STUDI DAN IMPLEMENTASI STEGANOGRAFI PADA *FILE* AUDIO DENGAN TEKNIK *SPREAD SPECTRUM*

Vipkas Al Hadid Firdaus[1], Ali Mustofa, ST., MT.[2], Ir. Muhammad Aswin, MT. [2]
[1]Mahasiswa Teknik Elektro Univ. Brawijaya, [2]Dosen Teknik Elektro Univ. Brawijaya
Jurusan Teknik Elektro Fakultas Teknik Universitas Brawijaya
Jalan MT. Haryono 167, Malang 65145, Indonesia
E-mail: ubvipkas@gmail.com

***Abstract*— The development of information has grown so rapidly. Messages, data, or information that is so easily accessible to everyone today, and the need for the transmission of information via internet poses a new problem that the security aspects of the data itself. So, comes a method of securing data is known as steganography. Steganography is one of solution for protecting confidential messages are delivered via Internet in a way to hide the message so that the message of the steganography process will not be visible and will not arouse suspicion. Spread Spectrum is one method that can be used in a steganography technique on digital audio media files in a transform domain.**

***Index Terms*— Steganography, Spread Spectrum, Digital Audio, WAV.**

***Abstrak*– Perkembangan informasi telah berkembang begitu pesat. Pesan, data, atau informasi yang begitu mudah diakses oleh setiap orang saat ini dan kebutuhan akan pengiriman informasi lewat media internet menimbulkan sebuah permasalahan baru yaitu aspek keamanan dari data itu sendiri. Sehingga muncullah sebuah metode pengamanan data yang di kenal dengan istilah steganografi. Steganografi adalah salah satu solusi untuk melindungi pesan yang bersifat rahasia yang disampaikan melalui internet dengan cara menyembunyikan pesan sehingga pesan dari proses steganografi ini tidak akan terlihat dan tidak akan menimbulkan kecurigaan. *Spread Spectrum* merupakan salah satu metode yang dapat digunakan dalam teknik steganografi pada media berkas audio *digital* dalam *domain transform*.**

***Kata Kunci*- Steganografi, *Spread Spectrum*, Audio *Digital*, WAV.**

I. PENDAHULUAN

Steganografi adalah metode paling populer saat ini untuk mengatasi masalah keamanan data, yaitu sebuah seni dan ilmu menyembunyikan pesan dengan suatu cara pada media lain sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Media tempat menyisipkn pesan dalam steganografi disebut *cover-object*. *Cover-object* yang digunakan bisa bermacam-macam misalnya pada arsip citra. Namun penggunaan cover object citra sebagai media penyisipan pesan ini sudah banyak dibuat dan dikembangkan sedangkan penggunaan media arsip suara (audio) relatif jarang.

Pada penelitian terdahulu penyisipan pesan pada arsip suara ini sudah di kembangkan dengan menggunakan metode steganografi yang cukup sederhana yaitu LSB. Metode tersebut bekerja dengan cara mengganti *least significant bit* dari setiap sampling point dengan rentetan bit *binary* dari data yang disembunyikan. Namun pada penggunaan metode LSB tersebut *noise* yang dihasilkan pada arsip suara lebih besar. Sehingga untuk meningkatan kualitas dari proses steganografi pada audio tersebut diusulkanlah penggunaan teknik *spread spectrum* dalam proses steganografi tersebut.

Spread spectrum adalah teknik pembangkitan sinyal yang dengan sengaja disebar pada rentang *bandwitch* yang lebih besar dari yang seharusnya. Metode ini pada awalnya adalah teknik yang digunakan untuk komunikasi gelombang radio untuk alasan keamanan dan menghindari jamming. Sinyal radio yang dikirim sengaja disebar pada rentang frekuensi yang lebih lebar. Hasil sinyal radio yang ditangkap hanya akan terlihat sebagai *noise* biasa dan tidak akan dapat diinterpretasi dengan cara biasa. Karena sifat-sifat tersebut, sehingga metode ini sangat cocok digunakan pada steganografi audio. Arsip yang akan digunakan

dalam hal ini adalah berformat WAV, arsip mentah suara yang umum berformat microsoft WAV 16 bit PCM.

