

Analyzing Digital Image Anti-Forensics Techniques and Countermeasures

Saurabh Agarwal¹, Rajeev Kumar^{2,3}, Abha Devi⁴, Ki-Hyun Jung³

¹Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea

²Blockchain Technology Research Lab, Department of Computer Science and Engineering, Delhi Technological University, New Delhi, 110042, India

³Department of Software Convergence, Andong National University, Gyeongbuk, 36729, Republic of Korea

⁴Department of English, JS(PG) College, Sikandrabad, Uttar Pradesh, India

saaurabh@yu.ac.kr, rajeevkumar@dtu.ac.in, abhachauhan17@gmail.com, kingjung@anu.ac.kr

Abstract—With the increasing use of digital media, digital forensics has become a crucial method for ascertaining authenticity and detecting manipulations in images. However, intentional anti-forensic manipulations to hide forensic clues have made verification more difficult. The efforts to develop countermeasures against anti-forensics have contributed to the evolution toward robust techniques in the field of anti-forensics; hence, the development of anti-forensic methods and their respective countermeasures will remain continuous. This work provides a scientometric analysis, a powerful tool for the study of the growth of research output in accordance with time and citation, author, organizational, and keyword co-occurrence analysis. It enhances state-of-the-art analysis by underlining highly influential authors, organizations, and works and stipulates knowledge gaps. This would consequently provide a platform for building a community where insights and inclusiveness among researchers, industry practitioners, and policymakers would all come together to guide their strategies and decisions for innovation in this dynamic field.

Index Terms—Image Forensics, Scientometric Analysis, Image Forgery, Fake Image

I. INTRODUCTION

Mobile phones and computers have become an integral part of life. They correspondingly improve with rapid development in information and communication technology. They bear big personal data in digital format, such as photographs, videos, and messages. They are more susceptible to tampering by resorting to available multimedia tools such as Adobe Photoshop, Corel Photo-Paint, and ACDSee. The ease of accessibility with which such images are manipulated poses a severe challenge. Manipulated images may result in defamation of character or tampered evidence in courts of law. In fact, the distribution of manipulated images can also lead to social unrest or political upheaval. Thus, the authenticity and integrity of digital images are very crucial in today's digital era, pertaining to image forgery attacks like image retouching, image splicing, copy-move, etc. Because of this, two primary methods can be used for digital image forgery detection: an active approach and a passive approach. In an active approach, specific details are embedded in the image so that it can detect

even the slight form of digital tampering. Examples of such can include name, date, signature, and other meta information of the image. This often requires a peculiar system to verify the authenticity of the digital image. In passive methods, duplicated objects in manipulated images are detected without using the original image watermark. Instead, the technique looks for traces left behind due to dissimilar steps involved in the image manipulation process. It can also locate the place and region where the forgery has taken place within the image. The source camera identification and alteration trace analyses are included in passive digital image forensics that verifies image manipulation. These methods take advantage of unique fingerprints left by the acquisition devices or apply signal analysis in order to disclose forgeries. However, these verifications have been complicated by the emergence of anti-forensic techniques that mask traces of manipulation. As a result of these developments, countermeasures against anti-forensics have driven further advancement of robust forensic techniques. This dynamic evolution keeps shaping anti-forensic methods and their countermeasures in the dynamic field of digital image forensics.

Sitara and Mehtre [1] discussed a survey of the anti-forensic domain through passive techniques for image and video tampering detection, along with their respective countermeasures. The authors also pointed out different limitations that have caused anti-forensic methods to grow along with digital forensics. Taneja et al. [2] presented a study related to anti-forensic attacks on JPEG compression, contrast enhancement, and median filtering. Their work presented a robust discussion on methodologies and summarized some existing state-of-the-art methods in tabular form. Al-Fehani and Al-Kuwari [3] discussed image and video forensics, including source identification, forgery detection, and problems arising from generative media. This work has stressed the attacks' liability in using the adversarial and, in turn, motivating the need for more robust methods of forgery detection. They have mentioned the generalized detection technique for forgery and the under-representation of research in GAN detection, in particular

for image forensics. They have also outlined that video anti-forensics, compared to the image, is underrepresented in literature and countermeasures, too. They also talked about the legality of forensic evidence and were motivated to emphasize the justification of the authenticity of the evidence. Some problems arise from the fact that deep learning has started to replace traditional solutions in the understanding of decisions taken by classifiers, being an issue for forensic experts. Their overall review highlighted the changing nature of multimedia forensics and the need for adaptive methods in order to meet several new challenges.

