Hindawi
Security and Communication Networks
Volume 2021, Article ID 1631496, 8 pages
https://doi.org/10.1155/2021/1631496

*Research Article*

# 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. Khosravi**[1] **and Varun G. Menon**[2]

[1]*Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz, Iran*
[2]*Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Kerala 683582, India*

Correspondence should be addressed to Mohammad R. Khosravi; m.khosravi@sutech.ac.ir

Received 10 May 2021; Revised 25 August 2021; Accepted 17 September 2021; Published 12 October 2021

Academic Editor: Hao Wang

This 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 and 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 study is that in some uncommon cases, fake websites (clone versions) may sometimes convince a scientometric database in order to be fully/partially indexed along with an abstracting of their hijacked papers while these websites steal identity of the legal journals. Therefore, as a result, we should check both of WoS and Scopus at the same time for verifying a fake website to obtain more reliability.

## 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 is always to identify and eliminate these predatory journals. Since the last few years, a similar type of fake publishers with many hijacked journals has attacked the research community extensively and intensively. Fake journals are indeed versions with hijacked 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 may copy all the contents available in the website of the legitimate journal such as Impact Factor (IF), ISSN, Editorial Board Members (EBMs) information, and indexing and archiving information. They then send attractive calls for papers to researchers around the world inviting them to publish with these fake journals for a high fee (but normally these fees are not much high compared with 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* Perish existing in many countries, many academicians fall in this trap. Authors receiving these e-mails are attracted by the indexing information such as Scopus, Web of Science (WoS), or the IF value of journal. They then click on the link of the hijacked version of the journal given in the e-mail 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 (maybe!) 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 to 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 [7–9].

The rest of this paper is organized as follows. First, the case study will be discussed, and then we try to verify its identity through different tools. At the end, a conclusion on the work will be given. This paper is the final publication for the preprint version published by *TechRxiv* [10].

## 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 semiannually, 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.

Although our paper is about a case study, e.g., JET, the final solution presented by us is completely general. The case study in our research is a very unique case in the first step of the study, done in 2019 (see the Acknowledgments section), so that we can show some shortcoming of the hijacked platforms detection process through it whereas no other case could reveal the lacks.

## 3. Google Scholar Results

In this section, result of searching the fake website of JET through Google Scholar search engine is discussed. As seen in Figure 4, Google Scholar as an altmetric tool for promoting scientific work is not a reliable way to verify originality of a journal website. These works are based on an artificial intelligence-assisted Google robot to extract scientific information and then to make abstracting of them.

## 4. Scopus Results

Here, we want to detail how to use Scopus database for 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 5, this ISSN belongs to a journal indexed by both WoS and Scopus), and then we are going to verify it using Scopus.

Figure 1 shows some papers published in this doubtful website (http://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 6, its title has been searched through Scopus search engine, and the search result is according to Figure 7. 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 here. 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, and so on) 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 as starting point of our study, we could not find 2017 papers again on Scopus), we could still find a paper of this website published in 2018 among many papers from the original journal. Figure 3 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 observable in blue box of Figure 1.

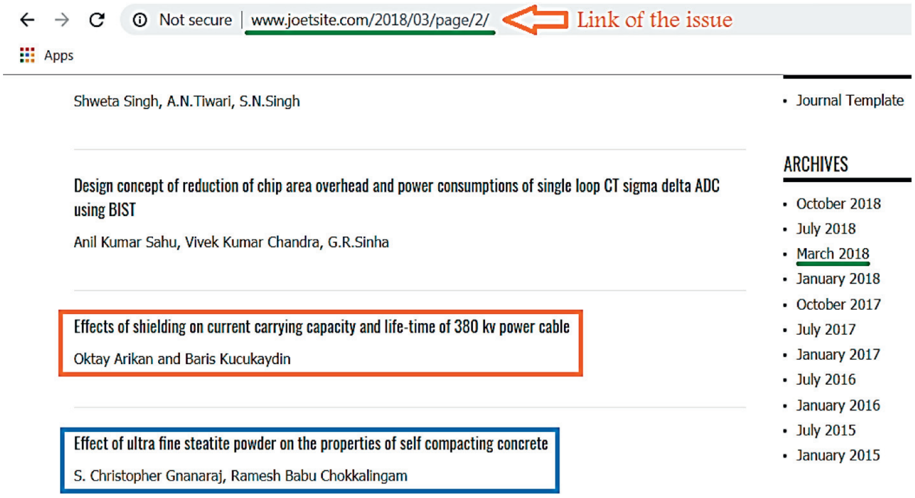
## 5. Web of Science Results

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 prefered 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 clone version (see Figures 9 and 10) interpreted as follows:

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

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

* 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 in 2019; 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 3 (by Sriraman et al., 2017) via this link https://www.asee.org/public/conferences/78/papers/17663/view#).*** Based on the Scopus record through ScimagoJR, the main website of this journal is https://www.engtech.org/jet; however, we could not approve it in 2019 through its contents.