II. TINJAUAN PUSTAKA

A. Audio *Digita* WAV

WAV disebut dengan sebutan singkat untuk Waveform Audio Format. standar format file audio yang dikembangkan oleh Microsoft dan IBM. WAV merupakan varian dari format bitstream RIFF dan mirip dengan format IFF dan AIFF yang digunakan komputer Amiga dan Macintosh.

Baik WAV maupun AIFF kompatibel dengan operating system Windows dan Macintosh. meski WAV dapat menampung audio dalam bentuk terkompresi, umumnya format WAV merupakan audio yang tidak terkompresi. Sehingga jika ingin menyimpan dan dapat terbaca oleh sebuah komputer maka suara tersebut harus disimpan dalam bentuk digital hal ini bisa dilakukan dengan mengambil sampel sejumlah bagian gelombang per detiknya, lalu disimpan ke computer dalam bentuk format WAV .

Jenis format Wave ini merupakan jenis file Wave yang paling umum dan hampir dikenal oleh setiap program. Format Wave PCM (Pulse Code Modulation) adalah file wave yang tidak terkompresi, akibatnya ukuran file sangat besar jika file mempunyai durasi yang panjang.

Pada audio berformat WAV ini terdiri atas 2 buah SubChunk2 yaitu: “fmt ” dan “data”. Dalam hal ini SubChunk “fmt “ menggambarkan format data sound sedangkan SubChunk “data” terdiri atas ukuran besar data dan data sound sebenarnya. Berikut ini adalah format file WAV.

B. *Linier Congretial Generator*

Linear Congruental Generator (LCG) adalah salah satu algoritma pembangkitan bilangan *pseudo random*. Deret bilangan *Pseudo Random* adalah deret bilangan yang kelihatan acak dengan kemungkinan pengulangan sangat kecil. Algoritma ini merupakan pembangkit bilangan acak yang sederhana yang diciptakan oleh D. H.Lehmer pada tahun 1951. Deret bilangan bulat dalam LCG diformulasikan sebagai berikut :

$Xn = (aXn – 1 + b) \bmod m$

Dengan :

Xn = bilangan acak ke-n dari deretnya

Xn-1 = bilangan acak sebelumnya

a = faktor pengali

b = increment

m = modulus

Untuk memulai bilangan acak ini dibutuhkan sebuah bilangan bulat X0, yang dijadikan sebagai nilai awal (bibit pembangkitan). Bilangan acak pertama yang dihasilkan selanjutnya menjadi bibit pembangkitan bilangan bulat acak selanjutnya. Jumlah bilangan acak yang tidak sama satu sama lain (unik) adalah sebanyak m. Semakin besar nilai m, semakin kecil kemungkinan akan dihasilkan nilai yang sama.

Dengan demikian nilai X0 terdefinisi pada :

$0 = X_0 = n-1$, $n = 1, 2, 3, \ldots$

C. *Fast Fourier Transform*

Pada tahun 1960, J. W. Cooley dan J. W. Tukey, berhasil merumuskan suatu teknik perhitungan algoritma Fourier Transform yang efisien. Teknik perhitungan algoritma ini dikenal dengan sebutan *Fast Fourier Transform* atau lebih populer dengan istilah FFT yang diperkenalkan oleh J.S.Bendat dan A.G.Piersol pada 1986. *Fast Fourier Transform* adalah Transformasi Fourier Cepat yang merupakan sumber dari suatu algoritma untuk menghitung *Discrete Fourier Transform* (transformasi *fourier diskrit* atau DFT) dengan cepat, efisien dan inversnya.

DFT merupakan metode transformasi matematis untuk sinyal waktu diskrit ke dalam domain frekuensi. Secara sederhana dapat dikatakan bahwa DFT merupakan metode transformasi matematis sinyal waktu diskrit, sementara FFT adalah algoritma yang digunakan untuk melakukan transformasi tersebut.

