Implementasi Steganografi Dengan Metode *End Of File* Pada Media Audio Dan Kriptografi Metode RSA Serta *Vigenere Cipher* Berbasis Java Desktop Untuk Mengamankan Data

Muhammad Agung A. Djafar[1)], Noni Juliasari[2)]
[1]*Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budiluhur*
[1,2]*Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260*
Telp. (021) 5853753, Fax. (021) 5866369
*E-Mail :*1411503061@student.budiluhur.ac.id[1)],nonijuliasari@budiluhur.ac.id[2)]

Abstrak

Direktorat Prasarana Perhubungan Darat Subdit Pelabuhan Sungai dan Danau merupakan unsur pelaksana yang berada di bawah Kementerian Perhubungan yang mempunyai tugas menyusun kebijakan rencana kerja anggaran berupa rencana strategis kegiatan yang ada di Direktorat Prasarana. Perlindungan data kebijakan rencana kerja anggaran masih lemah karena selama ini data tersebut hanya disimpan di komputer, namun komputer kantor tidak memiliki hak akses untuk setiap penggunanya. Dengan kata lain siapapun dapat mengakses segala arsip dokumen yang berada di dalamnya. Hal tersebut mengakibatkan dokumen dapat dengan mudah diketahui oleh banyak orang atau pihak yang tidak berwenang untuk mengubah, menghapus, atau membaca informasi dokumen tersebut. Dengan ditambahkannya kriptografi pada penyisipan file dokumen steganografi ini, maka file dokumen yang disimpan dalam komputer ataupun yang akan dikirim lebih terjaga kerahasiaannya dan diharapkan dapat membantu upaya dalam peningkatan keamanan informasi dokumen. Penelitian ini bertujuan untuk menghasilkan suatu aplikasi dengan penerapan algoritma end of file, Rivest Shamir Adleman (RSA), dan Vigenere cipher sebagai alat bantu mengamankan file dokumen tersebut. Aplikasi dibangun berbasis desktop dengan menggunakan bahasa pemograman java. Proses perlindungan file dokumen akan melalui proses pengenkripsian file terlebih dahulu dengan teknik kriptografi menggunakan algoritma Rivest Shamir Adleman (RSA) dan Vigenere cipher, kemudian file yang telah di enkripsi disisipkan ke dalam file audio menggunakan teknik steganografi dengan algoritma end of file. Pengujian dilakukan dengan metode white box. Berdasarkan hasil pengujian, aplikasi keamanan data menggunakan teknik steganografi metode End Of File (EOF) dan kriptografi dengan metode RSA serta Vigenere Cipher ini, dapat mengamankan file dokumen atau informasi yang ada pada Direktorat Prasarana Perhubungan Darat Subdit Pelabuhan Sungai dan Danau menjadi lebih aman. Namun waktu yang digunakan untuk melakukan proses enkripsi file dokumen dan penyisipan (embed) file dokumen ke dalam audio berbanding lurus dengan ukuran file yang di proses. Semakin kecil ukuran file yang diproses, maka semakin cepat proses enkripsi dan embed dilakukan. Begitupun juga dengan proses pengembalian file seperti semula.

Kata Kunci*:* Steganografi, Kriptografi, End Of File (EOF), Rivest Shamir Adleman (RSA), Vigenere Cipher.

1. PENDAHULUAN

Seiring dengan adanya perkembangan teknologi informasi dan komunikasi saat ini yang begitu pesat dan memberikan pengaruh besar bagi kehidupan masyarakat, memudahkan kita untuk melakukan pertukaran dengan data orang lain secara cepat. Namun terkadang keamanan pertukaran data tersebut, kurang disadari oleh kita. Sehingga menyebabkan salah satu dampak negatif dalam perkembangan teknologi yaitu pencurian *file*atau data, yang merupakan masalah yang paling ditakuti oleh jaringan komunikasi. Kekhawatiran inilah yang membuat berkembangnya teknik-teknik keamanan informasi yang cukup terkenal seperti steganografi dan kriptografi.

Steganografi adalah teknik untuk menyembunyikan suatu pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak dapat menyadari ada sesuatu di dalam pesan tersebut [8]. Sedangkan kriptografi adalah seni untuk mengacak informasi atau data yang memiliki arti menjadi sesuatu yang tidak dapat dimengerti atau seakan-akan tidak berarti sehingga pesan atau data yang dikirim oleh *sender* dapat disampaikan kepada *recivier* dengan aman [5]. Dengan ditambahkannya kriptografi pada penyisipan *file* dokumen steganografi ini, maka *file* dokumen yang disimpan dalam komputer ataupun yang akan dikirim lebih terjaga kerahasiaannya dan diharapkan dapat membantu upaya dalam peningkatan keamanan informasi.

