

Implementasi Steganografi dengan Metode Ranked Positional Weight Untuk File Mp3

Desman Siregar

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia

Email: siregardesman94@gmail.com

Abstrak—Abstrak Melindungi informasi termasuk dokumen multimedia merupakan suatu kebutuhan utama dalam era keterbukaan informasi seperti saat ini. Salah satu cara untuk mengatasi situasi diatas adalah menggunakan teknik steganografi. Steganografi adalah ilmu dan seni menyisipkan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Untuk mengimplementasikan steganografi menggunakan metode Ranked Positional Weight yaitu dengan memodifikasi bit yang kurang signifikan atau bit terakhir dalam satu byte data dengan menggunakan File MP3 sebagai media penampung. Hasil penelitian menunjukkan bahwa aplikasi berhasil 100% melakukan penyisipan dan melakukan pemanggilan kembali pesan yang telah disisipkan. Hasil ekstraksi pesan memiliki tingkat kesesuaian karakter pesan 100% terhadap isi pesan asli. Ukuran Mp3 setelah dilakukan penyisipan pesan 100% sama dengan ukuran Mp3 asli. File Mp3 hasil steganografi mempunyai kualitas sangat baik diatas 50dB. Akan tetapi steganografi dengan metode RPW ini tidak tahan terhadap serangan kompresi yang akan menyebabkan isi pesan didalam file Mp3 hasil steganografi hilang.

Kata Kunci: Text, File Mp3, Steganografi, Ranked Positional Weight.

Abstract—Abstract Protecting information including multimedia documents is a major requirement in the era of information disclosure as it is currently. One way to overcome the above situation is to use steganography techniques. Steganography is the science and art of inserting secret messages in other messages so that the existence of the secret message cannot be known. To implement steganography using the Ranked Positional Weight method by modifying the least significant bit or the last bit in one byte of data by using MP3 files as a storage medium. The results showed that the application was 100% successful in inserting and recalling messages that had been inserted. The result of message extraction has a message character compatibility level of 100% to the original message content. The size of the Mp3 after inserting a message is 100% the same as the size of the original Mp3. Mp3 files from steganography have very good quality above 50dB. However, steganography with the RPW method is not resistant to compression attacks that will cause the contents of the message in the Mp3 file to be lost.

Keywords: Text, Mp3 Files, Steganography, Ranked Positional Weight.

1. PENDAHULUAN

Perkembangan teknologi audio digital adalah teknologi yang dapat digunakan untuk merekam, menyimpan, menghasilkan, memanipulasi, dan mereproduksi suara dengan menggunakan sinyal audio yang dikodekan dalam bentuk digital. seiring dengan perkembangan yang signifikan selama kurun waktu 1970an, audio digital dengan cepat menggantikan teknologi audio analog di banyak rumah produksi musik, perekayasa suara dan telekomunikasi di seluruh dunia. Sebuah mikrofon mengubah suara menjadi sinyal listrik analog, kemudian sebuah konverter analog-ke-digital mengubah sinyal analog menjadi sinyal digital, begitu juga dengan konverter digital-ke-analog melakukan proses sebaliknya, mengubah sinyal digital kembali menjadi sinyal analog, dimana sirkuit analog memperjelas sinyalnya dan mengirimnya ke pengeras suara. Sistem audio digital dapat mencakup kompresi, penyimpanan, pengolahan dan komponen komponen lain transmisi. Konversi ke format digital memungkinkan kenyamanan dalam hal manipulasi, penyimpanan, transmisi dan pengambilan sinyal audio [1].

Steganografi Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos*, yang artinya tersembunyi atau terselubung, dan *graphia* yang artinya menulis, sehingga arti steganografi adalah "menulis (tulisan) terselubung". Dengan steganografi, kita dapat menyisipkan pesan rahasia ke dalam media lain dan mengirimkannya tanpa ada yang menyadari keberadaan pesan tersebut. Steganografi adalah ilmu yang digunakan untuk menyisipkan data di dalam media lainnya. Steganografi membutuhkan dua media, yaitu penampung dan data yang akan disisipkan. Secara teori, semua berkas digital yang ada di dalam komputer dapat digunakan sebagai media penampung, misalnya citra berformat JPG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI [2].

MP3 Pertama kali ditemukan oleh peneliti IIS-FHG (Institut Integrierte Schaltungen Fraunhofer Gesellschaft), sebuah lembaga penelitian terapan di Munich, Jerman dalam penelitian sumber *coding audio perceptual*. Penelitian mengenai pemampatan berkas audio ini dipimpin langsung oleh Karl Heinz Brandenburg, dan menghasilkan sebuah algoritma MPEG-1 Layer 3 yang kemudian dikenal sebagai MP3 [3].

