Advanced Pharmaceutical Bulletin

Adv Pharm Bull. 2024;14(4):722-728
doi: 10.34172/apb.44002
https://apb.tbzmed.ac.ir

TUOMS PRESS

Editorial

A Decade in Hijacked Journals: What Will be the Future Trend?

Mihály Hegedűs[1,2], Mehdi Dadkhah[3*], Lóránt Dénes Dávid[4,5,6,7]

[1]Department of Finance and Accounting, Tomori Pál College, Budapest, Hungary.
[2]Chamber of Hungarian Auditors, Budapest, Hungary.
[3]Department of Sustainable Tourism, Institute of Rural Development and Sustainable Economy, Hungarian University of Agriculture and Life Sciences (MATE), Gödöllő, Hungary.
[4]Department of Tourism and Hospitality, Faculty of Economics and Business John von Neumann University, Kecskemét, Hungary.
[5]Department of Sustainable Tourism, Institute of Rural Development and Sustainable Economy, Hungarian University of Agriculture and Life Sciences (MATE), Gödöllő, Hungary.
[6]Savaria Department of Business Economics, Savaria University Centre, Faculty of Social Sciences, Eötvös Loránd University, Szombathely, Hungary.
[7]Department of Tourism and Hospitality, Kautz Gyula Faculty of Business and Economics, Széchenyi István University, 9026 Győr, Hungary.

Article info

Article History:
Received: November 28, 2024
Accepted: December 2, 2024
epublished: December 5, 2024

Keywords:
Hijacked journals, Medicine, Bibliometrics, Publication ethics, Artificial intelligence, Sustainable development goals, Circular economy, Circular society

Abstract

Purpose: Hijacked journals are fraudulent websites that mimic legitimate journals and, by charging authors, publish manuscripts. The current editorial endeavors to provide a close view of current literature. This editorial piece analyzes 10 years of research on hijacked journals and endeavors to shed light on future trends.

Methods: Current research uses a bibliometric approach to analyze data and discuss results. The OpenAlex has been used for data collection. Some of the data analysis was conducted using OpenAlex. The other study was done using Bibliometrix, and the date is limited to publication between 2014 and 2024.

Results: The findings provide a close view of the published literature in terms of access type, growth, topics, most frequent words, country contribution, top publishers, and alignment of literature with sustainable development goals.

Conclusion: The gap in current literature is the limitation in easily usable methods to be accessible by all researchers for hijacked journal detection and data analysis. The use of artificial intelligence can be promising.

Introduction

There is literature about hijacked journals, and this phenomenon has been discussed in various papers. The term "hijacked journals" describes fraudulent activity in which a second illegal web domain(s) (or URL) mimics the original website of a legitimate journal to deceive researchers. In this scam, hackers promote the illegal web address as the original websites of journals, then by charging authors, publish manuscripts without peer review.[1,2] The history of hijacked journals comes back to about 2011, when a cybercriminal registered an expired domain "sciencerecord.com" and launched three hijacked journals "Science Series Data Report", "Innova Ciencia", and "Science and Nature" in 2012 after another hijacked journal "Archives des sciences" that was online in 2011.[3] From that date till now, there have been many cases of journal hijacking, from simple to advanced ones. There are hijacked journals by just launching a similar web domain to original journals or more advanced ones that use the old domain of indexed journals. In some advanced types of journal hijacking, the content can be indexed in Scopus.[1] In 2024, we published some editorials on this topic to increase awareness of potential audiences in *Advanced Pharmaceutical Bulletin.*[4,5] However, it seems that the phenomenon of journal hijacking will not be stopped. Conversely, hijacked journals are becoming increasingly extensive and complex. This editorial piece analyzes 10 years of research on hijacked journals and endeavors to shed light on future trends.

Methods

Current research uses a bibliometric approach to analyze data and discuss results. Based on Van Leeuwen, "Bibliometrics is the field of science that deals with the development and application of quantitative measures and indicators for sciences and technology based on

***Corresponding Author:** Mehdi Dadkhah, Email: d_mehdi@av.amrita.edu

bibliographic information".[6] The OpenAlex (https://openalex.org) has been used for data collection. OpenAlex is a comprehensive database that provides extensive access to literature and allows for a systematic review of literature.[7] It also provides options for some primary analysis of the provided data. Many studies used OpenAlex to collect related data.[8–10] Some of the analysis of the data was conducted by using OpenAlex. other part of study has been done by using Bibliometrix, a tool in the R programming language for bibliometric analysis.[11] The term "hijacked journal*" has been searched in OpenAlex, and the date is limited to publication between 2014 and 2024. OpenAlex provided more results than other citation bases when searching for publications on the topic of hijacked journals. Because results contain papers that include the keyword "hijacked journal" in any sections of the paper, not only the title, abstract, and keywords.

