PENGEMBANGAN SISTEM KEAMANAN INFORMASI MENGGUNAKAN METODE KRIPTOGRAFI 3DES DAN STEGANOGRAFI RANDOM BYTE POSITION ENCODING PADA AUDIO

Ely Setyo Astuti[1], Meyti Eka Apriyani[2], Mochamad Resa Qulyubi[3]

[1,2]Program Studi Teknologi Infomasi, Teknik Informatika, [3]Politeknik Negeri Malang
[1] nugelys2005@yahoo.com, [2] meyti24@gmail.com, [3]resaqulyubi@gmail.com

Abstrak

Salah satu upaya dalam menjamin keamanan dan keutuhan dari suatu data adalah proses penyandian. Sistem pengamanan pesan dapat dilakukan dengan menggunakan teknologi kriptografi. Selain itu, dikenal juga teknologi steganografi yang merupakan seni menyembunyikan pesan rahasia ke dalam suatu media sehingga tidak ada yang mengetahui atau menyadari selain pengirim dan penerima bahwa terdapat sebuah pesan rahasia.

Dalam skripsi ini, sebuah "Sistem Keamanan Informasi Menggunakan Metode Kriptografi 3DES dan Steganografi Random Byte Position Encoding pada Audio" dikembangkan dalam upaya menjamin keamanan dan keutuhan data. Implementasi steganografi akan disertai dengan penerapan kriptografi berupa enkripsi dan dekripsi. Teknik kriptografi yang akan digunakan adalah 3DES. Langkah pengamanan informasi dilakukan dengan enkripsi terhadap teks atau *image* terlebih dahulu menggunakan metode 3DES yang selanjutnya akan disisipkan menggunakan metode random byte posistion encoding. Hasil dari implementasi kriptografi dan steganografi ini mengandung *noise* yang terdengar secara langsung ketika media dijalankan di pemutar musik.

Hasil dari 28 kali pengujian pada proses penyisipan menghasilkan tingkat keberhasilan 86% dan kegagalan penyisipan 14% yang disebabkan oleh kapasitas audio. Pengujian mendapatkan analisa dari tingkat keberhasilan proses enkripsi dan proses dekripsi, kecepatan proses, perubahan audio, dan media pengiriman yang digunakan. Perubahan audio pada penyisipan gambar mendapat rentang pebedaan RMS volume antara sebelum dan sesudah penyisipan sebesar 0,01 dB hingga 3,02 dB. Metode Kriptografi 3DES dan Steganografi *Random Byte Position Encoding* disimpulkan dapat mengamankan dengan baik dan memberikan hasil dekripsi dengan kecocokan 100% dengan pesan asli.

Kata kunci : kriptografi, *random byte encoding*, *audio* steganografi

1. Pendahuluan

Popularitas dari media digital telah menyuarakan banyak keprihatinan yang serius kepada masalah keamanan yang terkait. Serangan keamanan maupun ancaman dalam bentuk eavesdropping, masquerading dan data manipulation maupun dalam bentuk gangguan lain yang umum terjadi saat ini Brenstein (2017). Pada abad ke-21 hampir setiap aktivitas, mulai dari aktivitas personal hingga pemerintahan bertumpu pada penggunaan teknologi informasi Budi (2017).

Kebutuhan atas keamanan informasi yang meningkat maka teknik kriptografi saja tidak cukup. Untuk menambah tingkat keamanan dalam sistem pengamanan informasi maka dibutuhkan kemanan lebih pada informasi. Data hiding adalah pelengkap untuk enkripsi (kriptografi). Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan Munir (2008), steganografi dan kriptografi akan berjalan bersama sehingga memberikan keamanan lebih pada data.

Data hiding merupakan salah satu teknik yang muncul dengan tujuan untuk memberikan kemanan dengan menyembunyikan informasi rahasia ke dalam media tertentu dengan mengubah beberapa komponen yang tidak penting pada cover file. Information hiding, Steganography, and Watermarking merupakan tiga bidang terkait yang memiliki banyak pendekatan teknis yang berbeda. Information hiding (data hiding) merupakan istilah umum yang mencakup berbagai masalah dalam lingkup embedding message ke dalam media tertentu. Steganografi adalah ilmu yang digunakan untuk menjaga keamanan dari pihak yang tidak memiliki hak akses terhadap suatu data baik berupa e-mail, dokumen, maupun berkas pribadi. Steganography berasal dari Stegos bahasa Yunani, yang berarti tertutup dan Graphia, yang berarti menulis, merupakan seni dan ilmu untuk menyembunyikan informasi kedalam informasi Vicky (2016).

