Terbit pada laman web jurnal : **http://ojsamik.amikmitragama.ac.id**

JURNAL JARINGAN SISTEM INFORMASI ROBOTIK (JSR)
Vol. 7 No. 2 TAHUN 2023 E - ISSN : 2579-373X

KEAMANAN DATA MENGGUNAKAN TEKNIK STEGANOGRAFI DENGAN METODE *END OF FILE* (EOF)

Nurhasanah[1], Mokhamad Yusron Rafi [2], Perani Rosyani3

[1]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan. Indonesia
Email: [1]dosen01123@unpam.ac.id, [2] mokhamadyusronrafi23@gmail.com, [3]dosen00837@unpam.ac.id

Abstrak

Perkembangan dunia teknologi komunikasi dan informasi yang sangat pesat belakangan ini berpengaruh besar dalam segala aspek kehidupan manusia. Cepatnya perkembangan teknologi informasi saat ini didukung dengan pentingnya kebutuhan akan mendapatkan informasi. Dalam proses pengamanan data sangat penting untuk pertukaran pesan dan informasi yang akan dikirim. Informasi yang diambil maupun ditukar mempunyai banyak jenis, seperti teks, audio, video maupun gambar (*citra digital*). Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian informasi pada suatu media sedemikian rupa sehingga keberadaannya tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. PT. Pos Indonesia yang memiliki banyak data, ada yang sifatnya penting dan bukan sekedar data biasa. Permasalahan dari yang sedang berjalan saat ini salah satu isu yang sering dibahas adalah persoalan keamanan data, untuk menjaga kerahasiaan data tersebut. Penelitian ini betujuan untuk merancang dan membangun aplikasi sistem yang dapat menjaga keamanan data sehingga keberadaannya tidak dapat diketahui oleh pihak lain yang tidak berhak atas data pesan atau informasi tersebut. Pada penelitian ini menggunakan teknik steganografi dengan metode *End of File* (EOF) berbasis desktop dengan menggunakan bahasa pemrograman *Java.* Dengan adanya teknik steganografi pada media *citra digital*, maka penyimpanan suatu data yang bersifat rahasia akan memiliki tingkat keamanan yang baik. Sehingga pada akhirnya dengan sistem keamanan data yang dibangun ini, perusahaan PT. Pos Indonesia dapat meningkatkan keamanan data yang dikirimkan khususnya surat digital yang bersifar rahasia.

Kata Kunci: Steganografi, *Citra Digital*, Metode End of File, *Keamanan Data*, *Sistem Informasi*

Abstract

The growth of the world of communication and information technology that is currently rapid has the big influence all in aspects of human life. The current rapid growth of information technology is supported by the importance of gaining information. In the process of securing data, it is very important for the messages-reciprocity and information which will be sent. The retrieved-information or exchanged have many types such as text, audio, video and images (digital images). Steganography is the study and art that studies how to hide information on a certain media in such a way that its presence is not detected by other parties which are not rightful to the information. PT. Pos Indonesia, that has a lot of data, some of which are important and not just an ordinary data. One of the issues that is currently being discussed is the data security issue to maintain the secrecy of the data. This research aims to devise and create the system application that is able to preserve data security to make its presence is not detected by other parties which are not rightful to these data and information. This research employs the steganography technique with the desktop-based End of File (EOF) method using the Java programming language. In employing the steganography technique on digital image media, the storage of certain classified data will have the decent level of security. Eventually, with the data security system that is created, PT. Pos Indonesia is able to upgrade the sent-data security, specifically digital letters that are confidential.

