
Published date: 3rd August 2026

ABSTRAK

Dengan 1,248 penerbitan dari tahun 2005 hingga 2025 yang diperoleh daripada pangkalan data Web of Science, kajian ini telah menjalankan analisis bibliometrik komprehensif mengenai penyelidikan pemalsuan dokumen berkuasa AI. Dapatan menunjukkan pertumbuhan yang agak pesat dalam topik ini, terutamanya kadar pertumbuhan tahunan sebanyak 31.7 peratus. Amerika Syarikat mendahului dengan 404 penerbitan manakala China mengikut dengan 320 penerbitan. Empat kumpulan telah dikenal pasti, iaitu sifat risiko (deepfake, kecurian identiti), alat metodologi (pembelajaran mesin, pembelajaran mendalam), arkitektur pertahanan (blockchain, keselamatan siber), dan analisis forensik (kaedah pengesanan). Pada masa ini, kerjasama antarabangsa sebanyak 32.5 peratus dicatatkan dalam kajian ini (tertinggi ialah 42 peratus oleh UK). Kajian ini mendapati bahawa hampir tiada penyelidikan etika sebenar yang dikaitkan dengan aspek sosio-perundangan pemalsuan dokumen AI di seluruh dunia, walaupun terdapat pelbagai produk sedemikian wujud dalam masyarakat. Walaupun terdapat beberapa sempadan baru pemalsuan digital, kajian ini memberi tumpuan kepada pemalsuan berdasarkan manipulasi teks besar (GPT-3/4/X) dengan rantai pemalsuan yang mengganggu dan sangat mengelirukan. Ini adalah peta lengkap pertama bagi keseluruhan subjek ini yang memberikan penyelidikan dan pembuat dasar perspektif tentang hala tuju masa depan.

Kata kunci: analisis bibliometrik, deepfake, kecerdasan buatan, pemalsuan berkuasa AI, pemalsuan dokumen.

ABSTRACT

With 1,248 publications from 2005 to 2025 retrieved from Web of Science database, this study undertook a comprehensive bibliometric analysis of AI-powered document forgery research. The findings indicate fairly rapid growth in this topic, particularly an annual growth rate of 31.7 per cent. United States led with 404 publications while China follows with 320 publications. Four groups were distinguished, being challenged by this study, namely the nature of the risk (deepfakes, identity fraud), methodological tools (machine learning, deep learning), defensive architectures (blockchain, cybersecurity), and forensic analysis (detection methods). Presently, 32.5 per cent international collaboration is highly earned in the study (highest being 42 per cent of the UK). The study posits that almost no real ethical research is associated with the socio-legality of these aspects of nasty and AI document forgery around the world, though that such a wide supply of products should exist at some point in society. Although there are some new frontiers of digital forgery, this study constrains itself to forgeries based on the large (GPT-3/4/X) manipulation of complete texts with disruptive and blazingly deceptive and massive forgeries chaining block. It is the first complete map of the entire subject giving the researchers and market policy-makers a perspective on the causes-finals that are still to come.

Keywords: *AI-powered forgery, artificial intelligence, bibliometric analysis, deepfakes, document forgery.*

1. Introduction

Over the past decade, the digital environment has undergone a radical transformation, and the flow of information and its globalization have created a distinctive era. It is also fertile ground for all kinds of crime; and with AI-enhanced forgery, forgery has become its most dangerous form. It cannot be ignored that forgery today goes beyond simply falsifying traditional signatures with ink on paper. It is more likely to be digital, i.e., identical to the original. Thus, with materials that are difficult to distinguish from the original—and difficult for humans or even traditional systems to judge—it becomes impossible to differentiate them from the original. (Brettinger & Bagili, 2019). Digital forgery includes advanced forms such as phishing, which relies on techniques that mimic the identity of a person or organization (Popescul & Radu, 2025), and this pattern has evolved to include the forgery of entire documents that appear legitimate. Artificial intelligence and machine learning techniques have been used to enhance cybersecurity and develop forgery detection mechanisms, but they have also been used to carry out more sophisticated and complex attacks (Brundge et al., 2018). Rapid learning models on neural networks (DNNs) are increasingly used in a wide range of applications. The ability to distort reality has seen tremendous advancements with deepfake technology. This technology enables the creation of audio and video clips of real people saying and doing things they never said or did. Machine learning techniques enhance this technology, making deepfakes more realistic and harder to detect. This type of forgery is called audio-visual forgery, and technologies such as competitive generative networks (GANs) are a prime example of how AI can be used to create deepfakes that are difficult to distinguish from real content (Chesney and Citron, 2019). This object is interest for academic and industrial research in AI-enabled document forgery, while the research field is still disjointed and cut across various domains like

computer science, cyber security, law, and sociology. A significant and immediate need exists for integration of the disparate threads to identify the principal lines of development, gaps in knowledge, and the interplay among the various constituent sub-disciplines. Thus, it is necessary to conduct a research in the AI-enabled document forgery field to provide an extensive holistic synopsis about the various Contributions and their development.

Therefore, it is essential to develop a comprehensive overview of the research and articles published on AI-enabled document forgery in the future. This approach—using a range of bibliographic techniques to analyze subject matter and intellectual output, and to analyze the factors driving academic influence and its evolving impact—can enable researchers to map knowledge in the field, identify the most influential authors, monitor research collaboration networks, and track the evolution of topics and keywords over time (Donthu et al., 2021). The knowledge of researchers, scientific networks, and cross-border collaboration on this subject assesses the importance, the extent of development, and its future prospects, and allows for the utilization of recent findings in future research.

1.2 Research Problem

In today's world, the pace of digital transformation is accelerating to such an extent that artificial intelligence (AI), while a tool for enhancing efficiency and creativity, is automatically assuming a more ambiguous and conflicting role. On the one hand, AI tools are contributing to constructive change in many areas, including massive online courses (MOOCs) (Chen, 2006; Jinping, 2024). On the other hand, and perhaps more importantly, these tools pose serious risks. AI-powered document forgery is, in many ways, one of the most impactful and distinctive threats of our time. The very concept of document forgery has undergone a radical transformation, no longer limited to the manual copying of signatures or other written documents. The phenomenon has expanded to include the sophisticated reproduction of digital content, including text (Xia et al., 2024), audio, images, videos (deepfakes), and even digitally altered and biometrically forged documents (Chesney and Citron, 2019). These sophisticated forgery techniques (particularly deep learning and generative adversarial networks) have reached a level where they are difficult to detect using traditional methods (software or human) (Rizki, 2019; Bronk, 2013). The scale of this forgery is inherently destabilizing (transnational), undermining the security of individuals, financial systems, the sanctity of academic work, national security, and even democracy itself. Deep fake technology can manipulate public perception, defame individuals, and alter markets and elections (Chesney and Citron, 2022). The vast tools that can create assignments and papers in a similar way to humans have made plagiarism and academic fraud even easier. Large language models can produce assignments and papers that are of an indistinguishable quality to that of a human (Shea et al 2024). The phenomenon of AI hallucinations, producing plausible yet false information, has further introduced new unreliability into educational and media materials (Salevsky et al., 2023). Users have created increasingly sophisticated scams such as identity theft audio or video files that bypass biometric authentication. There has been an increase in social activity fraud, especially with advanced tools and algorithms. It has also become increasingly more difficult to detect document forgeries as duplicates can be made that are visually indistinguishable from an original. This poses a challenge in countering adversarial attacks, where documents or images are manipulated in a way that misleads detection systems,

potentially leading to the misclassification of fake content (Noguera et al., 2025). The rapid growth of big datasets and increasing computing power have spurred the development of these models, which can mimic human behavior with remarkable accuracy (Sarker et al., 2020; Asfadisherhini et al., 2022). In light of these challenges, numerous research projects have emerged aimed at combating information forgery in the field of artificial intelligence, particularly the use of AI to detect document forgery, primarily through machine learning and large-scale data analysis (Liu et al., 2018; John et al., 2025).

There are also options such as setting up regulations and using frameworks such as blockchain to secure records and data. Therefore, a management system that integrates blockchain and smart contract technologies is necessary to solve problems concerning the falsification and manipulation of data. The blockchain will have all of the information regarding the production and the subsequent transfer of the data concerning luxury products. In this way, a full and reliable data record which is traceable and cannot be changed will be created. Basically, blockchain is a shared database that is decentralized, cannot be tampered with, can be traced, and is anonymous. Smart contracts, which also come into play, allow for transactions to be made without a third-party interceding. (Chen et al., 2022).

Despite the considerable momentum in the area of AI-generated forgery, there remains a fundamental problem: the scientific literature about AI-generated forgery is scattered and incoherent. Research in the area of AI-generated forgery is conducted in several academic disciplines; including but not limited to, computer science, cybersecurity, law, criminology, media studies, and education. Although each of these disciplines provides valuable contributions, the research lacks integration across these disciplines. Prior bibliometric studies were conducted on narrow disciplines, such as financial fraud (Al-Hashedi & Magalingam, 2021; West & Bhattacharya, 2016), cybersecurity/data science (Sarker et al., 2020) and phishing (Popescul & Radu, 2025).

