PENERAPAN STEGANOGRAFI MENGGUNAKAN ALGORITMA *LEAST SIGNIFICANT BIT* DENGAN MEMANFAATKAN AUDIO DIGITAL SEBAGAI *COVER-OBJECT*

Andri Zakariya[1], Dinisfu Sya'ban[2], Nazori Agani[3]

Magister Ilmu Komputer Program Pascasarjana Universitas Budi Luhur
[1]andri.zakariya@gmail.com, [2]zidinis_zidane@yahoo.com, [3]nazori@budiluhur.ac.id

ABSTRAK

Makin rentannya keamanan informasi dalam pelaksanaan komunikasi di berbagai media komunikasi seperti internet menjadikan pengamanan terhadap informasi hal yang tidak terpisahkan dalam pelaksanaan komunikasi. Teknik yang dapat digunakan dalam pengamanan informasi dan data dalam komunikasi adalah teknik kriptografi ataupun dengan menggunakan teknik steganografi. Steganografi atau teknik penyembunyian data dapat dijadikan alternatif pengamanan data atau informasi rahasia, dalam teknik ini data yang akan dilindungi disembunyikan dalam data lainnya sedemikian sehingga data yang dilindungi tersebut tidak dapat diketahui oleh pihak yang tidak berkepentingan. Salah satu algoritma steganografi yang paling terkenal adalah Least Significant Bit (LSB). Berbagai penelitian telah dilakukan dalam rangka menerapkan algoritma LSB untuk steganografi yang menggunakan citra digital sebagai file cover atau pembawa pesan rahasia yang disembunyikan. Penulis mencoba menerapkan LSB untuk steganografi dengan menggunakan jenis file multimedia yang berbeda dari penelitian-penelitian sebelumnya. Pada penelitian ini penulis menggunakan audio digital sebagai file cover-object atau pembawa pesan rahasia yang disembunyikan. Dari hasil penelitian yang dilakukan maka dapat disimpukan bahwa aplikasi steganografi yang telah diterapkan menggunakan algoritma LSB pada audio digital dapat digunakan dengan baik untuk menyembunyikan pesan sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut.

Keywords : ***audio, steganografi, cover-object, LSB, dan PSNR.***

I. PENDAHULUAN

Teknologi informasi dan komunikasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Salah satu cerminannya yaitu perkembangan jaringan internet yang memungkinkan berbagai pihak untuk saling bertukar informasi secara cepat bahkan *real time* dimanapun dan kapanpun. Seiring dengan perkembangan tersebut, kejahatan teknologi informasi dan komunikasi juga turut berkembang, seperti yang sering kita dengar adalah *hacker*, *cracker*, *carder*, *phreaker* dan sebagainya dengan berbagai teknik yang mencoba untuk mengakses informasi yang bukan haknya. Oleh karena itu sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan pengamanannya.

Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah teknik steganografi. Teknik sudah dipakai lebih dari 2500 tahun yang lalu untuk menyembunyikan pesan rahasia. Berbeda dengan teknik kriptografi, steganografi menyembunyikan pesan rahasia agar bagi orang awam tidak menyadari keberadaan dari pesan yang disembunyikan. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut. Dengan berkembangnya dunia multimedia, maka steganografi modern menggunakan file-file multimedia ini sebagai *cover* untuk menyembunyikan pesan. Lalu lintas file-file multimedia di internet sudah lumrah sehingga akan mengurangi kecurigaan akan adanya pesan rahasia.

Salah satu algoritma steganografi yang paling terkenal adalah *Least Significant Bit* (LSB). Dengan menggunakan LSB pesan dapat disembunyikan pada suatu file multimedia dengan cara menyisipkannya pada bit rendah atau bit yang paling kanan pada data yang menyusun file multimedia tersebut. Berbagai penelitian telah dilakukan dalam rangka menerapkan algoritma LSB untuk steganografi yang menggunakan citra digital sebagai file *cover* atau pembawa pesan rahasia yang disembunyikan [1][7][9][10].

Penulis akan mencoba menerapkan LSB untuk steganografi dengan menggunakan jenis file multimedia yang berbeda dari penelitian-penelitian sebelumnya. Pada penelitian ini penulis menggunakan audio digital sebagai file *cover-object* atau pembawa pesan rahasia yang disembunyikan.

Dari latar belakang tersebut, permasalahan yang diidentifikasi dalam rangka pengamanan informasi menggunakan kriptografi adalah timbulnya kecurigaan terhadap data yang dienkripsi menggunakan teknik kriptografi. Sedangkan dengan steganografi menyembunyikan pesan rahasia agar bagi

orang awam tidak menyadari keberadaan dari pesan yang disembunyikan.

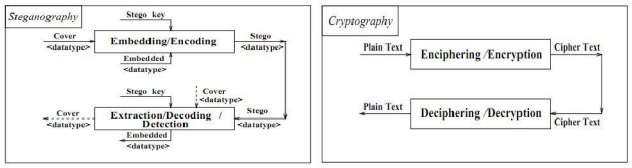
Penulis dalam melalukan penelitian ini memiliki keterbatasan dari sisi waktu dan sumber daya lainnya. Agar dapat menyelesaikan penelitian ini tepat waktu dan dengan sumber daya yang dimiliki, maka permasalahan yang akan dibahas harus dibatasi. Adapun batasan masalah pada penelitian ini yaitu format audio digital yang digunakan dalam penelitian adalah format wav dan simulasi dilakukan menggunakan aplikasi MATLAB.

