IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4 DAN METODE STEGANOGRAFI AUDIO 2LSB PADA SISTEM KEAMANAN INFORMASI

Ely Setyo Astuti [2], Binar Prihadmantyo[1], Meyti Eka Apriyani [3]

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

Abstrak

Providing security and confidentiality to information is essential when exchanging information through communication networks. It is intended that the information sent by the sender can be received completely by the recipient without any interference from unauthorized parties to the information. Cryptography and steganography techniques can be used to secure confidential messages. By building applications that combine these two techniques can provide security to the secret messages well. Security techniques that can be used is cryptographic techniques using RC4 algorithm to secure secret messages in the form of text or images, and insertion of secret messages with 2LSB steganography method into the audio media. The analysis performed is the success rate of insertion process and message extraction, process speed, audio stego attack, and audio quality. Results from 18 instances of insertion testing and message extraction, a 100% success percentage with different processing times depends on the size of the message being inserted. The resulting audio stego has good quality and does not cause noise that can be heard by the human sense of hearing directly, but the audio stego is not resistant to attacks that cause changes to stego byte file values. So it can be concluded that the combination between RC4 cryptographic algorithm and 2LSB steganography method can secure the message well and provide the results of decryption without any changes to the message is inserted.

Kata kunci: kriptografi, steganografi, RC4, 2LSB

PENDAHULUAN

Semakin berkembangnya teknologi dan layanan internet membuat setiap orang dapat dengan mudah untuk melakukan pertukaran data atau informasi kepada orang lain tanpa dibatasi oleh batas-batas jarak dan waktu. Hal tersebut juga turut mempengaruhi berkembangnya kejahatan yang memanfaatkan teknologi informasi dan komunikasi. Informasi yang ditransmisikan pada jaringan komunikasi dari pengirim ke penerima, rentan untuk diakses oleh pihak lain yang tidak berkepentingan. Dengan demikian, keamanan dan kerahasiaan menjadi suatu kebutuhan penting dalam melakukan pertukaran informasi yang ditransmisikan melalui jaringan komunikasi.

Dalam bidang keamanan informasi, terdapat dua teknik yang digunakan untuk mengamankan informasi, yaitu teknik kriptografi dan steganografi. Kriptografi merupakan teknik untuk menyamarkan informasi dalam bentuk pesan bermakna menjadi pesan yang tidak bermakna. Sedangkan steganografi ialah teknik untuk menyembunyikan informasi ke dalam suatu media atau wadah pembawa informasi.

Kriptografi memiliki manfaat yaitu untuk menjaga atau mengamankan informasi dari pihak-pihak yang tidak berkepentingan, dengan cara menyandikan informasi tersebut. Informasi dienkripsi dengan algoritma tertentu agar tidak dapat dibaca dan dimengerti oleh orang lain. Salah satu algoritma kriptografi adalah RC4. Algoritma kriptografi RC4 populer dengan kecepatan dan sederhana, sehingga mudah diimplementasikan dan dikembangkan secara efisien pada *software* maupun *hardware* [7]. Namun karena informasi yang telah dienkripsi memiliki struktur acak dan sulit dimengerti maknanya, maka sangatlah mungkin menimbulkan kecurigaan orang lain, sebab informasi yang seperti demikian pasti sudah diolah dan menunjukkan bahwa informasi tersebut bersifat penting dan rahasia. Hal ini dapat menarik orang lain untuk memecahkan informasi rahasia tersebut. Untuk menghindari permasalahan tersebut, dapat diatasi dengan menggunakan teknik steganografi.

Steganografi memiliki manfaat yaitu untuk menyembunyikan informasi kedalam suatu media pembawa informasi, sehingga keberadaan informasi

yang dikirimkan tidak dapat diketahui oleh orang lain. Aspek terpenting dari steganografi biasanya terletak pada penyembunyian informasi kedalam media pembawa informasi, dengan tingkat perubahan yang tidak signifikan pada media pembawa informasi sebelum dan setelah disisipi pesan. Salah satu metode steganografi adalah *Least Significant Bit* (LSB). Metode LSB melakukan penyisipan pesan dengan mengganti bit terendah dalam sebuah *byte* media pembawa pesan. Kapasitas penyimpanan pada metode LSB dapat ditingkatkan lagi dengan metode 2LSB, yang melakukan penyisipan pesan dengan mengganti dua bit terendah dalam sebuah *byte* media pembawa pesan [3].

