Steganografi Audio Stereo Tersinkronisasi Berbasis SS Dengan Metode Gabungan LWT-SVD

Rizky Eka Liyanty[1], Bambang Hidayat[2], Gelar Budiman[3]
[1,2,3]Fakultas Teknik Elektro, Universitas Telkom, Bandung, Jawa Barat 40257
ekaliyanty@gmail.com[1], bhidayat@telkomuniversity.ac.id [2], gelarbudiman@telkomuniversity.ac.id[3]

Abstrak *- Steganografi dalam audio stereo adalah teknik untuk menyembunyikan data atau informasi rahasia pada media berupa audio stereo tanpa menimbulkan kecurigaan pihak lain. Dalam penelitian ini akan diimplementasikan suatu sistem steganografi audio stereo dalam domain frekuensi dengan menggunakan metode Compressive Sampling (CS), Spread Spectrum (SS), Lifting Wavelet Transform (LWT), dan Singular Value Decomposition (SVD) dengan sinkronisasi dan Quantization Index Modulation (QIM). Pertama, dilakukan transformasi sinyal audio dengan LWT kemudian didekomposisikan pada matriks nilai singular oleh proses SVD. Terdapat dua proses yang dilakukan yaitu proses embedding untuk menyisipkan pesan rahasia yang berupa teks ke dalam cover audio dan proses ekstraksi. Sebelum proses embedding, data rahasia dimodulasi dengan SS lalu dikompres oleh CS kemudian ditambahkan bit sinkronisasi. Di penerima dilakukan proses ekstraksi yang merupakan proses kebalikan dari teknik yang dilakukan pada sisi pengirim. Hasil yang diharapkan dari usulan metode steganografi ini yaitu performansi yang optimal terhadap robustness, imperceptibility, fidelity, dan recovery.*

Kata kunci: *Stereo Audio Steganography, LWT, SVD, SS.*

1. Pendahuluan

Sekarang ini teknologi informasi dan komunikasi berkembang semakin canggih dan modern. Pertukaran informasi dapat dilakukan dimanapun dan kapanpun dengan menggunakan internet secara *real time*. Namun dibalik kenyamanan yang diberikan oleh teknologi internet terdapat kekurangan dari segi keamanannya yaitu pihak lain dapat mengetahui informasi yang dikirimkan selain pengirim dan penerima. Oleh karena itu dibutuhkannya suatu teknik untuk dapat mengamankan informasi tersebut.

Steganografi adalah salah satu teknik untuk menyembunyikan data atau informasi pada suatu media tanpa menimbulkan kecurigaan pihak lain karena yang mengetahui informasi tersebut hanya pengirim dan penerima saja [1]. Data rahasia yang akan disisipkan disebut *file stego* sedangkan media penyisipannya disebut cover/*host* yang berupa audio. Penyisipan informasi kedalam *host* dilakukan dengan menggunakan *key* yang hanya diketahui oleh pengirim dan penerima saja [2].

Agar dapat dikatakan *file* stego yang baik, ada empat kriteria yang harus diperhatikan dalam steganografi, yaitu:

1. *Imperceptible*
   Cover dan *file stego* harus tidak dapat dibedakan oleh indra manusia agar pesan tidak dapat dipersepsi oleh manusia.
2. *Fidelity*
   Mutu *cover* sebelum dan setelah disisipi pesan rahasia tidak jauh berubah. Sehingga perubahan tersebut tidak dapat dideteksi oleh indra manusia.

3. *Recovery*
   Pesan rahasia yang disembunyikan pada *cover* harus dapat diekstrak kembali agar dapat digunakan oleh penerima.
4. *Robustness*
   Pesan rahasia yang disembunyikan harus tahan terhadap berbagai operasi manipulasi yang dilakukan pada *cover*, seperti kompresi, *resampling, echo, pitch shifting*, dan lain-lain.

Dalam beberapa penelitian terkait sebelumnya,seperti pada hasil penelitian [3][4] dengan metode *spread spectrum* memiliki ketahanan yang kuat terhadap serangan umum pemrosesan sinyal dan memiliki kualitas persepsi yang tinggi. Namun dari [3] beberapa serangan yang diujikan, terdapat hasil paling rendah pada tipe serangan MPEG *compression*. Pada penelitian [5] didapatkan hasil bahwa dengan metode gabungan *Discrete Wavelet Transform* (DWT) dan *synchronization codes* menghasilkan *robustness* yang baik untuk beberapa serangan. Tetapi untuk jenis serangan *echo* dihasilkan nilai ketahanan yang paling rendah. Penggabungan metode DWT dengan beberapa metode lain pada penelitian [6][7] memiliki nilai ODG, BER dan PSNR yang baik serta tahan terhadap berbagai serangan. Metode LWT pada penelitian [8][9] menghasilkan nilai SNR yang tinggi dengan robustness yang kuat setelah dilakukan beberapa uji coba serangan seperti *gaussian noise, low pass filter, resample*, dan lain-lain. Pada penelitian [10][11] digunakan metode SVD dan didapatkan hasil bahwa audio watermark memiliki kualitas serta *imperceptibility* yang baik. Metode *compressive sampling* pada penelitian [12] menghasilkan peningkatan kapasitas *embedding,* keamanan dan *transparency* yang lebih baik, namun pada uji coba serangan berupa AWGN menghasilkan nilai terendah dibandingkan serangan yang lain. Sedangkan pada penelitian [13] digunakan metode modifikasi *embedding* dengan *multicarrier modulation* dimana dihasilkan nilai ODG>-1 dan BER<5% yang memiliki ketahanan yang baik terhadap serangan yang diujikan.

