International Journal of Computer Science and Engineering Survey (IJCSES)
Vol.16, No.1/2/3/4/5, October 2025

STEGANOGRAPHY RESEARCH LANDSCAPE: A BRIEF CENTURY-LONG BIBLIOMETRIC STUDY

Eltyeb Elsamani [1] and Yousif Elsamani [2]

[1] CS Department, Faculty of Computer Science and Information Technology, AL-Neelain University, Khartoum, Sudan
[2] Institute for Future Initiatives, The University of Tokyo, Tokyo 113-0033, Japan

ABSTRACT

This study presents a century-long bibliometric review of steganography based on 8,241 articles and 49,572 citation links. Using direct citation analysis, we mapped the field's intellectual landscape and identified nine major clusters, ranging from classical image-based methods and foundational theory to audio, text, reversible, video-based techniques, and emerging AI-driven paradigms such as deep learning and GANs. Temporal mapping reveals a shift from foundational principles to AI-enabled and quantum-informed approaches, while geographic analysis highlights China's leading role, followed by India and the United States. The review also identifies critical gaps in unified security frameworks, evaluation metrics, and human factors, and outlines future opportunities in quantum steganography, blockchain, coverless methods, and application-driven domains.

KEYWORDS

Steganography, Systematic Review, Citation Network, Bibliometrics, Research Landscape

1. INTRODUCTION

Steganography, derived from the Greek words "steganos" (covered) and "graphein" (writing), represents the art and science of concealing information within seemingly innocuous carriers in a manner that masks the very existence of the hidden communication [1]. Unlike cryptography, which encrypts messages to make them unintelligible but visible, steganography aims to hide the presence of secret communication entirely [2]. This fundamental distinction positions steganography as a critical component in the broader landscape of information security, offering complementary protection that addresses the vulnerability of encrypted communications to detection and targeted attacks [3].

The practice of steganography has evolved dramatically from its ancient origins—where messages were hidden using invisible inks, concealed within wax tablets, or tattooed on shaved heads of messengers—to sophisticated digital techniques that exploit the characteristics of modern media formats [1], [4]. Contemporary steganographic methods predominantly utilize digital carriers such as images, audio files, video sequences, and text documents, with digital images emerging as the most popular medium due to their ubiquity, high redundancy, and the human visual system's limited sensitivity to subtle changes in pixel values [5].

Digital image steganography encompasses diverse approaches, including spatial domain techniques that directly modify pixel values (such as least significant bit substitution and pixel-value differencing), transform domain methods that embed data in frequency coefficients (DCT, DWT, or SVD), and adaptive techniques that adjust embedding strategies based on image

DOI: 10.5121/ijcses.2025.16525

characteristics [3], [6]. The evolution of these methods reflects an ongoing tension between three fundamental objectives: imperceptibility (ensuring visual quality remains uncompromised), capacity (maximizing the amount of hidden data), and security (resisting detection by steganalysis tools) [1]. This "steganographic triangle" represents an inherent trade-off, as optimizing for one objective typically comes at the expense of others [7].

The applications of steganography extend across numerous domains, from secure communication and copyright protection to medical data privacy and military intelligence [8]. In healthcare, steganographic techniques safeguard sensitive patient information by embedding it within medical images, preserving both data confidentiality and the diagnostic value of the images [9]. In digital rights management, steganography enables copyright protection through imperceptible watermarking that can later verify content ownership [10], [11]. The financial sector employs steganographic methods to enhance document security, while intelligence agencies utilize these techniques for covert communication [2].

However, the dual-use nature of steganography presents significant challenges. The same technologies that enable legitimate privacy protection can potentially facilitate illicit activities, including unauthorized data exfiltration and covert communication by malicious actors [1]. This duality has intensified research interest in both steganography and steganalysis—the counterpart science focused on detecting hidden communications—creating an evolutionary arms race that continues to drive innovation in both fields [4].

Recent technological advancements have dramatically transformed the steganography landscape. The integration of artificial intelligence, particularly deep learning and generative adversarial networks (GANs), has revolutionized both embedding techniques and detection methods [11]. Quantum steganography has emerged as a frontier domain, leveraging quantum information principles to establish fundamentally new approaches to information hiding [12]. Meanwhile, the concept of coverless steganography represents a paradigm shift by establishing mappings between secret messages and inherent features of existing media without actual modification [3].

Despite steganography’s long history and growing significance in contemporary data security, several important gaps hinder a comprehensive understanding and future advancement of the field. Most notably, steganography research currently lacks a thorough bibliometric analysis that clearly delineates its intellectual structure, major research clusters, and their historical progression over the past century. While previous surveys have focused on specific aspects or limited periods [1], [4], [5], they have not fully captured the extensive evolution and thematic connections within the discipline [3]. The fragmentation of steganographic research across diverse domains, including image processing, information theory, artificial intelligence, and quantum computing, has resulted in siloed communities with limited cross-domain integration [11]. This fragmentation complicates efforts to establish unified theoretical frameworks and standardized performance benchmarks, thereby creating inconsistencies in evaluation methodologies across different studies [6]. Additionally, the rapid advancement in machine learning-based steganalysis methods has created an urgent demand for more robust and fundamentally undetectable steganographic techniques [13], [14]. Furthermore, systematic assessments of current steganographic approaches remain sparse, limiting the identification of their strengths and weaknesses [15]. Lastly, the field has not adequately explored geographical and institutional patterns of contribution, despite their significance in understanding global research trends and collaborative dynamics.

To address these challenges, this study undertakes a comprehensive bibliometric review of steganography research spanning a century, carefully tracing the evolution of its primary thematic areas and methodological approaches. Utilizing direct citation analysis, this research maps the intellectual landscape, identifies key clusters, examines their temporal development, and clarifies interconnections among different thematic areas. It further investigates the progression of steganographic methods from early historical techniques to contemporary, sophisticated approaches. Additionally, the study evaluates institutional and geographical contributions, highlighting significant research hubs. By identifying critical research gaps, the study proposes specific areas for further investigation and outlines promising directions for future research. Ultimately, this analysis aims to serve as a valuable resource for new researchers by providing accurate and up-to-date insights into the prevailing methodologies, central challenges, and state-of-the-art advancements in steganography. By offering a unified and integrated perspective, the study intends to guide targeted and impactful future research efforts.

The rest of this paper is organized as follows. Section 2 reviews the literature and introduces our conceptual framework. Section 3 details the data and methods. Section 4 presents the results of the bibliometric analysis. Section 5 discusses key findings. Section 6 concludes with implications, and Section 7 outlines future research directions.

2. LITERATURE REVIEW

The field of steganography has witnessed substantial scholarly attention, with numerous review studies and analyses examining its various aspects. This section provides a critical examination of previous literature review studies and bibliometric analyses in steganography research, establishing the foundation and context for our comprehensive century-spanning review. Additionally, we propose a novel conceptual framework that integrates multiple dimensions of steganography research to guide our analysis.

2.1. Past Literature Review Studies on Steganography

Literature reviews in steganography have evolved significantly over time, reflecting the field's expanding scope and increasing sophistication. Cheddad et al. [1] provided one of the most influential surveys on digital image steganography, analyzing various methods while establishing evaluation criteria focused on undetectability, robustness, and capacity. Their framework helped standardize comparisons but was limited by its emphasis on image-based methods, leaving other media largely unexplored. Building on this foundation, Mandal et al. [4] conducted a more comprehensive survey of spatial and transform domain techniques, emphasizing security considerations. However, their analysis primarily catalogued approaches and offered little critique of methodological weaknesses or evaluation inconsistencies.