Dengan mengombinasikan antara teknik kriptografi dan steganografi, dapat memberikan keamanan yang baik dalam mengamankan pesan rahasia. Pesan yang telah disandikan menggunakan algoritma kriptografi tertentu, kemudian disembunyikan kedalam suatu media pembawa pesan, agar tidak menimbulkan kecurigaan terhadap orang lain yang melihatnya.

Dalam penelitian ini menerapkan penggabungan antara teknik steganografi dan kriptografi, sehingga dapat mengamankan pesan rahasia dengan baik. Implementasi enkripsi dan dekripsi pesan dengan menggunakan algoritma kriptografi RC4. Pesan yang telah dienkripsi kemudian disembunyikan pada media audio menggunakan metode 2LBS.

1. Tinjauan Pustaka

1.1 Kriptografi

Kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengeri lagi maknanya [5]. Konsep utama kriptografi adalah enkripsi (*encryption*) dan dekripsi (*decryption*) [1]. Enkripsi adalah sebuah proses menyandikan plainteks menjadi cipherteks. Sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula. Dalam melakukan enkripsi dan dekripsi pesan, dibutuhkan kunci sebagai parameter yang digunakan untuk transformasi.

Kriptografi terbagi menjadi dua, yaitu :

a. Kriptografi klasik (mode karakter)
   - Cipher substitusi
   - Cipher transposisi
b. Kriptografi modern (mode binary)
   - Cipher kunci simetris : cipher aliran (stream cipher) dan cipher blok (block cipher)
   - Cipher kunci asimetris

1.2 Steganografi

Steganografi adalah ilmu dan seni untuk menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia [4]. Teknik Steganografi membutuhkan dua properti utama, yaitu wadah penampung dan pesan/ data rahasia yang disembunyikan.

Proses penyisipan pesan rahasia ke dalam media dinamakan *encoding*, sedangkan ekstrasi pesan dari stego object dinamakan *decoding*. Kedua proses ini biasanya memerlukan kunci rahasia (stegokey) agar pihak yang berkepentingan saja yang dapat melakukan penyisipan pesan dan ekstrasi.

1.3 Audio

Audio adalah suara atau bunyi yang dihasilkan dari getaran suatu benda. Di butuhkan getaran minimal 20 kali/detik, agar audio dapat didengar oleh telinga manusia. Sinyal audio dibagi menjadi dua macam, yaitu *analog* dan *digital* [2]. audio analog memproduksi variasi suara dengan membuat atau membaca variasi sinyal listrik. Sedangkan audio *digital* memproduksi suara dengan mengambil sampel tekanan suara atau level sinyal pada rate tertentu dan mengubahnya menjadi angka.

1.4 Algoritma Kriptografi RC4

RC4 merupakan jenis dari aliran kode yang berarti operasi enkripsinya dilakukan setiap karakter 1 byte (8 bit) untuk sekali operasi. Algoritma ini ditemukan pada tahun 1978 oleh Ronald Rivest dan menjadi simbol keamanan RSA. RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte [6]. Tabel tersebut digunakan untuk generasi berikut dari pseudo random yang melakukan XOR dengan plainteks untuk menghasilkan keluaran berupa cipherteks.