Secara matematis, DFT dapat dirumuskan sebagai berikut :

$$X[k] = \sum_{n=0}^{N-1} x[n].W_N^{nk} \quad ; k = 0,1,2,\ldots,N-1$$

Sementara itu, transformasi balikan atau *Inverse Discrete Fourier Transform* (IDFT) dapat dirumuskan sebagai berikut :

$$x[n] = \frac{1}{N}\sum_{k=0}^{N-1} X[k].W_N^{-nk} \quad ; n = 0,1,2,\ldots,N-1$$

FFT dipergunakan untuk mengurangi kompleksitas transformasi yang dilakukan dengan DFT. Sebagai perbandingan, bila kita menggunakan DFT, maka kompleksitas transformasi kita adalah sebesar $O(N^2)$, sementara dengan menggunakan FFT, selain waktu transformasi yang lebih cepat, kompleksitas transformasi pun menurun, menjadi O(N log (N)). Untuk jumlah *sample* yang sedikit mungkin perbedaan kompleksitastidak begitu terasa, namun lain ceritanya bila kita mengambil jumlah *sample* yang sedikit lebih banyak. Misalnya kita hanya mengambil 2 *sample*, dengan menggunakan DFT, tingkat kompleksitas transformasi kita adalah 4, sementara dengan menggunakan FFT

kompleksitasnya sebesar 0,602. Perbedaan yang semakin mencolok tampak bila kita mengambil jumlah *sample* yang lebih banyak lagi, misalnya kita ingin meninjau 64 titik *sample*, maka kompleksitas dengan menggunakan DFT adalah sebesar 4096, sementara dengan menggunakan FFT kompleksitasnya menjadi 115,6. Perbedaan yang sangat besar, melihat perbandingan yang mencapai hampir 40 kali lipatnya. Kompleksitas transformasi ini terutama menjadi vital saat diimplementasikan pada perangkat riil.

D. Spread Spectrum

Spread spectrum adalah sebuah teknik transmisi dimana kode *psedo noise* digunakan sebagai gelombang modulasi untuk "menyebarkan" energi sinyal melalui sebuah *bandwith* yang jauh lebih besar daripada *bandwith* sinyal informasi. Pada awalnya metode ini dikembangkan untuk kepentingan militer dan intelejen. Ide dasarnya adalah untuk menyebarkan sinyal informasi melalui *bandwidth* yang lebih luas untuk mencegah dilakukannya pencegatan informasi dan gangguan-gangguan lainnya. Istilah *spread spectrum* digunakan karena pada sistem ini sinyal yang ditransmisikan memiliki *bandwidth* yang jauh lebih lebar dari *bandwidth* sinyal informasi. Proses penebaran *bandwidth* sinyal informasi ini disebut *spreading*. Penyebaran ini berguna untuk menambah tingkat redudansi. Besaran redudansi ditentukan oleh faktor pengali cr yang bernilai skalar. Panjang bit-bit hasil penyebaran ini menjadi cr kali panjang bit-bit awal.

E. Steganografi

Steganografi secara umum adalah teknik menyisipkan pesan kedalam suatu media. Steganografi berasal dari bahasa yunani yaitu stegos yang berarti menyembunyikan dan graptos yang berarti tulisan sehingga steganografi berarti tulisan yang disembunyikan. Steganografi sudah dikenal oleh bangsa Yunani. Herodatus, penguasa Yunani, mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini, rambut budak dibotaki, lalu pesan rahasia ditulis pada kulit kepala budak. Ketika rambut budak tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya.

Steganografi menggunakan sebuah berkas yang disebut dengan cover, tujuannya sebagai kamuflase dari pesan yang sebenarnya. Banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Pada jaman modern seperti saat ini, steganografi biasanya dilakukan dengan melibatkan berkas-berkas data digital seperti teks, audio, dan gambar.