As the field diversified, specialized reviews addressed narrower areas. Hussain et al. [5] examined spatial domain techniques in detail, tracing progress from simple LSB substitution to adaptive methods that incorporate human visual system properties. Yet their review lacked discussion of scalability and cross-domain applicability. Similarly, Singh et al. [2] provided a broad overview across carriers, but their synthesis did not adequately assess comparative performance across modalities, limiting its utility in identifying research priorities.

The integration of artificial intelligence into steganography prompted reviews that tracked this technological convergence. Singh et al. [10] surveyed watermarking techniques using soft computing approaches, including neural networks and evolutionary algorithms, showing improved adaptability and robustness. Nonetheless, they overlooked critical challenges such as adversarial vulnerability and explainability of AI models. Mansour and Abdelrahim [17] proposed an evolutionary computing model resilient to RS steganalysis, but their focus on a single application domain restricted the generalizability of findings. Similarly, Evsutin et al. [11] reviewed AI-driven methods but provided limited discussion on their scalability or ethical implications, which are increasingly relevant in practice.

Application-specific reviews further expanded the scope. Douglas et al. [8] examined steganography for biometric protection, highlighting privacy benefits but neglecting usability and real-world deployment challenges. Magdy et al. [9] systematically reviewed medical image security, yet their focus on healthcare overlooked broader cross-sectoral lessons. Sajjad et al. [18] proposed a mobile-cloud medical framework, but its technical feasibility in diverse healthcare infrastructures was not critically examined. Rathore et al. [19] extended applications to the Internet of Vehicles, integrating encryption and steganography, though without addressing interoperability with existing IoT standards. AlSabhany et al. [20] provided a systematic classification of digital audio steganography, but their scope was confined to carrier-specific issues rather than cross-modal integration.

Comprehensive surveys began to emphasize methodological and evaluative aspects. Kadhim et al. [3] reviewed image steganography techniques and evaluation methodologies, stressing the need for standardized frameworks. However, their analysis did not propose actionable paths toward such standardization. Setiadi et al. [6] expanded on goals, datasets, and methods, offering a more holistic view, yet the rapid evolution of AI-driven techniques since 2020 makes parts of their review quickly outdated. Kaur et al. [21] examined computational image steganography, identifying algorithmic advances but offering limited reflection on how these approaches address long-standing challenges such as balancing imperceptibility and security. Collectively, these reviews catalogued progress but often lacked critical synthesis, leaving the field without a unified perspective on persistent gaps, trade-offs, and research priorities.

2.2. Past Bibliometric Analyses on Steganography

Despite the abundance of technical reviews, comprehensive bibliometric studies of steganography remain limited. While bibliometric methods have been widely applied in cryptography and digital forensics, steganography has not received comparable scientometric attention [22]. This lack of systematic mapping has constrained understanding of its intellectual evolution and collaborative structures.

The few existing bibliometric analyses are narrow in scope. Reinel et al. [23] examined deep learning-based steganalysis, while Azam et al. [24] focused on cover selection methods. Other niche studies considered quantum steganography [12] or medical applications [9]. Although valuable, these works relied heavily on descriptive statistics such as citation counts and authorship patterns. They did not apply advanced techniques such as clustering or semantic mapping, thereby missing the opportunity to uncover deeper intellectual structures or cross-domain linkages. As Donthu et al. [25] emphasized, methods like co-citation analysis and direct citation networks remain underutilized in this domain.

This methodological gap has left unanswered questions about the field’s maturity, its thematic interconnections, and the drivers of its evolution. By failing to integrate temporal, geographic, and institutional perspectives, past bibliometric work has provided only fragmented insights. Our study addresses this limitation by offering the first century-spanning bibliometric analysis of steganography. Using advanced techniques such as direct citation clustering and semantic linkage analysis, we provide a macroscopic, data-driven perspective that complements and extends prior technical reviews.

2.3. Conceptual Framework for Steganography Research Analysis

We propose a three-dimensional framework to analyze steganography research, integrating technical evolution, application domains, and evaluation paradigms.

The technical evolution dimension traces the field's progression from spatial to transform domain methods, from fixed to adaptive strategies, and from handcrafted to learning-based approaches, extending to quantum and biological computing. Early models by Lee and Chen [26] and more advanced approaches such as Fakhredanesh et al. [16] exemplify this trajectory, aligning with Li et al.'s [27] comprehensive classification.

The application domains dimension highlights diversification beyond secure communication to areas such as copyright protection, healthcare, military intelligence, and IoT. Examples include Sajjad et al.'s [18] medical image framework, Rathore et al.'s [19] Internet of Vehicles model, and Zear et al.'s [28] medical watermarking technique.

The evaluation paradigms dimension covers the shift from visual inspection to statistical, application-specific, and adversarial methods. Mansour and Abdelrahim's [17] RS attack-resilient model and Subhedar and Mankar's [29] multi-dimensional framework underscore this evolution. These dimensions clarify how technical innovation, practical application, and evaluation intersect, offering a structured basis for identifying gaps and guiding future research directions. The three-dimensional framework offers a holistic view of steganography research by linking how methods evolve, where they are applied, and how they are evaluated. This integration clarifies research maturity, uncovers underexplored intersections, and provides a structured basis for guiding future work.

3. DATA AND METHODS

3.1. Data

We retrieved bibliographic data from the Web of Science Core Collection, which is widely used for bibliometric analysis due to its structured content and complete citation linkages [30]. The search query ALL=("Steganograp*") was used to collect articles containing "Steganography" and its variations (e.g., "Steganographic") in the title, abstract, or keywords. The dataset includes publications from April 1, 1924, to the retrieval date, February 4, 2025, totaling 9,403 records.

3.2. Methods

We mapped the research landscape using direct citation analysis. Previous studies have shown that this method effectively captures the structure of research fields and identifies emerging academic topics [31]. We applied the Louvain modularity maximization algorithm [32] to form clusters, ensuring that only strongly connected nodes were retained. This algorithm was selected for its ability to effectively handle large networks and produce interpretable clustering solutions that maximize modularity, ensuring more connections exist within clusters than between them [33]. For each resulting cluster, we calculated key quantitative data including the number of articles, average publication year, and average citation count. We then labeled (i.e., named) clusters based on their most common keywords and the content of their most-cited articles.

To examine the relationship between Steganography research clusters, we conducted a semantic linkage analysis by comparing vocabulary across clusters from different networks. This approach allowed us to identify topical overlaps and potential synergies between research clusters. To do so, we employed a sentence-transformer approach based on BERT (Bidirectional Encoder Representations from Transformers) to convert these aggregated cluster texts into dense vector representations [34]. Unlike traditional bag-of-words approaches that treat words as independent units, BERT-based transformers process text bidirectionally, allowing the model to understand words in context by considering both preceding and following terms. This contextual understanding enables the model to capture polysemy (words with multiple meanings), semantic relationships, and domain-specific terminology that might be missed by simpler vectorization methods. The following flowchart (Figure 1) summarizes the methods used to conduct this review. We began by retrieving articles on steganography from the Web of Science database. These articles were then represented as nodes in a citation network constructed using direct citation links. Weakly connected and isolated nodes were removed, and the Louvain algorithm was applied to group the remaining articles into clusters. Each cluster was labeled based on common keywords and the themes of its most-cited papers. Finally, we analyzed the semantic similarity between clusters using cosine similarity measures to explore topical overlaps and relationships across the research landscape.