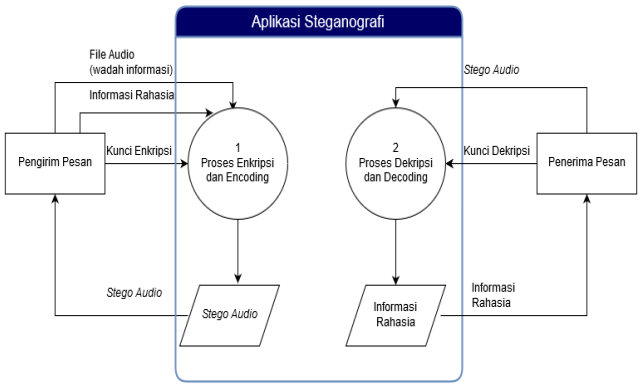
1.5 Metode Least Significant Bit (LSB)

Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan [4]. Pada susunan bit di dalam sebuah byte (1 *byte* = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Sedangkan pada teknik modifikasi 2LSB, pergantian bit dilakukan pada 2 bit LSB. Teknik 2LSB memiliki kelebihan pada kapasitas

penyimpanan pesan yang disisipkan yaitu dua kali lebih besar dari teknik LSB.

2. Perancangan dan Implementasi

Desain sistem dari aplikasi yang digunakan pada penelitian ini dapat dilihat pada gambar 1.



Gambar 1 Desain sistem

Gambar diatas merupakan proses yang dijalankan oleh sistem. Proses tersebut antara lain :

1. Proses enkripsi dan *encoding* (penyisipan) : proses ini memerlukan masukan berupa file audio sebagai wadah pembawa pesan, informasi atau pesan rahasia berupa teks atau citra, dan kunci enkripsi. Pertama dilakukan proses enkripsi terhadap pesan rahasia menggunakan algoritma kriptografi RC4 dengan kunci enkripsi yang telah dimasukkan. Selanjutnya dilakukan proses penyisipan yaitu pesan rahasia yang telah terenkripsi disispkan kedalam file audio berekstensi .wav menggunakan metode steganografi 2LSB. Penyisipan dimulai pada *byte* audio ke 51 dan dilakukan dengan mengganti 2 bit terakhir setiap *byte* audio dengan bit-bit pesan rahasia. Setiap penyisipan dilakukan dengan memberikan jarak 5 *byte* dengan penyisipan berikutnya hingga bit-bit pesan rahasia tersisipkan seluruhnya, sehingga menghasilkan keluaran berupa file stego audio.
2. Proses *decoding* (ekstraksi) dan dekripsi : proses ini memerlukan masukan berupa file stego audio dan kunci dekripsi. Pertama dilakukan proses ekstraksi untuk mengambil pesan rahasia yang disisipkan didalam file stego audio menggunakan metode steganografi 2LSB. Proses ini dilakukan dengan mengambil bit-bit pesan rahasia dari *byte* stego audio. Pengambilan bit-bit pesan rahasia dimulai pada *byte* stego audio ke 51 dan dilakukan dengan mengambil 2 bit terakhir pada setiap *byte* stego audio. Setiap pengambilan bit-bit pesan rahasia dilakukan dengan memberikan jarak 5 *byte* dengan pengambilan berikutnya hingga bit-bit pesan rahasia terambil seluruhnya. Selanjutnya, pesan rahasia yang telah diekstraksi dari file stego audio dilakukan proses dekripsi menggunakan algoritma kriptografi RC4 dengan kunci dekripsi agar pesan dapat dibaca dan dimengerti oleh penerima pesan.

3. Hasil Pengujian

Pengujian aplikasi yang dilakukan menggunakan file uji citra dan plainteks sebagai pesan rahasia yang disisipkan kedalam media audio. Detail dari file uji citra dan plainteks ditunjukkan pada tabel 1 dan 2.

Tabel 1 File uji citra

No	Nama File Citra	Ukuran File	Ukuran Pixel
1	Uji_1.jpg	571 *byte*	30 x 30
2	Uji_2.jpg	6.839 *byte*	350 x 350
3	Uji_3.jpg	15.315 *byte*	250 x 260

Tabel 2 Uji teks

No	Teks Pengujian	Pesan Teks	Panjang Plainteks
1	plainteks 1	Hallo, nama saya Binar Prihadmantyo.	36 karakter (36 *byte*)
2	plainteks 2	Hallo, nama saya Binar Prihadmantyo. Saya kuliah di Politeknik Negeri Malang, jurusan Teknologi Informasi.	106 karakter (106 *byte*)

	plainteks 3	Hallo, nama saya Binar Prihadmantyo. Saya kuliah di Politeknik Negeri Malang, jurusan Teknologi Informasi. Usia saya 22 tahun, tinggal di Perum Permata Saxofone E-6, Kelurahan Jatimulyo, Kecamatan Lowokwaru, Kota Malang.	220 karakter (220 *byte*)

Sedangkan, file audio pembawa pesan menggunakan 3 file uji berekstensi wav. Detail dari file uji audio ditunjukkan pada tabel 3.