Keywords*: Steganography, Digital Image, End of File Method, Data Security, Information System*

1. PENDAHULUAN

Perkembangan dunia teknologi komunikasi dan informasi yang sangat pesat belakangan ini berpengaruh besar dalam segala aspek kehidupan manusia. Cepatnya perkembangan teknologi informasi saat ini didukung dengan pentingnya kebutuhan akan mendapatkan informasi. Dalam proses pengamanan data sangat penting untuk pertukaran pesan dan informasi yang akan dikirim. Informasi yang diambil maupun ditukar mempunyai banyak jenis, seperti teks, audio, video maupun gambar (citra digital) [1]. Ancaman terhadap keamanan informasi yang dibutuhkan

semakin besar, maka perlu perkembangan penerapan teknologi dibidang pengamanan data dan informasi terutama untuk informasi yang dirahasiakan tersebut. Perkembangan teknologi juga sangat mempengaruhi pertukaran informasi sehingga sangat rentan terjadinya pencurian informasi dan manipulasi data, sehingga informasi penting tersebut dapat disebarluaskan [2].

Kekhawatiran inilah yang membuat berkembangnya teknik penyembunyian data agar kerahasian dan keamanan data pesan dan informasi dapat dikirimkan tanpa diketahui oleh orang yang tidak berhak mengetahui informasi tersebut [3]. Dimana file yang tidak disembunyikan dengan baik atau tidak aman dapat dengan mudah dibongkar jika hanya mengandalkan keamanan dasar dari komputer itu sendiri. Karena itu sangat diperlukan sebuah teknik dan metode khusus dalam pengamanannya supaya dapat meningkatkan keamanan dari data pesan informasinya.

Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian informasi pada suatu media sedemikian rupa sehingga keberadaannya tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. Steganografi berfungsi untuk menyamarkan keberadaan data rahasia dengan menyisipkan pesan pada objek lain sehingga sulit dideteksi [4]. Steganografi membutuhkan dua bagian yang sangat penting yaitu berkas atau media penampung seperti citra digital, suara (audio), atau video yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia dan data rahasia yang akan disembunyikan [5].

Teknik steganografi memiliki beberapa metode yang dapat digunakan seperti metode End of File (EOF), metode ini memiliki ciri tersendiri dalam proses enkripsi dan dekripsi data. Metode ini juga digunakan dalam menyisipkan data yang memiliki ukuran file yang sama dengan sebelum disisipkan dan ditambah dengan ukuran data yang disisipkan kedalam file tersebut [6].

Menanggapi permasalahan yang ada dari yang sedang berjalan saat ini, salah satu isu yang sering dibahas adalah persoalan keamanan data dan juga untuk mencari solusi dari permasalahan tersebut. Peneliti bermaksud melakukan penelitian mengenai Sistem Keamanan Data Menggunakan Teknik Steganografi Dengan Metode *End of File* (EOF) Berbasis *Desktop* (Studi Kasus: PT. Pos Indonesia). Sehingga pada akhirnya dengan sistem keamanan data yang akan dibangun ini, perusahaan PT. Pos Indonesia dapat meningkatkan keamanan data yang dikirimkan khususnya surat digital yang bersifar rahasia.

2. METODOLOGI PENELITIAN

Pada bagian ini menjelaskan beberapa tahapan metode atau cara yang digunakan peneliti dalam mencapai tujuan penelitian. Langkah-langkah metode penelitian yang dilakukan adalah sebagai berikut.

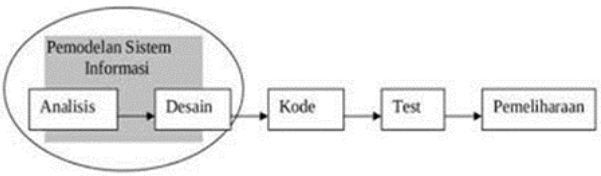
2.1 Metode Pengumpulan Data

Pengumpulan data dilakukan dengan memperoleh informasi yang dibutuhkan untuk mencapai tujuan riset penelitian pada PT. Pos Indonesia [7]. Data penelitian yang dapat diperoleh diantaranya sebagai berikut:

a. Metode Observasi (*Observation Method*)
   Pada metode ini peneliti melakukan pengamatan terhadap masalah yang ada secara langsung terkait proses pengirimin data pesan atau informasi yang bersifat pribadi pada saat ini, dan mengumpulkan data yang berkaitan dengan permasalahan lain yang mungkin masih bisa diatasi pada perusahaan PT. Pos Indonesia.
   b. Metode Wawancara (*Interview Method*)
      Suatu metode yang dilakukan untuk memperoleh data-data dengan melakukan tanya jawab langsung kepada narasumber pada bagian terkait pelayanan pengiriman data pesan atau informasi yang bersifat pribadi, supaya dapat memahami hal yang akan diteliti.
   c. Metode Studi Pustaka (*Library Method*)
      Metode Pengumpulan data yang dilakukan dengan mempelajari jurnal yang meneliti tentang steganografi dan keamanan data. buku-buku yang terkait dengan keamanan digital, dan juga mengumpulkan informasi dari website yang didapat melalui internet membahas tentang teknik steganografi dalam mengamankan data ke dalam sebuah citra digital dalam bentuk file gambar [8].

2.2 Metode Pengembangan Sistem

Pada penelitian ini metode penelitian yang digunakan dalam pengembangan perangkat lunak sistem ini adalah menggunakan metode *waterfall* model SDLC (*Software Development Life Cycle*). Model waterfall adalah salah satu metode pengembangan perangkat lunak dengan model SDLC yang paling sederhana dan mudah untuk diterapkan secara sistematis mendekati spesifikasi yang tidak berubah-ubah [9].



Gambar 1. Pengembangan Sistem Metode *Waterfall*

Pemodelan langkah alur pengembangan sistem mekanisme waterfall meliputi fase-fase berikut ini:

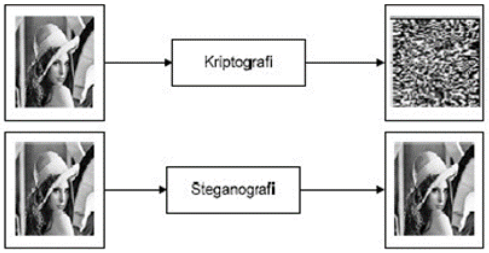
a. Analisis Kebutuhan (*Requirement Analysis*)
   Merupakan tahapan menganalisis segala hal yang ada pada pembuatan atau pengembangan proyek perangkat lunak yang bertujuan untuk memahami sistem yang ada, mengidentifikasi masalah dan mencari solusinya [10].
b. Desain (*Design*)
   Merupakan tahapan yang menerjemahkan keperluan atau data yang telah dianalisis ke dalam bentuk desain perancangan yang mudah dimengerti oleh pengguna (user).
c. Pembuatan Kode Program (*Coding*)
   Merupakan tahapan yang menerjemahkan data yang dirancang ke dalam bahasa pemrograman yang telah ditentukan [11].
d. Pengujian (*Testing*)
   Merupakan tahapan pengujian terhadap sistem atau program yang telah selesai dibuat.
e. Pemeliharaan (*Maintenance*)
   Merupakan tahapan menerapkan sistem secara keseluruhan disertai pemeliharaan jika terjadi perubahan struktur sistem, baik dari bagian software maupun *hardware.*

2.3 Teknik Steganografi

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Steganografi membutuhkan dua jenis berkas, yaitu berkas *cover* sebagai media penampung pesan dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara (audio), teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara (audio), teks, atau video [12].

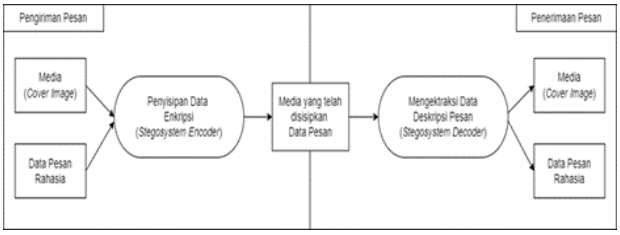
Berikut ini adalah perbedaan antara steganografi dan kriptografi, yaitu:

a. Steganografi
   Pesan rahasia yang dibungkus dengan media lain (teks, gambar, video, audio), sehingga sangat sulit bagi orang lain untuk mengetahui pesan rahasia yang ada di dalam file media penyembunyian. Mengingat bahwa steganografi tidak menimbulkan kecurigaan pada orang lain, karena sekilas media gambar, audio, atau video nampak normal.
b. Kriptografi
   Pesan rahasia yang diacak susunannya maupun polanya, sehingga pesan tidak dapat diketahui oleh orang lain. Namun bisa dapat menimbulkan kecurigaan bagi orang lain, karena adanya pesan yang disandikan.