Qureshi and El-Alfy [4] presented a bibliographic review about anti-forensics and relative countermeasures; the goal was to help researchers and practitioners find their place in the current panorama. This review underlines that countering AFMs is an essential task for making forensic techniques reliable against tampering with images. It points out the never-ending conflict between forensic and anti-forensic techniques, which imposes the necessity of constant development and adaptation. The authors firmly believe that new computational methods, such as the addition of dithering noise, have to be explored in order to find adequate countermeasures against emerging anti-forensic strategies. This investigation is based on the finding that the quality of images essentially defines forensic trace concealment. Moreover, they recommend the extension of anti-forensics and related countermeasures research to new fields of video, disk, and network forensics. The work raises questions concerning the reliability and trustworthiness of the existing forensic techniques, proposing a study of relationships among several picture artifact metrics for devising more secure methods. It advocates for thorough benchmark systems, embedding recent deep learning developments, and multi-sensor cameras that will improve forensic capabilities. Finally, the review discusses how cloud computing could support forensic solutions in a scalable way in the future.

More research is needed in the domain of anti-forensics. Only a few papers [1]–[4] present organized research on different anti-forensic schemes. Paper [2] discusses anti-forensic attacks on JPEG, contrast enhancement, and median filtering. It introduces image forgery, JPEG compression, contrast enhancement, and median filtering. After presenting the detailed anti-forensic methods, it shows the current state-of-the-art methodologies in a tabular form for clarity. Al-Fehani and Al-Kuwari, [3] in their work, review some of the recent works on image and video forensics that involve source identification, forgery detection, and challenges from generative media. Anti-forensics and countermeasures will be presented, focusing on the general problem of susceptibility to adversarial attacks. The review also highlights the need for more research on GAN detection, especially in the context of image forensics. Robustness in forgery detection methods is needed. It underlines a promising generalized forgery detection technique and calls for more research related to GAN detection, especially for image forensics. This paper points out that, compared to image forensics, the literature dealing with video anti-forensics and

related countermeasures needs to be revised. It also considers in some depth legal issues with respect to forensic evidence and emphasizes the need for a description of the rationale for the authenticity of evidence. This movement into deep learning methods is at the price of well-understood classification decisions that might concern forensic practitioners. In general, it highlights the dynamic nature of multimedia forensics and the implication for adaptive approaches towards rising challenges. A review [4] on anti-forensics and countermeasures against digital image forensics gives an overview to help researchers and practitioners better understand the status quo in this arena. Therefore, countering AFMs is of vital importance to guarantee that forensic techniques against image tampering are reliable. It realizes the never-ending battle between forensic and anti-forensic techniques and further identifies the need for development and adaptation. It points out that new computational methodologies, such as adding noise with dithering, should be explored to counter emerging anti-forensic strategies successfully. Critical roles of image quality in masking the forensic traces are outlined in this work, and further investigation of the topic is presented. The paper also stresses the importance of extending research studies on anti-forensics and countermeasures to new emerging areas like video, disk, and network forensics, as this will contribute to the development of more secure forensic techniques. Furthermore, it suggests developing comprehensive benchmark systems, integrating deep learning advancements, and using multi-sensor cameras to improve forensic capabilities further. It finally discusses how cloud computing could enable scalable forensic solutions in the near future—surveys [1] anti-forensic techniques relating to passive image and video tampering detection, discussing countermeasures. Limitations within the current literature pertaining to tampering detection are noted, which have led to the development of anti-forensic methods, changing with digital forensics.

We previously examined key survey papers concerning anti-forensics and its countermeasures. In the next section, we will delve into Scientometric Analysis.

II. SCIENTOMETRIC ANALYSIS

This study will help explain productivity, seminal articles, productive authors, and organization and collaboration dynamics in the domain of anti-forensics. Scientometric analysis in research output related to anti-forensics encompasses several steps methodologically: the selection of appropriate bibliographic databases, formulating the search queries, retrieving the literature, and applying scientometric indicators quantifying the impact of research and collaboration patterns. It would naturally also involve a well-articulated search strategy to identify relevant publications, preprocessing for quality and consistency of data, computation of scientometric indicators such as counts of citations, impactful authors networks, and several visualization techniques to interpret.

