



[< Back to results](#) | 1 of 1
[Export](#)
[Download](#)
[Print](#)
[E-mail](#)
[Save to PDF](#)
[Add to List](#)
[More... >](#)
[Full Text](#)
[View at Publisher](#)

 Indonesian Journal of Electrical Engineering and Computer Science
 Volume 12, Issue 2, November 2018, Pages 716-721

Concealment of files blocked by gmail with EOF-based image steganography (Article)

 Taufik, I.^a , Syaripudin, U.^a, Kaffah, F.M.^a, Ismail, N.^b, Sobirin, J.G.^a, Gunawan, T.S.^c 
^aInformatic Engineering Department, Faculty of Science and Technology, UIN Sunan Gunung Djati, Jalan A.H Nasution 105, Bandung, 40614, Indonesia

^bElectrical Engineering Department, Faculty of Science and Technology, UIN Sunan Gunung Djati, Jalan A.H Nasution 105, Bandung, 40614, Indonesia

^cDepartment of Electrical and Computer Engineering, Kulliyah of Engineering International Islamic University Malaysia, Jalan Gombak, Kuala Lumpur, 53100, Malaysia

Abstract

[View references \(13\)](#)

Nowadays, due to security concern, not all the process of sending files via email runs smoothly. There are several types of file extensions that are blocked when sent via email. For examples, there are several file extensions blocked by Gmail. This paper discusses steganographic implementation using End of File (EOF) algorithm to insert special file into image cover file with JPG and PNG format so that files with these extensions can be sent via email. Before a special extension file is inserted into the cover file, a compression process should be conducted first to make the file size smaller. The proposed algorithm is implemented on Visual Basic.Net software. Based on the tests performed, the application can insert Gmail-blocked file system to the image cover file, without changing the physical bit of the image cover file or file system that inserted with 100% success rate. The stego-image file is also successfully sent via email without being blocked. © 2018 Institute of Advanced Engineering and Science. All rights reserved.

Author keywords

[End of file](#)
[Gmail](#)
[Image cover file](#)
[Insertion](#)
[Steganography](#)
ISSN: 25024752

Source Type: Journal

Original language: English

DOI: 10.11591/ijeecs.v12.i2.pp716-721

Document Type: Article

Publisher: Institute of Advanced Engineering and Science

References (13)

[View in search results format >](#)
 All
 [Export](#)
[Print](#)
[E-mail](#)
[Save to PDF](#)
[Create bibliography](#)

- 1 Mabry, F.J., James, J.R., Ferguson, A.J.
Unicode steganographic exploits

 (2007) *IEEE Security and Privacy*, 5 (5), pp. 32-39. Cited 3 times.
doi: 10.1109/MSP.2007.128

[View at Publisher](#)

Metrics

0 Citations in Scopus

0 Field-Weighted Citation Impact



PlumX Metrics

Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert >](#)
[Set citation feed >](#)

Related documents

Comparative review on feature-content based of public key steganography trends

 Abdul-Razak, N.H. , Din, R. , Ahmad, M.
(2018) *International Journal of Engineering and Technology(UAE)*

Study on Information Hiding Technology Based on Digital Image

 Chen, C.
(2018) *IOP Conference Series: Materials Science and Engineering*

An approach towards novel video steganography for consumer electronics

 Sushmitha, M.C. , Suresh, H.N. , Manikandan, J.
(2018) *2017 IEEE International Conference on Consumer Electronics-Asia, ICCE-Asia 2017*

View all related documents based on references

2 Gunawan, T.S., Lim, M.K., Zulkurnain, N.F., Kartiwi, M.

On the review and setup of security audit using Kali Linux

(2018) *Indonesian Journal of Electrical Engineering and Computer Science*, 11 (1), pp. 51-59. Cited 2 times.
<http://www.iaescore.com/journals/index.php/IJEECS/article/download/12645/8634>
doi: 10.11591/ijeecs.v11.i1.pp51-59

[View at Publisher](#)

3 Kour, J., Verma, D.

Steganography Techniques –A Review Paper

(2014) *International Journal of Emerging Research in Management & Technology*, 3, pp. 132-135. Cited 13 times.

4 Kaur, M., Sharma, V.K.

Encryption based LSB Steganography Technique for Digital Images and Text Data

(2016) *IJCSNS International Journal of Computer Science and Network Security*, 16, pp. 90-97. Cited 2 times.

5 Ramkumar, M., Akansu, A.N.

Capacity estimates for data hiding in compressed images

(2001) *IEEE Transactions on Image Processing*, 10 (8), pp. 1252-1263. Cited 50 times.
doi: 10.1109/83.935040

[View at Publisher](#)

6 Mstafa, R.J., Elleithy, K.M., Abdelfattah, E.

A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC

(2017) *IEEE Access*, 5, art. no. 7893733, pp. 5354-5365. Cited 4 times.
<http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639>
doi: 10.1109/ACCESS.2017.2691581

[View at Publisher](#)

7 Khodaei, M., Faez, K.

New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing

(2012) *IET Image Processing*, 6 (6), pp. 677-686. Cited 38 times.
doi: 10.1049/iet-ipr.2011.0059

[View at Publisher](#)

8 Tiwari, A., Yadav, S.R., Mittal, N.K.

A Review on Different Image Steganography Techniques

(2014) *International Journal of Engineering and Innovative Technology (IJETT)*, 3, pp. 121-124. Cited 2 times.

9 Rakhigawande, S.

A Review on Steganography Methods

(2013) *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2, pp. 4635-4638. Cited 6 times.

Find more related documents in
Scopus based on:

[Authors >](#) [Keywords >](#)