Result and Discussion

The analysis of access types to full texts indicates that nearly 70 percent of publications are open-access (Figure 1). It means that hijacked journals are more concerned with open-access journals than subscription ones. It may be due to hijacked journals usually mimicking open-access journals. Free access to papers on the topic of hijacked journals and their detections can be valuable because it allows the free sharing of related literature and eliminates the number of victims. The number of papers is variants in each year, but there was an increase in 2015 that highlights a concern about the challenges of hijacked journals (Figure 2).

The primary topics of most papers are bibliometrics, literature reviews, academic misconduct, or phishing attacks (Figure 3). The papers mentioned hijacked journals as the source of unreliable data and tried to warn about such papers to exclude from citation or provide guidelines for authors to prevent from publishing in these journals.[12-14] These publications endeavor to increase awareness about the bad practices of hijacked journals by introducing this phenomenon, the consequences of publishing in these journals, providing methods for detection of them, etc. The naming of hijacked journals as phishing attacks is another main theme. Both phishing attacks and hijacked journals use identity theft and mimic the original legitimate domain.[15] The concept of hijacked journals has technical, ethical, and criminal aspects. Academic misconduct, flaws in website structures, and criminal activity shape a hijacking attack. This concept has potential for future research, as current inspection shows that most of the current literature is classified as an article (Figure 4). It means that the hijacked journals' literature requires more than just providing public awareness, and needs research on providing solutions, evaluating current hurt, considering information security aspects, etc.

As shown in Figure 5, Springer Nature, Wiley, Springer Science, Elsevier, and Emerald are the top five publishers on the topics. It highlights the importance of topics. Since most of the hijacked journals have been published by small publishers, addressing the issue of hijacked journals by standout publishers shows the concern of these publishers about the growth of hijacked journals and the dissemination of non-peer review science into the literature.

The published papers on the topic of hijacked journals usually contribute to sustainable development goals (SDG) provided by the United Nations.[16,17] The top SDGs are "peace, justice, and strong institutions", "quality education", and "gender equality" (Figure 6). The hijacked journals publish non-peer-reviewed science and compromise the integrity of the scientific record.[1,3] This can hurt the trust of academic institutes. Hijacked journals charge authors[3] (and sometimes readers); This can create financial strain and exacerbate existing inequalities. This journal deceives researchers, and as their paper will be published in non-legitimate journals, the author's scientific careers will face challenges. Hijacked journals waste authors' efforts, time, and institutes' budgets. These journals do not meet academic standards and negatively impact the quality of education. These journals can hurt the integrity of science in various disciplines, especially