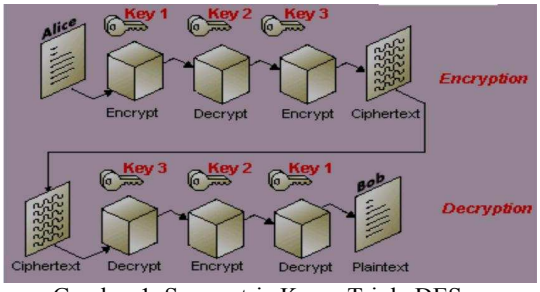
Sebagai informasi tertanam dengan sinyal, hal itu akan diubah tetapi modifikasi ini harus dibuat tak terlihat ke telinga manusia. objek digital lain seperti image, video juga dapat diambil tapi steganografi audio yang lebih berbeda karena fitur Human Auditory System (HAS) semakin besar daya,semakin lebar frekuensi audio dan jangkauan dengar Singh (2014). Namun, steganografi audio dianggap lebih sulit daripada steganografi gambar atau video karena Auditory Sistem Manusia (HAS) lebih sensitif dari Human Visual System (HVS). Untuk melakukan audio yang steganography berhasil, teknik yang diadopsi harus bekerja melawan HAS Anjaliraj (2014).

Pada penelitian sebelumnya yang berjudul "Implementasi Kriptografi dan Steganografi pada File Audio Menggunakan Metode DES dan Parity Coding" dilakukan oleh Yoga bagus perkhasa tahun 2012 telah berhasil dilakukan steganografi di media audio WAV Bagus, dkk (2012). Pada penelitian ini proses enkripsi yang dilakukan adalah metode DES. Selain metode DES pada penelitian ini ditambahkan dengan steganografi dengan metode Parity Coding. Hasil dari penelitian ini berupa audio yang didalamnya terdapat pesan rahasia. Penelitian ini terbukti berhasil dilakukan dengan sistem keamanan yang baik. Kualitas berkas audio yang dihasilkan tergantung dari besarnya ukuran pesan.

Oleh karena itu, Penelitian ini menggunakan algoritma kriptografi 3DES dan Metode steganografi random byte position encoding , sehingga dapat mengamankan informasi rahasia dengan lebih baik. 3DES (Triple Data Encryption Standard) dirancang dengan menggunakan key berukuran 168 bit, dan ukuran tersebut dirasa cukup untuk menjalankan teknik enkripsi yang aman.

2. Tinjauan Pustaka

Menurut R. A. Mollin Kriptologi terdiri dari enkripsi dan dekripsi, informasi asli disebut sebagai "plaintext", dan informasi dienkripsi sebagai "ciphertext". Untuk mengkonversi plaintext ke ciphertext perlu algoritma untuk menerapkan dan menggunakan kunci rahasia untuk jaminan keamanannya Barje (2013). Dengan prinsip bahwa metode kriptografi 2DES mungkin tidak cukup kuat untuk mencegah serangan telah menyebabkan perkembangan 3DES, yang dikembangkan pada tahun 1999 oleh IBM oleh tim yang dipimpin oleh Walter Tuchman Sobh, dkk (2008). Algoritma ini menyediakan solusi sederhana tanpa perlu menciptakan algoritma yang baru, yaitu menjalankan Algoritma DES (Data Encryption Standard) sebanyak 3 kali untuk masing-masing blok data.



Gambar 1. Symmetric Key – Triple DES

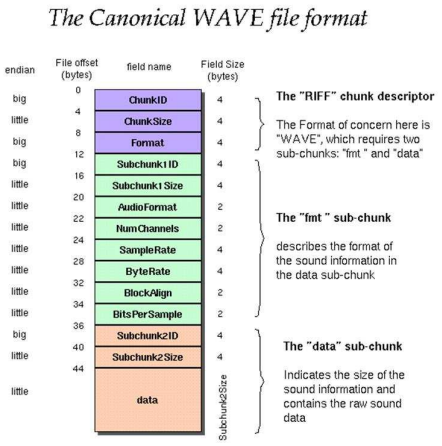
Informasi yang telah terenkripsi kemudian disisipkan kedalam Cover file berupa audio dengan steganografi bermetode random byte position encoding. penyisipan informasi rahasia dilakukan secara acak . Untuk melakukan penyisipan secara acak, bit-bit data rahasia tidak disisipkan dengan mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak.

