Jurnal Sains Riset (JSR)
p-ISSN 2088-0952, *e*-ISSN 2714-531X

OPTIMALISASI STEGANOGRAFI AUDIO UNTUK PENGAMANAN INFORMASI

Sayed Achmady[1], Laila Qadriah[2]

[1,2]Fakultas Teknik, Universitas Jabal Ghafur Sigli, Aceh
Jl, Garot-Lamlo, Gle Gapui. 24163
[1,2]sayedachmady@unigha.ac.id[1], laila_qadriah@unigha.ac.id[2]

ABSTRAK

Dalam komunitas internet saat ini, transfer data yang aman terbatas karena adanya serangan terhadap data komunikasi. Jadi metode yang lebih baik digunakan untuk memastikan transfer data yang aman salah satunya adalah menyematkan audio kedalam gambar (Steganografi audio). Teknik yang biasa digunakan untuk audio steganografi adalah domain temporal dan teknik transformasi domain, di mana teknik frekuensi domain dan teknik domain wavelet berada di bawah transformasi domain. Dimana teknik yang dipelajari domain wavelet menunjukkan kapasitas persembunyian informasi rahasia yang tinggi dan transparansi. Berbagai teknik diterapkan pada domain wavelet koefisien untuk meningkatkan kapasitas persembunyian dan transparansi persepsi. Cenderung ke arah merancang sistem yang memastikan kapasitas persembunyian data yang tinggi dan aman dengan teknik steganografi. Dalam makalah ini, kami menuliskan tentang teknik steganografi audio digital.

Kata kunci : Keamanan data digital, steganografi audio, penyembunyian informasi, sinyal stego, Embedding.

Pendahuluan

Steganografi, yang berarti "tulisan tertutup" telah menarik perhatian banyak orang beberapa tahun terakhir ini. Tujuan utamanya untuk menyembunyikan informasi rahasia tentang komunikasi antara dua pihak. Pengirim yang menyematkan data rahasia dalam bentuk apapun dengan menggunakan kunci file sampul didalam digital untuk menghasilkan file stego, sehingga pengamat tidak dapat mendeteksi keberadaan pesan yang tersembunyi. Di sisi lain, penerima memproses file stego yang diterima untuk diekstrak pesan yang tersembunyi. Informasi komunikasi rahasia yang menggunakan sinyal audio cover tidak berbahaya, seperti percakapan telepon atau konferensi video.

Untuk meminimalkan perbedaan antara media asli dan pesan yang setelah diproses dengan menanamkan data tersembunyi, di satu sisi teknik steganografi baru-baru ini mendapat manfaat dalam persepsi pendengaran dan visual manusia, dan di sisi lain dari sifat-sifat media digital dimanfaatkan untuk menutupi komunikasi rahasia kendaraan. Steganografi berbasis gambar dan video bergantung pada manusia yang terbatas dalam sistem visual pada variasi pencahayaan dan tingkat yang lebih besar dari 1 dalam 240 dan pada tingkat abu-abu yang seragam atau 1 dalam 30 pada pola acak. Namun, steganografi berbasis audio mengeksploitasi Sistem Pendengaran (HAS) pada properti efek masking dari Manusia. Berbagai fitur yang memengaruhi kualitas metode steganografi audio. Tapi, keuntungan dan dampak tergantung pada aplikasi dan lingkungan transmisi dari masing-masing.

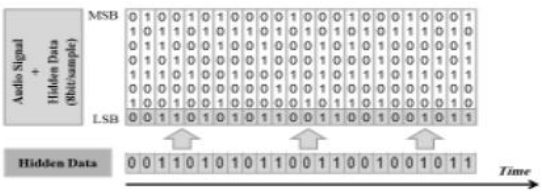
Properti paling penting pada ketahanan terhadap kebisingan dan manipulasi sinyal, keamanan, dan kapasitas menyembunyikan data yang disematkan. Persyaratan ketahanan berkaitan erat dengan aplikasi dan yang menantang sistem steganografi. Selain itu, ada tradeoff antara ketahanan dan kapasitas penyembunyian informasi rahasia. Secara umum, mereka hampir tidak hidup berdampingan dalam sistem steganografi yang sama. Dalam ulasan ini, penggunaan file audio sebagai

media sampul untuk komunikasi rahasia kendaraan secara menyeluruh. Beberapa karya seni dalam steganografi audio akan dibahas dalam jurnal ini.