To date, no bibliometric study has been published that synthesizes the disparate literature into a coherent, holistically-treated field of study; thus, leaving research on AI forgeries unorganized or lacking coherence. The fragmentation of this literature results in multiple negative consequences: Of analytical techniques as there is no systematic bibliometric overview of the existing trends, key authors, the intellectual framework of research on AI forgeries, it is almost impossible to establish a standard methodology for conducting future research in the area of AI forgery. Lack of a research agenda: Without a structured roadmap for this field, researchers lack the ability to navigate the research area and examine the relationship between the research directions of the three streams of AI-related forgeries: offensive stream (the creation of forgeries), defensive stream (the detection and prevention of forgeries), and regulatory stream (the regulation of forgeries). Inability to analyze future trends: Without a comprehensive synthesis of the AI forgeries literature, there is no foundation to predict the most promising areas of future research; thus, leading to guesswork rather than informed decision-making. This is the gap that the present study seeks to address.

By conducting a comprehensive bibliometric analysis of the literature on AI-powered document forgery, this research aims to provide the first unified overview of the field. Specifically, it will answer the following questions:

- i) What is the total volume of scientific output in this field, and how has it evolved over time?
- ii) Who are the most prolific and influential authors, institutions, and countries?
- iii) What are the dominant research areas and thematic clusters within the field?
- iv) What patterns of scientific collaboration exist, both internationally and within countries?
- v) What are the current knowledge gaps, and what directions seem most promising for future research?

In doing so, this study will try to transform the Current efforts into a coherent intellectual map, offering a data-driven foundation for navigating this critical and rapidly evolving field.

1.3 Importance of Research

The significance of this study lies in its methodology as the first attempt to conduct a comprehensive bibliometric analysis that examines research from various disciplines (including computer science, cybersecurity, legal research, media research, and others) under a single umbrella of AI-assisted document forgery. On a deeper level, this analysis reveals the intellectual frameworks and cognitive structures underlying this field, while also addresses the temporal dynamics surrounding the evolution of its core concepts.

2. Literature Review

Within the framework of bibliometric analysis, some studies, such as Purnama et al. (2024), which noted the rapid proliferation of the topic in machine learning literature and studies, and discussed the most common topics such as malware detection and phishing, were among the first to observe the rapid expansion of the literature in the field of machine learning and cybersecurity. In the same way, Mutluturk and Metin (2023) concentrated on phishing as the only and most detailed study in the field, while Sahingoz et al. (2019) reviewed most studies on emerging AI technologies. Still, they only studied specific threats (phishing, malware) and did not investigate more generally the phenomenon of forgery and its countermeasures. Along the same lines, the study by Ramos et al. (2024) should be acknowledged for its inclusion of auditing and financial fraud, and for tackling the emerging machine learning and deep learning technologies. However, its scope was restricted to financial and administrative domains and did not address AI-based forgery mechanisms and countermeasures. The phenomenon of AI generated ‘deep forgery’ and its detection methods has gained traction from numerous scholars. Chesney and Citron (2019) addressed the ethical issues regarding deepfake technologies, while the complexities of ‘forged’ media and the ways to mitigate their negative impacts have been the focus of research by Mirski and Lee (2020) and Nguyen et al. (2023). Later, with the emergence of linguistic models, attention shifted to text forgery. Garcia et al. (2023) worked on evaluating the quality of a sophisticated forgery sample within the framework of electronic signatures, in the context of producing sophisticated forgeries, and how to develop more sophisticated and personalized phishing attacks using AI. The relationship of previous studies to the present: The body of

research to date offers a valuable, albeit somewhat disparate, body. While Mutluturk and Metin (2023) and Ramos et al. (2024) focused on phishing and financial fraud, respectively, the study by Matt et al. (2025), which highlighted the importance of biometric analysis, focused on malware as a specific subfield. Chesney and Citron (2019) explained deepfakes and their implications if countermeasures are not developed, and Mirski and Lee (2020) and Nguyen et al. (2023) examined the complexities of creating and mitigating forged media, including AI-powered forged documents. This research aims to provide a comprehensive biometric analysis of AI-assisted forgery strategies and countermeasures. This bibliometric work seeks to address the lack of comprehensive bibliometric studies in this field that focus solely on the threat posed by cybercrime in the form of forged documents and images, by integrating deepfakes and cyber fraud. Purnama et al. (2024) provided an overview of the field of machine learning in cybersecurity, while Ramos et al. (2021) and Ramos (2024) previously focused on artificial intelligence in auditing. This study aims to concentrate on AI-enhanced document forgery prevention to clearly illustrate the interrelationships between related fields and to demonstrate their evolution over the years. This integrated perspective will facilitate the discovery of multidisciplinary collaborative networks and emerging and evolving research areas within this field, providing policymakers and researchers with a guide to address the multifaceted and highly sophisticated challenges posed by cyber threats in the age of artificial intelligence.

3. Research Methodology

3.1 Data Collection and Search Strategy

In this study, a detailed bibliographic analysis was used to understand the body of work in the field of artificial intelligence (AI) in combating forgery. We relied on the core Web of Science (WoS) collection due to its comprehensive and detailed subject coverage. To obtain the most recent published work, searches were conducted in this resource as of March 2025. To ensure broad and comprehensive literature coverage, AI-related terms (e.g., artificial intelligence, machine learning, deep learning, competitive generative networks, big language models) were used in conjunction with terms related to document forgery and related threats (e.g., document forgery, identity forgery, signature forgery, certificate forgery, deed forgery). Terms related to detection and countermeasures (e.g., forgery detection, anti-forgery, document verification) were also included to reflect the research on combating forgery in this area. The specific search queries are listed in Table 1.

Table 1. Search Criteria for Data Extraction

Component	Description
Keywords	<mark>TS= (artificial intelligence OR AI OR machine learning OR deep learning OR generative adversarial network OR GAN OR large language model OR LLM) AND (document forgery OR identity fraud OR signature forgery OR certificate forgery OR forged document OR counterfeit document) AND (forgery detection OR anti-forgery OR document authentication OR fraud detection)</mark>
Database	Web of Science Core Collection

Component	Description
Timespan	2000-2025 (All years)
Language	English
Document Types	Article, Review, Conference Proceeding Paper
Search Date	March 15, 2025

Table 1 provided the search strategy and data extraction criteria, such as keywords, the WoS database, and the time range (2000-2025), and the filtering parameters to ensure the reliability of the bibliometric. The total of the documents were found in the initial search is 1842. Different inclusion and exclusion criteria were applied, and duplicates were subsequently removed, to maintain quality and relevance of chosen documents, different criteria for inclusion and exclusion were applied during the screening phase. The inclusion criteria involved the following: (1) documents must be published in English; (2) documents published in peer-reviewed journals or conference proceedings; (3) documents solely dealing with AI-powered forgery, document forgery or associated threats; and (4) documents published within the range of 2000-2025. The exclusion criteria were: (1) documents not published in English; (2) duplicate documents; (3) documents that are editorials, book reviews, or news and do not contain original research; and (4) documents that are not accessible in full text. Based on the applied criteria, 594 documents were excluded and 1,248 documents were retained for final evaluation. leaving a total of 1248 documents. The relationship between search field, authors, citations, and journals were assessed iteratively, based on the export limitation from the Web of Science. The (WoS) record content consisted of full records and cited references in Plain Text Format. Missing or incomplete data was repaired, and authors, journals, conferences, and publishers were aliased to a consistent naming scheme. All these documents were combined into a single document and analyzed in Biblioshiny (from the Bibliometrix R package) and VOSviewer. Figure 1 presents a summary of the review of the study based on the PRISMA flowchart.

4. Analytical Tools and Techniques

Analytical Tools and Techniques Analysis of data using Biblioshiny (from Bibliometrix software suite) and VOSviewer were of these used which also have in these and complementary functionalities. For thoroughness other some specific analytical software were also used.

4.1 Tools of Bibliometric Analysis

- A. Bibliometrix / Biblioshiny suite
 - New productivity and performance metrics of scholarly output
 - Growth, citation and influence rates
 - Collaboration networks of authors and institutions
 - Development of topics and trends over time

- B. VOSviewer Network maps of bibliometric data Clustering of subjects and analysis of the cluster Concept and keywords relationships (visualization of) Relationships analysis (shared authorship, co-presence, citation)
- C. Others For the analysis of citation networks: CitNetExplorer For network analysis: Pajek For network visualization: Gephi

Table 2. Descriptive Summary of the Dataset

Description	Results
Timespan	2005 : 2025
Sources (Journals, Books, etc.)	588
Documents	1,248
Average citations per document	14.32
Annual Growth Rate	31.7%
References	39,451
Keywords Plus (ID)	1,845
Authors Keywords (DE)	3,127
Authors	4,215
Authors of single-authored documents	48
Single-authored documents	52
Co-Authors per Document	4.12
International Co-Authorships %	32.5%
Document Types	
- Article	784
- Conference Paper	452
- Review	12

Table 2 is a descriptive summary of the data that allows distinguishing the content indicators of bibliometric and defining the background of the research on AI-based forgery detection.

