APLIKASI *WATERMARKING* DENGAN ALGORITMA AES UNTUK PEMBERIAN DATA HAK CIPTA PADA *FILE AUDIO*

Yusuf Durrachman, Arini, Muhamad Soleh
[1, 2, 3] Program Studi Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri
Syarif Hidayatullah Jakarta
E-mail : ydfm@rocketmail.com, arinizoel@yahoo.com, froozs_eighteen@yahoo.com, ,

Abstract

Watermarking audio files has recently become the attention focus. This is primarily due to faster data transmission rates on the Internet, which has allowed the often illegal proliferation of digital audio files. Watermarking may give the ability to enforce copyright protection of digital audio files products. The difficulties in watermarking audio lie in both the desire to preserve file quality and the need for the watermark to remain intact after a number of possibly damaging file operations. This topic discusses about watermarking on audio file with AES (Advanced Encryption Standard) – Rinjdael algorithms with embedding procedure and extraction to purpose protection Watermarking method to used embedding process and extraction is low bit coding method. None of the transformations to and from frequency domain are performed either in embedding or extraction part of the proposed scheme. Testing process done using 5 ways such as suitability of process and data, audio quality, audio size and the last is data robustness, those result showed that embedded watermark introduces uncertainly and the embedded watermark into audio signal very is difficult to be detected by human auditory system.

***Keywords** : Watermarking, AES (Advanced Encryption Standard), low bit coding, audio file, copyright*

I. Pendahuluan

Perkembangan teknologi komputer saat ini telah membawa perubahan bagi kita untuk melakukan akses serta mendistribusikan berbagai informasi dalam bentuk format digital. Sehingga saat ini sering disebut sebagai era digital, atau dunia digital. Dengan perkembangan komputer digital dan perangkat-perangkat lainnya yang serba digital dalam hal ini audio digital, telah membuat data digital semakin banyak digunakan dan mudah diduplikasi. Sehingga seringkali menimbulkan konflik. Konflik yang sering timbul adalah adanya sengketa antara beberapa pihak yang mengklaim bahwa pihaknya adalah pemilik sah dari sebuah audio digital. Konflik tersebut yang kemudian menyebabkan timbulnya kebutuhan untuk melindungi hak kepemilikan (hak cipta) pada file audio dengan memberikan data hak cipta pada audio digital untuk keaslian (otentikasi) pemilik.

Perlindungan hak cipta dengan pengontentifikasian dari isi data audio dapat digunakan untuk membuktikan keaslian dari suatu file audio yang disimpan atau beredar masih asli atau sudah mengalami perubahan. Jika isi data audio yang diekstraksi tidak sama dengan isi data audio asli, maka dapat disimpulkan file audio sudah tidak otentik lagi. Keontentikan kepemilikan juga dapat ditunjukan karena hanya pemilik yang mengetahui kunci untuk mengestrak atau membuka informasi yang disisipkan.

Untuk mengatasi permasalahan diatas dapat menggunakan teknik audio *watermarking* yang digabungkan dengan teknik kriptografi yaitu algoritna AES. Penyisipan informasi *watermark* dengan algoritma AES ke dalam audio dilakukan sedemikian sehingga tidak merusak kualitas audio yang telah disisipi informasi hak cipta. Informasi hak cipta ini kemudian harus dapat diekstrak kembali untuk pembuktian keaslian atas produk audio digital tersebut. Penggunaan *watermarking* dan algoritma AES secara bersamaan dimaksudkan untuk memberikan keamanan berlapis dalam pengamanan audio.

II. Dasar Teori

5.1. Watermarking

Watermarking bisa diartikan sebagai suatu teknik penyembunyian data atau informasi "rahasia" ke dalam suatu data lainnya dengan cara "menumpangi" (kadang disebut *host* data), tanpa orang lain menyadari adanya data tambahan pada data *host*-nya [1].
Disamping itu, data yang ter-*watermark* harus tahan (*robust*) terhadap serangan-serangan, baik secara sengaja maupun tidak sengaja untuk menghilangkan data *watermark* didalamanya. *Watermarking* ini

memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga [6].