Direktorat Prasarana Perhubungan Darat Subdit Pelabuhan Sungai dan Danau merupakan unsur pelaksana yang berada di bawah Kementerian Perhubungan yang mempunyai tugas menyusun kebijakan rencana kerja anggaran berupa rencana strategis kegiatan yang ada di Direktorat Prasarana. Untuk menjamin keamanan dokumen tersebut sebagai bukti pertanggungjawaban dalam pengelolaan dan pemanfaatan dokumen yang terpercaya, penulis memutuskan membuat aplikasi keamanan data dengan teknik audio steganografi dan kriptografi.

Penelitian yang berkaitan dengan steganografi dan kriptografi ini dibuat untuk mengamankan dokumen kantor yang bersifat pribadi atau rahasia, sehingga melindungi dokumen dari pengguna yang tidak berhak untuk mengakses seperti mengubah, menghapus, atau membaca informasi dokumen tersebut. Steganografi memiliki beberapa metode yang dapat digunakan, begitupun juga dengan kriptografi. Dalam penelitian ini penulis menggunakan metode *End Of File* (EOF) untuk menyisipkan mengamankan dokumen pada *file* induk berupa audio dengan format data .mp3 dan .wav. Namun sebelum disisipkan kedalam audio, *file* dokumen terlebih dahulu di enkripsi dengan menggunakan metode RSA dan Vigenere Cipher.

2. METODE PENELITIAN

Dalam penelitian ini penulis melakukan penilitian untuk mengumpulkan data atau informasi yang diperlukan. Adapun metodologi yang digunakan sebagai berikut :

2.1. Penelitian Lapangan

Penelitian lapangan, yaitu penelitian langsung pada lokasi riset dengan menggunakan teknik pengumpulan data sebagai berikut :

1. Studi lapangan, yaitu penelitian langsung di Kementerian Perhubungan yang diteliti untuk mendapatkan data atau informasi yang diperlukan.
2. Pengamatan, yaitu teknik pengumpulan data dengan mengamati langsung proses transfer file yang berisikan data-data penting.
3. Studi dokumentasi, yaitu mempelajari kumpulan dokumen yang berkaitan dengan permasalahan yang dibahas.

2.2. Metode Wawancara

Metode wawancara, yaitu proses tanya jawab langsung dan sistematis kepada orang yang mengetahui tentang permasalahan yang sedang diamati untuk meyakinkan hal-hal kegiatan observasi yang telah dilakukan.

2.3. Penelitian Kepustakaan

Penelitian kepustakaan, yaitu penelitan yang digunakan dengan cara mempelajari buku-buku, litelatur-litelatur, jurnal, sumber bacaan lainnya yang berkaitan erat hubungannya dengan pembahasan laporan penelitian ini.

2.4. Metode Pengembangan

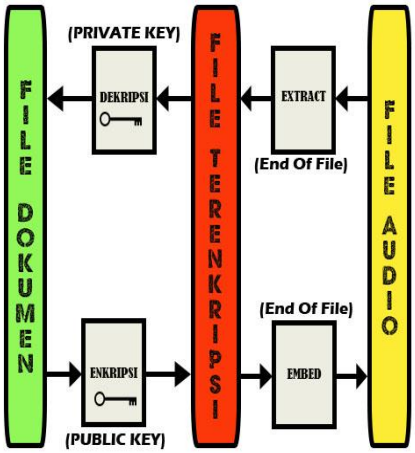
Metode pengembangan aplikasi yang digunakan dalam mengembangkan aplikasi ini adalah Waterfall. Dalam pengembangannya metode waterfall memiliki tahapan yang berturut yaitu, membuat *requirement, design*, implementasi program, *coding* & testing dan pengembangan program. Setiap proses tersebut harus dikerjakan secara berturut, jadi jika ada kebutuhan tambahan maka harus menunggu sampai tahap akhir.

