METODE PARITY CODING VERSUS METODE SPREAD SPECTRUM PADA AUDIO STEGANOGRAPHY

Riko Arlando Saragih
Jurusan Teknik Elektro Universitas Kristen Maranatha
Jl. Prof. Drg. Suria Sumantri 65, Bandung, Indonesia
Phone: +62222012186 Fax +62222015154
E-mail: riko_saragih@yahoo.com

ABSTRAKSI

Steganography adalah suatu ilmu yang mempelajari cara menyembunyikan informasi rahasia di dalam sebuah pesan. Audio steganography merupakan perkembangan ilmu dari steganography. Audio steganography mempunyai kesulitan yang lebih dibandingkan pada steganography pada gambar atau pada video karena pendengaran manusia lebih peka daripada penglihatan manusia, sehingga pada proses penyisipan data harus dibuat sebaik mungkin agar suara yang telah disisipkan data terdengar sama dengan suara sebelum disisipkan data.

Di dalam penelitian ini akan dibandingkan metode parity coding dan metode spread spectrum pada audio steganography. Data yang akan disisipkan berupa teks direpsentasikan dalam bentuk biner, sedangkan data cover adalah sinyal audio yang direkam dalam bentuk .wav.

Hasil pengamatan dari setiap percobaan diketahui bahwa pada metode parity coding nilai SNR pada sinyal audio cover yang berdurasi lebih panjang mempunyai nilai SNR lebih baik, sedangkan pada metode spread spectrum keamanan data lebih terjamin karena menggunakan kode penyebar yang tidak diketahui oleh pihak lain.

Kata kunci: *Audio Steganography, Parity Coding, Spread Spectrum, SNR*

1. PENDAHULUAN

Dalam era informasi sekarang ini begitu banyak informasi atau data yang dipertukarkan. Pertukaran data dapat dilakukan melalui LAN , Internet, atau dengan menggunakan berbagai media penyimpan data seperti harddisk atau USB drive sehingga suatu data dapat dengan mudah dapat disebarluaskan.

Data yang akan digunakan sebagai pembawa informasi adalah data dalam bentuk audio, video, dan gambar. Pada data ini akan disisipkan suatu pesan rahasia sehingga dapat digunakan untuk mengirimkan pesan kepada orang yang dituju dengan cara menyamarkan pesan itu ke dalam suatu *data cover* dengan tujuan mengelabui orang lain yang mungkin mendapatkan pesan yang dikirimkan.

Keuntungan dari digunakan cara ini adalah tidak akan mengubah isi dari *data cover*-nya, sehingga *data cover* akan berfungsi, terlihat, dan berperilaku seperti data biasa. Secara teori hampir semua data dapat dipakai sebagai *data cover* informasi tersembunyi.

Pada penelitian ini akan dibahas teknik menyembunyikan data teks di dalam suatu data berbentuk audio atau yang lebih dikenal dengan *audio steganography*. Metode yang digunakan dalam penyembunyian data adalah metode *parity coding* dan *spread spectrum*. Kedua metode tersebut akan dibandingkan nilai SNR-nya (*signal noise to ratio*) untuk melihat performansinya.

2. SEJARAH STEGANOGRAPHY

Steganography merupakan istilah yang berasal dari bahasa Yunani, yaitu *steganos* serta *graphia*. *Steganos* berarti tertutup atau rahasia sedangkan *graphia* artinya tulisan. Steganography sendiri adalah suatu ilmu yang mempelajari cara menyembunyikan informasi (ilmu yang mempelajari teknik penyembunyian pesan rahasia ke dalam pesan lain). Teknologi steganography (seperti teknik-teknik *watermark*) sudah dikenal sejak ribuan tahun yang lalu.Yang cukup dikenal adalah sejarah di jaman Herodotus, saat Histiaeus membuat pesan rahasia dengan mentato kepala ajudannya, kemudian membiarkan rambutnya tumbuh sebelum diutus ke Aristagoras, yang harus mencukur kepala ajudan tersebut sebelum mengetahui pesan yang dikirim [2].

