Ulum, M. B., Sandfreni, S. and Azizah, A. H. (2021) "Perbandingan Teknik Steganografi Domain Spasial dengan Domain Transformasi pada Audio", Sebatik, 25(2).
Submitted: 2021/11/15 Accepted: 2021/11/27 Published: 2021/12/01

Sebatik Vol. 25 No. 2 Desember 2021
ISSN: 1410-3737(p) 2621-069X(e)

DOI:10.46984/sebatik.v25i3.1642

PERBANDINGAN TEKNIK STEGANOGRAFI DOMAIN SPASIAL DENGAN DOMAIN TRANSFORMASI PADA AUDIO

Muhamad Bahrul Ulum[1)], Sandfreni[2)], dan **Anik Hanifatul Azizah[3)]**

[1]Teknik Informatika, Universitas Esa Unggul
[2,3]Sistem Informasi, Universitas Esa Unggul
[1,2,3]Jl. Arjuna Utara No.9, Duri Kepa, Kec. Kebon Jeruk, Jakarta Barat, 11510
E-mail : m.bahrul_ulum@esaunggul.ac.id[1)], sandfreni@esaunggul.ac.id[2)], anik.hanifa@esaunggul.ac.id[3)]

ABSTRAK

Internet memberikan kemudahan menyampaikan informasi atau bertukar data, data yang dikirimkan melalui jaringan internet bisa memiliki sifat yang sangat rahasia. Untuk menjaga kerahasiaan data yang dikirimkan diperlukan suatu teknik, salah satunya adalah dengan teknik Steganografi. Steganografi adalah suatu teknik penyembunyian data yang bersifat rahasia pada suatu data penampung, dimana keberadaan dari data tersebut tidak mengundang kecurigaan dari persepsi pengamatan oleh indra manusia. Teknik Steganografi memiliki beberapa metode, metode yang paling sering digunakan adalah metode *Least Significant Bit* (LSB) dan metode *Spread Spectrum* (SS). Pada penelitian ini diterapkan kedua metode di atas pada Audio digital. Kemudian hasilnya dianalisis untuk membandingkan kelemahan dan kelebihan masing-masing metode dengan cara membandingkan kualitas audio sebelum dan sesudah disisipi, serta kualitas pesan rahasia yang sudah diekstraksi. Dari pengujian yang dilakukan didapatkan bahwa kualitas audio steganografi yang dihasilkan metode *Spread Spectrum* lebih baik dari pada metode *Least Significant Bit* (LSB) dibuktikan oleh nilai SNR yang dihasilkan metode *Spread Spectrum* lebih besar atau lebih baik dibandingkan metode *Least Significant Bit* (LSB). Perbedaan nilai SNR yang dihasilkan oleh kedua metode memiliki selisih nilai yang kecil, nilai perbedaannya mencapai 8 db, tetapi kualitas pesan yang didapatkan pada hasil ekstraksi kedua metode sama baiknya.

Kata Kunci: *Audio digital, LSB, Steganografi, Spread Spectrum.*

1. PENDAHULUAN

Perkembangan dunia digital saat ini membuat lalu lintas pengiriman pesan atau data semakin pesat. Data yang dipertukarkan pun bervariasi baik dari jenisnya maupun tingkat kerahasiaannya. Mulai dari data pribadi, data organisasi sampai data negara yang sangat rahasia. Hal inilah yang menuntut adanya pengamanan data tersebut sehingga tidak sampai tersadap oleh pihak ketiga. Permasalahan mulai muncul ketika data digital tersebut mengandung rahasia dan privasi tanpa diketahui orang yang tidak dituju, hanya antara pengirim pesan dan penerima pesan saja. Oleh karena itu diperlukan suatu metode untuk dapat memberi perlindungan terhadap data digital yang memprioritaskan proses pengiriman informasi yang aman, sulit dideteksi dan akurat. Salah satu teknik yang dapat dipakai untuk menangani hal tersebut adalah steganografi.