Masalah yang di hadapi Pengambilan file mp3 pada saat menggunakan memori sering mengalami pada mp3 yang di sebabkan ada suara suara yang tidak jelas, memori yang buruk atau pun posisi saat pemasangan mp3. Pada mp3 tersebut pada umumnya terdistribusi secara normal (*Gaussian*). Pengaruh pada mp3 sangat mempengaruhi kualitas mp3 sehingga pada mp3 harus dihilangkan agar kualitas jauh lebih baik dari sebelumnya dimana kualitas mp3 merupakan salah satu proses awal dalam pengolahan mp3 (*mp3 preprocessing*). Penyisipan diperlukan karena sering kali mp3 yang dijadikan objek penyisipan yang buruk misalnya mp3 mengalami mp3 macet, mp3 kurang baik dan sebagainya [4].

Solusi pengurangan file untuk mp3 adalah salah satu proses dalam penyisipan text pada file Mp3 yang termasuk langkah awal dalam Mp3. Penyisipan text pada file Mp3 adalah solusi suatu teknik yang memperhatikan bagaimana mengurangi perubahan bentuk dan penurunan kualitas Mp3 yang diawali selama pembentukan Mp3 tersebut.

2. METODOLOGI PENELITIAN

2.1 Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos*, yang artinya tersembunyi atau terselubung, dan *graphia* yang artinya menulis, sehingga arti steganografi adalah "menulis (tulisan) terselubung". Dengan steganografi, kita dapat menyisipkan pesan rahasia ke dalam media lain dan mengirimkannya tanpa ada yang menyadari keberadaan *text* tersebut. Steganografi adalah ilmu yang digunakan untuk menyisipkan data di dalam media lainnya. Steganografi membutuhkan dua media, yaitu penampung dan data yang akan disisipkan. Secara teori, semua berkas digital yang ada di dalam komputer dapat digunakan sebagai media penampung, misalnya citra berformat JPG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI. Semua dapat dijadikan tempat bersembunyi, asalkan berkas tersebut memiliki bit-bit yang tidak signifikan atau terdapat *redundant bits* yang dapat dimodifikasi. Setelah dimodifikasi, berkas media tersebut tidak akan terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya [7].

2.2 Mp3

Asal-usul MP3 dimulai dari penelitian IIS-FHG (Institut Integrierte Schaltungen Fraunhofer Gesellschaft), sebuah lembaga penelitian terapan di Munich, Jerman dalam penelitian sumber *coding audio perceptual*. Penelitian mengenai pemampatan berkas audio ini dipimpin langsung oleh Karl Heinz Brandenburg, dan menghasilkan sebuah algoritma MPEG-1 Layer 3 yang kemudian dikenal sebagai MP3. Penelitian tersebut menghasilkan suatu algoritma yang menjadi standar sebagai ISO-MPEG Audio Layer-3 (MP3), yang merupakan berkas dengan teknik *lossy compression* [15].

2.3 Metode Ranked Positional Weight (RPW)

Metode *Ranked Positional Weight* (RPW) adalah metode yang diusulkan oleh Helgeson dan Birnie sebagai pendekatan untuk memecahkan permasalahan pada keseimbangan lini dan menemukan solusi dengan cepat. Konsep dari metode ini adalah menentukan jumlah stasiun kerja minimal dan melakukan pembagian task ke dalam stasiun kerja dengan cara memberikan bobot posisi kepada setiap task sehingga semua task telah ditempatkan kepada sebuah stasiun kerja. Bobot setiap task, misal task ke-*i* dihitung sebagai waktu yang dibutuhkan untuk melakukan task ke-*i* ditambah dengan waktu untuk mengeksekusi semua task yang akan dijalankan setelah task ke-*i* tersebut.

$$F(x, y) = \frac{\sum_{(x,y) \in S_{xy}} g(x,y)^{q+1}}{\sum_{(x,y) \in S_{xy}} g(x,y)^q} \quad (1)$$

Keterangan :