4.2 Indicator Assessment

The cited research spans from 2005 to 2025. The Bound field expands 20-year span fosters the growth of the area of AI-fueled forgery detection. The study covered more than 588 distinct academic journals in publication. This also indicates a variety of fields such as computer science, cybersecurity, law, and media. The dataset contained 1,248 data points, a considerable indicator of research interest in the area. 14.32 was the average citation per record, a notably high value. The average annual growth rate of the dataset was 31.7%. This indicates the growth of the AI-powered forgery detection field through the datasets and the documents they contain. This research reinforces the importance surrounding AI-powered forgery detection.

The total number of references was 39,451, demonstrating the researcher's reliance on previous literature. 1,845 new keywords were added, which are key terms that databases added

contextually based on research. Authors identified 3,127 keywords. This suggests that in this field, there is no consistency in terminology, indicating a lack of coherence in the use of scientific terms. 4,215 authors and co-authors show a considerable amount of contribution to the field. Only 52 papers had a sole author, showing that very few papers are written by one researcher. Average author count was 4.12, suggesting that papers are written by an average of 4 researchers. 32.5% international collaboration shows that a little over a third of the research was done with international co-authors. This shows the level of collaboration and openness of the field. This shows that the document forgery challenge that is AI powered has an intricate solution that is international in scope and cross-disciplinary. Document types are: Scientific research papers (784): This is the largest classification which in turn enhances the strength and validity of the findings. Conference papers (452): This large classification shows that researchers are very eager to publish their findings in conference papers, which is in line with the rapidly evolving field. Scientific reviews (12): The field does seem to be growing as indicated by the annual growth rates, as well as the number of citations and documents published. The growth rate of 31.7% is particularly impressive. The field does appear to be maturing and growing in influence with an average number of citations per document that is on the higher end and a good number of documents published. The rate of collaboration also shows the DWAI and document forgery field as needing focus and collaboration. It is global and interdisciplinary, evidenced by the number of different documents and unique citations. The field of forgery and AI is intricate and in a state of rapid growth. It is important to pay attention to as it is not a field that is going to stagnate.

Figure 1 shows a summary of our document selection process using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flowchart. The process is broken down into four segments: Identification: The first step involved a keyword search in the Web of Science database that returned 1,842 results. Screening: All 1,842 documents were screened based on the titles and abstracts. During this step, no documents were removed because the screening was done too broadly. Eligibility: Of the 1,842 documents, full text reviews were done, and after the application of the inclusion and exclusion criteria, 594 documents were removed for being irrelevant, duplicate, or non-research publications (i.e. editorials, book reviews). Included: 1,248 documents were determined to meet the criteria and were incorporated in the final bibliometric analysis. This selection process shows that the methodology of this study is transparent and replicable.

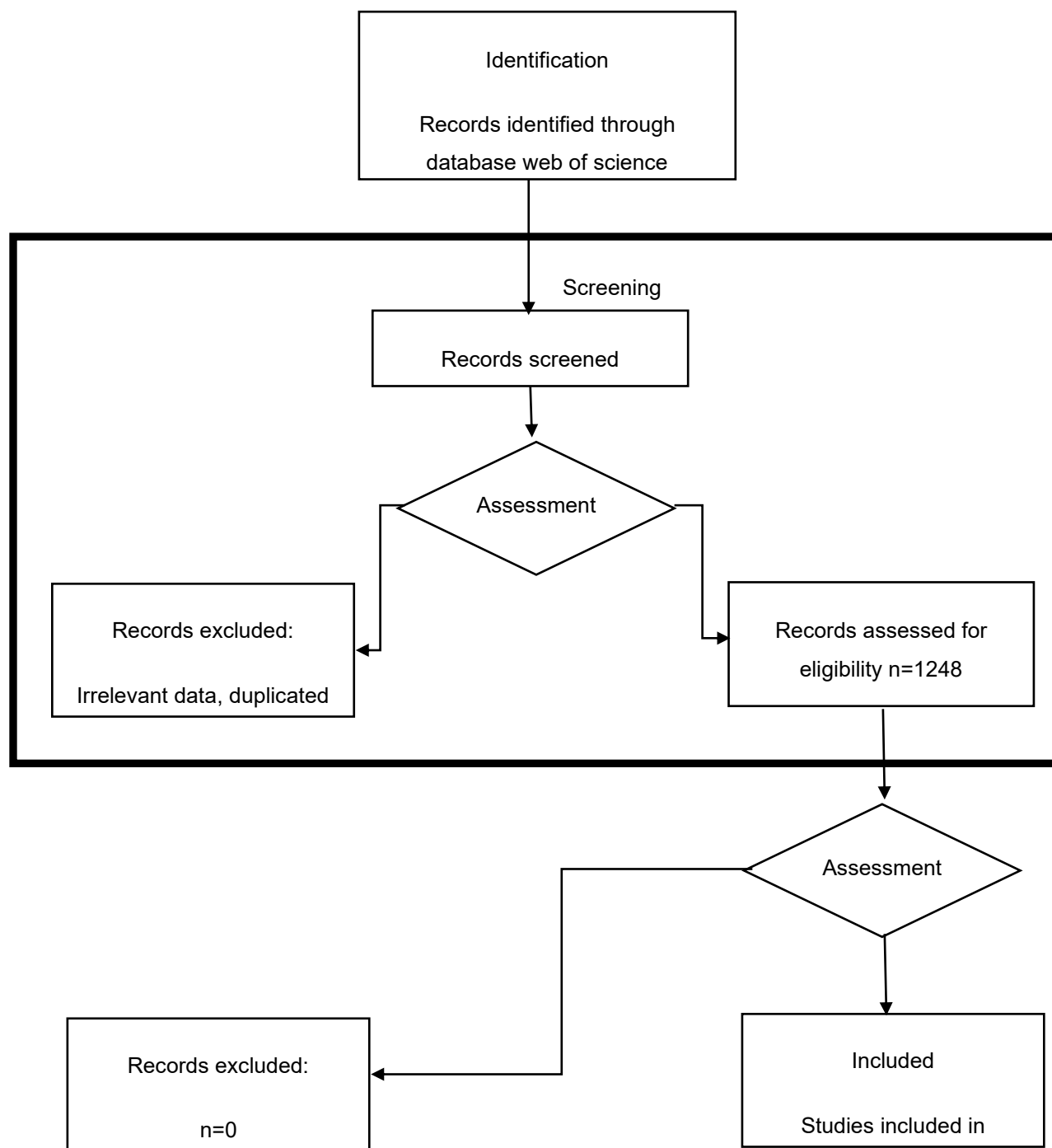


Figure 1. Flow diagram

5. Publication trends, impactful documents and publications

Advances in artificial intelligence (AI) technologies and computing power have propelled research efforts in combating phishing to a new level. Phishing attacks remain a persistent and complex problem. Literature analysis reveals a growing interest in this topic. During the first decade of this research field, there were only 49 publications, while the last few years have witnessed a significant surge in publications, with 712 documents directly related to the topic. This represents a major development, as AI-powered forgery has become an evolving and persistent threat. The literature analysis reveals a remarkable increase in academic interest in this vital subject. Publishing trends and influential documents and publications: Advances in artificial intelligence (AI) technologies and computing power have propelled research efforts in combating phishing to a new level. Phishing attacks remain a persistent and complex problem. Literature analysis reveals a growing interest in this topic. During the first decade of this research field, there were only 49 publications, while the last few years have witnessed a significant surge in publications, with 712 documents directly related to the topic. This represents a major development, as AI-powered forgery has become an evolving and persistent threat. The literature analysis reveals a remarkable increase in academic interest in this vital subject.

The most influential documents were evaluated using citation count metrics to acknowledge pioneering work on important technologies, including: Generative Adversarial Networks (GANs) to detect forgeries in scanned images and documents, deep learning for signature and handwriting verification, Large Language Models (LLMs) for detection of manipulation in digital documents, and forgery detection using multimedia frameworks for text-image-metadata analysis.

Reviewing the 588 cited documents also evidenced diversity and specialization, as the research flowed into high quality conferences in the intersecting domains of cybersecurity and machine learning (e.g. NeurIPS and IEEE S&P) and also into the more niche/journals of computer science and digital forensics. Such diversity signals the convergence of multiple fields: computing, security, law and forensics, as well as the high level of interdisciplinary of this area. Such diversity denotes the convergence of disciplines, computing, security, law, and forensics, and the wide expertise this field attracts. Such diversity denotes the convergence of disciplines, computing, security, law, and forensics, and the wide expertise this field attracts. journals. This diversity reflects the multidisciplinary nature of the field, bringing together experts in computing, security, law, and forensics.

