RANCANG BANGUN APLIKASI KEAMANAN DATA PADA MEDIA VIDEO STEGANOGRAFI DENGAN MENGGUNAKAN METODE *END OF FILE* BERBASIS JAVA DI CV LESTARI ELECTRIC

mahpud@ft-umt.ac.id

Abstract

CV Lestari Electric memiliki data rahasia, salah satunya data stok fast moving barang, data inventory perusahaan , daftar gaji, daftar penerimaan yang tidak boleh diketahui oleh pihak lain. Jika informasi tersebut diketahui oleh orang yang tidak bertanggung jawab akan menimbulkan kerugian bagi perusahaan, sehingga CV Lestari Electric membutuhkan suatu aplikasi yang mengamankan data tersebut. Aplikasi tersebut menggunakan algoritma steganografi EOF (*End Of File*), dengan bahasa pemrograman Java berbasis desktop. Algoritma EOF digunakan karena memiliki kapasitas jumlah karakter pesan yang tidak terbatas pada saat disisipkan. Data yang dapat dienkripsi dan disisipkan berupa *text* dan gambar, sedangkan untuk *file* penampung data tersebut berupa *file* video yang berjenis .mp4. Berdasarkan hasil uji coba yang dilakukan, aplikasi ini mampu memproses *file* yang ingin disisipkan dengan ukuran maksimal sebesar 5 MB dan maksimal ukuran *file* penampung berupa video sebesar 30 MB. Dan aplikasi ini membantu dalam menjaga kerahasiaan data / informasi pada perusahaan sehingga tidak dapat diketahui oleh orang yang tidak bertanggung jawab.

Kata kunci : Steganografi EOF(*End Of File*), Keamanan Data, CV Lestari Electric**.**

Cv Lestari Electric *have data secret , one of them data stock fast moving goods , data inventory company , list salary , list revenue should not be known by other parties .If the news known to the irresponsible will suffer loss for the company , so that cv lestari electric need an application that secures the data .The application is algorithm steganografy eof (end of file) , with programming language java based desktop .Algorithm eof used because they have capacity number of chars message that are not confined to when inserted .The data can encrypted and inserted in the form of text and pictures , while to file top data are in the form of video files who as .mp4 .Based on the results of the trial that has done , this application able to process file who want to inserted with max size as much as 5 mb and a maximum of file size top of video by up to 30 mb And this application help maintain the confidentiality of data / information to the company and cannot be known by those who are not responsible.*

***Key words** : Steganografy eof (end of the file), data security* Cv Lestari Electric.

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Pada era globalisasi seperti sekarang ini dan terus berkembangnya teknologi informasi, keamanan dalam penyimpanan data dan pengiriman data atau informasi merupakan hal penting dan tidak dapat diabaikan. Terlebih jika pesan yang disimpan dan kirim bersifat penting dan rahasia. Dengan semakin berkembangnya teknologi yang begitu pesat maka bertukar informasi menjadi hal yang sangat mudah dengan hanya mengandalkan internet sebagai media pertukaran informasi. Salah satu dampak negatif dalam perkembangan teknologi informasi adalah adanya pencurian data. Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting, karena suatu komunikasi jarak jauh belum tentu aman dari pencurian.

CV Lestari Electric adalah Perusahaan yang bergerak dalam bidang distributor panel maker yang berada di. Ruko Villa melati Mas Blok B.10 No. 20 Tangerang Selatan. Pusat dari CV Lestari Electric ini berada di daerah Jakarta Daan Mogot yang bernama PT Lestari Inti Utama perusahaan yang bergerak distributor panel produk dari SWISS, dan CV Lestari Electric yang mempunyai 3 (Tiga) anak cabang di daerah Cikarang, LTC Glodok, dan Surabaya, Karena begitu pentingnya sebuah informasi, maka dibutuhkan suatu metode yang dapat menjaga kerahasiaan informasi dan metode yang dimaksud adalah kriptografi dan steganografi.

Kriptografi bertujuan agar data atau informasi yang dikirim tidak dapat dibaca oleh orang yang tidak berhak. Dalam kriptografi ada yang disebut dengan enkripsi (*encryption*) yaitu proses penyamaran data dari *plaintext* (data asli) menjadi *ciphertext* (data tersandi) dan dekripsi (*decryption*) yaitu proses pengembalian *ciphertext* menjadi *plaintext* kembali.

Kriptografi dipercaya untuk menangani masalah keamanan suatu data atau informasi dalam proses pengiriman, penyimpanan dan keperluan lainnya agar data atau informasi tetap terjaga kerahasiaannya. Setelah data berhasil di kriptografi data tersebut di sisipkan kedalam beberapa media dengan cara steganografi. Steganografi adalah seni penyembunyian pesan ke dalam media lainnnya, sehingga orang lain tidak menyadari ada pesan di dalam media tersebut yang telah disisipkan data rahasia kantor tersebut

Dengan penggabungan kriptografi dan steganografi ini membuat data kantor menjadi lebih aman, dikarenakan data hasil enkripsi yang tidak bisa dibuka tanpa adanya dekripsi bisa menjadi pertanyaan oleh pihak lain sehingga dengan adanya steganografi tersebut hasil dari enkripsi dapat disisipkan ke dalam media *file* seperti video sehingga data rahasia yang disisipkan tidak terllihat dengan kasat mata, karena yang terlihat hanya video saja dan tidak mencurigakan.

