Jurnal Quancom
Vol.3, No.1, Juni 2025, pp. 18~24
e-ISSN: 2988-0998
P-ISSN: 2988-1005
DOI: https://doi.org/10.62375/jqc.v3i1.434

Metode Steganografi EOF untuk Penyisipan Pesan Teks Tersembunyi

Sarah Hutahaean [1]*, Mega Malau [2], Gilberd Siboro [3s]
[1, 2,3]Sarjana Terapan Teknologi Perangkat Lunak, Institut Teknologi Del
Sitoluama, Laguboti, Toba 22381
sarahhth12@gmaill.com[1],megamalau912@gmail.com[2],gsiboro11016@gmail.com[3]

Article Info

Article history:

Received 9 Desember 2024
Revised 24 Desember 2024
Accepted 26 Desember 2024

Keyword:

End of File, Fidelity, GifShuffle, Recovery, Steganografi

ABSTRACT

The transmission of information has become an essential aspect of human life in the modern technological era. Innovations continue to be developed to simplify and accelerate data exchange processes. However, threats to information security, such as data theft, sabotage, and unauthorized access, have also increased significantly. Therefore, innovative solutions are needed to protect information, especially confidential data involving two parties who wish to maintain its secrecy. In this context, research on steganography has become highly relevant. This study employs the End Of File (EOF) steganography technique, which enables embedding secret messages at the end of digital image files. This technique is chosen for its ability to conceal data without significantly altering the main structure of the image file. The embedding process is carried out meticulously so that the final product, known as the stego image, resembles an ordinary image file without any noticeable signs of modification. The primary advantage of the EOF technique lies in its efficiency in embedding and retrieving secret messages, making it a suitable solution for secure message transmission. The findings indicate that stego images produced using the EOF technique not only preserve the integrity of the original image but also enable quick and easy retrieval of messages by authorized recipients. This makes the technique an effective method to prevent data theft or sabotage during transmission. Amid the growing threats of cybercrime, EOF steganography offers an innovative solution to ensure information security while maintaining message confidentiality. Thus, it serves as a promising alternative for advancing future information security technologies.

PENDAHULUAN

Steganografi adalah seni menyembunyikan pesan teks sedemikian rupa sehingga tak seorang pun selain pengirim dan penerima yang dituju mengetahui keberadaan informasi tersebut. [1] Steganografi berfungsi untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi, dan juga dapat melindungi hak cipta dari suatu produk. Data rahasia yang disembunyikan dapat diungkapkan kembali sama seperti aslinya tanpa merusak media file dan pesannya. Steganografi menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hamper terlihat sama. [2] Steganografi sudah digunakan sejak dahulu kala sekitar 2500 tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi. Dan sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan pada kerahasian komunikasinya bukan pada datanya.[3]

Pada steganografi citra digital dapat digunakan untuk mengirimkan pesan atau informasi rahasia, sehingga steganografi citra harus diuji ketahanan nya terhadap serangan yang mungkin bisa terjadi. Salah satu ukuran kekuatan dalam metode steganografi adalah faktor kekokohan atau ketahanan. Untuk mengetahui kekokohan gambar hasil steganografi, dapat dilakukan pengujian robustness untuk

menunjukkan kemampuan informasi yang tersembunyi (payload) bertahan dari proses (embedding) dan ekstraksi, termasuk beberapa manipulasi seperti penyaringan (filtering), pemangkasan (cropping), rotasi (rotating), dan kompresi (compression). [4] Citra adalah suatu suatu gambaran atau kemiripan dari suatu objek. Citra analog tidak dapat direpresentasikan dalam komputer, sehingga tidak bisa diproses oleh komputer secara langsung. Citra digital adalah citra yang yang dapat diolah oleh komputer. Citra yang dihasilkan dari peralatan digital (citra digital) langsung bisa diolah oleh komputer. [5] Citra adalah suatu representasi (gambaran), kemiripan atau imitasi dari suatu objek. Secara harfiah, citra (Image) adalah gambar pada bidang dwimatra (2 dimensi). Ditinjau dari sudut pandang sistematis, citra merupakan fungsi continue dari intensitas cahaya pada bidang dwimatra (2D). [6] Tujuan utama steganografi adalah untuk menyembunyikan informasi dengan baik, sehingga penerima yang tidak berhak atas informasi tersebut tidak mencurigai media steganografi yang berisi data rahasia yang tersembunyi [7]