$f(x,y)$: Hasil *Ranked Positional Weight*

Q : Nilai *Ranked Positional Weight window*

$g(x,y)$: sub-data S_{xy}

S_{xy} : *window* daerah yang diliputi oleh Text

3. HASIL DAN PEMBAHASAN

MP3 merupakan gabungan audio dengan steganografi yang bergerak yang membentuk sebuah *frame* yang dapat dimanfaatkan untuk kepentingan bersama maupun pribadi. *Forensika* atau derau pada MP3 sangat mempengaruhi kejelasan dari sebuah MP3 dimana hasil Mp3 tersebut kurang jelas jika dilihat oleh mata, maka dengan itu *Forensika* pada MP3 harus dihilangkan agar steganografi tersebut dapat melakukan proses penyisipan text pada file MP3 agar lebih jelas. Adapun MP3 yang memiliki *Forensika* yang akan dijadikan sampel untuk menganalisa MP3 yang memiliki gangguan

3.1 Penerapan Metode Ranked Positional Weight

Ranked Positional Weight adalah metode yang diusulkan oleh Helgeson dan Birnie sebagai pendekatan untuk memecahkan permasalahan pada keseimbangan lini dan menemukan solusi dengan cepat. Konsep dari metode ini adalah menentukan jumlah stasiun kerja minimal dan melakukan penyisipan *text* ke dalam stasiun kerja dengan cara memberikan bobot posisi kepada setiap *text* sehingga semua task telah ditempatkan kepada sebuah stasiun kerja.

Pesan yang akan disisipkan pada mp3 adalah hasil dari “ Budi, Argana Trio.Mp, dan Wali ” akan di konversikan ke bilangan Biner dengan menggunakan *metode Randke positional weight* adalah sebagai berikut. Berdasarkan proses penyisipan pada tahap penyisipan, maka text yang di sisipkan akan diekstrak atau diungkap dari nilai biner derajat keabuan steganorafi tersebut. Proses pengungkapan text tersebut adalah sebagai berikut.

Misal Text : DESMAN

D : terletak di kolom 4 dan baris 4

Maka bilangan nya adalah $44_{(16)}$

$4=0100$

$4=0100$

Maka bilangan biner nya adalah $1000100_{(2)}$

E : terletak di kolom 4 dan baris 5

Maka bilangan nya adalah $45_{(16)}$

$4=0100$

$5=0101$

Maka bilangan biner nya adalah $1000101_{(2)}$

S : terletak di kolom 5 dan baris 3

Maka bilangan nya adalah $53_{(16)}$

$5=0101$

$3=0011$

Maka bilangan biner nya adalah $1010011_{(2)}$

M : terletak di kolom 4 dan baris D

Maka bilangan nya adalah $4D_{(16)}$

$4=0100$

$D=1101$

Maka bilangan biner nya adalah $1001101_{(2)}$

A : terletak di kolom 4 dan baris 1

Maka bilangan nya adalah $41_{(16)}$

$4=0100$

$D=0001$

Maka bilangan biner nya adalah $1000001_{(2)}$

N : terletak di kolom 4 dan baris E

Maka bilangan nya adalah $4E_{(16)}$

$4=0100$

$E=1110$

Maka bilangan biner nya adalah $1001110_{(2)}$

File : Argana.Mp3

Nilai biner derajat keabuan steganorafi tersebut. Proses pengungkapan text tersebut adalah sebagai berikut

:

A : terletak di kolom 4 dan baris 1

Maka bilangan nya adalah $41_{(16)}$

$4=0100$

$1=0001$

Maka bilangan binernya adalah $1000001_{(2)}$

r : terletak di kolom 7 dan baris 2

Maka bilangan nya adalah $72_{(16)}$

$7=0111$

$2=0010$

Maka bilangan binernya adalah $1110010_{(2)}$

g : terletak di kolom 6 dan baris 7

Maka bilangan nya adalah $67_{(16)}$

$6=0110$

$7=0111$

Maka bilangan binernya adalah $1100111_{(2)}$

a : terletak di kolom 6 dan baris 1

Maka bilangan nya adalah $61_{(16)}$

$6=0110$

$1=0001$

Maka bilangan binernya adalah $1100001_{(2)}$

n : terletak di kolom 6 dan baris E

Maka bilangan nya adalah $6E_{(16)}$

$6=0110$

$E=1110$

Maka bilangan binernya adalah $1101110_{(2)}$

a : terletak di kolom 6 dan baris 1

Maka bilangan nya adalah $61_{(16)}$

$6=0110$

$1=0001$

Maka bilangan binernya adalah $1100001_{(2)}$

T : terletak di kolom 5 dan baris 4

Maka bilangan nya adalah $54_{(16)}$

$5=0101$

$4=0100$

Maka bilangan binernya adalah $1010100_{(2)}$

r : terletak di kolom 7 dan baris 2

Maka bilangan nya adalah $72_{(16)}$

$7=0111$

$2=0010$

Maka bilangan binernya adalah $1110010_{(2)}$

i : terletak di kolom 6 dan baris 9

Maka bilangan nya adalah $69_{(16)}$

$6=0110$

$9=1001$

Maka bilangan binernya adalah $1101001_{(2)}$

o : terletak di kolom 6 dan baris F

Maka bilangan nya adalah $6F_{(16)}$

$6=0110$

$F=1111$

Maka bilangan binernya adalah 1101111

Misal Text : Wali

W : terletak di kolom 5 dan baris 7

Maka bilangan nya adalah $57_{(16)}$

$5=0101$

$7=0111$

Maka bilangan binernya adalah $1010111_{(2)}$

a : terletak di kolom 6 dan baris 1

Maka bilangan nya adalah $6F_{(16)}$

$6=0110$

$1=0001$

Maka bilangan binernya adalah $1100001_{(2)}$

l : terletak di kolom 4 dan baris C

Maka bilangan nya adalah $4C_{(16)}$

$6=0110$

$C=1100$

Maka bilangan binernya adalah $1101100_{(2)}$

i : terletak di kolom 6 dan baris C

Maka bilangan nya adalah $69_{(16)}$

$6=0110$

$9=1001$

Maka bilangan binernya adalah $1101001_{(2)}$

Berikut ini adalah salah satu bentuk gambar proses yang menunjukkan hasil penyisipan ,proses penyisipan pesan dilakukan dengan *button* proses. Setelah file berhasil disisipkan pesan, terdapat *button save* yang digunakan untuk menyimpan file audio setelah disisipi pesan. Pada halaman ini juga terdapat informasi tentang file audio, seperti nama file, ukuran file audio sebelum disisipi pesan, ukuran audio setelah disisipi text, nilai dan kualitas .

Setelah proses penyisipan,hal lain yang dapat di perbandingkan adalah ukuran berkas file mp3 sebelum dan setelah penyisip.

Proses untuk mengekstraksi pesan pada file Mp3 membutuhkan masukan berupa text yang telah disisipkan text dan yang akan digunakan untuk proses ekstraksi. Skema penyisipan pesan dapat dilihat pada Proses menggunakan Metode *Randked Positional Weight* ini terdiri dari dua proses, yaitu pengambilan text dan penyisipan. Proses Ekstraksi Langkah-langkah proses ekstraksi bit-bit pesan dari berkas audio steganografi adalah sebagai berikut ini :

1. Berkas audio stego dibaca dan byte-byte hasil pembacaan disimpan ke dalam variable "fid1".
2. 40 byte pertama dari "fid1" yang berisi informasi mengenai berkas audio dipindahkan ke dalam variable "header".
3. Byte sampel data (byte ke 44 sampai byte terakhir) dipindahkan ke dalam variable "data".

4. Bit pertama dari byte pertama sampai byte ke enam belas diekstrak dari data. Jika hasilnya sama dengan salah satu identitas pada saat penyisipan, maka di dalam berkas tersebut terdapat pesan rahasia dan proses ekstraksi dapat dilakukan.

5. Apabila pengecekan bernilai ya, maka langkah selanjutnya adalah bit ukuran pesan dan bit pesan diekstrak. Bit-bit pesan yang telah diekstrak dikembalikan ke bentuk semula berdasarkan ukuran pesan.

Hasil proses penyisipan pada tahap penyisipan, maka text yang di sisipkan akan kembali ke seperti semula dengan proses ekstraksi di kembalikan dari nilai biner. Proses penyisipan kembali seperti semula.