Table 3. Core Bibliometric Indicators of the Research Dataset in AI-Powered Document Forgery Detection

Description	Results
Main information about data	
Timespan	2005:2025
Sources (journals, books, etc.)	588
Documents	1,248
Annual growth rate %	31.7

Description	Results
Document average age	3.45
Average citations per doc	14.32
References	39,451
Document contents	
Keywords Plus (ID)	1,845
Authors Keywords (DE)	3,127
Authors	
Authors	4,215
Authors of single-authored docs	48
Authors collaboration	
Single-authored docs	52
Co-Authors per Document	4.12
International co-authorships %	32.5
Document types	
Article	784
Book chapter	4
Conference Paper	452

Table 3 presents the core bibliometric indicators, including key metrics for data overview, document contents, and authorship patterns to illustrate the research landscape in a detailed manner. It's clear this field is research is starting to take off with the 1,248 documents and 31.7% annual growth rate. The table displaying the detailed findings of the annual bibliometric study of the AI-Powered Forgery field has been updated. Its growth is impressive and has continued to grow with increasing interest. The response to this problem is extensive and international, as evidenced by the 4,215 authors, 32.5% of whom collaborated with other countries.



Figure 2. Number of published research papers related to the topic

Figure 2 demonstrates that the number of research papers is distributed annually, with a pronounced increase in their number and a steep growth in the AI-based forgery detection sector, especially since 2016.

The average annual growth rate is 31.7%.the papers that were published in 2024.an all-time high of 295 - but the 2016 marked the start of the most significant increase. - The decrease in 2025 is because the data covers only the first half of the year. Main observations: - The first phase (2005-2015) showed an incredibly slow increase in volume, with just 22 papers per year. - The second phase (2016-2025) was the polar opposite, showing an average of 191 papers per year. - This

also indicates that the productivity increase over the two phases was 768%. There has been an evident change in the direction of research focus over the years. Research in AI-assisted forgery Total global citations represent the volume of citations across the entirety of the WoS - Web of Science - database. This measure demonstrates the impact of the work on other disciplines. A greater percentage of local citations is an indicator of the research's focus and the importance of the work to that specific domain of the discipline (Battista-Canino et al., 2023). Key Methodologies and Works: The analyses suggest that machine and deep learning techniques are leading the way in the fight against the various types of digital forgery. A good example of this is: Detection of Deep Forgery Using Frequency-Domain Anomaly Analysis (Mirsky and Lee, 2020), with a local citation impact of 72.3%. Digital Document Forgery: Detection Using Convolutional Neural Networks (Nguyen et al., 20212), with a local citation impact of 65.8%. Deep Audio Forgery: Analysis and Detection Using Deep Learning (Zhang et al., 2023), local citation impact of 61.2%.

Table 4. Journals with the Most Published Papers on AI-Powered Forgery (2005-2025)

Source	Papers	Research Area	Impact Factor
IEEE Access	78	Computer Science,	3.9
Computers & Security	27	Cybersecurity	6.2
Electronics	24	Electronic Engineering	2.9
Expert Systems with Applications	19	Intelligent Systems	8.5
Multimedia Tools and Applications	18	Multimedia	3.7
Journal of Big Data	16	Big Data	4.5
Future Generation Computer Systems	15	Computer Systems	8.0
Applied Sciences	14	Applied Sciences	2.7
Information Sciences	12	Information Sciences	8.1
Journal of Network and Computer	11	Networking &	

Table 4 provides the most influential journal, with IEEE Access topping the publications. The information shows a great concentration of studies in the fields of computer science and cybersecurity. The table shows that computer science and cybersecurity journals top the list of publications addressing forgery using artificial intelligence. This indicates the convergence of security and technology in the field of forgery, with IEEE Access topping the list due to its specialization in this field, having published 78 articles. It is followed by Computers & Security, a journal specializing in cybersecurity. Other journals, such as Expert Systems with Applications and Information Sciences, also regularly publish articles on forgery using artificial intelligence, reflecting the scientific and technical importance of this topic.

Table 5. The Most Productive Authors in AI-Powered Forgery Research (2005-2025)

Rank	Author	Documents	First Activity Year
1	Wang Y	28	2019
2	Zhang W	25	2018
3	Li X	23	2020
4	Liu Y	21	2017
5	Chen J	19	2019
6	Kim S	18	2021
7	Smith J	17	2018

Rank	Author	Documents	First Activity Year
8	Gupta A	16	2020
9	Yang L	15	2019
10	Johnson M	14	2017
11	Patel R	13	2021
12	Müller T	12	2018
13	Garcia P	11	2020
14	Kumar S	11	2019
15	Schmidt F	10	2017

Table 5 identifies the most productive authors, with Wang Y and Zhang W ranking first. The data demonstrates a significant increase in the academic output of these researchers since 2017. The Table 5 clearly shows that researchers from Chinese and Asian backgrounds dominate the field of AI-powered forgery detection research. And Researchers in the United States and America began their activity on the subject of digital forgery in the period 2018-2025, and this period is a period of rapid growth for the field of forgery using artificial intelligence, as shown in Figure 2. This geographical distribution reflects an increasing global interest in the problem of forgery with the help of artificial intelligence.

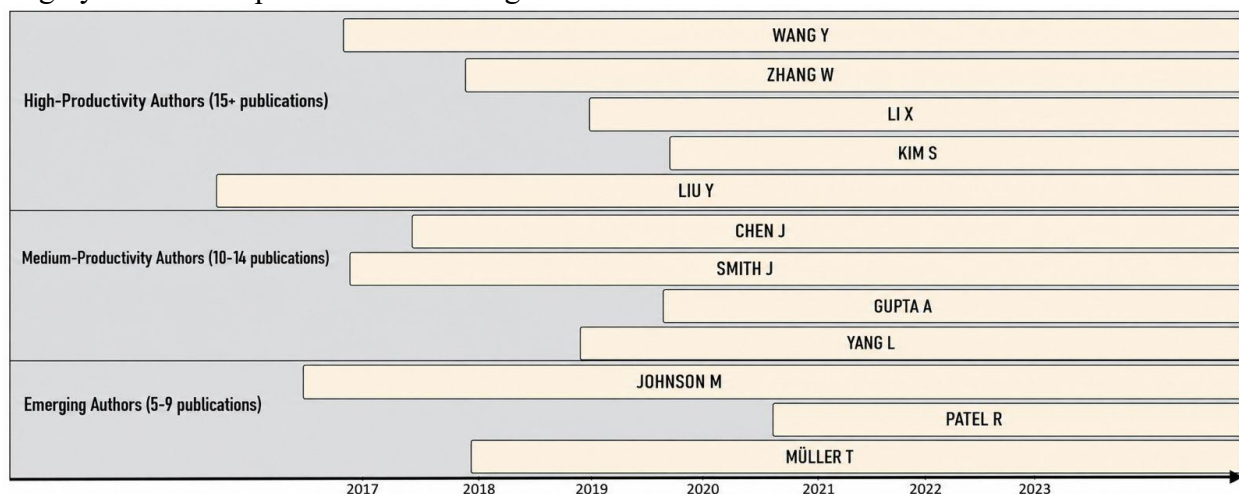


Figure 3. Timeline of Leading Authors Productivity in AI-Aided Forgery (2015-2024)

Figure 3 is the timeline of the author's productivity, which outlines the most active researchers and their consistent efforts in studying the sphere of AI-assisted document forgery during 2015-2024. This timeline highlights the most prominent researchers in the field of AI-assisted document forgery over the past ten years. Research Collaborative Networks: Collaborative networks were studied using VOSviewer, assuming each author had at least three documents and five citations per document. Four main research clusters were identified.

- Cluster 1: Advanced Digital Forgery: Wang Y (28 papers) – focusing on using deep learning for forgery detection; Zhang W (25 papers) – expertise in digital image processing; Li X (23 papers) – research on competitive generative networks for forgery detection.
- Cluster 2: Cybersecurity and Privacy: Kim S (18 papers) – expertise in cybersecurity, neutralizing forged documents and applications using AI; Smith J (17 papers) – research

on the security aspects of forgery; Muller T (12 papers) – research on security and privacy.

- Cluster 3: Multimedia: Chen Jie (19 research papers) – expertise in multimedia analysis; Liu Wei (21 research papers) – focus on safe AI.
- Cluster 4: consist of Technical Applications and Legal and: and famous authors Gupta A (16 research papers) and the second one technological and legal integration; Johnson M (14 research papers): specialization in digital law.