Dalam penelitian ini akan diimplementasikan metode LWT-SVD-SS-CS dalam suatu sistem steganografi audio stereo untuk meningkatkan kualitas terhadap *robustness*, *imperceptibility*, *fidelity,* dan *recovery*. Terdapat dua proses yang dilakukan yaitu proses embedding dan ekstraksi. Proses embedding adalah proses menyisipkan pesan rahasia ke dalam cover audio pada sisi pengirim. Pertama, dilakukan transformasi sinyal audio dengan metode LWT dalam pemilihan subband frekuensi dengan tiga tahap yaitu *split/merge*, *prediction,* dan *update* [14]. Frekuensi keluaran dari proses LWT akan didekomposisikan dengan matriks nilai singular oleh proses SVD [15][16]. Keluaran dari proses SVD yaitu berupa matriks U, δ, dan V. Kemudian dilakukan penyisipan data rahasia ke dalam dengan QIM. Sebelum proses embedding, data rahasia dimodulasi dengan SS lalu dikompres oleh CS untuk mendapatkan matriks yang lebih kecil dan ditambahkan bit sinkronisasi. Data rahasia yang digunakan berupa teks. Di penerima dilakukan proses ekstraksi untuk mendapatkan kembali pesan rahasia. Pada proses ekstraksi, dilakukan pembacaan terhadap file stego audio. Proses selanjutnya sama seperti pada proses embedding yaitu melalui proses LWT-SVD lalu dilakukan ektraksi dengan QIM. Setelah itu, ditambahkan bit sinkronisasi dan dilakukan proses rekonstruksi CS yang keluarannya akan didemodulasi dengan SS. Akhirnya, didapatkan pesan rahasia asli dengan nilai error minimum pada sisi penerima.

Paper ini dideskripsikan sebagai berikut: bagian 2 mendeskripsikan tentang konsep teoritis dan rumus dari metode yang digunakan dalam sistem steganografi. Pada bagian 3 menjelaskan pemodelan sistem, termasuk proses embedding dan ekstraksi dari metode steganografi ini. Kemudian, bagian 4 menjelaskan hasil dan analisis parameter kinerja dari metode yang digunakan. Akhir dari paper ini yaitu bagian 5 yang berisi simpulan dari penelitian ini.

ISBN: 978-602-512-810-3

2. Metode Penelitian

Pada penelitian ini digunakan beberapa metode gabungan yaitu:

2.1 Lifting Wavelet Transform (LWT)

Lifting Wavelet Transform (LWT) merupakan salah satu jenis dari transformasi wavelet [17]. LWT dirancang untuk mengurangi waktu komputasi dan kebutuhan memori. LWT memiliki beberapa sifat unik dibandingkan dengan wavelet tradisional.

Skema *lifting wavelet* terdiri dari beberapa langkah yaitu [18]:

1. *Split*, yaitu proses pembagian sampel menjadi genap (even) dan ganjil (odd).
   Data original $x(n)$ dibagi menjadi sample ganjil dan genap dengan rumus berikut:

$$xe(n) = x(2n) \tag{2.1}$$

$$xo(n) = x(2n+1) \tag{2.2}$$

2. *Predict*, *xe(n)* digunakan dalam memprediksi xo(n), dengan persamaan rumus berikut:

$$d(n) = xo(n) - p[xe(n)] \tag{2.3}$$

   dimana p adalah bagian yang memprediksi, *d(n)* adalah prediksi error yang menjadi koefisien wavelet (*high pass filter*).
3. *Update*, merupakan langkah menggantikan sampel genap dengan rata-rata nilai. Berikut adalah rumus fase *update*:

$$c(n) = xe(n) + u[d(n)] \tag{2.4}$$

   dimana *u* adalah operator *update*. Pada LWT, *c(n)* disebut koefisien skala *(low pass filter*).