Steganografi merupakan ilmu dan seni yang mempelajari cara menyembunyikan pesan rahasia ke dalam suatu media sedemikian sehingga pihak ketiga tidak menyadari keberadaan pesan tersebut (Edisuryana dkk, 2013). Kekukuhan, keamanan dan kapasitas persembunyian adalah tiga kriteria kinerja utama yang berkisar pada metode steganografi yang ada. Pada steganografi, tidak mengubah struktur pesan rahasia, melainkan disembunyikan di dalam media cover yang tidak bermakna (hanya sebagai pembawa) (Ghasemi dkk, 2011). Steganografi adalah bagian utama dari perkembangan yang cepat dalam area persembunyian informasi. Steganografi menyediakan teknik untuk menyembunyikan keberadaan pesan sekunder di hadapan pesan utama. Pesan utama disebut sebagai sinyal pembawa atau pesan pembawa, sinyal pembawa dapat berupa teks, audio, gambar dan video.

Tujuan utama dari steganografi adalah untuk berkomunikasi dengan aman dengan cara yang benar-benar tidak terdeteksi dan untuk menghindari kecurigaan menggambar untuk transmisi data tersembunyi. Hal ini tidak hanya mencegah orang lain dari mengetahui informasi yang tersembunyi, tetapi juga mencegah orang lain berpikir bahwa ada informasi yang tersembunyi (Bhowal dkk, 2013). Mampu menimbulkan kesalahan persepsi adalah salah satu kelebihan steganografi, manusia tidak memiliki insting untuk mencurigai adanya sesuatu yang tersembunyi dalam suatu *file*, terutama bila *file* tersebut tampak seperti *file* normal lainnya. Steganografi juga memiliki kelemahan, yaitu steganografi memerlukan banyak ruang untuk dapat menyembunyikan beberapa bit pesan. Akan tetapi, kelemahan ini sedikit demi sedikit dapat diatasi seiring dengan perkembangan teknik-teknik yang dapat diterapkan dalam steganografi.

Terdapat beberapa teknik steganografi yang telah ditemukan. Teknik ini dapat diklasifikasikan dalam dua kategori, yaitu domain spasial dan domain transformasi atau domain frekuensi (Kour, 2014). Penyisipan dalam

domain spasial berarti memodifikasi langsung nilai *byte* dari *cover-object* (nilai *byte* dapat merepresentasikan intensitas/warna *pixel* atau amplitudo). Sedangkan penyisipan dalam domain transformasi adalah memodifikasi hasil transformasi sinyal dalam ranah frekuensi.

Saat ini penelitian terkait perbandingan teknik steganografi masih terfokus pada citra dan teks (Jayaram dkk, 2011), (Dulera dkk, 2011) atau terfokus pada salah satu domain saja (Nehru & Dhar, 2012), optimalisasi steganografi video (Arraziqi & Haq, 2019) serta teknik pengamanan data (Ukkas dkk, 2017). Sedangkan kenyataan di lapangan menunjukkan bahwa pengiriman pesan rahasia pada audio juga sangat diperlukan, baik bagi kalangan industri musik atau konsumen. Berbagai metode sudah digunakan untuk menyembunyikan pesan *file* audio, misalnya dalam audio steganografi (Adhanadi dkk, 2020). Awalnya *Least Significant Bit* (LSB) sederhana, kemudian metode LSB yang dimodifikasi. Untuk itu penelitian ini ditujukan untuk mengetahui perbandingan teknik steganografi domain spasial dan domain transformasi pada audio.

2. RUANG LINGKUP

Dalam penelitian ini permasalahan mencakup:

1. Melakukan perbandingan teknik steganografi domain spasial dan domain transformasi pada audio
2. Pada domain spasial, teknik steganografi yang digunakan adalah teknik *Least Significant Bit* (LSB).
3. Pada domain transformasi, teknik steganografi yang digunakan adalah *Spread Spectrum.*

3. BAHAN DAN METODE

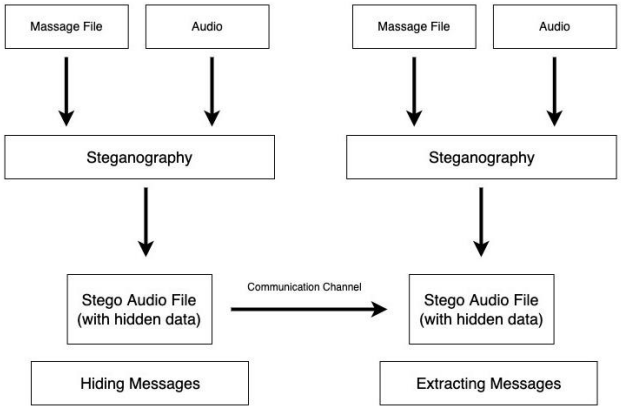
Bahan kajian, metode dan tahapan penelitian yang akan dilakukan dalam penelitian ini adalah sebagai berikut:

3.1 Data Audio

Pada penelitian ini, data yang digunakan adalah audio sebagai media cover dan teks sebagai pesan yang disembunyikan. Sehingga data awal harus direpresentasikan menjadi bentuk data biner terlebih dahulu.

3.2 Metode Steganografi Audio

Penelitian ini mencoba untuk membandingkan teknik steganografi domain spasial dengan domain transformasi pada audio (Saurabh & Ambhaikar, 2012), dapat dilihat pada gambar 1.



Gambar 1. Proses Steganografi Audio

Pendekatan penyisipan data dalam steganografi audio secara luas diklasifikasikan ke dalam domain spasial dan domain transformasi. Teknik domain spasial seperti pengodean bit rendah, menyematkan pesan rahasia secara langsung dalam domain waktu. Metode domain spasial menyembunyikan pesan rahasia berdasarkan karakteristik geometris sinyal pembawa audio. Sebagian besar domain spasial metode menggunakan teknik *Least Significant Bit* (LSB). Teknik LSB konvensional dan varian nya memberikan cara mudah untuk menyembunyikan informasi. Metode domain spasial sangat toleran terhadap penambahan kebisingan pada tingkat rendah tetapi dengan kapasitas penyembunyian data rendah.

Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi.

1. *Imperceptibility*. Keberadaan pesan tidak dapat di persepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga haruslah mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.
2. *Fidelity*. Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat di persepsi oleh indrawi.
3. *Recovery*. Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

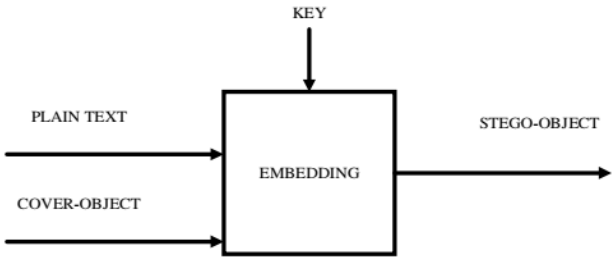
3.3 Properti Steganografi

Properti yang harus diperhatikan dalam melakukan penyembunyian data dengan menggunakan teknik steganografi adalah sebagai berikut:

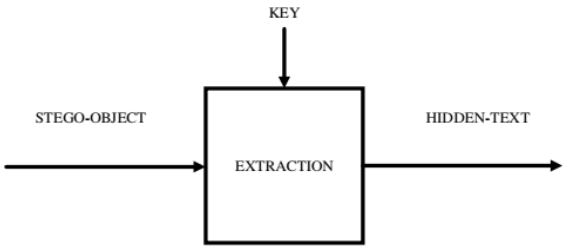
1. *Embedded message* (*hidden text)*: pesan yang disembunyikan.
2. *Cover-object* (*cover text):* pesan yang digunakan untuk menyembunyikan *embedded message*.

3. *Stego-object* (*stego text):* pesan yang sudah berisi pesan *embedded message*.
4. *Stego-key:* kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari stego text.

Dalam steganografi terdapat 2 proses yaitu proses *embedding* untuk menyembunyikan atau menyisipkan pesan dan proses ekstraksi untuk mengambil pesan tersembunyi (Situmorang dkk., 2012). proses tersebut dapat dilihat pada gambar 2 dan 3.