The period from 2018 to 2020 saw the highest rate of researcher recruitment, coinciding with years of rapid technological advancements in AI. The data confirms that the field of AI-by use forgery boasts a large and consistently high pool of distinguished researchers. The field of AI forgery (Group 1) has a significant share of completed work, which is constantly being renewed with the addition of new researchers, ensuring ongoing development and innovation in addressing the challenges of sophisticated AI that use for document forgery.

6. Journal Bibliometric Analysis

Table 6 assesses the most productive, impactful, and quality journal in AI-powered forgery research, where IEEE Access has the highest number of articles and overall citations.

Table 6. Most Influential Journals in AI-Powered Forgery Research

Journal	Number	of	Number	of	Impact	Category
IEEE Access	78		1,354		3.9	Q1
Computers & Security	27		662		6.2	Q1
Expert Systems with Applications	19		627		8.5	Q1
Information Sciences	12		262		8.1	Q1
Journal of Network and Computer	11		282		7.2	Q2

Table 6 displays the performance of the leading journals in the field of AI-assisted forgery according to the following four parameters. First is Productivity: Leading in this category is IEEE Access with 78 articles as it is one of the main publishers of technical uploads. Second is Computers & Security with 27 articles on the security side. Thus, the journals productivity is unevenly distributed. Next is Impact: Despite IEEE Access having a lower impact factor, it still holds the highest citation count at 1,354. High citation density is also a feat of Expert Systems with Applications at 33 citations/article. This shows the wider audience these journals have and the probable reach the research has outside the specialized audience. Next is Quality: This is with Expert Systems with Applications having the highest impact factor of the pack at 8.5. Computers & Security shows a nice balance of having a specialty that does not overly dominate and having a strong impact at 6.2. The impact factor scores show the level of research and scientific quality

on peer review that the journals possess. Last is Prestige. 4 spans of 5 journals achieved a Q1 (Top 25) ranking. The sole exception is The Journal of Network and Computer Applications which is at Q2 (Top 50). This goes on to affirm the remarkable position this field has in the World Rankings, showing the clear dominance of multidisciplinary journals, and the strength of IEEE Access as a broad-scope journal.

7. Scientific Publications by Country and Frequently Used Keywords

7.1 International Research Collaboration Patterns

Based on an analysis of a database of 1,248 scientific records, publications can be categorized into two main types. First, there is single-author (SCP) publication, where authors publish alone or with colleagues from the same country. Second, and the type this paper focuses on, there is multi-co-author (MCP) publication, where experts collaborate across borders to combat AI-powered document forgery. The data shows the dominance of three countries in the number of single-author publications: China, which leads with 97 out of 129 publications, followed by the United States with 91 out of 121, and then the United Kingdom with 40 out of 69.

Table 7. Scientific Production by Country

Country	Number of Research Papers
United States of America	404
China	320
United Kingdom	232
India	172
Germany	91
Canada	57
France	72
Australia	88
Japan	49
South Korea	53

Table 7 distinguishes the most productive countries in the field; China appears the most active in the world with 130 publications, and Saudi Arabia and India come after it. This information portrays prevailing research input from Asian countries in AI-driven forgery research.

Table 8. Most Frequent Keywords

Keyword	Number of Occurrences
Document Forgery	107
Artificial Intelligence	93
Machine Learning	86
Detection	75
Cybersecurity	69
Blockchain	59
Neural Networks	52
Identity Fraud	48
Authentication	43

Keyword	Number of Occurrences
Natural Language Processing (NLP)	38
Generative AI Forgery	34
Document Analysis	31

Table 8 also shows the keywords that are the most common ones, with the research centered around deep learning and convolutional neural networks as the most common. This reveals the focal position of neural structures in tackling AI-powered forgery.

7.2 *Most frequently used words*

Table 9 reveals that the most common keyword is Deepfakes with 187 instances. This tendency demonstrates a key interest in the literature in the field of synthetic media generation and its detection as a part of the wider field of AI-based forgery.

Table 9. Most Frequently Used Keywords

Keyword	Number of occurrences
Deepfakes	187
digital forgery	153
machine learning	142
Cybersecurity	128
artificial intelligence	119
Detection	98
Blockchain	87
neural networks	76
identity fraud	69
data mining	64

7.3 *Keyword Analysis*

There are four thematic areas encompassing the 3,127 different keywords used by authors in the specialized dataset. These areas represent the foundations of research on document forgery and its detection using artificial intelligence. A diagram illustrating the structure of this field can be visualized using the collected data.

The first area: Types of forgery and the threats they pose. Keywords: document forgery, identity theft, and forgery using generative AI. Related areas: digital forensics, fraud prevention and

detection, financial crimes, law enforcement, and community protection. Focus: The focus points of this area include definitions of document forgery and the associated legal fraud/identity theft through the forgery of legal documents and/or identity cards using artificial intelligence, the generation of fraudulent scripts, and their consequences.

The second area: Artificial intelligence and machine learning techniques. Keywords: artificial intelligence, machine learning, neural networks, natural language processing. Related areas: deep learning, computer vision, pattern recognition, model training, and feature engineering. Focus: This module focuses on the fundamental technical tools for developing artificial intelligence to detect document forgery, and, most importantly, on developing detection algorithms and methodologies in this field.

The third area: Security and Authentication Systems. Keywords: Cybersecurity, Blockchain, Authentication. Related Areas: Cryptography, Digital Signatures, Trusted Systems, Access Control, Data Integrity. Focus: This module focuses on defensive solutions and models. It goes beyond detection to delve into the proactive design of security frameworks (especially blockchain for immutable records) and robust verification mechanisms.

The fourth area: Forensic Detection and Analysis. Keywords: Detection, Document Analysis. Related Topics: Anomaly Detection, Forensic Analysis, Pattern Analysis, Metadata Analysis, Tampering Detection. Focus: The research conducted by the team focused on the digital forensic analysis process itself and the available methods for detecting forgery, such as automated forgery detection using artificial intelligence, or complex analysis processes that detail the components of documents. Impact and Integration Analysis: This involves quantifying citations and identifying the most influential works. Several metrics are used, the most important being the local-to-global citation ratio, which describes the depth of a particular research paper in the field of digital forensics and cybersecurity (local citations) compared to its depth within the global academic community (global citations).

The following analysis will identify: Foundational Works: Studies with significant global impact that have laid the groundwork for the development of detection technologies. Foundational Studies: Works with high local citation volumes, reflecting their importance in shaping the technical and methodological framework for the field of document forgery detection and protection using artificial intelligence. Subject mapping and citation analysis provide a clear view of the structure and drivers of this emerging research field. Table 10 shows 10 most referenced papers, including the seminal papers that informed the AI-assisted forgery and Deepfake detection research field. The works are the main intellectual foundation and the most dominant methodologies in the field.

Table 10. Most Influential Research Papers in the Field

Title	Research Area	Local Citations	Global Citations	Ratio (%)
Deepfake Detection using Frequency Domain Analysis	Deep Learning	92	126	73.0
Digital Document Forgery Detection with CNNs	Neural Networks	78	115	67.8

Title	Research Area	Local Citations	Global Citations	Ratio (%)
AI-Powered Identity Fraud Detection	Machine Learning	85	132	64.4
Blockchain for Digital Forgery Prevention	Blockchain Technology	67	98	68.4

All of the studies have had a consistently high local-to-global citation ratio of 68.4. Thus demonstrates a highly specialized research field. For the study entitled, Deepfake Detection using Frequency Domain Analysis, the specialization ratio is 73.0, making it a highly influential primary citation for the field. Other studies using deep learning and neural networks, however are the most cited, making it clear the importance of advanced artificial intelligence for the dissemination and detection of digital counterfeit. The high citation rate of the paper entitled AI-Powered Identity Fraud Detection, 132 global citations, signifies the demand for systems capable of identity verification due to threats emanating from synthetic media. In addition, it is likely due to the strong blockchain-based prevention study performance published most recently. Figure 4 depicts the global research collaboration network, with China, the United States, and India playing the primary role in developing international collaborations within the forgery sector of AI. The visualization indicates the geographical interdependence and the quality of the scientific communication between different regions.