A. Data Collection and Publication Trend

We have developed an exhaustive dataset of research publications from the WoS repository, one of the world-renowned databases containing exhaustive and quality research content for comprehensive analysis and synthesis of the anti-forensics field. The database includes all major indices, such as SCIE, SSCI, and BKCI-S. The search string (("antiforensic*" OR "counterforensic*" OR "anti-forensic*" OR "counterforensic*" OR ((anti OR counter*) NEAR/3 (forensic*)) AND (JPEG OR image)) yielded 220 publications dealing with research. Manual screening for non-relevant entries brought us to the number of 210 relevant publications that deal with the area. Figure 1 describes the annual progress of anti-forensics research publications that had cropped up as early as 2006. From 2013 onwards, the domain continued to show a significant number of publications throughout the year, except for 2016.

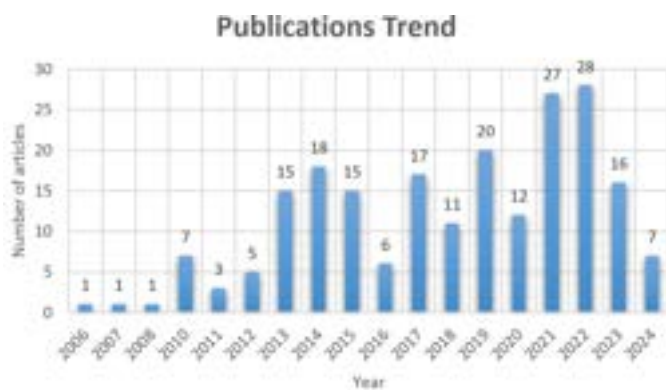


Figure 1. Yearly Publications of Anti-Forensics Research

B. Identification of Top Authors and Organizations with their country

Table I highlights the prominent researchers in the field of anti-forensics, showcasing a diverse group with significant contributions from China (four researchers), Italy (two researchers), and one each from the USA, India, Saudi Arabia, and South Korea. Barni, M. from Italy, leads the list of top contributing authors with six articles. He is followed by Stamm, MC from the USA, and Wu, JY from China, each authoring five articles.

Our analysis of the top contributing organizations, as per Table II, underscores the significant contributions of researchers from China, Italy, the USA, and India to the field of anti-forensics. Univ Maryland, Dept Elect and Comp Engn, College Pk (USA) has published the highest number of articles (8), followed by Beijing Jiaotong Univ, Inst Informat Sci, Beijing (China) with six articles, Drexel Univ, Dept Elect and Comp Engn, Philadelphia (USA) with five articles, and Sun Yat Sen Univ, Sch Informat Sci and Technol, Guangzhou (China) with four articles. Other organizations such as the Univ Siena, Dept Informat Engn and Math (Italy), TIET, Dept Elect and Commun Engn, Patiala, Punjab (India), Univ Siena, Dept Informat

TABLE I
TOP AUTHORS WITH THEIR COUNTRY

Sr. No.	Author	Country	Publications
1	Barni, M	Italy	6
2	Stamm, MC	USA	5
3	Wu, JY	China	5
4	Chen, C	China	4
5	Fahmy, G	Saudi Arabia	4
6	Uddin, K	South Korea	4
7	Chen, ZP	China	3
8	Singh, G	India	3
9	Marra, F	Italy	3
10	Cao, G	China	3
11	Dou, LY	China	3
12	Valenzise, G	Italy	3
13	Ding, F	China	3
14	Kumar, A	India	3
15	Zeng, H	China	3
16	Sameer, VU	India	3
17	Fan, W	France	2
18	Bharathiraja, S	India	2
19	Berthet, A	France	2

Engn and Math, Siena (Italy), Beihang Univ, Sch Comp Sci and Engg. (China), Shenzhen Univ, Shenzhen Key Lab Media Secur, Shenzhen (China), and Shenzhen Univ, Guangdong Key Lab Intelligent Informat Proc, Shenzhen (China) have also made significant contributions.

TABLE II
TOP INSTITUTES WITH NUMBER OF PUBLICATIONS

Sr. No.	Institute	Publications
1	Univ Maryland, Dept Elect & Comp Engn, College Pk, MD 20742 USA	8
2	Beijing Jiaotong Univ, Inst Informat Sci, Beijing 100044, China	6
3	Drexel Univ, Dept Elect & Comp Engn, Philadelphia, PA 19104 USA	5
4	Sun Yat Sen Univ, Sch Informat Sci & Technol, Guangzhou, China	4
5	Univ Siena, Dept Informat Engn & Math, I-53100 Siena, Italy	3
6	TIET, Dept Elect & Commun Engn, Patiala, Punjab, India	3
7	Univ Siena, Dept Informat Engn & Math, Siena, Italy	3
8	Beihang Univ, School of Comp Sci & Engn, Beijing 100191, China	3
9	Shenzhen Univ, Shenzhen Key Lab Media Security, Shenzhen, China	3
10	Shenzhen Univ, Guangdong Key Lab Intelligent Info Proc, Shenzhen, China	3