Maka bilangan biner nya adalah $1000100_{(2)}$

$4=0100$

$4=0100$

Maka bilangan nya adalah $44_{(16)}$

D : terletak di kolom 4 dan baris 4

Maka bilangan biner nya adalah $1000101_{(2)}$

$4=0100$

$5=0101$

Maka bilangan nya adalah $45_{(16)}$

E : terletak di kolom 4 dan baris 5

Maka bilangan biner nya adalah $1010011_{(2)}$

$5=0101$

$3=0011$

Maka bilangan nya adalah $53_{(16)}$

S : terletak di kolom 5 dan baris 3

Maka bilangan biner nya adalah $1001101_{(2)}$

$4=0100$

$D=1101$

Maka bilangan nya adalah $4D_{(16)}$

M : terletak di kolom 4 dan baris D

Maka bilangan biner nya adalah $1000001_{(2)}$

$4=0100$

$D=0001$

Maka bilangan nya adalah $41_{(16)}$

A : terletak di kolom 4 dan baris 1

Maka bilangan biner nya adalah $1001110_{(2)}$

$4=0100$

$E=1110$

Maka bilangan nya adalah $4E_{(16)}$

N : terletak di kolom 4 dan baris E

Hasil penyisipan kembali ke text : DESMAN

Maka bilangan binernya adalah $1010111_{(2)}$

$5=0101$

$7=0111$

Maka bilangan nya adalah $57_{(16)}$

W : terletak di kolom 5 dan baris 7

Maka bilangan binernya adalah $1100001_{(2)}$

$6=0110$

$1=0001$

Maka bilangan nya adalah $6F_{(16)}$

a : terletak di kolom 6 dan baris 1

Maka bilangan binernya adalah $1101100_{(2)}$

$6=0110$

$C=1100$

Maka bilangan nya adalah $4C_{(16)}$

I : terletak di kolom 4 dan baris C

Maka bilangan binernya adalah $1101001_{(2)}$

$6=0110$

$9=1001$

Maka bilangan nya adalah $69_{(16)}$

i : terletak di kolom 6 dan baris C

Hasil penyisipan kembali ke text : Wali

Proses menggunakan Metode *Randked Positional Weight* ini terdiri dari proses pengambilan text.

4. KESIMPULAN

Berdasarkan analisa dan pembahasan yang dilakukan, maka dapat disimpulkan sebagai berikut :

1. Penelitian ini telah berhasil menghasilkan aplikasi steganografi penyisipan teks (.txt) pada file Mp3 berbasis desktop dengan mengimplementasikan metode *Randked Positional Weight (RPW)*.
2. Aplikasi steganografi dengan metode *Randked Positional Weight (RPW)* memiliki kemampuan menyisipkan text sebesar 100% dipengaruhi oleh ukuran file MP3 dan file teks (.txt) yang disisipkan. Aplikasi juga berhasil mengambil kembali text dengan tingkat *recovery* yang sangat baik dengan tingkat error 0% pada Mp3 yang tidak dikenai serangan kompresi.
3. Berdasarkan hasil pengujian ukuran steganografi file, dapat dinyatakan bahwa ukuran file Mp3 sebelum dan sesudah disisipi text adalah 100% sama, dimana artinya penyisipan text tidak mempengaruhi ukuran Mp3 sebelum dan sesudah disisipi text.

REFERENCES

- [1] Kusrini, M.kom. 2007. Konsep Dan Aplikasi Sistem Pendukung Keputusan, C.V ANDI OFFSET : Yogyakarta.
- [2] Kusrini dan Sulistyani, Ester, 2006, pemanfaatan Analytical Hierarchy Process(AHP) sebagai model sistem pendukung keputusan.
- [3] Kusrini dan Sulistyani, Ester, 2006, pemanfaatan Analytical Hierarchy Process(AHP) sebagai sistem pendukung keputusan.
- [4] Turban, 2005, Decision Support System and Intelegence System
- [5] G. Anthony Gorry dan Michael S. Scott Morton. Keduanya adalah profesor di MIF. Sebagai Sistem Pendukung Keputusan.
- [6] Menurut Irwanto. 2006, system yang lebih menekankan pada komponen atau elemen yang digunakan.
- [7] Murdick dab Ross. 1993, mendefinisikan system yang lebih menekankan pada elemen atau komponennya.
- [8] Schronderberg (dalam Suridinata, 1996) secara ringkas menjelaskan system.
- [9] Sistem pendukung keputusan mempunyai empat karakteristik utama. Fathul Wahid, 2005.
- [10] System pendukung keputusan (*Decision Support Sistem*) merupakan system informasi interaktif, Alter 2002.
- [11] Penyusunan model keputusan suatu cara untuk mengembangkan hubungan – hubungan logika yang mendasari persoalan keputusan. Evi Indrayani dan Humdiata, 2009.
- [12] Proses keluarnya suatu keputusan. Budi Sutedjo Dharma Oetomo, 2006.
- [13] Menurut Saaty. 1993, hirarki sebagai suatu representasi dari sebuah permasalahan yang kompleks.
- [14] Menurut Mulyono. 1996, menjelaskan bahwa pada dasarnya metode AHP merupakan suatu teori umum.
- [15] Pernadi. 1996, menjelaskan peralatan umum metode AHP.
- [16] Faktor yang perlu di perhatikan dalam melakukan proses penjabaran hirarki. Suryadi & Ramadhani 1998.