Enhanced Audio Steganografi dengan Algoritma *Advanced Encryption Standard* Untuk Pengamanan Data Pada File Audio

Ida Bagus Adisimakrisna Peling[1], Nyoman Putra Sastra[2]

***Abstract*— Ease of accessing and delivering information makes the Internet more and more needed. But the ease also provides greater opportunities for leaking of information that is confidential. To handle the security of information exchange that is confidential then developed the method of data security on audio using AES (Advanced Encryption Standard) and EAS (Enhanced Audio Steganography) algorithm.**

From the research results can be concluded by using AES method as cryptography and EAS as steganography, audio file quality can be said good because of the overall test scenario conducted the lowest SNR value obtained is 49.33dB while the highest SNR value is 51.10dB.

***Keywords*— AES (*Advanced Encryption Standard*), EAS (*Enhanced Audio Steganography*), SNR (*Signal to Noise Ratio*), Cryptography, Audio**

***Intisari*—Kemudahan pengaksesan dan penyampaian informasi membuat internet semakin dibutuhkan. Namun kemudahan tersebut juga memberikan peluang lebih besar untuk bocornya suatu informasi yang sifatnya rahasia. Untuk menangani keamanan pertukaran informasi yang sifatnya rahasia maka dikembangkanlah metode pengamanan data pada audio menggunakan algoritma AES (*Advanced Encryption Standard*) dan EAS (*Enhanced Audio Steganography*). Dari hasil penelitian dapat diperoleh hasil bahwa dengan menggunakan metode AES sebagai kriptografi dan EAS sebagai steganografi menghasilkan kualitas file audio yang baik karena dari keseluruhan skenario pengujian yang dilakukan nilai SNR terendah yang didapat adalah 49,33 dB sedangkan nilai SNR tertinggi adalah 51,10 dB.**

***Kata Kunci*— AES (*Advanced Encryption Standard*), EAS (*Enhanced Audio Steganography*), SNR (*Signal to Noise Ratio*), Kriptografi, Audio.**

I. PENDAHULUAN

Teknologi informasi saat ini berkembang dengan sangat pesat, hal tersebut dibuktikan dengan dibutuhkannya dan berkembangnya media internet sebagai media informasi. Kemudahan pengaksesan dan penyampaian informasi membuat internet semakin dibutuhkan. Namun kemudahan tersebut juga memberikan peluang lebih besar untuk bocornya suatu informasi yang sifatnya rahasia.

Untuk menangani keamanan pertukaran informasi yang sifatnya rahasia maka dikembangkanlah metode pengamanan data pada audio menggunakan algoritma AES (*Advanced Encryption Standard*) dan steganografi EAS (*Enhanced Audio Steganography*) yang merupakan suatu metode untuk menyisipkan suatu pesan yang di enkripsi terlebih dahulu untuk memperkuat pesan rahasia dan kemudian disisipkan ke dalam file audio.

Enkripsi yang dilakukan pada pesan menggunakan algoritma AES (*Advanced Encryption Standard*) karena algoritma ini memiliki tingkat pengamanan yang tinggi. Untuk proses steganografi pada file audio dapat dilakukan dengan banyak cara salah satunya dengan menggunakan metode LSB (*Least Significant Bit*) Dimana pada metode ini proses penyisipan dilakukan pada *bit* paling belakang dengan mengganti *bit* audio degan *bit* pesan. Proses tersebut dilakukan secara berurutan hingga semua *bit* pesan tersisipkan [1].

Namun, memodifikasi *bit* file audio secara berurutan dapat membuat *noise* yang besar dan mengundang kecurigaan bagi orang lain bahwa ada pesan yang tersisipkan didalamnya. Metode yang mampu mengurangi terjadinya *noise* pada file audio setelah disisipkan pesan adalah metode EAS (*Enhanced Audio Steganography*). Metode EAS merupakan modifikasi dari metode LSB. Dimana pada metode EAS, byte yang digunakan sebagai penampung hanya selective byte saja, yaitu penyisipan *bit* pada media penampung hanya dilakukan pada blok yang bernilai 254 atau 255 byte saja, sehingga media penampung tidak akan mengalami kerusakan yang signifikan [2].

