ISSN : 2548-9704

ANALISA KOMBINASI PESAN TEKS KE DALAM FILE AUDIO MEMANFAATKAN ALGORITMA DATA ENCRYPTION STANDARD DAN METODE END OF FILE

ACHMAD FAUZI

STMIK KAPUTAMA ,
Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara
E-mail : fauzyrivai88@gmail.com

ABSTRAK

Perkembangan dunia teknologi informasi yang sangat pesat akhir-akhir ini berpengaruh dalam segala aspek kehidupan. Untuk menjaga dan mengamankan pesan maka digunakan banyak teknik yang berbeda dan tidak mudah untuk di lihat oleh orang lain. Dengan menggunakan dua metode ini digunakan untuk menjaga kerahasian pesan yang akan dikirim, guna melindungi pesan tersebut dari orang-orang yang tidak diberikan hak untuk melihat pesan yang bersifat rahasia tersebut. Algoritma DES (Data Encryption Standart) termasuk Algoritma kriptografi simetri yang tergolong jenis blok kode algoritma DES yang beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit teks asli menjadi 64 bit teks kode menggunakan 56 bit kunci internal (internal key) atau kunci (subkey) sedangkan kunci internal dapat dibangkitkan sedangkan Metode End Of File (EOF) merupakan salah satu teknik untuk menyisipkan data pada akhir file. Kedua Algoritma Data Encryption Standard (DES) Dengan Memanfaatkan Metode End Of File (EOF), akan muncul menamampilkan baca pesan Aplikasi Keamanan Pesan Teks Ke Dalam File Audio Menggunakan Algoritma Data Encryption Standard (DES) Dengan Memanfaatkan Metode End Of File (EOF

Kata Kunci: Algoritma DES, Metode End Off File (EOF), Sound, Data Teks

1. PENDAHULUAN

Perkembangan teknologi komputer pada saat ini menyebabkan terkaitnya manusia dengan komputer untuk memudahkan membantu penyelesaian dan komputerisasi. hal ini membuka banyak peluang dalam pengembangan aplikasi computer tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data. oleh karena itu, untuk melindungi data terhadap pencurian, piranti keamanan data komputer harus disediakan. Dalam hal ini penulis mencoba untuk membuat suatu aplikasi untuk mengamankan pesan teks karakter yang akan dilindungi kerahasiannya. Pada pesan teks karakter yang akan di amankan biasanya bersifat rahasia, dan butuh perancangan aplikasi lain untuk mengamankannya. aplikasi yang sudah dibuat misalnya aplikasi yang dapat mengkonversikan pesan teks karakter ke dalam bentuk biner, ada juga aplikasi yang dibuat untuk menyisipkan pesan teks, misalnya menyisipkan pesan teks karakter ke dalam gambar dan media lain. Mungkin saja pada saat ini pengamanan pesan belum banyak yang memanfaatkan media audio sebagai sarana untuk menyisipkan pesan tersebut. untuk tingkat keamanannya mungkin dapat ditambah dengan metode lain, misalnya menggabungkan dua metode berbeda untuk mengkonversi pesan teks karakter dan menyisipkannya ke dalam media audio supaya lebih aman dalam pengiriman dan terhindar dari pembajakan isi pesan. Banyak sudah aplikasi yang diciptakan guna menjaga keamanan pesan yang dibuat, yang bertujuan meningkatkan keamanan pesan yang akan dikirim, beberapa diantaranya yang penulis kutip dari beberapa referensi jurnal, yaitu **"Aplikasi Enkripsi SMS (Short Message Service) Menggunakan Algoritma Data Encryption Standart (DES) Berbasis Android (Syamsul Bahri Lubis)** dan **"Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File (EOF) (Sandro Sembiring)".** algoritma des merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh nist (national institue of standards

ISSN : 2548 - 9739

and technology) sebagai standar pengolah informasi federal as. data plaintext dienkrip dalam blok-blok 64 bit menjadi 64 bit data ciphertext menggunakan kunci 56 bit kunci internal (internal key). Sedangkan metode eof (*end of file*) merupakan salah satu teknik yang dapat 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.