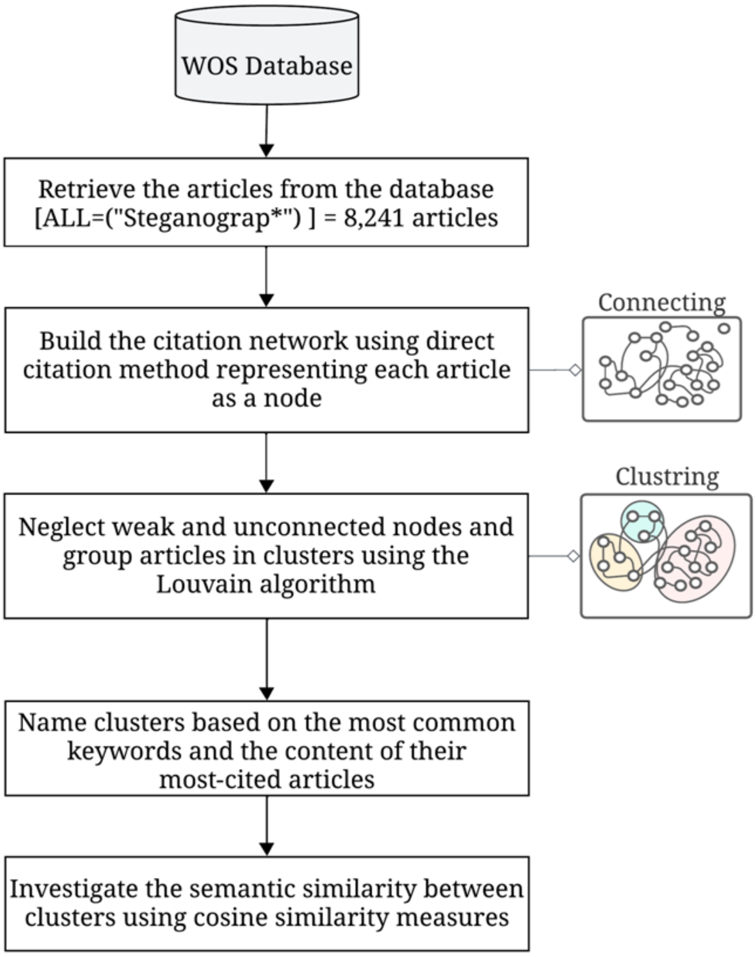
WOS Database
Retrieve the articles from the database [ALL=("Steganograp*")] = 8,241 articles
Build the citation network using direct citation method representing each article as a node
Connecting
Neglect weak and unconnected nodes and group articles in clusters using the Louvain algorithm
Clustring
Name clusters based on the most common keywords and the content of their most-cited articles
Investigate the semantic similarity between clusters using cosine similarity measures

Figure 1. Workflow of data retrieval, citation network construction, clustering, and semantic similarity analysis.

4. RESULTS

4.1. Overview of the Research Landscape

The bibliometric analysis of steganography research over the past century revealed a vibrant and evolving research landscape. The study mapped 8,241 articles connected by 49,572 direct citation links, forming nine major thematic clusters and an "Others" category comprising 13% of the articles. The two largest clusters, " Classical Image-Based Steganography" (21%) and " Foundational Steganography and Steganalysis " (18%), dominate the field in terms of volume. However, citation impact analysis indicates that cluster size does not always correlate with influence. Notably, " Machine Learning and Deep Steganography" (Cluster 3) and " Reversible Steganography and Media Integrity" (Cluster 7) exhibited the highest average citation counts (22.92 and 22.27, respectively).

In total, articles were disseminated across 220 different journals. The most frequent publication venues were MULTIMEDIA TOOLS AND APPLICATIONS with 539 articles, IEEE ACCESS with 206 articles, and IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY with 153 articles. The top three most prolific publishing authors were Chang (222 articles), Fridrich (132 articles), and Zhang (108 articles), with their most influential works cited as [34], [35], and [36] respectively.

Several overarching trends emerged across clusters. First, there is a notable rise in deep learning integration, particularly through convolutional neural networks and GANs. Second, interest in coverless steganography is expanding, representing a conceptual shift in hiding paradigms. Third, while nascent, quantum steganography and GAN-based steganographic applications are beginning to surface in keywords, suggesting new interdisciplinary research opportunities. Table 1 presents key information for the clusters, including each cluster’s name (representing the dominant topic discussed in the cluster’s articles), the number of articles, the average publication year of the articles (APY), and the top three authors and journals where research articles were published.

Table 1. Overview of the steganography research clusters by article count (N), average publication year (APY), and top contributing journals.

ID	Cluster name	N (%)	APY	Top 3 Journals	N
C1	Classical Image-Based Steganography	1770 (21%)	2017.3	MULTIMEDIA TOOLS AND APPLICATIONS	195
				IEEE ACCESS	50
				EXPERT SYSTEMS WITH APPLICATIONS	18
C2	Foundational Steganography and Steganalysis	1503 (18%)	2010.4	INFORMATION HIDING	42
				IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	27
				MULTIMEDIA TOOLS AND APPLICATIONS	27
C3	Machine Learning and Deep Steganography	930 (11%)	2019.4	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	76
				MULTIMEDIA TOOLS AND APPLICATIONS	61
				IEEE ACCESS	40

C4	Audio and Multimedia Steganography	929 (11%)	2015.1	MULTIMEDIA TOOLS AND APPLICATIONS	30
				SECURITY AND COMMUNICATION NETWORKS	25
				IEEE ACCESS	24
C5	GAN-Based and Coverless Steganography	488 (6%)	2021.3	IEEE ACCESS	33
				MULTIMEDIA TOOLS AND APPLICATIONS	20
				CMC-COMPUTERS MATERIALS & CONTINUA	18
C6	Linguistic and Semantic Text Steganography	465 (6%)	2018.2	IEEE SIGNAL PROCESSING LETTERS	26
				MULTIMEDIA TOOLS AND APPLICATIONS	21
				IEEE ACCESS	14
C7	Reversible Steganography and Media Integrity	425 (5%)	2015.3	MULTIMEDIA TOOLS AND APPLICATIONS	67
				INFORMATION SCIENCES	12
				JOURNAL OF VISUAL COMMUNICATION AND IMAGE REPRESENTATION	12
C8	Motion-Based and Compressed Video Steganography	342 (4%)	2018.1	MULTIMEDIA TOOLS AND APPLICATIONS	42
				IEEE ACCESS	13
				CMC-COMPUTERS MATERIALS & CONTINUA	7
C9	Multimodal Steganography Applications	337 (4%)	2013.2	MULTIMEDIA TOOLS AND APPLICATIONS	8
				IEEE TRANSACTIONS ON VISUALIZATION AND COMPUTER GRAPHICS	5
				INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING INFORMATION AND CONTROL	5
C10	Others	1052 (13%)	2016.7	-	-

In terms of geographic distribution, China leads steganography research output, particularly contributing heavily to Clusters 1, 3, 5, and 8. India and the United States follow, with India being notably active in Clusters 1, 2, and 4, while the United States shows a stronger presence in theoretical foundations and steganalysis research. Among institutions, Feng Chia University and the Chinese Academy of Sciences emerge as the most prolific, with SUNY Binghamton being particularly influential in advancing steganalysis methodologies.

Figure 2 illustrates the temporal evolution of the nine major steganography research clusters from 1990 to 2024, revealing distinct developmental patterns that reflect the field's dynamic nature. The utilized methods did not retain any articles with publication year before 1990. The "Foundational Steganography and Steganalysis" cluster (C2) dominated the early 2000s, peaking around 2008 before gradually declining, indicating the maturation of theoretical foundations. Conversely, "Classical Image-Based Steganography" (C1) shows remarkable growth from 2010 onward, becoming the predominant cluster by 2024, demonstrating the enduring importance of image-based techniques. Most notably, "Machine Learning and Deep Steganography" (C3) and

"GAN-Based and Coverless Steganography" (C5) exhibit steep upward trajectories from 2015 onward, reflecting the field's embrace of artificial intelligence approaches. Meanwhile, specialized domains like "Linguistic and Semantic Text Steganography" (C6) and "Audio and Multimedia Steganography" (C4) show moderate but steady growth, indicating diversification of carrier media. Taken together, the visualization captures a clear progression: steganography research has transitioned from theoretical and foundational concerns toward application-driven, AI-enhanced methods that align with broader advances in computer vision, data security, and machine learning. This pattern underscores both the stability of core image-based approaches and the accelerating influence of AI in shaping future research agendas.