Penelitian ini bertujuan untuk melakukan penelitian tentang penerapan steganografi pada audio digital dengan menggunakan algoritma LSB sebagai alternatif penyembunyian pesan rahasia. Manfaat penelitian ini secara teoritis yaitu untuk memberikan informasi tentang penerapan steganografi pada audio digital dalam mengamankan pesan rahasia menggunakan algoritma LSB. Sedangkan manfaat penelitian ini secara praktis yaitu untuk memberikan jaminan keamanan bagi para pihak yang ingin bertukar informasi atau pesan rahasi melalui internet.

II. TINJAUAN PUSTAKA

Steganografi

Kata Steganografi berasal dari Yunani yang artinya "menyembunyikan dalam pandangan yang jelas" [3]. Steganografi adalah seni atau ilmu menyembunyikan informasi dengan berbagai cara sedemikian sehingga dapat mencegah diketahuinya informasi yang disembunyikan [2]. Berbeda dengan kriptografi yang mana keberadaan pesan tidak disamarkan, tetapi isi dari pesan tersebut tidak terbaca sebagaimana mestinya (tersandi). Penggunaan steganografi biasanya menggunakan gambar sebagai media penyembunyiannya. Perbandingan antara model steganografi dan kriptografi dapat digambarkan pada Gambar 1.

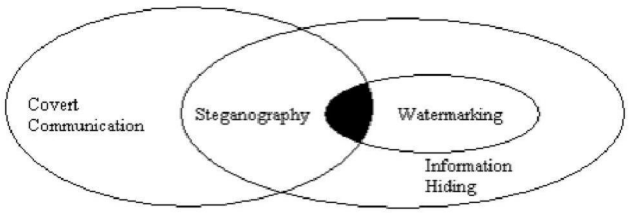


Gambar 1. Perbandingan model steganografi dan kriptografi

Sebagaimana digambarkan pada Gambar 1 di atas, komponen-komponen dari model steganografi dapat dijelaskan sebagai berikut:

1) *Embeded*: sesuatu yang ingin disembunyikan
2) Stego: output hasil proses penyembunyian, sesuatu telah disisipkan pesan ke dalamnya.
3) *Cover:* bentuk asli dari stego.
4) *Embedding*: proses penyembunyian pesan yang disisipkan.
5) *Extracting*: mengambil kembali pesan yang disisipkan keluar dari stego.
6) Stego *key*: kunci rahasia yang dibutuhkan dalam proses *embedding* untuk menyembunyikan pesan dan proses *extracting* untuk mengekstraksi pesan yang disembunyikan[6].

Ide dasar dari penyembunyian informasi kedalam media digital telah menyebar kebidang lain melebihi dari steganografi, seperti yang digambarkan pada Gambar 2. Teknik-teknik tersebut dilingkupi dalam sebuah aplikasi yang semuanya mengarah sebagai *information hiding*. Kasus khusus dari *information hiding* adalah *digital watermarking*. *Digital watermarking* adalah proses menyisipkan informasi ke dalam isi dari multimedia digital yang nantinya bisa diekstrak atau dideteksi untuk sebuah tujuan termasuk *copy prevention* dan kontrol [5]. Perbedaan antara *information hiding* dan *watermarking* adalah kehadiran dari pihak lawan yang aktif. Dalam aplikasi *watermarking* seperti *copyright protection* dan *authentication*, pihak lawan aktif berusaha mencoba untuk mengeluarkan, membuat tidak valid atau memalsukan *watermarking*.



Gambar 2. Hubungan antara steganografi dan bidang-bidang lainnya [5]

Semakin berkembangnya teknologi informasi dan komunikasi menjadikan komunikasi yang dilakukan dalam jaringan komputer seperti internet semakin banyak dan penggunaan teknologi digital semakin besar pula. Perubahan ini memberikan dampak pula terhadap penggunaan steganografi, dimana dalam era teknologi informasi ini, steganografi digunakan untuk menyembunyikan data digital dalam bentuk gambar, audio dan video tanpa mengganggu penggunaan steganografi dalam format data analog. Dalam penerapan steganografi pada data digital yang perlu kita lakukan adalah menyembunyikan rangkaian 0 dan 1 dalam data *cover*.

Algoritma LSB

Untuk menjelaskan algoritma LSB maka digunakan citra digital sebagai *cover-object*. Pada setiap byte terdapat bit yang paling kurang yaitu *Least Significant Bit* atau LSB. Misalnya pada byte 0001100**1**, maka bit LSBnya adalah **1**. Untuk melakukan penyisipan pesan, bit yang cocok untuk diganti adalah bit LSB, karena perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak akan

mengubah warna merah tersebut secara signifikan. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil. Sebagai contoh, urutan bit berikut ini menggambarkan 3 pixel pada *cover-image* 24-bit.

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Pesan yang akan disisipkan adalah karakter "A", yang nilai biner-nya adalah **10000001**, maka akan dihasilkan stego image dengan urutan bit sebagai berikut:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

Terdapat dua jenis teknik yang dapat digunakan pada metode LSB, yaitu penyisipan pesan secara sekuensial dan secara acak. Sekuensial berarti pesan rahasia disisipkan secara berurutan dari data titik pertama yang ditemukan pada file gambar, yaitu titik pada pojok kanan bawah gambar. Sedangkan acak berarti penyisipan pesan rahasia dilakukan secara acak pada gambar, dengan masukan kata kunci (stego-*key*).