File audio dengan format .wav yang digunakan sebagai media penampung karena file audio dengan format .wav tidak terkompresi dan memiliki kualitas suara yang baik, jadi ketika terjadi perubahan pada file audio tersebut tidak akan menimbulkan derau sehingga tidak mengundang kecurigaan.

Penelitian ini dilakukan untuk mengetahui kualitas file audio setelah disisipkan pesan yang terenkripsi dengan menggunakan metode steganografi EAS dan untuk mengetahui integritas data setelah dilakukan proses kriptografi dan steganografi.

II. STUDI LITERATUR

Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security, penelitian yang dilakukan oleh R. Sridevi, tahun 2009. Dilatar belakangi oleh perkembangan media internet yang sangat pesat membuat transfer data yang aman menjadi terbatas karena juga memberikan peluang yang besar untuk bocornya data. Salah satu solusi untuk mengatasinya adalah dengan Steganografi audio. Namun, sistem steganografi audio yang ada memiliki antarmuka yang buruk, penerapannya sangat rendah, sulit dipahami dan hanya berlaku untuk format audio tertentu dengan ukuran pesan terbatas. Enhanced Audio Steganography (EAS) adalah salah satu metode yang

[1]*Magister Teknik Elektro, Universitas Udayana Kampus Sudirman, Denpasar-Bali (tlp: 0361-239559; fax: 0361-239599; e-mail: adi.peling@gmail.com)*

[2]*Magister Teknik Elektro, Universitas Udayana Kampus Sudirman, Denpasar-Bali (tlp: 0361-239559; fax: 0361-239599; e-mail: putra.sastra@unud..ac.id)*

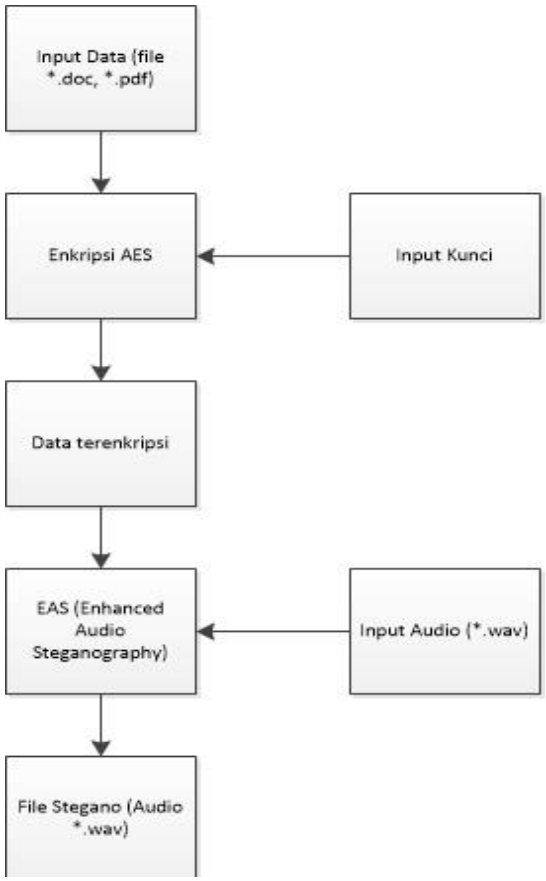
diusulkan berdasarkan Steganografi audio dan kriptografi, dipastikan transfer data yang dilakukan aman antara sumber dan tujuan. EAS merupakan algoritma enkripsi paling kuat yang sangat kompleks untuk dipecahkan. Menggunakan algoritma LSB (Least Significant Bit) yang dimodifikasi untuk mengkodekan pesan ke dalam audio. Dilakukan manipulasi tingkat bit untuk mengkodekan pesan. Ide dibalik penelitian ini adalah memberikan metode yang baik dan efisien untuk menyembunyikan data dari hacker dan dikirim ke tempat tujuan secara lebih aman. Kualitas suara tergantung pada ukuran audio yang pengguna pilih dan panjang pesannya. Meskipun menunjukkan penyimpangan tingkat bit pada bagan frekuensi, secara keseluruhan perubahan audio tidak dapat dibedakan [2].

