
APLIKASI STEGANOGRAFI DENGAN METODE SPREAD SPECTRUM PADA FILE WAVE

Yeni Risyani¹⁾, Edy M²⁾

STMIK IBBI

Jl. Sei Deli No. 18 Medan, Telp. 061-4567111 Fax. 061-4527548

e-mail: sukses7296@gmail.com, edy@yahoo.com

Abstrak

Keamanan dalam pengiriman informasi yang bersifat rahasia merupakan salah satu faktor penting yang harus dijaga. Salah satu teknik yang dapat dipakai untuk menangani hal tersebut adalah steganografi. Steganografi merupakan ilmu dan seni yang mempelajari cara menyembunyikan informasi rahasia ke dalam suatu media sehingga manusia tidak dapat menyadari keberadaan pesan tersebut. Media yang umumnya digunakan berupa media digital seperti citra, audio dan video. Pada steganografi terdapat beberapa metode dalam penyisipan pesan, salah satu di antaranya adalah metode spread spectrum. Metode spread spectrum dalam steganografi diilhami dari sistem komunikasi spread spectrum, yang melakukan penyebaran spectrum sinyal informasi dalam bandwidth yang jauh lebih lebar dibanding bandwidth sinyal informasi pada umumnya. Kegunaan dari penyebaran ini adalah untuk mengurangi kekhawatiran penyadapan karena data yang dikirimkan bersifat acak dan memiliki kecenderungan sifat seperti noise. Sebagai hasil akhir steganografi adalah perancangan sebuah perangkat lunak untuk implementasi steganografi dengan metode spread spectrum pada file audio wave.

Kata kunci: *Steganografi, Spread Spectrum, Bandwidth, Noise, File Audio Wave.*

Abstract

Security in transmission of confidential information is one important factor that must be maintained. One technique that can be used to deal with such matters is steganography. Steganography is the art and science which studies how the concealment of confidential information to the media so that a man can not realize the existence of the message. Media commonly used form of digital media such as images, audio and video. On steganography there are several methods in the insertion of messages, one of which is the method of spread spectrum. Spread spectrum steganography method inspired in spread spectrum communication system, the dissemination of information in the signal spectrum is much wider bandwidth than the information signal bandwidth in general. The usefulness of this deployment is to reduce fears tapping because transmitted data is random and has a tendency of properties like noise. As a final result steganography is a software design to implementation of spread spectrum steganography method in audio wave file.

Keywords: *Steganography, Spread Spectrum, Bandwidth, Noise, Wave Audio Files.*

1. Pendahuluan

Pengamanan data dalam bidang komputer memegang peranan yang penting dan merupakan suatu keharusan. Pengamanan data lebih diperlukan lagi mengingat data kadang-kadang ditransfer melalui jaringan yang tidak aman seperti *Internet*. Teknik *kriptografi* digunakan untuk melakukan pengacakan data, teknik yang lain adalah menyembunyikan data atau informasi ke dalam data yang lain, terakhir dikenal sebagai steganography.

Steganography adalah teknik menyisipkan pesan kedalam suatu media, dimana pesan rahasia yang akan dikirimkan tidak diubah bentuknya, melainkan disisipkan pada sebuah media lain (*cover object*). Media yang umumnya digunakan berupa media *digital* seperti *citra*, *audio* dan *video*.

Walaupun *steganografi* dapat dikatakan mempunyai hubungan yang erat dengan *kriptografi*, sebenarnya *steganografi* sangat berbeda dengan *kriptografi*. *Kriptografi* mengacak pesan sehingga tidak dimengerti, sedangkan *steganografi* menyembunyikan pesan sehingga tidak terlihat.