Format Audio WAV

WAV atau WAVE yang kependekan untuk format audio digital berbentuk gelombang adalah format standar file audio Microsoft dan IBM untuk menyimpan audio pada komputer. File WAV adalah varian dari metode RIFF format *bitstream* untuk menyimpan data dalam "*chunk*" (potongan). Demikian juga sama halnya pada format IFF dan AIFF yang digunakan pada komputer Amiga dan Macintosh. Keduanya, WAV dan AIFF kompatibel dengan sistem operasi Windows dan Macintosh. Format RIFF bertindak sebagai sebuah "*wrapper*" (pembungkus) untuk berbagai kompresi audio yang digunakan pada sistem operasi Windows. Meskipun sebuah file WAV dapat dikompresi, biasanya format WAV berisi audio yang tidak dikompresi dalam format *pulse-code modulation* (PCM).

PCM adalah sebuah metode yang biasa digunakan untuk menyimpan dan mentransmisikan audio digital yang tidak terkompresi. PCM digunakan pada CD audio dan *digital audio tapes* (DATs). PCM merupakan format yang biasa digunakan untuk file AIFF dan WAV. PCM adalah representasi langsung dari nilai biner (1 dan 0). Ketika PCM audio ditransmisikan, setiap "1" direpresentasikan sebagai pulsa voltase positif dan setiap "0" direpresentasikan oleh tidak adanya pulsa.

Dalam penelitian ini, tipe data audio berformat WAV digunakan sebagai data *cover* yang akan disisipkan pesan data yang disembunyikan.

***Peak Signal-to-Noise Ratio* (PSNR)**

Peak Signal-to-Noise Ratio (PSNR) merupakan suatu istilah yang digunakan untuk mengukur rasio antara nilai kekuatan maksimal dari suatu sinyal dan kekuatan yang hilang dari adanya noise yang mempengaruhi keaslian dari suatu data. Dikarenakan karakter sinyal yang memiliki rentan yang sangat banyak, maka PSNR dihitung dengan menggunakan skala logaritma decibel, dimana semakin besar nilai PSNR maka data tersebut dapat dinyatakan baik.

PSNR pada umumnya digunakan untuk menentukan nilai *perbandingan* antara kualitas sinyal asli dengan sinyal yang telah mengalami proses manipulasi, misalnya kompresi dan pengolahan sinyal lainnya. Umumnya PSNR dijadikan ukuran pendekatan secara kasar terhadap suatu kualitas data digital. Suatu data digital yang sama persis mempunyai nilai PSNR tak terhingga, atau semakin besar nilai PSNR maka akan semakin terlihat sama data digital yang dibandingkan. Dalam penelitian tentang pemberian *watermarking* umumnya nilai PSNR berkisar antara 30 sampai dengan 40 sudah dianggap berkualitas baik [4]. Untuk menghitung nilai PSNR dinyatakan sebagai berikut.

$$PSNR = 10.Log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20.Log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

MAX_I adalah nilai maksimal piksel dari suatu data yang dihitung dengan menggunakan 8 bit per sampel dimana *MSE* dinyatakan dengan:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2$$

MSE merupakan nilai *Mean Squared Error* dari dua buah data digital *I* dan *K* yang dinyatakan dalam bentuk spasial dengan ukuran *m* x *n*.

III.RANCANGAN PENELITIAN

A. Metode Penelitian

Metode penelitian yang akan digunakan dalam penelitian ini adalah penelitian eksperimen. Penelitian eksperimen adalah penelitian dimana peneliti dapat melakukan manipulasi kondisi yang ada sesuai dengan keinginan peneliti, dalam kondisi yang telah dimanipulasi ini, biasanya dibuat dua kelompok, yaitu kelompok kontrol dan kelompok pembanding. Kelompok kontrol akan diberikan perlakukan tertentu sesuai dengan tujuan penelitian, hasil dari perlakuan ini yang akan dijadikan pembanding terhadap kelompok pembanding [8].

B. Langkah Penelitian

Tahapan-tahapan yang dilakukan dalam rangka melakukan penelitian terhadap penerapan steganografi pada audio digital menggunakan algoritma LSB adalah sebagai berikut:

1) Studi Pustaka

Penelitian ini dimulai dengan melakukan studi pustaka terkait dengan penerapan steganografi pada media digital serta karakteristik apa saja yang harus dipenuhi dalam penerapan steganografi tersebut [1][7][9][10]. Selain itu, studi yang terkait dengan teknik-teknik yang dapat digunakan dalam penerapan steganografi juga menjadi bahan studi yang penting dalam penelitian ini, terutama teknik yang menggunakan algortima [1][7][9][10].