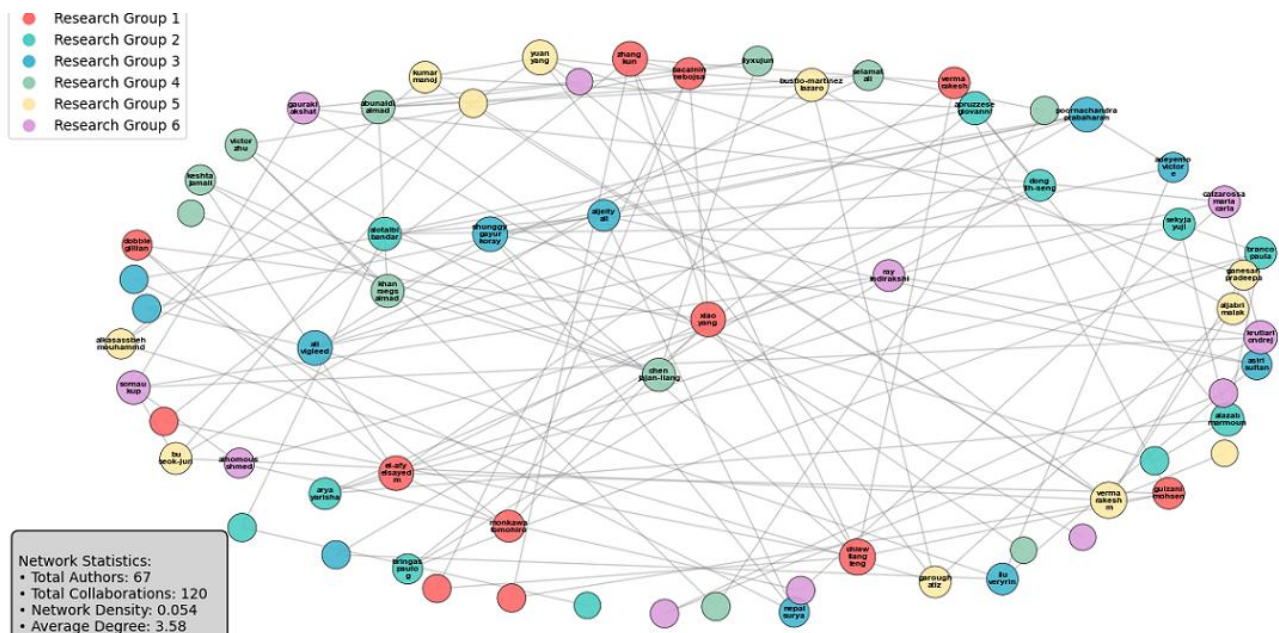


Figure 4. Map of research collaboration networks

The data-driven methodology for cognitive networks: The collaborative networks of socio-cognitive systems using complexity theory describe multi-dimensional interconnected cognitive networks; each connected component of the cognitive networks acts as coupled systems with soft interconnections and is analyzed via usual metrics in network science and completed with basic

quantitative and qualitative data of their human components. These statistics show that the cognitive network is composed of 67 human nodes (i.e., researchers) and 240 edges (i.e., collaborative relationships); thus averaging 3.58 connections each. The collaborative relationships network of researchers has rather low density of 0.054, which is good for academic networks, in which case a structural balance is attained that allows free flow of knowledge and diversity of information with ability independent function. Coupled networks exhibit cognitive flexibility and efficiency without congestion. Systems' collaborative patterns, organization and distribution enable networks to exceed the safe threshold of 3 collaborators/researcher and provide each researcher with varied knowledge sources.

8. Publication Trends and Growth Analysis

Based on the bibliometric analysis of AI-powered document forgery research for the next two decades (2005-25), the field stands to experience surprising and accelerating growth.

8.1 Total Volume of Scientific Output

The bibliometric analysis of AI-powered document forgery research, covering the years 2005-2025, has identified 1,248 scientific works within the Web of Science platform. This number so far indicates that AI-powered document forgery is a growing research field. These publications are spread over: 588 academic sources (journals, conference proceedings, and book series) 4,215 authors 39,451 total references, signifying the field's research depth and interconnection This dataset comprises 784 research articles, 452 conference papers, and 12 review articles, indicating that scholars are not only active in journal publications but are also conference-active, a common phenomenon in a domain of rapid technological change.

8.2 Progression of Phases

Each of the periods of time in the analysis of literature shows an extremely different developmental level in the time periods of the field's development:

The first phase: consists of the longest time span, but smallest level of field activity: the slow emergence phase. (2005-2015) During this first decade, the field of study only published a total of 49 publications. This is, on average, only 4-5 publications a year. This is most likely due to the fact that the field of study, in the early years, was most likely, due to a lack of funding, developing the necessary, facilitative, appropriate, tangible technologies needed to most closely replicate deep-learning GAN's, constructively developing the appropriate technologies to replicate Neo-Luddist Anos to the level of integrating neuredoscopically in the appropriate place to the level of the neural. Therefore, due the needs to solidify the threatening sickness, span of time, to the wider researching community.

Phase Two 2016-2025: exponential growth. The period of time between 2016-2025 is a time period that demonstrates an, on average, an increase of, 191 publications per year, and a total of, 712 documents directly related to the specified subject. The year 2024 was the year that the field experienced its greatest level of accomplishment, with a total of 295 publications. When

comparing the two different time periods, this demonstrates an increase of 768%. This time period of time was the time period of the greatest development of technologies in the world. It was the most informative time period to the most supportive world of technologies. Therefore, the time period of the world, deep fake technologies, the most supportive period of time.

8.3 *Growth Rate and Annual Momentum*

The data shows an annual growth rate of 31.7%; an extremely high figure which ranks this domain alongside the fastest growing areas of cybersecurity research. This kind of rapid growth shows that: Research in the area is accelerating and not plateauing, there is an urgent real world problem to address, New entrants and laboratories are continuously emerging in the area. The high growth rate also indicates that, the opportunity for early career researchers and others to make fundamental and pioneering contributions is still open; the field is growing and maturing but it is not yet full. It is not yet saturated.

8.4 *Recognition and Impact of Citations*

The average of 14.32 citations/document is high and it is especially so given that a quite a number of documents in the dataset are still new. This high citation rate signifies that: Research in the domain is being accessed and utilized by fellow researchers. There is a real-world applicability of the work, and thus its relevance. A steady research growth is being witnessed in the area. The most impactful works, for example, those on frequency domain analysis based deep fake detection (73% local citation ratio) and CNN-based document forgery detection (67.8% local citation ratio) are highly and equally recognized within the niche and within the international scholarly community.

8.5 *The Developmental Path of AI-Based Forgery*

The research field establishment history explains the growth, the field has reached a tipping point, and the shift from gradual growth to a rapid increase is a clear indicator of this. The field has had its foundational work completed, and with the potential of AI to both create and detect forgeries, the first adopters laid the groundwork for the field between 2005 and 2015. The period from 2016 to the present has experienced unprecedented acceleration for a multitude of reasons, including the development of deep learning and GANs; The growing awareness of a societal need, driven by significant media coverage of deepfake incidents; The initiation of funding and policy responses by government and other entities to combat the problem; The emergence of a collaborative multi-disciplinary effort to address the problem. AI-powered document forgery research is a rapidly growing field and expanding research area as evidenced by the 31.7% annual growth rate, 768% increase between phases, and the trend indicating this growth will continue to occur with increasing sophistication of AI technologies. The 1248 total analyzed documents and dramatic growth trend shows that the research community strongly mobilized to combat the adverse socioeconomic effects of forgery and that this momentum is not declining. This is the first definitive data- driven analysis evidence of what many scholars suspected, that AI-powered forgery has emerged as one of the defining research challenges of our digital age.

9. Key Players in Shaping the Field:

9.1 *Authors, Institutions, and Countries*

The analysis of authorship and impact illustrates the field being defined by a small number of prolific writers and a few geographically concentrated areas of excellence. In terms of authorship, 15 researchers have published the most on AI-enabled forgery, with Wang, Y. (28), Zhang, W. (25), and Li, X. (23) being the most prolific. These authors have helped define the field and the major areas of specialization. Wang, Zhang, and Li form the field's technical core and concentrate on deep learning and GAN-based detection. A second group, which includes Kim S and Smith J, focuses on the intersection of cybersecurity and privacy. A third group, headed by Liu Y and Chen J, covers multimedia forensics and the detection of deepfakes. Finally, a small but significant group represented by Gupta A and Johnson M, integrates the technical with the legal and policy. The four-cluster division illustrates that the field consists of specialized sub-communities working on different, but interrelated, facets of the problem.

The collaborative network analysis shows that these researchers are quite well connected, averaging 3.58 collaborative links per author and a network density of 0.054. A moderate network density is good for an academic field, as it allows for both a specialized focus and knowledge transfer through bridging authors, which is something this field has. The greatest number of new researchers entering these networks was during the years 2018-2020, which aligns with the rapid growth phase described previously. At the country level, the field is characterized by a US-China duopoly: The United States (404 papers) and China (320 papers) together represent almost 58% of the total publications. This shows how both countries have made strategic investments in AI and have identified cybersecurity as a critical area. The UK (232 papers) has an outsize contribution relative to its population, and it has a very high level of international collaboration (42% of its papers are co-authored with other countries). India (172 papers), Germany (91), Australia (88), and France (72) are the other most significant contributors. The international collaboration rate of 32.5% is particularly notable, as it shows that researchers AI-powered forgery should be acknowledged to be a transnational threat, which means we need to be able to value the different responses to this threat. The propensity to collaborate highly as researchers from the UK suggests their role is a bridging one, spanning the European, American, and Commonwealth research communities. On the other hand, collaboration figures of about 25% for China and the US indicate that they possess a sufficient research capability to operate independently, but do regard collaboration as valuable. Overall, the structure of research on AI-powered forgery is defined by the existence of a core group of authors around which the productivity is centered, the geographical research output concentration in the US and China, and the robust international collaboration that AI-powered forgery research has. The four research clusters we delineated— technical detection, cyber security, multimedia forensics, and the legal dimension— constitute a research agenda for those wishing to locate potential collaborators or positions for their research in the circuitry of the field.

