Jurnal ELKOMIKA
ISSN (p): 2338-8323
ISSN (e): 2459-9638

| Vol. 4 | No. 1 | Halaman 98 - 109
Januari - Juni 2016

Implementasi Teknik *Watermarking* menggunakan FFT dan *Spread Spectrum Watermark* pada Data Audio Digital

HANNAN HARAHAP[1], GELAR BUDIMAN[2], LEDYA NOVAMIZANTI[3]

[1,2,3]Program Studi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro
Telkom University

hannan.aulia@gmail.com

ABSTRAK

Penggunaan teknologi dan internet yang berkembang dengan pesat menyebabkan banyak pemalsuan dan penyebaran yang tidak sah terhadap data digital. Oleh karena itu, sangat diperlukan suatu teknologi yang dapat melindungi hak cipta data multimedia seperti audio. Teknik yang sering digunakan dalam perlindungan hak cipta adalah watermarking karena teknik ini memiliki tiga kriteria utama dalam keamanan data, yaitu robustness, imperceptibility, dan safety. Untuk itu, pada penelitian ini dirancang suatu skema yang dapat melindungi hak cipta data audio. Metode yang digunakan adalah Fast Fourier Transform, yang mengubah data audio asli ke dalam domain frekuensi sebelum dilakukan proses penyisipan watermark dan proses ekstraksi watermark. Watermark disebar pada komponen yang paling signifikan dari spektrum magnitude audio host. Teknik watermarking pada penelitian ini dapat menghasilkan Signal-to-Noise Ratio di atas 20 dB dan Bit Error Rate di bawah 5%.

***Kata kunci**: Audio watermarking, Copyright Protection, Fast Fourier Transform, Spektrum magnitude*

ABSTRACT

The use of technology and internet has grown rapidly that causes a lot of forgery and illegal proliferation of digital data. It needs a technology that can protect the copyright of multimedia data such as audio. The most common technique in copyright protection is watermarking because it has three main criteria in data security: robustness, imperceptibility, and safety. This research created a scheme that can protect a copyright of audio data. The method that we used is Fast Fourier Transform. This method changes the original audio data into frequency domain before the embedding and extraction process. The watermark is spread into the most significant component of the magnitude spectrum of audio host. This technique obtains Signal-to-Noise Ratio above 20 dB and Bit Error Rate below 5%.

***Keywords**: Audio watermarking, Copyright Protection, Fast Fourier Transform, Magnitude spectrum*

1. PENDAHULUAN

Perkembangan internet dan tempat penyimpanan data digital yang meluas menyebabkan banyaknya pemalsuan dan penyebaran data digital secara ilegal. Berdasarkan **(Fallahpour, 2012)**, industri musik sendiri mengalami masalah seperti miliaran *illegal download* di internet setiap tahunnya. Oleh karena itu, sangat diperlukan dilakukan suatu pengembangan teknologi yang kuat untuk melindungi hak cipta dari penyebaran ilegal dan sabotase data digital. Metode *digital watermarking* banyak dikembangkan untuk menyelesaikan masalah tersebut.

Digital audio watermarking adalah proses penyisipan suatu *watermark* (penanda) pada sinyal audio untuk menunjukkan keaslian dan kepemilikan. Penelitian mengenai metode *watermarking* telah banyak dilakukan untuk menciptakan suatu audio *watermark* yang kuat dan tidak terdeteksi. Beberapa metode yang sering digunakan adalah metode transformasi seperti *Discrete Cosine Transform* (DCT), *Discrete Wavelet Transform* (DWT), dan *Fast Fourier Transform (FFT)*. Pada penelitian dengan DCT berjudul "*Audio Watermarking in DCT: Embedding Strategy and Algorithm*" **(Zeng, 2008)**, dihasilkan SNR sebesar 27 dB hingga 28 dB dan *robust* terhadap serangan kompresi mp3. Penelitian lainnya dilakukan di domain *wavelet* yang mengacu pada besar SNR yang ditargetkan, semakin besar SNR yang diinginkan maka BER yang dihasilkan juga semakin besar **(Pooyan, 2007)**.

Salah satu contoh teknik *watermarking* yang menggunakan metode FFT berjudul "*Robust FFT Based Watermarking Scheme for Copyright Protection of Digital Audio Data*" **(Dhar, 2011)**. Penelitian tersebut menghasilkan *watermarked audio* yang *robust* dan nilai SNR yang cukup tinggi, namun *watermark* hanya disisipkan pada segmen tertentu dalam audio. Berdasarkan referensi tersebut, pada penelitian ini dilakukan proses *watermarking* pada domain frekuensi menggunakan FFT. Data *watermark* disebar sepanjang spektrum magnitude dari data *audio host* untuk meningkatkan ketahanan dan kualitas yang dihasilkan. FFT digunakan untuk mentransformasi data ke domain frekuensi dengan lebih cepat dibanding metode transformasi DFT.