2.1 Audio Steganografi

Seperti pada dokumen berupa gambar, file suara juga dapat dimodifikasi sedemikian rupa mereka Mengandung informasi dapat tersembunyi. Modifikasi tersebut harus dilakukan sedemikian rupa sehingga orang yang tidak berkepentingan tidak mungkin untuk menghapusnya, setidaknya tidak dapat tanpa merusak sinyal asli. Metode menyisipkan data dalam file suara menggunakan Sifat dari Human Auditory System (HAS). Sifat pada steganografi audio Barje (2013):

1. Confidentiality (kerahasiaan).
2. Imperceptibility (tak terlihat).
3. Accurateness (akurasi).
4. High capacity (penyimpanan tinggi).
5. Resistance (perlawanan).
6. Visibility (visibilitas).
7. Survivability (ketahanan).
8. Difficult detectability(pendektesian sulit).

Steganografi audio menjadi pendekatan yang lebih sulit untuk ditangani daripada steganografi gambar Karena sistem pendengaran manusia (Human Auditory system) lebih sensitif daripada sistem penglihatan manusia(Human visual system). Pada penyisipan pesan rahasia pada audio harus sesuai dengat format audio , seperti pada .wave (memiliki header pada 44 byte pertama) header tidak boleh disentuh karena dapat menyebabkan corrupted pada file audio, format wave seperti pada gambar berikut Karthik (2014):



Gambar 2. Wave File Format

2.2 Triple DES atau 3DES

Serangan merupakan Alasan utama mengapa 2DES digantikan oleh Triple DES atau 3DES, yang mana DES dengan tiga kunci yang berbeda. Hal ini penting untuk menghindari kunci yang sama untuk langkah-langkah enkripsi sejak output hanya akan menjadi versi yang lebih lambat dari DES. 3DES memiliki dua bentuk, satu membutuhkan tiga kunci yang sama sekali berbeda dan yang lainnya hanya ,,membutuhkan dua kunci yang berbeda. Metode pertama menggunakan tiga kunci untuk mengenkripsi *plaintext*, pertama menggunakan k1 kunci, diikuti dengan enkripsi dengan k2 kunci, dan terakhir enkripsi ketiga dilakukan dengan k3 kunci. Kita melakukan operasi C = EK3 (EK2 (EK1 (P))) untuk mengenkripsi *plaintext* dan P = DK3 (DK2 (DK1 (C))) untuk dekripsi. Meskipun 3DES menggunakan tiga kunci untuk memberikan keamanan tingkat tinggi, masih memiliki kelemahan sejak diperlukan 56 * 3 = 168 bit untuk kunci, yang dapat membuat pekerjaan lebih sulit dalam situasi praktis.

2.3 Teknik steganografi dengan Random Byte Position Encoding

Melalui prinsip dari steganografi LSB, dengan pengembangan keamanan lebih terjaga dilakukan pengacakan pada penyisipan file audio. Pola pengacakan yang digunakan dalam desain ini adalah dua kali lipat langkah pertama dari byte yang diketahui dan menjadi sampel penyisipan dilangkah kedua. Dengan cara ini *robustness* akan meningkat Barje (2013) . Algoritma adalah sebagai berikut:

Iterasi ke-1

- K = adalah ukuran file pesan
- $S_1 = K + 60$
- T_1 = total dari hasil penjumlahan dari tiap digit dari S_1
- $Q_1 = T_1 \% 8$

Jadi bit pertama dari pesan yang disisipkan berada di blok ke-S_1 , kemudian pesan disubtitusi di posisi bit ke-Q_1 dari 8 bit dari blok ke-S_1

, Keterangan notasi :

- K = adalah ukuran file pesan yang disisipkan (contoh: 144 byte)
- T_i = total dari hasil penjumlahan dari tiap digit dari S_i
- S_i = blok tempat pesan yang disisipkan
- Q_i = posisi ke- Q_i bit dari 8 bit