Watermarking merupakan suatu cara untuk penyembunyian atau penanaman data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau pendengaran), dan mampu menghadapi proses-proses pengolahan sinyal digital sampai pada tahap tertentu. Jadi *watermarking* dapat juga diartikan sebagai suatu teknik penyisipan atau penyembunyian data atau informasi "umum maupun rahasia" ke dalam data digital lainnya (*host* data) tanpa diketahui adanya data tambahan pada *host* datanya oleh indera manusia seperti mata dan telinga.

Ada beberapa karakteristik yang diinginkan dari pengguna *watermark* pada suatu dokumen, diantaranya tidak dapat terdeteksi (*imperceptible*), *robustness*, dan *security* [1].

a. ***Imperceptible*** : Memberikan karakteristik *watermark* agar sebisa mungkin harus tidak dapat terlihat atau berbeda dengan dokumen aslinya. Hal ini dimaksudkan untuk tidak merubah status dokumen yang bernilai tinggi secara hukum maupun komersial.
b. ***Robustness*** : Karakteristik ini tergantung aplikasi dari watermark itu sendiri. Apabila digunakan sebagai identifikasi kepemilikan/*copyright*, watermark harus memilki ketahanan terhadap berbagai macam modifikasi yang mungkin bisa dilakukan untuk merubah/menghilangkan *copyright*. Jika digunakan untuk mengautentifikasi *content*, watermark sebisa mungkin bersifat *fragile*, sehingga apabila isinya telah mengalami perubahan, maka watermark juga akan mangalamu perubahan/rusak, sehingga dapat terdeteksi adanya usaha modifikasi terhadap isi.
c. ***Security*** : Teknik *watermark* harus dapat mencegah usaha-usaha untuk mendeteksi dan memodifikasi informasi *watermark* yang disisipkan ke dalam dokumen. Kunci *watermark* menjamin hanya orang yang berhak saja yang dapat melakukan hal tersebut. Namun aspek ini tidak dapat mencegah siapapun untuk membaca dokumen yang bersangkutan.

5.2. Metode *Low-bit-coding*

Metode *Low-bit-coding* adalah cara yang paling sederhana untuk menyimpan data kedalam data yang lain. Dengan mengganti bit yang paling tidak penting atau *least significant bit (LSB)* pada setiap titik *sampling* dengan *string* berkode biner (*coded binary string*), kita dapat mengkode sejumlah besar data kedalam suara digital. Secara teori, kapasitas saluran adalah 1 kb per detik (1 kbps) per 1 kHz. Kelamahan metode ini adalah lemahnya kekebalan terhadap manipulasi. *Least Significant Bit* (LSB) termasuk ke dalam teknik penyisipan data ranah spasial (waktu), yaitu dengan memodifikasi langsung nilai *byte* dari *covertext* (nilai *byte* dapat mempresentasikan intensitas atau warna *pixel* atau amplitudo).

Penyembunyian data dilakukan dengan mengganti bit-bit data dalam segmen *covertext* dengan bit-bit dari data yang akan disembunyikan. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti (*Most Significant Bit* atau *MSB*) dan bit yang kurang berarti (*Least Significant Bit* atau *LSB*), contoh: Bit yang bisa diganti adalah bit *LSB*, karena perubahannya hanya akan mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut menunjukan warna merah, maka perubahan *byte* tersebut tidak memberi perubahan yang berarti pada warna merah tersebut, karena mata manusia tidak dapat menangkap perubahannya yang sedikit.

5.3. *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) dipublikasikan oleh NIST (*National Institute of Standards and Technology*) pada tahun 2001. AES merupakan simetri *block cipher* untuk menggantikan DES (*Data Encryption Standard*) [1].

DES adalah sebuah algoritma kriptografi simetri dengan panjang kunci 56 bit dan blok data 64 bit [3].

Pada tahun 1990 panjang kunci DES dianggap terlalu pendek dan pada tahun 1998 algoritma DES sudah berhasil dipecahkan dalam 96 hari hingga akhirnya dibuatlah mesin khusus untuk memecahkan algoritma DES [1].

Dengan alasan tersebut maka, NIST mengadakan kompetisi untuk standar kriptografi yang terbaru, yang dinamakan AES (*Advanced Encryption Standard*). Dari hasil seleksi tahap pertama NIST memilih 15 algoritma, dan pada tahap kedua memilih 5 algoritma. NIST akhirnya mengumumkan standar baru pada November 2001. NIST memilih algoritma Rijndael yang dibuat oleh Dr. Vincent Rijmen dan Dr. Joan Daemen kriptografer dari Belgia sebagai algoritma AES [5].