2. LANDASAN TEORI

2.1. Steganografi

Steganografi berasal dari bahasa yunani yaitu *stegos* yang berarti penyamaran dan *graphia* yang berarti tulisan. Steganografi digunakan untuk menyembunyikan informasi rahasia ke dalam suatu media sehingga keberadaan pesan tersebut tidak diketahui oleh orang lain. Steganografi bertujuan untuk menghilangkan kecurigaan dengan cara menyamarkan pesan tersebut. (rinaldi, 2006, h. 301). Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. media tempat penyembunyian pesan tersembunyi dapat berupa media teks, gambar, audio atau video. (sadikin, 2012, h. 10)

Menurut (rinaldi, 2006, h. 12) ada beberapa hal yang diperlukan untuk menyembunyikan pesan yaitu:

1. Algoritma penyisipan (*embeding algorithm*).
   Algoritma ini digunakan untuk menyisipkan suatu pesan yang disembunyikan ke dalam suatu data yang akan dikirim. proses penyisipan ini diproteksi oleh sebuah *key-word* sehingga hanya orang-orang yang mengetahui *key-word* ini yang dapat membaca pesan yang disembunyikan tersebut.
2. Fungsi detektor (*detector function*).
   fungsi detektor ini adalah untuk mengembalikan pesan-pesan yang disembunyikan tersebut.
3. *Carrier document.*
   Merupakan dokumen yang berfungsi sebagai media yang digunakan untuk menyisipkan informasi. dokumen ini dapat berupa *file-file* seperti *file* audio,video atau *citra(gambar).*
4. *Key*
   Merupakan kata kunci yang ikut disisipkan kedalam dokumen berguna dan dipakai sebagai proses verifikasi sewaktu informasi akan ditampilkan atau diuraikan.
5. *Secret message/ plaintext* Merupakan pesan rahasia yang akan disisipkan kedalam *carrier document*. pesan inilah yang tidak ingin terlihat dan terbaca oleh orang yang tidak berkepentingan.

2.2. Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita [**bruce schneier** – *applied cryptography*]. “crypto” berarti “secret” (rahasia) dan “graphy” berarti “writing” (tulisan). Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupasinformasi yang telah disandi.

1. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. untuk menjaga integritas data, system harus memiliki kemampuan untuk mendeteksi manipulasi data

ISSN : 2548-9704

oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

2. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
3. Non-repudiasi., atau penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat. (munir, 2006, h. 9)

Tujuan pokok dari kriptografi adalah untuk mencapai keempat tujuan di atas baik secara teori maupun prakteknya. kriptografi merupakan ilmu yang berhubungan dengan pencegahan dan deteksi terhadap penjiplakan dan aktivitas kriminal lainnya. Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption). ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. menurut iso 7498- 2, terminologi yang lebih tepat digunakan adalah “encipher”. kriptografi bisa dilakukan dengan algoritma sandi. algoritma tersebut harus memiliki kekuatan untuk melakukan (dikemukakan oleh shannon):

1. Konfusi/pembingungan (confusion), dari teks terang sehingga sulit untuk direkonstruksikansecara langsung tanpa menggunakan algoritma dekripsinya.
2. Difusi/peleburan (difusion), dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

Sehingga dapat digunakan untuk mengamankan informasi. pada implementasinya sebuah algoritmas sandi harus memperhatikan kualitas layanan/quality of service atau qos dari keseluruhan sistem dimana dia diimplementasikan. algoritma sandi yang handal adalah algoritma sandi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri. teknik dan metode untuk menguji kehandalan algoritma sandi adalah kriptanalisa. Secara umum berdasarkan kesamaan kuncinya, algoritma sandi dibedakan menjadi :

1. Kunci-simetris/symetric-key, sering disebut juga algoritma sandi konvensional karena umumnya diterapkan pada algoritma sandi klasik.
2. Kunci-asimetris/asymetric-key.