3. HASIL DAN PEMBAHASAN

3.1.Rancangan Program

Program yang dibuat terdiri dari form *login* dan form menu utama, form menu utama terdiri dari form *embed*, form *extract*, form *generatekey*, form *help*, form cetak riwayat dan form about. Untuk melakukan enkripsi dan penyisipan *file* dokumen ke dalam media audio, *user* dapat memilih form embed. Namun sebelum melakukan enkripsi dan embed *file*,*user*harus mendapatkan sebuah kunci *private* dan kunci *public* dengan membuatkannya pada form generate key. Berikut merupakan rancangan program yang akan dibuat dapat dilihat pada Gambar 1.

Gambar 1 : Racangan Program



3.2. Rancangan Layar

1. Rancangan Layar Form Embed

Apabila user ingin melakukan embed atau penyembunyian dokumen rahasia, maka user dapat memilih menu embed. Pada menu ini terdapat form yang dapat digunakan untuk memulai proses embed terhadap dokumen rahasia tersebut. Namun sebelum melakukan proses embed, langkah pertama yang harus dilakukan user adalah mengenkripsi file dokumen terlebih dahulu. Dimulai dari pemilihan file dokumen yang akan dirahasiakan, memilih kunci public, memilih tempat penyimpanan file, kemudian melakukan proses enkripsi. Setelah enkripsi selesai, barulah selanjutnya user bisa melakukan penyembunyian dokumen rahasia yang telah di enkripsi. Pertama – tama *user* memilih *filecover* audio digital berupa .mp3 maupun .wav, kedua pemilihan dokumen yang telah di enkripsi, ketiga memilih penyimpanan *file*, dan terakhir lakukanproses embed. Gambar 4 berikut ini merupakan rancangan layar form pada menu embed.

Gambar 4 : Rancangan Layar Form Embed

2. Rancangan Layar Form *Extract*

Apabila user ingin melakukan *extract* ataupengembalian *file* yang telah di embed, maka *user* dapat memilih menu *extract*. Pada menu ini terdapat form untuk melakukan proses extract dimulai dari pemilihan *file* yang ingin di *extract* dan menyimpannya ke dalam direktori komputer. Namun setelah melakukan extract, user belum bisa langsung membuka *file* karena masih dalam keadaan terenkripsi. Oleh karena itu, user akan diminta untuk melakukan proses dekripsi. Gambar 5 berikut ini adalah rancangan layar form extract.

Gambar 5 : Rancangan Layar Form Extract

3.3. Tampilan Form Embed

Gambar 6 berikut ini merupakan tampilan setelah form pada menu *embed*telah berhasil di *embed* dan enkrip.

Gambar 3 : Tampilan File Berhasil diembed dan enkrip

3.4. Tampilan Form Extract

Gambar 7 berikut ini adalah tampilan setelah selesai melakukan *extrac*t dan dekrip.

Gambar 7 : Tampilan Form Extract

3.5. Tabel Hasil Pengujian

Dalam tabel ini pengujian aplikasi ini akan menjelaskan tentang perbandingan antara proses enkripsi dan dekripsi serta proses embed dan extract. File yang diuji meliputi file yang berformat (*.doc, *.docx, *.xls, *.xlsx). pengujiannya yaitu antara lain perbandingan ukuran audio sebelum di embed dan ukuran audio hasil extract, ukuran file asli dengan ukuran file hasil enkripsi dan dekripsi, serta waktu proses enkripsi, dekripsi, embed dan extract sampai selesai.

Tabel 1 : Tabel Hasil Embed

Nama File Audio	Nama File Rahasia	Ukuran File Audio (Byte)	Waktu Proses Embed (Milidetik)	Ukuran File Audio Hasil Embed (Byte)
adera lebih indah.mp3	encrypted.laporan pendahuluan.docx	3395256	31	3433388
Cold Play – fix you.mp3	encrypted.MALUT 1-TOR Honor Operasional Satuan Kerja 2017.doc	9473811	398	9864311
Sheila On 7 - Sebuah Kisah Klasik Untuk Masa Depan.mp3	encrypted.damri rev 2.xls	4024324	101	4245992
Roland.wav	encrypted.RAB.xlsx	688116	94	727368
Rata - Rata		4395376,75	156	4567765

Tabel 2 : Tabel Hasil Extract

Nama File Dokumen Hasil Extract	Ukuran File Dokumen (Byte)	Waktu Proses Dekripsi (Milidetik)	Ukuran File Hasil Dekripsi (Byte)
pengujian1.docx	38120	820	14295
pengujian2.doc	390488	33	146432
pengujian3.xls	221656	74	83121
pengujian4.xlsx	221656	818	14713
Rata - Rata	217980	436,25	64640,25