Jadi Iterasi ke- i+1 seperti berikut :

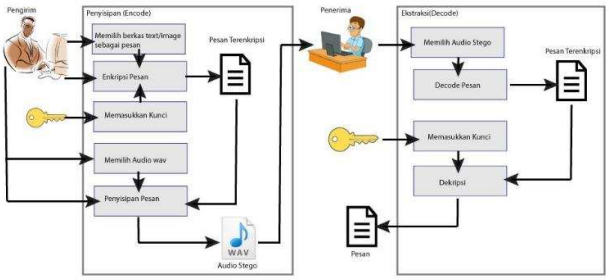
- $S_{i+1} = S_i + Q_i$
- $S_i = S_{i+1}$
- T_i = total dari hasil penjumlahan dari tiap digit dari S_i
- $Q_{i+1} = T_i \% 8$
- $Q_i = Q_{i+1}$

Jadi bit pertama dari pesan yang disisipkan berada di blok ke-S_i , kemudian pesan disubtitusi di posisi bit ke-Q_i dari 8 bit dari blok ke-S_i.

3. Perancangan dan Implementasi

3.1 Gambaran Umum Sistem

Aplikasi ini menggunakan algoritma 3DES untuk proses enkripsi dan dekripsi dengan penggabungan proses algoritma DES sebanyak tiga kali sebagai keamanan terhadap informasi yang akan disisipkan. Sedangkan metode steganografi yang digunakan yaitu metode Random Byte Encoding untuk proses encoding dan decoding pesan. Tahapan-tahapan yang dilakukan pada setiap prosesnya yaitu sebagai berikut:



Gambar 3. Gambaran Umum Aplikasi

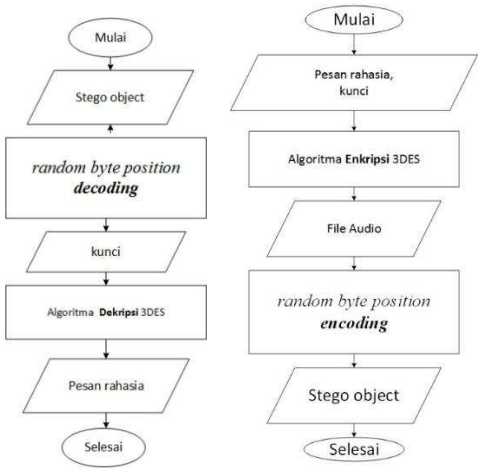
Keterangan gambar dapat dijelaskan sebagai berikut :

1. Proses Penyisipan(encoding)
   a. Pengirim memilih file pesan yang serta memberikan kunci.
   b. Pengirim melakukan enkripsi terhadap pesan menggunakan algoritma 3DES.
   c. Pengirim memilih file audio wav yang akan digunakan sebagai media penampung dari pesan.
   d. Pengirim melakukan proses penyisipan menggunakan metode Random Byte Encoding.

2. Proses Ekstraksi (Decoding)
   a. Penerima memilih file audio wav yang telah disisipkan pesan (stego object)
   b. Penerima melakukan proses ekstraksi menggunakan metode Random byte encoding.
   c. Penerima melakukan dekripsi terhadap pesan menggunakan 3DES.
   d. Penerima menyimpan pesan yang telah diekstraksi dari audio.

3.2 Flow Chart Aplikasi

Flow chart telah dikenal dan umum digunakan untuk menggambarkan alur proses atau langkah-langkah secara berurutan. Flowchart dari sistem diperlihatkan oleh Gambar 4:



Gambar 4. (Kiri) Proses Enkripsi Dan Encoding ,(Kanan) Prosen Decoding Dan Dekripsi

Pada Sistem Terdapat 4 lapisan :

- Enkripsi (proses penyandian pesan rahasia : plaintext menjadi ciphertext)
- Encoding (Proses steganografi untuk menyisipkan pesan pada file audio)
- Decoding (proses pengambilan pesan rahasia dari file audio)
- Dekripsi (proses ciphertext menjadi plaintext)