Berdasarkan arah implementasi dan pembabakan jamannya dibedakan menjadi :

1. Algoritma sandi klasik classic cryptography.
2. Algoritma sandi modern modern cryptography. (sadikin, 2012, h. 9)

2.3. *Data Encryption Standard* (Des)

DES (Data Encrytion Standard) adalah algoritma cipher blok yang popular karena dijadikan standard algoritma enkripsi kunci-simetri, meskipun saat ini standard tersebut telah digantikan dengan algoritma yang baru. sebenarnya DES adalah nama standard enkripsi simetri, nama algoritma enkripsinya adalah DEA (data encryption algorithm), namun nama DES lebih popular dari dea. algoritma DES dikembangkan di ibm, algoritma ini didasarkan pada algoritma luciferyang dibuat oleh horstfeistel.

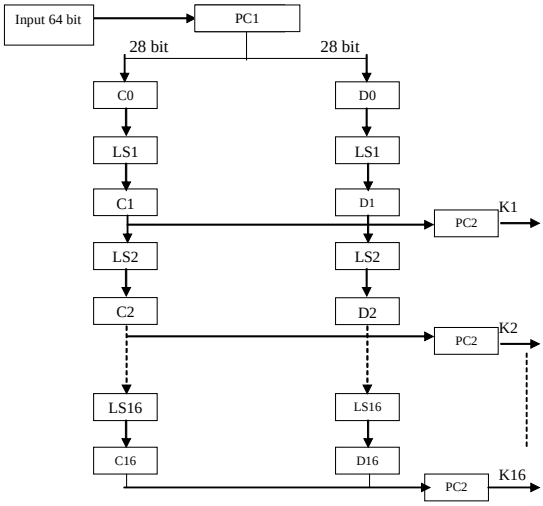
algoritma ini telah disetujui oleh *national bureau of standard (nbs)* setelah penilaian kekuatannya oleh *national security agency (nsa)* amerika serikat. (munir, 2006, h. 136).

ISSN : 2548 - 9739

DES (Data Encryption Standart) termasuk sistem kriptografi simetri dantergolong jenis blok kode. des beroperasi pada ukuran blok 64 bit. des mengenkripsikan 64 bit teks asli menjadi 64 bit teks kode menggunakan 56 bit kunci internal (internal key) atau upa kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit. Blok teks - asli dipermutasi dengan matriks permutasi awal (initial permutation). Bisa ditulis x0 = IP (x) = L0R0, dimana L0 terdiri dari 32 bit pertama dari x0 dan 32 bit terakhir dari R0. Sumber : (Fauzi, 2016)

Hasil permutasi awal kemudian di – enciphering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda dengan perhitungan Li dan Ri $1 \leq i \leq 16$, dengan mengikuti aturan berikut : Li = Ri – 1

Ri = Li – 1 f (Ri – 1, Ki)



Gambar II.1 Algoritma Enkripsi DES permutasi Awal

2.4 *End Of File* (Eof)

Metode *end of file* (EOF) metode ini merupakan metode pengembangan lsb.dalam metode ini pesan disisipkan diakhir berkas.pesan yang disisipkan dengan metode ini jumlahnya tidak terbatas.akan tetapi efek sampingnya adalah ukuran berkas menjadi lebih besar dari ukuran semula. ukuran berkas yang terlalu besar dari yang seharusnya, tentu akan menimbulkan kecurigaan bagi yang mengetahuinya.

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 *ctrl-z* yang diberikan pada setiap akhir *file*.

EOF menggunakan *redundant* bits sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitif sehingga seakan-akan tidak ada perbedaan yang terlihat antara sebelum atau sesudah pesan disisipkan.

Kemudahan melakukan *steganalysis* merupakan suatu cara dalam melacak keberadaan pesan rahasia yang disisipkan melalui proses *steganography*. dengan meletakkan pesan rahasia setelah tanda khusus sebagai pengenal *start* dari data tersebut, algoritma pelacakan pesan akan semakin mudah, karena yang perlu dilakukan adalah membaca isi data pada posisi pengenal *start* diletakkan.