Shweta Singh, A.N.Tiwari, S.N.Singh

Design concept of reduction of chip area overhead and power consumptions of single loop CT sigma delta ADC using BIST

Anil Kumar Sahu, Vivek Kumar Chandra, G.R.Sinha

Effects of shielding on current carrying capacity and life-time of 380 kv power cable

Oktay Arikan and Baris Kucukaydin

Effect of ultra fine steatite powder on the properties of self compacting concrete

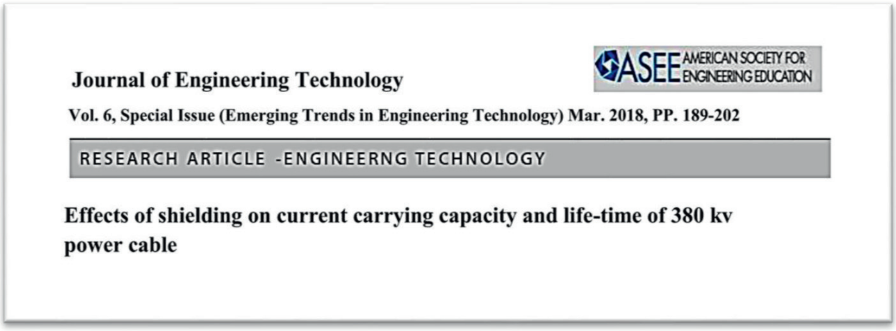
S. Christopher Gnanaraj, Ramesh Babu Chokkalingam

- Journal Template

ARCHIVES

- October 2018
- July 2018
- March 2018
- January 2018
- October 2017
- July 2017
- January 2017
- July 2016
- January 2016
- July 2015
- January 2015

Figure 1: Fake website for the Journal of Engineering Technology (http://www.joetsite.com). This figure shows two evaluated articles in Volume 6, Issued in March (Special Issue), 2018.



Journal of Engineering Technology

Vol. 6, Special Issue (Emerging Trends in Engineering Technology) Mar. 2018, PP. 189-202

RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

Effects of shielding on current carrying capacity and life-time of 380 kv power cable

Figure 2: A paper published by the fake website of JET (http://www.joetsite.com).

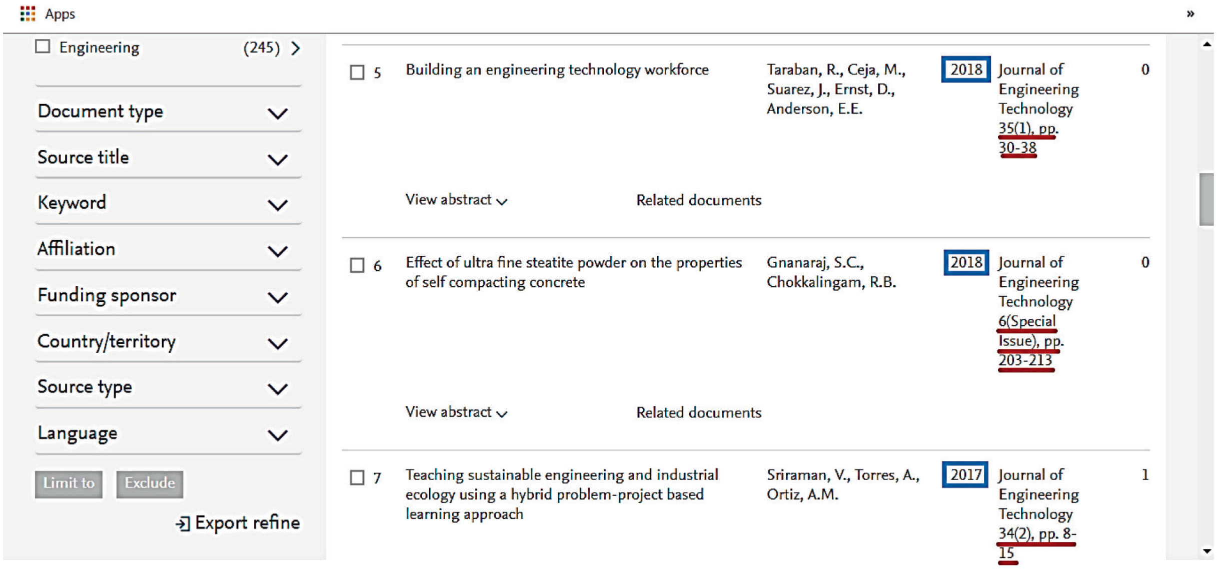
(i) Finding from Figure 9: it is obvious that the number of published papers is about 10 yearly according to WoS, and this number is much less than the records observed in the clone version of the journal (when it was alive in 2018–2020, later this sentence will be explained).