2) Pembuatan Program Simulasi

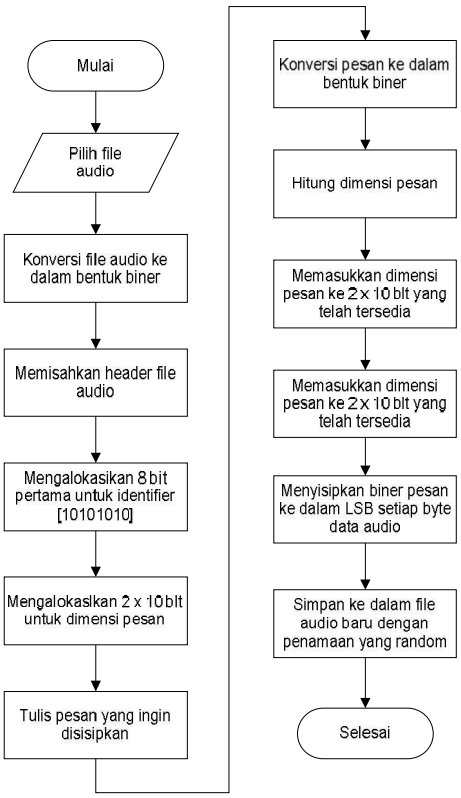
Setelah memahami teknik-teknik steganografi pada audio digital, maka tahap selanjutnya adalah membuat program beserta dengan *graphical user interface* (GUI)-nya dengan memanfaatkan aplikasi MATLAB. Aplikasi MATLAB dipilih sebagai perangkat lunak pemrograman karena sudah tersedianya *toolbox* untuk pengolahan audio digital dan fungsi-fungsi matematika, sehingga mempermudah proses pemrograman dan simulasi.

3) Eksperimen dan Pengujian

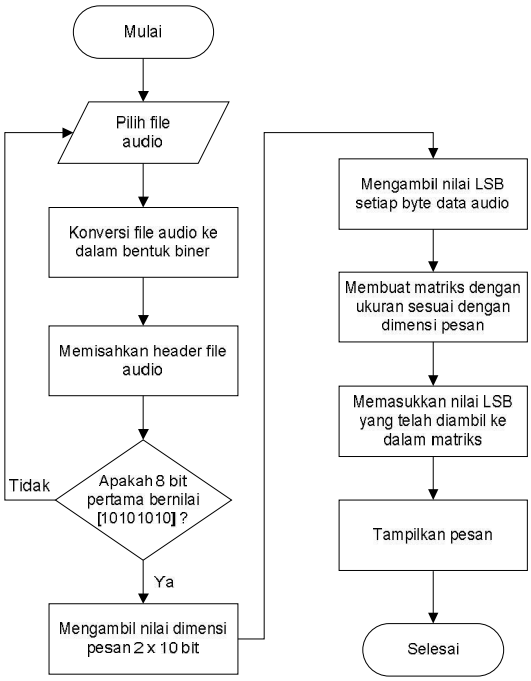
Setelah dilakukan pembuatan program simulasi, selanjutnya dilakukan perhitungan matematis dengan PSNR untuk mengetahui secara matematis nilai perbandingan data audio yang belum disisipkan pesan rahasia dengan data audio yang telah disisipkan pesan.

C. Rancangan Penerapan Algoritma LSB

Secara garis besar terbagi menjadi dua proses utama yaitu penyisipan pesan dan ekstraksi atau pendekteksian kembali pesan yang tersembunyi. Pada proses penyisipan pesan dimulai dengan memilih file audio digital yang akan dijadikan *cover object* untuk menyisipkan dan menyembunyikan pesan, kemudian mengalokasikan beberapa byte untuk *identifier* atau pengenal bahwa file audio tersebut tersebut merupakan file audio yang telah disisipi pesan dan untuk alokasi *buffer* dimensi pesan, selanjutnya penyisipan pesan ke dalam LSB setiap byte data audio. Sedangkan pada proses ekstraksi pesan dimulai dengan memilih file audio yang telah disisipi pesan, kemudian melakukan pengecekan *identifier* atau pengenal dan mengambil pesan dari LSB setiap byte data audio.
Gambaran yang jelas mengenai alur proses penyisipan dan ekstraksi pesan dapat dilihat masing-masing pada Gambar 3 dan 4 di bawah ini.



Gambar 3. Alur proses penyisipan pesan



Gambar 4. Alur proses ekstraksi pesan

IV. EKSPERIMEN DAN ANALISIS

A. Spesifikasi Perangkat Komputer

Dalam rangka melakukan penelitian tentang penerapan steganografi menggunakan algoritma LSB pada audio digital, perangkat komputer yang digunakan memiliki spesifikasi sebagai berikut:

Tabel 1 Spesifikasi perangkat computer

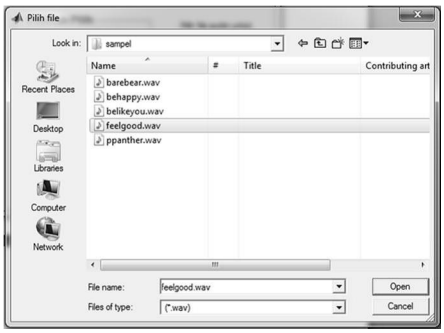
No.	Keterangan
1.	Sistem operasi: Microsoft Windows 7 Ultimate
2.	CPU: Intel Core i5 2,4 Ghz
3.	RAM: 6 GB

B. Simulasi Program

Dari hasil pemrograman yang dilakukan menggunakan MATLAB, di bawah ini merupakan GUI simulasi program yang dapat digunakan untuk melakukan steganografi atau penyembunyian pesan rahasia menggunakan data *cover* berupa audio digital.

Gambar 5. GUI simulasi program steganografi pada audio digital

Pilihan "Sembunyikan Pesan" merupakan pilihan yang digunakan untuk melakukan proses steganografi pesan rahasia menggunakan audio digital. Setelah *radio button* "Sembunyikan Pesan" dipilih selanjutnya yaitu memilih file audio yang yang akan dijadikan *cover* steganografi dengan menekan tombol "Pilih File Audio".