Rinjdael mendukung panjang kunci dari 128 sampai 256 bit dengan step 32 bit. Karena AES menetapkan panjang kunci adalah 128, 192, dan 256, maka dikenal sebagai *AES*-128, *AES*-192, dan *AES*-256, yang perbedaannya akan ditunjukan oleh table 2.1.

Tabel 1. Tiga buah versi *AES* [3].

	Panjang Kunci (Nk *words*)	Ukuran Blok (*Nb words*)	Jumlah Putaran (*Nr*)
AES-128	4	4	10
AES-196	6	4	12
AES-256	8	4	14

III. Metodologi Penelitian

Dua metode penelitian yang digunakan adalah metode pengumpulan data dan metode pengembangan sistem.

3.1. Metode Pengumpulan Data

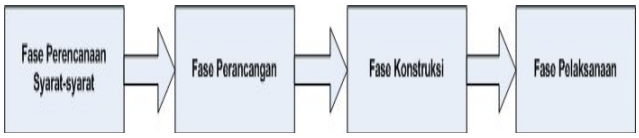
Pada metode melakukan :

1. **Studi Pustaka.**
   Melakukan pengumpulan data dan informasi dengan mencari dan memperoleh data-data yang diperlukan terkait dengan apliaksi yang akan dibangun dari berbagai buku, *e-book*, dan sumber lainya yang berkaitan

2. **Studi Literatur**
   Mencari dan menggunakan instrumen atau penelitian sejenis yang sudah dibuat/ada sebelumnya.

3.2. Metode Pengembangan Sistem

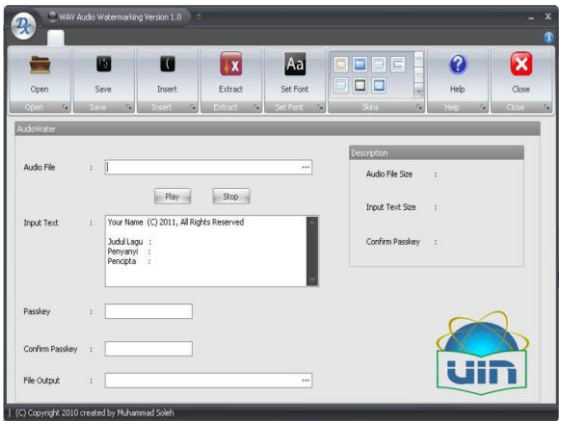
Metode pengembangan sistem yang digunakan adalah model pendekatan Pengembangan Aplikasi Cepat (PAC) atau *Rapid Application Development* (RAD) seperti dapat dilihat pada gambar dibawah ini 1 dibawah ini.



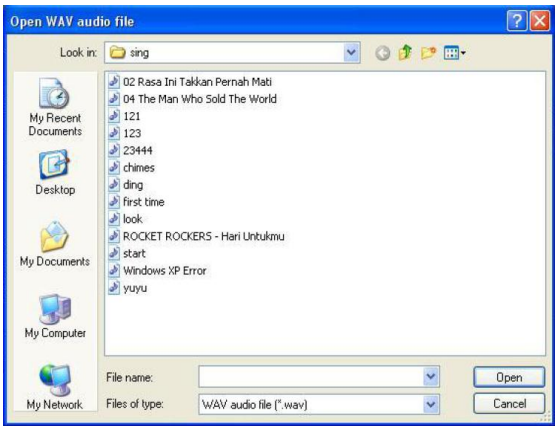
Gambar 1. Fase-fase RAD James Martin [4].