Adapun algoritma dari metode eof ini adalah sebagai berikut :

1. Baca informasi *file*, tentukan dimana posisi karakter pengenal *start* berada.
2. Tandai posisi pengenal *start* sebagai awal baris penyisipan pesan.
3. Sisipkan pesan dimulai dari posisi pengenal *start* hingga akhir pesan.

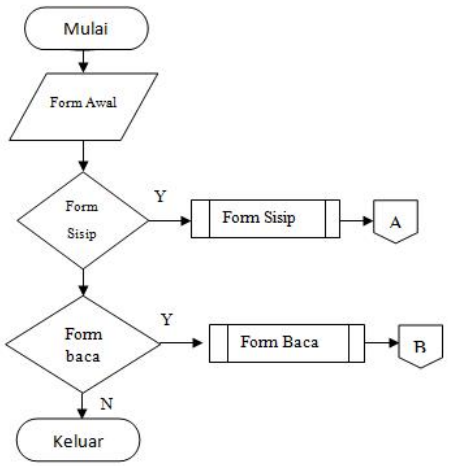
3. Dengan menyisipkan sebuah pesan setelah karakter pengenal *start* (*end of file*), pada saat *file* tersebut dieksekusi, pesan yang disisipkan tidak akan terbaca oleh sistem. hal ini disebabkan oleh karena sistem hanya akan membaca isi dari sebuah *file* dimulai dari karakter awal *file* tersebut hingga sistem menemukan karakter pengenal start (*end of file*). Sebagai contoh, akan disisipkan sebuah pesan pada sebuah citra digital dengan dimensi 120 x 160 pixel. Maka pesan akan ditempatkan pada baris ke 121 sampai selesai sesuai dengan

ISSN : 2548-9704

panjang dari pesan yang disisipkan. Setiap baris akan memetakan pesan sebanyak 160 karakter (sesuai dengan ukuran citra) hingga seluruh pesan disisipkan seluruhnya. Kemudahan Melakukan *Steganalysis* merupakan suatu cara dalam melacak keberadaan pesan rahasia yang disisipkan melalui proses *steganography*.

3. ANALISIS DAN PERANCANGAN

Adapun rancangan pada penelitian dapat dilihat pada gambar 3.1 dibawah ini :



Gambar III.1 *Flowchart* Aplikasi Form Awal

Misalnya pada sebuah gambar disisipkan pesan yang berbunyi "Computer". dengan key(k) : 13 34 57 79 9b bc df f1 enkripsi dengan algoritma *data encryption standard* (des) langkah pertama ubahlah plaintext kedalam bentuk biner

x_o =
c : 01000011
o : 01001111
m: 01001101
p : 01010000
u : 01010101
t : 01010100
e : 01000101
r : 01010010
ubahlah key kedalam bentuk biner
k =
19 : 00010011
62 : 00110100
87 : 01010111
125 : 01111001
9b : 10011011
bc : 10111100
df :11011111
f1 : 11110001
langkah ke-dua tabel IP
Tabel. 1. Tabel PC- 1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

ip(x) : 11111111 10111000 01110110 01010111 00000000 00000000 00000110 10000011
l_0 : 11111111 10111000 01110110 01010111
r_0 : 00000000 00000000 00000110 10000011

Langkah ke-tiga :

cd(k) : 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111
c_0 : 1111000 0110011 0010101 0101111(tabel pc-1 warna kuning)
d_0 : 0101010 1011001 1001111 0001111

langkah ke-empat

c_0 : 1111000 0110011 0010101 0101111
d_0 : 0101010 1011001 1001111 0001111
digeser 1 bit ke kiri
c_1 : 1110000 1100110 0101010 1011111
d_1 : 1010101 0110011 0011110 0011110
digeser 2 bit ke kiri
c_2 : 1100001 1001100 1010101 0111111
d_2 : 0101010 1100110 0111100 0111101
digeser 2 bit ke kiri