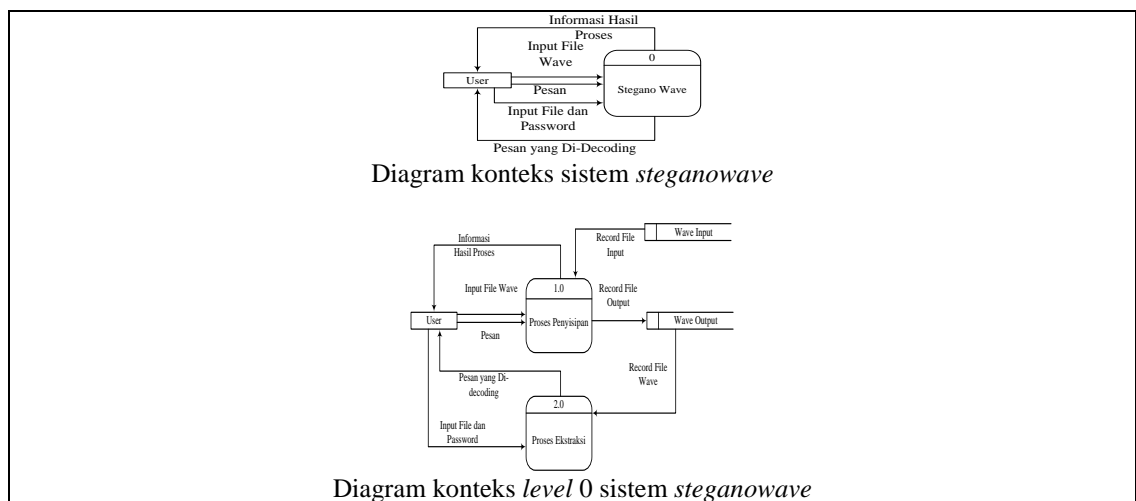
Pada *steganografi* terdapat beberapa metode dalam penyisipan pesan, salah satu di antaranya adalah metode *spread spectrum*. Metode *spread spectrum* dalam *steganografi* diilhami dari sistem komunikasi *spread spectrum*, yang melakukan penyebaran *spectrum* sinyal informasi dalam *bandwith* yang jauh lebih lebar dibanding *bandwith* sinyal informasi pada umumnya. Kegunaan dari penyebaran ini adalah untuk mengurangi kekhawatiran penyadapan karena data yang dikirimkan bersifat acak dan memiliki kecenderungan sifat seperti *noise*.

2. Metodologi Penelitian

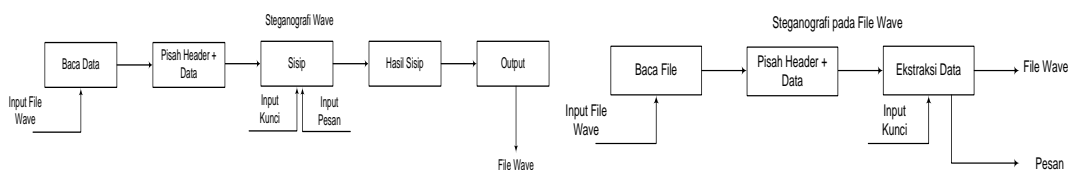
Metodologi penelitian dilakukan dengan mengumpulkan data terlebih dahulu. Proses pengumpulan data dilakukan adalah studi kepustakaan. Studi kepustakaan dilakukan untuk memahami proses perancangan sistem informasi seperti mengumpulkan teori-teori yang berhubungan dengan perancangan sistem, metode dan steganografi.

Metode yang dipergunakan adalah metode Spread spectrum. Spread spectrum adalah teknik pembangkitan sinyal (elektrik, elektromagnetik atau akustik) yang dengan sengaja disebar pada rentang bandwidth yang lebih lebar dari yang seharusnya. Teknik ini dilakukan dengan berbagai alasan, diantaranya untuk jaringan komunikasi yang aman, memperkuat gelombang yang dikirim terhadap interferensi atau jamming dan menghindari pendeteksian. Spread spectrum pada awalnya adalah teknik yang digunakan untuk komunikasi gelombang radio untuk alasan keamanan dan menghindari jamming. Sinyal radio yang dikirimkan sengaja disebar pada rentang frekuensi yang lebih lebar. Hasil sinyal radio yang ditangkap hanya terlihat sebagai noise biasa (static noise) dan tidak dapat diinterpretasi dengan cara biasa. Spread spectrum memiliki kelebihan yang sangat penting, yaitu ketahanannya terhadap jamming dan interferensi. Andaikata sinyal yang dibuat mengalami kerusakan ditengah jalan, informasi yang disampaikan masih dapat dipersepsi. Sifat ini cocok digunakan untuk steganografi audio yang format filenya mungkin mengalami kompresi, terutama kompresi lossy seperti MP3.