IV. Implementasi

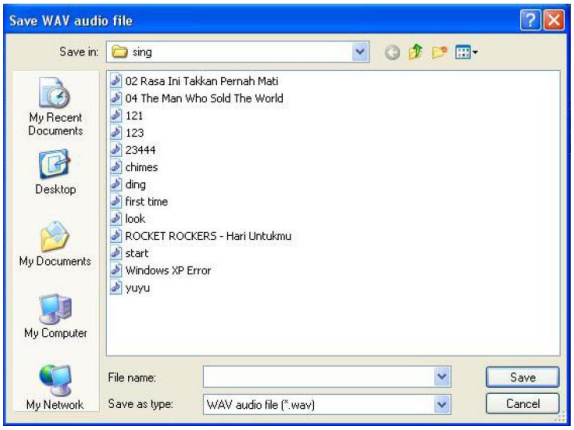
Lingkungan yang digunakan untuk membangun aplikasi watermarking *file audio* dengan algoritma AES (kami beri nama *AudioWater*) adalah lingkungan berbasis Windows. Bahasa pemrograman yang digunakan adalah bahasa pemograman C# dan Microsoft Framework .NET 3.5.



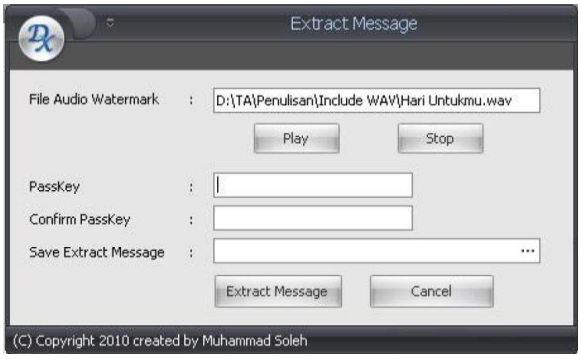
Gambar 2. Tampilan *Form* Utama



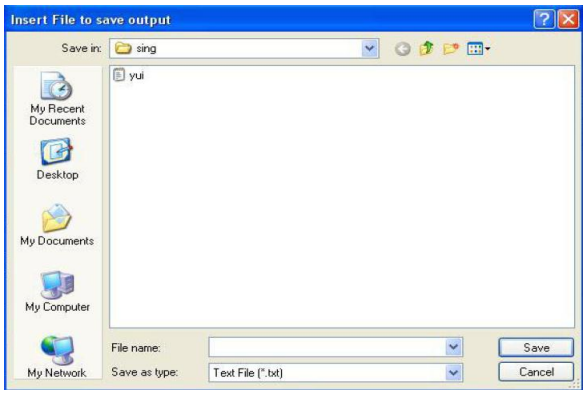
Gambar 3. Tampilan *Open File Audio*



Gambar 4. Tampilan *Save Output File Audio*



Gambar 5. Tampilan *Form Extract*



Gambar 6. Tampilan *File Save Output Text*

Gambar 7. Tampilan *Form* bantuan

V. Pengujian

Pengujian dilakukan berdasarkan spesifikasi sistem dan pengujian ketahanan data. Pengujian ini diuraikan menjadi lima faktor pengujian yaitu sebagai berikut :

1. Kesesuaian proses, yaitu perangkat lunak dapat melakukan proses penyisipan dan ekstraksi.
2. Kesesuaian data, yaitu pengujian kesesuaian antara data yang berhasil diekstrak dengan data yang disisipkan.
3. Kualitas Suara, yaitu pengujian sama tidaknya suara WAV berlabel dengan suara WAV asli.
4. Ukuran *file* terhadap *file carrier*
5. Ketahanan data terhadap pemrosesan suara WAV berlabel.

Tabel 2. Spesifikasi *File Carrier* yang akan diuji

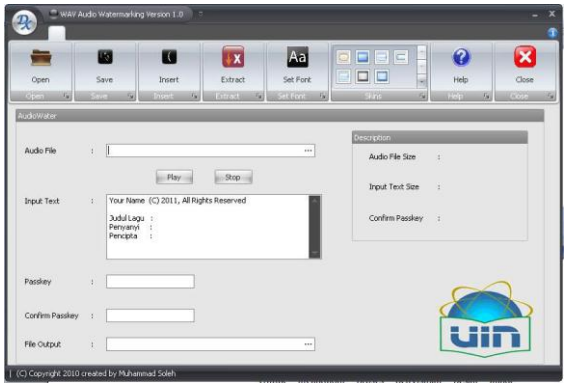
No	Nama File Audio WAV	Ukuran Data (byte)	Audio Format
1	Rocket Rockers – Hari Untukmu.wav	1321808	PCM
2	RadioHead – Creep.wav	20805150	PCM
3	Luna4Melo – First Time	27265582	PCM
4	Andra And The Backbone – Surrender	46886446	PCM

Untuk melakukan kelima pengujian diatas, digunakan beberapa buah berkas suara WAV dengan spesifikasi yang terdapat pada Tabel 2 diatas.