Teknik steganography pada kertas mulai muncul tahun 1282 di Italia setelah ditemukannya teknologi pembuatan kertas oleh bangsa Cina ribuan tahun sebelumya. Tujuan dan arti pemberian teknik steganography saat itu kurang begitu jelas. Kemungkinan digunakan untuk alasan praktis, yaitu untuk menandai kertas mengenai informasi pembuatnya. Pada lain hal, kemungkinan juga digunakan dengan alasan mistik, yaitu merepresentasikan simbol-simbol magis atau hanya sekedar hiasan belaka. Pada abad kedelapanbelas, mulai muncul istilah *watermark* dan mulai diberikan pada kertas yang dibuat di Eropa dan Amerika untuk identifikasi hak milik, tanggal pembuatan, pabrik pembuat, dan informasi ukuran

kertas. Pada abad tersebut juga *watermark* mulai digunakan sebagai tanda keaslian dokumen dan uang kertas. Asal kata watermark sendiri muncul dari bahasa Jerman, yaitu *wassermarke*. Dengan munculnya teknologi *watermark* pada uang kertas, pada waktu yang sama juga muncul teknik untuk melakukan perusakan atau manipulasi lainnya (*counterfeiting*). Hal tersebut pertama kali dilaporkan oleh Gentelman's Magazine pada tahun 1779 dengan adanya usaha tersebut untuk melakukan penipuan/kecurangan (*fraud*) terhadap bank [2].

Steganography berbeda dengan teknik *cryptography* yang mengubah susunan pesan menjadi tidak terbaca sama sekali. Dalam teknik steganography pesan yang dikirimkan sendiri tetap dapat terbaca oleh siapapun, namun pesan rahasia tetap tersembunyi sampai ada pihak yang mengerti cara/kunci penyembunyian pesan rahasia tersebut. Sifat seperti ini dimanfaatkan salah satunya untuk *watermark* sebagai aplikasi pelindung hak cipta suatu dokumen digital. Steganography kuno kemudian diganti dengan teknologi tinta yang tidak terlihat dan *microdot* serta pesan *null cipher* (pesan tersembunyi namun tak terenkripsi dan dibuat sebagai pesan yang tidak mencurigakan) [2].

Sejalan dengan perkembangan teknologi komputer, steganography memberikan kontribusi yang besar dalam aplikasi penyembunyian data, di antaranya adalah [2]:

1. Industri-industri broadcasting dan penerbitan memerlukan teknologi yang dapat menyisipkan tanda hak cipta atau kepemilikan pada produk digital mereka sebagai salah satu usaha untuk memerangi pembajakan.
2. Adanya motivasi untuk mempelajari dan mengembangkan teknologi steganography akibat dibatasinya ketersediaan layanan-layanan kriptography oleh pemerintah negara-negara dunia, seperti Amerika Serikat yang membatasi kriptography maksimal 128 bit.

Steganography modern mulai menerapkan penyembunyian pesan pada data dengan format atau jenis lain seperti pada gambar, teks, audio, email, IP header dan sebagainya [3].