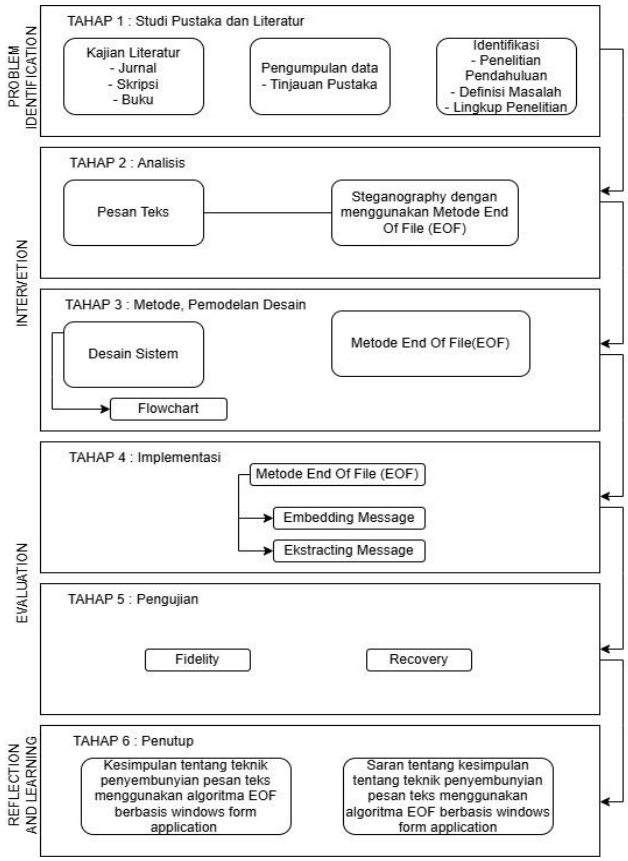
melakukan penelitian steganografi untuk menyembunyikan pesan teks menggunakan algoritma End of File, dalam tersebut menggunakan algoritma End of File dan menyisipkan informasi kedalam media citra digital pada bagian akhir file gambar, pada penelitian tersebut dilakukan dua pengujian yaitu, pengujian tanpa serangan dan pengujian dengan menggunakan serangan. Pada pengujian tanpa serangan hanya mengukur dari segi kualitas dan mutu gambar, sesuai dengan skenario pengujian, hasil dari pengujian membuktikan bahwa stego-image yang dihasilkan dengan metode end of file tidak memberikan perubahan signifikan dikarenakan gambar hasil steganografi ini hanya mengubah ukuran gambar bukan merubah piksel maupun intensitas warna sehingga dapat disimpulkan secara kasat mata, indera manusia tidak dapat mendeteksi perubahan gambar tersebut. [8]

Algoritma EoF merupakan pengembangan dari algoritma LSB, dimana algoritma LSB merupakan algoritma terapan dari algoritma substitusi. Teknik ini menggantikan bit yang paling akhir dari data asli dengan bit pesan. Sehingga pesan yang disisipkan terbatas sedangkan algoritma EoF menambahkan data atau pesan pada akhir file. Pada algoritma EoF perhitungan ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah ukuran data rahasia yang telah diubah menjadi encoding file. Dari ketiga algoritma diatas algoritma EoF memiliki kelebihan dari kedua algoritma LSB dan GifShuffle yaitu dapat menyisipkan pesan yang lebih banyak. Pada algoritma LSB pesan yang disisipkan terbatas sedangkan pada GifShuffle hanya dapat disisipkan pesan dengan ukuran yang relatif lebih kecil yaitu 209 byte. [9]Teknik ini digunakan dengan cara menambahkan data atau pesan rahasia pada akhir file. Perhitungan ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah ukuran data rahasia yang telah diubah menjadi encoding file. [10]