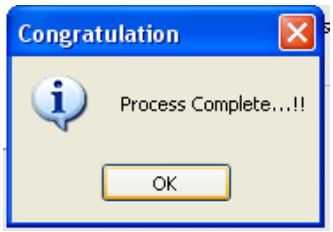
5.1. Pengujian Kesesuaian Proses

Pengujian terhadap proses dilakukan untuk mengetahui apakah sistem dapat melakukan proses penyisipan dan ekstraksi. Kriteria pengujian adalah sistem dapat melakukan proses penyisipan dan ekstraksi.

a. Pengujian Proses Penyisipan, dengan memasukkan *file audio input*, *password* dan *output file* pada *form* utama dengan benar maka akan terbukti berhasil jika ditandai dengan munculnya *message box Process Complete*.



Gambar 8. Tampilan *Form* Penyisipan



Gambar 9. Tampilan Message Box Penyisipan Berhasil

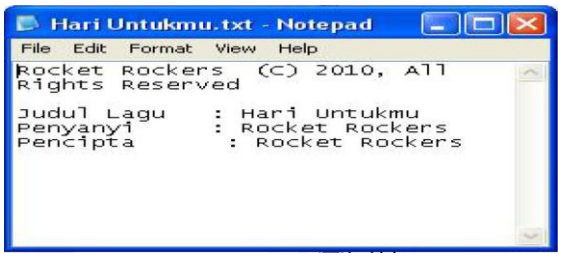
b. Proses Ekstraksi, dengan menekan tombol *extract* dan mengisikan *password*, dan lokasi *file* akhir, proses ekstraksi terbukti berhasil dengan ditandai *message box extract finished*.

Gambar 10. Tampilan *Form Extract*

Gambar 11. Tampilan *Message Box Extract Finished*

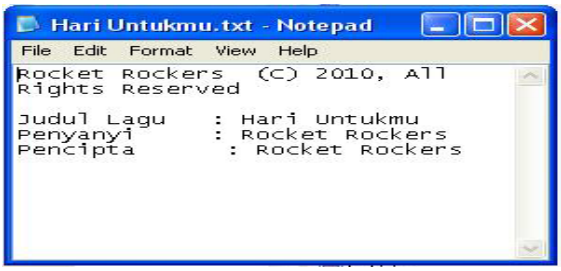
5.2. **Pengujian Kesesuaian Data**

Pengujian terhadap kesesuaian data dilakukan untuk mengetahui apakah data yang berhasil diekstrak dari suara WAV berlabel bersesuaian dengan data yang disisipkan. Kriteria pengujian adalah data yang berhasil diekstrak dari suara WAV berlabel bersesuaian dengan data yang disisipkan.



Gambar 12. Pesan Asli pada *File Audio* Hari Untukmu

Gambar 13. Pesan Asli yang telah di enkripsi pada *File Audio* Hari Untukmu



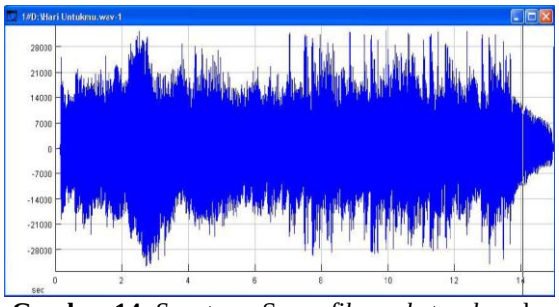
Gambar 14. File pesan yang diambil dari *File Audio* Hari Untukmu