Sedangkan untuk proses kebalikan dari LWT yaitu I*nvers* LWT (ILWT) dilakukan beberapa langkah yaitu:

1. *Update*
   Pada ILWT dilakukan proses kebalikan dari LWT yaitu pengurangan dengan rumus berikut:

$$(n)=(n)-U[d(n)] \tag{2.5}$$

2. *Predict*
   Pada LWT dilakukan pengurangan dengan nilai prediksi, maka pada ILWT untuk mendapatkan sinyalnya dilakukan penambahan antara detail sinyal dan prediksi sinyal sehingga didapatkan sinyal ganjil.

$$(n)=(n)+P[xe(n)] \tag{2.6}$$

3. *Merge*
   Langkah terakhir untuk mendapatkan sinyal asli adalah dengan menggabungkan antara sinyal ganjil dan sinyal genap, sebagai berikut.

$$x(2n) = xe(n) \tag{2.7}$$

$$(2n+1)=(n) \tag{2.8}$$

$$(n)=(n)+xo(n) \tag{2.9}$$

2.2 Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) merupakan suatu teknik untuk mendekomposisikan matriks berukuran apa saja untuk mempermudah pengolahan data. SVD diaplikasikan dalam memilih subband. Berikut merupakan persamaan dari perhitungan SVD [10] :

$$\text{I} = \text{U} \sum V^T = \sum_{i=1}^{r} \delta(i)u(i)v(i)^T = \sum_{i=1}^{r} u(i)\delta(i)v(i)^T \tag{2.10}$$

ISBN: 978-602-512-810-3

Dimana I € R^{NxM}, U € R^{NxM} , ∑€ R^{MxN}, dan V € R^{MxN}, $\delta(i)$ merupakan *singular value* dari matriks I (elemen diagonal dari ∑) dengan ketentuan berikut:

$$\delta(1) \geq \delta(2) \geq ... \geq \delta(r) > \delta(r+1) = ... \delta(r) = 0 \quad (2.11)$$

Pada proses *Invers* SVD (ISVD) dilakukan proses kebalikan dari SVD untuk mendapatkan sinyal stego audio, dengan menggunakan persamaan berikut:

$$A(i)^s = U \sum V^T \quad (2.12)$$

Dimana A adalah sinyal input yang akan didekomposisikan kedalam *singular vector* matriks U, V adalah *singular vector matrix,* dan δ adalah diagonal matriks yang memiliki nilai eigen dari sinyal input seperti bagian diagonal.

2.3 Spread Spectrum (SS)

Metode *Spread Spectrum* (SS) merupakan metode yang memanfaatkan domain frekuensi. Proses modulasi ini dilakukan dengan cara setiap bit diwakili oleh berbagai bit menggunakan *spreading code* yang disebarkan pada frekuensi yang lebih luas. Adapun algoritma dalam SS yaitu [19]:

$$w(n) = \sum_{m=0}^{M-1} a_m \, s(n - mN_b) \quad (2.13)$$

Sinyal spreading *w(n)* dicapai dengan menyebarkan *M* bit *k* (dalam {0,1}) dari sinyal stego yang menggunakan sinyal *spread spectrum s(n)* lalu dikombinasikan dengan N_b sample.
Dimana a_m merupakan sebuah simbol dalam {-1,+1} yang diberikan oleh a_m = *2k-1* dan bisa disesuaikan dengan vector direction berikut [19]:

w_m = +s ; jika a_m = +1 (2.14)
w_m = -s ; jika a_m = -1 (2.15)

2.4 Compressive Sampling (CS)

Compressive Sampling merupakan metode kompresi yang dalam prosesnya diambil *sample* dengan jumlah sedikit dan acak berdasarkan pada transformasi proyeksi yang digunakan. Pada prinsipnya, CS bergantung pada dua prinsip: *sparsity* yang berkaitan dengan sinyal yang menarik, dan inkoherensi yang berkaitan dengan modalitas penginderaan.

Tujuan dari *Compressive Sampling* adalah untuk memperoleh lebih sedikit dari jumlah sampel yang diperlukan sebelumnya dimana sinyal *recovery* masih sempurna.
Transformasi pada CS meliputi:

1. *Sparsity transform* (ψ).
   Membuat suatu sinyal menjadi bersifat *sparse*, dipakai untuk mencari komponen *sparse* dari sinyal.
2. *Projection transform* (ϕ).
   Mengompres atau mencuplik suatu sinyal, digunakan dalam operasi pengukuran dan pengamatan.