Metode perancangan yang dilakukan terdiri dari perancangan diagram konteks, diagram blok dan perancangan database



Gambar 1. Diagram konteks sistem steganowave



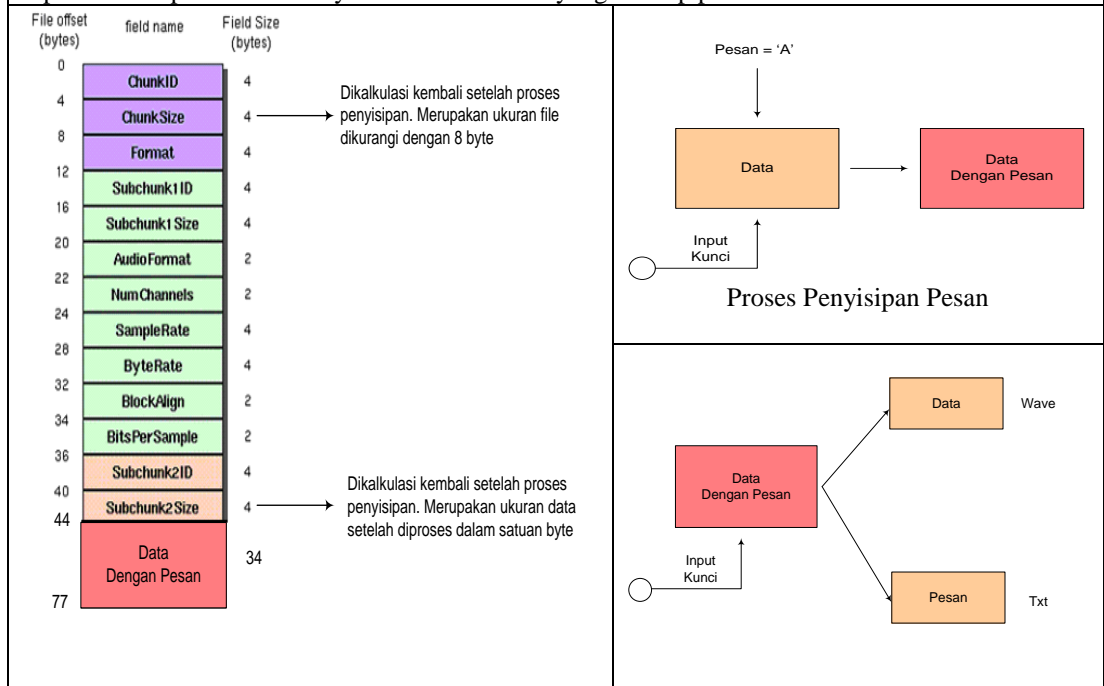
Gambar 2. Diagram blok proses penyisipan pada file audio

Tabel 1. Contoh file audio wave yang mempunyai panjang 72 byte

File offset (bytes)	field name	Field Size (bytes)	File offset (bytes)	field name	Field Size (bytes)
0	ChunkID	4	0	ChunkID	4
4	ChunkSize	4	4	ChunkSize	4
8	Format	4	8	Format	4
12	Subchunk1ID	4	12	Subchunk1ID	4
16	Subchunk1 Size	4	16	Subchunk1 Size	4
20	AudioFormat	2	20	AudioFormat	2
22	NumChannels	2	22	NumChannels	2
24	SampleRate	4	24	SampleRate	4
28	ByteRate	4	28	ByteRate	4
32	BlockAlign	2	32	BlockAlign	2
34	BitsPerSample	2	34	BitsPerSample	2
36	Subchunk2ID	4	36	Subchunk2ID	4
40	Subchunk2 Size	4	40	Subchunk2 Size	4
44	data	28	43	Subchunk2 Size	4
71					

