A New SVM-STEG Embedding Model in Steganography

Publisher: IEEE

Hanizan Shaker Hussain ; Fazali Ghazali ; Hafiza A. S. ; Hanif Mohd Ali ; Anbuselvan Sangodiah ; Kante Koli Oumar **All Authors**

Abstract: One of the sub-fields in information security is called information hiding and can be applied to protect data and information nowadays. This is a method in where secret-m... **View more**

Metadata

Abstract:
One of the sub-fields in information security is called information hiding and can be applied to protect data and information nowadays. This is a method in where secret-messages are hidden stealthily in an image file. This method has been used in various fields especially in digital image steganography. Most of the techniques proposed to date have various problems i.e., non-random changes will obviously occur especially when the secret message is embedded in an inappropriate area and when the load capacity exceeds the number of bits allowed. This paper proposes a machine learning steganographic method called SVM-Steg model that uses embedding and extracting algorithms by exploiting SVM classification and SVM-Steg embedding to achieve good performance. In addition, the distance of the embedding location is also taken into account so that more pixels can be embedded at more distance locations. The results show a quality cover-image when high peak signal-to-noise ratio (PSNR) values are recorded greater for all types of cover images. In comparison to the other technique, all PSNRs for the proposed technique, SVM-Steg Method achieved 40 or higher. It is not only succeeding in providing a secure embedding position, but also increases the number of secret-bits embedded.

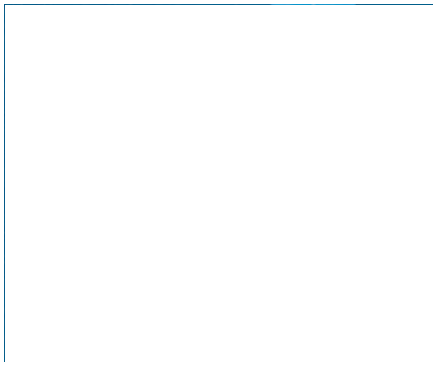
Published in: 2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS)

Date of Conference: 25-27 August 2023 **DOI:** 10.1109/ICSECS58457.2023.10256390

Date Added to IEEE *Xplore*: 26 September 2023 **Publisher:** IEEE

ISBN Information: **Conference Location:** Penang, Malaysia

Contents



» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

8th International Conference on Software Engineering and Computer Systems, ICSECS 2023 • Pages 336 - 341 • 2023 • 8th IEEE International Conference on Software Engineering and Computer Systems, ICSECS 2023 • Penang • 25 August 2023through 27 August 2023 • Code 192961

Document type
Conference Paper

Source type
Conference Proceedings

ISBN
979-835031093-1

DOI
10.1109/ICSECS58457.2023.10256390

A New SVM-STEG Embedding Model in Steganography

Hussain, Hanizan Shaker[a] ; Ghazali, Fazali[b] ; Hafiza A.S.[c] ; Ali, Hanif Mohd[b] ; Sangodiah, Anbuselvan[a] ; Oumar, Kante Koli[a]

[a] Quest International University, Faculty of Computing and Engineering, Malaysia

[b] Universiti Islam Antarabangsa Sultan, Abdul Halim mu'Adzam Shah, Kulliyyah of Muamalat & Management Sciences, Malaysia

[c] Universiti Poly-Tech Malaysia, Faculty of Computing and Multimedia, Malaysia

Abstract

One of the sub-fields in information security is called information hiding and can be applied to protect data and information nowadays. This is a method in where secret-messages are hidden stealthily in an image file. This method has been used in various fields especially in digital image steganography. Most of the techniques proposed to date have various problems i.e., non-random changes will obviously occur especially when the secret message is embedded in an inappropriate area and when the load capacity exceeds the number of bits allowed. This paper proposes a machine learning steganographic method called SVM-Steg model that uses embedding and extracting algorithms by exploiting SVM classification and SVM-Steg embedding to achieve good performance. In addition, the distance of the embedding location is also taken into account so that more pixels can be embedded at more distance locations. The results show a quality cover-image when high peak signal-to-noise ratio (PSNR) values are recorded

greater for all types of cover images. In comparison to the other technique, all PSNRs for the proposed technique, SVM-Steg Method achieved 40 or higher. It is not only succeeding in providing a secure embedding position, but also increases the number of secret-bits embedded. © 2023 IEEE.

Author keywords

Digital Image Steganography; Information hiding; Machine learning; Secret-messages; Support Vector Machine

Indexed keywords

SciVal Topics

References (44)

View in search results format >

All

Export Print E-mail Save to PDF Create bibliography

1 Sasmal, M., Mula, D.

An enhanced method for information hiding using LSB steganography

(2021) *Journal of Physics: Conference Series*, 1797 (1), art. no. 012015. Cited 4 times.
http://iopscience.iop.org/journal/1742-6596
doi: 10.1088/1742-6596/1797/1/012015

View at Publisher

2 Nolkha, A., Kumar, S., Dhaka, V.S.

Image Steganography Using LSB Substitution: A Comparative Analysis on Different Color Models

(2020) *Smart Innovation, Systems and Technologies*, 141, pp. 711-718. Cited 10 times.
http://www.springer.com/series/8767
ISBN: 978-981138405-9
doi: 10.1007/978-981-13-8406-6_67

View at Publisher

3 Mados, B., Balaz, A., Adam, N., Hurtuk, J.

Information hiding into OBJ format file using vector steganography techniques

(2018) *SACI 2018 - IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, art. no. 8440965, pp. 91-95. Cited 4 times.
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8412770
ISBN: 978-153864640-3
doi: 10.1109/SACI.2018.8440965

View at Publisher

4 Tao, J., Li, S., Zhang, X., Wang, Z.

Towards Robust Image Steganography

(2019) *IEEE Transactions on Circuits and Systems for Video Technology*, 29 (2), art. no. 8533349, pp. 594-600. Cited 125 times.
doi: 10.1109/TCSVT.2018.2881118

View at Publisher

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us