CS dapat merekonstruksi sinyal dengan menggunakan sejumlah pengukuran acak yang disebut *sensing matrix* dan sinyalnya harus berjarang. Suatu sinyal $x \in R^N$ adalah *k-sparse* ketika hampir seluruh elemen k dari x adalah *non-zero*. Bila $f \in R^N$ adalah sinyal *k-sparse* pada ruang ψ yang merupakan kombinasi linear dari N, maka ψ merupakan suatu basis ortonormal dan f muncul dengan persamaan

$$f = \psi x \quad (2.16)$$

Lalu sinyal x bisa merepresentasikan suatu sinyal *sparse* dengan menggunakan persamaan

$$x = \psi' f \quad (2.17)$$

dan

$$y = \emptyset f \quad (2.18)$$

ISBN: 978-602-512-810-3

dimana $y \in R^M$ adalah vektor perhitungan dan $\emptyset$ adalah $M \times N$ *sensing matrix*. Lalu persamaan sebelumnya akan diubah menjadi

$$y = \emptyset f = \emptyset \psi x = \phi x \tag{2.19}$$

dimana $\phi \in R^{M \times N}$ merepresentasikan *underdetermined matrix* dengan $M \ll N$.

$$M = O(k)\ log\left(\frac{N}{k}\right) \tag{2.20}$$

Ketika ϕ adalah matriks *random Gaussian*, maka perhitungan merepresantasikan baris dari *sensing matrix* [12].

Pada penelitian ini dipilih model ℓ1-min karena code ini memiliki kelebihan yaitu: (a) fleksibilitas untuk memasukkan informasi sebelumnya ke dalam model decoding, dan (b) *recoverability* yang seragam.

Persamaan untuk ℓ1-min yaitu [20]:

$$\min\{\|x\|_1 : \|Ax - b\|_2 \leq \gamma\} \tag{2.21}$$

Dimana $= Ax$, x adalah *k-sparse* untuk menentukan komponen penting, sedangkan A adalah matriks dengan $A \in R^{m \times n}$.

2.5 Quantization Index Modulation (QIM)

QIM adalah proses pemberian pendekatan nilai terhadap suatu sampel sinyal. Dalam metode ini sinyal *host* terkuantisasi terhadap *file stego* dengan dua atau lebih quantizer, di mana setiap quantizers memiliki indeks masing-masing. Rumus dari QIM yaitu [21]:

$$S(x,m) = Q_m(x) \tag{2.22}$$

Dimana m adalah *file stego* dan $Q_m(x)$ adalah fungsi kuantisasi.

2.5.1 QIM Encoding

Diketahui x adalah host audio yang berisi N sampel dan data disisipkan dalam L sampel, didapatkan persamaan berikut:

$$d[k,1] = d[k,0] + \Delta/2 \qquad d[k,0] < 0$$

$$d[k,1] = d[k,0] + \Delta/2 \qquad d[k,0] > 0 \tag{2.23}$$

dengan $k = 1,2, \ldots, N/L$

Dimana, *d[k,0]* merupakan urutan acak suatu bit data yang terdistribusi uniform dari *[-Δ /2, Δ /2]* dan Δ adalah ukuran jarak kuantisasi. Panjang tiap vector kurang lebih N/L sesuai dengan panjang data yang akan disisipkan pada host audio. *d[k,0]* dan *d[k,1]* digunakan untuk menyisipkan bit 0 dan 1.

Host audio dikuantisasi dengan urutan persamaan vector dalam fungsi embedding berikut:

$$S(x;M_k) = q_\Delta(x + d[k,M_k]) - d[k,M_k] \tag{2.24}$$

Dimana q_Δ adalah fungsi kuantisasi dengan ukuran jarak Δ, yang dapat dirumuskan yaitu:

$$q_\Delta(x) = round(x/\Delta)\,\Delta \tag{2.25}$$

2.5.2 QIM Decoding

Pada proses ekstraksi dilakukan proses kebalikan dari QIM encoding. Rumus untuk QIM decoding yaitu:

ISBN: 978-602-512-810-3

$$\hat{m}_k = arg\ _{i\in(0,1)}\ min\ (\hat{S}(k) - S_i(k))^2 = arg\ _{i\in(0,1)}\ min\ (\hat{S}(n) - S_i\ (n))^2 \quad (2.26)$$

dengan $n = 1,2, \ldots., N/L$

dimana $S_i(k)$ adalah sinyal yang diterima, L adalah jumlah sampel host audio.