METODE

Penelitian ini dilakukan melalui beberapa tahapan sistematis untuk mencapai tujuan yang telah ditentukan, yaitu mengimplementasikan metode steganografi End Of File (EOF) dalam penyisipan pesan rahasia pada file citra digital berformat JPG. Tahapan penelitian diawali dengan Studi Pustaka dan Literatur, yang mencakup kajian mendalam terhadap literatur dari jurnal, skripsi, dan buku untuk memahami dasar-dasar steganografi dan metode EOF. Tahap ini bertujuan untuk mengidentifikasi penelitian terdahulu, mendefinisikan masalah, dan menentukan lingkup penelitian yang akan dilakukan. Selanjutnya, pada Tahap Analisis, dilakukan eksplorasi terhadap konsep penyisipan pesan teks ke dalam file citra menggunakan metode EOF. Analisis ini memastikan bahwa pesan dapat disisipkan tanpa merusak integritas file pembawa. Hasil analisis tersebut menjadi dasar untuk Tahap Pemodelan dan Desain, di mana sistem dirancang secara konseptual menggunakan flowchart untuk memvisualisasikan alur proses penyisipan (embedding) dan ekstraksi (extracting) pesan. Desain ini difokuskan untuk menciptakan metode yang efisien dan andal dalam menyisipkan pesan rahasia ke dalam file citra. [11]

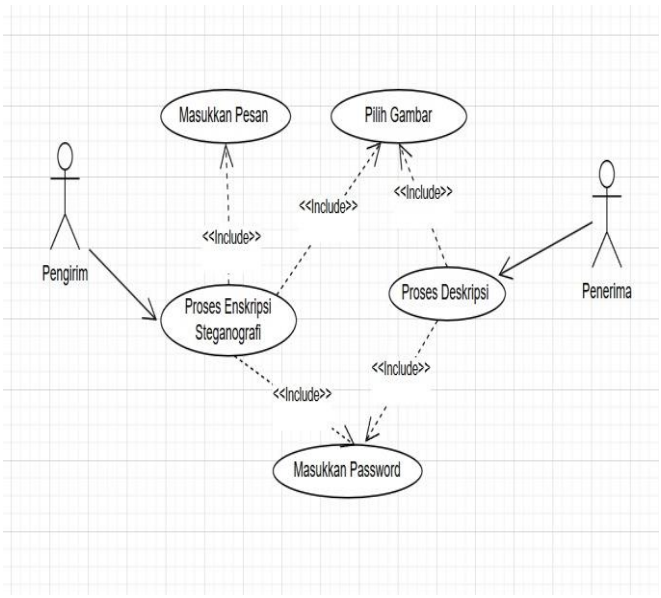
Pada Tahap Implementasi, metode EOF diimplementasikan ke dalam dua proses utama: penyisipan pesan (embedding) dan ekstraksi pesan (extracting). Implementasi ini bertujuan untuk merealisasikan desain yang telah dirancang sebelumnya, memastikan pesan dapat disisipkan dan diambil kembali tanpa kehilangan data. Setelah implementasi, sistem diuji pada Tahap Pengujian dengan menggunakan dua parameter utama: fidelity dan recovery. Fidelity mengukur apakah kualitas file citra tetap terjaga setelah proses penyisipan pesan, sementara recovery memastikan bahwa pesan yang disisipkan dapat diekstraksi kembali secara utuh dan sesuai dengan aslinya.Penelitian diakhiri pada Tahap Penutup, di mana kesimpulan ditarik berdasarkan hasil implementasi dan pengujian. Kesimpulan ini memberikan gambaran tentang keberhasilan metode EOF dalam menyisipkan dan mengekstrak pesan teks pada file citra digital berbasis aplikasi Windows. Selain itu, saran disampaikan untuk pengembangan lebih lanjut, seperti optimalisasi algoritma atau penerapan pada format file lain. Dengan pendekatan ini, penelitian diharapkan dapat memberikan kontribusi signifikan dalam pengembangan teknologi steganografi yang efisien dan aman. [12]



Gambar 1. Tahapan penelitian

A. Diagram Use-Case

Diagram *use case* ini menggambarkan proses pengiriman pesan menggunakan steganografi dan enkripsi. Pengirim memulai dengan memasukkan pesan, memilih gambar, dan memasukkan kata sandi, yang semuanya terhubung dalam proses utama "Proses Enkripsi Steganografi". Proses ini menghasilkan sebuah gambar yang berisi pesan terenkripsi, yang kemudian dikirimkan ke Penerima. Untuk membaca pesan, Penerima melakukan "Proses Deskripsi" dengan menggunakan kata sandi yang sama untuk mendekripsi dan mengambil pesan tersembunyi. Relasi <<Include>> menunjukkan bahwa langkah-langkah seperti memasukkan pesan, memilih gambar, dan memasukkan kata sandi adalah bagian integral dari proses enkripsi. Diagram ini menunjukkan alur kerja aplikasi yang mengamankan pesan melalui penyisipan data dalam gambar dengan perlindungan berbasis kata sandi.