Implementasi dari teknik *watermarking* ini dilakukan menggunakan lima buah data audio dengan *genre* yang berbeda dan satu buah citra hitam putih sebagai data *watermark* yang akan disisipkan ke dalam audio.

1.1 *Digital Watermarking*

Digital watermark banyak digunakan sebagai sistem perlindungan hak cipta dari data digital multimedia, seperti audio, gambar, dan video. Data penanda atau *watermark* tersebut dapat berupa gambar, suara, atau teks dan tidak harus sama dengan data asli yang menjadi *host* penyisipan watermark. Pada penelitian yang dilakukan Cox **(Cox, 2008)** disebutkan bahwa ada tiga aspek penting yang membedakan *watermarking* dengan teknik lain. Pertama, *watermark* bersifat tidak terlihat, tidak seperti *bar code*, *watermark* tidak mengurangi estetika dari data gambar *host*. Yang kedua, *watermark* tidak dapat dipisahkan dari data *host* tempat *watermark* tersebut disisipkan. Dan yang terakhir, *watermark* menjalani proses transformasi yang sama dengan data *host*. Artinya transformasi atau proses yang terjadi pada data tersebut dapat diketahui dari *watermark* yang dihasilkan. Ketiga hal tersebut menjadi atribut penting dalam beberapa aplikasi *watermarking*.

Teknik *watermarking* dibagi menjadi dua proses, yaitu proses penyisipan *watermark* dan proses ekstraksi *watermark*. Proses penyisipan *watermark* merupakan proses penggabungan antara data *host* dengan data *watermark*. Proses ektraksi *watermark* adalah proses untuk

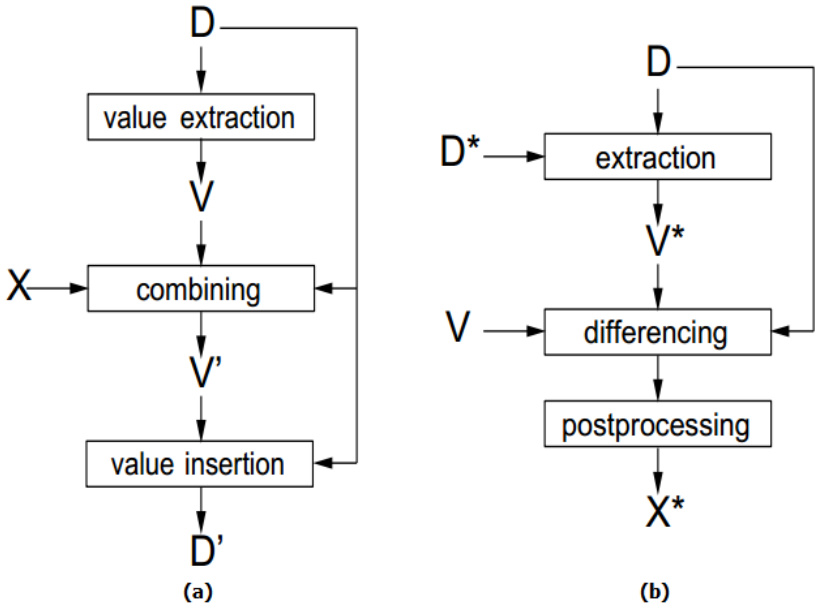
mendapatkan kembali data *watermark* yang telah disisipkan. Secara umum, proses penyisipan dilakukan dengan salah satu dari ketiga persamaan berikut ini:

$$V_i' = V_i + \alpha X_i \quad (1)$$

$$V_i' = V_i(1 + \alpha X_i) \quad (2)$$

$$V_i' = V_i(e^{\alpha X_i}) \quad (3)$$

dimana V_i adalah nilai dari data *host* dan V_i' adalah nilai yang telah disisipkan *watermark*. Variabel X_i merupakan data watermark berupa nilai (0,1) atau (-1,1) dan $\boldsymbol{\alpha}$ adalah skala/intensitas sisipan. Penggunaan salah satu dari ketiga persamaan di atas bergantung dari metode yang digunakan dan tujuan dari *watermarking* yang ingin dicapai. Alur dari teknik *watermarking* pada data digital dapat dilihat pada gambar 1.