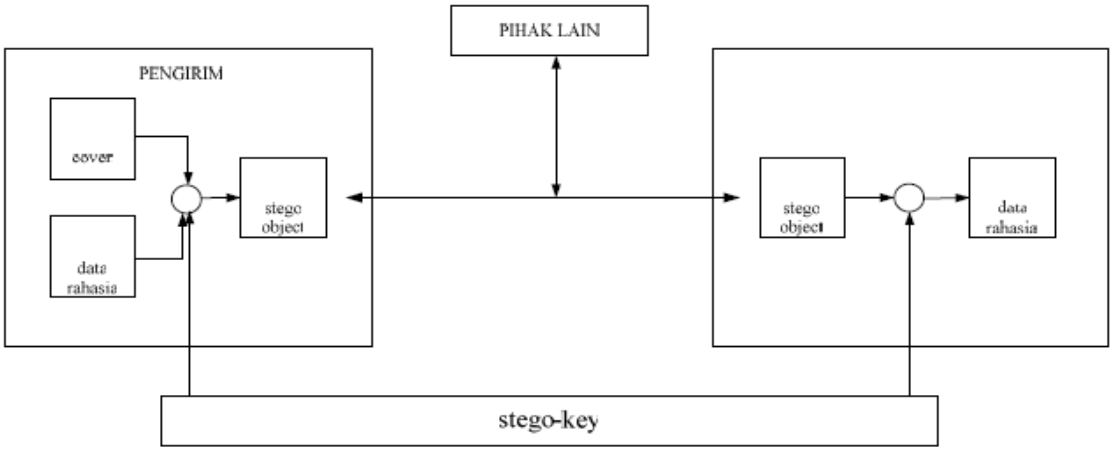
3. PRINSIP KERJA STEGANOGRAPHY

Kerangka kerja dari pengiriman data dalam steganography adalah data rahasia disisipkan ke sebuah data lain (cover) dengan menggunakan suatu kunci atau yang dikenal dengan stego-key sehingga menghasilkan data baru atau yang dikenal dengan stego-object . Data yang menjadi media kirim harus terlihat berarti sehingga tidak menimbulkan kecurigaan pihak lain. Setelah data diterima pihak penerima harus mengetahui stego-key agar dapat mengambil data rahasia yang telah disisipkan.

Pada kenyataanya tidak semua data dapat dijadikan cover untuk pengiriman data rahasia, diperlukan modifikasi data agar data rahasia tidak terlihat. Data yang dijadikan cover harus lebih besar dari data rahasia agar data rahasia tidak terlihat. Data yang digunakan sebagai cover sebaiknya digunakan satu kali. Apabila digunakan lebih dari satu kali, maka akan menimbulkan kecurigaan pihak lain.

4. AUDIO STEGANOGRAPHY

Audio steganography merupakan perkembangan ilmu dari *steganography*. *Audio steganography* mempunyai kesulitan yang lebih dibandingkan pada *watermarking* digital pada gambar dan *watermarking* digital pada video. Karena pendengaran manusia lebih peka daripada penglihatan manusia, sehingga pada proses penyisipan data harus dibuat sebaik mungkin agar audio yang telah disisipkan data terdengar sama dengan suara sebelum disisipkan data [3].



Gambar 1. Skema kerangka kerja pengiriman data rahasia [2]

Audio steganography dapat digunakan dalam beberapa aplikasi, di antaranya proteksi hak cipta, pembuktian keaslian, penulisan teks (captioning) dan *Digital Right Management* (DRM). Setiap aplikasi mempunyai cara perancangan yang berbeda sesuai dengan performa yang diinginkan yang diinginkan. Performa-performa tersebut berpengaruh pada kualitas *audio steganography* yang akan dirancang. Berikut merupakan performa yang harus diperhatikan dalam *audio steganography*, yaitu:

1. Kualitas Audio

Dasar yang paling penting pada *audio steganography* adalah penyisipan data tidak boleh mengubah kualitas suara dari sinyal audio yang digunakan sebagai *cover*. Jadi data rahasia yang disisipkan tidak boleh terdeteksi oleh pendengar. Performa ini sangat penting pada aplikasi proteksi hak cipta.Parameter yang digunakan dalam menentukan kualitas audio yang telah disisipkan data adalah SNR (*signal to noise ratio*) [3]. Persamaan untuk menghitung SNR adalah sebagai berikut:

$$SNR = 10 \log_{10} \left\{ \frac{\sum_{n=0}^{N-1} x^2(n)}{\sum_{n=0}^{N-1} [\tilde{x}(n) - x(n)]^2} \right\} \qquad (1)$$

Keterangan: $x(n)$ adalah sinyal *audio cover* dari panjang sampel N dan $\tilde{x}(n)$ adalah sinyal data yang disisipkan.