Enkripsi Dan Dekripsi Dengan Algoritma AES 256 Untuk Semua Jenis File, penelitian yang dilakukan oleh Yuniat, tahun 2011. Kriptografi merupakan salah satu solusi atau metode pengamanan data yang tepat untuk menjaga kerahasiaan dan keaslian data, serta dapat meningkatkan aspek keamanan suatu data atau informasi. Metode ini bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau Internet, tidak dapat diketahui atau dimanfaatkan oleh orang atau pihak yang tidak berkepentingan. Kriptografi mendukung kebutuhan dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan. Hasil penelitian menunjukkan bahwa algoritma AES dengan panjang kunci 256 bit dapat menyandikan isi suatu file sehingga dapat mengamankan file tersebut. Ukuran file enkripsi akan bertambah 11 bytes dari file asli karena adanya proses penambahan header yang berisi informasi ekstensi file. Dalam pengembangan sistem berikutnya diharapkan sistem dapat mempunyai fasilitas untuk menyembunyikan folder yang digunakan untuk menyimpan file enkripsi maupun file dekripsi [6].

Pada penelitian yang akan dilakukan adalah mengkombinasikan antara metode steganografi dengan metode kriptografi untuk meningkatkan keamanan suatu data atau informasi. Dimana metode steganografi yang digunakan adalah EAS yang merupakan metode LSB yang dimodifikasi dengan mengganti bit LSB pada byte-byte audio yang bernilai 254 atau 255, dan metode kriptografi menggunakan metode AES.

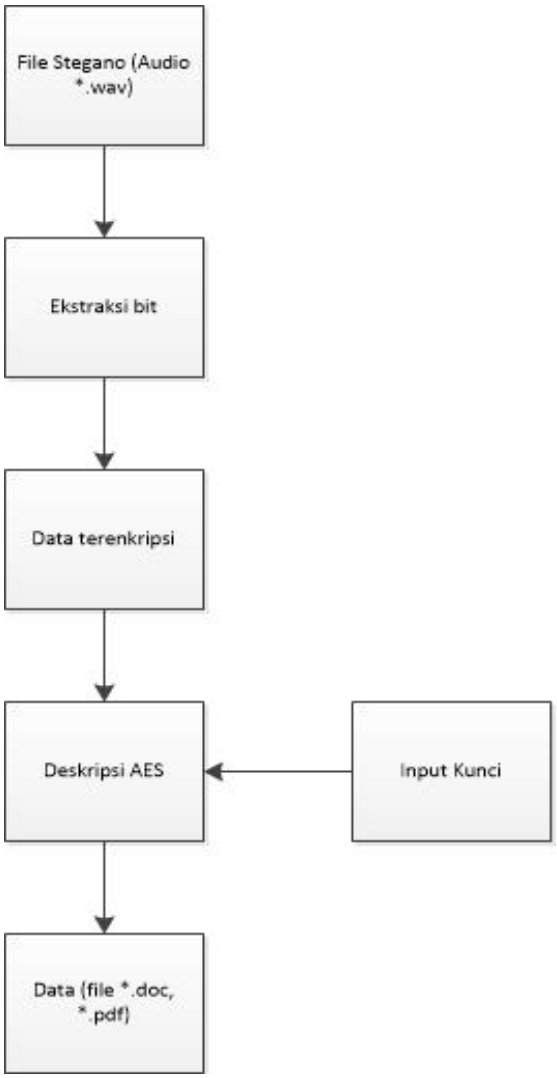
III. DESAIN SISTEM

Penelitian ini akan mengimplementasikan Steganografi dengan pesan yang telah terenkripsi, sesuai dengan diagram blok pada Gambar 1. File audio dengan format WAVE digunakan sebagai media penampungan (*cover text*). Untuk dapat menyisipkan pesan rahasia ke dalam media penampung membutuhkan sebuah metode yang dapat memodifikasikan objek menjadi objek yang baru dengan informasi rahasia di dalamnya tanpa terjadi perubahan yang mencolok dari objek awal. Metode yang digunakan dalam penelitian ini adalah metode EAS (Enhanced Audio Steganography) dan untuk mengenkripsi pesan digunakan algoritma AES.