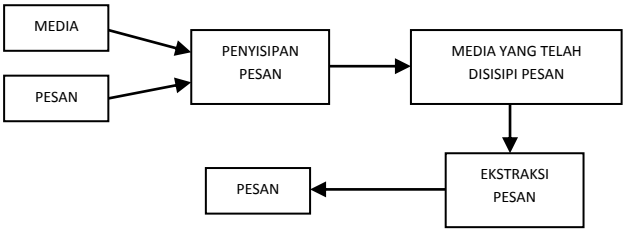
Penyembunyian data rahasia ke dalam audio digital akan mengubah kualitas audio tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah :

1. *Fidelity*
   Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih dapat terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat pesan rahasia.
2. *Robustness*
   Data yang disembunyikan harus tahan (*robust*) terhadapp berbagai operasi manipulasi yang dilakukan terhadap citra penampung.
3. *Recovery*
   Data yang disembunyikan harus dapat diungkapkan kembali (*reveal).* Karena tujuan dari steganografi adalah penyembunyian data, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

III. PERANCANGAN APLIKASI

A. Blok diagram sistem

Pada sistem steganografi terdiri dari beberapa langkah yang dapat digambarkan menjadi blok diagram dengan model seperti Gambar berikut :



Gambar 3. Diagram Blok Sistem Secara Keseluruhan

Fungsi masing-masing bagian dalam diagram blok ini adalah senagai berikut :

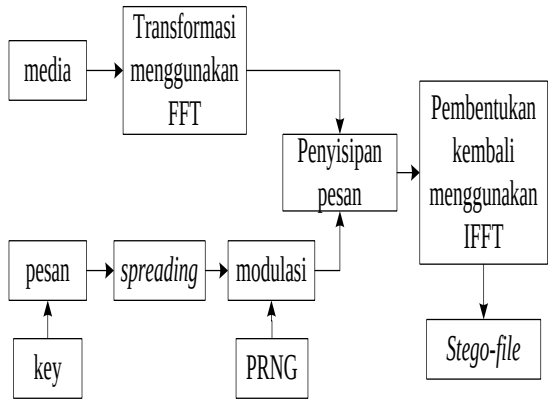
1. Pesan dan media penampung pesan digunakan sebagai *input* sistem.
2. Melakukan *audio processing* penyisipan pesan kedalam media.
3. Proses penyisipan pesan menghasilkan *stego-object*.
4. Melakukan proses ekstraksi pesan dari *stego-image*.

B. Perancangan Perangkat Lunak

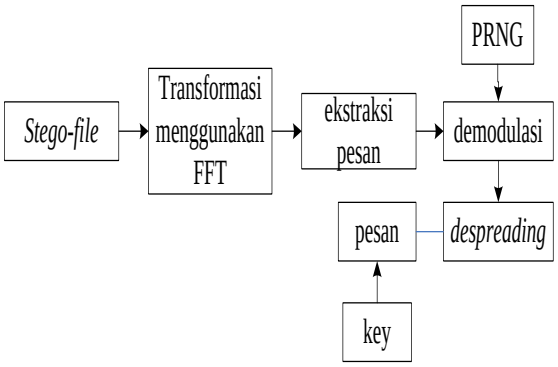
Pada bagian perancanan ini perangkat lunak yang akan dibuat menggunakan bahasa pemrograman *Microsoft Visual Studio C#.NET 2012* dan sistem yang digunakan untuk membangun perangkat lunak ini dirancang dengan spesifikasi mampu melakukan hal-hal berikut :

1. Pesan dan media penampung pesan digunakan sebagai input sistem.
2. Melakukan proses penyisipan pesan kedalam media.
3. Proses penyisipan pesan menghasilkan stego-object.
4. Melakukan proses ekstraksi pesan dari stego-object.

Sedangkan untuk detail desain aplikasi secara umum akan ditunjukkan pada gambar 4 dan 5.



Gambar 4. Rancangan Umum Proses Penyisipan Pesan.