4. Hasil Pengujian

Dari uji coba yang telah dilakukan menggunakan 4 audio diital yang menggunakan 4 fil teks dalam melakukan proses enkripsi hasil yang didapatkan adalah perubahan pesan ke bentuk yang tidak dapat diartikan atau *chipertext* sebagai berikut :

Tabel 1. Enkripsi *Plaintext*

NO	Chipertext	Plaintext	Kunci 3DES	Kunci Stego
1	068b50430c916f3c	POLINEMA	polinemapolinemapolinema	8
2	edaf4cb39406739bd3d58a280e1ebfe961264483eb4968e64c14b8a9306693...	saya masuk polinema pada tahun 2013, di ...	TI Polinema 2013 Skripsi	136

Dari data tersebut, *ciphertext* yang dihasilkan disisipkan ke dalam gambar yang telah dipilih dengan rincian sebagai berikut:

Tabel 2. Hasil Penyisipan Atau Encode

No	Nama Audio	ukuran	Pesan Teks	Ukuran	Waktu Proses enkripsi/encode	Waktu Proses dekripsi/decode
1	Marimba.wav	4032994	Polinema.txt	8	0:0:0:4/0:0:4:519	0:0:0:200/0:0:1:117
			Saya.txt	136	0:0:2:208/0:0:44:371	0:0:2:194/0:0:6:984
2	shakuhachi.wav	4648352	Polinema.txt	8	0:0:0:5/0:0:3:898	0:0:0:200/0:0:0:135
			Saya.txt	136	0:0:2:225/0:0:38:848	0:0:1:134/0:0:7:2
3	gtr-nylon22.wav	220972	Polinema.txt	8	0:0:0:4/0:0:1:534	0:0:0:200/0:0:0:351
			Saya.txt	136	0:0:2:226/0:0:29:157	0:0:1:423/0:0:6:12
4	gtr-jaz-2.wav	1870348	Saya.txt	136	0:0:2:233/0:0:33:55	0:0:2:183/0:0:6:784
			nevrquit.txt	8	0:0:0:3/0:0:2:389	0:0:0:182/0:0:1:122

*ukuran dalam byte

Dari tabel waktu diatas dapat disimpulkan menggunakan grafik yang dilihat pada Gambar 5 dan 6 berikut:

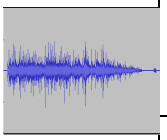
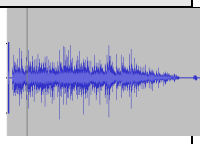
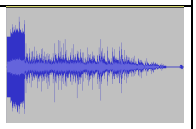
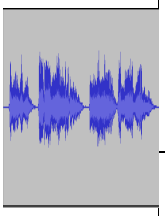
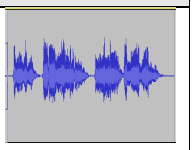
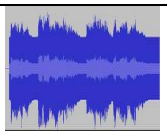
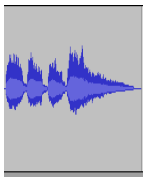
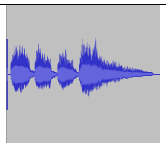
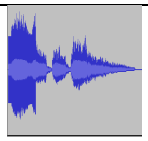
Gambar 5. Kecepatan Enkripsi Dan Dekripsi Berdasarkan Ukuran Pesan

Kecepatan enkripsi dan dekripsi bergantung pada ukuran pesan yang di proses. Semakin besar pesan teks atau gambar, maka proses akan semakin lambat.Begitu juga dengan penyisipan dilihat dari Gambar 6.

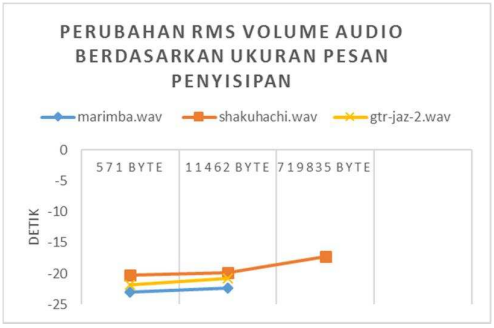
Gambar 6. Kecepatan Penyisipan Dan Ekstraksi

Perbandingan audio sebelum proses enkripsi dan penyisipan (*cover-audio*) dengan audio setelah proses enkripsi dan penyisipan (*stego-audio*) sebagai berikut :