Gambar 1. Alur (a) Penyisipan Watermark (b) Ekstraksi Watermark (Cox, 1995)

Terdapat beberapa kegunaan atau aplikasi dari *digital watermarking*, seperti *broadcast monitoring*, identifikasi kepemilikan, bukti kepemilikan, pelacakan transaksi, autentikasi, *copy control*, *device control*, dan *legacy enhancement*. Setiap aplikasi tersebut memiliki kebutuhan dan limitasi yang berbeda dari teknik watermarking **(Cox, 2008)**.

1.2 *Fast Fourier Transform*

Fast Fourier Transform (FFT) adalah suatu transformasi yang mengubah data digital ke domain frekuensi. FFT merupakan salah satu algoritma yang paling sering digunakan dalam menganalisis dan manipulasi data digital. Penelitian **(Rockmore, 2000)** menunjukkan bahwa FFT dapat diterapkan untuk banyak hal, seperti *electroacoustic music* dan pengolahan sinyal audio, pengolahan citra, *medical imaging*, *pattern recognition*, *computational chemistry*, dan lain-lain.

FFT merupakan perhitungan DFT (*Discrete Fourier Transform*) yang lebih efisien. DFT didefinisikan dengan persamaan:

$$\hat{X}(k) = \sum_{j=0}^{N-1} X(j) W_N^{jk} \quad (4)$$

$$\text{dimana } W_N = \exp(\frac{2\pi\sqrt{-1}}{N}) \quad (5)$$

Persamaan tersebut dapat dilihat sebagai matriks dari perkalian titik vektor W_N^{jk} dengan X. *Invers* dari DFT didefinisikan sebagai:

$$X(j) = \frac{1}{N} \sum_{k=0}^{N-1} \hat{X}(k)_j \, W_N^{-jk} \quad (6)$$

Maka, DFT akan membutuhkan perhitungan sebanyak N^2, sedangkan dengan menggunakan FFT perhitungan yang dilakukan hanya sebanyak ($N \log_2 N$).

1.3 Serangan Pada *Watermarking*

Serangan pada *watermarking* dilakukan untuk menguji ketahanan dari teknik *watermarking* tersebut. Serangan diberikan pada *watermarked audio* sebelum melewati proses ektraksi *watermark*. Beberapa contoh serangan yang diberikan adalah *filtering,* kompresi, *resampling*, penambahan *noise*, dan lain-lain. Berikut adalah penjelasan dari serangan tersebut:

a. *Filtering* adalah proses menyaring frekuensi tertentu pada data digital. *Filtering* sendiri dibagi empat, yaitu *low pass filter, high pass filter, band pass filter,* dan *band stop filter*. Frekuensi yang akan disaring ditentukan dari frekuensi *cut-off*.
b. Kompresi adalah proses untuk memperkecil ukuran data digital dengan mengubah *bit rate* data tersebut. Semakin kecil *bit rate* suatu data, maka akan semakin kecil ukurannya.
c. *Resampling* adalah mengubah frekuensi *sampling* dari suatu data digital kemudian mengubah kembali ke frekuensi *sampling* awal.
d. Penambahan *noise* atau derau adalah menambahkan *noise* seperti White noise, Pink noise, Gaussian noise, ke data digital.

1.4 Parameter Evaluasi

Untuk mengevaluasi penelitian ini, diperlukan parameter-parameter untuk menilai keseluruhan performansi. Pada penelitian ini, akan digunakan dua buah parameter untuk mengevaluasi sistem yang dirancang, yaitu SNR dan BER.

SNR atau *Signal-to-Noise Ratio* adalah perbandingan daya dalam suatu sinyal terhadap daya yang dikandung oleh *noise* yang muncul. Semakin besar SNR maka semakin baik kualitas yang dihasilkan. SNR dihitung dengan menggunakan persamaan:

$$SNR = 10 \ log_{10} \frac{\sum_{n=1}^{N} S^2(n)}{\sum_{n=1}^{N} [S(n) - S^*(n)]^2} \quad (7)$$

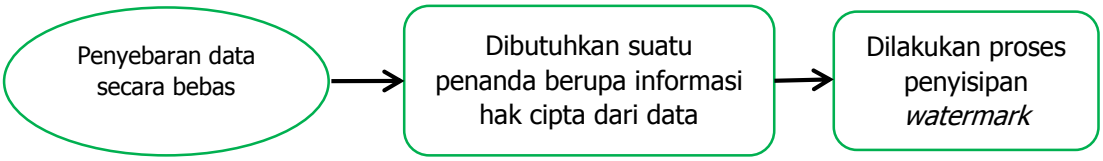
BER atau *Bit Error Rate* adalah perbandingan antara jumlah *error* dengan total data. Semakin besar BER yang dihasilkan maka semakin jelek performansi sistem yang dilakukan. BER dihitung dengan persamaan:

$$BER = \frac{N_{error}}{N_{bits}} \quad (8)$$

2. METODOLOGI PENELITIAN

Tujuan dari penelitian ini adalah mengimplementasikan suatu teknik *watermarking* pada data audio digital yang dapat memproteksi hak cipta data tersebut. Untuk mencapai tujuan tersebut, metodologi dalam penelitian ini terdiri dari beberapa tahap yaitu:

1. Identifikasi masalah penelitian
   Pada tahap ini dilakukan identifikasi dari permasalahan yang ada menggunakan studi literatur. Literatur yang diambil berasal dari hasil penelitian baik dari *paper journal*, *paper conference*, maupun *textbook* yang berkaitan dengan tema penelitian.
2. Desain model dan formulasi masalah
   Pada tahap ini dilakukan desain model dari permasalahan yang akan diselesaikan. Berikut adalah alur desain model dan formulasi masalah:



Gambar 2. Model dan Formulasi Masalah

3. Desain model pemecahan masalah dan kuantifikasi kompleksitas
   Pada tahap ini didesain skema pemecahan masalah tentang teknik *audio watermarking*. Teknik ini dilakukan dengan menggabungkan dua buah data, yaitu data audio *host* dan data *watermarking*, yang menghasilkan suatu data digital yang kuat terhadap serangan *signal processing* dan data ini juga tidak mengubah kualitas dari data *host*. Dengan demikian, data digital tersebut memiliki suatu penanda atau ciri khas yang dapat menjadi bukti kepemilikan.
4. Model pemecahan masalah dan validasi penelitian
   Pada tahap ini dilakukan pengujian terhadap teknik pemecahan masalah secara objektif dan subjektif. Pengujian secara objektif dilakukan dengan perhitungan SNR untuk menganalisis kualitas dari *watermarked audio* dan perhitungan BER untuk menganalisis ketahanan dari *watermarked audio*. Pengujian secara subjektif dilakukan dengan melakukan survei yang membandingkan audio asli dengan *watermarked audio* untuk mendukung analisis dari kualitas *watermarking*.
5. Pengumpulan data dan analisis data
   Data yang digunakan merupakan data hasil pengujian. Analisis yang akan dilakukan adalah untuk mengetahui performansi dari sistem yang dilakukan dengan menghitung SNR dan BER.
6. Penyimpulan hasil
   Kesimpulan penelitian diambil berdasarkan data-data hasil pengujian dan capaian tujuan.

3. HASIL DAN DISKUSI

Untuk melakukan pengujian dari skema yang dirancang, digunakan lima buah data audio yang akan digunakan sebagai audio *host*, dan satu buah citra hitam putih berukuran 130x128 piksel yang akan digunakan sebagai *watermark*. Berikut adalah rincian dari data yang digunakan pada proses pengujian:

Tabel 1. Data Audio *Host*

No.	Nama Audio	*Genre* Audio	Tipe Audio
1	Audio 1	Musik Metal	Wav file, 44100 Hz
2	Audio 2	Musik Klasik	Wav file, 44100 Hz
3	Audio 3	Musik Jazz	Wav file, 44100 Hz
4	Audio 4	Suara Manusia	Wav file, 44100 Hz
5	Audio 5	Musik Pop	Wav file, 44100 Hz

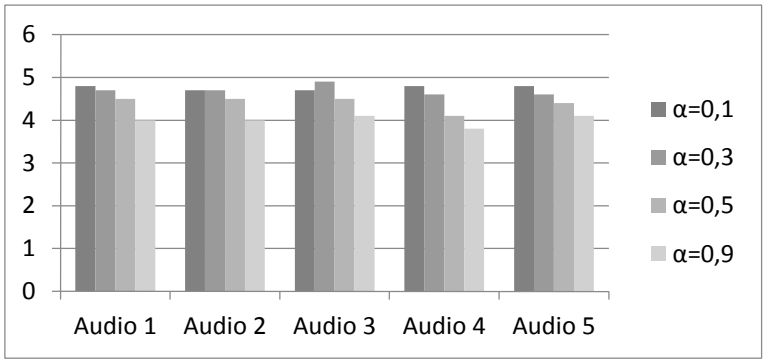
Gambar 3. Citra *Watermark*

3.1 Hasil Uji Kualitas

Pengujian kualitas teknik *watermarking* pada penelitian ini dilakukan dengan dua cara, secara objektif dan subjektif. Pengujian secara kualitas dilakukan dengan melakukan survey kepada 10 orang yang mendengarkan dan membandingkan audio *host* dengan *watermarked audio*. Nilai yang diberikan dari 1-5. Skala penilaian MOS (*Mean Opinion Score*) dapat dilihat pada Tabel 2. Hasil survey dapat dilihat pada Gambar 4.