Gambar 6. Memilih file audio yang akan dijadikan sebagai *cover*

Setelah file audio dipilih selanjutnya masukkan pesan rahasia yang akan disisipkan pada file audio tersebut dengan mengetikkan pesan pada kolom yang telah tersedia. Selanjutnya tekan tombol "Proses Steganografi" untuk melakukan proses penyisipan pesan menggunakan algoritma LSB.

Gambar 7. Memasukkan pesan rahasia yang akan disisipkan

Selanjutnya hasil steganografi atau penyembunyian pesan akan disimpan ke dalam file audio dengan format wav dan dengan nama file "stegano[*random*].wav".

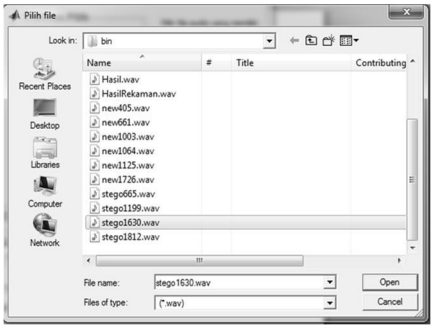
Gambar 8. Hasil proses steganografi

File tersebut kemudian dapat dikirimkan kepada pihak yang berhak untuk mengetahui pesan rahasia yang disembunyikan tersebut melalui internet (misalnya *email*). Pengirim dapat meminimalisir kekhawatiran akan jatuhnya pesan rahasia tersebut ke pihak yang tidak berhak membaca karena file audio yang dikirimkan layaknya file audio biasa sehingga tidak menimbulkan kecurigaan apabila ada pihak yang menyadap komunikasi pengiriman file tersebut.

Di sisi penerima apabila telah menerima file audio tersebut selanjutnya adalah melakukan ekstraksi pesan rahasia. Pada proses ekstraksi pesan dilakukan pertama-tama dengan memilih pilihan "Ekstrak Pesan".

Gambar 9 Memilih pilihan "Ekstrak Pesan" untuk proses ekstraksi pesan

Selanjutnya pilih file audio yang telah disisipkan pesan tersembunyi dengan menekan tombol "Pilih File Audio".



Gambar 10. Memilih file audio yang telah disisipi pesan rahasia

Kemudian pesan rahasia tersebut akan ditampilkan pada kolom yang tersedia. Proses ekstraksi dilakukan secara otomatis seketika file tersebut dibuka pada simulasi program yang dibuat.

Gambar 11. Hasil ekstraksi pesan rahasia

C. Eskperimen dan Pengujian

Sampel data yang digunakan dalam penelitian terdiri dari *cover* audio dengan format file wav sejumlah 4 buah dan pesan rahasia yang berupa karakter teks dengan masing-masing memiliki kapasitas yang berbeda. Pada prinsipnya proses penyisipan data pesan ke dalam data *cover* audio adalah data pesan dibaca nilai binernya untuk kemudian dimasukan ke LSB pada data cover audio. Adapun data yang digunakan dalam eksperimen ini dapat dilihat pada Tabel 2 dan 3 di bawah ini. Sedangkan representasi grafik dari setiap sampel data *cover* audio dapat dilihat pada Gambar 12.

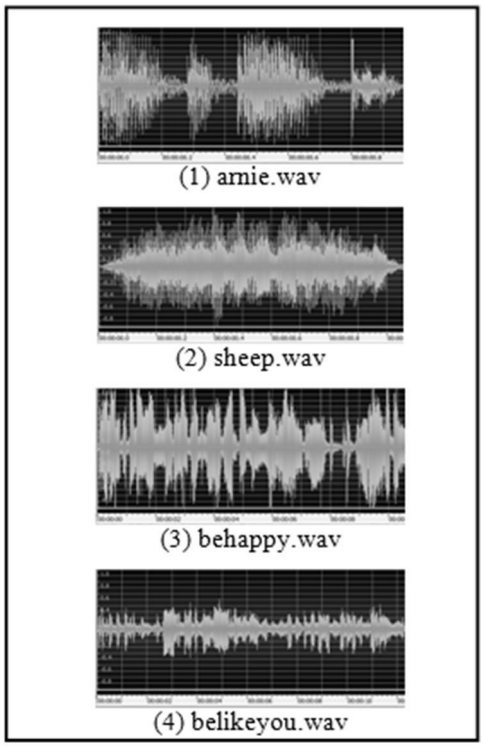
Tabel 2. Data pesan rahasia yang akan disisipkan

No.	Pesan Rahasia	Ukuran
1.	Lepaskan saja dia sebelum fajar	31 bytes
2.	Malam ini teroris akan menyerang kantor kita	44 bytes
3.	Jangan sampai salah orang, lakukan dengan bersih dan tanpa suara	64 bytes
4.	Data intelijen kita menyembutkan bahwasanya dalam tempo kurang dari 2 bulan akan ada kudeta yang dipimpin oleh ABC	114 bytes