2. Bit Rate

Tujuan dari bit rate adalah untuk menghitung banyaknya data rahasia yang mungkin disisipkan ke sinyal *audio cover* per satuan waktu. Beberapa aplikasi *steganography*, seperti penyisipan nomor serial dan pengidentifikasian hak cipta membutuhkan hanya sedikit data yang disisipkan pada sinyal *audio cover*.

3. Keamanan

Untuk mencegah pendeteksian dan penghapusan data yang disisipkan oleh pihak lain, maka proses penyisipan data harus dibuat seaman mungkin dalam berbagai aplikasi. Setiap aplikasi membutuhkan tingkat keamananyang berbeda. Skema penyisipan data akan aman apabila diketahui algoritma yang akan digunakan. Pihak lain selain pengirim dan penerima tidak akan bisa mengambil data walaupun pihak tersebut mengetahui bahwa terdapat data lain didalam sinyal audio tersebut dan mengetahui metode penyisipan data. Biasanya metode penyisipan diberitahukan kepada pihak lain, tetapi *secret key* tidak diberikan. Pada beberapa aplikasi misalnya komunikasi tersembunyi data yang akan disisipkan dienkripsikan terlebih dahulu sebelum disisipkan ke sinyal *audio cover* [3].

4. Kesulitan Perhitungan

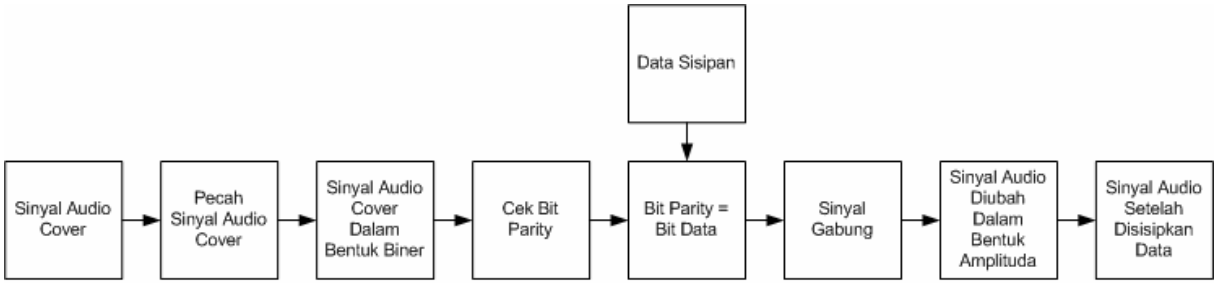
Kesulitan perhitungan berdasarkan pada proses yang dibutuhkan untuk menyisipkan data ke dalam sinyal audio dan pengambilan data tersebut dari sinyal audio. Hal ini merupakan yang paling esensial dan kritis apabila aplikasi digunakan secara on-line baik dalam penyisipan dan pengambilan data. Kesulitan algoritma juga merupakan hal yang penting yang mempengaruhi pemilihan struktur implementasi atau arsitektur pemrosesan sinyal digital [3].

5. METODE PARITY CODING

Data rahasia yang disisipkan pada metode *parity coding* merupakan teks dalam kode ASCII dan kombinasi bitnya disisipkan dalam bit *parity* [1]. Diagram blok proses penyisipan data pada metode *parity coding* diperlihatkan pada Gambar 2.

Secara umum cara kerja penyisipan data rahasia dari metode *parity coding* adalah mengganti nilai *parity* bit pada tiap sinyal audio yang dipecah. Berikut merupakan prosedur kerja dari metode *parity coding:*

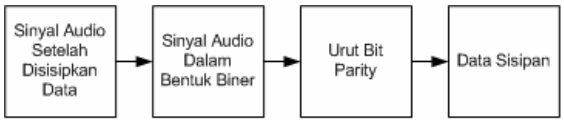
1. Sinyal *audio cover* dipecah menjadi beberapa frame sebanyak l(m) sesuai dengan banyak bit data (m_i) yang akan disisipkan dengan ($1 \le i \le l(m)$).
2. Pada setiap frame dikodekan menjadi bilangan biner.