Gambar 2. Ilustrasi Kriptografi dan Steganografi pada Citra Digital

Keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan bagi pihak ketiga. Dalam steganografi, proses penyembunyian pesan ke dalam media cover disebut penyisipan (*enkripsi*), sedangkan proses sebaliknya disebut *ekstraksi* (deskripsi). Berikut gambaran dari aliran proses steganografi:



Gambar 3. Cara Aliran Kerja Proses Steganografi Secara Umum

2.4 Metode *End of File* (EOF)

Metode *End of File* (EOF) merupakan salah satu teknik untuk menyisipkan data pada akhir file dan merupakan pengembangan daripada metode *Least Significant Bit* (LSB) [13]. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran file asli (sebelum disisipkan data) ditambah dengan ukuran data yang akan disisipkan ke file tersebut [14]. Sebagai contoh, jika akan menyisipkan sebuah pesan ke dalam sebuah file audio, maka file audio tidak berubah, tidak rusak dan dapat diputar seperti file audio asli. Ini yang menjadi salah satu keunggulan metode EOF dibandingkan dengan metode steganografi yang lain [15]. Karena disisipkan pada akhir file, pesan yang disisipkan tidak bersinggungan dengan isi file, hal ini menyebabkan integritas data dari file yang disisipi tetap dapat terjaga dan tidak mengubah format file dari media yang dipakai sebagai tempat penyisipan pesan atau informasi rahasia tersebut [16].

3. HASIL DAN PEMBAHASAN

Pada bagian ini menjelaskan beberapa tahapan hasil implementasi aplikasi sistem yang sudah dibuat dan pembahasan kasus hasil pengujian sistem yang digunakan peneliti dalam mencapai tujuan akhir penelitian [17]. Langkah-langkah hasil penelitian yang dilakukan adalah sebagai berikut.

3.1 Sistem Implementasi Antar Muka Pengguna (User Interface)

Pengertian sistem antar muka adalah salah satu layanan yang disediakan sistem operasi sebagai sarana interaksi antara user dengan sistem operasi komputer [18]. Implementasi antar muka pengguna dilakukan dengan menggunakan bahasa pemrograman *Java* [19]. Hasil implementasinya adalah sebagai berikut ini:

a. Implementasi Tampilan *Login*

Tampilan ini halaman awal ketika membuka aplikasi sistem keamanan data.

Gambar 4. Implementasi Tampilan *Login*

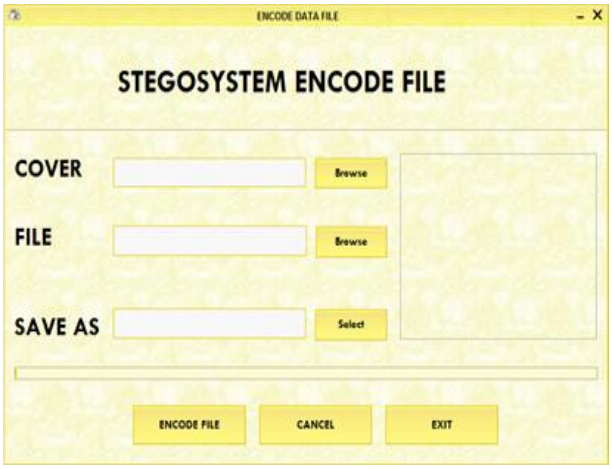
b. Implementasi Tampilan Menu Utama

Tampilan ini merupakan halaman Menu Utama ketika user sudah berhasil *Login.* Setelah itu user dapat memilih akan melakukan proses *Encode File* atau *Decode File* dan dapat memilih menu informasi (*About*) dan bantuan (*Help*).