Gambar 2. Proses Penyisipan Pesan



Gambar 3. Proses Ekstraksi Pesan

Pada domain spasial teknik steganografi yang digunakan adalah teknik *Least Significant Bit* (LSB). Teknik LSB konvensional dan variasinya menyediakan cara mudah untuk menyembunyikan informasi (Anwar, 2018). Metode domain spasial sangat toleran terhadap penambahan *noise* pada level rendah tetapi dengan kapasitas menyembunyikan data rendah. Langkah-langkah untuk menyembunyikan informasi rahasia menggunakan *Least Significant Bit* (LSB) adalah (Kadam dkk, 2012):

1. Menyembunyikan *file* audio ke dalam aliran bit.
2. Mengonversi setiap karakter dalam informasi rahasia ke dalam aliran bit.
3. Mengganti bit LSB dari *file* audio dengan bit LSB dari karakter dalam informasi rahasia.

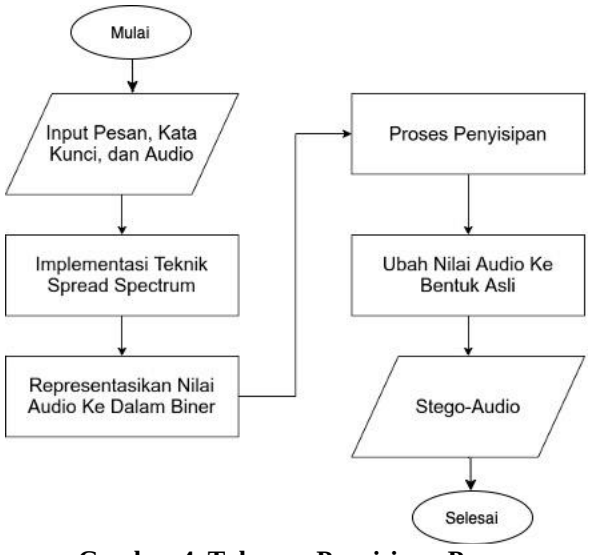
Pada domain transformasi teknik steganografi yang digunakan adalah *Spread Spectrum*. Metode *Spread Spectrum* merupakan metode untuk menyisipkan data dengan cara menyebarkan data rahasia sepanjang sinyal *audio cover*. Metode *Spread Spectrum* mentransmisikan sebuah sinyal pita informasi yang sempit (*narrowband*) ke dalam sebuah kanal pita lebar (*wideband*) dengan penyebaran frekuensi. Penyebaran ini berguna untuk menambah tingkat redundansi. Ini dapat dilakukan dengan memodulasi gelombang sinyal *narrowband* pada gelombang *wideband*. Setelah disebar, energi dari sinyal *narrowband* akan melemah dan akan sulit dideteksi. Dalam konteks steganografi, sinyal *narrowband* dapat kita asumsikan sebagai data atau pesan rahasia yang ditumpangkan, dan *wideband* sebagai *cover carrier*, ini akan menyebabkan nilai *Signal to Noise Ratio* (SNR) menjadi rendah. Hal ini menunjukkan bahwa tidak mudah mendeteksi adanya pesan rahasia pada *cover carrier*.

4. PEMBAHASAN

Parameter yang digunakan untuk membandingkan teknik steganografi domain spasial dengan domain transformasi adalah dalam hal kualitas audio sebelum dan sesudah disisipkan, serta kualitas pesan rahasia yang sudah diekstraksi.

4.1 Penyisipan Pesan

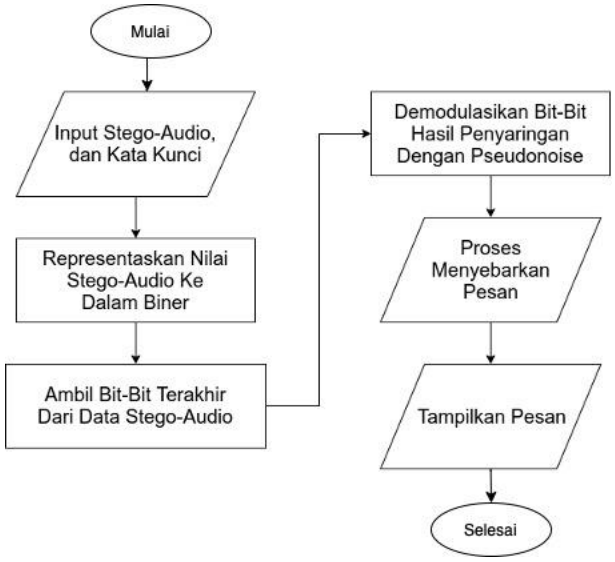
Sistem untuk menyisipkan pesan pada audio membutuhkan masukan berupa audio dengan format MP3 (*cover-file*), pesan yang akan disisipkan (*message*), kunci (*key*), dan faktor pengali cr. Untuk proses penyisipan pesan, pertama dilakukan proses penyebaran (*spreading*) bit–bit informasi dari pesan yang akan disisipkan (*message*) dengan mengalikan bit-bit pesan dengan faktor pengali cr. Setelah itu, bit–bit informasi hasil penyebaran itu akan dimodulasi dengan pseudo-noise signal yang dibangkitkan menggunakan algoritma LCG secara acak berdasarkan kunci penyembunyian nya (*key*). Hasil dari proses modulasi ini akan disisipkan sebagai noiseke dalam sebuah berkas media audio MP3 *(cover-file*). Media yang telah disisipi inilah yang disebut stego-audio. Alur proses penyisipan pesan menggunakan metode *Spread Spectrum* ditunjukkan pada Gambar 4.