Tabel 3. Pengujian Proses dan Kesesuaian Data

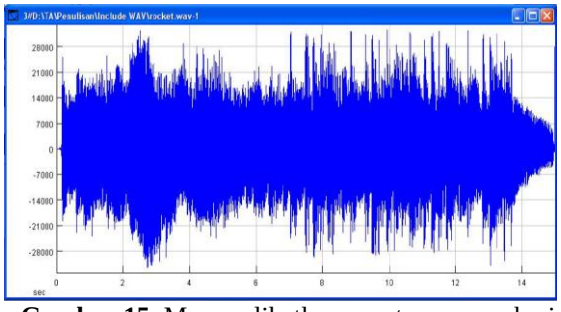
Nama File Audio WAV	Ukuran Data (byte)	Secret File	Size (byte)	Penyisipan Pesan	Ekstraksi Pesan	Kesesuaian Data
Rocket Rockers – Hari Untukmu.wav	1321808	Hari Untuk mu.txt	529	Berhasil	Berhasil	Sesuai
RadioHead – Creep.wav	20805150	Creep.txt	1747	Berhasil	Berhasil	Sesuai
Luna4Melo – First Time	27265582	First Time.txt	2068	Berhasil	Berhasil	Sesuai
Andra And The Backbone – Surrender	46886446	Surrender.txt	3490	Berhasil	Berhasil	Sesuai

5.3. **Pengujian Kualitas Suara**

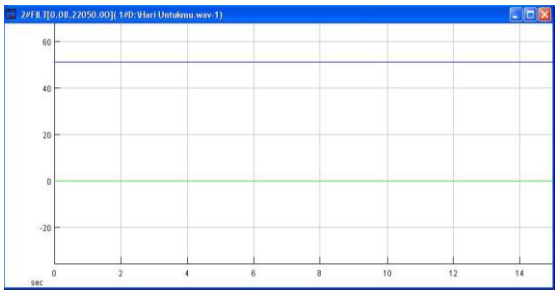
Pengujian kualitas suara WAV berlabel dilakukan secara subjektif dan objektif. Pengujian dengan cara subjektif, yaitu dengan mendengarkan langsung suara WAV berlabel dan suara WAV asli kemudian dibandingkan. Pengujian dengan cara objektif dilakukan dengan membandingkan grafik sinyal suara WAV asli dengan grafik sinyal suara WAV berlabel dan dengan melihat korelasi antara suara WAV asli dengan suara WAV berlabel. Pengujian dengan korelasi untuk melihat derajat atau hubungan antara suara WAV sebelum disisipi data teks dengan suara WAV setelah disisipi data teks. Kriteria pengujian adalah berhasil jika data yang telah disisipkan kedalam suara WAV tidak dapat dideteksi oleh sistem pendengaran manusia.



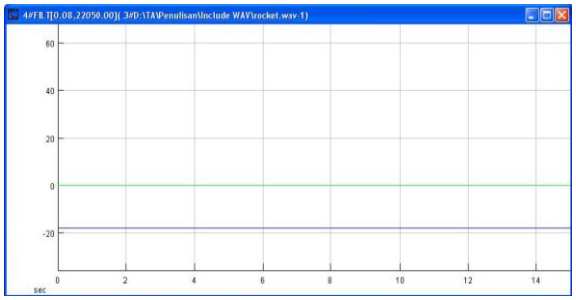
Gambar 14. *Spectrum* Suara *file rocketrockers* hari untukmu.wav asli



Gambar 15. Memperlihatkan *spectrum* suara hari untukmu setelah disisipi pesan ”*rocket_rockers*.txt”



Gambar 16. *Spectrum* suara hari untukmu.wav dengan *filter bandstop*



Gambar 17. *Spectrum* suara *file* hari untukmu.wav yang sudah disisipi pesan dengan *filter bandstop*

5.4. **Pengujian Ukuran *File***

Pengujian ini bertujuan untuk mengetahui batasan ukuran pesan yang dapat disisipkan ke dalam file *carrier*.

Tabel 4. Tabel Uji Ukuran *File* Pesan terhadap *File Carrier.*

Nama File Audio WAV	Ukuran Data (byte)	Secret File	Size (byte)
Rocket Rockers – Hari Untukmu.wav	1321808	Hari Untuk mu.txt	529
Rocket Rockers – Hari Untukmu.wav	1321808	Hari Untuk mu2.txt	1616
RadioHead – Creep.wav	20805150	Creep.txt	1747
RadioHead – Creep.wav	20805150	Creep2.txt	21674
Luna4Melo – First Time	27265582	First Time.txt	2068
Luna4Melo – First Time	27265582	First Time2.txt	28796
Andra And The Backbone – Surrender	46886446	Surrender.txt	3490
Andra And The Backbone – Surrender	46886446	Surrender2.txt	39305