Tabel 3 File uji audio

No	Nama File Audio	Ukuran File	Durasi Audio
1	all.wav	3.985.688 *byte*	1:30
2	alone.wav	4.546.052 *byte*	1:42
3	life.wav	6.204.800 *byte*	2:20

3.1 Pengujian Penyisipan dan Ekstraksi

Dari sampel data yang ditunjukkan diatas, dilakukan pengujian penyisipan dan ekstraksi terhadap pesan rahasia. Pengujian penyisipan dan ekstraksi menggunakan kunci yang sama yaitu ‘polinema2017’, yang digunakan untuk enkripsi maupun dekripsi pesan rahasia. Hasil pengujian penyisipan pesan rahasia ditunjukkan pada tabel 4.

Tabel 4 Hasil pengujian penyisipan

No	File Audio	Informasi Rahasia	File Keluaran	Keterangan
Pesan Teks				
1	all.wav	plainteks 1	all1.wav	Berhasil
		plainteks 2	all2.wav	Berhasil
		plainteks 3	all3.wav	Berhasil
2	alone.wav	plainteks 1	alone1.wav	Berhasil
		plainteks 2	alone2.wav	Berhasil
		plainteks 3	alone3.wav	Berhasil
3	life.wav	plainteks 1	life1.wav	Berhasil
		plainteks 2	life2.wav	Berhasil
		plainteks 3	life3.wav	Berhasil
Citra				
4	all.wav	uji_1.jpg	all_1.wav	Berhasil
		uji_2.jpg	all_2.wav	Berhasil
		uji_3.jpg	all_3.wav	Berhasil
5	alone.wav	uji_1.jpg	alone_1.wav	Berhasil
		uji_2.jpg	alone_2.wav	Berhasil
		uji_3.jpg	alone_3.wav	Berhasil
6	life.wav	uji_1.jpg	life_1.wav	Berhasil
		uji_2.jpg	life_2.wav	Berhasil
		uji_3.jpg	life_3.wav	Berhasil

Berdasarkan hasil pengujian yang ditunjukkan pada tabel diatas, sebanyak 18 kali pengujian didapatkan hasil: 9 pesan teks dan 9 file citra berhasil disisipkan. Kegagalan dalam penyisipan dapat dikarenakan ukuran pesan lebih besar dari pada ukuran maksimal pesan yang dapat disisipkan kedalam audio (> 4% ukuran audio).

Setelah melakukan pengujian penyisipan, selanjutnya dilakukan pengujian ekstraksi pesan rahasia dari file stego audio. Berdasarkan pengujian ekstraksi pesan rahasia, sebanyak 18 kali pengujian didapatkan hasil: 9 pesan teks dan 9 file citra berhasil diekstraksi. Hasil pengujian ekstraksi pesan rahasia ditunjukkan pada tabel 5.

