PLAGIARISME DAN METADATA

ROBBI RAHIM, S.KOM., M.KOM

WORKSHOP PENULISAN ARTIKEL ILMIAH
UNIVERSITAS ANDALAS PADANG
6-7 JULI 2018

LIST MATERI

1. PLAGIARISM/SIMILARITY

2. METADATA

PLAGIARISME

Plagiarisme adalah tindakan mengklaim karya orang lain baik tulisan, lagu, maupun ide menjadi milik sendiri.

PLAGIARISME

Dampak Plagiarisme

1. Merupakan ketidakjujuran akademik
2. Kurangnya integritas dan bisa menghancurkan karir akademik anda

PLAGIARISME

Cara menghindari Plagiarisme

1. Hindari kutipan langsung sebisa mungkin, maksimal hanya 10%.
2. Teknik paraphrase diperlukan untuk menghindari kemiripan kata/kalimat
3. Selalu ingat untuk mencitasi kutipan
4. Pada bidang Engineering/Physical Science **Kutipan Langsung Tidak Diperbolehkan**
5. Internal Citation digunakan untuk memberikan kredit kepada author yang hasil karyanya kita gunakan, biasanya ditandai dengan () atau “”, dan jangan lupa memberikan citasi

SIMILARITY CHECK

Apa itu Similarity Check

1. Teknik atau cara yang digunakan untuk memeriksa kemiripan kata/kalimat
2. Kata atau Kalimat yang sama belum tentu PLAGIAT, ex: common knowledge
3. Sebagai alat bantu pemeriksa **BUKAN PENGAMBIL KEPUTUSAN**, dikarenakan perlu pemeriksaan kembali secara manual oleh PEMERIKSA (Reviewer/Editor/TIM PAK)

SUMBER DATA aplikasi pendeteksi = *similaritas* :

! PENTING

- BAHWA SANGKAAN PLAGIASI SANGAT OFENSIF, JADI PERLU HATI² SAAT MEMUTUSKANNYA.
- BAHWA APLIKASI² YG ADA DI PASARAN ADALAH PENDETEKSI KEMIRIPAN $\neq$ PENDETEKSI PLAGIASI

- KOMUNIKASI DUA ARAH SANGAT PENTING.

DIBUAT OLEH : DASAPTA ERWIN IRAWAN
[ITB / INARXIV]

CC-BY

SIAPA YG PERLU MEMAHAMI?

POTENSI MASALAH DAPAT TIMBUL KARENA ...

Aplikasi Similarity Checker (ASC) mendeteksi beberapa hal sbb:

- 1) Kemiripan antara artikel dengan artikel lain dari penulis/tim penulis yang sama:**
 - a. versi *preprint* (versi *pra-peer-review*), *postprint* (versi setelah *peer-review*), yang diunggah ke repositori,
 - b. versi dokumen tugas akhir (skripsi/tesis/disertasi) yang diunggah ke repositori,
 - c. versi dalam laman blog, liputan pada laman berita, laman medsos (yang tidak diproteksi),

POTENSI MASALAH DAPAT TIMBUL KARENA ...

Aplikasi Similarity Checker (ASC) mendeteksi beberapa hal sbb:

- d. yang telah diperiksa sebelumnya oleh orang atau penulis yang lain (kasus Turnitin/iThenticate),**
- e. yang telah terbit sebelumnya, membahas topik yang berbeda, tapi dalam rangkaian riset yang sama,**

POTENSI MASALAH DAPAT TIMBUL KARENA ...

Aplikasi Similarity Checker (ASC) mendeteksi beberapa hal sbb:

- 2) **Kemiripan rujukan (daftar pustaka)** yang disitir dalam artikel dengan artikel lain dari penulis yang sama atau dari penulis yang berbeda.
- 3) **Kemiripan kata hubung, frasa**, yang tidak membentuk kalimat pernyataan lengkap pada artikel yang berbeda (baik dari penulis yang sama atau berbeda)

POTENSI MASALAH DAPAT TIMBUL KARENA ...

Aplikasi Similarity Checker (ASC) mendeteksi beberapa hal sbb:

- 4) Dalam kasus yang diinput adalah berkas PDF/DOCX lengkap satu terbitan prosiding konferensi atau terbitan jurnal, kesamaan antara judul artikel dengan daftar isi, daftar penulis, bahkan dengan *header/footer* juga akan terdeteksi,
- 5) Tautan terbuka (open-shared link) dari draft artikel yang ditulis menggunakan piranti lunak daring, misal: Google Docs, Authorea, Overleaf dan yang sejenisnya.