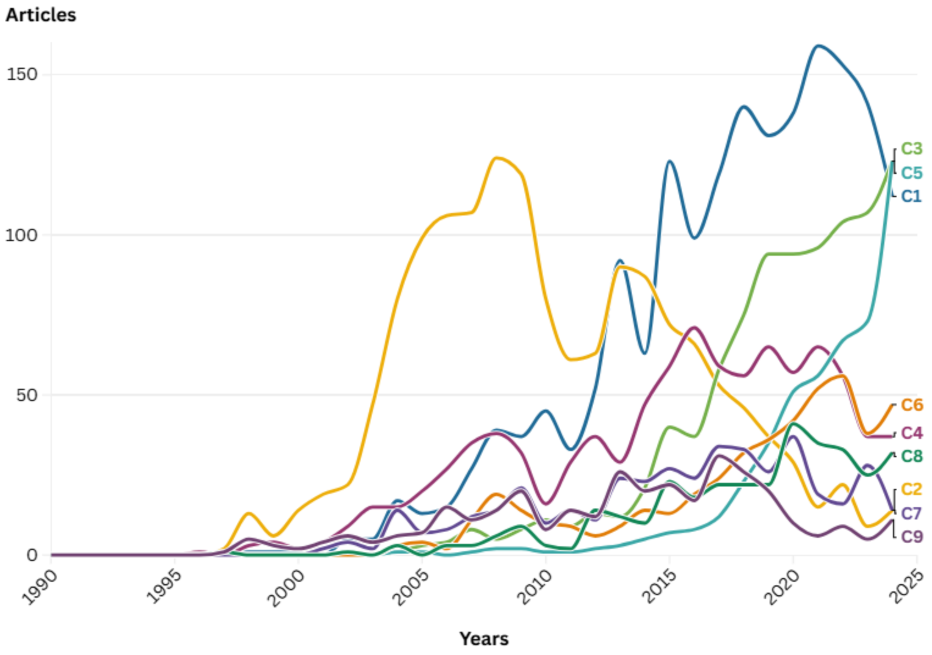

Figure 2. Temporal evolution of the nine steganography research clusters (1990–2024).

To examine the relationship between thematic maturity and scholarly impact across steganography research, Figure 3 plots the average publication year against the average citation count for the top nine clusters. The resulting distribution reveals a nuanced landscape of evolving subfields. Clusters like "Machine Learning and Deep Steganography" (C3) and "Reversible Steganography and Media Integrity" (C7) stand out with the highest citation impact, reflecting the growing academic and practical value of AI-powered steganalysis and lossless data hiding methods. In contrast, "GAN-Based and Coverless Steganography" (C5) is the most recent in terms of average publication year, underscoring its emergence as a cutting-edge domain that redefines traditional embedding through generative models. Meanwhile, "Foundational Steganography and Steganalysis" (C2) retains its relevance with high citation scores despite its early emergence, due to its theoretical grounding and methodological influence. Clusters such as "Linguistic and Semantic Text Steganography" (C6) and "Motion-Based and Compressed Video Steganography" (C8) exhibit lower citation density, likely reflecting their specialized, domain-specific nature and more recent expansion. Importantly, this temporal-impact mapping highlights how research maturity does not always translate into declining influence: foundational clusters continue to anchor the field, while newer AI-driven areas gain rapid recognition despite limited time to accumulate citations. This dynamic suggests an evolving balance where established theories provide continuity, even as disruptive innovations reshape the research frontier.

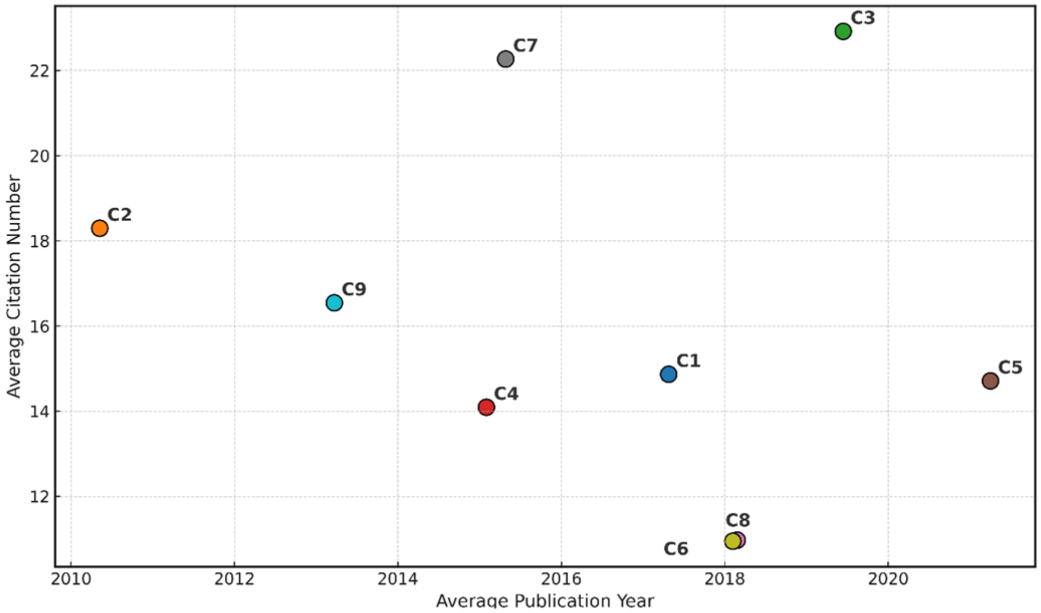

Figure 3. Average publication year versus citation counts across the nine clusters.

4.2. Cluster-Level Analysis

The largest research cluster, Classical Image-Based Steganography (Cluster 1), centers on traditional techniques such as Least Significant Bit (LSB) embedding, pixel-value differencing, and histogram-based methods. These methods emphasize simplicity, imperceptibility, and minimal distortion. Foundational works in this cluster include studies on JPEG quantization table manipulation [34] and directional embedding strategies [36], which remain highly cited for their practicality and influence. The cluster reflects the foundational architecture of image steganography and maintains a significant presence despite a declining trend in recent years, likely due to the emergence of deep learning–driven alternatives. Its persistence, however, illustrates the continued importance of low-complexity, interpretable methods in scenarios where computational resources or transparency are critical.

Foundational Steganography and Steganalysis (Cluster 2) encompasses the theoretical and algorithmic basis for both embedding and detection strategies. It includes work on adaptive embedding, LSB matching analysis, and JPEG-specific steganographic schemes. Pioneering steganalysis techniques for grayscale and JPEG images [35], [37], as well as frameworks for evaluating detectability and robustness, are central to this cluster. Although its average publication year skews earlier, the intellectual foundations laid here have strongly shaped newer methodological developments. Its continued influence highlights how theoretical underpinnings remain relevant for benchmarking and for guiding the design of more advanced detection-resistant models.

The third cluster, Machine Learning and Deep Steganography, marks a transition to data-driven approaches using convolutional neural networks, ensemble classifiers, and rich feature models. Seminal contributions include ensemble/rich feature models for image steganalysis [38] and

CNN-based classifiers for image steganalysis [39]. With the highest citation impact across all clusters, this research domain exemplifies the field's shift toward optimization, adversarial learning, and automated detection and embedding. Its growth also indicates the increasing convergence between steganography and mainstream machine learning research, though challenges of adversarial robustness and explainability remain open.