Gambar 2. Diagram Blok Penyisipan Data Rahasia Pada Metode *Parity Coding*

3. Nilai bit *parity* setiap frame dicek. Apabila bit 1 berjumlah ganjil, maka nilai *parity* bitnya bernilai 1. Jika bit 1 berjumlah genap, maka nilai *parity* bitnya bernilai 0.
4. Setiap bit dari data rahasia (m_i) disamakan dengan nilai bit *parity* setiap frame. Jika nilai bit parity tidak sama dengan bit data rahasia, maka nilai bit *parity* disesuaikan dengan bit dari data rahasia.
5. Setiap frame yang sudah disisipkan data rahasia digabung kembali.
6. Sinyal *audio cover* yang masih berbentuk bilangan biner diubah kembali menjadi bentuk amplituda.

Untuk proses pengambilan data, maka penerima harus mengetahui panjang frame sehingga bisa mengetahui banyaknya data yang disisipkan pada sinyal *audio cover*. Diagram blok proses pengambilan data pada metode *parity coding* diperlihatkan pada Gambar 3.



Gambar 3. Diagram Blok Pengambilan Data Rahasia Pada Metode *Parity Coding*

Cara kerja umum pengambilan data rahasia dari metode *parity coding* adalah dengan cara mengurutkan nilai bit *parity* pada setiap frame. Berikut merupakan prosedur kerjanya:

1. Sinyal *audio cover* yang diterima dipecah menjadi beberapa frame.
2. Pada setiap frame dikodekan menjadi bilangan biner.
3. Nilai bit *parity* berada di *Least Significant Bit* (LSB) dari setiap frame.
4. Urut nilai bit *parity* sehingga menghasilan data rahasia

6. METODE SPREAD SPECTRUM

Metode *spread spectrum* merupakan metode menyisipkan data dengan cara menyebarkan data rahasia sepanjang sinyal *audio cover* [1]. Data rahasia yang disisipkan pada sinyal *audio cover* disebar dengan *Direct Sequence Spread Spectrum* (DSSS). Diagram blok proses penyisipan data pada metode *spread spectrum* diperlihatkan pada Gambar 4.

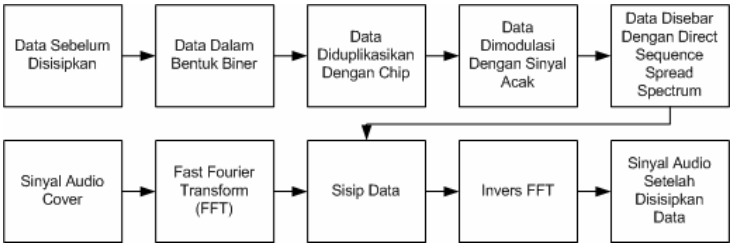
Berikut merupakan prosedur kerjanya:

1. Data rahasia direpresentasikan dalam bentuk bilangan biner.
2. Data rahasia yang berbentuk bilangan biner diduplikasi dengan *chip*.
3. Data rahasia dimodulasi dengan sinyal acak sehingga menghasilkan sinyal *pseudorandom*.
4. Data rahasia disebar dengan menggunakan *direct sequence spread spectrum*, dengan bilangan biner 1 direpresentasikan dengan 1 dan bilangan biner 0 direpresentasikan dengan -1.
5. Data rahasia yang bernilai 1 direpresentasikan dengan bentuk *imajiner* 1i dan yang bernilai -1 direpresentasikan dalam bentuk *imajiner* -1i.
6. Sinyal *cover* direpresentasikan dalam bentuk *Fast Fourier Transform* (FFT).
7. Data rahasia disisipkan ke sinyal *cover*.
8. Data rahasia yang sudah disisipkan diubah ke bentuk amplituda sehingga menghasilkan sinyal *audio* yang mengandung data rahasia.