SEKILAS TENTANG PREPRINT, POSTPRINT, PUBLISHED VERSION

Ini adalah dokumen yang sama, tapi bisa muncul dalam tiga versi:

- Versi preprint (pra-peer-review)
- Versi post-print (pra-peer-review)
- Versi terbit (published version)

Tiga versi ini kemiripannya bisa sangat tinggi atau sama persis, bergantung kepada hasil peer-review.

Di [era sains terbuka](#) ini, [mengapa saat ini kita dibolehkan mengunggah versi preprint/postprint?](#)

PEMBUAT MASALAH?

Umumnya pembuat masalah (**yang sebenarnya bukan masalah**) adalah Pre-Print, Post-Print, Repository UnPublished Work.... Masih banyak beranggapan bahwa ini adalah publikasi...

POINT PENTING

Selagi artikel/dokumen belum terdapat di ISBN/ISSN cetak maupun online maka tidak dapat di bilang **PUBLISHED WORK** dan kemiripan yang terjadi adalah BIASA dan bukan PLAGIAT

PRE-PRINT apakah LEGAL? Self-Archiving Policy

Pre-Print By Springer

<https://www.springer.com/gp/open-access/authors-rights/self-archiving-policy/2124>

Pre-Print By Elsevier/Scopus

<https://www.elsevier.com/about/policies/sharing>

Pre-Print by Emerald

http://www.emeraldgrouppublishing.com/authors/writing/author_rights.htm

SIMILIARITY CHECK

Tool Similarity Checker

1. Turnitin -> Premium
2. iThenticate -> Premium
3. PlagiarismCheckerX -> Premium, free with limited
4. Grammarly -> Premium, free with limited
5. Whitesmoke -> Premium
6. Plagscan -> Premium
7. Unplag -> Premium

SIMILIARITY CHECK

Contoh Pemeriksaan

The screenshot shows a Microsoft Word document with the following content:

Navigation

Search document

HEADINGS | PAGES | RESULTS

Create an interactive outline of your document.

It's a great way to keep track of where you are or quickly move your content around.

To get started, go to the Home tab and apply Heading styles to the headings in your document.

Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm

*usurobbi85@zoho.com

Abstract. This study aims to hide data or information on pixel image using EOF method and to improve the security of hidden data than combine with cryptography algorithm Modular Multiplication Block Cipher algorithm for the encryption process. The image file used as the test sample consists of 3 types of image types (JPG, BMP, PNG), this file type is the most widely used by users with different width and height as well as various file sizes. The results of this study prove that the data could embed in pixel image using EOF method after encryption process are perform, and also all embedded data can extract and read well without any restrictions, pixel image also back to original form before steganography processed.

1. Introduction

The era of information as it is today, data or information that is important and secret has become a precious asset [1]–[4]. Such valuable data or information will undoubtedly pose a risk if it can be freely accessed by unauthorized parties [5], [6]. Therefore, how data to be secure needs particular attention [7], [8].

One way to avoid crime against a data is to hide data from other media such as image [9]–[11], this technique is called steganography technique[12]. Steganography is the science and art of hiding messages within other media so that the existence of messages cannot be known [9], [12]–[14]. One of steganography method that is simple and easy to implement is End Of File (EOF) method [13]. The weakness of the EOF method is the secret messages can be easily extract using EOF method as well [15]. An improvement of embedded messages is necessary like using cryptography [16], one of an algorithm that can be used is Modular Multiplication Block Cipher [3], in this research Modular

PAGE 1 OF 5 1474 WORDS ENGLISH (UNITED STATES)

SIMILIARITY CHECK

GRAMMARLY PLAGIARISM DETECTION

The image is a screenshot of a Grammarly document editor. The title of the document is "Pixel Image Steganography Using EOF...". The main text of the document is as follows: "Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm", "The results of this study prove that the data could embed in pixel image using EOF method after encryption", and "The results of this study prove that the data could embed in pixel image using EOF method after encryption". The Grammarly interface shows a plagiarism score of 1% and a 12% unoriginal text score. The document text includes: "Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm", "The results of this study prove that the data could embed in pixel image using EOF method after encryption", and "The results of this study prove that the data could embed in pixel image using EOF method after encryption".

SIMILIARITY CHECK

PLAGIARISM CHECKER X DETECTION

Print Save

Plagiarism Checker X Originality Report

Plagiarism Quantity: 12% Duplicate

Date	Sunday, February 04, 2018
Words	176 Plagiarized Words / Total 1478 Words
Sources	More than 22 Sources Identified.
Remarks	Low Plagiarism Detected - Your Document needs Optional Improvement.

Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm
*usurobbi85@zoho.com Abstract. This study aims to hide data or information on pixel image using EOF method and to improve the security of hidden data than combine with cryptography algorithm Modular Multiplication Block Cipher algorithm for the encryption process. The image file used as the test sample consists of 3 types of image types (JPG, BMP, PNG), this file type is the most widely used by users with different width and height as well as various file sizes.