Audio and Multimedia Steganography (Cluster 4) addresses data hiding in non-image formats, particularly focusing on audio, VoIP streams, and network traffic. Research here includes Quantization Index Modulation (QIM) [40], network-layer steganography [41], and codec-based concealment in compressed audio formats [42]. The interdisciplinary nature of this cluster links communication theory with real-time media security, making it central to multimedia transmission applications. Its more modest size relative to image-based research reflects both the dominance of visual carriers and the technical challenges of embedding in perceptually sensitive audio streams.

Closely aligned in its innovation trajectory, GAN-Based and Coverless Steganography (Cluster 5) represents one of the most recent and rapidly growing clusters. It encompasses work on generative models, coverless embedding, and semantic encoding techniques. Notable studies include the use of GANs to generate undetectable images for hiding [43] and distortion learning methods to improve imperceptibility [44]. This cluster demonstrates the move away from modifying existing media and toward synthetic generation for information concealment. Its sharp rise underscores the transformative role of generative AI but also raises open questions about standardization, reproducibility, and the potential misuse of synthetic content.

Linguistic and Semantic Text Steganography (Cluster 6) is characterized by approaches that manipulate textual structure, syntax, and semantics using models like VAEs and RNNs. Techniques such as synonym substitution, syntactic tree manipulation, and semantic coherence optimization dominate this space. Research contributions in this area, including linguistic embedding via deep recurrent models [45], reflect a growing convergence between natural language processing and secure communication. However, the relatively lower citation density of this cluster suggests it remains a niche domain, partly due to the complexity of maintaining semantic fidelity across languages and the limited applicability of text steganography in bandwidth-intensive scenarios.

Reversible Steganography and Media Integrity (Cluster 7) focuses on lossless data hiding methods that allow exact restoration of original content post-extraction. Key approaches include histogram shifting [46], predictive coding, and reversible vector quantization. Applications are prominent in domains requiring data integrity, such as medical imaging [47]. Influential works in this cluster demonstrate how to maintain media fidelity while supporting high-capacity, secure data embedding [48]. The strong applied orientation of this cluster highlights the importance of context-specific requirements, especially in regulated sectors like healthcare, where data integrity cannot be compromised.

Motion-Based and Compressed Video Steganography (Cluster 8) addresses the challenges of hiding data in temporally structured media. It includes techniques leveraging motion vectors, inter-frame differences, and advanced video codecs like HEVC [49]. While smaller in volume, the cluster shows increasing relevance in light of rising video data usage. Recent studies demonstrate effective embedding in motion streams while preserving playback quality [50]. Despite this promise, the distinct challenges of temporal consistency and high compression rates mean video-based steganography remains less mature compared to image-based approaches.

The final primary cluster, Multimodal Steganography Applications (Cluster 9), aggregates application-driven research across diverse data types, including 3D mesh steganography [51], hybrid embedding schemes, and security-enhanced use cases. Early works on geometric modifications and cross-media embedding are cited prominently [52]. While the cluster exhibits a slightly older average publication year, its broad scope highlights the diversity of steganography's real-world applications. Its heterogeneity, however, makes it less cohesive than other clusters, reflecting the application-driven rather than methodological orientation of the studies it aggregates.

To complement the temporal and volume analysis, Figure 4 explores the semantic proximity between research topics by presenting a cosine similarity heatmap. High similarity values (closer to 1) indicate substantial thematic overlap, while lower values suggest more differentiated research areas. Several important patterns emerge based on the actual similarity metrics.

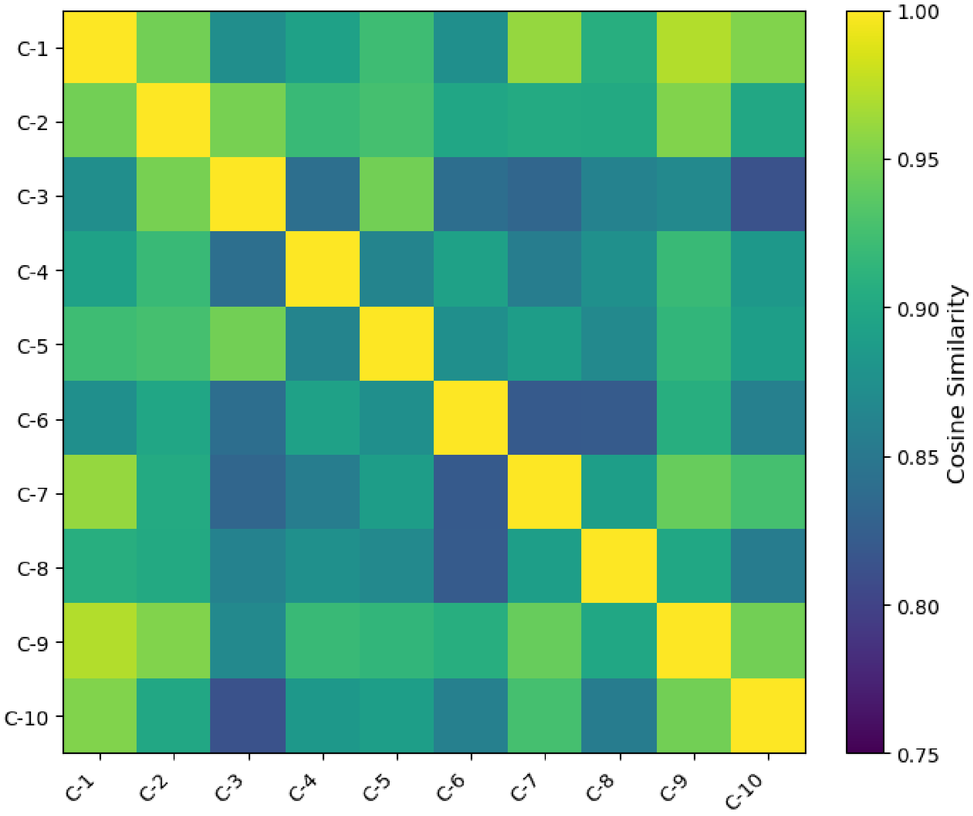

Figure 4. Cosine similarity heatmap of semantic proximity among the nine clusters.

Clusters 1 (Classical Image-Based Steganography) and 9 (Multimodal Steganography Applications) exhibit a very high cosine similarity of 0.97. This strong proximity reflects their shared reliance on traditional embedding techniques, particularly in image domains, and their focus on practical applications like covert communication and watermarking. Likewise, Clusters 1 and 7 (Reversible Data Hiding and Lossless Data Embedding) also show high semantic similarity (0.96), driven by common technical underpinnings such as pixel-based manipulations, histogram shifting, and predictive coding to balance concealment and media integrity.

Cluster 2 (Foundational Steganography and Steganalysis), which covers general steganographic principles and steganalysis, demonstrates strong similarity with Cluster 3 (Machine Learning and Deep Steganography) at 0.95. This suggests that while Cluster 3 introduces advanced machine learning techniques, its roots are firmly anchored in the core problems and structures outlined in classical steganography. Meanwhile, Cluster 5 (GAN-Based and Coverless Steganography) shows moderately high similarity with Clusters 3 and 6, reflecting their converging use of modern AI models, particularly generative approaches, but with differences based on data modalities (e.g., images vs. text).

Lower similarity values highlight the distinctiveness of certain research streams. For instance, Cluster 6 (Linguistic and Semantic Text Steganography) records relatively low similarity (around 0.78–0.82) with most image- or audio-based clusters. This gap arises because text steganography focuses on linguistic structures, syntactic transformations, and semantic integrity rather than pixel, vector, or frequency-domain manipulations. Similarly, Cluster 8 (Motion-Based and Compressed Video Steganography) maintains moderate similarity scores with image-related clusters but diverges significantly from text-focused and reversible hiding studies, reflecting its unique challenges such as temporal coherence and motion compensation.