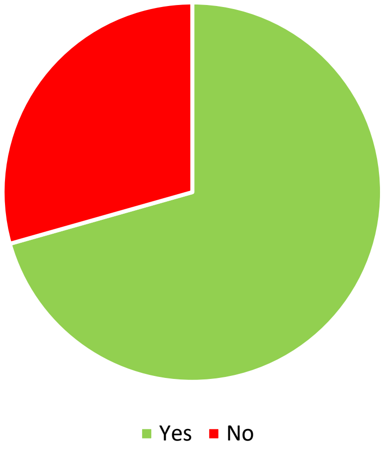

Figure 1. Number of open-access papers

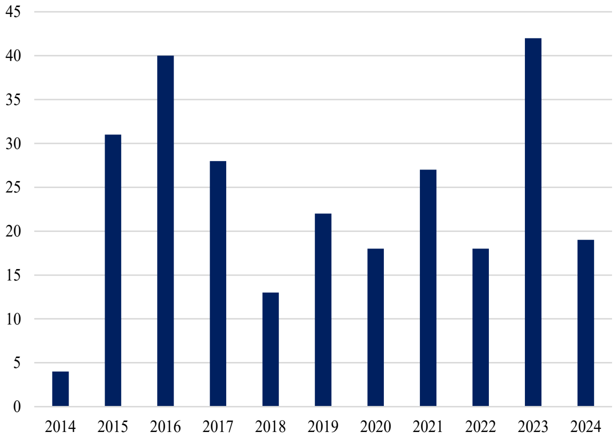

Figure 2. Published papers per year

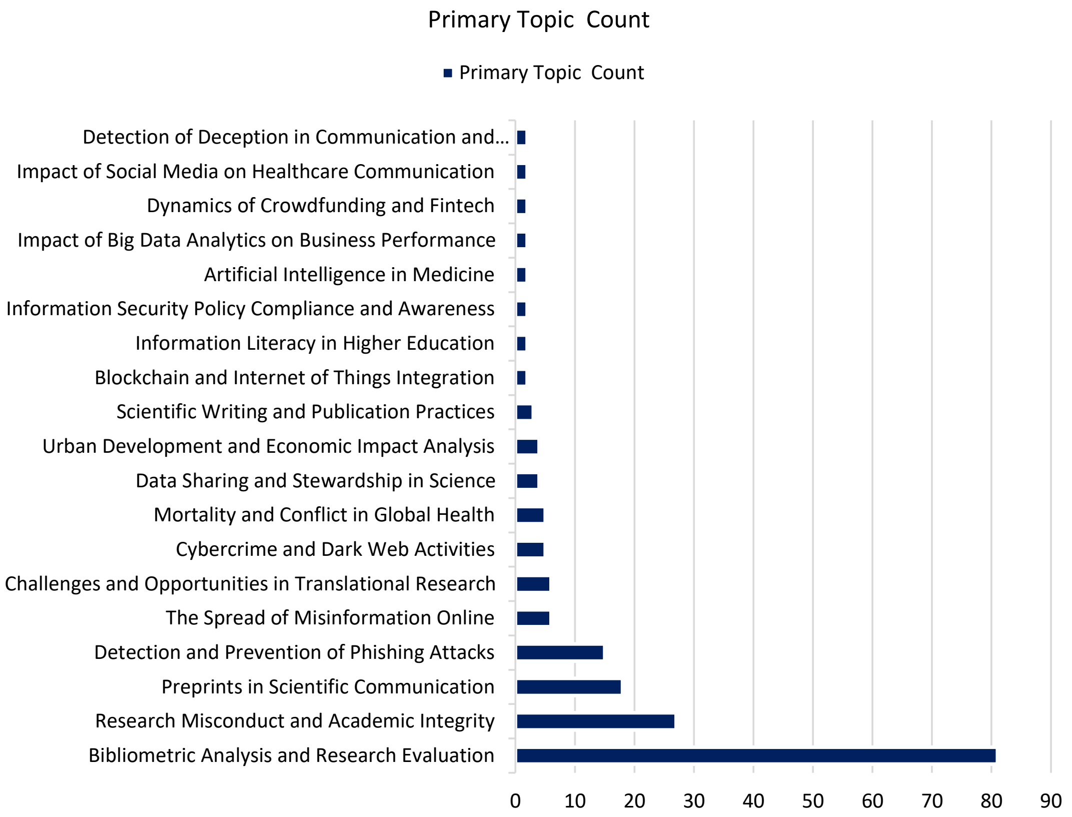

Figure 3. Primary topics in published papers

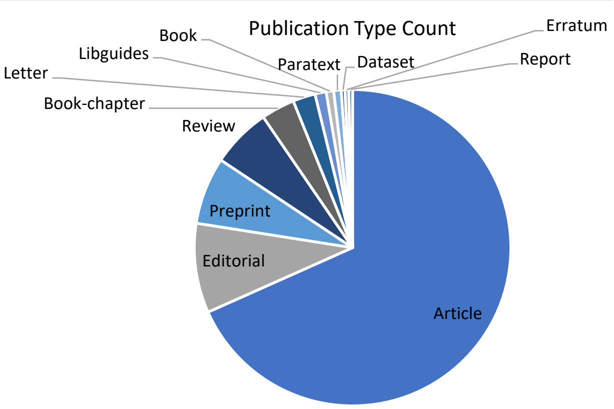

Figure 4. Publication Type

health science, with negative consequences for public health, environmental protection, and social policy.[18-20] The published papers by hijacked journals are a warning for sustainable development; a study shows that the content published in hijacked journals can contribute to SDGs, but they are non-peer reviews so, they can disseminate misinformation or hurt institution ranks.[21]

Figures 7 and 8 show the top frequent keywords and words co-occurrence in sequence. They somewhat provide similar concepts such as the primary topics of published papers, but there are keywords about the hijacked journals detection. The keywords bot detection, impact factor, plagiarism, spam detection, phishing, citation analysis, and similar keywords emerged due to available publications on the topic of hijacked journal detection or prevention. The spam call for papers is key for most hijacked journals to find potential victims.[22] They are analyses of citations to hijacked journals and plagiarism or similarity analysis to find a network of hijacked journals.[23,24] The evidence indicates that some hijacked journals use the same content as each other.[23] The hijacked journals may use bogus impact factors to look legitimate or gain more visibility, especially among authors from developing countries.[25,26] Some research considers hijacked journals similar to phishing attacks and presents methods for the detection of them.[15] There are machine learning or artificial intelligence-based methods for hijacked journal detection.[5] However, the simplest method that can be used is a list of hijacked journals. The most recent and updated one is the Retraction Watch Hijacked Journals Checker (RWHJC), which is regularly updated.[27]

The majority of publications about hijacked journals are from Iran, the USA, and India. A limited number of authors are dedicated to the continuous research of this topic. This means that this field is looking for continued research and funding support to grow (Figure 9).