Tabel 2. Skala Penilaian MOS

Quality		***Impairment***	
5	*Excellent*	**5**	*Impreceptible*
4	*Good*	**4**	*Perceptible, but not anoyying*
3	*Fair*	**3**	*Slightly annoying*
2	*Poor*	**2**	*Annoying*
1	*Bad*	**1**	*Very Annoying*

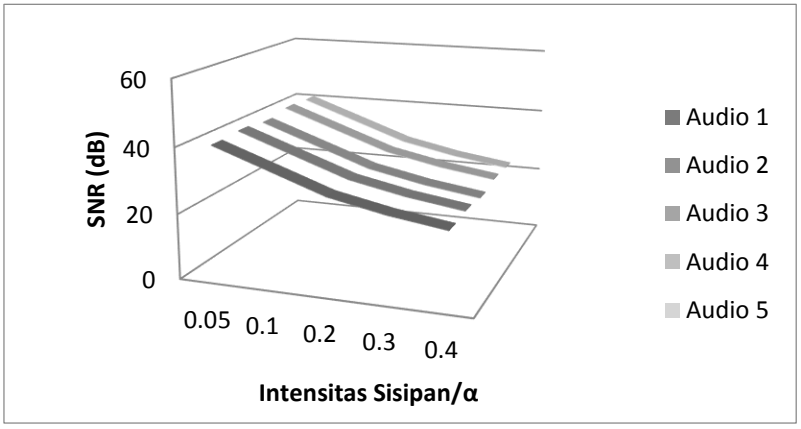


Gambar 4. Grafik *Mean Opinion Score*

Dari Gambar 4 dapat dilihat bahwa *watermarked audio* yang dihasilkan memiliki nilai di atas 3. Hal ini menunjukkan bahwa teknik *watermarking* yang dilakukan tidak mengubah kualitas dari audio aslinya. Pengujian kualitas juga dilakukan secara objektif dengan melakukan perhitungan SNR. Hasil SNR dari penelitian ini dapat dilihat pada Tabel 3.

Tabel 3. Hasil SNR

Name	α=0.05	α=0.1	α=0.2	α=0.3	α=0.4
Audio 1	40,22	34,20	28,17	24,65	22,15
Audio 2	40,71	34,68	28,66	25,14	22,64
Audio 3	39,78	33,76	27,74	24,22	21,72
Audio 4	41,08	35,06	29,04	25,51	23,01
Audio 5	40,64	34,62	28,59	25,07	22,57



Gambar 5. Grafik Pengaruh α Terhadap SNR

Dari Gambar 5 dapat dilihat bahwa besar intensitas yang disisipkan mempengaruhi SNR yang dihasilkan. Semakin besar nilai α maka SNR yang dihasilkan akan semakin rendah. SNR yang dihasilkan dari kelima *genre* audio yang berbeda memiliki nilai yang tidak jauh berbeda. Berdasarkan Tabel 4 dapat dilihat bahwa skema teknik *watermarking* ini dapat menghasilkan nilai SNR yang sangat baik. SNR yang dihasilkan lebih besar dari 20 dB untuk intensitas yang lebih kecil dari 0,4.
Dari hasil MOS dan SNR di atas, dapat disimpulkan bahwa teknik *watermarking* yang dilakukan bersifat *imperceptible* karena tidak mengubah kualitas dari sinyal *host*.

3.2 Hasil Uji Ketahanan

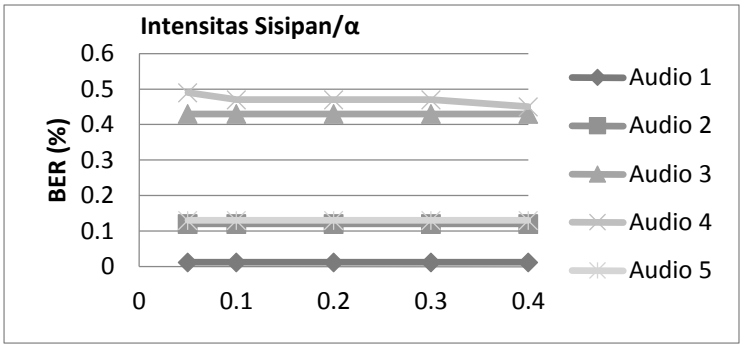
Pengujian ketahanan dilakukan dengan membandingkan dua buah citra hitam-putih, yaitu citra yang didapat setelah hasil ekstraksi dengan citra asli yang disisipkan. Semakin banyak perbedaan antara kedua citra tersebut maka akan semakin besar BER yang dihasilkan. Pengujian ini dilakukan dengan dua cara, dengan menambahkan serangan dan dengan tanpa serangan. Serangan yang ditambahkan berupa *Low Pass Filter* (LPF), penambahan *noise* AWGN, *resampling*, dan kompresi.