2.6. Synchronization Code

Kode sinkronisasi adalah cara untuk mencari posisi tersembunyi bit informatif setelah desinkronisasi serangan. Kode sinkronisasi digunakan untuk meningkatkan keamanan [22]. Persamaan dari proses sinkronisasi tersebut yaitu:

$$(k+1) = \begin{cases} 2x(k) & if \quad 0 \le x(k) \le \frac{1}{2} \\ 2x(k) - 1 & if \quad \frac{1}{2} \le x(k) \le 1 \end{cases} \quad (2.27)$$

di mana $x(k) \in (0,1)$ sebagai kunci rahasia dan ditentukan sebagai $x(k)$ yang dipetakan dalam urutan sinkronisasi $C = \{C(k), 1 \le k \le Lsyn\}$ dengan aturan berikut

$$c(k) = \begin{cases} 1 & if\ x(k) > \tau \\ 0 & if\ otherwise \end{cases} \quad (2.28)$$

Sebelum proses embedding, kode sinkronisasi harus disusun menjadi urutan data biner. Bagian kode sinkronisasi penyisipan dipotong menjadi *Lsyn* segmen audio dan setiap segmen audio yang memiliki sampel P berikut:

$$(k) = (k.P + u) \quad 1 \le l \le L_{syn}, \quad 1 \le u \le \le P \quad (2.29)$$

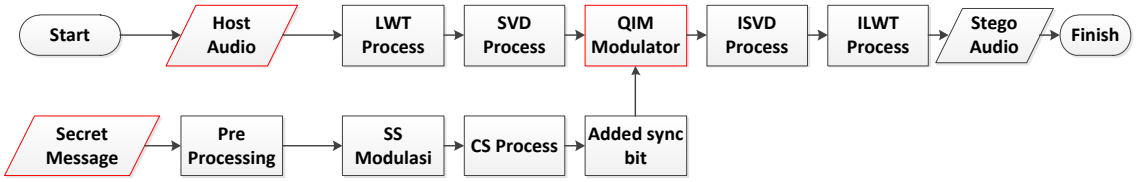
Kemudian masing-masing bit dari kode sinkronisasi yang disisipkan ialah sebagai (k).

2.7 Desain Sistem

Dalam bab ini, dijelaskan proses steganografi. **S**teganografi terdiri atas dua proses, yaitu proses embedding atau penyisipan pesan rahasia dan proses ekstraksi atau proses mendapatkan kembali pesan rahasia yang telah ditumpangkan tersebut.

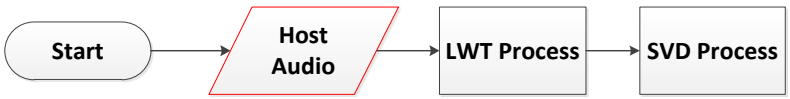
2.7.1 Proses *Embedding*

Berikut merupakan alur proses penyisipan dari steganografi audio:



Gambar 2.1. Diagram Alir Proses *Embedding*

Proses embedding merupakan proses penyisipan pada sisi pengirim sebelum *file* asli menjadi *stego-audio* seperti pada gambar 2.1 di atas.
Pada bagian input yang berupa *host audio* dilakukan proses:



Gambar 2.2. Proses dengan input Host Audio

ISBN: 978-602-512-810-3

Langkah 1: Membaca host audio *x(n)*.
Langkah 2: Lalu dekomposisikan menggunakan LWT untuk mengkonversi data dari bentuk spasial ke bentuk frekuensi dengan persamaan pada (2.1) sampai (2.4). Proses LWT akan menentukan subband frekuensi dalam menyisipkan data rahasia.
Langkah 3: Lakukan proses SVD dengan persamaan (2.10) untuk mendekomposisikan matriks U, δ dan V. Matriks δ akan diteruskan ke proses modulasi QIM.

Sedangkan bagian input yang berupa *secret message* dilakukan proses:

Gambar 2.3. Proses dengan input *Secret Message*

Langkah 4: Ubah pesan rahasia yang berupa *.txt menjadi bit-bit kode dengan pre-processing agar sesuai dengan dimensi host audio. Kemudian pesan rahasia akan disisipkan ke dalam band frekuensi yang diinginkan.
Langkah 5: Stelah itu, pada proses SS modulasi, dilakukan penyebaran bit informasi terhadap band frekuensi dengan persamaan (2.13).
Langkah 6: Pada proses CS, *d(n)* dibagi menjadi 2 proses yaitu bagian *sparsity* (ψ) dan bagian *projection* (Φ).
Langkah 7: Kemudian dilakukan proses penambahan bit sinkronisasi dengan rumus (2.27) dimana akan dilakukan perbandingan antara bit pesan rahasia terhadap host audio agar diketahui posisi awal pesan rahasia pada host audio dari hasil korelasinya.