Dengan demikian mengambil judul "RANCANG BANGUN APLIKASI KEAMANAN DATA PADA MEDIA VIDEO STEGANOGRAFI DENGAN MENGGUNAKAN METODE *END OF FILE* BERBASIS JAVA DI CV LESTARI ELECTRIC". Baik teknik kriptografi dan steganografi memiliki kelebihan dan kekurangan masingmasing, oleh sebab itu diharapkan aplikasi ini dapat berguna dalam teknik pengamanan data, sehingga data pada kantor tersebut akan lebih aman dan terjamin kerahasiaannya

B. Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan di atas, adapun beberapa masalah yang ada di dalam penulisan tugas akhir ini adalah sebagai berikut :

1. Bagaimana cara mengamankan data supaya tidak mudah di ketahui ?
2. Bagaimana merancang aplikasi yang dapat menyembunyikan data atau *file* sehingga pengamanan data di CV
   Lestari Electric lebih aman ?

C. Tujuan Dan Manfaat Penelitian

Adapun penulisan yang di wujudkan dalam tugas akhir ini mempunyai tujuan dan manfaat sebagai berikut :

Tujuan Penulisan

Tujuan penulisan ini adalah sebagai berikut:

1. Untuk Membuat keamanan data dan *file* dengan teknik steganografi pada CV. Lestari Electric
2. Untuk mengetahui bagaimana kendalakendala yang timbul dalam sistem keamanan data pada CV. Lestari Electric
3. Dengan memanipulasi *file* yang di dalamnya terdapat data rahasia sehingga pesan tersebut tidak dapat diketahui keberadaanya, dengan mengacak isi data dan menyisipkan data pada file video, secara kasat mata tidak terjadi perubahan pada file hasil manipulasi sehingga tidak akan menimbulkan kecurigaan

Manfaat Penulisan

Penulis berharap agar penulisan tugas akhir ini dapat memberikan manfaat untuk banyak pihak antara lain :

1. Bagi Penulis

Penulisan Skripsi ini dapat menambah pengetahuan dan memperoleh gambaran praktek langsung dalam perusahaan di tempat dimana penulis bekerja. 2. Bagi Perusahaan

Laporan Skripsi ini dapat dijadikan sebagai bahan pertimbangan dalam menentukan kebijaksanaan perusahaan di masa yang akan datang dan dapat menjadi masukan untuk membantu kelancaran perusahaan, khususnya pada prosedur sistem keamanan data atau *file.* 3. Bagi Univesitas

Laporan Tugas Akhir ini dapat dimanfaatkan sebagai penambah pengetahuan dan pemahaman tentang suatu analisa tentang kemaanan data, juga dapat dijadikan sebagai bahan referensi / acuan peneliti skripsi bagi penulis selanjutnya, dapat dikembangkan

menjadi lebih baik lagi, khususnya bagi mahasiswa/i Tekhnik Informatika Universitas
Muhammadiyah Tangerang.

BAB II
TINJAUAN PUSTAKA

A. Landasan Teori

1) **Rancang bangun** Rancang bangun adalah kegiatan menerjemahkan hasil analisa ke dalam bentuk paket perangkat lunak kemudian menciptakan sistem tersebut ataupun memperbaiki sistem yang sudah ada
(Zulfiandri,2014:474).

Rancang Bangun adalah penggambaran, perencanaan, dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah kedalam suatu kesatuan yang utuh dan berfungsi (Hasyim,dkk,2014:2). Dari pengertian diatas Penulis menyimpulkan bahwa Rancang Bangun adalah tahap awal dari membuat gambaran dan bentuk sketsa yang belum pernah dibuat sama sekali lalu dikelolah menjadi gambaran atau sketsa yang memiliki fungsi yang diinginkan.

Menurut Taufik Ramadhan (2014), rancang bangun merupakan serangkaian prosedur untuk menerjemahkan hasil analisis dari sebuah sistem kedalam bahasa pemrograman untuk mendeskripsikan. Dengan secara detail bagaimana komponen - komponen sistem diimplementasi.

2) **Aplikasi**

Menurut Aris (2016), aplikasi dapat didefinisikan dengan suatu sub kelas perangkat lunak computer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna. Biasanya dibandingkan dengan perangkat lunak sistem yang mengintegrasikan berbagai kemampuan komputer, tapi tidak secara langsung menerapkan kemampuan tersebut untuk mengerjakan suatu tugas yang menguntungkan pengguna.