Gambar 5. Implementasi Tampilan Menu Utama

c. Implementasi Tampilan Enkripsi Data (*Encode File*)

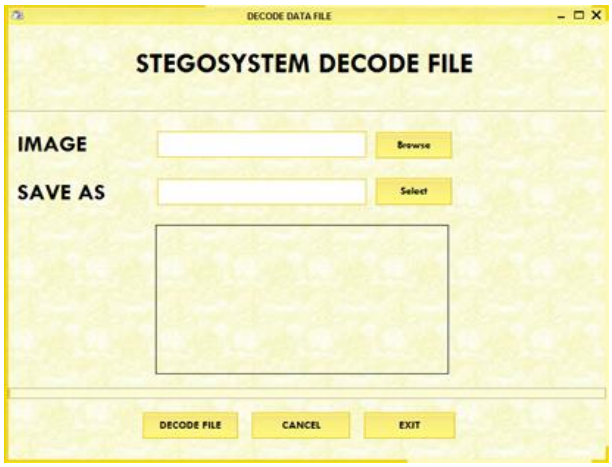
Tampilan ini merupakan halaman *Encode File* untuk menyembunyikan file data ke dalam objek gambar dan secara otomatis telah tersimpan ke dalam *folder* yang sudah ditentukan setelah proses encode berhasil dan selesai.



Gambar 6. Implementasi Tampilan Enkripsi Data (*Encode File*)

d. Implementasi Tampilan Ekstraksi Data (*Decode File*)

Tampilan ini merupakan halaman *Decode File* untuk mengembalikan file data yang sudah disisipkan ke dalam gambar (decode) dan dapat dibaca file datanya.



Gambar 7. Implementasi Tampilan Ekstraksi Data (*Decode File*)

e. Implementasi Tampilan

Tampilan ini tentang aplikasi sistem kemanan data yang dibuat dengan Teknik Steganografi.

Gambar 8. Implementasi Tampilan Informasi (*About*)

f. Implementasi Tampilan Bantuan (*Help*)

Tampilan ini mengetahui cara-cara untuk melakukan penyembunyian dan pengembalian *file* data.

Gambar 9. Implementasi Tampilan Bantuan (*Help*)

g. Implementasi Tampilan *Logout*

Tampilan ini merupakan halaman *Logout* untuk untuk menutup aplikasi sistem keamanan data dimana aplikasi sistem menampilkan pemberitahuan kepada pengguna untuk keluar aplikasi.

Gambar 10. Implementasi Tampilan *Logout*

3.2 *Pengujian Black Box Testing*

Pengujian *Black Box Testing* merupakan pengujian program berfokus pada fungsi perangkat lunak, tester atau penguji dapat mendefinisikan kumpulan kondisi input dan melakukan pengujian pada spesifikasi fungsional sistem program perangkat lunak [20]. Berdasakan rencana pengujian yang telah disusun, maka dapat dilakukan pengujian sebagai berikut:

Tabel 1. Rencana Pengujian

No.	Kelas Uji	Butir Pengujian	Jenis Pengujian
1.	*Login*	Input *username* dan *password* yang salah	*Black Box*
2.	*Login*	Input *username*	*Black Box*

		dan *password* yang benar	
3.	Menu Utama	Pilih fitur menu-menu pada halaman menu utama	*Black Box*
4.	Menu *Encode File*	Input *cover* gambar digital wadah penampung	*Black Box*
5.	Menu *Encode File*	Input *file* pesan data pesan rahasia yang disisipkan	*Black Box*
6.	Menu *Encode File*	Pilih tempat penyimpanan *Stego-data*	*Black Box*
7.	Menu *Encode File*	Tombol proses *encode file*	*Black Box*
8.	Menu *Decode File*	Input gambar *Stego-data* yang belum disisipi pesan	*Black Box*
9.	Menu *Decode File*	Input gambar *Stego-data* yang sudah disisipi pesan	*Black Box*
10	Menu *Decode File*	Pilih tempat simpan hasil ekstraksi data	*Black Box*
11.	Menu *Decode File*	Tombol proses *decode file*	*Black Box*
12.	Menu *About*	Pilih *back* untuk menuju menu utama	*Black Box*
13.	Menu *Help*	Pilih *back* untuk menuju menu utama	*Black Box*
14.	*Logout*	Pilih "*Yes*" untuk keluar dari aplikasi	*Black Box*
15.	*Logout*	Jika pilih "*No*" tetap di Menu Utama	*Black Box*