ISSN : 2548 - 9739

c_3 : 0000110 0110010 1010101 1111111
d_3 : 0101011 0011001 1110001 1110101
digeser 2 bit ke kiri
c_4 : 0011001 1001010 1010111 1111100
d_4 : 0101100 1100111 1000111 1010101
digeser 2 bit ke kiri
c_5 : 1100110 0101010 1011111 1110000
d_5 : 0110011 0011110 0011110 1010101
digeser 2 bit ke kiri
c_6 : 0011001 0101010 1111111 1000011
d_6 : 1001100 1111000 1111010 1010101
digeser 2 bit ke kiri
c_7 : 1100101 0101011 1111110 0001100
d_7 : 0110011 1100011 1101010 1010110
digeser 2 bit ke kiri
c_8 : 0010101 0101111 1111000 0110011
d_8 : 1001111 0001111 0101010 1011001
digeser 1 bit ke kiri
c_9 : 0101010 1011111 1110000 1100110
d_9 : 0011110 0011110 1010101 0110011
digeser 2 bit ke kiri
c_{10} : 0101010 1111111 1000011 0011001
d_{10} : 1111000 1111010 1010101 1001100
digeser 2 bit ke kiri
c_{11} : 0101011 1111110 0001100 1100101
d_{11} : 1100011 1101010 1010110 0110011
digeser 2 bit ke kiri
c_{12} : 0101111 1111000 0110011 0010101
d_{12} : 0001111 0101010 1011001 1001111
digeser 2 bit ke kiri
c_{13} : 0111111 1100001 1001100 1010101
d_{13} : 0111101 0101010 1100110 0111100
digeser 2 bit ke kiri
c_{14} : 1111111 0000110 0110010 1010101
d_{14} : 1110101 0101011 0011001 1110001
digeser 2 bit ke kiri
c_{15} : 1111100 0011001 1001010 0001111 1010111
d_{15} : 1010101 0101100 1100111 1000111
digeser 1 bit ke kiri
c_{16} : 1111000 0110011 0010101 0101111
d_{16} : 0101010 1011001 1001111

Sampai 16 kali permutasi dan setelah itu akan dikalukan XOR dengan Kunci sehingga akan menghasilkan cipher seperti dibawah ini :

Penyisipan dengan metode *end of file* (EOF) misalkan tingkat derajat audio sebagai berikut :

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

kode biner pesan disisipkan di akhir audio, sehingga audio 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
44 66 99 125 190 200
56 f1 d5 c8 52 af 81 3f

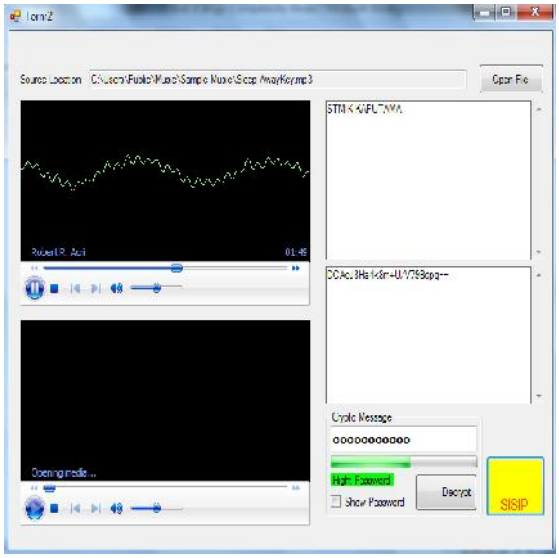
4. PEMBAHASAN DAN IMPLEMENTASI

Program Aplikasi Keamanan Pesan Teks Ke Dalam File Audio Menggunakan Algoritma Data Encryption Standard (DES) Dengan Memanfaatkan Metode End Of File (EOF) ini dibangun dengan tujuan untuk menjaga keamanan teks yang dikirimkan ke *user* lain dengan cara menyisipkan isi