(ii) Finding from Figure 10: the clone version was an open access jounal, but Figure 10 shows a citation record as much less than a record for an open access venue considering the number of publications in Figure 9.

Since WoS has important features compared with the other two tools (Table 2), the checking with it as the final step is essential and highly recommended to be done.

## 6. General Findings and Discussion

Thus, researchers can avoid fake journals and can publish their research papers in legitimate journals with confidence [11–15]. 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, 16, 17]. In the time of publishing this current version of our research, the clone version addressed in the paper is no longer available, maybe due to our first report about in 2019 [13] (also, see the Acknowledgments section) and repeating the same report in [16] based on our finding. However, this availability is not important because the same things will/may appear in future such that some of them have been reported in [16] just now. In total,



Apps »

☐ Engineering (245) >

Document type

Source title

Keyword

Affiliation

Funding sponsor

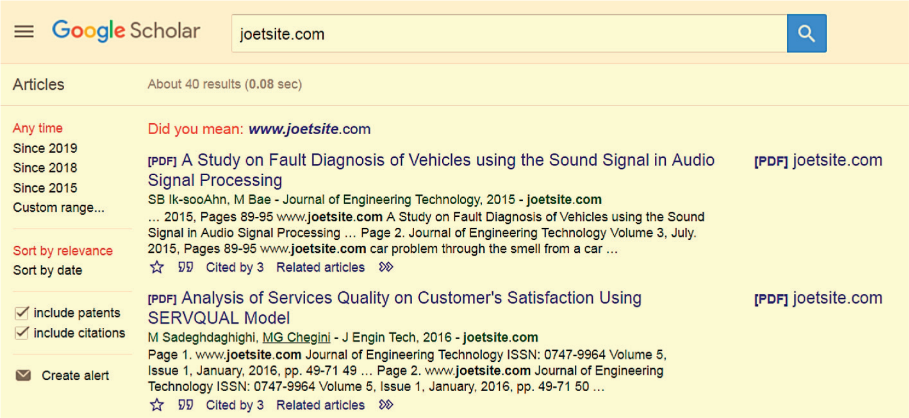
Country/territory

Source type

Language

| | | | | | |
|---|---|---|---|---|---|
| ☐ 5 | Building an engineering technology workforce | Taraban, R., Ceja, M., Suarez, J., Ernst, D., Anderson, E.E. | 2018 | Journal of Engineering Technology 35(1), pp. 30-38 | 0 |
| ☐ 6 | Effect of ultra fine steatite powder on the properties of self compacting concrete | Gnanaraj, S.C., Chokkalingam, R.B. | 2018 | Journal of Engineering Technology 6(Special Issue), pp. 203-213 | 0 |
| ☐ 7 | Teaching sustainable engineering and industrial ecology using a hybrid problem-project based learning approach | Sriraman, V., Torres, A., Ortiz, A.M. | 2017 | Journal of Engineering Technology 34(2), pp. 8-15 | 1 |

Figure 3: Three articles found for "ISSN: 0747–9964" on Scopus, data acquired in Nov 2018 (source: Scopus).



Google Scholar joetsite.com

Articles About 40 results (0.08 sec)

Any time
Since 2019
Since 2018
Since 2015
Custom range...