The dark side

Despite considerable research on the topic, hijacked journal literature still presents certain drawbacks. The

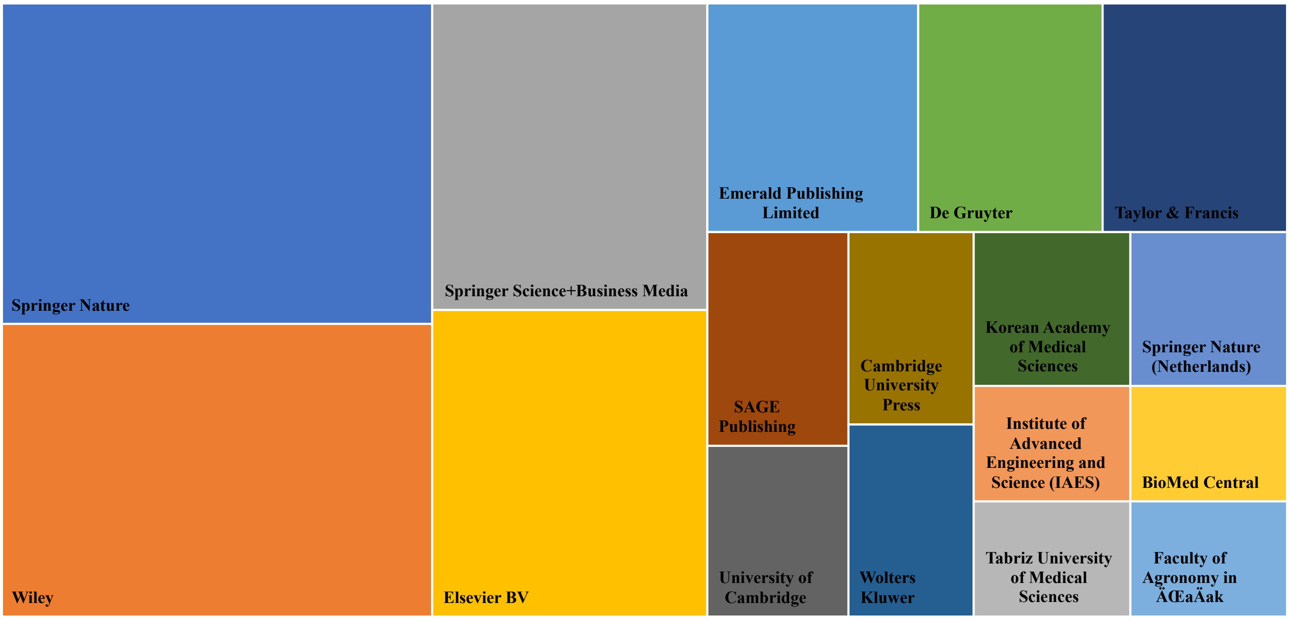

Figure 5. Top publishers

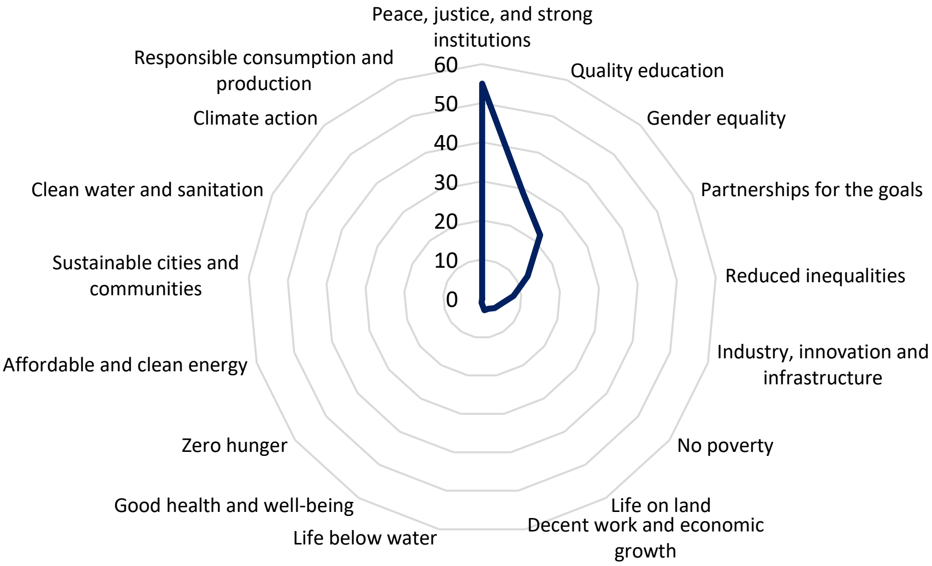

Figure 6. Alignment with sustainable development goals

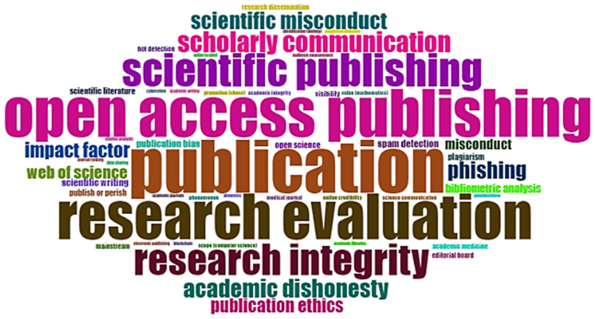

Figure 7. Word cloud

current number of hijacked journals remains unclear due to the complexity of their detection process. The growth rate of this journal is not clear, as there are hijacked journals that disappeared after launching without any detection. It's unclear how many hijacked journals have indexed their content in citation bases, and we don't know how many of these journals are indexed in reputable databases. The total number of citations to published manuscripts in hijacked journals is not accessible. We have not yet inspected the patent-based citations to published papers in hijacked journals. Addressing the many open questions surrounding hijacked journals is necessary.

The future solution

It seems that the use of AI for dealing with hijacked journals can be promising. AI can be used to develop interactive chatbots for users and help them query