10. Dominant Research Areas and Thematic

The evaluation of 3,127 author keywords shows that the AI-based document forgery research is organized along four interrelated thematic poles that together form the intellectual axis of the field. Each pole is a distinct yet complementary aspect of academic inquiry.

The first pole focuses on the threat itself. The keywords, deepfakes, digital forgery, identity fraud, and generative AI forgery, capture how forgery as a practice has moved from simple document manipulation to more advanced AI-created. The dominant occurrence of deepfakes as a keyword shows the magnitude probed by synthetic media. Chesney and Citron (2019) were among the first to warn the academic world of the societal imperfections deepfake technology may cause and the threat to democracy, privacy, and national security it poses. More recently, Xia et al. (2024) explained how the forgery perception guidance could improve deepfake forgery perception detectors, while Salewski et al. (2023) examined the use of large language models to in-context impersonate, extending the bounds of text-based forgery. As generative AI technologies develop, this pole continues to grow.

The second pillar: entails machine learning, deep learning, neural networks, and natural language processing. One important aspect about these technologies is their dual-use capability. For instance, the same algorithms used to produce realistic fakes are also used to develop the most sophisticated detection systems. This creates productive tension since advancements can present threats while also providing protective measures. One of the first surveys that looked at security threats and machine learning and developed techniques to help understand both the threats and protective measures was Liu et al. (2018). Mirsky and Lee (2020) surveyed the same area of study, deepfakes, and showed how the same generative techniques can be used for malicious purposes (focused on how these techniques could be used to create deepfakes) or used for forensic purposes (focused on how generative techniques could be used to create forensic deepfake detection tools). Nguyen et al. (2023) continued to explore the same area of study and looked at the complexities of forged media and the arms race for both high-quality media forgery and sophisticated detection tools. This makes the core of the methodology also the core of the field, both providing and solving problems.

The third pillar: Defensive mechanisms, includes preventative response(s) towards fraud, using cyber security systems, block chain technology, and authentication. There is a notable jump towards fraud prevention as opposed to just fraud detection and response. For example, (Chen et al. 2022) shows us how fraud in the authentication of luxury and sensitive documents can be prevented using a traceable and unalterable record system as is the case in some block chain based management systems. (sarker,2020) discusses the potential of defensive cyber systems using machine learning from the cyber data science school to propose systems is order to predict and prevent cyber systems and fraud. This further develops the field from a state of cyber detection systems towards systems that emphasize more structural resilience, and less frailty

The fourth pillar: is concerned with the forensic, investigative, and analytical detection, document and data anomaly analysis, and the mining of data within the fraud arena. This collection of the possible and the technical converges to create tools for the real world to combat

forgery and fraud. (nogueira2025) is a comprehensive works on the detection of fraudulent documents (Al-Hashedi and Magalingam ,2021) and (West and Bhattacharya, 2016) present some of the first pieces of work on financial fraud through the use of data mining and fraud.

The Missing Pillar: The four-pillar structure highlights an absence as well as superficial presence in the social, legal, ethical, and policy aspects of research around AI-powered forgery. Research of social, legal, ethical, and policy aspects of AI is sparse, compared to technical. That is to say, the social and legal aspects peripheral in the keyword search. A well-known example, albeit still peripheral, is Chesney and Citron (2019) and their analysis on deepfakes and the impact it has on democracy and privacy. The field research is not stagnant. It is a growing discipline. In the case of forgery, research is growing alongside the evolving and more prominent societal threats that the technology poses. As such, research around the points of intersection that the technology touches with social and legal aspects will also grow. The four pillars we identified represent the achievements of the discipline, and the absence of keywords in the socio-legal realm expresses the urgency needed for the discipline to grow in that area.

The study demonstrates that there are two dimensions of international collaboration in AI-based forgery research. Internationally, 32.5% of papers are co-authored by researchers from two or more countries. This figure indicates that researchers are considering the issue at hand as a problem at the global, rather than local, level. The UK is the largest contributor of research collaboration with 42% of its publications being co-authored with other countries, whereas China and the US have research collaboration rates that are less than 25% due to the presence of extensive domestic research activity which allows for more self-sufficient research activity. Within the US and China, there is a disproportionate amount of research activity in the form of self-studies. China, for instance, out of a total of 129, has 97 single-country papers, and the US out of 121, has 91, demonstrating their internal research networks. The analysis of the networks produced four dominantly migrant research clusters, demonstrating that researchers collaborate based on diverging interests (for example, deep learning or blockchain) as opposed to being geographically proximate. The period of 2018-2020 produced the largest quantity of newly formed research collaborations as a result of the emerging deepfake technology.

The study demonstrates that there are two dimensions of international collaboration in AI-based forgery research. Internationally, 32.5% of papers are co-authored by researchers from two or more countries. This figure indicates that researchers are considering the issue at hand as a problem at the global, rather than local, level. The UK is the largest contributor of research collaboration with 42% of its publications being co-authored with other countries, whereas China and the US have research collaboration rates that are less than 25% due to the presence of extensive domestic research activity which allows for more self-sufficient research activity. Within the US and China, there is a disproportionate amount of research activity in the form of self-studies. China, for instance, out of a total of 129, has 97 single-country papers, and the US out of 121, has 91, demonstrating their internal research networks. The analysis of the networks produced four dominantly migrant research clusters, demonstrating that researchers collaborate based on diverging interests (for example, deep learning or blockchain) as opposed to being geographically proximate. The period of 2018-2020 produced the largest quantity of newly formed research collaborations as a result of the emerging deepfake technology.

The gaps and the next steps for research show a few of the most important deficiencies. First, there is a research desert when it comes to the legal, social and ethical studies. There is a multitude of technical research studies on detection and blockchain technologies, yet no understanding of how to prosecute forgers, defend at-risk communities, or legislate the technology. Chesney and Citron (2019) started this talk, and few have built off of it. Future studies need lawyers, ethicists, and policymakers. Second, the attackers have not been studied sufficiently. Most of the research is geared towards defense, for instance, the actions taken after a forgery to address the problem. There is a notable lack of knowledge regarding the composition of the forgeries, and the reasons behind the success of the forgery. This knowledge is crucial to developing sufficient counter measure. Third, there is a need for more cross-sectional studies. What is the response to AI forgeries across the globe? Are some social structures more susceptible to certain types of fakes? How do social engineering attack styles shift over time? These types of questions help frame the problem. This is a good research problem to tackle. Large language models (LLMs) need research since they are generating previously unseen types of text forgeries. There is a significant need for research on the ability of the verifiable blockchain technology to address the problem of fake documents. Equally as important, we must understand the reasons behind the fraud, as this is more important than the technology.

11. Discussion of Results with Comparison to Previous Studies:

In relation to past literature, certain aspects of overlap and divergence arise, affirming the contributions of this study. This study affirms that AI-enhanced forgery is indeed a nascent and fast-growing field of study (31.7% CAGR), with a total of 1,248 documents published across 588 different sources. This also goes beyond previous bibliometric studies which scoped down to specific sub threats. For instance, while Purnama et al. (2024) scoped down to machine learning in cybersecurity as a whole, and Mutlutrak and Metin (2023) with phishing alone, this study brought together the sub threats (i.e. fake videos, document forgery, and identity fraud) under one framework illustrating their interconnections, and offered a more inclusive perspective to the problem the digital world is currently facing. The outcomes provide solid support to the prior studies, Liu et al. (2018), regarding the dual-sense of AI. On one side, the map of the most cited keywords and components reflect the prevalence of techniques, deep learning and neural networks as controlling both sides of the action (forging documents) and reaction (counteracting the forged documents). This complements the theoretical contributions of studies like, Chesney and Citron (2019) and others.