3.2.1 Tanpa Serangan

Hasil dari pengujian ketahanan *watermarking* tanpa ditambahkan serangan dapat dilihat pada Tabel 4 dan Gambar 6.

Tabel 4. Hasil BER Tanpa Serangan

Name	α=0.05	α=0.1	α=0.2	α=0.3	α=0.4
Audio 1	0,012%	0,012%	0,012%	0,012%	0,012%
Audio 2	0,12%	0,12%	0,12%	0,12%	0,12%
Audio 3	0,43%	0,43%	0,43%	0,43%	0,43%
Audio 4	0,49%	0,47%	0,47%	0,47%	0,45%
Audio 5	0,13%	0,13%	0,13%	0,13%	0,13%



Gambar 6. Grafik Pengaruh α Terhadap BER

Dari Gambar 6 dapat dilihat bahwa α tidak memberikan pengaruh yang signifikan terhadap nilai BER. BER yang dihasilkan justru bergantung pada jenis audionya. Pada Gambar 5 dapat dilihat bahwa Audio 3 dan Audio 4 memiliki hasil yang hampir sama. Hal ini dikarenakan keduanya memiliki area *silence*. Audio 2 dan Audio 5 juga menunjukkan hasil yang hampir sama karena kedua audio ini memiliki amplituda yang hampir sama. Audio 1 menunjukkan nilai BER yang paling rendah karena audio ini memiliki spektrum magnitude yang besar. Citra hasil ekstraksi dari setiap audio yang memiliki BER yang paling tinggi, yaitu pada α=0,05, dapat dilihat pada Gambar 7.

Gambar 7. Citra Hasil Ekstraksi dengan α=0,05 Pada (a) Audio 1 (b) Audio 2 (c) Audio 3 (d) Audio 4 (e) Audio 5

3.2.2 Dengan Serangan LPF

Pengujian ini dilakukan dengan melakukan *low pass filter* pada *watermarked audio* sebelum melakukan proses ekstraksi. *Filtering* dilakukan dengan frekuensi *cut-off* yang berbeda-beda. Hasil pengujian dengan serangan LPF dapat dilihat pada Tabel 5.

Tabel 5. BER Setelah Serangan LPF

Frekuensi *Cut-off*	BER (%)				
	Audio 1	Audio 2	Audio 3	Audio 4	Audio 5
4000 Hz	9,68	7,05	8,49	4,23	9,14
8000 Hz	1,17	0,45	2,71	0,73	5,99
12000 Hz	0,36	0,12	0,80	0,47	3,06
16000 Hz	0,12	0,12	0,44	0,47	0,4

Dari tabel di atas dapat dilihat bahwa BER yang dihasilkan meningkat. Besar frekuensi *cut-off* juga mempengaruhi besar BER. Jika frekuensi *cut-off* mendekati frekuensi 22050 Hz (fs/2), BER yang dihasilkan akan semakin kecil. Hasil ektraksi citra dengan BER tertinggi dapat dilihat pada Gambar 8.

Gambar 6. Citra Hasil Ekstraksi Setelah LPF dengan Frekunsi *Cut-off* 4000 Hz Pada (a) Audio 1 (b) Audio 2 (c) Audio 3 (d) Audio 4 (e) Audio 5

Dari Gambar 8 dapat dilihat bahwa citra hasil ektraksi tetap bisa terlihat dengan jelas. Oleh karena itu, teknik *watermarking* yang dilakukan memiliki ketahanan yang baik terhadap serangan LPF.

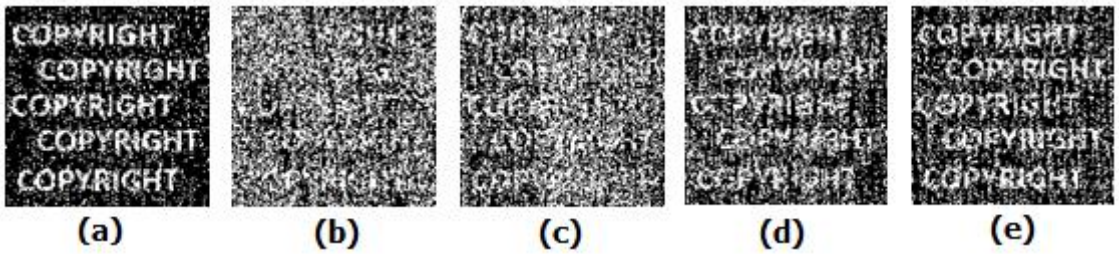
3.2.3 Dengan Serangan AWGN

Pengujian ini dilakukan dengan menambahkan AWGN atau *Addaptive White Gaussian Noise* ke *watermarked audio* sebelum melewati proses ekstraksi. Hasil Pengujian ini dapat dilihat pada Tabel 6.

