

Visit [Nature news](#) for the latest coverage and read [Springer Nature's statement on the Ukraine conflict](#)



## Source Code Obfuscation: Novel Technique and Implementation

ICT Systems and Sustainability pp 197-204 | Cite as

Conference paper

**First Online:** 01 January 2022

115

Downloads

Part of the [Lecture Notes in Networks and Systems](#) book series (LNNS, volume 321)

### Abstract

In today's world the sheer amount and increasing range of unlicensed practices by injecting malicious programs, hackers are able to gain forbidden access to the devices and private information. Fortunately, the businesses who frame up the web world and therefore the security professionals that support them have their own set of repositories to retaliate. The basic idea behind source code obfuscation is to alter the computer programs in order to cover their delicate information while retaining their original functionality. The objective of the proposed method is to keep the code basic, without any crucial changes, here the invader will be unable to recognize the difference between the original code and the obfuscated code, and also, the code will be well obfuscated. Results evaluate that to what scale the code obfuscation is in a position to form attacks harder to be performed and disclose that obfuscation can attenuate the result of things which will alter the odds of a successful attack.

### Keywords

Code obfuscation   Decryption   Encryption   Functionality

This is a preview of subscription content, [log in](#) to check access.

### References

1. Ahire P, Abraham J (2020) Mechanisms for source code obfuscation in C: novel techniques and implementation. *IEEE*, 2020. 978-1-7281-5263-9/20  
[Google Scholar](https://scholar.google.com/scholar?q=Ahire%20P%2C%20Abraham%20J%20%282020%29%20Mechanisms%20for%20source%20code%20obfuscation%20in%20C%3A%20novel%20techniques%20and%20implementation.%20IEEE%2C%202020.%20978-1-7281-5263-9%2F20) (<https://scholar.google.com/scholar?q=Ahire%20P%2C%20Abraham%20J%20%282020%29%20Mechanisms%20for%20source%20code%20obfuscation%20in%20C%3A%20novel%20techniques%20and%20implementation.%20IEEE%2C%202020.%20978-1-7281-5263-9%2F20>)
2. Balakrishnan A, Schulze C (2005) Code obfuscation literature survey. In: *CS701 construction of compilers*, 2005  
[Google Scholar](https://scholar.google.com/scholar?q=Balakrishnan%20A%2C%20Schulze%20C%20%282005%29%20Code%20obfuscation%20literature%20survey.%20In%3A%20CS701%20construction%20of%20compilers%2C%202005) (<https://scholar.google.com/scholar?q=Balakrishnan%20A%2C%20Schulze%20C%20%282005%29%20Code%20obfuscation%20literature%20survey.%20In%3A%20CS701%20construction%20of%20compilers%2C%202005>)
3. Tiella R, Ceccato M (2017) Automatic generation of opaque constants based on the KC lique problem for resilient data obfuscation. *IEEE*