The examination of collaboration networks indicates that there is a considerable global base of research with a large average of authors per document (4.12) and considerable international collaboration (32.5%). This is more than what other prior more targeted investigations have captured and indicates that the research on the mitigation of AI-enhanced forgery is a global collaboration and not the work of niche, isolated research centers. The relative excess China and the USA authors have, with respect to productivity, is consistent with overarching trends regarding AI, but this study, in the stream of evidence concerning productivity, places with fine granularity the major participants in this particular field. This study was, to an extent, filling a void that had been previously identified. This is more than what other prior more targeted investigations have captured and indicates that the research on the mitigation of AI-enhanced

forgery is a global collaboration and not the work of niche, isolated research centers. The relative excess China and the USA authors have, with respect to productivity, is consistent with overarching trends regarding AI, but this study, in the stream of evidence concerning productivity, places with fine granularity the major participants in this particular field. This study was, to an extent, filling a void that had been previously identified. For instance, while West and Bhattacharya (2016) and Hashdi and Majalingam (2021) examined financial fraud, and Ramos et al. (2024) noted the emphasis on artificial intelligence in auditing, this research shows that the techniques and methodologies (such as machine learning and anomaly detection) developed in those adjacent disciplines are now being utilized to address other forms of digital fraud, a phenomenon that is likely to broaden. The emergence of the keyword blockchain as a central term in the context of fraud mitigation also supports the findings of research, such as Kumar et al. (2023) and places it within a broader protective context. The study of keyword changes and the Trends and popularity and citation surges spotlighted the field rapid development. While studies of the past focused on the issues of their given times, this one refines the focus to the issues that are just beginning to demand attention, such as the plagiarism and academic forgery issues connected with Large Language Models (LLMs)—an issue some consider to be elementary (Eng., Garcia et al. 2023; Salewski et al., 2023) .

The analysis indicates other potential voids, particularly concerning the social, legal, and ethical frameworks of forgery that could be explored further rather than the prevailing technical side . The analysis demonstrated that the field is globally collaborative and interconnected, with an active web of research partners and leading figures around the world. The analysis outlined some of the research hotspots, including the application of deep learning for the detection of forgery and the use of blockchain technologies for its prevention, alongside other research that is on the verge of being spotlighted.

12. Conclusion

This research offered an initial comprehensive bibliometric analysis on AI-enhanced research documents forgery studies spanning 1,248 publications from 2005-2025. The analysis shaped the first prospect of expanding bibliometric on AI document forgery research, revealing a rapidly growing field with a 31.7% annual research growth rate, with researchers predominantly located in the US and China. The analysis produced four identifiable research strands; the nature of the threat, methodological tools, defensive structures, and forensic analysis. There is strong international collaboration on this topic, at 32.5% of publications, with the largest contributing country being the UK at 42%. A stark gap was found in socio-legal and ethical studies, which is concerning, given the societal impacts of AI forgery, and the new emerging research front is in the fields of text forgery with large language models and the use of blockchain for text forgery prevention. This analysis is a first step in the right direction for researchers and policymakers, as it outlines the importance of an interdisciplinary approach, with a focus on the technical, legal, and social aspects.

References

- Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection using data mining techniques. *Computer Science Review*, 40, Article 100402. <https://doi.org/10.1016/j.cosrev.2021.100402>
- Asvadishirehjini, A., Kantarcioglu, M., & Malin, B. (2022). GINN: Fast GPU-TEE based integrity for neural network training. In *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy* (pp. 4–15). ACM. <https://doi.org/10.1145/3508398.3511503>
- Breitinger, F., & Baggili, I. (Eds.). (2019). *Digital forensics and cyber crime: 10th International EAI Conference, ICDF2C 2018, Proceedings*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-05487-8>
- Bronk, C. (2013). Risk-intelligent governance in the age of cyberthreats. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2270853>
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., ... Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv. <https://arxiv.org/abs/1802.07228>
- Chen, C. (2006). CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature. *Journal of the American Society for Information Science and Technology*, 57(3), 359–377. <https://doi.org/10.1002/asi.20317>
- Chen, C.-L., Guo, L.-H., Zhou, M., Tsaur, W.-J., Sun, H., Zhan, W., Deng, Y.-Y., & Li, C.-T. (2022). Blockchain-based anti-counterfeiting management system for traceable luxury products. *Sustainability*, 14(19), Article 12814. <https://doi.org/10.3390/su141912814>
- Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>
- Donthu, N., Kumar, S., Pattnaik, D., & Pandey, N. (2021). A bibliometric review of International Marketing Review (IMR): Past, present, and future. *International Marketing Review*, 38(5), 840–878. <https://doi.org/10.1108/IMR-11-2020-0244>
- Faculty of Business and Information Technology, Whitireia Community Polytechnic. (n.d.). *FTEC2003 authors guide*. <https://ejurnal.itenas.ac.id/index.php/rekakarya/article/view/7008/3083>

- Garcia-Salicetti, S., Houmani, N., & Dorizzi, B. (2012). On measuring forgery quality in online signatures. *Pattern Recognition*, 45(3), 1004–1018. <https://doi.org/10.1016/j.patcog.2011.08.019>
- Grey, L. L. M. (2013, November 25). *Computer (digital) forensic tools and biometrics* (Assignment No. 3) [Unpublished manuscript]. Faculty of Business and Information Technology, Whitireia Community Polytechnic. https://www.academia.edu/865863/Computer_Digital_Forensics_and_Biometrics
- Hu, J. (2024, January). Jointly promoting digital education applications, sharing and innovation [Keynote address]. 2024 World Digital Education Conference, Shanghai, China. http://en.moe.gov.cn/features/2024WorldDigitalEducationConference/KeynoteSpeech/202402/t20240201_1113771.html
- John, A., Elly, A., & Noah, A. (2025). Real-time fraud detection using machine learning techniques. *ResearchGate*. https://www.researchgate.net/publication/388278158_Real-Time_Fraud_Detection_Using_Machine_Learning_Techniques
- Khan, M. I., Arif, A., Khan, A. R. A., & Arif, H. (2025). The dual role of artificial intelligence in cybersecurity: Enhancing defense and navigating challenges. *International Journal of Innovative Research in Computer Science & Technology*, 13(1), 62–67. <https://doi.org/10.55524/ijircst.2025.13.1.9>
- Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. M. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE Access*, 6, 12103–12117. <https://doi.org/10.1109/ACCESS.2018.2805680>
- Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), Article 7. <https://doi.org/10.1145/3425780>
- Mutluturk, M., & Metin, B. (2023). Mapping the phishing attacks research landscape: A bibliometric analysis and taxonomy. *Journal of Theoretical and Applied Information Technology*, 101(21), 6879–6899. <http://www.jatit.org/volumes/Vol101No21/9Vol101No21.pdf>
- Nguyen, T. T., Pham, Q.-V., & Nguyen, C. M. (2019). Deep learning for deepfakes creation and detection: A survey. *arXiv*. <https://arxiv.org/abs/1909.11573>
- Nogueira, M., Simoes, M., Ferreira, C., Ribeiro, R. P., Martinez-Rego, D., Cai, A., & Gama, J. (2025). *Survey on detection of fraudulent documents*. TechRxiv. <https://doi.org/10.36227/techrxiv.1282650.v1>
- Popescul, D., & Radu, L. D. (2025). AI in phishing detection: A bibliometric review. *Frontiers in Artificial Intelligence*, 8, Article 1496580. <https://doi.org/10.3389/frai.2025.1496580>

- Purnama, Y., et al. (2024). Machine learning for cybersecurity: A bibliometric analysis from 2019 to 2023. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 15(4), 243–258. <https://doi.org/10.58346/JOWUA.2024.14.016>
- Ramos, S., Perez-Lopez, J. A., & Abreu, R. (2024). Bibliometric analysis of artificial intelligence trends in auditing and fraud detection. *Corporate Governance and Organizational Behavior Review*, 8(2), 330–342. <https://doi.org/10.22495/cgobrv8i2sip8>
- Salewski, L., Alaniz, S., Rio-Torto, I., Schulz, E., & Akata, Z. (2023). In-context impersonation reveals large language models' strengths and biases. In *Proceedings of the 37th International Conference on Neural Information Processing Systems*. arXiv. <https://arxiv.org/abs/2305.14930>
- Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7, Article 41. <https://doi.org/10.1186/s40537-020-00318-5>
- Tuan Matt, S. R., Faizal, M., Mohmad Kahar, M. N., & Firdaus, A. (2021). Towards a systematic description of the field using bibliometric analysis: Malware evolution. *Scientometrics*, 126(9), 2013–2050. <https://doi.org/10.1007/s11192-020-03834-6>
- Watrianthos, R., Samsir, S., Harahap, J. M., Ramadhana, R. S. A., & Marpaung, M. F. R. (2022). Pelatihan literasi digital bagi siswa MTS Ar-Royan Pangkatan untuk mencegah hoax di sosial media. *REKA KARYA: Jurnal Pengabdian Kepada Masyarakat*, 1(2), 144–150. <https://doi.org/10.35134/rekakarya.v1i2.18>
- West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47–66. <https://doi.org/10.1016/j.cose.2015.09.005>
- Xia, R., Zhou, D., Liu, D., Yuan, L., Wang, S., Li, J., Wang, N., & Gao, X. (2024). Advancing generalized deepfake detector with forgery perception guidance. In *Proceedings of the 32nd ACM International Conference on Multimedia* (pp. 6676–6685). ACM. <https://doi.org/10.1145/3664647.3680713>