Gambar 4. Tahapan Penyisipan Pesan

4.2 Ekstraksi Pesan

Sistem untuk ekstraksi pesan dari audio membutuhkan masukan berupa stego-audio, kunci (*key*), dan faktor pengali cr. Untuk proses ekstraksi pesan, pertama dilakukan proses penyaringan terhadap media yang telah disisipi (*stego-file*) untuk mendapatkan noise. *Noise* ini yang kemudian akan di-dimodulasi dengan menggunakan *pseudo-noise signal* yang sama dengan *pseudo-noise signal* hasil pembangkitan berdasarkan kunci (*key*) pada proses penyisipan, untuk mendapatkan bit–bit yang berkorelasi. Proses selanjutnya adalah melakukan proses de-spreading menggunakan faktor pengali cr untuk menghasilkan bit–bit informasi sesungguhnya. Alur proses ekstraksi pesan menggunakan metode *Spread Spectrum* ditunjukkan pada Gambar 5.



Gambar 5. Tahapan Ekstraksi Pesan

4.3 Pembangkitan Bilangan Acak Semu

Proses penyisipan dan ekstraksi membutuhkan kunci sebagai *seed* dalam pembangkitan deretan bilangan acak. Deretan bilangan acak ini memakai algoritma LCG (*Linear Congruently Algorithm*) yang menghasilkan bilangan semu acak (*pseudorandom*). Deret bilangan *pseudorandom* adalah deret bilangan yang kelihatan acak dengan kemungkinan pengulangan yang sangat kecil atau periode pengulangan yang sangat besar. Jumlah bilangan acak yang dihasilkan adalah sebanyak biner pesan.

4.4 Pengukuran Kualitas Audio

Penilaian kualitas berkas audio MP3 tersebut dilakukan secara subjektif dan objektif. Penilaian subjektif dengan cara mendengarkan suara hasil pemutaran berkas audio MP3. Penilaian objektif dengan cara menghitung nilai PSNR (*Peak Signal to Noise Ratio*). PSNR didefinisikan sebagai rasio antara maksimum kekuatan yang mungkin dari sinyal dan kekuatan distorsi *noise* yang mempengaruhi kualitas sinyal (R. Kumar, 2016). Nilai PSNR dalam satuan desibel (dB) dihitung dengan persamaan (1)

$$\text{PNSR}=10\log_{10}\left(\frac{\text{P1}^2}{\text{P1}^2+\text{P0}^2-2\text{P1P0}}\right) \qquad (1)$$

Dari persamaan (1) dengan P_0 menyatakan kekuatan sinyal awal dan P_1 menyatakan kekuatan sinyal setelah disisipi data. P_0 dan P_1 diukur dalam satuan desibel (dB). Nilai PSNR yang wajar pada pembandingan dua berkas audio berkisar pada 30-50 dB.

4.5 Domain Spasial (LSB)

Dalam pengujian ini menggunakan dalam satu *cover file* yaitu Maher Zain – Barakallah.mp3. *File-file* yang pengujian ini untuk mengetahui pengaruh ukuran file yang disisipkan terhadap ukuran akhir *stego file*.