- Google Scholar** (<https://scholar.google.com/scholar?q=Tiella%20R%20C%20Ceccato%20M%20%282017%29%20Automatic%20generation%20of%20opaque%20constants%20based%20on%20the%20KC%20lique%20problem%20for%20resilient%20data%20obfuscation.%20iIEEE>)
4. Demissie BF, Ceccato M, Tiella R (2015) Assessment of data obfuscation with residue number coding. *IEEE Google Scholar* (<https://scholar.google.com/scholar?q=Demissie%20BF%20C%20Ceccato%20M%20Tiella%20R%20%282015%29%20Assessment%20of%20data%20obfuscation%20with%20residue%20number%20coding.%20iIEEE>)
  5. Heffner K, Collberg C (2007) The obfuscation executive. In: Information security. Springer, pp 428–440. [5] Jakubowski MH, Saw CW, Venkatesan R (2007) Iterated transformations and quantitative metrics for software protection. In: SECRYPT, pp. 359–368. [6] Anckaert B, Madou M, Sutter BD, Bus BD, Bosschere KD, Preneel B (2007) Program obfuscation: a quantitative approach. In: QoP'07: proceedings of the 2007 ACM workshop on quality of protection. ACM, New York, NY, USA, pp 15–20  
**Google Scholar** (<https://scholar.google.com/scholar?q=Heffner%20K%20C%20Collberg%20C%20%282007%29%20The%20obfuscation%20executive.%20In%3A%20Information%20security.%20Springer%20%20pp%20428%E2%80%93440.%20%282007%29%20Iterated%20transformations%20and%20quantitative%20metrics%20for%20software%20protection.%20In%3A%20SECRYPT%20%20pp.%20359%E2%80%93368.%20%282007%29%20Anckaert%20B%20%20Madou%20M%20%20Sutter%20BD%20%20Bus%20BD%20%20Bosschere%20KD%20%20Preneel%20B%20%282007%29%20Program%20obfuscation%20a%20quantitative%20approach.%20In%3A%20QoP%20%20pp.%2015%E2%80%9320>)
  6. Xu H, Zhou Y, Kang Y, Iyu MR (2017) On secure and usable program obfuscation: a survey. Cornell University Library, [arXiv:1710.01139v1](https://arxiv.org/abs/1710.01139v1), (<http://arxiv.org/abs/1710.01139v1>) <https://arxiv.org/pdf/1710.01139.pdf> (<https://arxiv.org/pdf/1710.01139.pdf>)
  7. Yasin A, Nasra I (2016) Dynamic multi levels java code obfuscation technique. *Int J Comput Sci Sec* 10:140–160  
**Google Scholar** (<https://scholar.google.com/scholar?q=Yasin%20A%20%20Nasra%20I%20%282016%29%20Dynamic%20multi%20levels%20java%20code%20obfuscation%20technique.%20Int%20J%20Comput%20Sci%20Sec%20%2010%3A140%E2%80%93160>)
  8. Ahire P, Abraham J (2018) Perceive core logical blocks of a C program automatically for source code transformations. In: Proceedings of 18th international conference on intelligent systems design and applications. Springer, 2018. 978-3-030-16657-1\_36  
**Google Scholar** ([https://scholar.google.com/scholar?q=Ahire%20P%20%20Abraham%20J%20%282018%29%20Perceive%20core%20logical%20blocks%20of%20a%20C%20program%20automatically%20for%20source%20code%20transformations.%20In%3A%20Proceedings%20of%20the%2018th%20international%20conference%20on%20intelligent%20systems%20design%20and%20applications.%20Springer%20%202018.%20978-3-030-16657-1\\_36](https://scholar.google.com/scholar?q=Ahire%20P%20%20Abraham%20J%20%282018%29%20Perceive%20core%20logical%20blocks%20of%20a%20C%20program%20automatically%20for%20source%20code%20transformations.%20In%3A%20Proceedings%20of%20the%2018th%20international%20conference%20on%20intelligent%20systems%20design%20and%20applications.%20Springer%20%202018.%20978-3-030-16657-1_36))
  9. Collberg CT, Low D (1998) Manufacturing cheap, resilient, and stealthy opaque constructs. In: Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on principles of programming languages  
**Google Scholar** (<https://scholar.google.com/scholar?q=Collberg%20CT%20%20Low%20D%20%281998%29%20Manufacturing%20cheap%20%20resilient%20%20and%20stealthy%20opaque%20constructs.%20In%3A%20Proceedings%20of%20the%2025th%20ACM%20SIGPLAN-SIGACT%20symposium%20on%20principles%20of%20programming%20languages>)
  10. Schrittwieser S, Katzenbeisser S Code obfuscation against static and dynamic reverse engineering. Springer J  
**Google Scholar** (<https://scholar.google.com/scholar?q=Schrittwieser%20S%20%20Katzenbeisser%20S%20Code%20obfuscation%20against%20static%20and%20dynamic%20reverse%20engineering.%20Springer%20J>)
  11. Protect your C/C++ Code: Stunnix Obfuscator. <http://stunnix.com/prod/cxxo/> (<http://stunnix.com/prod/cxxo/>)
  12. OBFUSCATOR: obfuscate C & C++. <https://picheta.me/obfuscator> (<https://picheta.me/obfuscator>)
  13. The Tigress C Diversifier/Obfuscator. <http://tigress.cs.arizona.edu/> (<http://tigress.cs.arizona.edu/>)
  14. Mangle-It C/C++ Obfuscator. [https://cnet.com/Mangle-It-C-Code-Obfuscator/3000-2229\\_4-190341.html](https://cnet.com/Mangle-It-C-Code-Obfuscator/3000-2229_4-190341.html) ([https://cnet.com/Mangle-It-C-Code-Obfuscator/3000-2229\\_4-190341.html](https://cnet.com/Mangle-It-C-Code-Obfuscator/3000-2229_4-190341.html))
  15. Source Code Obfuscator: Semantic Design. <http://www.semdesigns.com/Obfuscators> (<http://www.semdesigns.com/Obfuscators>)
  16. Obfuscator for Assembler Source Code. <https://www.pelock.com/obfuscator/> (<https://www.pelock.com/obfuscator/>)
  17. CodeMorph C/C++ Obfuscator. <http://www.sourceformat.com/code-obfuscator-cpp.htm> (<http://www.sourceformat.com/code-obfuscator-cpp.htm>)
  18. Zarate C, Garfinkel SL, Heffernan A, Gorak K, Horras S (2014) A survey of XOR as a digital obfuscation technique in a corpus of real data. DTIC Document, Technical Report, 2014  
**Google Scholar** (<https://scholar.google.com/scholar?q=Zarate%20C%20%20Garfinkel%20SL%20%20Heffernan%20A%20%20Gorak%20K%20%20Horras%20S%20%282014%29%20A%20survey%20of%20XOR%20as%20a%20digital%20obfuscation%20technique%20in%20a%20corpus%20of%20real%20data.%20DTIC%20Document%20%20Technical%20Report%20%202014>)