Tabel 3. Data *cover* audio

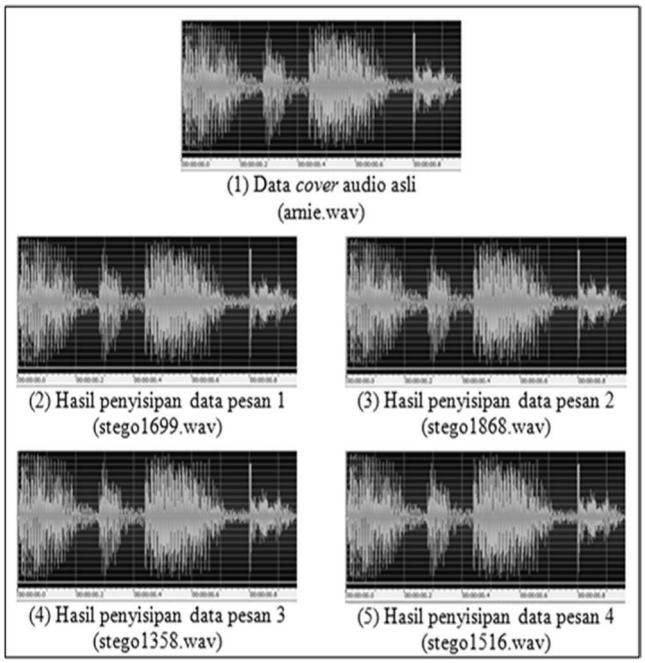
No.	File Audio	Ukuran
1.	arnie.wav	21 KB
2.	sheep.wav	23 KB
3.	behappy.wav	114 KB
4.	belikeyou.wav	265 KB

Representasi grafik dari setiap sampel data *cover* audio dapat dilihat pada Gambar 12 di bawah ini.

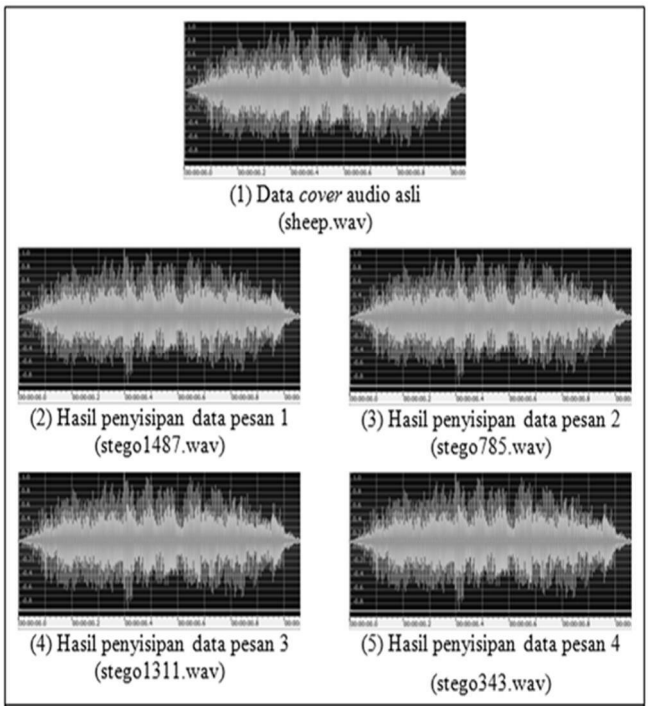


Gambar 12. Representasi grafik data *cover* audio

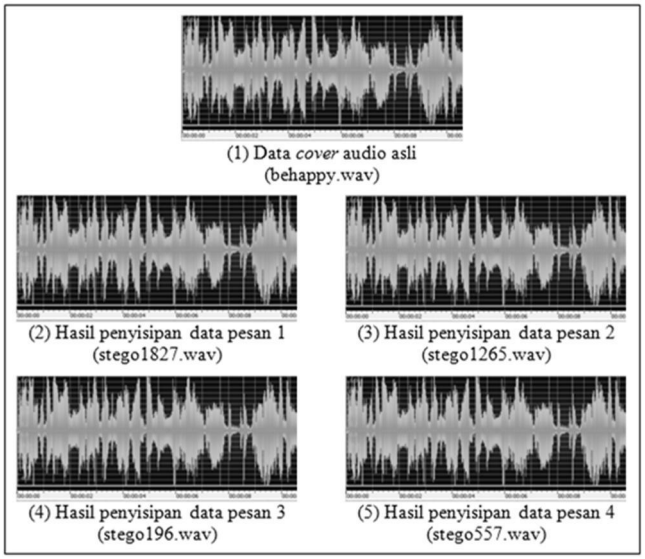
Seluruh data *cover* audio sebagaimana terlihat pada Gambar 12 di atas kemudian disisipkan oleh masing-masing data pesan rahasia.



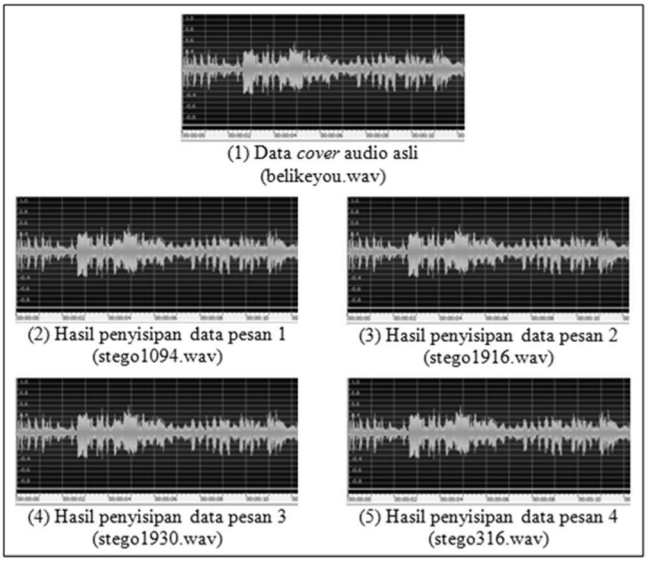
Gambar 13. Representasi grafik hasil penyisipan pesan pada file arnie.wav