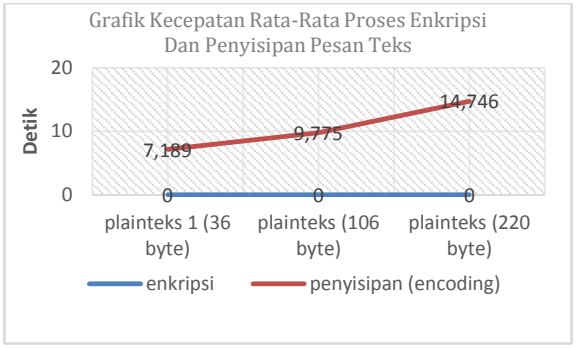
Tabel 5 Hasil pengujian ekstraksi

No	File Audio	Keluaran	Keterangan
Pesan Teks			
1	all1.wav	plainteks 1	Berhasil
	all2.wav	plainteks 2	Berhasil
	all3.wav	plainteks 3	Berhasil
2	alone1.wav	plainteks 1	Berhasil
	alone2.wav	plainteks 2	Berhasil
	alone3.wav	plainteks 3	Berhasil
3	life1.wav	plainteks 1	Berhasil
	life2.wav	plainteks 2	Berhasil
	life3.wav	plainteks 3	Berhasil
Citra			
4	all_1.wav	uji_1.jpg	Berhasil
	all_2.wav	uji_2.jpg	Berhasil
	all_3.wav	uji_3.jpg	Berhasil
5	alone_1.wav	uji_1.jpg	Berhasil
	alone_2.wav	uji_2.jpg	Berhasil
	alone_3.wav	uji_3.jpg	Berhasil
6	life_1.wav	uji_1.jpg	Berhasil
	life_2.wav	uji_2.jpg	Berhasil

	life_3.wav	uji_3.jpg	Berhasil

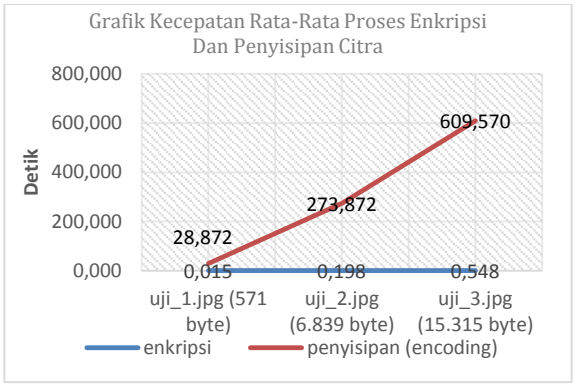
3.2 Pengujian Kecepatan Proses

Kecepatan proses enkripsi dan penyisipan pesan rahasia bergantung pada ukuran pesan yang disisipkan. Semakin besar ukuran pesan yang disisipkan, maka semakin lama waktu proses yang dibutuhkan. Dari hasil pengujian kecepatan proses enkripsi dan penyisipan pesan teks, maka kecepatan rata-rata proses yang dibutuhkan dapat digambarkan dalam grafik seperti pada gambar 2.



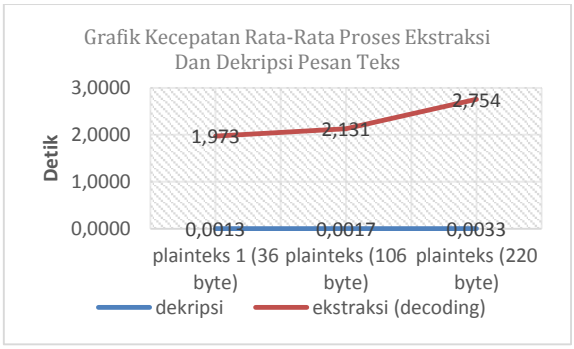
Gambar 2 Grafik kecepatan rata-rata proses enkripsi dan penyisipan pesan teks

Sedangkan dari hasil pengujian kecepatan proses enkripsi dan penyisipan citra, maka kecepatan rata-rata proses yang dibutuhkan dapat digambarkan dalam grafik seperti pada gambar 3.



