ISBN: 978-602-52720-1-1
Januari 2019
Hal: 890 - 893

Penyisipan Pesan Rahasia Kedalam Audio Menggunakan Algoritma F5

Tri Nusanti Sianturi, Rinaldo Gomgom Hutagaol

Prodi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338, Medan, Indonesia

Abstrak

Teknologi informasi dan telekomunikasi yang semakin berkembang saati ini, telah mempengaruhi perhatian pada tingkat keamanan terhadap data dan informasi. Saat ini telah banyak kasus penyalahgunaan data dan nformasi yang didistribuskan, khususnya yang menggunakan layanan internet. Peningkatan keamanan pengiriman data dapat dilakukan dengan menggunakan steganografi. Steganografi adalah teknik menyembunyikan pesan ke dalam sebuah media pembawa (carrier). Salah satu media yang dapat digunakan adalah berkas audio. Penelitian ini membahas tentang penerapan steganografi pada berkas audio dan metode steganografi yang digunakan adalah metode F5. Hasil uji coba, diketahui bahwa dengan metode F5 penyisipan dan ekstraksi pesan dapat dilakukan dengan baik. Penyisipan pesan tidak berpengaruh terhadap ukuran berkas audio, akan tetapi berkas audio yang telah disisipi pesan (stego) tidak tahan terhadap kompresi, manipulasi amplitudo dan pemotongan audio.

Kata Kunci: Steganografi, Algoritma F5, Pesan, Audio, Wav

1. PENDAHULUAN

Perkembangan teknologi pada industri musik saat ini sangat pesat. Perkembangan industri musik juga memiliki banyak masalah, salah satunya pembajakan hak cipta audio. Hingga saat ini audio masih menjadi salah satu media yang sering digunakan dalam bertukar pesan atau informasi penting. Tingkat keamaan dalam pegiriman informasi dalam bentuk audio sangatlah penting agar kerahasiaan dan keaslian audio tersebut tetap terjaga. Pesan adalah setiap pemberitahuan, kata, atau komunikasi baik lisan maupun tertulis, yang dikirimkan dari satu orang ke orang lain[1].

Teknik steganografi merupakan salah satu teknik yang cukup aman sebagai upaya untuk mengatasi permasalah di atas. Steganografi bertujuan untuk megamankan data dengan meyisipkan pesan rahasia kedalam suatu media, sehingga hanya pihak yang terkait saja yang dapat mengetahui bahwa ada pesan rahasian [2]. Teknik ini diperkuat karena dalam proses ekstraksi pesan rahasia, harus menggunakan kata sandi atau passwond yang sama. Algoritma F5 adalah metode yang mampu mejaga sifat-sifat histogram DCT dengan baik cukup unggul dalam kapasitas supaya data pesan rahasia tersebut tidak dapat dibajak oleh orang lain. Algoritma F5 bekerja dengan menyisipkan bit pesan kedalam bit koefisien DCT hasil kuantisasi yang telah dipermutasi [3]. Penelitian ini membahas proses penerapan algoritma F5 untuk menyembunyikan pesan rahasia sebagai penanda hak cipta pada sebuah pesan audio dengan tujuan agar keaslian dari pesan audio dapat dideteksi.

Tabel 1. Penelitian Terkait

No	Penulis	Judul	Kesimpulan
1	Patrisius Batarius dan Martinus Maslim	Perbandingan Metode dalam Teknik Steganografi [4]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa Steganografi dapat digunakan sebagai salah satu teknik dalam keamanan suatu data serta dalam penyampaian suatu pesan. Metode yang digunakan dapat dibagi menjadi dua yaitu spatial domain dan transform domain
2	Ermadi Satriya Wijaya dan Yudi Prayudi	Konsep Hidden Message dengan Menggunakan Teknik Steganografi Dynamic Cell Spreading[5]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa dengan steganografi, maka masalah yang terkait dengan hak cipta dan kepemilikan dapat dipecahkan, hal ini mengacu pada sifat dasar steganografi yaitu menyembunyikan pesan
3	Derwin Suhartono, Afan Galih Salman, Rojali dan Christian Octavianus	Aplikasi Penyembunyian Pesan pada Citra JPEG dengan Algoritma F5 dalam Perangkat Mobile Berbasis Android [6]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa penerapan algoritma F5 menghasilkan citra yang tidak jauh berbeda dengan citra aslnya, sehingga dapat mengoptimakan keamanan informasi.