Menurut Taufik Ramadhan (2014), aplikasi komputer adalah sebuah perangkat lunak (*software*) program komputer yang ditulis dalam bahasa pemrograman dan berfungsi melakukan perintah sesuai dengan keinginan dari pembuat aplikasi. Aplikasi komputer dibuat untuk memudahkan pengguna dalam mengerjakan sesuatu menggunakan komputer.

Dari pernyataan di atas, penulis menyimpulkan bahwa aplikasi adalah program siap pakai yang dibuat untuk melaksanakan suatu fungsi bagi pengguna atau aplikasi yang lain dan dapat digunakan oleh sasaran yang dituju. Aplikasi juga merupakan software sistem yang memanfaatkan kemampuan komputer langsung dalam menjalankannya.

3) **Steganografi**

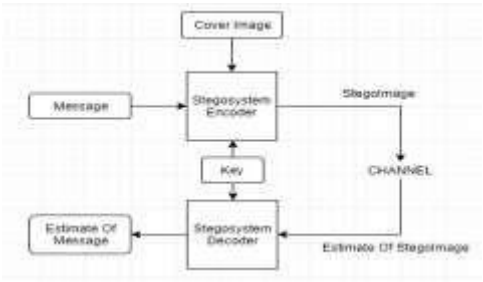
Steganografi merupakan seni dan ilmu menulis atau menyembunyikan pesan dengan suatu cara sehingga selain *sender* dan *receiver*, tidak ada seorangpun yang

mengetahui atau menyadari bahwa ada suatu pesan rahasia. Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein*, yang artinya menulis, sehingga kurang lebih artinya adalah menulis sesuatu yang tersembunyi atau terselubung.

Penggunaan steganografi antara lain bertujuan untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi dan melidungi hak cipta suatu produk. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan steganografi *ciphertext* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya. Steganografi membutuhkan dua poperti yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, daftar barang, kode program atau pesan lain.

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. Ini berbeda dengan kriptografi dimana ciphertext menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia. Berikut gambaran dari aliran proses steganografi : (Martono dan Irawan, 2014)



4) ***End Of File*** **(EOF)**

Metode Metode *End of File* (EOF) merupakan salah satu teknik yang menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran *file* sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam *file* tersebut. Dalam teknik EOF, data yang disisipkan pada akhirfile diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut.

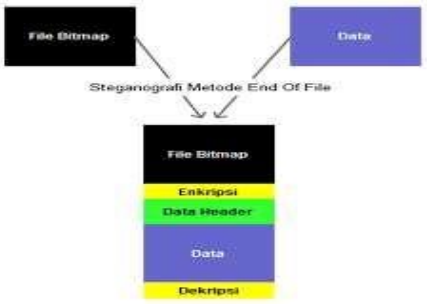
Metode EOF merupakan sebuah metode yang diadaptasi dari metode penanda akhir file (*End Of File*) yang digunakan oleh sistem operasi *windows*. Dalam sistem operasi *windows*, jika ditemukan penanda EOF pada sebuah *file*, maka sistem akan berhenti melakukan pembacaan pada *file* tersebut. Prinsip kerja EOF menggunakan karakter/simbol khusus yang diberikan pada setiap akhir *file*.

Karakter/simbol ini biasanya digunakan pada sistem operasi DOS untuk menandakan akhir dari sebuah penginputan data. Dengan berkembangnya *system* operasi

windows, penggunaan karakter seperti ini dikembangkan untuk menandakan akhir dari sebuah *file*.

Dari metode yang telah penulis baca, metode *End Of File* (EOF) dengan *Least Significant Bi*t (LSB) tidak begitu banyak perbedaan dalam alur algoritmanya, namun terdapat perbedaan yaitu pada pesan yang disisipi dan output. Pada metode LSB, pesan yang disisipi ukurannya harus lebih kecil dari citra yang akan disisipi, tetapi lain halnya pada metode EOF ukuran pesan yang akan disisipi bisa lebih besar dari ukuran citranya. Pada metode LSB citra yang telah disisipi pesan (*hidden text*) tidak terlalu mempengaruhi ukuran citranya, tetapi akan mempengaruhi kualitas citranya.

Sedangkan pada metode EOF, kualitas citra setelah disisipi pesantidak berubah, tetapi akan mengubah ukuran citranya. Misalkan kita memiliki citra asal yang berukuran 150x200 pixel. Pesan yang disisipkan ada 422 karakter. Ukuran citra setelah disisipkan menjadi 153x200, dengan kata lain 422 karakter yang ada memakan tempat sebanyak 3 baris. Dengan metode EOF, secara umum media steganografi (file yang akan disisipi data) memiliki struktur seperti gambar ini:
(Yayuk dan Dolly, 2014)



Sebagai contoh pada sebuah citra grayscale 6x6 piksel disisipkan pesan yang berbunyi “aku”. Untuk menandai akhir pesan digunakan karakter yang jarang dipakai, misalnya karakter #. Sehingga pesan yang dimaksud adalah “#aku”. Kode ASCII dari pesan diberikan sebagai berikut (Hariady,2015) :
97 107 117 35