Sort by relevance
Sort by date

☑ include patents
☑ include citations

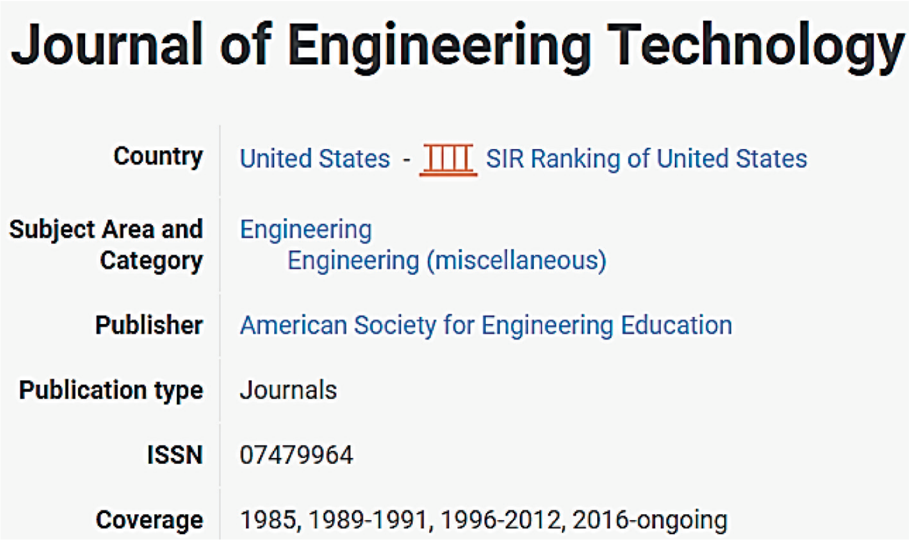
Create alert

Did you mean: *www.joetsite*.com

[PDF] A Study on Fault Diagnosis of Vehicles using the Sound Signal in Audio Signal Processing [PDF] joetsite.com
SB Ik-sooAhn, M Bae - Journal of Engineering Technology, 2015 - **joetsite.com**
... 2015, Pages 89-95 www.**joetsite.com** A Study on Fault Diagnosis of Vehicles using the Sound Signal in Audio Signal Processing ... Page 2. Journal of Engineering Technology Volume 3, July. 2015, Pages 89-95 www.**joetsite.com** car problem through the smell from a car ...
☆ 99 Cited by 3 Related articles

[PDF] Analysis of Services Quality on Customer's Satisfaction Using SERVQUAL Model [PDF] joetsite.com
M Sadeghdaghighi, MG Chegini - J Engin Tech, 2016 - **joetsite.com**
Page 1. www.**joetsite.com** Journal of Engineering Technology ISSN: 0747-9964 Volume 5, Issue 1, January, 2016, pp. 49-71 49 ... Page 2. www.**joetsite.com** Journal of Engineering Technology ISSN: 0747-9964 Volume 5, Issue 1, January, 2016, pp. 49-71 50 ...
☆ 99 Cited by 3 Related articles

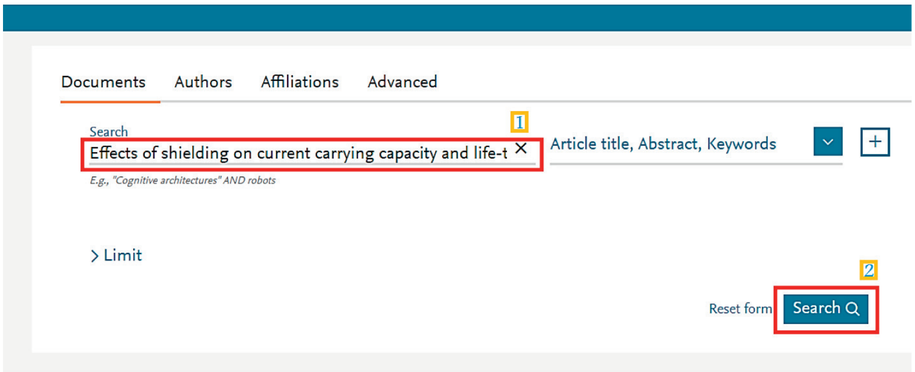
Figure 4: Google Scholar supports the fake website of JET (source: Google Scholar).



Journal of Engineering Technology

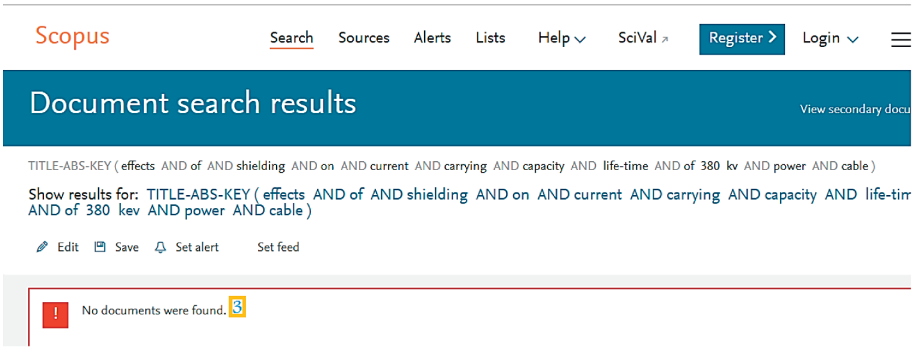
| | |
|---|---|
| Country | United States - SIR Ranking of United States |
| Subject Area and Category | Engineering<br>Engineering (miscellaneous) |
| Publisher | American Society for Engineering Education |
| Publication type | Journals |
| ISSN | 07479964 |
| Coverage | 1985, 1989-1991, 1996-2012, 2016-ongoing |