Gambar 1 : Blok Diagram Proses Encode

Gambar 1, menunjukkan proses encode yang akan dilakukan yaitu, Pertama input pesan yang berformat *.doc atau *.pdf, akan dienkripsi menggunakan algoritma AES, proses enkripsi diawali dengan menginputkan plaintext dan kunci. Setelah pesan terenkripsi selanjutnya proses embedding menggunakan metode EAS. Input file audio yang akan digunakan sebagai penampung, setelah itu file yang sudah terenkripsi akan disisipkan pada file audio. Pada proses embedding dilakukan hitung besar lokasi yang tersedia pada file audio. File audio yang digunakan sebagai media penampung harus memiliki jumlah byte bernilai 254 atau 255 yang cukup untuk menampung file pesan. Kemudian penyisipan bit file pesan di LSB byte file media penampung. Proses ini bersifat selektif karena penyisipan hanya dilakukan pada byte file media penampung yang bernilai 254 atau 255 saja. Selanjutnya pembacaan diteruskan lagi ke byte berikutnya. Proses tersebut diulangi sampai semua bit file pesan selesai disisipkan. Setelah proses selesai, file audio disimpan sebagai file baru.

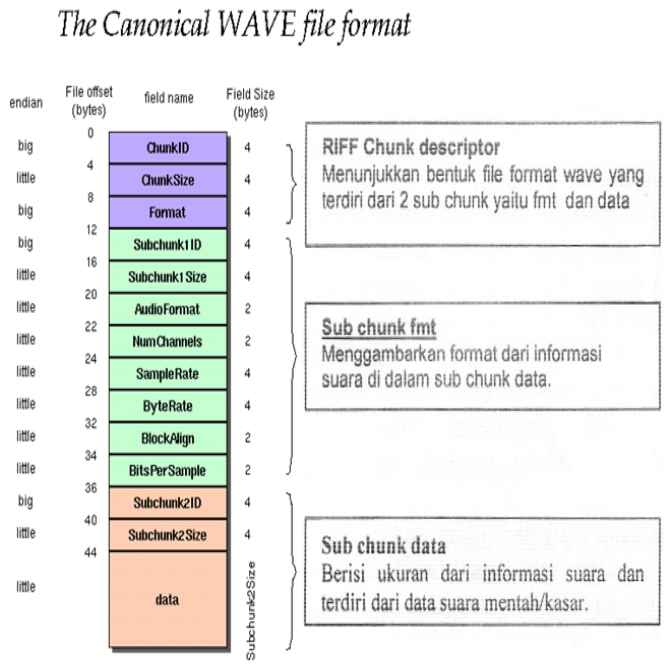


Gambar 2 : Blok Diagram Proses Decode

Gambar 2 menjelaskan tentang proses decode yang merupakan proses untuk membaca pesan di dalam file audio. Ketika file audio dimasukkan, sistem akan membaca apakah ada data yang disisipkan atau tidak. Sistem akan membaca panjang data yang disisipkan di dalam byte file audio dan mengecek apakah byte tersebut bernilai 254 atau 255. Setelah itu pesan akan diekstrak sesuai dengan informasi panjang pesan dengan membaca bit terakhir (LSB) dan disimpan ke penampung pesan. Proses ini akan diulangi hingga semua bit selesai terbaca. Pesan yang didapatkan kemudian akan dideskripsi, dan disimpan sebagai file baru.

A. *WAVE*

File WAVE yang digunakan sebagai penampung dari data yang disembunyikan memiliki struktur data yang ditunjukkan pada Gambar 2.



Gambar 3 : Struktur File WAVE

Dari Gambar 3, dapat diketahui bahwa sebuah file WAVE secara umum terdiri dari tiga bagian dasar, yaitu (1) deskripsi chunk RIFF, (2) format *subchunk* dan (3) data *sub-chunk*.

B. *Steganografi dengan Metode EAS*

Terdapat dua komponen penting pada steganografi, yaitu pesan yang akan disisipkan (Hidden text) dan media penampung (Cover text). Media yang digunakan sebagai penampung dapat berupa berkas digital termasuk multimedia seperti citra, audio, atau video [3]. Penelitian ini akan menggunakan media penampung (format) dan hidden text (format).

Untuk menghindari kerusakan yang signifikan pada cover-object, metode EAS (Enhanced Audio Steganography) dapat digunakan untuk menyembunyikasn pesan. Metode EAS merupakan modifikasi dari metode LSB. Modifikasi yang dilakukan adalah dengan mengganti bit LSB pada byte-byte yang telah ditentukan. Jadi proses encoding hanya dilakukan pada byte audio yang bernilai 254 atau 255. EAS memiliki keunggulan dibandingkan dengan teknik LSB pada umumnya, yaitu byte yang digunakan sebagai penampung hanya selective byte saja, maka media penampung yang digunakan akan mengalami kerusakan yang kecil [2].