The heatmap reveals two broad semantic groupings: (1) a highly interconnected cluster of traditional and AI-augmented media steganography (Clusters 1, 2, 3, 5, 7, and 9) and (2) more specialized, distinct subfields such as text steganography (Cluster 6) and video-based concealment (Cluster 8). This division underscores how the field is consolidating around image- and AI-driven research, while maintaining smaller, domain-specific frontiers. The differentiation also signals opportunities for cross-domain innovation, particularly in bridging text, video, and multimodal approaches with the more established image- and AI-centric research streams.

5. DISCUSSION

5.1. Evolution of Steganography Research Paradigms

The bibliometric analysis reveals a clear evolutionary trajectory in steganography research over the past century, characterized by distinct paradigm shifts that reflect both technological advancements and changing security requirements. The field has progressed from foundational theoretical concepts to increasingly specialized and sophisticated approaches, with each major transition building upon previous knowledge while introducing novel conceptual frameworks.

The temporal distribution across clusters demonstrates this evolution, with "Foundational Steganography and Steganalysis" (Cluster 2, APY = 2010.4) establishing the theoretical underpinnings that guided subsequent developments. Early research focused on fundamental principles of information hiding, security models, and basic detection techniques [37], [53]. These foundational works created the intellectual framework necessary for understanding both embedding and detection principles, with their continued citation in recent publications underscoring their enduring influence.

As digital media became ubiquitous, research shifted toward specialized techniques for specific carrier types, with image steganography (Cluster 1, APY = 2017.3) emerging as the dominant paradigm. This period saw the development of now-classical techniques such as LSB embedding, pixel-value differencing [54], and histogram-based methods. The concentration of research in this area reflects both the practical utility of images as steganographic carriers and the rich opportunities they present for information hiding due to their inherent redundancy and perceptual characteristics.

The most recent paradigm shift, evident in "Machine Learning and Deep Steganography" (Cluster 3, APY = 2019.4) and "GAN-Based and Coverless Steganography" (Cluster 5, APY = 2021.3), represents the integration of artificial intelligence into steganographic practice. This transition marks a fundamental reconceptualization of the field, moving from hand-crafted algorithms to data-driven approaches that can automatically optimize for competing objectives such as imperceptibility, capacity, and security. The rapid growth of these clusters, despite their relative recency, signals a transformative moment in steganography research.

Particularly noteworthy is the emergence of GAN-based techniques, which represent not merely an incremental improvement but a conceptual reimagining of the steganographic process. Rather than modifying existing carriers, these approaches generate steganographic content from scratch, fundamentally altering the traditional detect-and-modify paradigm. This shift from "hiding in existing media" to "generating media with hidden content" constitutes perhaps the most significant paradigmatic evolution in the field's recent history.

5.2. Geographic and Institutional Contributions

The geographic distribution of steganography research reveals significant patterns of regional specialization and institutional leadership that have shaped the field's development. China's dominance in overall research output (26.5%), particularly in Clusters 1, 3, 5, and 8, reflects its substantial investment in information security research and digital media technologies. This concentration of effort has contributed significantly to advancements in image-based techniques, deep learning integration, and emerging approaches such as coverless steganography.

India (16.4%) and The United States (9.5%), while producing fewer publications overall, have exerted disproportionate influence in theoretical foundations and steganalysis research. U.S. institutions like SUNY Binghamton have made seminal contributions to detection methodologies, particularly in Cluster 3's machine learning approaches [55], [56]. Indian contributions are notable in Clusters 1, 2, and 4, demonstrating a focus on both foundational techniques and practical applications in multimedia steganography [57], [3]. Taiwan (7.2%) and Iran (2.9%) follow the leading three countries, making them among the most active contributors to steganography research.

At the institutional level, Feng Chia University and the Chinese Academy of Sciences emerge as the most prolific contributors, establishing themselves as centers of excellence in steganography research. The concentration of high-impact work at specific institutions suggests the importance of specialized research groups and established expertise in driving innovation. The citation patterns indicate that while quantity of publications varies significantly across institutions, influence is more concentrated, with a smaller number of institutions producing the most highly cited works.

The temporal analysis of geographic contributions reveals an interesting shift in the center of research gravity. Earlier work was predominantly from North American and European institutions, while more recent clusters show increasing dominance from East Asian contributors. This shift parallels broader trends in computer science research and reflects changing global research capacity and priorities. The emergence of new institutional players in recent years, particularly from regions previously underrepresented in the literature, suggests an ongoing democratization of steganography research that may further diversify the field's perspectives and approaches.

5.3. Technological Convergence and Research Gaps

The steganography research landscape exhibits interesting patterns of technological convergence that have shaped its evolution, alongside persistent research gaps that present opportunities for future investigation. The convergence of steganography with artificial intelligence represents perhaps the most significant technological integration in recent years, transforming both embedding and detection capabilities as evidenced by the rapid growth of Cluster 3. This integration has enabled more sophisticated adaptive strategies that can automatically identify optimal embedding locations and patterns based on carrier characteristics.

The marriage of steganography with generative adversarial networks in Cluster 5 has created entirely new paradigms for covert communication, fundamentally altering traditional approaches to carrier selection and modification. Emerging intersections with blockchain technology and quantum information [58], [12] signal new frontiers of technological convergence that are still nascent but potentially transformative, offering novel security guarantees and communication channels that may address limitations of traditional approaches.

Despite substantial progress, several significant research gaps persist. A notable gap exists in comprehensive security models that account for modern adversarial capabilities. While individual techniques are often evaluated against specific detection methods, there is limited work on unified frameworks that can assess steganographic security across different carrier types and against diverse adversarial models. The increasing sophistication of machine learning-based steganalysis highlights the need for more robust security evaluation frameworks that can account for adaptive and learning adversaries.

The evaluation metrics employed across the literature exhibit considerable inconsistency, making comparative assessment challenging. While certain metrics such as PSNR and SSIM are commonly used for image steganography [57], there is less consensus on appropriate metrics for other media types. Furthermore, the relationship between these technical metrics and practical security remains inadequately explored. The development of standardized, cross-media evaluation frameworks would significantly enhance the field's ability to assess progress and compare competing approaches.

Human factors in steganography represent an underexplored dimension. While technical imperceptibility is extensively studied, the psychological aspects of steganographic security—how human observers perceive and detect anomalies—receive comparatively little attention. This gap is particularly relevant for applications where human adversaries, rather than automated systems, represent the primary threat. The intersection of steganography with fields such as human perception, cognitive psychology, and human-computer interaction offers rich opportunities for addressing this limitation.

6. CONCLUSION

This bibliometric review of steganography research across a century highlights a dynamic field shaped by evolving paradigms, distinct clusters, and emerging frontiers. From 8,241 articles and 49,572 citation links, nine major clusters were identified, mapping the intellectual structure and evolution of the discipline.

Image-based approaches remain dominant, with foundational methods such as LSB embedding forming the largest cluster. Foundational theory continues to anchor the field, while machine learning and GAN-based methods mark a clear paradigm shift toward AI-driven techniques with high impact despite their recency. Diversification into audio, text, video, and reversible steganography illustrates the adaptability of research to new carriers and application domains.

Geographically, China leads in output, followed by India and the United States, with institutions such as Feng Chia University, the Chinese Academy of Sciences, and SUNY Binghamton shaping progress in both methodology and theory. Temporally, the field has advanced from early principles to deep learning, blockchain, and quantum approaches, reflecting a steady transition toward more sophisticated frameworks.