DOMAIN SEMENTARA

Pengkodean LSB

LSB (Least Significant Bit), adalah salah satu metode populer yang digunakan untuk menyembunyikan informasi yang terdiri dalam menyematkan setiap bit dari pesan dalam bit yang paling tidak signifikan dari audio sampul dengan cara yang deterministic. Jadi, untuk audio sampel 16 kHz, 16 kbps data yang disematkan. Metode LSB memungkinkan penyematan kapasitas yang tinggi untuk menyembunyikan data yang relatif mudah diimplementasikan atau digabungkan dengan teknik persembunyian lainnya. Namun Teknik ini ditandai dengan ketahanan yang rendah terhadap penambahan noise. Oleh karena itu, keamanannya juga rendah karena sangat rentan bahkan terhadap serangan sederhana. Memfilter, menguatkan, menambah noise atau kompresi stego-audio akan sangat memungkinkan untuk menghancurkan data. Seorang penyerang dapat dengan mudah mengungkap pesan dengan hanya menghapus seluruh LSB. Secara sederhana, strategi LSB telah diterapkan untuk menanamkan pesan suara dalam komunikasi nirkabel.



Gambarr.1: LSB dalam sinyal 8b / sampel ditimpa oleh sedikit bit data tertanam.

Untuk meningkatkan ketahanan terhadap distorsi dan kebisingan metode LSB yang telah meningkatkan kedalaman menyematkan informasi lapisan ke-4 dari lapisan ke-8 LSB tanpa mempengaruhi transparansi persepsi stego sinyal audio. Hanya dalam bit pada posisi keenam dari masing-masing 16 bit sampel dari sinyal host asli diganti dengan bit dari pesan. Untuk meminimalkan kesalahan embedding, bit lain dapat dibalik agar memiliki sampel baru yang lebih dekat dengan yang asli.

Fakta bahwa embedding terjadi pada bit kedelapan akan sedikit meningkatkan kekokohan metode ini dibandingkan dengan metode LSB konvensional. Namun, kapasitas persembunyiannya akan berkurang karena beberapa sampel harus dibiarkan yang tidak dapat diubah untuk mempertahankan persepsi kualitas sinyal audio.

Pengkodean paritas

Salah satu karya sebelumnya dalam teknik penyembunyian data audio adalah teknik pengkodean paritas. Mengalihkan untuk memutus sinyal turun menjadi sampel individu, metode pengkodean paritas memecahkan sinyal menjadi beberapa bagian sampel yang terpisah dan mengkodekan setiap bit dari pesan rahasia di bit paritas wilayah sampel. Jika paritas sedikit dari wilayah yang dipilih tidak cocok dengan bit rahasia yang akan dikodekan, proses yang dilakukan yaitu dengan membalik LSB dari salah satu sampel di wilayah tersebut. Dengan demikian, pengirim memiliki lebih banyak pilihan dalam penyandian bit rahasia, dan sinyal dapat diubah dengan cara yang lebih aman dan tidak berpengaruh pada mode.

Menyembunyikan Gema

Teknik menyembunyikan gema yaitu dengan menanamkan informasi rahasia dalam file suara dengan memasukkan gema ke dalam sinyal diskrit. Echo persembunyian memiliki keunggulan dalam memberikan tingkat transmisi data yang tinggi dan ketahanan yang unggul jika dibandingkan dengan metode lain. Hanya satu bit informasi rahasia yang dapat disandikan jika hanya satu gema yang dihasilkan dari sinyal asli. Oleh karena itu, sebelum proses pengkodean dimulai, sinyal asli dipecah menjadi beberapa blok. Sekali proses pengkodean dilakukan, blok-blok digabungkan kembali untuk menciptakan sinyal akhir. Untuk menyembunyikan data yang telah berhasil, ada tiga parameter gema

yang bervariasi: amplitudo, tingkat peluruhan dan offset (waktu tunda) dari sinyal asli. Ketiga parameter diatur di bawah ambang pendengaran manusia, sehingga gema tidak mudah terselesaikan. Selain itu, offset bervariasi untuk mewakili pesan biner yang akan dikodekan.

Karena tingkat embedding yang rendah dan keamanan yang rendah, tidak ada system steganografi audio berdasarkan penyembunyian gema, hanya beberapa teknik yang telah diusulkan untuk watermarking audio. Untuk meningkatkan ketahanan sistem watermark terhadap pemrosesan sinyal umum, waktu penyembunyian gema yang menarik teknik penyebaran telah diusulkan dibandingkan dengan sistem penyembunyian gema konvensional.