Tabel 6. BER Setelah Serangan AWGN

PSNR AWGN	BER (%)				
	Audio 1	Audio 2	Audio 3	Audio 4	Audio 5
30 dB	11.91	39.30	37.28	26.53	21.03
40 dB	0.93	20.75	20.06	10.97	5.08
50 dB	0.012	5.48	6.00	1.98	0.22
60 dB	0.012	0.26	0.77	0.55	0.14

Dengan menambahkan AWGN dengan PSNR (*Peak Signal to Noise Ratio*) sebesar 30 dB dapat merusak citra *watermark* yang disisipkan. Tetapi pada AWGN dengan PSNR di atas 40 dB, citra hasil ektraksi tidak terlalu rusak dan mulai terlihat jelas. Citra hasil ekstraksi dengan BER tertinggi pada kelima data audio tersebut dapat dilihat pada Gambar 9.



Gambar 7. Citra Hasil Ekstraksi Setelah Serangan AWGN sebesar 30 dB Pada (a) Audio 1 (b) Audio 2 (c) Audio 3 (d) Audio 4 (e) Audio 5

Dari Gambar 9 dapat dilihat bahwa citra hasil ekstraksi setelah serangan AWGN memiliki dampak yang cukup signifikan. Tetapi untuk Audio 1 dan Audio 5 citra hasil ekstraksi masih dapat terlihat dengan jelas. Oleh karena itu dapat disimpulkan bahwa teknik *watermarking* yang dilakukan memiliki ketahanan yang baik untuk semua jenis audio terhadap serangan AWGN dengan PSNR di atas 40 dB.

3.2.4 Dengan Serangan *Resampling*

Pengujian ini dilakukan dengan mengubah frekuensi *sampling* data audio *host* menjadi frekuensi yang lebih rendah, kemudian dikembalikan ke nilai frekuensi *sampling* asalnya. Hasil pengujian dengan *resampling* dapat dilihat pada Tabel 7.

Tabel 7. BER Setelah Serangan *Resampling*

Frekuensi *Sampling*	BER (%)				
	Audio 1	Audio 2	Audio 3	Audio 4	Audio 5
11025 Hz	1.85	0.78	3.50	0.96	6.17
22050 Hz	0.018	0.11	0.58	0.46	2.10
33075 Hz	0.012	0.12	0.44	0.46	0.34

Hasil di atas menunjukkan nilai BER yang cukup rendah. Jika frekuensi *sampling* yang diujikan semakin mendekati frekuensi *sampling* aslinya, maka akan semakin kecil *error* yang dihasilkan. Hal ini menunjukkan bahwa teknik yang dilakukan memiliki ketahanan yang baik terhadap serangan *resampling*. Citra hasil ekstraksi juga tidak menejukkan banyak perbedaan dengan citra aslinya dan masih dapat dilihat dengan jelas. Citra hasil ekstraksi setelah serangan *resampling* dengan BER tertinggi dapat dilihat pada Gambar 10.

Gambar 8. Citra Hasil Ekstraksi Setelah Serangan *Resampling* 11025 Hz Pada (a) Audio 1 (b) Audio 2 (c) Audio 3 (d) Audio 4 (e) Audio 5

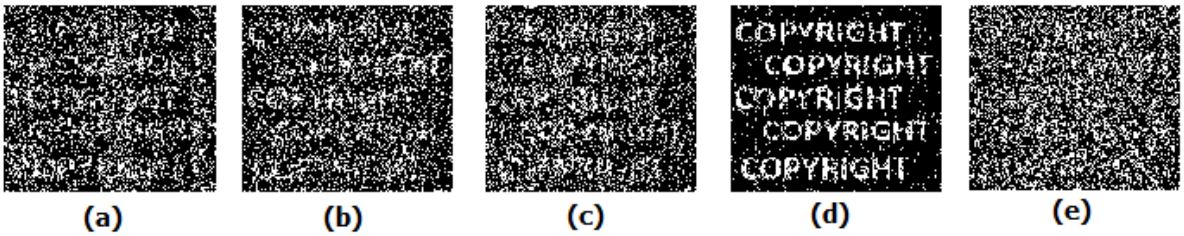
3. 2. 5 Dengan Serangan Kompresi

Proses kompresi banyak dilakukan pada data digital untuk mendapatkan data dengan ukuran yang lebih kecil. Maka dari itu, perlu dilakukan pengujian ketahanan *watermarking* terhadap kompresi. Kompresi dilakukan dengan mengubah audio asli dalam format wav dengan bit rate 1411 kbit/s ke dalam format mp4 dengan *bit rate* yang berbeda-beda. Berikut adalah hasil uji ketahanan watermarking terhadap kompresi:

Tabel 8. BER Setelah Serangan Kompresi

Bit Rate	BER(%)				
	Audio 1	Audio 2	Audio 3	Audio 4	Audio 5
96 kbit/s	27.09	25.74	27.19	7.76	33.05
128 kbit/s	27.09	25.74	27.19	7.76	33.05
160 kbit/s	27.09	25.74	27.19	7.76	33.05
192 kbit/s	27.09	25.74	27.19	7.76	33.05

Hasil di atas menunjukkan nilai BER yang sangat tinggi untuk pada saat *watermarked audio* dikompresi. Perbedaan *bit rate* pada proses kompresi tidak mempengaruhi nilai BER yang dihasilkan. Citra hasil ekstraksi setelah serangan kompresi dapat dilihat pada Gambar 11.



Gambar 9. Citra Hasil Ekstraksi Setelah Serangan Kompresi Pada (a) Audio 1 (b) Audio 2 (c) Audio 3 (d) Audio 4 (e) Audio 5

Dari Gambar 9 dapat dilihat bahwa audio 4 memiliki citra hasil ekstraksi yang cukup jelas, sedangkan citra hasil ekstraksi pada data audio lainnya memiliki hasil yang tidak dapat dilihat dengan jelas. Maka, dapat disimpulkan bahwa teknik *watermarking* yang dilakukan hanya memiliki ketahanan yang baik terhadap kompresi pada jenis audio tertentu saja.

4. KESIMPULAN

Penelitian ini dilakukan dengan dua buah data digital, yaitu citra hitam putih sebagai *watermark* dan audio sebagai *host*. Kedua data tersebut kemudian akan melewati proses penyisipan dan proses ekstraksi *watermark*. Dari hasil implementasi skema *watermarking* yang dilakukan dapat diambil beberapa kesimpulan, yaitu:

1. Intensitas sisipan *watermark* mempengaruhi kualitas dari *watermarked audio* tetapi tidak memiliki pengaruh yang signifikan pada ketahanan *watermarked audio*. Hal ini ditunjukkan pada nilai SNR yang semakin rendah jika nilai intensitas sisipan semakin besar, sedangkan nilai BER yang dihasilkan cenderung konstan dengan besar intensitas sisipan dari 0,05 sampai 0,4.
2. Skema *watermarking* yang dilakukan bersifat *imperceptible*. Hal ini dapat dilihat dari nilai SNR di atas 20 dB dan MOS di atas 4 dengan BER di bawah 1%.
3. Teknik *watermarking* ini memiliki ketahanan yang baik terhadap serangan LPF, *resampling*, dan penambahan AWGN dengan PSNR di atas 40 dB.
4. Dengan memberikan serangan kompresi, teknik *watermarking* ini hanya memberikan ketahanan yang cukup baik untuk tipe audio suara manusia. Untuk *genre* audio lain, BER yang dihasilkan sangat tinggi dan citra hasil ekstraksi tidak terlihat dengan jelas

DAFTAR RUJUKAN

Fallahpour, M., & Megias, D. (2012). High Capacity Robust Audio Watermarking Scheme Based on FFT and Linear Regression. *International Journal of Innovative Computing, Information and Control (IJICIC)*, 2477-2489.

Zeng, G., & Qiu, Z. (2008). Audio Watermarking in DCT Embedding Strategy and Algorithm. *International Conference on Signal Processing (ICSP)* (pp. 2193-2196).

Pooyan, M., & Delforouzi, A. (2007). Adaptive and Robust Audio watermarking in Wavelet Domain. *Intelligent Information Hiding and Multimedia Signal Processing* (pp. 287-290).

Dhar, P., & Echizen, I. (2011). Robust FFT Based Watermarking Scheme for Copyright Protection of Digital. *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* (pp. 181-184).

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2008). *Digital Watermarking and Steganography*. San Francisco: Morgan Kauffman.

Rockmore, D. (2000). The FFT - an algorithm the whole family can use. *Computing in Science & Engineering* (pp. 60-64).