Gambar 14. Representasi grafik hasil penyisipan pesan pada file sheep.wav



Gambar 15 Representasi grafik hasil penyisipan pesan pada file behappy.wav

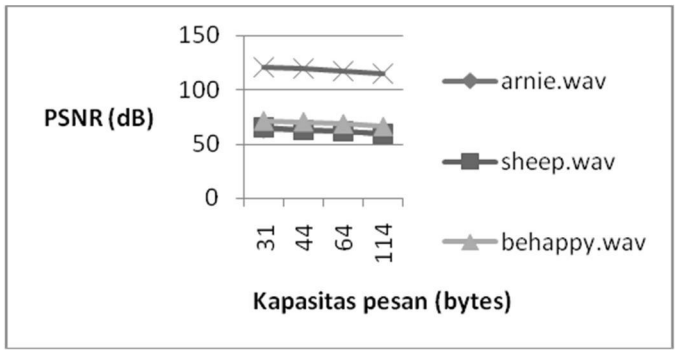


Gambar 16 Representasi grafik hasil penyisipan pesan pada file belikeyou.wav

Dari gambar representasi grafik data audio yang telah *disisipkan* pesan rahasia tersebut secara kasat mata tidak terlalu terlihat terjadi perubahan pada sinyal, hal tersebut terjadi karena proses penyisipan data pesan ke dalam LSB *cover* audio memiliki kapasitas yang tidak terlalu signifikan. Di bawah ini adalah nilai PSNR yang dihasilkan dari perbandingan *cover* audio asli dengan audio yang telah disisipi pesan (*stego* audio).

Tabel 4 Nilai PSNR

No.	*Cover* Audio	*Stego* Audio	Pesan	Nilai PSNR
1.	arnie.wav	stego1699.wav	1	64,11 dB
		stego1868.wav	2	62,61 dB
		stego1358.wav	3	61,39 dB
		stego1516.wav	4	58,94 dB
2.	sheep.wav	stego1487.wav	1	65,13 dB
		stego785.wav	2	62,83 dB
		stego1311.wav	3	61,78 dB
		stego343.wav	4	59,08 dB
3.	behappy.wav	stego1827.wav	1	71,36 dB
		stego1265.wav	2	70,49 dB
		stego196.wav	3	68,61 dB
		stego557.wav	4	66,06 dB
4.	belikeyou.wav	stego1094.wav	1	120,44 dB
		stego1916.wav	2	118,90 dB
		stego1930.wav	3	117,38 dB
		stego316.wav	4	114,87 dB



Gambar 17 Grafik perbandingan nilai PSNR terhadap kapasitas pesan yang disisipkan

Dari hasil percobaan di atas terhadap lima buah file *cover* audio yang disisipkan pesan dengan kapasitas yang bervariasi serta jumlah karakter yang terus ditambahkan pada setiap pengujiannya yakni dari 31, 44, 64 dan 114 bytes diperoleh hasil nilai desibel dari masing-masing *cover* audio yang berbeda untuk setiap jumlah karakter yang disisipkan.

Hasil pengujian nilai PSNR dari setiap *cover* audio yang diuji dapat dilihat dari tabel di atas dan grafik perbandingan nilai PSNR terhadap jumlah kapasitas pesan yang disisipkan dapat pula dilihat pada Gambar IV.13 dari grafik tersebut terlihat jelas bahwa jumlah karakter yang disisipkan pada setiap *cover* audio berpengaruh terhadap nilai PSNR yang dihasilkan atau dengan kata lain *cover* audio yang digunakan mengalami perubahan sesuai dengan jumlah karakter yang disisipkan ke dalamnya. Semakin banyak karakter yang disisipkan maka semakin berkurang pula kualitas audio yang dihasilkan.

Hal ini ditandai dengan berkurangnya nilai PSNR yang dihasilkan oleh masing-masing *cover* audio, dimana dari uji coba pengujian penyisipan karakter dengan jumlah karakter yang berbeda-beda, diperoleh hasil PSNR yang semakin berkurang sesuai dengan banyaknya karakter yang disisipkan, seperti pada file audio belikeyou.wav dimana pada penyisipan 31 karakter diperoleh nilai PSNR 120,44 dB dan nilai PSNR yang semakin menurun sesuai dengan banyaknya karakter yang disisipkan sampai dengan 114,87 dB pada penyisipan 114 karakter.

Besarnya ukuran file *cover* audio juga mempengaruhi perolehan nilai PSNR. Nilai PSNR yang dihasilkan dari keempat file *cover* audio bervariasi sesuai dengan ukuran file *cover* audio yang digunakan, seperti yang terlihat pada Tabel 4.3 bahwa nilai PSNR yang dihasilkan semakin berkurang sesuai dengan besar ukuran file audio yang digunakan dengan jumlah penyisipan karakter yang sama, hal ini dapat dilihat pada file audio belikeyou.wav yang memiliki kapasitas sebesar 265 KB dengan file audio sheep.wav yang memiliki kapsitas 23 KB dimana pada dengan penyisipan pesan 31 karakter pada file audio belikeyou.wav diperoleh nilai PSNR sebesar 120,44 dB sedangkan pada file audio sheep.wav diperoleh nilai PSNR sebesar 65,13 dB.