Dari tabel 1 dan 2 dapat dilihat bahwa kualitas *stego file* yang dihasilkan bergantung pada ukuran file yang disisipkan ke dalam *cover file*. Semakin besar ukuran file yang disisipkan maka akan semakin besar pula penurunan kualitas *stego file* yang dihasilkan. Selain itu penyisipan file yang terlalu besar akan merusak kualitas *file* itu sendiri.

Tabel 1. Uji Coba Penyisipan *File*

Cover *File* (MP3)	**Ukuran (Mb)**	***File* yang disisipkan**		**Ukuran Akhir (Mb)**
Maher Zain - Barakallah	3,69	Nama	Ukuran (Kb)	
		Cv.doc	33	3,69
		Gambar.jpg	15	3,69

Tabel 2. Hasil *Retrieve File*

Cover *File* (MP3)	**Ukuran (Mb)**	***File* yang disisipkan**		**Ukuran setelah retrieve (Kb)**
Maher Zain – Barakallah	3,69	Nama	Ukuran (Kb)	
		Cv.doc	33	33
		Gambar.jpg	15	15

4.6 Domain Transformasi (*Spread Spectrum*)

Proses dari pengujian ini adalah pertama menyisipkan pesan ke dalam audio, kemudian melakukan ekstraksi untuk mendapatkan kembali pesan. Audio yang menjadi media penyisipan adalah sebuah berkas audio MP3 (Barakallah.mp3). *File* yang menjadi pesan adalah sebuah *file* teks dan *file* gambar, yang isinya ditunjukkan pada Tabel 3. String kunci yang digunakan adalah string ‘audio’ dengan faktor pengali cr = 3. Setelah proses penyisipan, dilakukan proses ekstraksi untuk mendapatkan pesan dari masing-masing audio. Digunakan kunci yang sama yaitu string “audio”, sehingga diharapkan isi pesan yang dihasilkan juga sama. Isi dari file hasil ekstraksi, dapat dilihat pada Tabel 4.

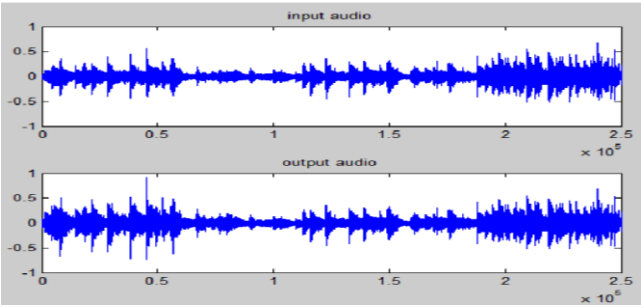
Tabel 3. Isi *File* Penyisipan

Jenis *File*	Isi *File*
File Teks	Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian pesan rahasia ke dalam suatu media sedemikian sehingga pihak ketiga tidak menyadari keberadaan pesan tersebut.
File Gambar	

Tabel 4. Isi *File* Ekstraksi

Jenis *File*	Isi *File*
File Teks	Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian pesan rahasia ke dalam suatu media sedemikian sehingga pihak ketiga tidak menyadari keberadaan pesan tersebut.
File Gambar	

Seperti yang ditunjukkan pada gambar 6, kami mengambil *file* mp.3 musik dan *file* gambar. Dalam *imperceptibility* dari algoritma yang diberikan dievaluasi dengan menghitung PSNR, Nilai PSNR dari sinyal audio tertanam adalah 40.02 dB.



Gambar 6. Input dan Output Audio

Dari hasil pengujian pada tabel 5, dapat dilihat bahwa nilai PSNR berada dalam kisaran nilai PSNR yang wajar, yang berarti indra manusia tidak dapat membedakan perbedaan yang ada pada kedua audio. Kualitas audio steganografi yang dihasilkan metode *Spread Spectrum* lebih baik dari pada metode *Least Significant Bit* (LSB) dibuktikan oleh nilai SNR yang dihasilkan metode *Spread Spectrum* lebih besar atau lebih baik dibandingkan metode *Least Significant Bit* (LSB). Untuk menyisipkan *file* yang berukuran besar membutuhkan *cover file* yang berukuran besar pula.