Misalkan sebuah citra *grayscale* dengan kode warna:

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200

Nilai desimal pesan berdasarkan tabel ascii disisipkan diakhir citra, sehingga citra menjadi:

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200
97	107	117	35		

Teknik EOF tidak mengubah isi awal dari file yang disisipi. Sebagai contoh, jika pengguna menyisipkan sebuah pesan kedalam sebuah dokumen, isi dari dokumen tidak akan berubah. Ini yang menjadi salah satu keunggulan metode EOF dibandingkan dengan metode steganografi yang lain. Karena disisipkan pada akhir file, pesan yang disisipkan tidak akan bersinggungan dengan isi file, hal ini menyebabkan integrasi data dari file yang disisipi tetap terjaga. (Ulan dkk,
2017)

5) **Java**

Java dikembangkan oleh perusahaan Sun Microsystem. *Java* menurut definisi dari Sun Microsystem adalah nama untuk sekumpulan teknologi untuk membuat dan menjalankan perangkat lunak pada komputer *standalone* ataupun pada lingkungan jaringan. *Java* 2 adalah generasi kedua dari *java platform*. (Rosa A.S dan M.Shalahuddin, (2014:103), *Rekaya Perangkat Lunak.* Jakarta: PT Elex Media Komputindo)

Java merupakan bahasa berorientasi objek untuk pengembangan aplikasi mandiri, aplikasi berbasis internet, aplikasi untuk perangkat cerdas yang dapat berkomunikasi lewat internet/ jaringan komunikasi. Melalui teknologi *java*, dimungkinkan perangkat *audio streo* dirumah terhubung jaringan komputer.

Java tidak lagi hanya untuk membuat *applet* yang memperintah halaman *web* tapi *java* telah menjadi bahasa untuk pengembangan aplikasi skala *interprise* berbasis jaringan besar (Bambang Haryanto, (2017:2) *Esensi-esensi Bahasa Pemrograman Java*. Yogyakarta: Andi)

Dari pengertian diatas maka dapat disimpulkan bahwa *Java* merupakan bahasa pemrograman berorientasi objek yang dapat digunakan untuk membuat dan menjalankan perangkat lunak pada komputer dan berbagai *platform.*

BAB III
METODELOGI PENELITIAN A. Desain Penelitian

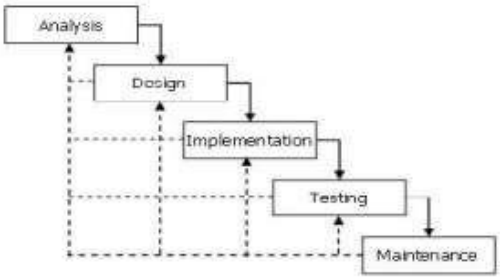
Desain penelitian ini penulis menggunakan metode deskriptif yaitu metode pengumpulan data studi rancangan yang memusatkan sistem operasional keamanan data .Dengan cara mengumpulkan data kemudian di susun dan di analisis untuk memperoleh gambaran mengenai masalah yang di hadapi pada saat penelitian.

B. Metode Pengembangan Sistem

Untuk pengembangan sistem penelitian ini menggunakan model SDLC (*Software*

Development Life Cycle). *System Development Life Cycle* (SDLC) adalah proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sebuah sistem. SDLC juga merupakan pola yang diambil untuk mengembangkan sistem perangkat lunak, yang terdiri dari tahaptahap: rencana (*planning*), analisis (*analysis*), desain (*design*), implementasi (*implementation*), uji coba (*testing*) dan pengelolaan (*maintenance*).

Model SDLC yang dipakai dalam penelitian ini adalah model *Waterfall*. *Waterfall Model* atau *Classic Life Cicle* merupakan model yang paling banya dipakai dalam *Software Enginnering* (SE). Menurut Bassil (2012) disebut waterfall karena tahap demi tahap yang harus dilalui menunggu selesainya tahap sebelumnya dan berjalan berurutan.



Metode *Waterfall* menurut Bassil (2012)

C. Metode Implementasi Sistem

Implementation untuk dapat dimengerti oleh mesin, dalam hal ini adalah komputer, maka desain tadi harus diubah bentuknya menjadi bentuk yang dapat dimengerti oleh mesin, yaitu ke dalam bahasa pemrograman melalui proses coding. Tahap ini merupakan implementasi dari tahap *design* yang secara teknis nantinya dikerjakan oleh programmer. Pada tahap ini, peneliti membangun sebuah aplikasi berdasarkan desain "*blueprint*" yang telah dibuat. Pengembangan aplikasi ini dilakukan dari awal hingga aplikasi siap dijalankan. Dari fungsi-fungsi yang dibutuhkan hingga tampilan untuk pengguna.