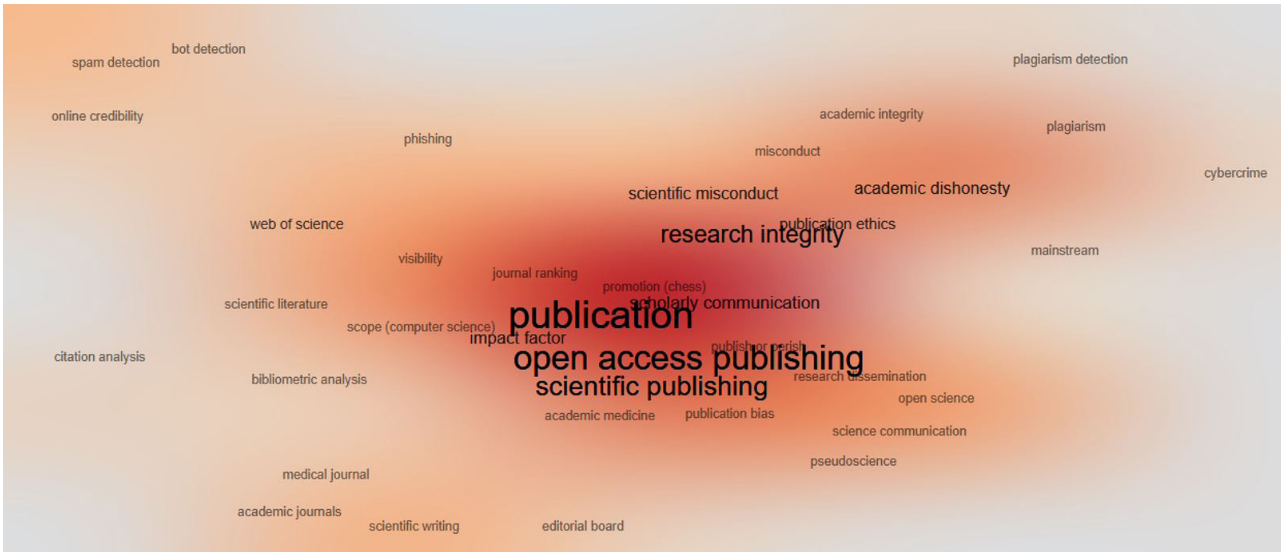

Figure 8. Co-occurrence Network

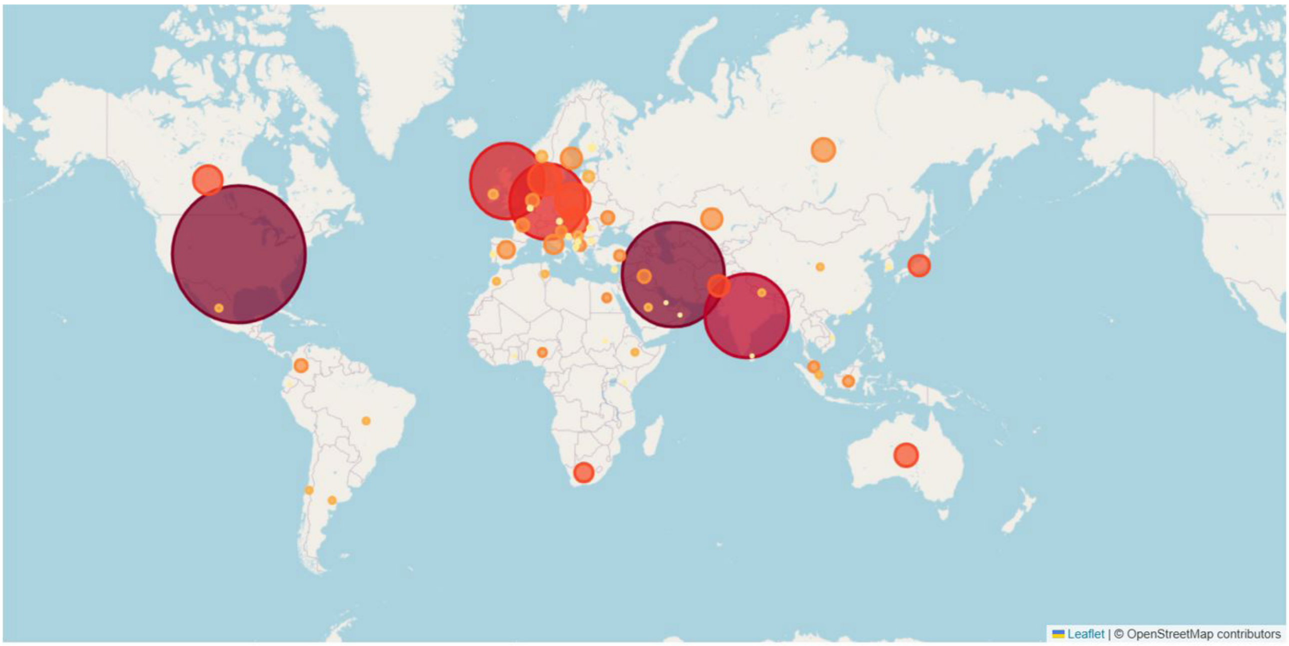

Figure 9. Authors' countries (visualization made with Poe and AI, based on extracted data)

journals and analyze possible ones against some criteria to ensure a journal is hijacked or original. The anonymized transferred data from users' accounts can be analyzed to detect potential hijacked journals. Some studies indicate that most of the victims of hijacked journals are from certain countries or even certain research institutes[4,21]; when queries about a certain journal from a geographic area increase in an AI chatbot, the potentially questionable journals can be detected and several victims will be eliminated. The AI tool can be used to find suspected calls for papers and label them as fraud. The AI tool can be developed to analyze data in citation bases and find potential indexes from the side of hijacked journals. All of these are topics for future research and request efforts, time, and budgets. Figure 10 illustrates current literacy on the topic of hijacked journals and future potential in a simple manner.

Conclusion

Various papers in the literature discuss hijacked journals and try to increase the awareness of authors and eliminate victims. However, there is a lack of papers to direct future research. It seems that the literature on hijacked journals is mature, but this consideration is not true. Most papers only introduce the current harm of hijacked journals or methods for detection of them, but no easily usable tool is available to all researchers. The current editorial tried to provide a close view of the current literature and provide some key trends for future research in this area.