The results of this study prove that the data could embed in pixel image using EOF method after encryption process are perform, and also all embedded data can extract and read well without any restrictions, pixel image also back to original form before steganography processed. Introduction The era of information as it is

Sources found:

Click on the highlighted sentence to see sources.

Internet Pages

- <1% <https://www.scribd.com/document/36281216>
- <1% <https://link.springer.com/article/10.100>
- <1% https://en.wikipedia.org/wiki/Portable_N
- 1% <http://www.snapfiles.com/Freeware/gmm/fw>
- 1% <https://www.ripublication.com/ijaer18/ij>
- <1% <https://www.reddit.com/r/Steganography/c>
- <1% <https://www.researchgate.net/profile/Jun>
- <1% <https://www.google.com.au/patents/US7035>
- 1% <https://www.linkedin.com/learning/learni>
- 1% <http://ijsrst.com/paper/650.pdf>
- <1% <https://issuu.com/fcomfreelance/docs/key>

SIMILIARITY CHECK

PLAGIARISM CHECKERX DETECTION

Print Save

×

This study aims to hide data or information on pixel image using EOF method and to improve the security of hidden data than combine with cryptography algorithm Modular Multiplication Block Cipher algorithm for the encryption process. The image file used as the test sample consists of 3 types of image types (JPG, BMP, PNG), this file type is the most widely used by users with different width and height as well as various file sizes.

The results of this study prove that the data could embed in pixel image using EOF method after encryption process are perform, and also all embedded data can extract and read well without any restrictions, pixel image also back to original form before steganography processed. Introduction The era of information as it is today, data or information that is important and secret has become a precious asset [1]–[4]. Such valuable data or information will undoubtedly pose a risk if it can be freely accessed by unauthorized parties [5], [6].

Therefore, how data to be hidden in pixel image is a very important issue. One way to avoid crime against a data is called steganography technique [12]. Steganography is the science and art of hiding messages within other media so that the existence of messages cannot be known [9], [12]–[14]. One of steganography method that is simple and easy to implement is End Of File (EOF) method [13].

Duplicate content found on
<https://www.ripublication.com/ijaer18/ij>

The weakness of the EOF method is the secret messages can be easily extract using EOF method as well [15]. An improvement of embedded messages is necessary like using cryptography [16], one of an algorithm that can be used is Modular Multiplication Block Cipher [3], in this research Modular Multiplication Block Cipher are combined with EOF method for additional security. This research tries to combine Modular Multiplication Block Cipher with EOF method for securing embedded message in the pixel image.

Embedded message in the pixel will make a distortion/noise as if the image damaged due to faulty retrieval or incomplete data from transmission process [17]. The distortion in the image is the message itself and to read the message must be used EOF method and Modular Multiplication Block Cipher algorithm for decryption.

SIMILIARITY CHECK

PLAGIARISM CHECKERX DETECTION

Print Save

Educ., vol. 15, no. 3, pp. 292-297, 2017. [7] J. Arvin S. Lat, R. Xavier R. Bondoc, and K. C. V. Atienza, "SOUL System: secure online USB login system," Inf. Manag. Comput. Secur., vol. 21, no. 2, pp. 102-109, 2013. [8] M. xiaojuan, "Research and Implementation of Computer Data Security Management System," Procedia Eng., vol. 174, pp. 1371-1379, 2017. [9] D. Rachmawati, A. Amalia, and J. Surya, "Combination of Huffman Coding Compression Algorithm and Least Significant Bit Method for Image Hiding," in Journal of Physics: Conference Series, 2017, vol.

801, no. 1. [10] B. S. Champakamala, K. Padmini, R. D. K. A. Professors, and D. Bosco, "Least Significant Bit algorithm for image steganography Overview of Steganography," Int. J. Adv. Comput. Technol., vol. 3, no. 4, p. 5, 2014. [11] P. Sethi and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography," in Procedia Computer Science, 2016, vol. 87, pp. 61-66. [12] H. Nurdyanto and R.

Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," in 2017 3rd International Conference on Science in Information Technology (ICSITech), 2017, pp. 366-371. [13] H. Wandani, M. Budiman, and A. Sharif, "Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem," Alkhawarizmi, 2012. [14] R. Bhardwaj and V. Sharma, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution," in Procedia Computer Science, 2016, vol.

93, pp. 832-838. [15] C. Iswahyudi, E. Setyaningsih, and N. Widyastuti, "Pengamanan kunci enkripsi Citra pada algorithm super enkripsi menggunakan metode end of file," Pros. Semin. Nas. Apl. Sains Teknol. Periode III, no. November, pp. 278-285, 2012. [16] H. Nurdyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," J. Phys. Conf. Ser., vol. 930, no. 1, p.