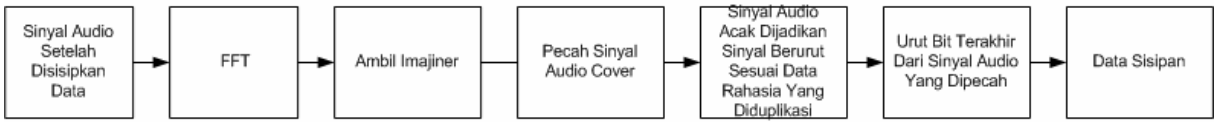
Untuk proses pengambilan penerima harus mempunyai algoritma sinyal acak. Diagram blok proses pengambilan data pada metode *spread spectrum* diperlihatkan pada Gambar 5.

Berikut merupakan prosedur kerja pengambilan data dari metode *spread spectrum*:

1. Sinyal audio yang sudah disisipkan data direpresentasikan dalam bentuk *Fast Fourier Transform* (FFT).
2. Bagian imajiner dari sinyal *audio cover* diambil.



Gambar 4. Diagram Blok Penyisipan Data Rahasia pada Metode *Spread Spectrum*



Gambar 5. Diagram Blok Pengambilan Data Rahasia pada Metode *Spread Spectrum*

3. Bentuk imajiner dari 1i diubah menjadi nilai biner 1 dan bentuk imajiner dari -1i diubah menjadi nilai biner 0.
4. Sinyal *audio* dipecah menjadi beberapa frame.
5. Sinyal audio yang acak dijadikan sinyal berurut kembali sesuai dengan data rahasia yang diduplikasi.
6. Bit terakhir dari setiap frame diurut sehingga menghasilkan data rahasia.

7. HASIL DAN PEMBAHASAN

Dalam penelitian ini dilakukan simulasi untuk membandingkan metode *parity coding* dan metode *spread spectrum* dengan menggunakan perangkat lunak MATLAB versi 7.0. Kualitas sinyal suara dapat diukur secara obyektif dengan menghitung perbandingan daya sinyal terhadap daya *noise* atau *Signal to Noise Ratio* (SNR).

Pengujian dilakukan sebanyak 6 kali dengan teks sisipan sebanyak tiga macam dan tiga sinyal *audio cover*. Data teks sisipan direpresentasikan dalam bentuk ASCII. Sinyal *audio cover* semuanya berbentuk irama lagu dan disampling dengan frekuensi 8 kHz dan jumlah bit kuantisasi sebanyak 8 bit.

Perincian teks sisipan beserta kode ASCII nya diperlihatkan pada Tabel 1.

Tabel 1. Teks masukan yang direpresentasikan dalam bentuk ASCII

Teks Sisipan	*Kode ASCII*
ABC	0 1 0 0 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 0 0 1 1
ABCDEFG	0 1 0 0 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 0 0 1 1 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 1 0 1 0 0 0 1 1 0 0 1 0 0 0 1 1 1
ABCDEFGHIJKL	0 1 0 0 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 0 0 1 1 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 1 0 1 0 0 0 1 1 0 0 1 0 0 0 1 1 1 0 1 0 0 1 0 0 0 0 1 0 0 1 0 0 1 0 1 0 0 1 0 1 0 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 0

Spesifikasi sinyal *audio cover* diperlihatkan pada Tabel 2.

Tabel 2. Spesifikasi sinyal *audio cover*

Nama File	*Durasi*
Intro.Wav	9,89 detik
Haunted.Wav	12,48 detik
Bigshow.Wav	14,82 detik

Tabel 3 sampai dengan Tabel 5 merupakan hasil pengamatan dari metode *parity coding*.