Tabel 2. Hasil Pengujian Sistem Keamanan Data

No.	Kelas Uji	Skenario Pengujian	Hasil Pengamatan	Kesimpulan
1.	*Login*	Input *username* dan *password* yang salah	Tampil pesan *user name* dan *password* salah	Valid
2.	*Login*	Input *username* dan *password* yang benar	Menampilkan halaman menu utama ketika *login* berhasil	Valid
3.	Menu Utama	Pilih fitur menu-menu halaman menu utama	Menampilkan halaman menu Utama dan dapat pilih menu	
4.	Menu *Encode File*	Input *cover* gambar digital wadah penampung	Menampilkan untuk memilih gambar *cover*	Valid
5.	Menu *Encode File*	Input *file* pesan data pesan rahasia yang disisipkan	Menampilkan untuk memilih file dokumen rahasia	Valid
6.	Menu *Encode File*	Pilih tempat penyimpanan *Stego-data*	Menampilkan untuk memilih tempat penyimpanan	Valid
7.	Menu *Encode File*	Tombol proses *encode file*	Tampil *text alert message* "Proses Embed Berhasil"	Valid
8.	Menu *Decode File*	Input gambar *Stego-data* yang belum disisipi pesan	Menampilkan *text alert* Error! "Tidak Memiliki File Rahasia"	Valid
9.	Menu *Decode File*	Input gambar *Stego-data* yang sudah disisipi pesan	Gambar yang benar dan sudah disisipkan akan tampil dikolom *Image*	Valid
10	Menu *Decode File*	Pilih tempat simpan hasil ekstraksi data	Menampilkan untuk memilih tempat penyimpanan	Valid
11.	Menu *Decode File*	Tombol proses *decode file*	Tampil *text alert message* "File SUKSES dilakukan *Decode File* disimpan"	Valid
12.	Menu *About*	Pilih *back* untuk menuju menu utama	Menampilkan kembali halaman Menu Utama	Valid
13.	Menu *Help*	Pilih *back* untuk menuju menu utama	Menampilkan kembali halaman Menu Utama	Valid

No.	Kelas Uji	Skenario Pengujian	Hasil Pengamatan	Kesimpulan
14.	*Logout*	Pilih "*Yes*" untuk keluar dari aplikasi	Menampilkan kembali halaman *Login*	Valid
15.	*Logout*	Jika pilih "*No*" tetap di Menu Utama	Pengguna tetap berada di halaman Menu Utama	Valid

3.3 *Kasus dan Hasil Pengujian Aplikasi*

Dalam pengujian aplikasi sistem keamanan data peneliti mengambil beberapa dokumen *file* rahasia dan berkas gambar untuk uji coba aplikasi ini yang nantinya akan disimpan dalam objek *cover gambar media digital*. Berkas-berkas yang akan digunakan adalah sebagai berikut:

a. Pengujian *Black Box* Enkripsi Data (*Encode File*)

Tabel 3. Pengujian *Black Box* Enkripsi Data (*Encode File*)

Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengamatan	Kesimpulan
Masukkan gambar *cover* media digital (*.jpg atau *.png)	Menampilkan *File Explorer* pada komputer untuk memilih gambar *cover*	Tampil *File Explorer* untuk memilih gambar *cover* 	Berhasil
Setelah pilih gambar *cover* media digital (*.jpg atau *.png)	Gambar *cover* media digital akan tampil dikolom *Image*	Tampil gambar *cover* 	Berhasil
Masukkan data file rahasia yang akan disisipkan (*.doc, *.docx, atau *.pdf)	Menampilkan *File Explorer* pada komputer untuk memilih file dokumen rahasia	Tampil *File Explorer* untuk memilih *file* dokumen 	Berhasil
Masukkan nama file untuk gambar yang sudah disisipkan file rahasia	Menampilkan *File Explorer* untuk memilih tempat penyimpanan	Tampil *File Explorer* untuk memilih tempat simpan *file*  Tempat simpan *encode file*	Berhasil
Klik tombol *Encode File* untuk proses enkripsi	Menampilkan *text alert message* "File SUKSES disisipkan"	Tampil *text alert message* "Proses Embed Berhasil"   Tampil *text alert* "Waktu Proses Embed: 5.613 detik" 	Berhasil

b. Pengujian *Black Box* Ekstraksi (*Decode File*)

Tabel 4. Pengujian *Black Box* Ekstraksi (*Decode File*)

Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengamatan	Kesimpulan
Masukkan	Menampilkan *text*	Memilih gambar yang salah	Berhasil

Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengamatan	Kesimpulan
gambar yang salah dan belum disisipkan file rahasia	*alert* ERROR! "Tidak Memiliki File Rahasia"	 Tampil *alert* ERROR! "Tidak Memiliki File Rahasia" 	
Masukkan gambar yang benar dan sudah disisipkan *file* rahasia	Menampilkan *File Explorer* pada komputer untuk memilih gambar *Stego-data*	Memilih gambar yang benar 	Berhasil
Setelah pilih gambar yang benar dan sudah disisipkan file rahasia	Gambar yang benar dan sudah disisipkan akan tampil dikolom *Image*	Tampil gambar yang sudah disisipkan *file* rahasia 	Berhasil
Masukkan nama yang baru untuk *file* dokumen yang telah dipisahkan	Menampilkan *File Explorer* untuk memilih tempat penyimpanan	Tampil *File Explorer* untuk memilih tempat simpan *file*  Tempat simpan *decode file*	Berhasil
			
Klik tombol *Decode File* untuk proses ekstraksi	Menampilkan *text alert message* "File SUKSES dilakukan *Decode File* disimpan"	Tampil *text alert message* "File SUKSES dilakukan *Decode File* disimpan" 	Berhasil

4. KESIMPULAN

Dari hasil pembahasan tentang aplikasi sistem keamanan data menggunakan teknik steganografi dengan metode *End of File* (EOF) berbasis desktop yang telah dilakukan terhadap permasalahan dan aplikasi program yang dikembangkan, maka terdapat beberapa kesimpulan sebagai berikut:

a. Pengamanan dokumen menggunakan teknik steganografi dengan metode *End of File* (EOF) telah berhasil di implementasikan. Dengan demikian file dokumen rahasia atau penting yang ada di perusahaan PT. Pos Indonesia dapat lebih aman kerahasiannya dari orang-orang yang tidak bertanggung jawab.
b. Aplikasi yang dibuat mampu untuk menyembunyikan *file* ke dalam objek *cover* gambar media digital dengan baik. Hasil dari proses *Encode File* menjadikan dokumen tersembunyi dalam stego-image tanpa ada perubahan dan file gambar masih dapat dipergunakan seperti biasa.
c. Pada tahap *Decode File* dokumen yang sudah disisipkan dapat dikembalikan menjadi dokumen rahasia secara utuh, data yang orisinil tanpa mengalami perubahan sedikipun.
d. Dengan adanya steganografi, pengiriman pesan dengan menyisipkan pada sebuah media penampung (*cover*) akan lebih aman dan tidak mudah menimbulkan kecurigaan dari pada dengan menggunakan teknik kriptografi. Dengan menggunakan teknik steganografi ini jika dikaitkan dengan hak cipta dan

kepemilikan maka hak cipta akan dapat terjaga dengan baik.