Kemudian pada *embedding* dilakukan proses penggabungan antara *secret message* dan *host audio* yaitu:

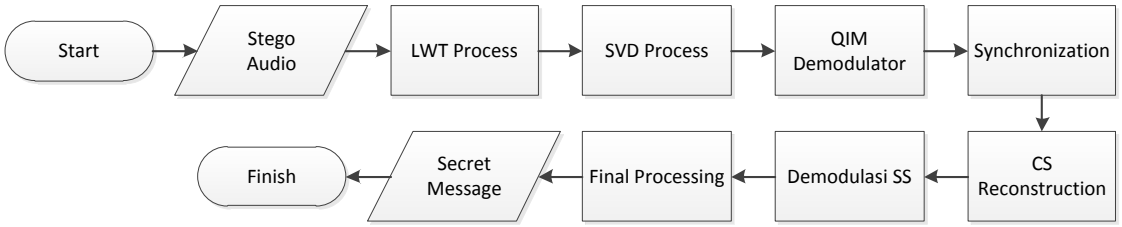
Gambar 2.4. Proses Penyisipan

Langkah 8: Setelah itu pada proses QIM dengan rumus (2.22), dilakukan penyisipan antara host audio dari keluaran proses SVD dengan data rahasia setelah proses sinkronisasi.
Langkah 9: Langkah selanjutnya yaitu proses invers dengan proses ISVD dengan persamaan (2.12).
Langkah 10: Lakukan proses ILWT lakukan proses yang sama yaitu dengan rumus (2.5) sampai (2.9) untuk mendapatkan *stego-audio*.

2.7.2 Proses Extraksi

Berikut merupakan alur proses ekstraksi di sisi penerima sehingga dapat diperoleh pesan rahasia yang telah disisipkan oleh pengirim :

ISBN: 978-602-512-810-3



Gambar 2.5. Diagram Alir Proses Ekstraksi

Proses ekstraksi adalah proses pengambilan pesan rahasia yang disisipkan pada *stego file*. Kunci yang ada pada sisi penerima digunakan untuk mengetahui pada bagian mana pesan rahasia berada. Sebelum dilakukan ekstraksi, *stego-audio* harus melalui proses yang sama pada sisi pengirim

Proses ekstraksi sesuai gambar 2.5 dapat dijelaskan seperti berikut:

Langkah 1: Lakukan pembacaan terhadap *stego audio.*

Langkah 2: Konversikan stego *audio* ke bentuk domain waktu dengan persamaan LWT sesuai persamaan (2.1) sampai (2.4).

Langkah 3: Pilih *band* frekuensi untuk dilakukan proses SVD dengan rumus (2.10), dimana hasilnya akan berupa matriks δ yang akan di teruskan ke proses demodulasi QIM

Langkah 4: Kemudian dilakukan sinkronisasi bit untuk mengetahui posisi awal dari pesan rahasia dalam host audio tersebut dengan persamaan (2.27).

Langkah 5: Lakukan pembagian terhadap *stego-audio* dan pesan rahasia dengan CS rekonstruksi dengan persamaan $\ell 1$-min (2.21).

Langkah 6: Lakukan proses demodulasi SS untuk mengambil bit informasi yang ditumpangkan.

Langkah 7: Lalu ubah pesan rahasia yang berupa bit-bit tersebut menjadi bentuk teks aslinya pada proses *final processing*.

3. Hasil dan Analisis

3.1. Parameter Pengujian secara Objektif

Parameter pengujian secara objektif terbagi menjadi tiga kriteria yaitu:

1. *Signal to Noise Ratio* (SNR)

Signal to Noise Ratio adalah nilai yang menyatakan tingkat noise atas audio yang telah disisipi pesan. SNR digunakan untuk mengukur kualitas audio secara objektif sesuai standar audio yang ada dan batas SNR yang ada dikatakan bagus untuk audio > 25 dB :

$$SNR = 10\ log_{10}\ \frac{\sum_{i=0}^{N-1} S^2(n)}{\sum_{i=0}^{N-1}[\hat{S}(n)-S(n)]^2} \tag{3.1}$$

Dimana :

$S(n)$ = sampel sinyal audio sebelum disisipkan (*host audio*).

$\hat{S}(n)$ = sampel sinyal audio setelah disisipkan (*stego audio*).

N = panjang audio

2. *Bit Error Rate* (BER)

Bit Error Rate merupakan parameter pengujian dimana bagus tidaknya sistem steganografi dan ekstraksi yang telah dibuat didasarkan pada benar atau tidaknya sistem dalam mengekstraksi bit-bit pesan yang telah dikirimkan.

ISBN: 978-602-512-810-3

Adapun cara penghitungan BER, yaitu :

$$\text{BER} = \frac{\sum Bit\ salah}{\sum Bit\ total} \quad (3.2)$$

3. *Objective Difference Grade* (ODG)

Objective Difference Grade adalah parameter pengukuran objektif yang dihitung dengan evaluasi persepsi dari algoritma kualitas audio. Penilaian ODG berkisar dari 0 sampai -4 seperti yang tertuang pada :

Tabel 3.1. Skala ODG

Skala ODG	Deskripsi Kerusakan	Kualitas
0	Tidak terdengar	Baik sekali
-1	Terdengar, tapi tidak mengganggu	Baik
-2	Sedikit mengganggu	Cukup
-3	Mengganggu	Buruk
-4	Sangat mengganggu	Sangat buruk