Dari hasil uji coba proses ekstraksi pesan yang terdapat pada file audio dalam aplikasi steganografi menggunakan algoritma LSB ini, pesan atau informasi yang disisipkan pada file audio dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan atau gangguan yang menyebabkan isi pesan tidak dapat diperoleh sepenuhnya.

Hal ini membuktikan bahwa pada aplikasi steganografi yang dibuat ini menghasilkan hasil yang cukup baik untuk setiap penyembuyian pesan k edalam file audio bergantung dari pemilihan *cover*-object atau file audio yang akan digunakan dan banyaknya karakter yang disisipkan pada file audio, karena semakin besar ukuran file audio yang digunakan dan semakin sedikit karakter yang disisipkan pada file audio maka semakin sedikit perubahan yang terjadi setelah proses penyisipan pada file audio atau kualitas sebelum penyisipan dan setelah penyisipan tidak berpengaruh banyak pada perubahan kualitas *cover* audio.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari penelitian ini maka dapat disimpukan bahwa aplikasi steganografi yang telah diterapkan menggunakan algoritma LSB pada audio digital dapat digunakan dengan baik untuk menyembunyikan pesan sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Pada proses ekstraksi, pesan atau informasi yang disisipkan pada file audio dalam aplikasi steganografi ini, dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan atau gangguan yang menyebabkan isi pesan tidak dapat diperoleh sepenuhnya.

Hasil pengujian nilai PSNR terhadap file audio yang dihasilkan dari aplikasi steganografi inipun menunjukkan nilai yang cukup baik bergantung pada besar ukuran file audio yang digunakan dan besarnya jumlah karakter yang disisipkan pada file audio tersebut. Semakin besar kapasitas file audio yang digunakan maka semakin baik nilai PSNR yang diperoleh dibandingkan dengan file audio yang berukuran lebih kecil dengan jumlah sisipan karakter yang sama. Hal ini menunjukkan bahwa untuk memperoleh file audio yang baik setelah proses penyisipan, dan tidak mengalami perubahan yang cukup berarti dari file audio sebelumnya maka kapasitas file audio dan banyaknya karakter yang akan disisipkan perlu diperhatikan untuk memperoleh hasil yang baik. Dengan demikian pesan rahasia yang disisipkan ke dalam file audio tidak akan menimbulkan kecurigaaan dan menjaga keamanan pesan rahasia yang disisipkan dalam file audio tersebut.

B. Saran

Pada aplikasi steganografi ini, file audio yang dihasilkan setelah proses penyisipan mengalami pengurangan kualitas yang cukup banyak bergantung dari jumlah karakter yang disisipkan, dimana semakin banyak karakter yang disisipkan maka semakin besar pula pengurangan kualitas audio yang diperoleh yang ditandai dengan pengurangan nilai PSNR. Oleh karena itu, untuk meningkatkan kualitas audio yang dihasilkan maka ke depannya diharapkan dapat dikembangkan suatu aplikasi steganografi dengan metode lain yang lebih baik agar kualitas audio yang dihasikan tidak jauh berbeda dengan kualitas *cover* audio.

Selain itu, untuk memenuhi tuntutan perkembangan jaman teknologi informasi, maka penelitian ini dapat dilanjutkan untuk membangun program aplikasi penerapan steganografi dengan algoritma LSB dalam pengamanan informasi yang diimplementasikan pada berbagai perangkat termasuk *mobile device*.

DAFTAR PUSTAKA

[1] Alatas, Putri, "Implementasi Teknik Steganografi Dengan Metode LSB pada Citra Digital" Bachelor Thesis, Universitas Gunadarma, Depok, 2009.

[2] Bakshin, Nishesh., *Steganography*, Syracuse University, 2007.

[3] Cummins J., et al., *Steganography and Digital Watermarking*, School of Computer Science, The University of Birmingham, 2004.

[4] Jaya, Danang., "Perbandingan Algoritma Tipe Blind Dan Non Blind Pemberian Tanda Air Pada Citra Digital Berbasis Singular Value Decomposition", Depok, Universitas Indonesia, 2007.

[5] Kharrazi, Mehdi., *Image Steganography: Concept and Practice*, Polytechnice University, Brooklyn USA: 2004.

[6] Mohanty, S. P., *Digital Watermarking: A Tutorial Review*, 1999.

[7] Pakereng, MA. Ineke., et.al., "Perbandingan Steganografi Metode Spread Spectrum dan Least Significant Bit (LSB) Antara Waktu Proses dan Ukuruan File Gambar", *Jurnal Informatika*, vol. 6, (April, 2010): 68-86.

[8] Prasetyo, Bambang dan Jannah, Lina Miftahul., Metode Penelitian Kuantitaif, Jakarta: PT. Rajagrafindo Persada, 2005.

[9] Saputra, Hasbian., et.al., "Implementasi Algoritma Steganografi Embedding Dengan Metode Least Significant Bit (LSB) Insertion dan Huffman Coding Pada Pengiriman Pesan Menggunakan Media MMS Berbasis J2ME", Institut Teknologi Sepuluh Nopember (ITS) Surabaya, Surabaya, 2011.

[10] Setyawan, Henry., et.al., "Implementasi Steganografi Dengan Metode Least Significant Bit (LSB)", *Jurnal Rekayasa Elektrika*, vol. 8, (April, 2009): 8-13.