Tabel 3. Perbandingan Audio Asli Dan Audio Stego

No	Gelombang Audio asli/durasi/*RMS Volume*/Ukuran file	Ukuran Pesan	Gelombang Audio Stego/durasi/ *RMS Volume*/ukuran file
1.	marimba.wav  00:00:21 /(-23.05 dB)/ 4032994 byte	571 byte	 00:00:21 /(-23.02 dB)/ 4032994 byte
		11462 byte	 00:00:21 / (-22.32 dB)/ 4032994 byte
2	shakuhachi.wav  00:00:24 /(-20.24 dB) /4648352 byte	571 byte	 00:00:24 /(-20.23 dB)/ 4648352 byte
		134921 byte	 00:00:24 /(-17.22 dB)/ 4648352 byte
3	gtr-jaz-2.wav  00:00:09 / (-21.91 dB) 1870348 bytes	571 byte	 00:00:09 / (-21.86 dB)/ 1870348 bytes
		11462 byte	 00:00:09 (-20.73 dB)/ 1870348 bytes

Perubahan gelombang audio pada penyisipan pesan bergantung pada ukuran pesan yang disisipkan beserta presentase penggunaan audio yang dipakai untuk melakukan penyisipan. Semakin besar byte pesan yang disisipkan, dilihat dari Gambar 7.



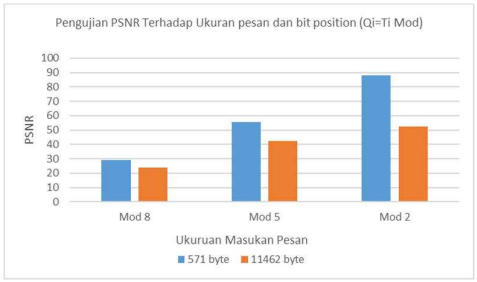
Gambar 7. Grafik Perubahan RMS Volume Tehadap Ukuran Pesan

Semakin besar perbedaan RMS Volume nya. Hal ini terlihat pada tabel 6.13 pada kolom difference RMS Volume dengan memperhatikan pada file uji nomor 2 dengan disisipkan pesan 134921 byte mendapat rentang 3.02 dB RMS Volume, yang berawal -20.24 dB menjadi -17.22 dB.

Tabel 4. Pengujian PSNR dengan Qi =Ti Mod 2

No	Audio Wav asli	Pesan masukan	Hasil objek Steganografi	Pengujian	
				Subjektif	PSNR
1	gtr-jaz-2.wav (1.870.348 byte) (-24,5750398 dB)	8 byte	(1.870.348 byte) (-24,9387451dB)	baik	36,72249969 db
		11462 byte	(1.870.348 byte)(-24,51512812 dB)	baik	52,23845214 dB
2	gtr-nylon22.wav (220.972 byte) (-29,0526864 dB)	8 byte	(220.972 byte) (-29,05268641 dB)	baik	Tidak bisa dihitung
		571 byte	(220.972 byte) (-29,051514 dB)	baik	87,88179213 dB

Pengukuran noise pada objek steganografi dilakukan dengan menggunakan PSNR (*Peak Signal to Noise Ratio*). Noise ini dapat di dengar secara langsung ketika media objek steganografi di jalankan di pemutar musik. Secara matematis perhitungan noise akan memakai perhitungan nilai PSNR dengan nilai minimal 30 DB. Nilai PSNR ini sendiri dipengaruhi oleh dua hal yaitu besarnya pesan yang disembunyikan dan bit letak (Qi=Ti Mod) penyisipan pesan pada media steganografi yang dapat dilihat pada Gambar grafik 8.



Gambar 8. Grafik Pengujian PSNR Terhadap Ukuran Pesan Dan Bit Position

Semakin besar nilai PSNR media maka semakin baik pula kualitas audio tersebut secara subjektif. Jika nilai PSNR yang didapat lebih kecil dari 30 dB maka akan terdengar noise yang sangat jelas terdengar oleh telinga manusia.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Kemanan data sangat penting untuk melindungi konten pada data yang terkait. Tingkat keberhasilan dari 28 kali pengujian penyisipan mendapat keberhasilan program 86% dan tingkat kegagalan program 14%. Berdasarkan pengujian penyisipan pesan menghasilkan rata-rata pesan yang dapat tersisipkan dengan metode random byte encoding sebesar 2,86% dari ukuran file audio.

