Reliability of Hijacked Journal Detection Based on Scientometrics, Altmetric Tools and Web Informatics: A Case Report Using Google Scholar, Web of Science and Scopus

Mohammad R. Khosravi1, Varun G. Menon2*
1Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz, Iran
2Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Kerala 683582, India

Emails: m.khosravi@sutech.ac.ir; varunmenon@scmsgroup.org

Abstract: This short paper presents a case report on detecting hijacked journals. Towards identification of a fake journal website and preventing a hijacked paper, we can use different tools including Google Scholar (an altmetric tool), Web of Science (WoS) and Scopus (both as scientometric databases) to distinguish a fake website from a legal journal website. Our evaluation shows that analysis of a doubtful website for a targeted journal based on Google Scholar is not reliable. In fact, the use of scientometric tools for tracking prior publications of the targeted journal is compulsory. Another result of this case study is that in some uncommon cases, fake websites may sometimes convince a scientometric database in order to be partially indexed along with an abstracting of their hijacked papers while these websites steal identity of the legal journals. Therefore as a results, we should check both of WoS and Scopus for verifying a fake website at the same time to obtain more reliability.

Keywords: Hijacking, Web of Science (WoS), Scopus, Web Informatics, Ethics and Moral Issues.

1. INTRODUCTION
Predatory journals and publishers have been a major threat to academic research community for many years [1]-[3]. The major challenge for researchers always is to identify and eliminate these predatory journals. Since the last few years, a similar type of fake publishers with many hijacked journals have attacked the research community in a big way. Hijacked journals are indeed versions with fake identity for legitimate academic journals such that some duplicate/fake websites are created by malicious third party or criminals. Probably, a different type of Phishing attack is done by these fake websites to find some academicians as victim. These fake websites copy all the contents available in the website of the legitimate journal like Impact Factor (IF), ISSN number, Editorial Board Members (EBMs) information, and indexing and archiving information. They then send attractive calls for papers to researchers all over the world inviting them to publish with these fake journals for a high fee (but normally these fees are not much high compared to fees of legal open access journals in that area). These attackers particularly target the researchers in desperate need for publications. With the concept of Publish or Persih existing in many countries, many academicians fall in this trap. Authors receiving these emails are attracted by the indexing information like Scopus, Web of Science (WoS) or the IF value of the journal. They then click on the link of the hijacked version of the journal given in the email and proceed with a submission, and a short time later with payment of the authors' fees, and finally publication of their papers. Thus money, time and the research work would be lost forever through these fake websites [4]-[6].

Currently, the academic community is in a dilemma, and unable to efficiently resolve this problem. Many right persons have started to display the list of fake journals in their own websites to help potential authors, however having a general guideline to reveal any new case is more of interest which is tried to be handled in this paper. The objective of us here is to show the research community how duplicate/fake journals can be identified using Google Scholar, Web of Science and Scopus through a case study. We believe that the idea behind this paper would become a valuable reference for all the researchers [7]-[10].

The rest of this paper is organized as follows. First, the case study will be discussed, then we try to verify its identity through different tools. At the end, a conclusion on the work will be given.
2. CASE STUDY

In this study, we aim to evaluate a major databases-indexed journal entitled *Journal of Engineering Technology* (JET). This journal has some features which make it suitable for hijacking, see Table 1 for more details. According to Scopus/ScimagoJR in 2019, “JET is a refereed journal published semi-annually, in spring and fall, by the Engineering Technology Division (ETD) of the American Society for Engineering Education (ASEE), and is indexed by the Engineering Index (EI) Compendex and the Science Citation Index (SCI). The journal was first published in 1984 and has since become one of the major publication venues of refereed scholarly works for engineering technology educators. The purpose of the *Journal of Engineering Technology* is spelled out in the JET Editorial Policy document”. In Figures 1 and 2, some papers published in a fake website for this journal are observable.