D. Metode Pengujian Sistem *Testing / Verification* Sesuatu yang dibuat haruslah diujicobakan. Demikian juga dengan *software*. Semua fungsifungsi *software* harus di ujicobakan, agar *software* bebas dari *error*, dan hasilnya harus benar-benar sesuai dengan kebutuhan yang sudah didefinisikan sebelumnya. Setelah proses pembangunan aplikasi selesai, peneliti melakukan pengujian pada tahap ini. Aplikasi diuji berdasarkan metode *black box* untuk mengetahui tingkat keberhasilan dari bagian sistem. Selain itu, peneliti juga melakukan pengujian secara langsung pada setiap sesi perkuliahan di UMT (khususnya di Jurusan Teknik Informatika).

BAB IV
ANALISIS DAN PEMBAHASAN

A. Analisis Sistem Berjalan

Analisis sistem merupakan penjabaran dari suatu sistem informasi yang utuh ke dalam berbagai macam bagian komponennya dengan maksud agar kita dapat mengidentifikasi atau mengevaluasi berbagai macam masalah maupun hambatan yang akan timbul pada sistem sehingga nantinya dapat dilakukan penanggulangan, perbaikan atau juga pengembangan. Pada tahap ini di lakukan survei tehadap sistem yang sedang berjalan antara lain mengumpulkan data dan informasi dari perusahaan CV Lestari Electric, yang di lakukan dengan cara observasi dan interview atau wawancara langsung pada karyawan perusahaan yang ada di tempat untuk memperoleh data yang diperlukan.

B. Gambaran Sistem Berjalan

Pada Proses keamanan data yang ada di perusahaan CV.Lestari Electric masih belum menggunakan sistem yang berbasis keamanan data. Proses keamanan data yang di gunakan di perusahaan ini hanya menggunakan email dan pengiriman jasa kurir yang belum bisa di percaya keamanan nya

C. Penerapan Perangkat Keras (*Hardware*), Perangkat Lunak (*Software*)

Agar aplikasi ini dapat berjalan dengan baik dan bekerja sesuai dengan apa yang diharapkan, spesifikasi perangkat keras dan perangkat lunak yang dipakai untuk menerapkan aplikasi ini juga harus mendukung. Berikut spesifikasi yang bisa mendukung penerapan aplikasi ini, diantaranya adalah
:

1) Perangkat Keras (*Hardware*)

Perangkat keras (*hardware*) yang dipakai untuk menerapkan aplikasi ini adalah sebagai berikut :

a. Laptop Lenovo G40
b. *Processor* Intel Core i3 CPU @1.90 GHz
c. *Memory* DDR3 2GB
d. *Display* 14” 1366 x 768 (32-bit)
e. *Hard Drive* 512 GB data

2) Perangkat Lunak (*Software*)

Perangkat lunak (*software*) yang dipakai untuk menerapkan aplikasi ini adalah sebagai berikut : a. Windows 10 64-bit
b. Netbeans IDE 8.2
c. Ms. Word 2010

D. Kebutuhan Pengguna (Brainware)

Pengoperasian sistem dan penginputan dilakukan oleh pengirim data yang harus di rahasiakan kunci dari kode pengaplikasian yang nanti di beritahukan ke penerima bila ingin
membuka dokumen tersebut

E. Implementasi Perancangan Sistem

1. Tampilan *Form* Menu Utama

Tampilan layar dari *form* Menu Utama pada gambar di bawah ini muncul pada saat pertama kali aplikasi dijalankan dan

terlihat beberapa menu yang bisa digunakan seperti *Generate Key, Encode, Decode, About, Help* dan *Exit* untuk keluar dari aplikasi.

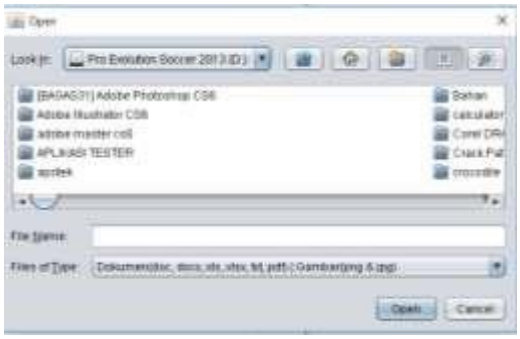
Tampilan Layar *Form* Menu Utama

2. Tampilan Layar *Form Generate Key*

Tampilan layar dari *form Generate Key* pada gambar di bawah ini muncul pada saat pertama kali aplikasi dijalankan untuk membuat *Public* dan *Private Key*.

Tampilan Layar *Form Generate Key*

Tampilan Gambar menggambarkan memilih folder untuk menyimpan hasil dari pembuatan kunci.

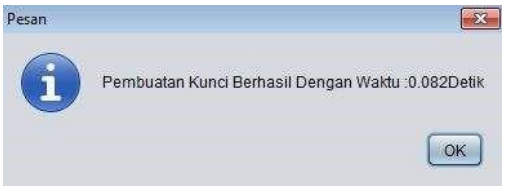


Tampilan Layar *Save* Folder *Generate Key*

Tampilan Gambar di bawah ini jika form belum lengkap atau ada salah satu *form* yang belum di input.