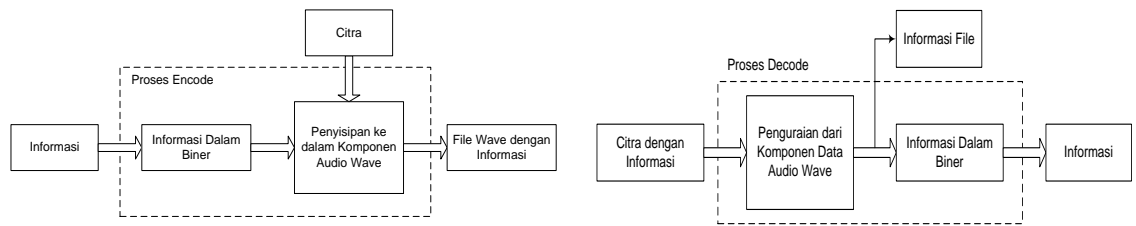
Pembacaan Seluruh Isi File Proses Ekstraksi

Pada saat pembacaan seluruh isi file wave yaitu 72 byte akan dibaca seluruhnya dan hasilnya akan ditampung ke sebuah variabel sementara. Pada proses ekstraksi akan dipisahkan bagian header dari file wave dan bagian datanya. Hasil proses ekstraksi ini akan disimpan ke dua variabel yang terpisah yaitu WaveHeader dan WaveData. Selanjutnya adalah bagian data ini akan dibaca dikonversikan ke dalam bentuk string untuk diproses dengan teknik penyisipan spread spectrum. Input kunci diperlukan hasilnya adalah data wave yang tersisip pesan.



Proses Penyimpanan Proses Ekstraksi Pesan

Setelah selesai bagian yang data telah diproses akan digabungkan kembali dan kemudian hasilnya disimpan dalam bentuk format wave. Sebelum file disimpan maka pada bagian ChunkSize dan Subchunk2Size akan dihitung nilainya kembali baru kemudian seluruh hasilnya disimpan. Untuk proses ekstraksi langkah-langkah prosesnya sama, hanya berbeda pada bagian penyisipan (teknik spread spectrum dilakukan secara terbalik untuk menghasilkan pesan kembali)



Gambar 3. Diagram blok penyisipan dan pembacaan informasi pada *file wave*

Proses penyisipan informasi ke dalam *file wave* dimulai dengan mengubah informasi ke dalam bentuk biner. *Bit-bit* informasi tersebut kemudian disisipkan ke dalam tiap data wave sesuai dengan bit-bit informasi. Proses ini akan diulang hingga seluruh informasi termuat ke dalam *data audio wave*.

Proses pembacaan informasi dilakukan dengan cara mengambil bit terakhir dari tiap komponen *data audio*. Proses ini dilakukan berulang hingga semua informasi terkumpul. Semua informasi yang telah terkumpul tersebut kemudian diubah ke dalam kode ASCII (*American Standard Code for Information Interchange*) dan siap ditulis ke dalam bentuk informasi kembali sesuai dengan bentuk dan format aslinya.

3. Analisis dan Hasil

3.1. Analisis Ukuran File Wave dengan Ukuran File Pesan

Proses dari pengujian ini adalah pertama menyisipkan pesan ke *audio*, kemudian akan dilakukan pengecekan terhadap ukuran *file wave* dan ukuran pesan yang akan disisipkan. sistem dapat melakukan pengecekan ukuran *file wave* dan ukuran pesan sebelum melakukan penyisipan. Pada proses penyisipan pesan yang berhasil dilakukan, ukuran *file wave output* mengalami penambahan sebesar 4 *byte* karena dilakukan penyimpanan *pseudonoise signal* pada *file wave* tersebut.