3.2 Pengujian Secara Subjektif

Mean Opinion Score (MOS) merupakan salah satu parameter pengujian secara subjektif berdasarkan indera pendengaran manusia untuk mengukur tingkat *inaudibility* terhadap perbandingan audio asli dengan audio yang telah disisipkan pesan rahasia. Hasil penelitian terhadap responden diukur dengan kriteria sebagai berikut :

Tabel 3.2. Penilaian MOS

No.	**Skala MOS**	**Kualitas Audio**	**Level Distorsi**
1	$4{,}5 \leq \text{MOS} \leq 5$	Amat Baik	Tidak ada file stego dan audio terdengar jelas
2	$3{,}5 \leq \text{MOS} < 4{,}5$	Baik	File stego masih terasa sedikit namun tidak mengganggu audio
3	$2{,}5 \leq \text{MOS} < 3{,}5$	Cukup	File stego audio masih terasa namun sedikit mengganggu audio
4	$1{,}5 \leq \text{MOS} < 2{,}5$	Kurang	File stego mengganggu namun audio masih dapat didengar
5	$1 \leq \text{MOS} < 1{,}5$	Buruk	File stego mengganggu dan audio tidak terdengar

3.3 Serangan

Adapun beberapa serangan dalam melakukan uji coba pada metode ini yaitu:

1. LPF (*Low Pass Filter*)
   Serangan ini dilakukan dengan cara hanya melewatkan frekuensi rendah saja.
2. *Resampling*
   Resampling merupakan sebuah serangan dengan melakukan pengubahan pada jumlah sampel sinyal.
3. Kompresi MP3
   Serangan ini merupakan tipe kompresi MP3 yang berfungsi untuk memperkecil ukuran audio dan menghasilkan ekstensi MP3 dengan rate kompresi tertentu.

ISBN: 978-602-512-810-3

4. *Echo*
   Serangan ini berupa penambahan reverberasi pada sinyal audio dengan faktor delay dan faktor pengali dari sinyal aslinya.
5. *Pitch Shifting*
   Serangan ini dilakukan dengan memodifikasi skala frekuensi pada audio.
6. Serangan Rekaman secara Wired (DA/AD)
   Serangan DA/AD adalah serangan dengan merekam audio yang akan diambil data rahasianya secara wired. Pengambilan data atau ekstraksi dilakukan pada audio yang telah direkam.

3.4 Hasil Pengujian

Berdasarkan hasil penelitian dengan metode gabungan LWT-SVD-SS-CS dihipotesiskan mampu menghasilkan sistem steganografi audio yang baik dengan kualitas yang tinggi setelah dilakukan beberapa pengujian terhadap serangan. Kualitas ini ditentukan dari beberapa parameter utama, yaitu pengujian secara objektif dengan parameter *Signal to Noise Rasio* (SNR) > 25, *Objective Different Grade* (ODG) > -1, dan *Bit Error Rate* (BER) < 5%, serta pengujian secara subjektif dengan parameter *Mean Opinion Score* (MOS).

4 Kesimpulan

Berdasarkan penggabungan metode dalam penelitian ini, maka dapat didapatkan hasil bahwa steganografi audio dengan metode gabungan LWT-SVD-SS-CS memiliki nilai parameter *Signal to Noise Rasio* (SNR) > 25, *Objective Different Grade* (ODG) > -1, dan *Bit Error Rate* (BER) < 5%. Hal ini mendakan bahwa metode steganografi ini memiliki performansi yang optimal terhadap *robustness*, *imperceptibility*, *fidelity*, dan *recovery*.

Daftar Pustaka

[1] P. Joseph and S. Vishnukumar, "A study on steganographic techniques," *Glob. Conf. Commun. Technol. GCCT 2015*, pp. 206–210, 2015.

[2] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding : Steganography and Watermarking - Attacks and Countermeasures*, 1st ed., no. 1. New York: Kluwer Academic, 2001.

[3] X. Zhao, Y. Guo, J. Liu, and Y. Yan, "A spread spectrum audio watermarking system with high perceptual quality," *Proc. - 2011 3rd Int. Conf. Commun. Mob. Comput. C. 2011*, vol. 2, no. 3, pp. 266–269, 2011.

[4] A. S. Wibowo, A. S. Kusumanegara, and G. Budiman, "Analisis Digital Audio Watermarking Berbasis Lifting Wavelet Transform Pada Domain Frekuensi dengan Metode Spread Spectrum," *Semin. Nas. Inov. Dan Apl. Teknol. Di Ind. 2017 ITN Malang*, pp. 1–6, 2017.

[5] H. Wang, M. Fan, and Q. Qian, "Efficiently Self-synchronized Audio Watermarking Against Re-sampling Attack," *IEEE Int. Conf. Comput. Sci. Eng.*, pp. 335–338, 2011.