Tabel 3. Hasil pengamatan dengan medium sinyal suara INTRO.WAV

No	*Data Sisipan*	*SNR(dB)*
1	ABC	77,23
2	ABCDEFG	60,98
3	ABCDEFGHIJKL	54,54

Tabel 4. Hasil pengamatan dengan medium sinyal suara HAUNTED.WAV

No	*Data Sisipan*	*SNR(dB)*
1	ABC	82,12
2	ABCDEFG	67,87
3	ABCDEFGHIJKL	52,56

Tabel 5. Hasil pengamatan dengan medium sinyal suara BIGSHOW.WAV

No	*Data Sisipan*	*SNR(dB)*
1	ABC	83,34
2	ABCDEFG	66,85
3	ABCDEFGHIJKL	60,45

Pada metode *parity coding*, nilai SNR berubah berdasarkan banyaknya data yang disisipkan. Semakin banyak data yang disisipkan, maka nilai SNR semakin kecil karena dipengaruhi oleh jumlah nilai *parity* yang sama antara sinyal *audio cover* dengan data sisipan. Selain itu, nilai SNR pada sinyal *audio cover* yang berdurasi lebih panjang cenderung mempunyai nilai SNR lebih baik karena *kemungkinan* jumlah nilai *parity* yang sama antara sinyal *audio cover* dengan data sisipan akan lebih banyak.

Tabel 6 sampai dengan Tabel 8 merupakan hasil pengamatan dari metode *spread spectrum*.

Tabel 6. Hasil pengamatan dengan medium sinyal suara INTRO.WAV

No	*Data Sisipan*	*SNR(dB)*
1	ABC	53,67
2	ABCDEFG	45,12
3	ABCDEFGHIJKL	30,78

Tabel 7. Hasil pengamatan dengan medium sinyal suara HAUNTED.WAV

No	*Data Sisipan*	*SNR(dB)*
1	ABC	51,24
2	ABCDEFG	36,45
3	ABCDEFGHIJKL	27,54

Tabel 8. Hasil pengamatan dengan medium sinyal suara BIGSHOW.WAV

No	*Data Sisipan*	*SNR(dB)*
1	ABC	54,46
2	ABCDEFG	48,68
3	ABCDEFGHIJKL	36,54

Pada metode *spread spectrum*, nilai SNR berubah berdasarkan banyaknya data yang disisipkan. Semakin banyak data yang disisipkan, maka nilai SNR semakin kecil, tetapi keamanan data lebih terjamin karena menggunakan kode penyebar yang tidak diketahui oleh pihak lain.

7. KESIMPULAN

a. Pada metode *parity coding* dan *spread spectrum*, nilai SNR berubah berdasarkan jumlah data yang disisipkan. Semakin banyak data yang disisipkan, maka nilai SNR akan semakin kecil.
b. Pada metode *parity coding*, nilai SNR pada sinyal *audio cover* yang berdurasi lebih panjang mempunyai nilai SNR lebih baik.
c. Pada metode *spread spectrum*, keamanan data lebih terjamin karena menggunakan kode penyebar yang tidak diketahui oleh pihak lain.

Ucapan Terima Kasih

Melalui tulisan ini, penulis hendak mengucapkan terima kasih kepada **Saudara Nurudin Abdurahman, ST.** yang telah membantu penulis di dalam menyelesaikan penelitian ini dan memberi ide-ide di dalam pelaksanaan simulasi.

Daftar Pustaka

[1] Cvejic, Nedeljko, *Algorithms for Audio Watermarking and Steganography*, Finland, Department of Electrical and Information Engineering , AUniverisyt of Oulu, 2004.
[2] Katzenbeisser, Stefan, and Petitcolas, Fabien A. P., 2000, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Inc, 685 Canton Street Norwood, MA 02062.
[3] Lu, Chun-Shien, 2005, *Multimedia Security: Steganography and Digital Watermarking Technique for Protection of Intellectual Property*, Idea Group.