Gambar 5. Rancangan Umum Proses Ekstraksi Pesan

C. Cara Kerja Aplikasi

Aplikasi steganografi pada audio digital ini menggunakan metode Spread spectrum dimana memiliki cara kerja yang dimulai dari pengambilan berkas audio (cover-object) yang akan digunakan sebagai media penyisipan pesan yang sebelumnya telah dilakukan tranformasi menggunakan FFT dan pesan rahasia yang ingin disampaikan, key digunakan sebagai pengacak pesan yang setelah itu kemudian dilakukan Spread Spectrum, setelah itu dilakukan penyisipan pesan ke dalam audio sehingga menghasilkan audio yang telah disisipi pesan (stego-object), setelah itu, dilakukan proses ekstraksi pesan dari stego-object sehingga menghasilkan pesan rahasia yang ingin disampaikan.

IV. HASIL DAN PEMBAHASAN

A. Pengujian Kebenaran Perangkat Lunak

Tabel 1. Hasil Pengujian Tingkat Keberhasilan Perangkat Lunak.

Nama Audio	*Size* (bytes)	Penyisipan	Ekstraksi
Aku yang terindah	20	berhasil	berhasil
Akuistik	30	berhasil	berhasil
Citra Scholastika - Pasti Bisa	35	berhasil	berhasil
Reason__ Instrumental	46	berhasil	berhasil

Tabel 2. Hasil Pengujian Tingkat Keberhasilan Memainkan Audio Hasil Penyisipan.

Nama Audio Setelah Disisipi	*Play*/di mainkan
Akuistik-hasil	Berhasil
Citra Scholastika - Pasti Bisa-hasil	Berhasil
Reason__Instrumental-hasil	Berhasil
Aku yang terindah-hasil	Berhasil

Dari hasil pengujian, terbukti bahwa perangkat lunak yang sudah dibuat telah berhasil menjalankan proses penyisipan dan ekstraksi pesan dengan baik. Semua pesan berhasil disisipkan dan diekstraksi dengan baik.

B. Pengujian Kinerja Perangkat Lunak

Pengujian dilakukan dengan cara melihat seberapa lama waktu yang dibutuhkan untuk melakukan proses penyisipan dan juga proses ekstraksi pesan. Pengujian dilakukan dengan menggunakan ukuran pesan serta berkas audio yang berbeda-beda. Hasil pengujian dapat dilihat pada Tabel 3 dan 4.

Tabel 3. Hasil Pengujian Waktu Proses Penyisipan

No	*Size*	Nama Audio	Pesan	Waktu Proses (detik)
1	4.45 MB	Akuistik	Tes 2	27:02
2	10.1 MB	Citra Scholastika - Pasti Bisa	Tes 2	32:06
3	15.4 MB	Reason__ Instrumental	Tes 2	37:04
4	20 MB	Aku yang terindah	Tes 2	42:06

Tabel 4. Hasil Pengujian Waktu Proses Ekstraksi

No	*Size*	Nama Audio	Pesan	Waktu Proses (detik)
1	4.45 MB	Akuistik	Tes 2	12:05
2	10.1 MB	Citra Scholastika - Pasti Bisa	Tes 2	17:16
3	15.4 MB	Reason__ Instrumental	Tes 2	21:09
4	20 MB	Aku yang terindah	Tes 2	25:05

Dari hasil pengujian terlihat bahwa waktu proses ekstraksi berbeda-beda tergantung dari panjang audio yang digunakan sebagai *cover-object.* Semakin besar kapasitas audio maka semakin lama pula waktu proses penyisipan dan ekstraksi. Dan dari hasil tersebut juga dapat terlihat bahwa waktu proses ekstraksi berada sekitar setengah dari waktu penyisispan.

Pengujian selanjutnya adalah pengujian kualitas audio hasil dari penyisipan. Pengujian ini dilakukan dengan dua cara, baik secara subjektif maupun objektif.

Untuk cara subjektif, dilakukan dengan membandingkan berkas audio hasil penyisipan dengan asli nya. audio hasil penyisipan tidak dapat dibedakan dengan audio asli. Yaitu dengan cara mendengarkannya secara langsung melalui indera pendegaran telinga.