Nama File Audio Stegano	Ukuran File Audio Stegano (Byte)	Waktu Proses Extract (Milidetik)	Nama File Dokumen Hasil Extract	Ukuran File Dokumen Hasil Extract (Byte)
pengujian1.mp3	3433388	40	pengujian1.docx	38120
pengujian2.mp3	9864311	32	pengujian2.doc	390488
pengujian3.mp3	4245992	92	pengujian3.xls	221656
pengujian4.mp3	727368	360	pengujian4.xls	221656
Rata - Rata	4567764,75	131		217980

Tabel 3 : Tabel Hasil Pengujian Proses Enkripsi

Nama File Dokumen	Ukuran File Dokumen (Byte)	Waktu Proses Enkripsi (Milidetik)	Ukuran File Hasil Enkripsi (Byte)	Nama File Hasil Enkripsi
laporan pendahuluan.docx	14295	12	38120	encrypted.laporan pendahuluan.docx
MALUT 1-TOR Honor Operasional Satuan Kerja 2017.doc	146432	24	38120	encrypted.MALUT 1-TOR Honor Operasional Satuan Kerja 2017.doc
damri rev2.xls	83121	56	38120	encrypted.damri rev 2.xls
RAB.xlsx	14713	50	39240	RAB.xlsx
Rata - Rata	64640,25	35,5	38400	

Tabel 4 : Tabel Hasil Dekripsi

3.6. Kelebihan Program

1) Aplikasi dapat mengembalikan *file* yang telah di enkripsi dan disisipkan ke dalam audio kembali secara utuh seperti semula tanpa mengalami kerusakan.
2) Proses enkripsi – dekripsi dapat memakan waktu cepat jika *file* dalam berukuran kecil.
3) Proses *embed* (penyisipan *file*) ke dalam audio tidak memakan waktu yang lama jika ukuran *file* yang di sisipkan tidak berukuran besar.
4) Tidak merusak audio yang telah disisipkan *file* dan masih bisa dijalankan sehingga sulit dibedakan dengan audio aslinya.
5) Dapat mencetak *history* atau riwayat *file* apa saja yang telah di sisipkan ke dalam audio.
6) Performasi metode *End Of File (EOF)* diuji dengan menggunakan kriteria *imperceptibility*, *fidelity*, dan*recovery*. Ternyata bahwa aplikasi ini berhasil melewati uji *imperceptibility*, *fidelity*, dan *recovery*.
7) Adanya fiitur *login* untuk keamanan pengguna.

3.7. Kekurangan Program

1) Ukuran *file* yang dapat di enkripsi dibatasi maksimal 3MB.
2) Aplikasi hanya dapat mengenkripsi dan menyisipkan *file* yang berformat *.doc, *.docx, *.xls, dan *.xlsx.
3) Semakin besar ukuran *file*, maka semakin lama proses enkripsi dan dekripsi. Begitupun juga dengan proses embed dan extract. Jika semakin besar *file* rahasia dan *cover* (media), maka semakin lama waktu proses *embed* dan *extract.*
4) Saat melakukan proses dekripsi dengan kunci private yang berbeda pada *file* dokumen, program tetap dapat melakukan proses dekripsi namun tidak muncul popup pemberitahuan bahwa kunci private yang digunakan berbeda. Akan tetapi *file* yang telah didekrip dengan kunci berbeda tetap saja tidak dapat dibuka atau dibaca.
5) Media *file* (*file* audio) yang telah disisipi pesan atau dokumen, ukuran *file*akan menjadi lebih besar.
6) Tidak tahannya *file stego* terhadap manipulasi *file* seperti proses *editing* oleh perangkat lunak.
7) Berhubungan dengan tidak tahannya *filestego* terhadap manipulasi *file*, menunjukkan bahwa performasi EOF jika diuji dengan menggunakan kriteria *robustness* maka aplikasi ini tidak mampu lolos terhadap kriteria *robustness.*
8) Fitur *login* yang masih statis.