Untuk ilustrasi proses penyisipan pesan ke dalam file audio dengan menggunakan metode ini. Jika diperoleh byte audio dengan susunan sebagai berikut:

255	254	10	250
160	100	255	255

Maka sebagai contoh, dapat disisipkan lima bit pertama 0011. Setelah proses penyisipan, hasilnya sebagai berikut:

nilai *byte*	**255**	**254**	10	250
binary	**11111111**	**11111110**	00001010	11111010
sisip	**0**	**0**		
hasil sisip	**11111110**	**11111110**	00001010	11111010
nilai *byte*	160	100	**255**	**255**
binary	10100000	01100100	**11111111**	**11111111**
sisip			**1**	**1**
hasil sisip	10100000	01100100	**11111111**	**11111111**

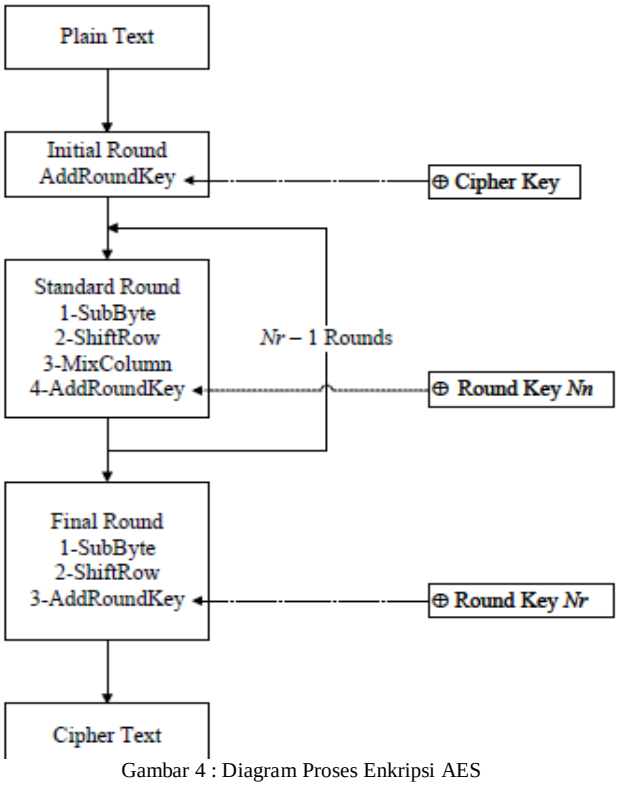
Hasil akhir penyisipan:

254	254	10	250
160	100	255	255

Dari 8 byte tersebut terdapat perubahan satu byte, yaitu pada blok pertama dari 255 menjadi 254 byte.

C. Kriptografi dengan Algoritma AES

Algoritma AES adalah algoritma enkripsi cipher blok dengan kunci simetris yang terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi cipherteks. Kunci cipher dari AES terdiri dari kunci dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah putaran (round) yang akan diimplementasikan pada algoritma AES ini [6].



Gambar 4 : Diagram Proses Enkripsi AES

a. SubBytes

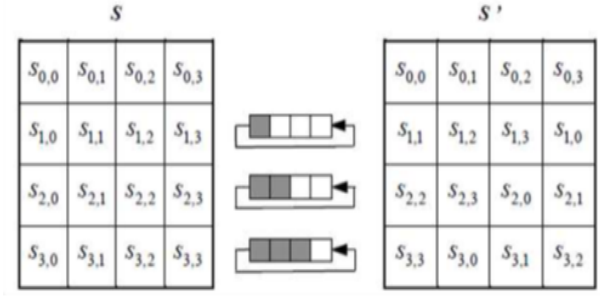
Transformasi SubBytes() memetakan setiap byte dari array state dengan menggunakan tabel substitusi S-box yang ditunjukkan oleh Gambar 5.

x \ y	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 5 : Tabel S-Box

b. ShiftRows

Transformasi ShiftRows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit). Proses pergeseran ShiftRow ditunjukkan dalam Gambar 6 berikut:



Gambar 6 : Transformasi ShiftRows

c. MixColumns

MixColumns mengoperasikan setiap elemen yang berada dalam satu kolom pada state. Secara lebih jelas, transformasi MixColumns dapat dilihat pada perkalian matriks berikut ini:

$$\begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

Gambar 7 : Transformasi MixColumns

d. AddRoundkey

Transformasi yang paling penting adalah transformasi yang melibatkan kunci cipher. Jika kunci cipher tidak ditambahkan pada state di setiap putaran, maka akan sangat mudah bagi kriptanalis untuk mendapatkan plaintext. AES menggunakan mekanisme ekspansi kunci yang memberikan Nr+1 kunci putaran dari kunci cipher.

D. SNR (Signal to Noise Ratio)

SNR merupakan suatu parameter yang umum digunakan untuk mengukur berbagai aplikasi pengolahan sinyal digital. SNR ini digunakan untuk mengukur kualitas sinyal dengan cara menghitung perbandingan sinyal asli dengan tingkat *noise* yang dihasilkan [6]. Nilai SNR dapat dihitung menggunakan persamaan (1)

$$SNR = 10^{*}\log_{10}\left[\frac{\sum_{i=0}^{n} f^2(n)}{\sum_{i=0}^{n}(g(n)-f^2(n))^2}\right] \quad \text{.....(1)}$$

Dari rumus diatas, f(n) merupakan sample audio asli dan g(n) merupakan sample audio tersteganografi. Kualitas *stegofile* dapat dikatakan baik apabila nilai SNR diatas 20 dB (nilai standar distorted file). Jadi semakin tinggi nilai SNR maka kualitas berkas audio dikatakan bagus sebab ratio sinyal terhadap derau semakin tinggi [7].

TABEL I

PENGUJIAN INTEGRITAS DATA

Stegofile	Pesan	MD5 Pesan (sebelum)	MD5 Pesan (sesudah)	Kesimpulan
audio1 (3.246MB)	Uji1.pdf (21KB)	7BA1820995BCB295050FFD40EE0C2FBF	7BA1820995BCB295050FFD40EE0C2FBF	Sukses
audio1 (3.246MB)	Uji2.pdf (38KB)	69363D1588CD4C9E5753E6518E7CB084	69363D1588CD4C9E5753E6518E7CB084	Sukses
audio2 (4.746MB)	Uji3.pdf (49KB)	F6106041FD63DF73AF9A341B3AF29805	F6106041FD63DF73AF9A341B3AF29805	Sukses
audio2 (4.746MB)	Uji4.pdf (81KB)	4782BED742B4F2CA8B912D75FEC0278F	4782BED742B4F2CA8B912D75FEC0278F	Sukses
audio3 (6.621MB)	Uji5.pdf (39KB)	B61C1193C5BA996FB8CFB46265B6C49A	B61C1193C5BA996FB8CFB46265B6C49A	Sukses
audio3 (6.621MB)	Uji6.pdf (12KB)	1CECED7A59E9EED6E5E52E883FDAD843	1CECED7A59E9EED6E5E52E883FDAD843	Sukses
audio4 (8.496MB)	Tes1.doc (47KB)	2A0411FFD184E17D1B4B4E123581B9B3	2A0411FFD184E17D1B4B4E123581B9B3	Sukses
audio4 (8.496MB)	Tes2.doc (51KB)	5083B0DECA35AE3BBC6060891DAFBF54	5083B0DECA35AE3BBC6060891DAFBF54	Sukses
audio5 (11.389 MB)	Tes3.doc (49KB)	897855CF774F22D96CF96383017E5128	897855CF774F22D96CF96383017E5128	Sukses
audio5 (11.389 MB)	Tes4.doc (83KB)	11DC9645261D5348E9A1D0A07A536863	11DC9645261D5348E9A1D0A07A536863	Sukses

IV. EVALUASI DAN PENGUJIAN SISTEM

Pengujian dilakukan untuk mengetahui kualitas file audio setelah disisipkan pesan dan untuk mengetahui integritas data setelah dilakukan proses kriptografi dan steganografi. Pengujian kualitas file audio dilakukan dengan membandingkan file audio asli dengan file audio yang telah disisipkan pesan menggunakan pengujian SNR dan pengujian integritas data dilakukan menggunakan algoritma MD5, dimana dilakukan dengan cara membandingkan pesan asli dengan pesan yang telah di ekstraksi dari file audio dan kemudian dideskripsi. Terjadi perubahan atau tidak pada pesan tersebut.