Tabel 5. Hasil Pengukuran

Jenis *file* pesan	Nilai PSNR (dB)
File teks	41.75
File gambar	40.02

5. KESIMPULAN

Ukuran akhir (*stego file*) memiliki ukuran yang sama dengan *cover file*, karena pesan hanya disisipkan dengan cara mengganti bit terakhir *cover file* bukan menambahkan ke dalam *cover file*. Ini menunjukkan pada metode LSB ukuran pesan yang dimasukkan tidak akan mengubah ukuran *cover file*. Kekurangan penggunaan teknik LSB dalam steganografi adalah kualitas *stego file* yang dihasilkan bergantung pada ukuran *file* yang disisipkan ke dalam cover *file.* Semakin besar ukuran *file* yang disisipkan maka akan semakin besar pula penurunan kualitas *stego file* yang disebabkan, selain menyebabkan penurunan kualitas *stego file*, penyisipan *file* yang terlalu besar akan merusak kualitas *file* itu sendiri.

Metode *Spread Spectrum* mampu memberikan kontribusi kinerja yang lebih baik di beberapa daerah dibandingkan dengan pengodean LSB, tetapi penyebaran metode *Spectrum* memiliki satu kelemahan utama yang dapat memperkenalkan kebisingan ke dalam sebuah file audio.

6. SARAN

Saran untuk penelitian ini adalah bisa menggunakan teknik steganografi yang lain, sehingga didapat hasil yang lebih bervariasi.

7. DAFTAR PUSTAKA

Adhanadi, F., Novamizanti, L., & Budiman, G. (2020). DWT-SMM-based audio steganography with RSA encryption and compressive sampling. *Telkomnika (Telecommunication Computing Electronics and Control)*, *18*(2), 1095–1104. https://doi.org/10.12928/TELKOMNIKA.v18i2.14833

Anwar, N. (2018). Perancangan Steganografi Hidden Message Dengan Metode Least Significant Bit Insertion (Lsb) Berbasis Matlab. *Jurnal Algoritma, Logika Dan Komputasi*, *1*(1), 25–30. https://doi.org/10.30813/j-alu.v1i1.1107

Arraziqi, D., & Haq, E. S. (2019). Optimization of video steganography with additional compression and encryption. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(3), 1417–1424. https://doi.org/10.12928/TELKOMNIKA.V17I3.9513

Bhowal, K., Bhattacharyya, D., Jyoti, A., & Kim, P. T. (2013). *A GA based audio steganography with enhanced security*. 2197–2198. https://doi.org/10.1007/s11235-011-9542-0

Dulera, S., Jinwala, D., & Dasgupta, A. (2011). *E XPERIMENTING WITH THE N OVEL A*

PPROACHES. *3*(6).

Edisuryana, M., Isnanto, R. R., & Somantri, M. (2013). Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End of File. *Transien*, *2*, 1–9.

Ghasemi, E., Shanbehzadeh, J., & Fassihi, N. (2011). *High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm*. *I*, 16–19.

Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011). *INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY*. *3*(3), 86–96.

Kadam, K., Koshti, A., & Dunghav, P. (2012). *Steganography Using Least Signicant Bit Algorithm*. *2*(3), 338–341.

Kour, J. (2014). *Steganography Techniques – A Review Paper*. *9359*(5), 132–135.

Kumar, R. (2016). *Audio Steganography using QR Decomposition and Fast Fourier Transform*. *December 2015*. https://doi.org/10.17485/ijst/2015/v8i1/69604

Nehru, G., & Dhar, P. (2012). *A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach*. *9*(1), 402–406.

Saurabh, J., & Ambhaikar, A. (2012). *Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security*. *1*(2), 62–65.

Situmorang, M., Arisandi, D., & Utara, U. S. (2012). *Implementasi Steganografi Pesan Text Ke Dalam File Sound (. Wav) Dengan Modifikasi Jarak Byte Pada Algoritma Least Significant Bit (Lsb)*. *1*(1), 50–55.

Ukkas, M. I., Andrea, R., & Anggen, A. B. P. (2017). Teknik Pengamanan Data Dengan Steganografi Metode End of File (Eof) Dan Kriptografi Vernam Cipher. *Sebatik*, *17*(1), 20–26. https://doi.org/10.46984/sebatik.v17i1.82