Gambar 2. Use case diagram

B. Flowchart Embedding Pesan

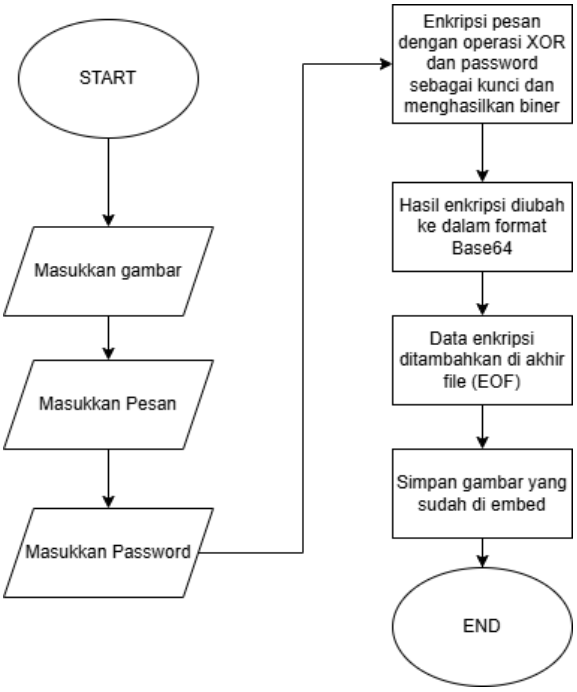
Pada proses *Embedding* pesan ini menyembunyikan pesan rahasia ke dalam sebuah gambar, yang dikenal sebagai embedding, merupakan teknik yang umum digunakan dalam steganografi, yaitu seni dan ilmu menyembunyikan informasi. Proses ini dimulai dengan pemilihan gambar yang akan berfungsi sebagai media atau "cover" untuk pesan rahasia. Setelah gambar dipilih, pengguna memasukkan pesan teks yang ingin disembunyikan, yang kemudian diubah menjadi bentuk digital, biasanya dalam format biner. Selanjutnya, pengguna juga diminta untuk memasukkan kata sandi (password) yang berfungsi sebagai kunci untuk mengenkripsi pesan sebelum disembunyikan.

Pesan tersebut kemudian dienkripsi menggunakan operasi logika biner XOR, di mana password berperan sebagai kunci. Operasi ini menghasilkan data biner yang aman. Hasil enkripsi selanjutnya diubah ke dalam format Base64, yang merupakan representasi biner dalam bentuk karakter ASCII, sehingga memudahkan penggabungan data ke dalam gambar. Proses embedding dilanjutkan dengan menambahkan data terenkripsi tersebut di akhir file gambar (EOF), posisi yang dipilih karena biasanya tidak diperiksa dan tidak merusak tampilan visual gambar. Setelah proses ini selesai, gambar yang telah berisi pesan rahasia disimpan, dan tampilan gambar akhir akan tetap sama dengan gambar aslinya, sehingga keberadaan pesan tersembunyi tidak akan terlihat oleh orang yang tidak mengetahui cara mengekstraknya.

Keunggulan metode ini terletak pada keamanan, di mana pesan rahasia sulit dideteksi jika tidak diketahui cara mengekstraknya, serta kapasitasnya yang mampu menyimpan pesan berukuran cukup besar tergantung pada ukuran gambar. Selain itu, prosesnya relatif sederhana dan dapat

diimplementasikan menggunakan berbagai bahasa pemrograman. Namun, metode ini juga memiliki beberapa kekurangan, seperti kerentanan terhadap perubahan pada gambar, yang dapat merusak atau menghilangkan pesan rahasia jika gambar mengalami kompresi atau pengeditan.