Sedangkan untuk objektif, dilakukan dengan mencari nilai PSNR dari masing-masing audio. Hasil pengujian dapat dilihat pada Tabel 5. Dari hasil penunaian pada Tabel 5 terlihat bahwa jumlah karakter yang disisipkan pada audio uji berpengaruh terhadap nilai PSNR yang dihasilkan. Semakin banyak karakter yang disisipkan maka semakin berkurang kualitas audio *segi-object* dengan menurunnya PSNR

Tabel 5. Hasil Pengujian Kualitas Audio berdasrkan PSNR

No	*Size audio*	Durasi	*Size* pesan (bytes)	PSNR (dB)
1	10.1 MB	01:00 menit	20	41.75
2	10.1 MB	01:00 menit	30	40.55
3	10.1 MB	01:00 menit	35	40.06
4	10.1 MB	01:00 menit	46	38.02

V. PENUTUP

A. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, pengujian dan analisis sistem maka dapat diambil kesimpulan sebagai berikut :

1. Steganografi dengan teknik Spread Spectrum dapat diterapkan pada berkas audio WAV.
2. Perangkat lunak yang mengimplementasikan steganografi dengan teknik Spread Spectrum pada berkas audio .WAV berhasil dibangun. Kebutuhan fungsionalitas dari perangkat lunak, seperti proses penyisipan dan ekstraksi pesan, serta penggunaan kunci dan memainkan berkas audio .WAV secara keseluruhan dapat dilakukan dengan benar.
3. Kualitas berkas audio yang dihasilkan bergantung dari besarnya ukuran pesan. Dalam hal ini faktor pengali alfa juga mempengaruhi dari kualitas berkas audio yang dihasilkan.
4. Pengujian kinerja perangkat lunak menunjukan bahwa perangkat lunak dapat digunakan dengan baik dan efisien. Dan dari nilai PSNR menunjukkan bahwa nilai PSNR menurun seiring dengan bertambahnya ukuran pesan yang disisipkan. Jika ukuran pesan yang disipkan semakin besar maka nilai PSNR semakin kecil yang berarti kualitas berkas audio yang disisipi semakin buruk.

B. SARAN

Dalam perancangan dan pembuatan aplikasi steganografi menggunakan Spread Spetrum ini masih terdapat kekurangan dan kelemahan, oleh karena itu masih diperlukan adanya penyempurnaan dalam rangka pengembangan ke depan. Adapun hal yang dapat dikembangkan ke depan adalah sebagai berikut :

1. Perlu dilakukan pengembangan untuk meningkatkn kapasitas penyisipan agar lebih besar.
2. Perlu dilakukannya pengembangan dan analisa lebih lanjut terhadap beberapa kesalahan yang muncul.
3. Perlu adanya analisa lebih lanjut dan implementasi Spread Spectrum pada format audio lainnya seperti OGG, EMA, MP3, ACC.
4. Perlu dilakukan analisa lebih lanjut untuk meningkatan kecepatan waktu dari proses penyisipan maupun ekstraksi pesan.

DAFTAR PUSTAKA

[1] Stallings, William. 2005. "Cryptography and Network Security, 4th edition".

[2] Stallings, William. 2011. "Komunikasi Data dan Komputer, edisi 8".

[3] Munir, Rinaldi, M.T., "Kriptografi.", INFORMATIKA, 2006.

[4] Gias Vembrina, Yus. "*Spread Spectrum Steganography*", Sekolah Teknik Elektro dan Informatika-Institut Teknologi Bandung.

[5] Unnisa Fitri S, Auliya. "Mengoptimalisasi Steganografi pada File Audio", Sekolah Teknik Elektro dan Informatika-Institut Teknologi Bandung.

[6] http://www mmsp.ece.mcgill.ca/Documents/ AudioFormats/WAVE/WAVE.html

[7] http://en.wikipedia.org/wiki/WAV

[8] http://en.wikipedia.org/wiki/Fast_Fourier_ transform

[9] http://www.relisoft.com/science/physics /fft.html

[10] http://www.csharp-station.com/Tutorial.aspx

[11] http://msdn.microsoft.com/en-us/vstudio/hh388566