Tampil Pesan Data Belum Lengkap.

Tampilan Gambar di bawah ini menggambarkan ketika kunci *public* dan *private* berhasil dibuat atau *Generate Key* berhasil dilakukan dan akan tampil informasi waktu pembuatan kunci.



Tampil Pesan Data Pembuatan Kunci

Berhasil

3. Tampilan Layar *Form Encode File*

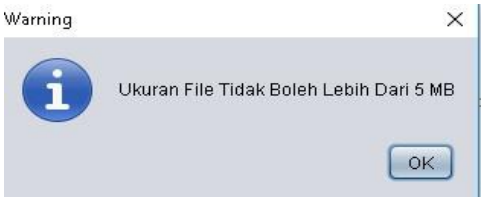
Tampilan layar dari *form Encode File* pada gambar di bawah ini muncul pada saat menu *Encode File* dijalankan.

Tampilan Layar *Form Encode File*

Tampilan Gambar di bawah ini menggambarkan memilih *file* yang akan dienkripsi, adapun jenis *file* yang bisa digunakan yaitu *docx, *xlsx, dan *jpg. Tetapi batas maksimum *file* yang bisa diekripisi adalah 5 MB.

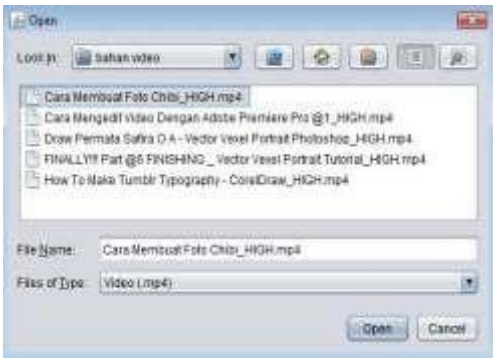
Tampilan Layar Pilih *File* Asli.

Jika *file* yang akan di enkripsi melebihi 5 MB maka akan muncul pesan seperti di bawah ini.



Tampilan Layar Pesan Batas Maksimal

Tampilan Gambar di bawah ini menggambarkan memilih *file video* yang akan disisipin oleh *file* hasil enkripsi, adapun jenis *file* yang bisa digunakan yaitu *MP4*. Tetapi batas maksimum *file* video yang akan menjadi tempat penyisipan adalah 30 MB.



Tampilan Layar *Browse Video*

Jika melebihi batas masksimal akan muncul pesan ukuran *video* tidak boleh lebih dari 30 MB seperti pada Gambar di bawah ini.

Tampilan Layar *Video* Tidak Boleh Melebihi batas 30 MB

Tampilan Gambar di bawah ini menggambarkan memilih folder untuk menyimpan hasil *file* yang telah *diencode*

Tampilan Layar *Save Folder Encode File*

Tampilan Gambar di bawah ini menggambarkan memilih *Public Key* yang digunakan untuk melakukan proses *encode*.

Tampilan Layar Pilih *PublicKey*

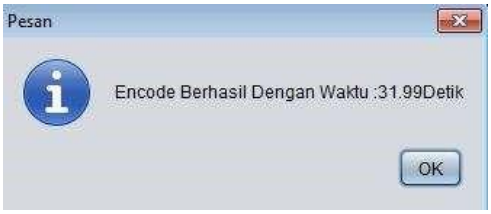
Tampilan Gambar di bawah ini jika *form* belum lengkap atau ada salah satu *form* yang belum di *input*.

Tampilan Pesan Lengkapi *Form*

Tampilan Gambar di bawah ini menggambarkan pesan ketika enkripsi berhasil dilakukan atau *Encode* berhasil dilakukan

Tampilan Layar Pesan *Encode* Berhasil

Tampilan Gambar di bawah ini menggambarkan ketika proses enkripsi berhasil dilakukan dan akan tampil informasi waktu proses *encode*.

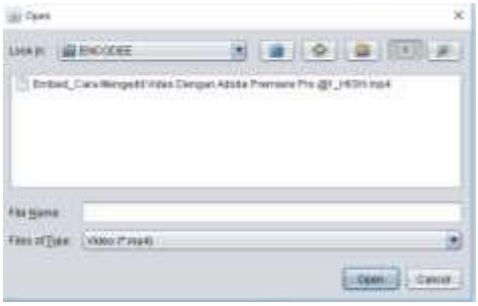


Tampilan Layar Proses *Encode* Berhasil

4. Tampilan Layar *Form Decode File*

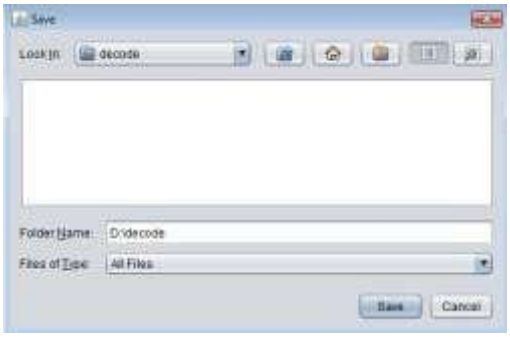
Tampilan layar dari *Form Decode File* pada gambar di bawah ini muncul pada saat menu *Decode File* dijalankan.