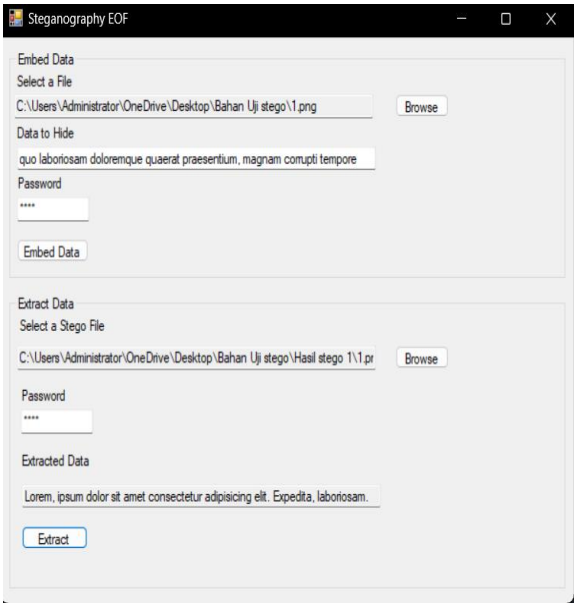
Keterbatasan kapasitas penyimpanan pesan juga menjadi perhatian, karena kapasitas tersebut dibatasi oleh ukuran gambar. Penerapan teknik embedding ini sangat luas, mencakup steganografi untuk menyembunyikan informasi rahasia, digital watermarking untuk menandai kepemilikan karya digital, serta kriptografi untuk melindungi data sensitif.



Gambar 3. Flowchart embedding pesan

HASIL DAN PEMBAHASAN

Pengujian steganografi dilakukan untuk mengevaluasi keberhasilan aplikasi dalam menyisipkan dan mengekstraksi pesan teks pada cover image menggunakan teknik EOF (End of File). Pesan teks yang dimasukkan pengguna dienkripsi menggunakan algoritma XOR dengan password, kemudian dikonversi ke dalam format Base64 untuk mempermudah penyisipan. Data hasil enkripsi ini ditambahkan ke bagian akhir file gambar tanpa mengubah struktur utama file, diawali dengan penanda khusus seperti EOF:. Ekstraksi dilakukan dengan membaca kembali file gambar, mencari penanda EOF:, dan mengambil data setelahnya untuk didekripsi menggunakan password. Keberhasilan diuji dengan memastikan data teks dapat disisipkan tanpa merusak file gambar dan dapat diekstraksi kembali secara utuh.



Gambar 4. Tampilan aplikasi

A. Skenario Pengujian

Pengujian dilakukan melalui dua skenario, yaitu tanpa serangan dan dengan serangan. Pada skenario tanpa serangan, pengujian difokuskan pada kualitas citra setelah melalui proses steganografi, meliputi fidelity dan recovery. Sementara itu, pada skenario dengan serangan, citra yang telah disisipi data diuji ketahanannya (*robustness*) dengan memberikan berbagai serangan, seperti pemotongan (*cropping*) dan perputaran (*rotation*) pada stego image.

B. Pengujian Tanpa Serangan

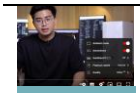
Pengujian ini dilakukan tanpa serangan, yaitu hanya berfokus pada pengukuran kualitas dan mutu citra yang dihasilkan melalui nilai-nilai tertentu. Adapun pengujian yang dilakukan meliputi fidelity, akurasi penyisipan data, dan kemampuan pemulihan data (recovery) setelah proses steganografi :

C. Fidelity

Pengujian ini dilakukan untuk memastikan bahwa mutu media tidak mengalami perubahan signifikan setelah proses penyisipan data. Pada pengujian *fidelity* ini akan dilakukan pengujian :

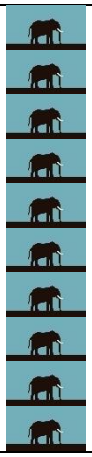
Pengujian dengan menggunakan 10 gambar sebagai media penampung dengan ukuran yang beragam dengan pesan yang disisipkan 500 karakter. Pengujian kedua dilakukan menggunakan media penampung yang sama, tetapi dengan variasi jumlah pesan yang disisipkan untuk mengamati pengaruhnya terhadap mutu dan kualitas media.