Table 1. A hijacked journal for case study (data was collected in Dec. 2018)

| Journal Name                      | Indexing          | ISSN       | Original Website | Fake Website      |
|----------------------------------|-------------------|------------|------------------|-------------------|
| Journal of Engineering Technology * | WoS (SCIE/JCR)   | 0747-9964  | N/A***           | http://www.joetsite.com |
|                                  | Scopus            |            |                  |                   |
|                                  | EBSCO             |            |                  |                   |

* This journal mainly publishes extended versions of some conference papers presented at conferences of American Society for Engineering Education (ASEE).

** We could not find it, however it seems that the website does not exist. Only some of titles published by real journal can be found as conference versions on the ASEE website; for example see the case ordered as 7th in Figure 7 (by Sriraman et al., 2017) via this link (https://www.asee.org/public/conferences/78/papers/17663/view#).

*** Based on Scopus record through ScimagoJR, the main website of this journal is (https://www.engtech.org/jet), however we cannot approve it.

Figure 1. Fake website for the *Journal of Engineering Technology* (www.joetsite.com); this figure shows two evaluated articles in Volume 6, Issue in March (Special Issue), 2018
3. GOOGLE SCHOLAR RESULT

In this section, result of searching the fake website of JET through Google Scholar search engine is discussed. As seen in Figure 3, Google Scholar as an altmetric tool for promoting scientific works is not a reliable way to verify originality of a journal website.

![Google Scholar Result](source.png)

Figure 3. Google Scholar supports the fake website of JET (Source: Google Scholar)

4. SCOPUS RESULT

Here, we want to detail how to use Scopus database in identifying fake websites? Checking articles claimed as published documents of doubtful websites in Scopus and Web of Science (WoS) is a very reliable way to take a decision about authenticity of a journal website. If there are many recent papers (do not select online first/ahead of print/early-cite papers, and also papers from the last published issue, because indexing may be time-consuming) which have not been abstracted in the claimed indexing databases, the website is then fake. For example, we could find the doubtful website claiming the Journal of Engineering Technology with ISSN: 0747-9964 (as per Table 1 and Figure 4, this ISSN belongs to a journal indexed by both WoS and Scopus), then we are going to verify it using Scopus.

Figure 1 showed some papers published in this doubtful website (www.joetsite.com). Two papers were selected which are observable in two color boxes (orange and blue boxes). In this step, we do analysis on the paper of Figure 2. As seen in Figure 5, its title has been searched through Scopus search engine and the search result is according to Figure 6. The result is “No documents were found”. If we find many such cases in this website, therefore we can surely say that this website is fake and there is a fraud. In this specific case, it is fake because there many unavailable papers on Scopus.
In addition to the above case, some published papers of the original journal may be published in a fake website, so in the cases that some papers of a doubtful website are searchable through Scopus or WoS and some are not, you should carefully check its publishing information and resolve its Digital Object Identifier.
(DOI), if applicable (having a valid DOI related to a doubtful website is not important, so the main point is to resolve the mentioned DOI in Scopus or WoS towards that doubtful website). In a very infrequent case in 2017, we observed that the fake website could convince Scopus in order to indexing/abstracting of papers as the original source on which Scopus did abstracting for papers published in this website. A wonderful point in this experience was to see some papers of both original journal and hijacked version concurrently whereas they have different publishing information (volume, issue, etc.) but under a unique ISSN. As follows, we will detail the observation. Thus as a result, we think that authors should check both WoS and Scopus, not just one of them (if applicable). In our case study on the journal described in Table 1, although Scopus has removed most of papers received from the fake website (in Nov. 2018, we could not find 2017 papers again on Scopus), but we could still find a paper of this website published in 2018 among many papers from the original journal. Figure 7 indicates three papers for the journal with ISSN: 0747-9964 whereas one of them is for the fake website and has some completely different publishing information. This paper is indeed observable in blue box of Figure 1.