Tabel 5. Tabel Hasil Uji Ukuran *File* Pesan terhadap *File Carrier*

Nama File Audio WAV	Ukuran Data (byte)	Secret File	Size (byte)	Output WAV	Ukuran data	Size (byte)	Size (byte)
Rocket Rockers – Hari Untukmu.wav	1321808	Hari Untuk mu.txt	529	R R.wav	1321808	Hari Untuk mu.txt	529
RadioHead – Creep.wav	20805150	Creep.txt	1747	RadioHead.wav	20805150	Creep.txt	1747
Andra And The Backbone – Surrender	46886446	First Time.txt	2068	Andra And The Backbone.wav	46886446	First Time.txt	2068
Luna4Melo – First Time	27265582	Surrender.txt	3490	Luna4Melo.wav	27265582	Surrender.txt	3490

Tabel 6. Tabel Hasil Uji Spesifikasi Sistem

Nama File Audio WAV	Ukuran Data (byte)	**Secret File**	**Size (byte)**	**Penyisipan Pesan**	**Dibutuhkan (byte)**	**Tersedia (byte)**
Rocket Rockers – Hari Untukmu.wav	1321808	Hari Untuk mu.txt	529	Berhasil	520954	660858
Rocket Rockers – Hari Untukmu.wav_1	1321808	Hari Untuk mu2.txt	1616	Tidak	1407850	660858
RadioHead – Creep.wav	20805150	Creep.txt	1747	Berhasil	78459965	10402529
RadioHead – Creep.wav_1	20805150	Creep2.txt	21674	Tidak	16960476	10402529
Luna4Melo – First Time	27265582	First Time.txt	2068	Berhasil	10676543	13632745
Luna4Melo – First Time_1	27265582	First Time2.txt	28796	Tidak	21713176	13632745
Andra And The Backbone – Surrender	46886446	Surrender.txt	3490	Berhasl	22465656	23443177
Andra And The Backbone – Surrender_1	46886446	Surrender2.txt	39305	Tidak	38132052	23443177

5.5. **Pengujian Ketahanan Data**

Pengujian ketahanan data dilakukan terhadap suara WAV berlabel. Pengujian ketahanan data yang akan dilakukan dengan pengujian kompresi, dengan menggunakan aplikasi xilisoft. Pengujian dengan kompresi dilakukan untuk melihat apakah data yang terdapat di dalam suara WAV berlabel masih dapat diekstrak setelah mengalami kompresi. Pengujian kompresi dilakukan dengan mengubah suara WAV berlabel menjadi suara dalam format (MP3, AAC, dan midi) dengan ekstensi berkas (.mp3, .aac, dan .midi), kemudian suara dalam format (MP3, AAC, dan midi) diubah kembali menjadi suara dalam format WAV (dengan ekstensi berkas .wav). Kriteria pengujian adalah berhasil jika data dapat diekstrak setelah suara WAV berlabel dikompres.

Tabel 7. Tabel Uji Ketahanan Data

Nama File Audio WAV	Ukuran Data (byte)
R R.wav	1321808
R R_1.wav	1321808
RadioHead.wav	20805150
RadioHead_1.wav	20805150
Luna4Melo.wav	27265582
Luna4Melo_1.wav	27265582
Andra And The Backbone.wav	46886446
Andra And The Backbone_1.wav	46886446

Tabel 8. Tabel Hasil Uji Ketahanan Data WAV-MP3

Nama File Audio WAV	Ukuran Data (byte)	**Ekstraksi Pesan**	**Secret File**
RR – Hari Untukmu.wav	1321808	Berhasil	Rocker.txt
RR _1.wav	1321808	Tidak	kosong
RadioHead.wav	20805150	Berhasil	Hidden.txt
RadioHead_1.wav	20805150	Tidak	Kosong
Luna4Melo.wav	27265582	Berhasil	Andra.txt
Luna4Melo_1.wav	27265582	Tidak	Kosong
Andra And The Backbone.wav	46886446	Berhasl	Luna.txt
Andra And The Backbone_1.wav	46886446	Tidak	Kosong