5. KESIMPULAN

Dari penilitian yang telah dilakukan, penulis mengambil kesimpulan berdasarkan perancangan program, pembuatan program, serta serangkaian uji coba dan analisa dari apikasi pengamanan data ini, maka didapati kesimpulan sebagai berikut ini :

a. Dengan adanya aplikasi pengamanan data dengan teknik steganografi metode *End Of File (EOF)* dan kriptografi menggunakan algortima *Rivest Shamir Adleman (RSA)* serta *Vigenere Cipher* ini, dapat mengamankan *file* dokumen atau informasi yang ada pada Direktorat Prasarana Perhubungan Darat Subdit Pelabuhan Sungai dan Danau menjadi lebih aman.
b. Kriptografi *Rivest Shamir Adleman(RSA),Vigenere Cipher* dan steganografi *End Of File (EOF)* dapat diimplementasikan pada aplikasi keamanan dokumen.
c. Satu kunci *public* dan *private* bisa digunakan berkali – kali dengan jenis ataupun *file* yang berbeda.
d. Aplikasi ini dapat mengembalikan isi *file* seperti awal secara utuh yang telah dilakukan pada proses *extract* dan dekripsi.
e. Perbedaan aktu yang digunakan untuk melakukan proses enkripsi dan dekripsi berbanding lurus dengan ukuran *file* yang di proses. Semakin kecil ukuran *file* yang diproses, maka semakin cepat proses enkripsi dan dekripsi dilakukan. Begitupun juga dengan proses *embed* dan *extract*. Jika semakin besar *file* rahasia dan cover (media), maka semakin lama waktu proses *embed* dan *extract*.
f. Rata – rata ukuran *file* dokumen yang berekstensi *.doc, *.docx, *.xls, *.xlsx di enkripsi adalah 38400 *byte* dan rata – rata ukuran *file* audio setelah di*embed* dokumen dengan ekstensi *.doc, *.docx, *.xls, *.xlsx adalah 4567765 *byte*.
g. Rata – rata waktu proses enkripsi pada *file* dokumen dengan ekstensi *.doc, *.docx, *.xls, *.xlsx adalah 35,5 milidetik, dan rata – rata waktu proses embed *file* dokumen yang berekstensi *.doc, *.docx, *.xls, *.xlsx adalah 156 milidetik.
h. Rata – rata waktu proses *extract* pada *file* dokumen *.doc, *.docx, *.xls, *.xlsx adalah 131 milidetik, dan rata – rata waktu proses dekripsi *file* dokumen berekstensi *.doc, *.docx, *.xls, *.xlsx adalah 436,25 millidetik.
i. Performasi metode *End Of File (EOF)* diuji dengan menggunakan dengan menggunakan kriteria *imperceptibility*, *fidelity*, *robustness*, dan *recovery*. Ternyata bahwa EOF berhasil melewati uji *imperceptibility, fidelity,* dan *recovery* namun tidak mampu lolos terhadap kriteria *robustness.*

DAFTAR PUSTAKA

[1] Anggraini, Y. and Sakti, D. V. S. Y. (2014) 'Penerapan Steganografi *Metode End of File* (EOF) Dan Enkripsi Metode *Data Encryption Standard* (DES) Pada Aplikasi Pengamanan Data Gambar Berbasis Java', Konferensi Nasional Sistem Informasi, STMIK Dipanegara Makassar, (September 2016), pp. 1743–1753.

[2] Basri (2016) 'Kriptografi Simetris Dan Asimetris DalamPerspektif Keamanan Data Dan Kompleksitas Komputasi', Jurnal Ilmiah Ilmu Komputer, 2(2), pp. 2442–4512.

[3] Efrand, Asnawati, Y. (2014) 'Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher', JurnalMedia Infotama, 10(2), pp. 120–128.

[4] Ginting, A., Isnanto, R. R. and Windasari, I. P. (2016) 'Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email', Jurnal Teknologi dan Sistem Komputer, 3(2), pp. 253–258. doi: 10.14710/JTSISKOM.3.2.2015.253-258.

[5] Iswahyudi, C., Setyaningsih, E. andWidyastuti, N. (2012) 'Pengamanan Kunci Enkripsi Citra PadaAlgoritma Super Enkripsi Menggunakan Metode End of File', Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III, (November), pp. 278–285.

[6] Lovebbi, Dodick Z, S. (2012) 'RancangBangun Aplikasi Steganografi dengan Metode Least Significant Bit diAudio pada Sistem Operasi Android', ULTIMATICS, IV(1), pp. 7–16.

[7] Sembiring, S. (2013) 'PerancanganAplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End of File', Pelita Informatika Budi Darma, IV(Agustus), pp. 45–51.

[8] Situmorang, M., Arisandi, D. and Utara, U.S. (2012) 'Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan Modifikasi Jarak Byte Pada Algoritma Least Significant Bit (LSB)', Jurnal Dunia Teknologi Informasi, 1(1), pp. 50–55.