The majority of analyses in this edition are based on

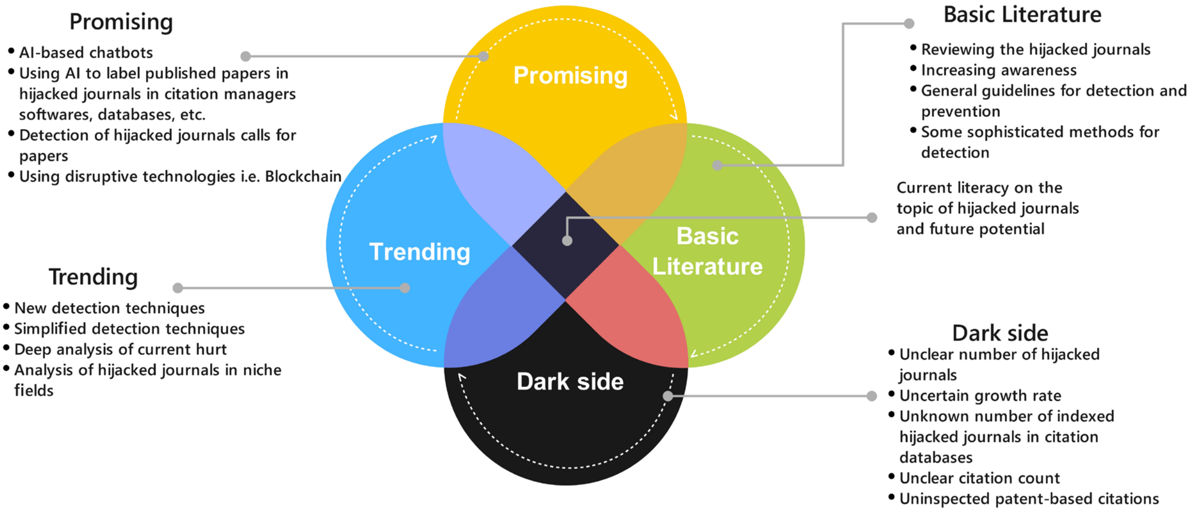
Promising
• AI-based chatbots
• Using AI to label published papers in hijacked journals in citation managers softwares, databases, etc.
• Detection of hijacked journals calls for papers
• Using disruptive technologies i.e. Blockchain
Trending
• New detection techniques
• Simplified detection techniques
• Deep analysis of current hurt
• Analysis of hijacked journals in niche fields
Basic Literature
• Reviewing the hijacked journals
• Increasing awareness
• General guidelines for detection and prevention
• Some sophisticated methods for detection
Current literacy on the topic of hijacked journals and future potential
Dark side
• Unclear number of hijacked journals
• Uncertain growth rate
• Unknown number of indexed hijacked journals in citation databases
• Unclear citation count
• Uninspected patent-based citations
Promising
Trending
Basic Literature
Dark side

Figure 10. Current literacy on the topic of hijacked journals and future potential

a data science approach and maybe some tolerances in value. Also, we used OpenAlex to cover the most possible extent of published contents; it means that some papers completely contribute to hijacked journal literature and this contribution for some papers may be limited.

AI Usage

The AI tools have been used to improve readability in some parts of the paper. The other usage of AI tools has been declared in the methodology section.

Acknowledgments

Authors would like to thank the Flagship Research Groups Programme of the Hungarian University of Agriculture and Life Sciences (MATE).

Authors' Contribution

Conceptualization: Mehdi Dadkhah, Mihály Hegedűs, Lóránt Dénes Dávid.
Data curation: Mehdi Dadkhah, Mihály Hegedűs.
Formal analysis: Mihály Hegedűs, Mehdi Dadkhah, Lóránt Dénes Dávid.
Investigation: Mehdi Dadkhah, Mihály Hegedűs, Lóránt Dénes Dávid.
Methodology: Mehdi Dadkhah, Lóránt Dénes Dávid, Mihály Hegedűs.
Project administration: Mehdi Dadkhah, Lóránt Dénes Dávid.
Resources: Lóránt Dénes Dávid
Software: Mehdi Dadkhah.
Supervision: Lóránt Dénes Dávid.
Validation: Mihály Hegedűs, Mehdi Dadkhah, Lóránt Dénes Dávid.
Writing–original draft: Mihály Hegedűs, Mehdi Dadkhah.
Writing–review & editing: Lóránt Dénes Dávid.

Competing Interests

None declared.

Ethical Approval

Not applicable.

Funding

This work was supported by the Flagship Research Groups Programme of the Hungarian University of Agriculture and Life Sciences (MATE).