Figure 5: JET details provided by ScimagoJR, a product of Scopus (source: Scimago JR in 2019).



Search
Effects of shielding on current carrying capacity and life-t ✕
E.g., "Cognitive architectures" AND robots

FIGURE 6: Searching article determined by orange color box in Figure 1 using Scopus search engine (source: Scopus).

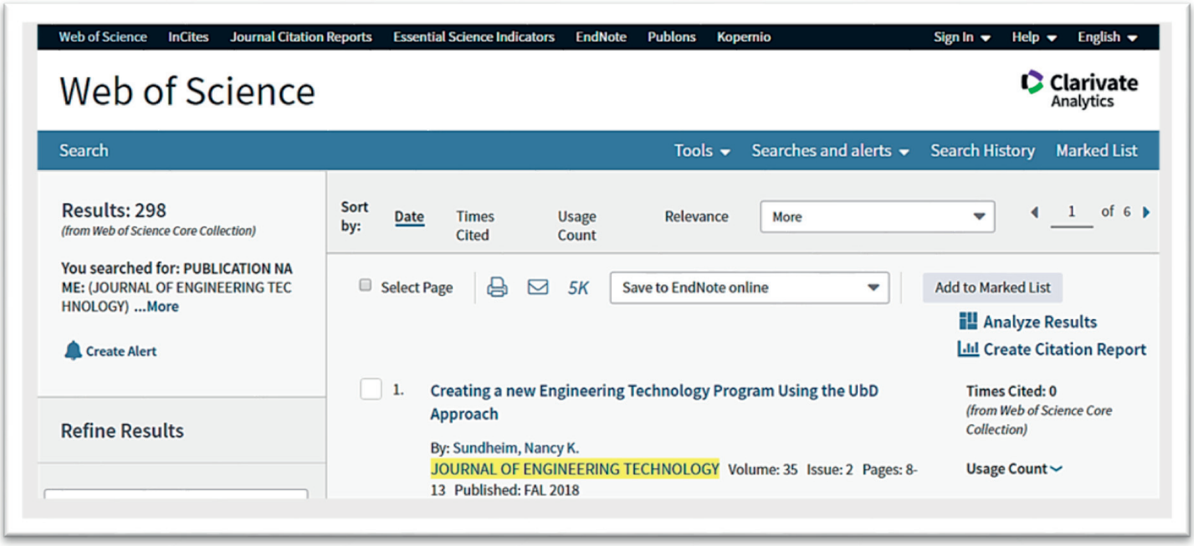


TITLE-ABS-KEY ( effects AND of AND shielding AND on AND current AND carrying AND capacity AND life-time AND of 380 kv AND power AND cable )

Show results for: TITLE-ABS-KEY ( effects AND of AND shielding AND on AND current AND carrying AND capacity AND life-tim AND of 380 kev AND power AND cable )

No documents were found.

FIGURE 7: Result of the search engine for the case searched in Figure 6 (source: Scopus).



Results: 298
(from Web of Science Core Collection)

You searched for: PUBLICATION NAME: (JOURNAL OF ENGINEERING TECHNOLOGY) ...More

1. Creating a new Engineering Technology Program Using the UbD Approach

By: Sundheim, Nancy K.

JOURNAL OF ENGINEERING TECHNOLOGY Volume: 35 Issue: 2 Pages: 8-13 Published: FAL 2018

Times Cited: 0
(from Web of Science Core Collection)

FIGURE 8: WoS search for JET does not include papers of the clone version, data acquired in Nov 2018 (source: Web of Science).

it is a critical point that making a safer data environment for cloud-based big data services must be taken more seriously [18, 19], especially for the science. We hope this research with its historical view on a case study during over four years evaluation (2017–2021) can help the scientists find a secure way of publishing their academic and industrial findings. Security and privacy not only must be provided with computational methods but also in the modern form of data exchange; it is covered by intelligent and policy-based solutions [20, 21], similar to the approach of the current paper. As brief, our contributions are as follows:

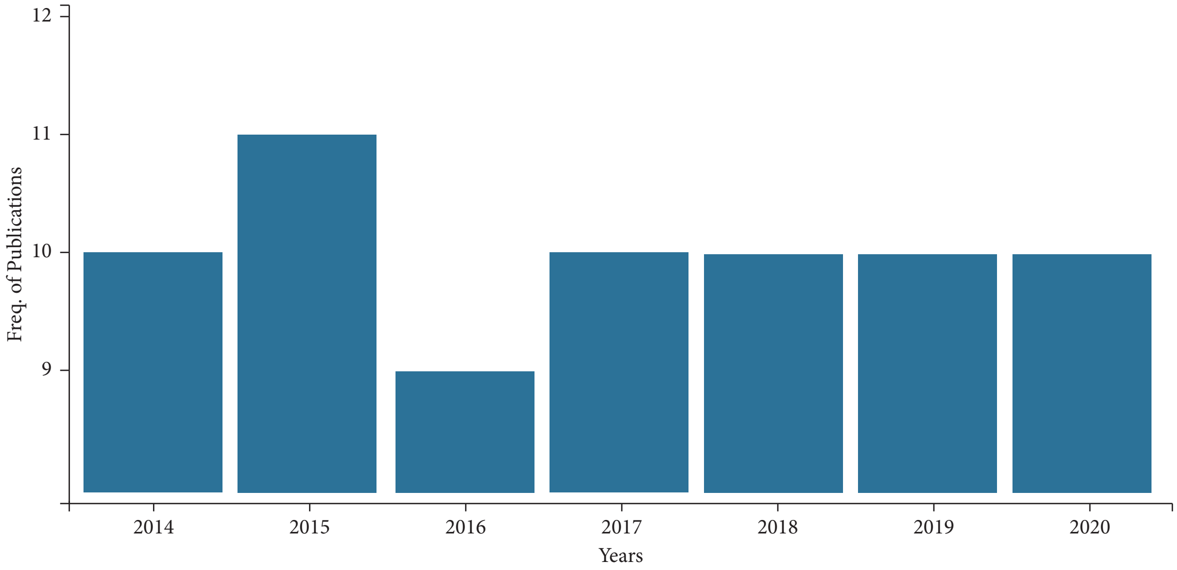


Figure 9: Number of publications per year for the main journal according to WoS, data acquired in June 2021; JET has had a continuous coverage by WoS since 1998 (source: Web of Science).

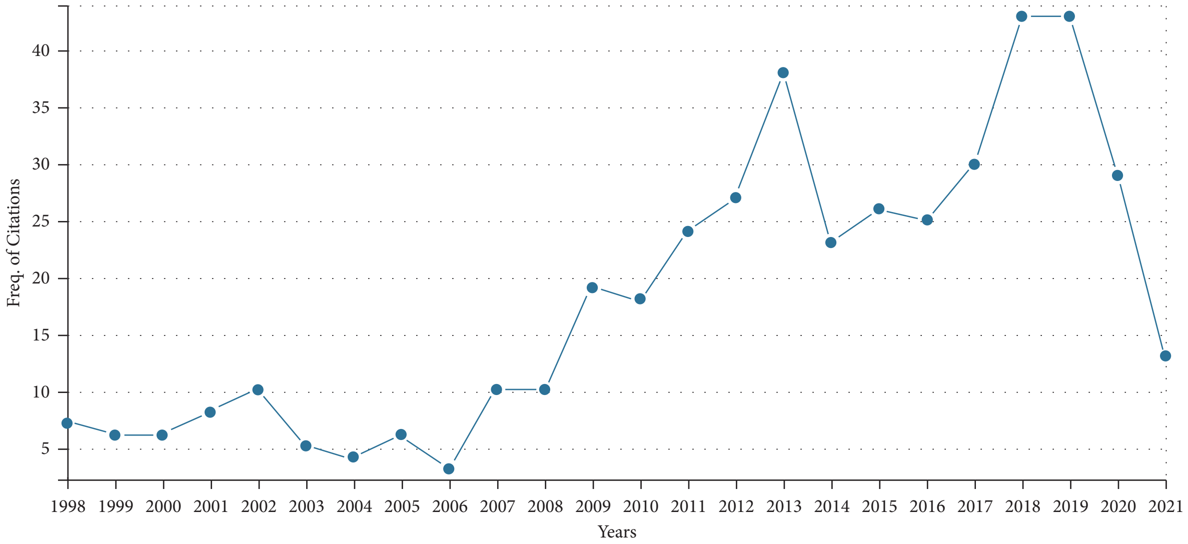


Figure 10: Citation rate (times per year) of the main journal in WoS, data acquired in June 2021 (source: Web of Science).