ISSN : 2548-9704

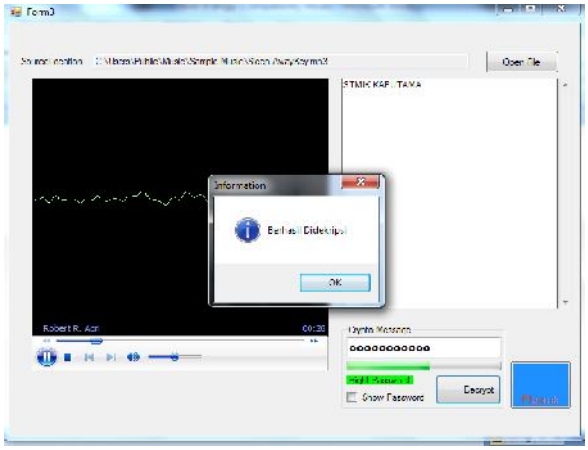
tersebut dan membaca kembali isi tersebut agar pesan asli dapat dibaca, dalam hal ini *user* haruslah memiliki aplikasi ini

Gambar 4.1 Tampilan Awal Aplikasi



Gambar IV.2 Tampilan penyisipan teks dengan aplikasi

Form di atas merupakan form penyisipan teks. *Sender* dapat melakukan penginputan audio sebagai media penampung, Teks yang ingin



Gambar IV. 2 Tampilan membaca teks dengan aplikasi

Form di atas merupakan form pembacaan teks. *Receiver* dapat melakukan penginputan audio yang telah disisip teks, kemudian password sebagai kunci. Audio yang telah disisip teks akan dibaca menggunakan metode *End Of File* (EOF), untuk mengeluarkan teks dalam audio. Teks dikeluarkan dari audio masih berbentuk *plainteks.*

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari hasil pengujian dan analisis yang dilakukan, maka diambil kesimpulan sebagai berikut:

1. Dapat diproteksi password dengan panjangnya tidak terbatas.
2. File yang ukurannya lebih kecil dapat menampung teks yang ukurannya lebih besar.
3. Kriptografi dengan menggunakan algoritma DES dengan memanfaatkan metode EOF dapat dilakukan dengan menyembunyikan hasil pesan teks yang telah di enkripsi ke dalam media audio
4. Hasil audio yang telah disisipkan pesan bertambah kapasitas menjadi lebih besar dari audio yang belum disisipkan pesan sebelumnya.

5.2. Saran

Beberapa saran untuk pengembangan program dan penelitian lebih lanjut adalah sebagai berikut:

1. Efisiensi dalam penyembunyian teks diharapkan dapat lebih ditingkatkan, dengan metode pengolahan audio yang lain sehingga dapat menyisipkan lebih banyak pesan tanpa mempengaruhi penampungnya.

ISSN : 2548 - 9739

2. Untuk Pengembangan lebih lanjut diharapkan dapat menambahkan sistem keamanan yang lebih baik lagi pada perangkat lunak ini.
3. Menggunakan penggabungan antara *kriptografi* dengan *steganografi* dalam proses penyembunyian pesan, sehingga dapat menghasilkan teks yang aman disisipkan dalam audio.
4. Perlu dilakukan penelitian lebih lanjut agar file yang telah disisip ini bisa tahan terhadap proses konversi format ke dalam format lainnya.
5. Implementasi perancangan sistem dapat diujicobakan menggunakan bahasa pemrograman visual selain,VB.net 2010 misal: Delphi 7.0, Visual C++, C# dan sebagainya dengan tambahan basis-data.

DAFTAR PUSTAKA

[1]. Binanto, I. 2010. *Media Digital*. Teknik Informatika Institut Teknologi Bandung.

[2]. Kurniawan, E. 2010. *Visual Studio 2011*. Penerbit Andi, Yogyakarta.

[3]. Lubis, S.B. 2013. *Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File (EOF).* Teknik Informatika Stmik Budidarma Medan**.**

[4]. Munir, R. 2006. *Kriptografi*, Penerbit Informatika, Bandung

[5]. Sadikin, R. 2012. *Kriptografi*. Penerbit Andi, Yogyakarta.

[6]. Fauzi, Achmad & Maulita, Yani. 2016. Analisis Hybrid Crytosystem Algoritma Elgamal dan Algoritma Triple DES.