C. Document citation linkages

A full-scale VoS analysis was performed on the WoS corpus for research related to anti-forensics, which covered 210 published documents. This paper analyzed the citations among those documents using a full counting method that had to be at least two citations each. It identified the top ten cited documents, including their total citations, publication venues, and the years of publication. The paper spearheads the list "Do GANs Leave Artificial Fingerprints?" with 127

TABLE III
MOST CITED ARTICLES WITH PUBLICATION VENUE AND NUMBER OF CITATIONS

No.	Authors	Title	Venue	Year	Citations
1	Marra et al.	Do GANs Leave Artificial Fingerprints?	IEEE MIPR, 2019	2019	[5]
2	Cao et al.	Forensic detection of median filtering	IEEE ICME, 2010	2010	[6]
3	Ansari et al.	Fluorescent materials for fingerprints detection	Coord. Chem. Rev., Elsevier	2022	[7]
4	Stamm et al.	Anti-forensics of JPEG compression	IEEE ICASSP, 2010	2010	[8]
5	Ding et al.	Anti-Forensics for Face Swapping Videos	IEEE Trans. on Multimedia	2021	[9]
6	Stamm et al.	JPEG Compression Anti-forensics	IEEE ICIP	2010	[10]
7	Cao et al.	Anti-Forensics of Contrast Enhancement	MM&Sec '10	2010	[11]
8	Fan et al.	JPEG anti-forensics via variational approach	IEEE ICASSP, 2013	2013	[12]
9	Wu et al.	Anti-forensics of median filtering	IEEE ICASSP, 2013	2013	[13]
10	Valenzise et al.	JPEG compression anti-forensics cost	IEEE ICASSP, 2011	2011	[14]

citations. Next is "Forensic Detection of Median Filtering in Digital Images" by Cao et al., which secured the second position with 107 citations. The document "Recent Progress of Fluorescent Materials for Fingermarks Detection in Forensic Science and Anti-counterfeiting" by Ansari et al. has been cited 88 times, hence placing third. The last five documents in Table III have less than 50 citations each. A key observation from this analysis is the crucial role of IEEE and conferences in promoting highly influential research work in the anti-forensics domain. The majority of high-impact papers are by IEEE, and a large fraction of them are conference papers. This underlines key works and highly influential papers that establish these publications as essential milestones in pushing the research frontier on anti-forensics.

D. Keyword Co-occurrence Networks

Figure 2 illustrates the co-occurrence networks of keywords in the anti-forensics domain based on a comprehensive analysis of the Web of Science (WoS) document corpus. The WoS search identified 649 unique keywords, with the study focusing on 140 keywords that appeared at least twice.

The co-occurrence grids are color-coded to represent different clusters:

- Cyan: The keyword "anti-forensics" forms the most significant node, frequently co-occurring with "privacy," "security," and "disk forensics."
- Blue: This network centers around "digital forensics," indicating a significant research thrust in this area.
- Yellow: Keywords related to "image forensics" dominate this cluster, highlighting its prominence in the field.
- Green: The "forensics" keyword forms the core of this cluster, encompassing a broad range of related topics.

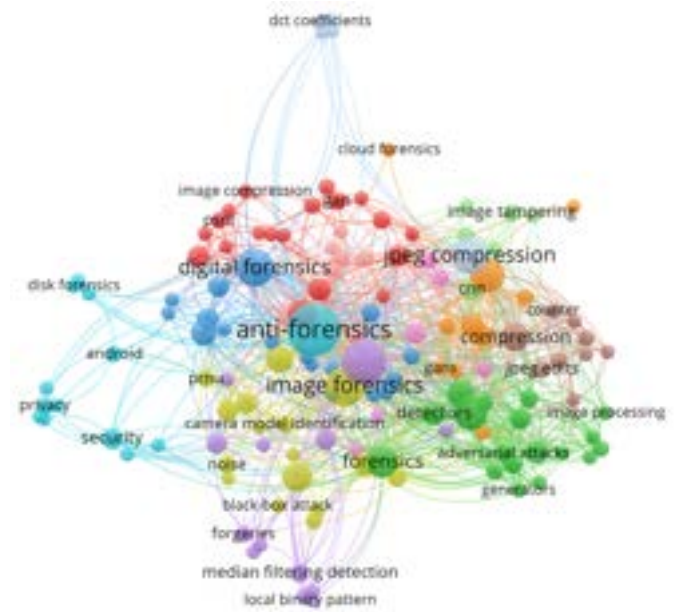


Figure 2. Keyword Co-occurrence Networks in Anti-Forensics Research

- Smaller Clusters: These include frequent keywords such as "CNN," "cloud forensics," "forgery," "local binary pattern," and "compression," each forming distinct, smaller clusters.