Tampilan Layar *Form Decode File*
Tampilan Gambar di bawah ini menggambarkan ketika memilih *file* yang akan dikembalikan seperti semula atau akan di *decode*.



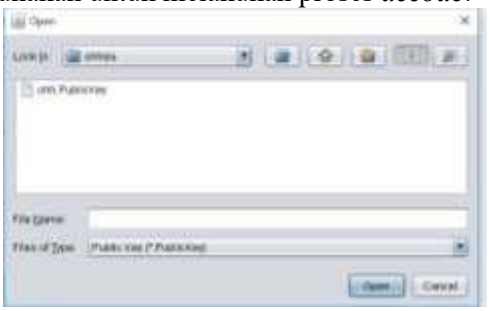
Tampilan Layar Pilih *File* Hasil *Encode*

Tampilan Gambar di bawah ini menggambarkan memilih *folder* untuk menyimpan hasil *file* yang telah di *decode*



Tampilan Layar Pilih *Save Folder Decode File*

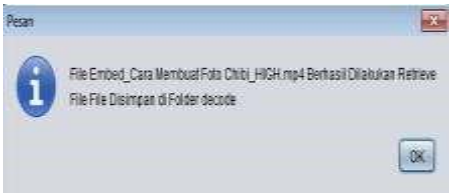
Tampilan Gambar di bawah ini menggambarkan memilih *Private Key* yang digunakan untuk melakukan proses *decode*.



5.

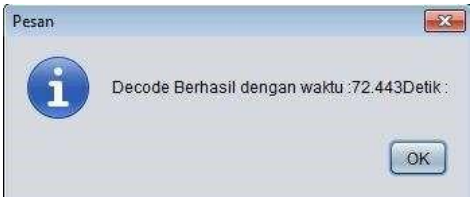
Tampilan Layar Pilih *PrivateKey*

Tampilan Gambar di bawah ini menggambarkan pesan ketika dekripsi berhasil dilakukan atau *Decode* berhasil dilakukan.



Tampilan Layar Pesan *Decode* Berhasil

Tampilan Gambar menggambarkan ketika proses *decode* berhasil dilakukan dan akan tampil informasi waktu proses *decode*.



Tampilan Layar Proses *Decode* Berhasil

Tampilan Layar *Form Help*

Pengguna dapat melihat informasi cara penggunaan aplikasi dengan melihat tampilan layar *form help* ini yang dibagi menjadi tiga. Tampilan layar *form help* dapat dilihat pada gambar di bawah ini.

Tampilan Layar *Form Help*

Tampilan Layar *Form Help Generate Key*

Pengguna dapat melihat informasi cara penggunaan menu *Generate Key*. Tampilan layar *form help* dapat dilihat pada gambar di bawah ini.

Tampilan Layar *Form Help Generate Key*

Tampilan Layar *Form Help Decode File*

Pengguna dapat melihat informasi cara penggunaan menu *Decode File*. Tampilan layar *form Help Decode File* dapat dilihat pada gambar di bawah ini.

Tampilan Layar *Form Help Decode file*

Pengguna dapat melihat informasi cara penggunaan menu *Encode File*. Tampilan layar *Help Encode File* dapat dilihat pada gambar di bawah ini

Tampilan Layar *Form Help Encode file*

6 Tampilan Layar *Form About*

Pada tampilan layar *form About,* pengguna dapat melihat informasi tentang aplikasi ini. Tampilan layar *form about* dapat dilihat pada gambar di bawah ini.

Tampilan Layar *Form About.*

BAB V
PENUTUP

A. Kesimpulan

Berdasarkan perancangan, pembuatan, serangkaian uji coba dan analisa program dari aplikasi kriptografi dan steganografi ini, maka dapat diambil suatu kesimpulan antara lain :

a. Waktu yang digunakan untuk melakukan proses *encode* dan *decode* berbanding lurus dengan ukuran *file* yang diproses (semakin kecil ukuran *file* yang diproses, semakin cepat proses encode dan decode dilakukan, semakin besar ukuran *file* yang diproses, semakin lama proses encode dan decode dilakukan).
b. Satu kunci *public* dan *private* bisa digunakan berkali-kali dengan jenis ataupun *file* yang berbeda
c. Proses *decode* dengan kunci yang sesuai akan mengembalikan *file* menjadi *file* semula tanpa mengalami perubahan sedikitpun.
d. Dengan adanya aplikasi kriptografi dan steganografi ini, proses penyimpanan dan pertukaran informasi menjadi lebih aman.