REFERENCES

[1] R. Indrayani, "Human perception evaluation toward end of file steganography method's implementation using multimedia file (image, audio, and video)," *2019 4th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2019*, pp. 200–204, Nov. 2019, doi: 10.1109/ICITISEE48480.2019.9003759.

[2] D. Darwis, "Implementasi Steganografi pada Berkas Audio Wav untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding," *Expert J. Manaj. Sist. Inf. dan Teknol.*, vol. 5, no. 1, 2015, doi: 10.36448/jmsit.v5i1.715.

[3] E. B. Adhi, *Implementasi Keamanan Data Menggunakan Metode EOF (End of File) pada PT. TELEKOMUNIKASI SELULER*. Jakarta: Universitas Budi Luhur, 2015.

[4] D. Ayu Irawati, E. Dinda Rachmawati, and J. Teknologi Informasi Politeknik Negeri Malang Jalan Soekarno-Hatta No, "Perancangan Aplikasi Steganografi Menggunakan Algoritma IDEA dan Metode EOF," *103.23.20.161*, vol. 2018, no. November, pp. 195–205, 2018.

[5] D. Watni and S. Chawla, "A Comparative Evaluation of Jpeg Steganography," *Proc. IEEE Int. Conf. Signal Process. Control*, vol. 2019-October, pp. 36–40, Oct. 2019, doi: 10.1109/ISPCC48220.2019.8988383.

[6] M. Masri, M. Masri, H. Widya, D. Yuhendri, and M. I. Fauzi, "Perancangan Aplikasi Penyisipan Pesan Pada Pixel Citra Menggunakan Metode End Of File," *J. Electr. Technol.*, vol. 4, no. 3, pp. 178–184, 2019.

[7] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D*, 1st ed. Bandung: Penerbit Alfabeta Bandung, 2018.

[8] S. Rachmad Hakim, "Definisi Aplikasi Desktop," *Seputar Pengetahuan*, 2016. [Online]. Available: https://www.seputarpengetahuan.co.id/.

[9] A. A. Wahid, "Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, no. November, pp. 1–5, 2020.

[10] Yurindra, *Software Engineering*. Yogyakarta: Deepublish, 2017.

[11] I. Fita Puspita Sari, *Pembuatan Software Rekam Medis dengan Java Netbeans + MySQL*. Yogyakarta: Gava Media, 2014.

[12] A. S. Abdul Kadir, *Teori dan Aplikasi Pengolahan Citra*. Yogyakarta: ANDI, 2013.

[13] U. A. Anti, A. H. Kridalaksana, and D. M. Khairina, "Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF)," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 12, no. 2, p. 104, 2017, doi: 10.30872/jim.v12i2.658.

[14] A. Fauzi and R. P. Rahayu, "Penerapan Metode End Of File Pada Steganografi Citra Gambar dengan Memanfaatkan Algoritma Affine Cipher sebagai Keamanan Pesan," *MEANS (Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 117–123, 2017.

[15] I. Gunawan, "Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 57, 2018, doi: 10.30645/j-sakti.v2i1.48.

[16] T. Tri Handayani and S. P. Yuliati, "Implementasi Steganografi Dengan Metode End Of File (EOF) Untuk Menyisipkan Pesan Teks Pada Gambar," *J. FASILKOM J. Teknol. Inf. dan ILmu Komput.*, vol. 11, no. 03, pp. 143–149, 2021.

[17] Y. P. A. Muhammad Rusli, I Komang Rinartha, *Belajar Pemrograman Java dengan Netbeans*. Bali: ANDI, 2016.

[18] M. S. Rosa A. S., *Rekayasa Perangkat Lunak: Terstruktur dan Berorientasi Objek*. Bandung: Informatika, 2015.

[19] B. Haqi, *Membuat aplikasi antrean dengan Java NetBeans IDE 8.0.2 dan database MYSQL*. Jakarta: Elex Media Komputindo, 2017.

[20] Sembiring Sandro, "Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End of File," *Pelita Inform. Budi Darma*, vol. IV, no. Agustus, pp. 45–51, 2013.