Tabel 2. Tabel ukuran file

No.	Nama File Wave	Ukuran File (byte)	Ukuran File Output (byte)	Kunci	Ukuran Pesan (byte)	Status
1.	Windows XP Menu Command.wave	1.404	1.408	Steganografi	165	Berhasil
2.	Ringout.wave	5.212	5.214	Steganografi	165	Berhasil
3.	Windows XP Balloon.wave	6.400	6.404	Steganografi	2564	Berhasil
4.	Ringin.wave	10.026	10.026	Steganografi	12.500	Gagal
5.	Windows XP Ringout.wave	22.070	22.070	Steganografi	25.000	Gagal

3.2 Analisis Penyisipan dan Ekstraksi Pesan dengan kunci yang sama

Proses pengujian ini dilakukan dengan menyisipkan pesan ke dalam *audio*, kemudian akan dilakukan ekstraksi untuk mendapatkan kembali pesan. *File wave* yang akan digunakan pada pengujian ini adalah *Windows XP Menu Command.wave* dengan ukuran file 1.404 *byte*. Kunci yang digunakan adalah 'Steganografi'.

Tabel 3. Analisis penyisipan pesan

Nama File Wav	: Windows XP Menu Command.wave
Kunci	: Steganografi
Ukuran File (byte)	: 1.404
Ukuran File Output (byte)	: 1.408
Ukuran Pesan (byte)	: 165
Pesan yang akan disisipkan	: Steganografi merupakan seni untuk mempelajari cara menyembunyikan pesan rahasia ke dalam suatu media sedemikian sehingga pihak ketiga tidak menyadari keberadaan pesan tersebut

Tabel 4. Analisis ekstraksi pesan

Nama File Wav	: Windows XP Menu Command.wav
Kunci	: Steganografi
Ukuran File (byte)	: 1.408
Pesan yang diperoleh	: Steganografi merupakan seni untuk mempelajari cara penyembunyian pesan rahasia ke dalam suatu media sedemikian sehingga pihak ketiga tidak menyadari keberadaan pesan tersebut

Hasil analisis : terbukti bahwa sistem dapat melakukan penyisipan dan ekstraksi dengan benar.

3.3 Analisis Penyisipan dan Ekstrasi Pesan dengan kunci yang berbeda

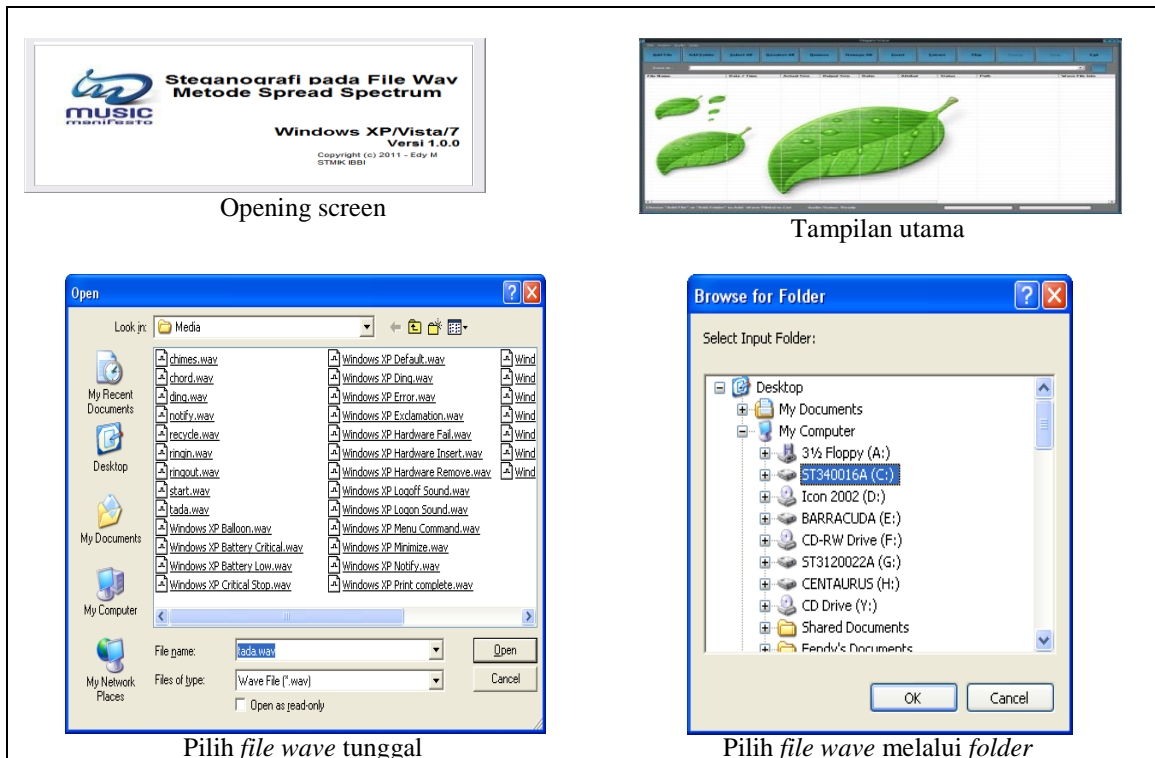
Analisis proses ekstraksi dengan menggunakan kunci yang salah yaitu 'Kriptografi', sehingga akan dihasilkan pesan yang berbeda.