[6] G. Budiman, L. Novamizanti, and I. Iwut, "Genetics algorithm optimization of DWT-DCT based image Watermarking," *J. Phys. Conf. Ser.*, vol. 755, p. 11001, 2016.

[7] S. M. Fadhilah, T. Kusumaningsih, G. Budiman, and I. Safitri, "Analisis Optimasi Metode Discrete Wavelet Transform Pada Audio Watermarking Berbasis Cepstrum dengan Algoritma Genetika," *Semin. Nas. Inov. Dan Apl. Teknol. Di Ind. 2017 ITN Malang*, pp. 1–8, 2017.

[8] H. I. Shahadi, R. Jidin, and W. H. Way, "Lossless Audio Steganography based on Lifting Wavelet Transform and Dynamic Stego Key," *Indian J. Sci. Technol.*, vol. 7, pp. 323–334, 2014.

[9] R. Arfina, M. R. Hariadi, and G. Budiman, "Analisis Audio Watermarking Menggunakan Lifting Wavelet Berdasarkan Karakteristik Statistik dari Sub-Band Koefisien dengan Optimasi Algoritma Genetika," *Semin. Nas. Inov. Dan Apl. Teknol. Di Ind. 2017 ITN Malang*, pp. 1–9, 2017.

ISBN: 978-602-512-810-3

[10] B. Lei, I. Y. Soon, and E. L. Tan, "Robust SVD-based audio watermarking scheme with differential evolution optimization," *IEEE Trans. Audio, Speech Lang. Process.*, vol. 21, no. 11, pp. 2368–2378, 2013.
[11] B. Sitompul, F. Raekania, and G. Budiman, "Optimasi Audio Watermarking Berbasis Discrete Cosine Transform dengan Teknik Singular Value Decompositon Menggunakan Algoritma Genetika," *Semin. Nas. Inov. Dan Apl. Teknol. Di Ind. 2017 ITN Malang*, pp. 1–7, 2017.
[12] A. M. Koya, "A Compressive Sensing Approach to DCT Watermarking System," *Int. Conf. Control. Commun. Comput. India*, pp. 495–500, 2015.
[13] G. Budiman, A. B. Suksmono, D. Danudirdjo, K. Usman, and D. H. Shin, "A modified multicarrier modulation binary data embedding in audio file," *Int. J. Electr. Eng. Informatics*, vol. 8, no. 4, pp. 762–773, 2016.
[14] P. K. Dhar, "A blind audio watermarking method based on lifting wavelet transform and QR decomposition," *8th Int. Conf. Electr. Comput. Eng. Adv. Technol. a Better Tomorrow, ICECE 2014*, pp. 136–139, 2015.
[15] P. K. Dhar and T. Simamura, "A Blind LWT-Based Audio Watermarking Using Fast Walsh Hadamard Transform and Singular Value Decomposition," *Circuits Syst. (ISCAS), 2014 IEEE Int. Symp.*, no. 1, pp. 125–128, 2014.
[16] P. K. Dhar and T. Shimamura, "Audio Watermarking in Transform Domain Based on Singular Value Decomposition and Quantization," *APCC*, pp. 516–521, 2012.
[17] C. Xuesongl, C. Haiman, and W. Fenglee, "A Dual Digital Audio Watermarking Algorithm Based on LWT," *Int. Conf. Meas. Inf. Control*, pp. 721–725, 2012.
[18] Q. Zhang, Z. Liu, and Y. Huang, "Adaptive Audio Watermarking Algorithm Based on Sub-band Feature," *J. Inf. Comput. Sci.*, vol. 2, no. February, pp. 305–314, 2012.
[19] S. Shokri, M. Ismail, N. Zainal, and A. Shokri, "Error probability in spread spectrum (SS) audio watermarking," *Int. Conf. Sp. Sci. Commun. Iconsp.*, no. July, pp. 169–173, 2013.
[20] Y. Zhang, "Theory of compressive sensing via ℓ1-minimization: a non-rip analysis and extensions," *J. Oper. Res. Soc. China*, vol. 1, no. 1, pp. 79–105, 2013.
[21] N. Khademi, M. A. Akhaee, S. M. Ahadi, M. Moradi, and A. Kashi, "Audio watermarking based on Quantization Index Modulation in the frequency domain," *ICSPC 2007 Proc. - 2007 IEEE Int. Conf. Signal Process. Commun.*, no. November, pp. 1127–1130, 2007.
[22] V. Bhat K, I. Sengupta, and A. Das, "An adaptive audio watermarking based on the singular value decomposition in the wavelet domain," *ELSEVIER - Digit. Signal Process.*, vol. 20, no. 6, pp. 1547–1558, 2010.

ISBN: 978-602-512-810-3