Tabel 9. Tabel Hasil Uji Ketahanan Data WAV-AAC

Nama File Audio WAV	Ukuran Data (byte)	**Ekstraksi Pesan**	**Secret File**
RR – Hari Untukmu.wav	1321808	Berhasil	Rocker.txt
RR _1.wav	1321808	Tidak	kosong
RadioHead.wav	20805150	Berhasil	Hidden.txt
RadioHead_1.wav	20805150	Tidak	Kosong
Luna4Melo.wav	27265582	Berhasil	Andra.txt
Luna4Melo_1.wav	27265582	Tidak	Kosong
Andra And The Backbone.wav	46886446	Berhasl	Luna.txt
Andra And The Backbone_1.wav	46886446	Tidak	Kosong

Tabel 10. Tabel Hasil Uji Ketahanan Data WAV-Midi

Nama File Audio WAV	Ukuran Data (byte)	**Ekstraksi Pesan**	**Secret File**
RR – Hari Untukmu.wav	1321808	Berhasil	Rocker.txt
RR _1.wav	1321808	Tidak	kosong
RadioHead.wav	20805150	Berhasil	Hidden.txt
RadioHead_1.wav	20805150	Tidak	kosong
Luna4Melo.wav	27265582	Berhasil	Andra.txt
Luna4Melo_1.wav	27265582	Tidak	kosong
Andra And The Backbone.wav	46886446	Berhasl	Luna.txt
Andra And The Backbone_1.wav	46886446	Tidak	kosong

VI. Kesimpulan dan Saran

6.1. Kesimpulan

Setelah melakukan pembahasan secara teoritis, implementasi, dan pengujian, serta analisis hasil pengujian, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Berdasarkan hasil uji spesifikasi sistem, aplikasi ini berhasil melakukan proses penyisipan file pesan ke dalam file *audio*.
2. Berdasarkan hasil uji spesifikasi sistem, aplikasi ini berhasil melakukan proses ekstraksi file pesan dari dalam file *audio*.
3. Berdasarkan hasil uji kualitas, penyisipan file pesan ke dalam file *audio* mempengaruhi kualitas suara yang dihasilkan, dengan adanya perubahan intensitas suara antara file asli dan file yang sudah disisipi pesan.
4. Berdasarkan uji ketahanan data menunjukan data teks tidak berhasil diekstrak, dimana artinya pesan dalam wav berlabel tidak dapat diekstrak setelah melalui konversi.
5. Metode *low bit coding* tidak menambah ukuran berkas suara WAV setelah disisipi data teks.
6. Berdasarkan hasil ukuran file diketahui bahwa file masukan dan file hasil keluaran memiliki jumlah bit yang sama persis, artinya penyisipan pesan tidak mempengaruhi besar ukuran pesan awal maupun akhir.
7. Banyaknya data teks yang dapat disisipkan kedalam suara WAV dengan metode *low bit coding* bergantung pada banyaknya data suara WAV dan jenis *channel* suara WAV.

6.2. **Saran**

Berdasarkan penelitian yang telah diperoleh, ada beberapa saran untuk pengembangan sistem lebih lanjut, sebagai berikut:

1. Penyisipan dapat dilakukan pada sampel suara dengan frekuensi tertentu, yaitu frekuensi yang tidak akan dibuang pada saat kompresi,

2. Aplikasi hanya menggunakan WAV sebagai media penampung, untuk pengembangan berikutnya dapat menggunakan file *MP3, MIDI* dan lain-lain sebagainya.
3. Aplikasi hanya dapat menyisipkan file txt, htm, cs, xml dan rtf ke media penampung, diharapkan dapat dikembangkan menggunakan berbagai macam file lainnya.

Referensi

[1] Ariyus, Doni. *Keamanan Multimedia*. Yogyakarta: Andi Offset, 2009.

[2] Ariyus, Doni. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu, 2006.

[3] Munir, Renaldi. *Kriptografi*. Bandung: Informatika, 2006.

[4] Kendall & kendall. *Analisis dan Perancangan Sistem*. Jakarta: Renhalindo, 2003.

[5] Stalling, William. *Cryptography and Network Security*, Principles and Practices, 3rded. New Jersey: Prentice Hall, 2003.

[6] Supangkat S. H., Kuspriyanto, Juanda, 2000, "*Watermarking sebagai Teknik Penyembunyian Label Hak Cipta PadaData Digital*", Departemen Teknik Elektro, Institut Teknologi Bandung. http://digitally1.paume.itb.ac.ids