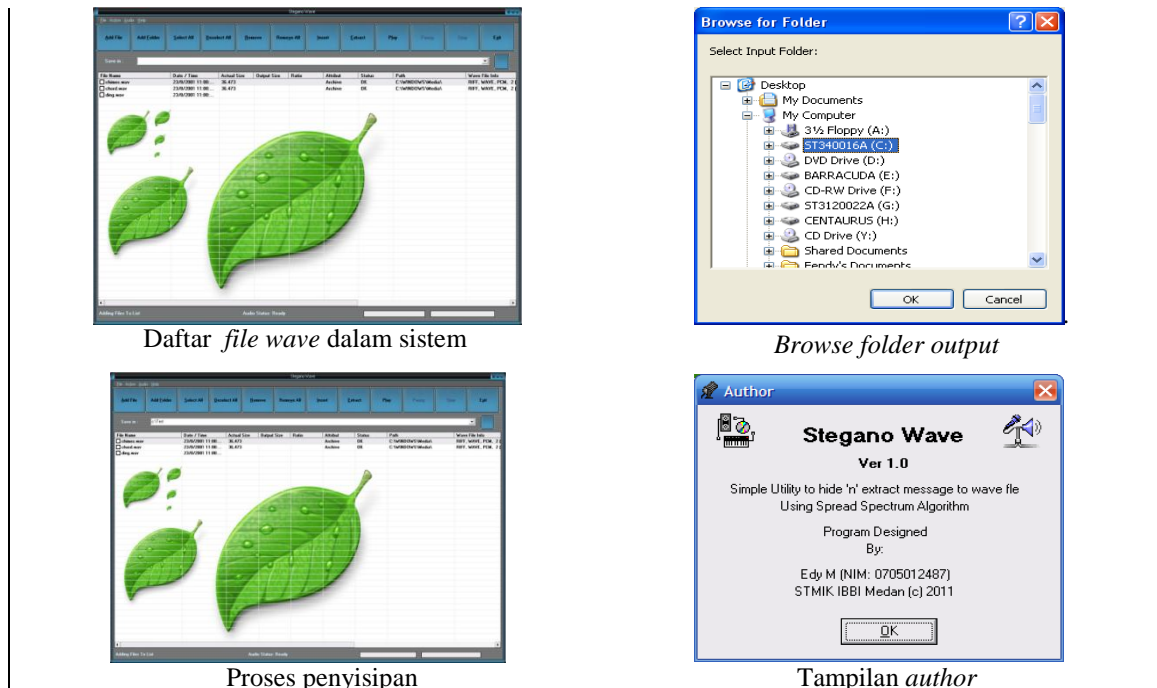
Tabel 5. Analisis ekstraksi dengan kunci yang salah