References

1. Abalkina A. Challenges posed by hijacked journals in Scopus. *J Assoc Inf Sci* Technol2024;75(4):395-422. doi: 10.1002/asi.24855
2. Graber ML, Plebani M. The growing threat of hijacked journals. *Diagnosis (Berl)* 2024;11(3):219. doi: 10.1515/dx-2024-0103
3. Jalalian M, Dadkhah M. The full story of 90 hijacked journals from August 2011 to June 2015. *Geogr Pannon* 2015;19(2):73-87. doi: 10.18421/gp19.02-06
4. Dadkhah M, Hegedűs M, Nedungadi P, Raman R, Dávid LD. Unveiling the hidden menace: a topic modeling analysis of hijacked medical journals. *Adv Pharm Bull* 2024;14(2):255-61. doi: 10.34172/apb.2024.029
5. Dadkhah M, Oermann MH, Hegedüs M, Raman R, Dávid LD. Diagnosis unreliability of ChatGPT for journal evaluation. *Adv Pharm Bull* 2024;14(1):1-4. doi: 10.34172/apb.2024.020
6. van Leeuwen T. Descriptive versus evaluative bibliometrics. In: Moed HF, Glänzel W, Schmoch U, eds. *Handbook of Quantitative Science and Technology Research: The Use of Publication and Patent Statistics in Studies of S&T Systems*. Dordrecht: Springer; 2005. p. 373-88. doi: 10.1007/1-4020-2755-9_17.
7. Hazarika R, Roy A, Sudhier KG. Mapping the open access publications of Indian non-profit organizations over the last 20 years based on OpenAlex insights. *Glob Knowl Mem Commun* 2024. doi: 10.1108/gkmc-02-2024-0106
8. Goncharova M, Sokolova E. Scientific review of climate science: a bibliometric analysis of trends. In: *E3S Web of Conferences*. Vol 542. EDP Sciences; 2024. p. 04008.
9. Okamura K. Atlas of science collaboration, 1971-2020. *SN Comput Sci* 2024;5(5):640. doi: 10.1007/s42979-024-02973-4
10. Bredahl L. Introduction to bibliometrics and current data sources. *Libr Technol Rep* 2022;58(8):5-11.
11. Aria M, Cuccurullo C. *bibliometrix*: an R-tool for comprehensive science mapping analysis. *J Informetr* 2017;11(4):959-75. doi: 10.1016/j.joi.2017.08.007
12. Abid HA, Yousif EA. Hijacked journals: tips for young researchers, to detect and avoid them. *Baghdad J Biochem Appl Biol Sci* 2022;3(4):232-6. doi: 10.47419/bjbabs.v3i04.179

13. Watson R. Hijackers on the open access highway. *Nurs Open* 2015;2(3):95-6. doi: 10.1002/nop2.36
14. Shen C, Shah L. Predatory publishing practices: what researchers should know before submitting their manuscript. *Insights UKSG J* 2023;36(6):19. doi: 10.1629/uksg.631
15. Ahmed M, Altamimi AB, Khan W, Alsaffar M, Ahmad A, Khan ZH, et al. PhishCatcher: client-side defense against web spoofing attacks using machine learning. *IEEE Access* 2023;11:61249-63. doi: 10.1109/access.2023.3287226
16. Raman R, Lathabai HH, Nedungadi P. Sustainable development goal 12 and its synergies with other SDGs: identification of key research contributions and policy insights. *Discov Sustain* 2024;5(1):150. doi: 10.1007/s43621-024-00289-0
17. Raman R, Lathabai HH, Patwardhan A, Harikumar S, Nedungadi P. Top 100 highly cited sustainability researchers. *Heliyon* 2024;10(7):e28604. doi: 10.1016/j.heliyon.2024.e28604
18. Moussa S. A "Trojan horse" in the reference lists: citations to a hijacked journal in SSCI-indexed marketing journals. *J Acad Librariansh* 2021;47(5):102388. doi: 10.1016/j.acalib.2021.102388
19. Jalalian M. Hijacked journals are attacking the reliability and validity of medical research. *Electron Physician* 2014;6(4):925-6. doi: 10.14661/2014.925-926
20. Jalalian M, Mahboobi H. Hijacked journals and predatory publishers: Is there a need to re-think how to assess the quality of academic research? *Walailak J Sci Technal* 2014;11(5):389-94. doi: 10.14456/wjst.2014.16
21. Dadkhah M, Hegedűs M, Dávid LD. Unmasking greenwashing: mapping hijacked medicine journals to the sustainable development goals. *Adv Pharm Bull* 2024;14(4):1-11. doi: 10.34172/apb.43763
22. Asadi A, Rahbar N, Asadi M, Asadi F, Khalili Paji K. Online-based approaches to identify real journals and publishers from hijacked ones. *Sci Eng Ethics* 2017;23(1):305-8. doi: 10.1007/s11948-015-9747-9
23. Abalkina A. Detecting a network of hijacked journals by its archive. *Scientometrics* 2021;126(8):7123-48. doi: 10.1007/s11192-021-04056-0
24. Abalkina A. Prevalence of plagiarism in hijacked journals: a text similarity analysis. *Account Res* 2024:1-19. doi: 10.1080/08989621.2024.2387210
25. Gutierrez FR, Beall J, Forero DA. Spurious alternative impact factors: the scale of the problem from an academic perspective. *Bioessays* 2015;37(5):474-6. doi: 10.1002/bies.201500011
26. Jalalian M. The story of fake impact factor companies and how we detected them. *Electron Physician* 2015;7(2):1069-72. doi: 10.14661/2015.1069-1072
27. Retraction Watch. The Retraction Watch Hijacked Journal Checker. 2024. Available from: https://retractionwatch.com/the-retraction-watch-hijacked-journal-checker/.