TABEL II

PENGUJIAN KUALITAS AUDIO

File Audio (MB)	Kapasitas penyimpanan pesan (KB)	File Pesan (%)	SNR (dB)
Audio1.wav (3,246)	21,706	100	50,62
Audio2.wav (4,746)	39,013	100	49,33
Audio3.wav (5,871)	39,779	100	50,40
Audio4.wav (6,621)	48,009	100	49,93
Audio5.wav (7,371)	50,973	100	50,16
Audio6.wav (8,496)	55,473	100	50,29
Audio7.wav (9,514)	39,714	100	51,10
Audio8.wav (11,389)	83,404	100	49,53
Audio9.wav (13,264)	87,016	100	49,94
Audio10.wav (47,389)	208,871	100	50,55

Pengujian selanjutkan dengan menggunakan SNR dilakukan pada file audio asli dan file audio yang telah disisipkan pesan. SNR dihitung dengan satuan dB (desibel). Kualitas stegofile dapat dikatakan baik apabila nilai SNR diatas 20 dB (nilai standar distorted file). Jadi semakin tinggi nilai SNR maka kualitas berkas audio dikatakan semakin baik, sebab ratio sinyal terhadap derau semakin tinggi. File pesan yang akan disisipkan adalah berukuran 100% dari ukuran pesan yang dapat ditampung oleh file audio.

V. KESIMPULAN

Algoritma AES (*Advanced Encryption Standard*) dan steganografi EAS (*Enhanced Audio Steganography*) dapat digunakan sebagai Sistem pengamanan data pada file audio. Hasil dari pengujian integritas data menunjukan tidak terjadi perubahan pesan antara pesan yang disisipkan ke file audio dengan pesan yang telah diektraksi. Dari perhitungan SNR, didapatkan bahwa file audio yang telah disisipkan pesan memiliki kualitas berkas audio yang baik karena memiliki nilai SNR diatas 20 dB.

Saran yang dapat diberikan oleh penulis untuk penelitian selanjutnya adalah dengan metode EAS (*Enhanced Audio Steganography*) ukuran pesan yang dapat disisipkan pada file audio tidak dapat ditentukan dengan pasti (*random*), karena pesan hanya akan disisipkan pada *byte* file audio yang bernilai 254 atau 255 saja dan itu tergantung pada jumlah *byte* yang bernilai 254 atau 255 pada file audio. Untuk itu disarankan untuk mencoba menggunakan metode lain yang dapat menampung pesan dengan ukuran yang besar pada file audio dan tetap menjaga kualitas file audio tersebut.

REFERENSI

[1] C. Parthasarathy dan S.K. Srivatsa, "Increased Robustness Of LSB Audio Steganography by Reduced Distortion LSB Coding", *Journal of Theoretical and Applied Information Technology* ©2005 - 2009 JATIT, 2009.

[2] R Sridevi, A Damodaram, SVL. Narasimham "Efficient Method or Audio Stagnography by modified LSB Algorithm and String Encryption Key with Enhanced Security". In Proc. JATITI. PP:768-771, 2005-2009.

[3] Sellers, 1996, "An Introduction to Steganography", University of Cape Town, South Africa.

[4] S. P. Kumar dan R.K. Aggrawal, "Enhancement of LSB Based Steganography for Hiding Image in Audio", (IJCSE) *International Journal on Computer Science and Engineering*, vol. 02, 2010.

[5] C. Parthasarathy dan S.K. Srivatsa, "Increased Robustness Of LSB Audio Steganography by Reduced Distortion LSB Coding", *Journal of Theoretical and Applied Information Technology* ©2005 - 2009 JATIT, 2009.

[6] Yuniati, V., Indriyanta, G., dan Rachmat, A. 2011. Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jenis *File. Jurnal Informatika Vol.5 No.1*. Yogyakarta.

[7] Munir, Renaldi. 2010. Kriptografi. *Jurnal Teknologi Informatika*. Bandung.