2. METODOLOGI PENELITIAN

2.1 Pesan

Pesan adalah setiap pemberitahuan, kata, atau komunikasi baik lisan maupun tertulis, yang dikirimkan dari satu orang ke orang lain. Pesan menjadi inti dari setiap proses komunikasi yang terjalin. Salah satu hal yang perlu diperharikan pada saat

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 890 - 893

melakukan proses penyisipan pesan ke dalam audio adalah ukuran audio harus lebih besar dari jumlah data yang harus disembunyikan atau diamankan, perubahan yang terjadi pada steganografi tidak signifikan dan masih tampak seperti audio normal karena *bit* yang mempengaruhi pada media audio adalah *byte* yang terendah[7].

2.2 Audio

Audio adalah suara atau bunyi yang dihasilkan oleh getaran suatu benda, agar dapat tertangkap oleh telinga manusia getaran tersebut harus kuat minimal 20 kali/detik. Suara yaitu suatu getaran yang dihasilkan oleh gesekan, pantulan dan lain-lain, antara benda-banda[8]. Media audio merupakan media yang dapat di gunakan sebagai media pengajaran yang di dalamnya mengandung pesan di dalam bentuk auditif yang berguna untuk dapat merangsang pikiran, perhatian, perasaan, dan juga kemauan penggunanya. Media audio sendiri merupakan suatu alat yang di dalamnya berisi pesan yang dapat diterima menggunakan media pendengaran saja.

2.3 Steganografi

Steganografi merupakan teknik untuk menyisipkan informasi kedalam media yang tidak dapat diduga oleh orang biasa, sehingga tidak menimbulkan suatu kecurigaan kepada orang yang melihatnya[4],[5],[9]. Cara kerja steganografi :

1. *Imperceptibility*, keberadaan pesan rahasia dalam media penumpang tidak dapat di deteksi.
2. *Fildelity*, keunggulan media penumpang setalah ditambahkan dengan media penumpang tidak jauh berbeda sebelum ditambahkan pesan rahasia.
3. *Recovery*, pesan rahasia yang disispkan dapat di ungkap kembali.
4. *Robustness*, pesan yang disembunyikan harus tahan terhadap operasi manipulasi yang dilakukan pada media penumpang.

Perbedaan antara berkas awal dan berkas ahkir dalam steganografi dapat dihutung dengan menghitung nilai MSE dan PSNR.

$$MSE= \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}\left[I(x,y) - I'(x,y)\right]^2 \quad (1)$$

MSE = Nilai *Mean Significant Error* dalam steganografi

$$PSNR= 10.\log\left(\frac{MAX\ i^2}{MSE}\right) \quad (2)$$

MAX i = Nilai *maximum* dari *pixel* yang digunakan

Semakin rendah nilai MSE, maka akan semakin baik dan semakin tinggi nilai PSNR, maka akan semakin baik kualiatas hasil steganografi.

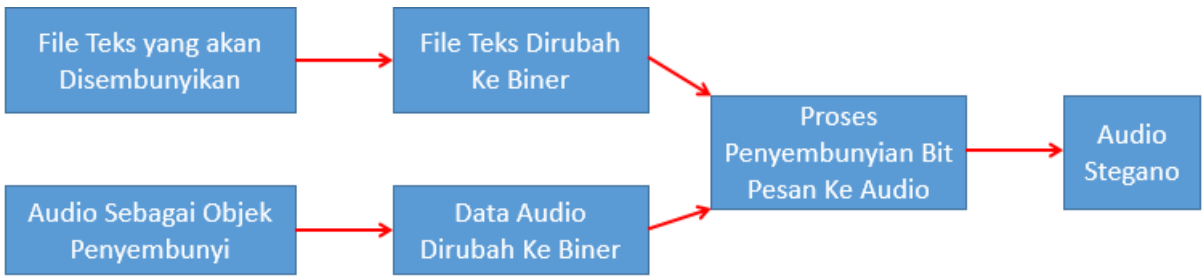
2.4 F5

Algoritma F5 menyisipkan bit pesan kedalam bit koefisien DCT hasil kuantisasi yang telah dipermutasi, penilaian sebuah algoritma steganografi yang baik salah satunya dapat dipandang dari banyaknya pesan yang dapat disisipkan dalam audio[6],[9],[10]. Proses embeddig terdiri dari langkah-langkah berikut:

1. Sediakan pesan yang disisipkan dalam audio
2. Menghitung kapasitas tanpa embedding matriks C=h_{DCT}/ 64-h(0)-h(1) +0.49h (1), dimana h_{DCT} adalah jumlah koefisien DCT h (0).
3. Password ditetukan oleh pengguna untuk menghasilkan nilai PSNR.
4. Jika ukuran pesan sesuai dengan perkiraan kapasitas maka proses embed berlaut, lain daripada itu error yang menunjukan panjang maksimal yang akan ditampilkan.

3. ANALISA DAN PEMBAHASAN

Langkah-langkah penyisipan pesan rahasia ke dalam audio :



Gambar 1. Bagan Penyisipan Teks Pada Audio

Langkah-langkah penyisipan bit-bit pesan ke dalam berkas audio adalah sebagai berikut :

a. Berkas audio dibaca dan byte-byte hasil pembacaan disimpan ke dalam variable “fid1”.

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 890 - 893

b. Informasi mengenai berkas audio disiapkan dengan cara mengambil 44 byte pertama dari "fid1" dan pindahkan ke dalam variable "info". Byte-byte ini berisi informasi mengenai chunk header, chunk fmt, chunk data dan tidak dapat disisipi bit pesan.
c. Byte sampel data (byte ke 45 sampai byte terakhir) dipindahkan ke dalam variable "dta".
d. Pesan berupa gambar diinput.
e. 16 bit unik disiapkan dan disimpan ke dalam variable "identitas". Bit-bit ini dibutuhkan sebagai penanda apakah di dalam berkas audio terdapat pesan gambar atau tidak. Identitas ini didefinisikan oleh programmer dengan seunik mungkin dan identitas yang digunakan adalah [1100110011001100].
f. Pesan dan ukurannya dibaca.
g. Sebelum dilakukan penyisipan, terlebih dahulu dicek apakah penyisipan dapat dilakukan atau tidak. Pengecekan dilakukan berdasarkan jumlah byte sampel data dan jumlah bit identitas + bit ukuran pesan + bit pesan. Jika jumlah bit identitas + bit ukuran pesan + bit pesan lebih kecil dari jumlah byte sampel data, maka proses penyisipan dapat dilakukan.
h. Apabila pengecekan bernilai ya, maka langkah selanjutnya adalah pesan dan ukurannya diubah ke dalam bentuk bit. Kemudian bit identitas, bit ukuran pesan, dan bit pesan disisipkan ke dalam "dta". Penyisipan dilakukan dengan mengganti bit pertama (bit yang tidak terlalu berpengaruh) dari setiap byte sampel data. Identitas disisipkan pada byte pertama sampai byte keenambelas. Sedangkan bit ukuran pesan dan bit pesan disisipkan pada byte ketujuh belas dan seterusnya.
i. Data audio yang telah disisipi pesan disimpan dengan mengikutsertakan informasi berkas audio dari variable "info". Informasi ini ditulis pada awal berkas. Bila informasi ini tidak diikutsertakan, maka berkas audio tidak dapat dikenali.

3.1 Pembahasan

Pada pengujian ini, disediakan 3 audio dengan format wav (*.wav) dengan ukuran resolusi berbeda yang diberi perlakuan yang sama yaitu disisipkan pesan sebanyak 500 karakter dan diberi password —I LOVE U. Pengujian ini dilakukan untuk mengetahui berapa bytes ukuran file audio setelah disisipkan pesan dengan panjang karakter yang sama dan berapa lama waktu encode yang diperlukan.
Berikut adalah gambar gelombang audio menggunakan program aplikasi Quik Time Player hasil steganografi

Gambar 2. Hasil Steganografi

Berdasarkan gambar 2 di atas dapat disimpulan bahwa audio hasil steganografi tidak jauh beda dengan gambar gelombang sebelumnya. Berdasarkan hasil perbandingan nila MSE dan PSNR maka diperoleh :