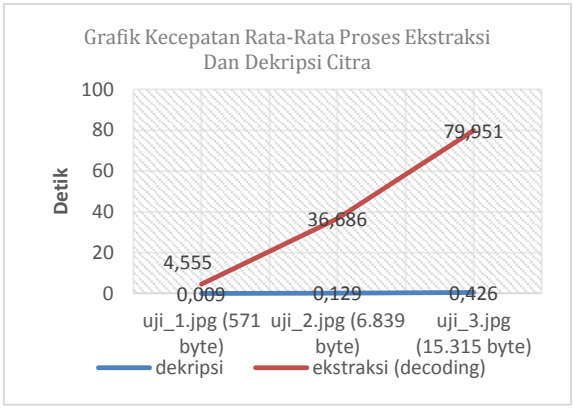
Gambar 3 Grafik kecepatan rata-rata proses enkripsi dan penyisipan pesan teks

Sama seperti proses enkripsi dan penyisipan, kecepatan proses ekstraksi dan dekripsi pesan rahasia juga bergantung pada ukuran pesan yang disisipkan. Dari hasil pengujian kecepatan proses ekstraksi dan dekripsi pesan teks, maka kecepatan rata-rata proses yang dibutuhkan dapat digambarkan dalam grafik seperti pada gambar 4.



Gambar 4 Grafik kecepatan rata-rata proses ekstraksi dan dekripsi pesan teks

Sedangkan dari hasil pengujian kecepatan proses ekstraksi dan dekripsi citra, maka kecepatan rata-rata proses yang dibutuhkan dapat digambarkan dalam grafik seperti pada gambar 5.



Gambar 5 Grafik kecepatan rata-rata proses ekstraksi dan dekripsi pesan teks

3.3 Pengujian Serangan Stego Audio

Terdapat berbagai macam serangan yang dapat dilakukan pada stego audio, seperti melakukan pemotongan durasi (*cropping*), membalik (*reversing*), dan mengubah amplitudo audio. Pengujian dilakukan dengan melakukan serangan pada stego audio, kemudian dilakukan proses dekripsi dengan menggunakan kunci yang sesuai. Sampel stego audio yang digunakan untuk pengujian serangan adalah 'all_1.wav'. Hasil dari pengujian serangan stego audio ditunjukkan pada tabel 6.

Tabel 6 Hasil pengujian serangan stego audio

No	Serangan Stego Audio	Stego Audio	Hasil Serangan Stego Audio	Hasil Keluaran

1.	Memotong durasi stego audio 5 detik dari belakang	all_1.wav 3.985.688 *byte* / 1:30	all_1.wav 3.753.928 *byte* / 1:25	Berhasil
2.	Memotong durasi stego audio 5 detik dari depan	all_1.wav 3.985.688 *byte* / 1:30	all_1.wav 3.765.688 *byte* / 1:25	Gagal
3.	Reverse	all_1.wav 3.985.688 *byte* / 1:30	all_1.wav 3.986.188 *byte* / 1:30	Gagal
4.	Mengubah amplitudo +1.5 dB	all_1.wav 3.985.688 *byte* / 1:30	all_1.wav 3.986.188 *byte* / 1:30	Gagal
5.	Mengubah amplitudo -1.5 dB	all_1.wav 3.985.688 *byte* / 1:30	all_1.wav 3.986.188 *byte* / 1:30	Gagal

Dari keseluruhan uji coba serangan yang dilakukan, hasil yang didapatkan membuktikan bahwa stego audio tidak tahan terhadap serangan. Hal tersebut terjadi karena adanya perubahan *byte* pesan pada file stego audio, sehingga pesan yang disisipkan tidak dapat diekstraksi dan didekripsi. Namun apabila serangan yang dilakukan tidak merubah *byte* pesan pada file stego audio, maka pesan yang disisipkan dapat diekstraksi dan didekripsi, seperti pada pengujian serangan yang pertama yaitu memotong durasi stego audio 5 detik dari belakang.

3.4 Pengujian Kualitas Audio

Proses penyisipan pesan kedalam file audio menghasilkan suatu file stego audio yang terdapat *noise*. Terjadinya *noise* diakibatkan perubahan bit yang dilakukan pada proses penyisipan pesan.