TABEL I
HASIL PENGUJIAN FIDELITY PERTAMA

Gambar	Ukuran (bytes)	Karakter	Ukuran Karakter (bytes)	Ukuran Stego (bytes)
	378,738	500	500	383,799
	8,853	500	500	13.914
	13,223	500	500	18,284
	13,008	500	500	18,069
	28,478	500	500	33,539
	8,057	500	500	13,118
	4,980	500	500	10,041
	18,505	500	500	23,566
	6,032	500	500	11,093
	6,644	500	500	11,705

Pada tabel menunjukkan hasil pengujian pada 10 gambar berbeda dengan penyisipan pesan berjumlah 500 karakter, di mana setiap karakter setara dengan 1 byte sehingga ukuran pesan menjadi 500 byte.. Hasil pengujian menunjukkan bahwa penyisipan pesan hanya menambah ukuran file gambar tanpa mempengaruhi intensitas warna pada setiap piksel. Namun, dengan pesan 500 karakter, terlihat adanya perubahan signifikan pada ukuran file gambar.

TABEL II
HASIL PENGUJIAN FIDELITY KEDUA

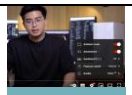
Gambar	Ukuran (bytes)	Karakter	Ukuran Karakter (bytes)	Ukuran Stego (bytes)
	8,853	10	10	8,954
	8,853	20	20	9,074
	8,853	30	30	9,162
	8,853	40	40	9,250
	8,853	50	50	9,382
	8,853	60	60	9,458
	8,853	70	70	9,574
	8,853	80	80	9,654
	8,853	90	90	9,770
	8,853	100	100	9,384

Dengan memeriksa 10 gambar identik dengan pesan tertanam yang bervariasi panjangnya dari 10 hingga 100 karakter, di mana setiap karakter sama dengan 1 byte, pesan tertanam berukuran antara 10 dan 100 byte. Dari hasil ini, dapat disimpulkan bahwa menambahkan sejumlah kecil pesan antara 10 dan 100 karakter tidak menyebabkan perubahan signifikan pada ukuran berkas gambar.

D. Pengujian Recovery

Pengujian recovery dilakukan untuk menguji apakah pesan rahasia yang disisipkan dalam citra digital dapat dipisahkan kembali dari stego-image-nya. Proses ini dilakukan dengan memeriksa keutuhan pesan yang diekstraksi dari beberapa citra uji. Berikut adalah langkah-langkah recovery yang dilakukan.

TABEL III
PENGUJIAN RECOVERY

Gambar	Normal	*Recovery*
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil
	✓	Berhasil

Dari hasil pengujian recovery yang tercantum dalam laporan pada tabel di atas, dapat disimpulkan bahwa pesan rahasia yang disisipkan pada sebuah citra dapat dipisahkan kembali dari stego-imagenya jika proses dilakukan dengan normal dan tanpa adanya serangan.

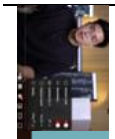
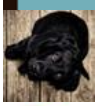
E. Pengujian Dengan Serangan

Pengujian ini dilakukan dengan serangan yang berarti melakukan sesuatu terhadap citra yang telah disisipkan pesan, dan untuk pengujiannya yaitu :

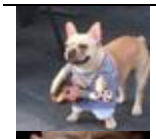
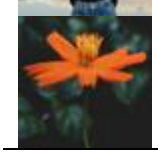
F. Robustness

Pengujian *robustness* bertujuan untuk mengevaluasi apakah pesan rahasia yang telah disisipkan ke dalam gambar steganografi dapat diekstraksi kembali dengan baik, meskipun gambar tersebut mengalami serangan seperti rotasi atau pemotongan.

TABEL IV
HASIL PENGUJIAN DENGAN GAMBAR ROTASI

Gambar	Ukuran Asli (bytes)	Ukuran Gambar Putar (bytes)	*Recovery*
	383,799	376,597	Gagal
	13.914	17,163	Gagal
	18,284	21,833	Gagal
	18,069	30,742	Gagal
	33,539	57,862	Gagal

TABEL V
HASIL PENGUJIAN DENGAN GAMBAR PEMOTONGAN

Gambar	Ukuran Asli (bytes)	Ukuran Gambar Putar (bytes)	*Recovery*
	13,118	11,828	Gagal
	10,041	9,566	Gagal
	23,566	22,044	Gagal
	11,093	9,960	Gagal
	11,705	9,254	Gagal

Pengujian robustness dilakukan dengan menyerang citra digital melalui rotasi dan pemotongan. Hasil pengujian menunjukkan bahwa rotasi pada citra yang telah disisipkan pesan rahasia, menggunakan rotasi ke kanan 90 derajat, menyebabkan peningkatan ukuran file, sedangkan pemotongan citra digital yang dilakukan secara acak justru mengurangi ukuran file tersebut. Namun, baik rotasi maupun pemotongan citra digital mengakibatkan pesan rahasia yang disisipkan tidak dapat diungkap kembali. Hal ini menunjukkan bahwa kedua serangan tersebut memiliki dampak yang signifikan terhadap integritas pesan rahasia yang disisipkan.