SIMILIARITY CHECK

TURNITIN SIMILIARITY CHECK

Feedback Studio - Mozilla Firefox

https://ev.turnitin.com/app/carta/en_us/?u=1047623450&lang=en_us&o=910713369&s=3

feedback studio

Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm

-- /0

3 of 8

Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm

*usurobbi85@zoho.com

Abstract. This study aims to hide data or information on pixel image using EOF method and to improve the security of hidden data than combine with cryptography algorithm Modular Multiplication Block Cipher algorithm for the encryption process. The image file used as the test sample consists of 3 types of image types (JPG, BMP, PNG), this file type is the most widely used by users with different width and height as well as various file sizes. The results of this study prove that the data could embed in pixel image using EOF method after encryption process are perform, and also all embedded data can extract and read well without any restrictions, pixel image also back to original form before steganography processed.

1. Introduction

The era of information as it is today, data or information that is important and secret has become a precious asset [1]–[4]. Such valuable data or information will undoubtedly pose a risk if it can be freely accessed by unauthorized parties [5], [6]. Therefore, how data to be secure needs particular attention [7], [8].

One way to avoid crime against a data is to hide data from other media such as image [9]–[11], this technique is called steganography technique[12]. Steganography is the science and art of hiding

Match Overview

16%

1	Robbi Rahim, Hendryan...	4%	>
	Publication		
2	ijair.id	2%	>
	Internet Source		
3	Submitted to Trident U...	1%	>
	Student Paper		
4	Submitted to Manav Ra...	1%	>
	Student Paper		
5	Submitted to Troy Univ...	1%	>
	Student Paper		
6	dblp.dagstuhl.de	1%	>
	Internet Source		
7	jurnal.usu.ac.id	1%	>
	Internet Source

SIMILIARITY CHECK

TURNITIN SIMILARITY CHECK

Feedback Studio - Mozilla Firefox

https://ev.turnitin.com/app/carta/en_us/?u=1047623450&lang=en_us&o=910713369&s=3

feedback studio

Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm

-- /0

3 of 8

Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm

*usurobbi85@zoho.com

Abstract. This study aims to hide data or information on pixel image using EOF method and to improve the security of hidden data than combine with cryptography algorithm Modular Multiplication Block Cipher algorithm for the encryption process. The image file used as the test sample consists of 3 types of image types (JPG, BMP, PNG), this file type is the most widely used by users with different width and height as well as various file sizes. The results of this study prove that the data could embed in pixel image using EOF method after encryption process are perform, and also all embedded data can extract and read well without any restrictions, pixel image also back to original form before steganography processed.

1. Introduction

The era of information as it is today, data or information that is important and secret has become a precious asset [1]–[4]. Such valuable data or information will undoubtedly pose a risk if it can be freely accessed by unauthorized parties [5], [6]. Therefore, how data to be secure needs particular attention [7], [8].

One way to avoid crime against a data is to hide data from other media such as image [9]–[11], this technique is called steganography technique[12]. Steganography is the science and art of hiding

Match Overview

0%

There are no matching sources for this report.

METADATA

1. Metadata adalah informasi yang dibuat pada web untuk dibaca oleh computer dan mesin pencari untuk memudahkan pencarian berdasarkan “Kata Kunci” tertentu, umumnya metadata merupakan informasi penting dari keseluruhan artikel/dokumen/informasi pada web-page
2. Metadata bersifat Publik baik pada Journal OA maupun non-OA
3. Pada jurnal, metadata berisi informasi umum pada artikel yang bisa di baca/extract oleh mesin pencari ataupun software khusus pembaca metadata seperti Mendeley dan EndNote

METADATA

Umumnya informasi metadata pada Artikel journal dan Publisher Proceeding (Scopus/GS) terdiri dari:

1. Nama Journal / Publisher
2. Volume, Issue, Tanggal Publikasi, Halaman
3. Judul Artikel
4. Author name dan Afiliasi
5. Abstrak
6. Keyword
7. References
8. ISSN/ISBN, DOI (if any)
9. Copyright Statement

MISCONDUCT in METADATA

Beberapa Misconduct Metadata – References:

1. Pengubahan reference pada artikel tanpa se-izin penulis
2. Manipulasi metadata pada sistem/ojs sehingga terjadi ketidak sinkron-an antara metadata sistem dan artikel
3. Fabrikasi, memoles data tanpa proses ilmiah dan kemudian dipublikasikan – Logbook salah satu cara untuk menghindari fabrikasi.
4. Falsifikasi, mengubah/membuang data hasil penelitian dan kemudian melaporkan hasil researchh secara sah – Termasuk peralatan yang digunakan.
5. Self-Citation
6. Conflict of Interest

PENUTUP

TERIMA KASIH