Proses enkripsi dan dekripsi menggunakan metode 3DES dinyatakan berhasil dengan kecocokan pesan teks dan gambar sebelum enkripsi dengan pesan yang telah terdekripsi dengan presentase keberhasilan sebesar 100% pada analisa yang dilakukan.

Pada Pengujian nilai PSNR menunjukkan bahwa nilai PSNR cenderung menurun seiring dengan bertambahnya ukuran pesan yang disembunyikan. Jika ukuran pesan yang disembunyikan semakin besar maka nilai PSNR semakin kecil yang berarti kualitas berkas audio yang disisipkan semakin buruk Semakin besar ukuran pesan yang disipkan pada audio, maka menimbulkan perubahan yang semakin besar pada audio. Hal tersebut berpengaruh pada perubahan amplitudo yang semakin menghasilkan noise. berdasarkan Uji coba perubahan audio pada penyisipan gambar mendapat rentang pebedaan RMS volume antara sebelum dan sesudah penyisipan sebesar 0.01 dB hingga 3,02 dB.

Waktu proses yang dibutuhkan sesuai dengan ukuran teks atau gambar yang digunakan, semakin besar ukuran pesan yang disisipkan pada audio semakin lama juga waktu yang dibutuhkan

alam proses enkripsi dan penyisipan atau encode maupun proses dekripsi dan ekstraksi atau decode.

5.1 Saran

Untuk Pengembangan selanjutnya aplikasi yang lebih kompleks digunakan untuk instansi yang membutuhkan keamanan pada digital. Selanjutnya dapat menggunakan algoritma penyisipan yang tidak merubah amplitudo dari audio.

Pegembangan dapat selanjutnya dapat meggunakan metode kunci public untuk proses enkripsi dan dekripsi. Dapat mencoba penyisipan pada file dengan bertipe lain , seperti tipe dokumen (pdf,doc,xls ,dsb)

Daftar Pustaka:

Bernstein et.al, (2017), "*Ancaman terhadap Penggunaan Internet*" , [Online], Tersedia: http://kahfiehudson.com/jenis-jenisancaman-threats-melalui-it-dan-kasuskasuscy berc rime-lainnya/ diakses pada tanggal 5 januari 2017 pada pukul 05.55 wib

Prof. Dr. Ir. Budi Susilo Soepandji, (2017),"*Pemanfaatan Teknologi Informasi Dalam Perspektif Ketahanan Nasional*", [Online], Tersedia:http://www.pusakaindonesia.org/pemanfaatan-teknologi-informasi-dalam-perspektif - ketahanan-nasional/ diakses pada tanggal 5 januari 2017 pada pukul 04.30 wib.

Munir, Rinaldi, (2008), *Kriptografi*. Jakarta: Penerbit Informatika.

Vicky, Bonifacus, (2016), "*Implementasi Sistem keamanan file dengan metode Steganografi EOF dan Ekripsi Caesar cipher*", Jurnal Sisfo Vol.06 No.01 1-16.

Singh, Kamred udham, (2014), "*LSB Audio Steganograpy Approach*" . [Online], Tersedia : www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014).

Anjaliraj. Dhanya, (2014), "*Three Layered Model for Audio Steganography for Secured Data Transfer*" . International Journal of Engineering Research & Technology (IJERT).

Bagus, Yoga., Suadi, Wahyu., Adi, Baskoro, (2012), "*Implementasi Kriptografi dan Steganografi pada Audio Menggunakan Metode DES dan Parity Coding*". Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember.

Barje, Lovey Rana, (2013), "*Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding*".International Journal of Engineering and Innovative Technology (IJEIT).

R. A. Mollin, (2005), "*Codes: The Guide To Secrecy From Ancient To Modern Times*", Chapman and Hall/CRC, Boca Raton.

S,Karthik .A,M Muruganandam, (2014), "*Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System*". International Journal of Scientific Engineering and Research (IJSER) www.ijser.in. Volume 2

T. Sobh, K. Elleithy and A. Mahmood, (2008), "*Novel Algorithms and Techniques In Telecommunications*", Automation and Industrial Electronics. Springer Science+ Business Media B. V., Bridgeport.