SIMPULAN

Pada pengujian *fidelity*, dapat disimpulkan bahwa penyisipan pesan dengan ukuran kecil (10–100 karakter) tidak menyebabkan perubahan signifikan pada ukuran file gambar, sementara penyisipan pesan yang lebih besar (500 karakter) menambah ukuran file secara signifikan, meskipun tetap tidak mempengaruhi intensitas warna pada setiap piksel gambar. Hal ini menunjukkan bahwa metode End of File (EOF) memiliki dampak minimal terhadap visualisasi gambar, tetapi perubahan ukuran file bergantung pada panjang pesan yang disisipkan. Dari hasil pengujian *robustness*, dapat disimpulkan bahwa serangan berupa rotasi dan pemotongan pada citra digital yang telah disisipkan pesan rahasia mempengaruhi ukuran file, dengan rotasi menyebabkan peningkatan ukuran dan pemotongan mengurangi ukuran. Namun, kedua jenis serangan tersebut mengakibatkan pesan rahasia tidak dapat dipulihkan, menunjukkan kelemahan metode terhadap manipulasi citra.

DAFTAR PUSTAKA

[1] Munir. Rinaldi, 2004, "*Pengolahan Citra Digital Dengan Pendekatan Algoritmik*", Informatika, Bandung

[2] Ariyus, Dony. 2009. "*Keamanan Multimedia*", Yogyakarta: Andi Publisher

[3] Alam, Ibnu. , "*Aplikasi Kode Huffman dalam Kompresi Gambar Berformat JPEG*", Makalah, Institut Teknologi Bandung.

[4] Ujianto, E.I.H., A,. Harjoko, R., Wardoyo, A., Moesirami,2015, "*Cascaded Image Steganography to Increase Robustness against attack of the Stego Image*", Journal of Theoretical and Applied Information Technology 30th September 2015. Vol.79. No.3.

[5] Andono, N, P., Sutojo., T., Muljono., 2017, "*Pengolahan Citra Digital, Andi*", Yogyakarta.

[6] Sembiring, S., 2013. "*Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File*". Jurnal Pelita Informatika Budi Darma, volume : iv, nomor:2.

[7] Shashikala,. C, Ajay, J., 2009, "*Steganography An Art of Hiding Data*", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

[8] Darwis., D., Kisworo., 2017, "*Teknik steganografi untuk penyembunyian pesan teks menggunakan algoritma end of file, Program Studi Manajemen Informatika*" , AMIK Teknokrat Lampung, Kedaton, Bandar Lampung.

[9] Darwis. Dedi, "*Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma Gifshuffle*", Jurnal TEKNOINFO, Vol.11, No.1, 2017, ISSN 1693-0010.

[10] Wasino., Tri Puji Rahayu., Setiawan. 2012. "*Implementasi Steganografi Teknik End Of File Dengan Enkripsi Rijndael. Seminar Nasional Teknologi Informasi dan Komunikasi*" 2012 : Yogyakarta. http : //fti.uajy.ac.id/ sentika/ publikasi /makalah /2012/2012-20.pdf, 01 September 2012.

[11] Sejati, Adiputra. 2007. "*Studi dan Perbandingan Steganografi Metode EOF (End of File) dengan DCS (Dynamic Cell Spreading)*". Bandung : Teknik Informatika Institut Teknologi Bandung

[12] Sukrisno, dan Utami, Ema. 2007. "*Implementasi Steganografi Teknik Eof Dengan Gabungan Enkripsi Rijndael, Shift Cipher Dan Fungsi Hash Md5*". Seminar Nasional Teknologi 2007 (SNT 2007). Yogyakarta : STMIK AMIKOM ISSN : 1978 – 9777