Overall, this study provides the most comprehensive mapping of steganography to date, clarifying its intellectual organization and highlighting its adversarial nature, where steganography and steganalysis co-evolve. For researchers, this synthesis offers orientation to past achievements, present challenges, and future opportunities, serving as both a reference and a roadmap for advancing the field.

7. Future Research Agendas

Our analysis points to several promising research directions. Quantum steganography stands out as a transformative frontier, offering fundamentally new security guarantees rooted in quantum principles. Coverless steganography, highlighted in Cluster 5, departs from traditional methods by mapping messages to inherent media features, potentially enhancing resistance to detection. Integration with blockchain, AI, and multimodal techniques opens further opportunities, alongside the urgent need for standardized evaluation frameworks to resolve current metric inconsistencies. Future work should also embrace human-centered evaluation, exploring psychological aspects of detection, and employ formal verification to strengthen theoretical foundations. Application-driven research in areas such as medical data protection, privacy-preserving machine learning, IoT security, and censorship resistance promises high societal impact. Long-term ambitions include unifying theories across carriers, achieving near-perfect security, developing human–machine collaborative systems, and designing adaptive frameworks for evolving threats.

Finally, as steganography advances, ethical considerations and governance models must guide its responsible use. The field’s century-long evolution provides a strong base for pursuing these ambitious research agendas and sustaining its relevance in an increasingly complex digital landscape.

References

[1] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, Mar. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[2] L. Singh, A. K. Singh, and P. K. Singh, “Secure data hiding techniques: a survey,” Multimed Tools Appl, vol. 79, no. 23–24, pp. 15901–15921, Jun. 2020, doi: 10.1007/s11042-018-6407-5.

[3] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research,” Neurocomputing, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.

[4] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, “Digital image steganography: A literature survey,” Information Sciences, vol. 609, pp. 1451–1488, Sep. 2022, doi: 10.1016/j.ins.2022.07.120.

[5] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, “Image steganography in spatial domain: A survey,” Signal Processing: Image Communication, vol. 65, pp. 46–66, Jul. 2018, doi: 10.1016/j.image.2018.03.012.

[6] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, “Digital image steganography survey and investigation (goal, assessment, method, development, and dataset),” Signal Processing, vol. 206, p. 108908, May 2023, doi: 10.1016/j.sigpro.2022.108908.

[7] S. Dhawan and R. Gupta, “Analysis of various data security techniques of steganography: A survey,” Information Security Journal: A Global Perspective, vol. 30, no. 2, pp. 63–87, Mar. 2021, doi: 10.1080/19393555.2020.1801911.

[8] M. Douglas, K. Bailey, M. Leeney, and K. Curran, “An overview of steganography techniques applied to the protection of biometric data,” Multimed Tools Appl, vol. 77, no. 13, pp. 17333–17373, Jul. 2018, doi: 10.1007/s11042-017-5308-3.

[9] M. Magdy, K. M. Hosny, N. I. Ghali, and S. Ghoniemy, “Security of medical images for telemedicine: a systematic review,” Multimed Tools Appl, vol. 81, no. 18, pp. 25101–25145, Jul. 2022, doi: 10.1007/s11042-022-11956-7.

[10] O. P. Singh, A. K. Singh, G. Srivastava, and N. Kumar, “Image watermarking using soft computing techniques: A comprehensive survey,” Multimed Tools Appl, vol. 80, no. 20, pp. 30367–30398, Aug. 2021, doi: 10.1007/s11042-020-09606-x.

[11] O. Evsutin, A. Melman, and R. Meshcheryakov, “Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions,” IEEE Access, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[12] K. Kadian, S. Garhwal, and A. Kumar, “Quantum walk and its application domains: A systematic review,” Computer Science Review, vol. 41, p. 100419, Aug. 2021, doi: 10.1016/j.cosrev.2021.100419.

[13] N. Provos, “Defending against statistical steganalysis,” in Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, in SSYM’01. USA: USENIX Association, Aug. 2001.

[14] Shunquan Tan and Bin Li, “Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting,” IEEE Signal Process. Lett., vol. 19, no. 6, pp. 336–339, Jun. 2012, doi: 10.1109/LSP.2012.2194702.

[15] X. Zhang and S. Wang, “Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security,” Pattern Recognition Letters, vol. 25, no. 3, pp. 331–339, Feb. 2004, doi: 10.1016/j.patrec.2003.10.014.

[16] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, “Steganography in discrete wavelet transform based on human visual system and cover model,” Multimed Tools Appl, vol. 78, no. 13, pp. 18475–18502, Jul. 2019, doi: 10.1007/s11042-019-7238-8.

[17] R. F. Mansour and E. M. Abdelrahim, “An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications,” Multidim Syst Sign Process, vol. 30, no. 2, pp. 791–814, Apr. 2019, doi: 10.1007/s11045-018-0575-3.

[18] M. Sajjad et al., “Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices,” Multimed Tools Appl, vol. 76, no. 3, pp. 3519–3536, Feb. 2017, doi: 10.1007/s11042-016-3811-6.

[19] M. S. Rathore et al., “A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography,” Computers and Electrical Engineering, vol. 102, p. 108205, Sep. 2022, doi: 10.1016/j.compeleceng.2022.108205.

[20] A. A. AlSabhany, A. H. Ali, F. Ridzuan, A. H. Azni, and M. R. Mokhtar, “Digital audio steganography: Systematic review, classification, and analysis of the current state of the art,” Computer Science Review, vol. 38, p. 100316, Nov. 2020, doi: 10.1016/j.cosrev.2020.100316.

[21] S. Kaur, S. Singh, M. Kaur, and H.-N. Lee, “A Systematic Review of Computational Image Steganography Approaches,” Arch Computat Methods Eng, vol. 29, no. 7, pp. 4775–4797, Nov. 2022, doi: 10.1007/s11831-022-09749-0.

[22] C. Chen, “Science Mapping: A Systematic Review of the Literature,” Journal of Data and Information Science, vol. 2, no. 2, pp. 1–40, Mar. 2017, doi: 10.1515/jdis-2017-0006.

[23] T.-S. Reinel, R.-P. Raul, and I. Gustavo, “Deep Learning Applied to Steganalysis of Digital Images: A Systematic Review,” IEEE Access, vol. 7, pp. 68970–68990, 2019, doi: 10.1109/ACCESS.2019.2918086.

[24] M. H. Noor Azam, F. Ridzuan, M. N. S. Mohd Sayuti, A. H. Azni, N. H. Zakaria, and V. Potdar, “A systematic review on cover selection methods for steganography: Trend analysis, novel classification and analysis of the elements,” Computer Science Review, vol. 56, p. 100726, May 2025, doi: 10.1016/j.cosrev.2025.100726.

[25] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," Journal of Business Research, vol. 133, pp. 285–296, Sep. 2021, doi: 10.1016/j.jbusres.2021.04.070.

[26] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," IEE Proc., Vis. Image Process., vol. 147, no. 3, p. 288, 2000, doi: 10.1049/ip-vis:20000341.

[27] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172, Apr. 2011.

[28] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," Multimed Tools Appl, vol. 77, no. 4, pp. 4863–4882, Feb. 2018, doi: 10.1007/s11042-016-3862-8.

[29] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," Computer Science Review, vol. 13–14, pp. 95–113, Nov. 2014, doi: 10.1016/j.cosrev.2014.09.001.

[30] C. Birkle, D. A. Pendlebury, J. Schnell, and J. Adams, "Web of Science as a data source for research on scientific and scholarly activity," Quantitative Science Studies, vol. 1, no. 1, pp. 363–376, Feb. 2020, doi: 10.1162/qss_a_00018.