Table 2: Comparison of the three scientific tools.

| Service | Type | Operation | Reliability |
|---|---|---|---|
| Google Scholar | Altmetric | Robot-based processing | Very low |
| Scopus | Scientometric | Evaluation departments, publishers | High |
| WoS | Scientometric | Evaluation departments, publishers | Very high |

(i) This research is one of the first investigations around a clone version of an indexed journal with the ability of abstracting in one of the major indexing services, i.e., Scopus. As mentioned, the author of [16] could later list several similar cases including the case study of our work. Such clone versions are named *advanced clones* because of their success in convincing the major indexing services.

(ii) We could suggest several solutions to avoid publishing in the advanced clones which are mainly a fake website for WoS/Scopus-indexed journals as follows:

Table 3: The history behind JET.

| Year | Description | Related documents |
|---|---|---|
| 2017 to Mid-2018 | Detecting the clone version with several abstracted papers on Scopus | N/A |
| Mid-2018 to 2019 | First report about the clone while one sample from the clone website could still be found on Scopus | Reference [13]; doi: 10.1108/LHTN-11-2018–0070<br>[10]; doi: 10.36227/techrxiv.11385849.v1 |
| 2020 | Further checking and updating the data, no case was found on Scopus for the clone | [10]; doi: 10.36227/techrxiv.11385849.v2 |
| 2021 | Integrating all reports and reaching the final output of the case study while the clone website had been suspended, and some new evidence about the legitimate journal is accessible | The current paper published by *SCN* |

Paying attention to the volume/issue number of the published papers of any doubtful website through Scopus/WoS and comparing with other abstracted papers to find any inconsistency. The experience says that the inconsistency is mostly found in Scopus, but WoS must be also double-checked, specifically for explaning any found difference.

The number of citations in Scopus/WoS is very important for the corresponding ISSN of the main journal (legitimate version)/fake website (clone version) to be monitored. Since clones are mainly open access and the main journal is not (whether having a website or not to have), thus we should expect a citation record similar to open access journals. When a clone version cannot do the abstracting of most/all of its publications, therefore, no citation will be found for those publications; for example, the JET citations are not considerable in WoS.

The number of abstracted papers in WoS/Scopus should be checked and compared with the number of papers in a clone version (under-doubt website).

Inconsistency in parallel WoS/Scopus indexing (= abstracting of published content here) of an under-doubt website claims both major indexes at the same time.

(iii) In other cases, similar checklists can be redesigned per case according to all claims and demands.

(iv) In the information retrieval about the case study in 2020/2021, some new happenings are seen as follows:

The clone version of JET has been suspended from service. The last time of access to the clone was in 2020 from our side.

Scopus has removed all publications of the clone version of JET.

ScimajoJR as a linked product of Scopus has introduced the legitimate website of JET (seems to be a newly launched homepage) and an e-mail address for JET. This action of Scopus and launching the formal web page of JET can be also strong reasons of unavailability of the clone version in addition to our first report in [13] and the link provided in the Acknowledgments section. The Scopus-related new information can be found in [22]. Table 3 summarizes the background of our study on JET.

## 7. Conclusions

Initially, we discussed the importance of eliminating predatory publishers and journals and then highlighted a similar version of predatory journals, i.e., the hijacked journals. Currently, the major challenge faced by the research community is inaccurate identification of these fake websites. Our research aimed at displaying the research community, how duplicate/fake journals can be identified using Google Scholar, Web of Science, and Scopus with 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 also showed the results with Google Scholar, Scopus, and Web of Science tools and made some deep analysis based on them. This solution can be easily replicated by other researchers and can be used to identify potential fake journals in any scientific field of research. Information science security concerning journal hijacking and clones is a kind of cybercrime analysis in computer and web technologies.

## Abbreviations

| | |
|---|---|
| ISSN: | International standard series number |
| JET: | Journal of Engineering Technology. |

## Data Availability

All the data can be tracked through the databases, and a copy of all is also accessible through the corresponding author.

## Disclosure

An initial draft of this paper was published as a preprint by TechRxiv preprint service in 2019 and has been updated in 2020. The aim behind posting this version was to collect insightful comments from the research community and monitor any updates regarding the original and clone versions. The readers can follow this preprint version and all its updates through: https://doi.org/10.36227/techrxiv.11385849. This current document published in 2021 is the third and last update of our study.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

[1] J. Beall, "Polish journal is hijacked," 2014, https://web.archive.org/web/20160305164252/.