19. Demissie BF, Ceccato M, Tiella R (2015) Assessment of data obfuscation with residue number coding. In: IEEE/ACM international workshop on software protection  
[Google Scholar](https://scholar.google.com/scholar?q=Demissie%20BF%2C%20Ceccato%20M%2C%20Tiella%20R%20%282015%29%20Assessment%20of%20data%20obfuscation%20with%20residue%20number%20coding.%20In%3A%20IEEE%2FACM%20international%20workshop%20on%20software%20protection) (https://scholar.google.com/scholar?q=Demissie%20BF%2C%20Ceccato%20M%2C%20Tiella%20R%20%282015%29%20Assessment%20of%20data%20obfuscation%20with%20residue%20number%20coding.%20In%3A%20IEEE%2FACM%20international%20workshop%20on%20software%20protection)
- 

## Copyright information

© The Author(s), under exclusive license to Springer Nature  
Singapore Pte Ltd. 2022

---

### About this paper

#### Cite this paper as:

Yadav K., Kamble R., Kale S., Pazare Y., Ahire P. (2022) Source Code Obfuscation: Novel Technique and Implementation. In: Tuba M., Akashe S., Joshi A. (eds) ICT Systems and Sustainability. Lecture Notes in Networks and Systems, vol 321. Springer, Singapore. [https://doi.org/10.1007/978-981-16-5987-4\\_21](https://doi.org/10.1007/978-981-16-5987-4_21)

#### First Online

01 January 2022

#### DOI

[https://doi.org/10.1007/978-981-16-5987-4\\_21](https://doi.org/10.1007/978-981-16-5987-4_21)

#### Publisher Name

Springer, Singapore

#### Print ISBN

978-981-16-5986-7

#### Online ISBN

978-981-16-5987-4

#### eBook Packages

[Intelligent Technologies and Robotics](#)

[Intelligent Technologies and Robotics \(R0\)](#)

[Reprints and Permissions](#)

#### SPRINGER NATURE

© 2020 Springer Nature Switzerland AG. Part of [Springer Nature](#).

Not logged in · Not affiliated · 103.86.180.108