5. WEB OF SCIENCE RESULT

In this section, verification is performed by WoS. Fortunately, WoS in this specific case is clear and does not cover any document of the fake website (this last sentence does not mean that we believe WoS is preferred than Scopus! We only wish to say check both for more reliability). Its sample results are shown in Figure 8 without coverage of the fake website. In addition, statistics provided by WoS would clearly demonstrate a fact against the fake website, see Figures 9 and 10.
6. CONCLUSIONS

Initially, we discussed the importance of eliminating predatory publishers and journals and then highlighted the new version of predatory journals, the hijacked journals. Currently, the major challenge faced by the research community is accurate identification of these fake websites. Our research aimed at displaying to the research community, how duplicate/fake journals can be identified using Google Scholar, Web of Science and Scopus based on a case study. We used the example of the legitimate and well-established journal, Journal of Engineering Technology and showed how fake journals exist with similar name and content. We displayed the results with Google Scholar, Scopus and Web of Science tools. This solution can be easily replicated by other researchers and can be used to identify potential fake journals. Thus, researchers can avoid fake journals and can publish their research papers in legitimate journals with confidence [11]-[14]. Furthermore, we aim to come up with a comprehensive list of hijacked journals and a simple tool that can be used by researchers to detect these fake journals [13].
REFERENCES

[1] Beall, J. (2014), “Polish journal is hijacked” archived version available at (current access): https://web.archive.org/web/20160305164252/https://scholarlyoa.com/2-014/05/02/red-alert-polish-scholarly-journal-is-hijacked/ (accessed 14 October 2018)

[2] Beall, J. (2016), “Hijacked journal’s list”, archived version available at: https://beallslist.weebly.com/hijacked-journals.html (accessed 11 October 2018)

[3] Cabells (2018), “The Journal Blacklist”, available at https://www2.cabells.com/about-blacklist (accessed 26 September 2018)

[4] Clarivate Analytics, (2018), “Master Journal List”, available at http://mjl.clarivate.com/cgi-bin/jrnlst/jrnlstresults.cgi?PC=MASTER&ISSN=0449-0576 (accessed 14 October 2018)

[5] Dadkhah, M. (2015), “Paper hijacking: hijackers are attacking journals for hijacking unpublished papers”, Journal of Digital Information Management, Vol. 13 No. 4, pp. 281-282.

[6] Dadkhah, M. & Borchardt, G. (2016), “Hijacked Journals: An Emerging Challenge for Scholarly Publishing”, Aesthetic Surgery Journal, Vol. 36, No. 6, pp. 739–741. https://doi.org/10.1093/asj/sjw026

[7] Dadkhah, M. (2016), “Types of hijacking in the academic world – our experiment in the scholarly publishing”, Library Hi Tech News, Vol. 33 No. 3 pp. 1 – 2. DOI: 10.1108/LHTN-09-2015-0065

[8] Jalalian, M. (2014), “Hijacked journals are attacking the reliability and validity of medical research”, Electronic Physician, Vol. 6 No. 4, pp. 925-926. DOI: 10.14661/ 2014.925-926.

[9] Jalalian, M. and Dadkhah, M. (2015), “The full story of 90 hijacked journals from August 2011 to June 2015”, Geographica Pannonica, Vol. 19 No. 2, pp. 73-87.

[10] Kolahi J. & Khazaei S, (2015), “Journal hijacking: A new challenge for medical scientific community”, Dent Hypotheses, vol. 6, No. 1, pp. 3-5. DOI: 10.4103/2155-8213.150858

[11] Menon, V. G. (2018), “How Are Predatory Publishers Preying on Uninformed Scholars? Don’t Be a Victim”, IGI Global’s Webinar Series, available on https://www.igi-global.com/symposium

[12] Khosravi, M. R. (2018), “Reliable of scholarly journal acceptance rates”, Library Hi Tech News, Vol. 35 No. 10 pp. 7 – 8.

[13] Menon, V. G., Khosravi, M. R. (2019), “Preventing Hijacked Research Papers in Fake (Rogue) Journals Through Social Media and Databases”, Library Hi Tech News. DOI: 10.1108/LHTN-11-2018-0070

[14] Menon, V. G. (2019), “Hijacked journals: what they are and how to avoid them”, Publons (Clarivate Analytics), https://publons.com/blog/hijacked-journals-what-they-are-and-how-to-avoid-them