[2] J. Beall, "Hijacked journal's list," 2016, https://beallslist.weebly.com/hijacked-journals.html.

[3] Cabells, "The Journal Blacklist," 2018, https://www2.cabells.com/about-blacklist.

[4] C. Analytics, "Master Journal List," 2018, http://mjl.clarivate.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&ISSN=0449-0576.

[5] M. Dadkhah, "Paper hijacking: hijackers are attacking journals for hijacking unpublished papers," *Journal of Digital Information Management*, vol. 13, no. 4, pp. 281-282, 2015.

[6] M. Dadkhah and G. Borchardt, "Hijacked journals: an emerging challenge for scholarly publishing," *Aesthetic Surgery Journal*, vol. 36, no. 6, pp. 739–741, 2016.

[7] M. Dadkhah, "Types of hijacking in the academic world - our experiment in the scholarly publishing," *Library Hi Tech News*, vol. 33, no. 3, pp. 1-2, 2016.

[8] M. Jalalian, "Occitan literature," *The Virgil Encyclopedia*, vol. 6, no. 4, pp. 925-926, 2014.

[9] M. Jalalian and M. Dadkhah, "The full story of 90 hijacked journals from August 2011 to June 2015," *Geographica Pannonica*, vol. 19, no. 2, pp. 73–87, 2015.

[10] M. R. Khosravi and V. G. Menon, "Reliability of hijacked journal detection based on scientometrics, altmetric tools and Web informatics: a case report using Google scholar, Web of science and Scopus," *TechRxiv Preprint Server*, vol. v1, 2019.

[11] S. Khazaei and J. Kolahi, "Journal hijacking: a new challenge for medical scientific community," *Dental Hypotheses*, vol. 6, no. 1, pp. 3–5, 2015.

[12] M. R. Khosravi, "Reliability of scholarly journal acceptance rates," *Library Hi Tech News*, vol. 35, no. 10, pp. 7-8, 2018.

[13] V. G. Menon and M. R. Khosravi, "Preventing hijacked research papers in fake (rogue) journals through social media and databases," *Library Hi Tech News*, vol. 36, no. 5, pp. 1–6, 2019.

[14] V. G. Menon, "Hijacked Journals: What They Are and How to Avoid Them: Publons (Clarivate Analytics)," 2019, https://publons.com/blog/hijacked-journals-what-they-are-and-how-to-avoid-them.

[15] V. G. Menon, ""How are predatory publishers preying on uninformed scholars? Don't Be a victim", IGI global's webinar Series," 2018, https://www.igi-global.com/symposium.

[16] A. Abalkina, "Hijacked Journals in Scopus," 2021, https://www.researchgate.net/publication/352062052.

[17] A. Abalkina, "How Hijacked Journals Keep Fooling One of the World's Leading Databases," 2021, https://retractionwatch.com/2021/05/26/how-hijacked-journals-keep-fooling-one-of-the-worlds-leading-databases.

[18] S. Goyal, S. Bhushan, Y. Kumar et al., "An optimized framework for energy-resource allocation in a cloud environment based on the whale optimization algorithm," *Sensors*, vol. 21, no. 5, p. 1583, 2021.

[19] A. W. Khan, M. U. Khan, J. A. Khan et al., "Analyzing and evaluating critical challenges and practices for software vendor organizations to secure big data on cloud computing: an ahp-based systematic approach," *IEEE Access*, vol. 9, pp. 107309–107332, 2021.

[20] X. Xu, Q. Geng, H. Cao et al., "Blockchain-powered service migration for uncertainty-aware workflows in edge computing," in *Dependability in Sensor, Cloud, and Big Data Systems and Applications. DependSys 2019*, G. Wang, M. Z. A. Bhuiyan, S. De Capitani di Vimercati, and Y. Ren, Eds., vol. 1123, pp. 217–230, Springer, Singapore, 2019.

[21] X. Chi, C. Yan, H. Wang, W. Rafique, and L. Qi, "Amplified locality-sensitive hashing-based recommender systems with privacy protection," *Concurrency and Computation: Practice and Experience*, pp. 1–21, 2020.

[22] Scopus, "The Details for Journal of Engineering Technology," 2021, https://www.scimagojr.com/journalsearch.php?q=12487&tip=sid&clean=0.