[31] K. W. Boyack and R. Klavans, "Co-Citation Analysis, Bibliographic Coupling, and Direct citation: Which citation approach represents the research front most accurately?," Journal of the American Society for Information Science and Technology, vol. 61, pp. 2389–2404, 2010.

[32] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," Journal of Statistical Mechanics: Theory and Experiment, vol. 2008, no. 10, p. P10008, Oct. 2008, doi: 10.1088/1742-5468/2008/10/P10008.

[33] M. E. J. Newman, "Modularity and community structure in networks," Proceedings of the National Academy of Sciences of the United States of America, vol. 103, no. 23, pp. 8577–82, 2006, doi: 10.1073/pnas.0601602103.

[34] C.-C. Chang, T.-S. Chen, and L.-Z. Chung, "A steganographic method based upon JPEG and quantization table modification," Information Sciences, vol. 141, no. 1–2, pp. 123–138, Mar. 2002, doi: 10.1016/S0020-0255(01)00194-3.

[35] J. Fridrich and M. Goljan, "Practical steganalysis of digital images: state of the art," presented at the Electronic Imaging 2002, E. J. Delp Iii and P. W. Wong, Eds., San Jose, CA, Apr. 2002, pp. 1–13. doi: 10.1117/12.465263.

[36] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," IEEE Commun. Lett., vol. 10, no. 11, pp. 781–783, Nov. 2006, doi: 10.1109/LCOMM.2006.060863.

[37] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," IEEE J. Select. Areas Commun., vol. 16, no. 4, pp. 474–481, May 1998, doi: 10.1109/49.668971.

[38] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble Classifiers for Steganalysis of Digital Media," IEEE Trans.Inform.Forensic Secur., vol. 7, no. 2, pp. 432–444, Apr. 2012, doi: 10.1109/TIFS.2011.2175919.

[39] J. Ye, J. Ni, and Y. Yi, "Deep Learning Hierarchical Representations for Image Steganalysis," IEEE Trans.Inform.Forensic Secur., vol. 12, no. 11, pp. 2545–2557, Nov. 2017, doi: 10.1109/TIFS.2017.2710946.

[40] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inform. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001, doi: 10.1109/18.923725.

[41] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-Based Survey and Categorization of Network Covert Channel Techniques," ACM Comput. Surv., vol. 47, no. 3, pp. 1–26, Apr. 2015, doi: 10.1145/2684195.

[42] Y. F. Huang, S. Tang, and J. Yuan, "Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec," IEEE Trans.Inform.Forensic Secur., vol. 6, no. 2, pp. 296–306, Jun. 2011, doi: 10.1109/TIFS.2011.2108649.

[43] Z. Zhou et al., "Secret-to-Image Reversible Transformation for Generative Steganography," IEEE Trans. Dependable and Secure Comput., vol. 20, no. 5, pp. 4118–4134, Sep. 2023, doi: 10.1109/TDSC.2022.3217661.

[44] W. Tang, S. Tan, B. Li, and J. Huang, “Automatic Steganographic Distortion Learning Using a Generative Adversarial Network,” IEEE Signal Process. Lett., vol. 24, no. 10, pp. 1547–1551, Oct. 2017, doi: 10.1109/LSP.2017.2745572.

[45] J. Wen, X. Zhou, P. Zhong, and Y. Xue, “Convolutional Neural Network Based Text Steganalysis,” IEEE Signal Process. Lett., vol. 26, no. 3, pp. 460–464, Mar. 2019, doi: 10.1109/LSP.2019.2895286.

[46] P. Tsai, Y.-C. Hu, and H.-L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Processing, vol. 89, no. 6, pp. 1129–1143, Jun. 2009, doi: 10.1016/j.sigpro.2008.12.017.

[47] J. Fridrich, M. Goljan, and R. Du, “Invertible authentication,” presented at the Photonics West 2001 - Electronic Imaging, P. W. Wong and E. J. Delp Iii, Eds., San Jose, CA, Aug. 2001, pp. 197–208. doi: 10.1117/12.435400.

[48] C.-F. Lee and Y.-L. Huang, “An efficient image interpolation increasing payload in reversible data hiding,” Expert Systems with Applications, vol. 39, no. 8, pp. 6712–6719, Jun. 2012, doi: 10.1016/j.eswa.2011.12.019.

[49] J. Yang and S. Li, “An efficient information hiding method based on motion vector space encoding for HEVC,” Multimed Tools Appl, vol. 77, no. 10, pp. 11979–12001, May 2018, doi: 10.1007/s11042-017-4844-1.

[50] H. A. Aly, “Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 14–18, Mar. 2011, doi: 10.1109/TIFS.2010.2090520.

[51] Y.-M. Cheng and C.-M. Wang, “A high-capacity steganographic approach for 3D polygonal meshes,” Visual Comput, vol. 22, no. 9–11, pp. 845–855, Sep. 2006, doi: 10.1007/s00371-006-0069-4.

[52] R. Ohbuchi, H. Masuda, and M. Aono, “Watermarking three-dimensional polygonal models through geometric and topological modifications,” IEEE J. Select. Areas Commun., vol. 16, no. 4, pp. 551–560, May 1998, doi: 10.1109/49.668977.

[53] C. Cachin, “An Information-Theoretic Model for Steganography,” in Information Hiding, D. Aucsmith, Ed., Berlin, Heidelberg: Springer, 1998, pp. 306–318. doi: 10.1007/3-540-49380-8_21.

[54] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, vol. 24, no. 9–10, pp. 1613–1626, Jun. 2003, doi: 10.1016/S0167-8655(02)00402-6.

[55] J. Fridrich and J. Kodovsky, “Rich Models for Steganalysis of Digital Images,” IEEE Trans.Inform.Forensic Secur., vol. 7, no. 3, pp. 868–882, Jun. 2012, doi: 10.1109/TIFS.2012.2190402.

[56] M. Boroumand, M. Chen, and J. Fridrich, “Deep Residual Network for Steganalysis of Digital Images,” IEEE Trans.Inform.Forensic Secur., vol. 14, no. 5, pp. 1181–1193, May 2019, doi: 10.1109/TIFS.2018.2871749.

[57] D. R. I. M. Setiadi, “PSNR vs SSIM: imperceptibility quality assessment for image steganography,” Multimed Tools Appl, vol. 80, no. 6, pp. 8423–8444, Mar. 2021, doi: 10.1007/s11042-020-10035-z.

[58] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, “A novel image steganography technique based on quantum substitution boxes,” Optics & Laser Technology, vol. 116, pp. 92–102, Aug. 2019, doi: 10.1016/j.optlastec.2019.03.005.

AUTHORS

Dr. Eltyeb Elsamani is an Associate Professor of Computer Science at Al Neelain University, Sudan, where he currently serves as Dean of the Deanship of Admissions and Registration. He earned his Ph.D. in Computer Science (Information Security, Encryption, and Information Hiding) from Al Neelain University in 2009. His research focuses on information security, machine learning, natural language processing, and data mining, with applications ranging from intrusion detection to sentiment and sarcasm analysis in Arabic text. Dr. Elsaman has published in international journals and conferences and has supervised numerous master’s and doctoral students. His recent work explores the use of artificial intelligence for decision support and e-learning systems.

Dr. Yousif Elsamani is a Project Researcher at the Center for Global Commons, Institute for Future Initiatives, University of Tokyo. His research focuses on innovation science and technology management, with a particular emphasis on how technological advances can drive sustainable societal transformation. He develops multilevel conceptual frameworks and applies advanced analytical approaches—including bibliometric analysis and data mining—to examine the intersections of innovation, technology, and sustainability. Dr. Elsamani holds a Ph.D. in Innovation Science from the Tokyo Institute of Technology.