Nama File Wav	: Windows XP Menu Command.wav
Kunci	: Kriptografi
Ukuran File (byte)	: 1.408
Pesan yang diperoleh	: Znö8\jİ7Ö"'+nVø_Ü£>- ßÖœ_āNÊZD-ü□%oiÓ+iØ_~kδβ³~δ'¹çzLÚÛ²_Í_Ç° Ÿ7δ{□_µmÊ†δ_δ_Æ;øf²('uÔaù~5ËC;À©_€_sØ³_%o,_S«È_% _Öüë†ùÄ□(á;¶,□2D"©†LÎt}œPCE VQ^OB6exÁic%o• 9a_ b[r*raOt_V¶MŠœ

Hasil analisis : terbukti bahwa perangkat lunak dapat melakukan aspek pengamanan dengan kunci. Proses ekstraksi dengan kunci yang berbeda menghasilkan pesan yang salah yaitu pesan yang tidak dapat terbaca dikarenakan menggunakan kunci yang berbeda, maka proses ekstraksi mengalami kesalahan *decoding* pesan.

3.4 Tampilan Hasil Implementasi





Gambar 4.

4. Kesimpulan dan Saran

Kesimpulan yang dapat ditarik oleh peneliti adalah sebagai berikut : steganografi dengan metode *spread spectrum* dapat diterapkan pada *file audio wave*. *Data audio* pada *file wave* yang telah disisipi pesan tidak dapat dikembalikan ke *data audio* semula karena pada proses penyisipan tidak dilakukan penyimpanan *data audio* aslinya, *SteganoWave* hanya memanfaatkan *data audio* dari berkas *wave*. Oleh karena itu perlu untuk dilakukan pengembangan dengan memanfaatkan data lain, sehingga diharapkan dapat menambah kapasitas data yang dapat disembunyikan misalnya data *bitmap* ataupun dari dokumen *word*. Untuk pengembangan lebih lanjut, peneliti menyarankan sebagai berikut : *SteganoWave* memanfaatkan *data audio* yang ditulis secara sekuensial dalam berkas, yang mungkin tidak sesuai dengan urutan waktu. Oleh karena itu perlu pengembangan agar proses penyisipan ini urutannya disesuaikan dengan urutan waktu dari setiap *data audio*, kembangkan lebih lanjut agar dapat digunakan dalam lingkungan perangkat keras *mobile* seperti telepon genggam, *data audio file wave* yang telah disisipi pesan dapat dikembalikan ke bentuk data awal sehingga proses penyisipan bersifat *lossless*.

Buku Teks :

- [1] Agus, Susanto. Studi dan Implementasi Steganografi pada Berkas MIDI. Departemen Teknik Informatika. Bandung: Institut Teknologi Bandung.
- [2] Andreas, Westfeld, Andreas Pfitzmann. Attacks on Steganographic: Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools - and Some Lessons Learned. Dresden University of Technology Department of Computer Science D-01062 Dresden. Germany. 2004.
- [3] Basalamah, Affah. Teknologi Multimedia MP3. Jakarta: PT. Elex Media Komputindo. 2001.
- [4] Bruce, Schneier. Crypto-Gram Newsletter. Counterpane Internet Security.
- [5] Flikkema, Paul G. Spread Spectrum Techniques for Wireless Communications. IEEE Signal Processing. 14(3):26-36. 1997.
- [6] [8] Munir, Rinaldi. Pengolahan Citra Digital dengan Pendekatan Algoritmik. Bandung: Penerbit Informatika. 2004.
- [7] Neil, F. Johnson, Sushil Jajodia. Exploring Steganography: Seeing the Unseen. George Mason University. 1998.
- [8] Niels, Provos and Peter Honeyman. Detecting Steganographic Content on the Internet. Center for Information Technology Integration University of Michigan. 2001.
- [9] Stefan, Hettzl, A Survey of Steganography. January 2002.