The visualization provides insights into the interconnectedness and primary focus areas within the anti-forensics research landscape.

III. CONCLUSION

This scientometric analysis explains the overall growth and path of anti-forensic research, outlining the significant trends and contributions that have set a mark in the area. Growth in publication since 2006 steepens in 2013, reflecting the rising importance and complexity of digital forensics as a response against advanced challenges caused by digital manipulation. In this respect, the study identifies significant contributors from institutions worldwide, especially in the USA, China, and Italy, which are driving the research and development of new methods to respond to both established and new threats. Citation analysis has shown how keynote works, published for the most part through IEEE venues, attest to the quality of research and the pivotal role of IEEE conferences in the dissemination of critical anti-forensic studies. Keyword analysis returns a dynamic network of themes, such as "privacy," "security," and "forensics," which is necessary to understand the focus of the field and to integrate diverse research areas into effective anti-forensic strategies.

ACKNOWLEDGMENT

This research was supported by Brain Pool program funded by the Ministry of Science and ICT through the National

Research Foundation of Korea (2021H1D3A2A01099390) and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2021R111A3049788).

REFERENCES

- [1] K. Sitara and B. M. Mehtre, "Anti-forensics for image and video tampering: A review," in *Cryptographic and Information Security*. Boca Raton, Florida: CRC Press, [2019], pp. 799–827.
- [2] N. Taneja, V. S. Bramhe, D. Bhardwaj, and A. Taneja, "Understanding digital image anti-forensics: an analytical review," *Multimed Tools Appl*, vol. 83, no. 4, pp. 10445–10466, Jan. 2024.
- [3] M. Al-Fehani and S. Al-Kuwari, "Recent advances in digital image and video forensics, anti-forensics and counter anti-forensics," Feb. 2024, [Online]. Available: <http://arxiv.org/abs/2402.02089>.
- [4] M. A. Qureshi and E. M. El-Alfy, "Bibliography of digital image anti-forensics and anti-anti-forensics techniques," *IET Image Process*, vol. 13, no. 11, pp. 1811–1823, Sep. 2019.
- [5] F. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, "Do gans leave artificial fingerprints?" in *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*. IEEE, 2019, pp. 506–511.
- [6] G. Cao, Y. Zhao, R. Ni, L. Yu, and H. Tian, "Forensic detection of median filtering in digital images," in *2010 IEEE International Conference on Multimedia and Expo*. IEEE, 2010, pp. 89–94.
- [7] A. A. Ansari, K. M. Aldajani, A. N. AlHaza, and H. A. Albrithen, "Recent progress of fluorescent materials for fingermarks detection in forensic science and anti-counterfeiting," *Coordination Chemistry Reviews*, vol. 462, p. 214523, 2022.
- [8] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Anti-forensics of jpeg compression," in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, Mar. 2010, pp. 1694–1697.
- [9] S. Bharathiraja and B. Rajesh Kanna, "Anti-forensics contrast enhancement detection (afced) technique in images based on laplace derivative histogram," *Mobile Networks and Applications*, vol. 24, no. 4, pp. 1174–1180, Aug. 2019.
- [10] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. R. Liu, "Undetectable image tampering through jpeg compression anti-forensics," in *2010 IEEE International Conference on Image Processing*. IEEE, 2010, pp. 2109–2112.
- [11] G. Cao, Y. Zhao, R. Ni, and H. Tian, "Anti-forensics of contrast enhancement in digital images," in *Proceedings of the 12th ACM Workshop on Multimedia and Security*, 2010, pp. 25–34.
- [12] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "A variational approach to jpeg anti-forensics," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, May 2013, pp. 3058–3062.
- [13] Z.-H. Wu, M. C. Stamm, and K. J. R. Liu, "Anti-forensics of median filtering," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, May 2013, pp. 3043–3047.
- [14] G. Valenzise, M. Tagliasacchi, and S. Tubaro, "The cost of jpeg compression anti-forensics," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, May. 2011, pp. 1884–1887.