Tabel 2. Nilai Pengujian

No	Nama File Audio	Ukuran Sebelum	Ukuran Setelah	Nilai PSNR
1	erwn1.wav	272 KB	21.3 KB	63.03195
2	erwn2.wav	23.3 KB	12.7 KB	72.32379
3	erwn3.wav	34.7 KB	12.2 KB	72.536

4. KESIMPULAN

Penyisipan pesan berdasarkan metode F5 dilakukan dengan mengganti bit pertama atau bit yang tidak terlalu berpengaruh dengan bit-bit pesan sehingga proses penyisipan dan ekstraksi pesan dapat dilakukan dengan baik. Penyisipan pesan dengan metode F5 juga tidak berpengaruh terhadap kualitas suara karena sulit dideteksi oleh pendengaran manusia serta tidak mengubah ukuran berkas audio atau dengan kata lain, ukuran berkas audio sebelum dan setelah penyisipanadalahsama. Berdasaran hasil pengujian ketahanan data, maka berkas audio yang telah disisipi pesan (steganografi) tidak tahan terhadap tiga faktor, yaitu kompresi, manipulasi amplitudo dan pemotongan audio. Pesan sama sekali tidak dapat diekstrak setelah audio stego dikompres atau dimanipulasi amplitudonya, hal ini disebabkan karena bagian audio yang dipotong tidak termasuk byte sampel data audio yang telah disisipi bit pesan dan bit informasi pendukung.

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 890 - 893

REFERENSI

[1] M. Magdalena, N. A. Putra, and E. P. Widiyanto, "Implementasi Algoritme F5 untuk Penyisipan Pesan Rahasia pada Citra Digital," pp. 1–14.
[2] T. Zebua, "Pengamanan Data Teks Dengan Kombinasi Cipher Block Chaining dan LSB-1," in *Seminar Nasional Inovasi dan Teknologi (SNITI)*, 2015, pp. 85–89.
[3] E. Pramunanto, Y. Perwira, A. Putra, and A. Zaini, "Penulisan Pesan Tersembunyi Pada Citra JPEG dengan Metode F5," vol. 10, no. 2, pp. 1–8, 2012.
[4] P. Batarius and M. Maslim, "Perbandingan Metode dalam Teknik Steganografi," in *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*, 2012, pp. 307–313.
[5] E. Satriya Wijaya and Y. Prayudi, "Konsep Hidden Message dengan Menggunakan Teknik Steganografi Dynamic Cell Spreading," *Media Inform.*, vol. 9, no. 9, pp. 121–126, 2011.
[6] D. Suhartono, A. Galih Salman, Rojali, and C. Octavianus, "Aplikasi Penyembunyian Pesan pada Citra JPEG dengan Algoritma F5 dalam Perangkat Mobile Berbasis Android," in *Seminar Nasional Aplikasi Teknologi Informasi*, 2012, pp. 1–6.
[7] S. Rohayah, G. W. Sasmito, and O. Somantri, "Aplikasi Steganografi Untuk Penyisipan Pesan," *J. Inform.*, vol. 9, no. 1, pp. 975–981, 2015.
[8] N. Q. Fitriyah and Y. Y. Prayudi, "Implementasi Steganografi Audio File Wav Dengan Metode Discrete Cosine Transform (Dct)," pp. 144–153, 2017.
[9] G. D. A, R. M. Rumani, and M. Nasrun, "Implementasi Kriptografi Dan Steganografi Pada Media Gambar Menggunakan Algoritma Blowfish Dan Metode Least Significant Bit Cryptography and Steganography Implementation in Image Using Blowfish Algorithm and Least Significant Bit Method," *Implementasi Kriptografi Dan Steganografi Pada Media Gambar Menggunakan Algoritm. Blowfish Dan Metod. Least Signif. Bit*, vol. 2, no. 2, p. 8, 2015.
[10] D. Suhartono, A. G. Salman, and C. Octavianus, "Aplikasi Penyembunyian Pesan Pada Citra Jpeg Dengan Algoritma F5 Dalam Perangkat Mobile Berbasis Android," vol. 2012, no. Snati, pp. 15–16, 2012.