Tabel 7 Hasil pengujian kualitas audio

Audio Asli	Pesan	Stego Audio	Pengujian	
			Subjektif	PSNR
all.wav (3.985.688 *byte*)	uji_1.jpg (571 *byte*)	all_1.wav (3.985.688 *byte*)	Baik	45,150 38819 dB
	uji_2.jpg (6.839 *byte*)	all_2.wav (3.985.688 *byte*)	Baik	45,168 26506 dB
	uji_3.jpg (15.315 byte)	all_3.wav (3.985.688 *byte*)	Baik	45,143 82346 dB

Pengukuran *noise* stego audio dilakukan dengan menggunakan PSNR (*Peak Signal to Noise Ratio*). Semakin besar nilai PSNR stego audio, maka semakin baik kualitas audio tersebut secara subjektif.

Apabila nilai PSNR < 30dB, maka *noise* akan terdengar jelas oleh indra pendengaran manusia.

Pengujian PSNR menggunakan sampel file uji audio 'all.wav', yang disisipi file uji citra dengan ukuran file yang berbeda-beda. Hasil dari pengujian kualitas audio ditunjukkan pada tabel 7.

Berdasarkan pengujian kualitas audio yang ditunjukkan pada tabel diatas, didapatkan nilai PSNR stego audio > 30 dB. Sehingga dapat disimpulkan bahwa kualitas stego audio yang dihasilkan baik dan tidak menghasilkan *noise* yang dapat terdengar oleh indra pendengaran manusia.

4. Kesimpulan dan Saran

4.1 Kesimpulan

1. Berdasarkan hasil pengujian penyisipan pada file audio, sebanyak 18 kali pengujian penyisipan pesan rahasia berupa pesan teks dan citra, didapatkan persentase keberhasilan sebesar 100%.
2. Pengujian ekstraksi pesan rahasia dengan mencocokkan antara pesan teks dan citra sebelum disisipkan dan setelah diekstraksi, didapatkan tingkat keberhasilan sebesar 100% dari 18 kali pengujian.
3. Kecepatan proses enkripsi dan penyisipan maupun ekstraksi dan dekripsi pesan bergantung pada ukuran pesan yang disisipkan. Semakin besar ukuran pesan yang disisipkan, maka semakin lama waktu proses yang dibutuhkan.
4. Stego audio tidak tahan terhadap serangan yang menyebabkan perubahan nilai *byte* pesan pada file stego. Hal ini dibuktikan dengan gagalnya proses ekstraksi dan dekripsi pesan.
5. Stego audio yang dihasilkan memiliki kualitas baik. Hal ini dibuktikan dengan nilai PSNR stego audio > 30 dB, sehingga tidak menimbulkan *noise* yang dapat didengarkan oleh indra pendengaran manusia secara langsung.

4.2 Saran

1. Pengembangan pesan yang diamankan menggunakan berbagai jenis tipe file, seperti file dokumen, audio, dan video.

2. Pengembangan keamanan penyisipan dengan melakukan pengacakan pola penyisipan pesan, misal menggunakan metode *Random Byte Position Encoding*.
3. Penyisipan pesan pada file pembawa pesan menggunakan metode yang tidak membatasi ukuran pesan yang disisipkan, misal menggunakan metode *End of File* (EOF).
4. Pengembangan aplikasi berbasis web dan android.

Daftar Pustaka

[1] Ariyus, Dony, 2008, "*Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*", Purwokerto, STMIK AMIKOM.
[2] Binanto, Iwan, 2010, "*Multimedia Digital – Dasar Teori dan Pengembangannya*", Yogyakarta, ANDI.
[3] Eko Krist Setyono dan M.A. Ineke Pakareng, 2014, "*Perancangan dan Implementasi Aplikasi Steganografi Citra Digital dengan Metode 2LSB*", Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.
[4] Munir, Rinaldi, 2004, "*Pengolahan Citra Digital Dengan Pendekatan Algoritmik*", Bandung, Informatika..
[5] Munir, Rinaldi, 2006, "*Kriptografi*", Bandung, Informatika
[6] Schneier, Bruce, 1996, "*Applied Cryptography: Protocols, Algorithms and Source Code in C*", John Wiley & Sons.
[7] Sekarsari, Galuh Adjeng. 2015, "*Analisa Algoritma Kriptografi RC4 Pada Enkripsi Citra Digital*", Fakultas Ilmu Komputer, Universitas Dian Nuswantoro.