B. Saran

Adapun saran yang mungkin diperlukan untuk membuat aplikasi ini dapat berjalan lebih baik lagi antara lain

a. Dikembangkan menggunakan algoritma kompresi agar ukuran *file* hasil *encode* diharapkan dapat menjadi lebih kecil lagi.
b. Waktu proses *encode* dan *decode* *file* yang rata-rata berukuran besar diharapkan dapat berjalan lebih cepat pada *hardware* yang lebih baik.
c. Aplikasi ini diharapkan dapat ditingkatkan kinerjanya sehingga tidak hanya dapat mengenkripsi *file* dokumen *.docx, *.xlsx dan *.jpg

saja, namun bisa juga untuk *file* video maupun *audio*.

DAFTAR PUSTAKA

Ainurrizan, 2014, implementasi steganografi pada file image menggunakan teknik spread spectrum. *Skripsi.* Fakultas Ilmu komputer/Informatika. Diponegoo.

Akhmad Sholikhin. 2013. Pembangunan Sistem Informasi Inventarisasi Sekolah Pada Dinas Pendidikan Kabupaten Rembang Berbasis Web. IJNS : Vol. 2, No.2. 50-57

Deni Mahdiana, 2011. Analisa Dan Rancangan Sistem Informasi Pengadaan Barang Dengan Metodologi Berorientasi Obyek: Studi Kasus PT. Liga Indonesia". Universitas Budi Luhur : Vol. 3, No. 2. 36-43

Destriana, R., Kom, M., Husain, S. M., Kom, S., Handayani, N., Kom, M., ... & Kom, S. (2021). Diagram UML Dalam Membuat Aplikasi Android Firebase" Studi Kasus Aplikasi Bank Sampah". Deepublish.

Destriana, R. (2018). Efektivitas Kinerja It Support Menggunakan Fungsi Service Desk Sebagai Single Point of Contact (Spoc): Studi Kasus Pt Xyz. JIKA (Jurnal Informatika), 2(1).

Destriana, R., Handayani, N., Husain, S. M., & Siswanto, A. T. P. (2021, March). A Research to Design, Develop and Implementation of Android Application System for Waste Bank Sharia Community at Kampung Hijau Kemuning. In IOP Conference Series: Materials Science and Engineering (Vol. 1115, No. 1, p. 012042). IOP Publishing.

Destriana, R., Taufiq, R., & Suryana, B. E. (2020). Rancang Bangun Sistem Informasi Document Managemen System Pada Lkp Itc-Pcb Berbasis Web. Jurnal Inovasi Informatika Universitas Pradita, 5(1), 64-71. http://jurnal.pradita.ac.id/index.php/jii/article/view/35 (Crossref) https://doi.org/10.51170/jii.v5i1.35

Destriana, R., Taufiq, R., & Suryana, B. E. (2020). Rancang Bangun Sistem Informasi Document Managemen System pada LKP ITC-PCB Berbasis WEB Menggunakan UML dan PHP. Jurnal Inovasi Informatika, 5(1), 64-71.

Destriana, R. (2021). Pengembangan Software ERP menggunakan Module Sales Management pada PT. XYZ. Jurnal Teknik, 10(1).

Faruq, Ahmad, 2013, Implementasi Sistem Keamanan Data Dengan Menggunakan Tehnik Steganografi Metode *End Of File* (EOF) Berbasis Java Programing, Universitas Budi Luhur Jakarta.

Nasutiyon, Y, R dkk, 2017. Aplikasi penyembunyian multimedia menggunakan metode end of file

(eof) dan huffman coding. *journal.* Teknik Informatika. Diponegoo. Vol. 5 No. 1 ISSN 2303-0755

Nurlaila Hasyim. 2014. Rancang Bangun Sistem Informasi Koperasi Berbasis Web Pada Koperasi Warga Baru Mts N 17 Jakarta. Universitas Islam Negeri Syarif hidayatullah Jakarta. 1-11

Siregar, H, F dan Sari, N. 2018. Rancang Bangun Aplikasi Simpan Pinjam Uang Mahasiswa Fakultas Teknik Universitas Asahan Berbasis Web, *journal teknologi Informasi* EISSN 2615- 2738. Vol.2, No.1.

Taufik Ramadhan, 2014. Rancang Bangun Aplikasi Mobile Untuk Notifikasi Jadwal Kuliah Berbasis Android *Studi Kasus Stmik Provisi Semarang*. STMIK PROVISI Semarang : Vol. 5, No.2. 47-55

Hakim, F, L 2015, rancang bangun ecommerce menggunakan uml*based web engineering* (uwe). *Skripsi.* Fakultas Ilmu komputer/Informatika. Diponegoo.

Hasyim N, Nur, A, H & Sarwoto, W, L, 2014. Rancang bangun sistem informasi koprasi berbasis web pada koprasi warga baru MTS N 17, Jakarta *journal dari sistem informasi.* ISSN 1979-0767.7(2) 1:11.

Zulfiandri, S, H & Mochammad A, 2014. Rancang bangun aplikasi poliklinik gigi , prosidimg sminar ilmiah nasional computer dan sistem intelejen, Vol 8: 472-482, ISSN 2302-3740