Metode mendeteksi bit watermark berdasarkan jumlah korelasi pada penerima tidak pada penundaan.

Transformasi Domain

Frekuensi domain

Penyisipan nada

Properti masking frekuensi dieksploitasi dalam metode penyisipan nada. Nada murni yang lemah ditutupi dari nada yang lebih kuat. Properti yang tidak dapat terdengar ini digunakan dengan berbagai cara untuk menyembunyikan informasi rahasia. Dengan memasukkan nada pada frekuensi tingkat daya yang rendah, penyisipan data tersembunyi yang diekstraksi tercapai. Penulis dari metode ini mengakui kapasitas persembunyian 250 bps ketika empat nada dimasukkan dalam setiap spektrum bicara. Setiap upaya untuk lebih meningkatkan kapasitas harus menggunakan lebih dari empat nada. Metode penyisipan nada dapat menahan beberapa serangan yang tidak disengaja seperti penyaringan low-pass dan bit.

Pengkodean fase

Pengkodean fase mengeksploitasi ketidakpekaan sistem audio manusia terhadap fase relatif dari berbagai komponen spektral. Ini didasarkan pada penggantian komponen fase yang dipilih dari spektrum pidato asli dengan data tersembunyi. Namun, untuk memastikan nada tidak terdengar, modifikasi komponen fase harus tetap kecil. Juga diakui bahwa di antara teknik penyembunyian data, pengkodean fase mentolerir distorsi sinyal yang lebih baik. Penulis telah memasukkan data dalam komponen fase menggunakan modulasi fase multi-band independen. Dalam pendekatan ini, fase tidak terlihat bahwa modifikasi yang dicapai menggunakan perubahan fase terkontrol dari audio host. Suara asli sinyal dipecah menjadi segmen yang lebih kecil yang panjangnya sama dengan ukuran pesan yang akan dikodekan.

Kerugian terkait dengan pengkodean fase adalah tingkat transmisi data yang rendah bahwa pesan rahasia dikodekan dalam segmen sinyal pertama saja dan untuk bias mengekstrak pesan rahasia dari file suara, penerima hanya saja bias mengetahui panjang segmen tersebut.

Spread spectrum

Teknik Spread spectrum menyebar data sinyal tersembunyi melalui spektrum frekuensi. Spread Spectrum (SS) adalah konsep yang dikembangkan dalam komunikasi untuk memastikan pemulihan sinyal yang dikirim dengan benar melalui saluran berisik dengan menghasilkan salinan sinyal data yang berlebihan. Dalam urutan langsung konvensional, Teknik spread spectrum (DSSS) diterapkan untuk menyembunyikan informasi rahasia audio digital MP3 dan WAV sinyal. Untuk tingkat persembunyian 20 bps lebih baik menggunakan teknik SS dalam domain sub-band. Koefisien subband dapat dipilih untuk mengatasi masalah ketahanan dan menyelesaikan ketidakpastian sinkronisasi didekoder.

Modifikasi amplitudo

Fenomena "efek topeng" menutupi frekuensi yang lebih lemah di dekat frekuensi resonansi yang kuat. Metode asli telah diusulkan di mana komponen frekuensi magnitudo ganjil asli diinterpolasi untuk menghasilkan sampel genap yang digunakan untuk menanamkan bit data. Pada penerima, sampel ganjil asli dan

sampel genap yang diinterpolasi sama dengan di coder. Metode ini memiliki kapasitas 3 kbps dan menyediakan kekokohan terhadap pemrosesan sinyal audio umum seperti gema, tambah noise, filtering, resampling dan MPEG kompresi.

Domain cepstral

Sinyal penutup diubah menjadi domain cepstral dan data disematkan dalam koefisien cepstrum yang dipilih untuk menerapkan manipulasi rata-rata statistik. Dalam metode ini, laju penyisipan mencapai 20 hingga 40 bps namun menjamin ketahanan untuk serangan sinyal umum. Dalam metode ini memastikan tingkat embedding yang dapat diandalkan sekitar 54 bit / s dan algoritma yang terakhir dapan menanamkan data dengan berbagai komponen frekuensi arbitrer di setiap frame untuk meningkatkan keamanan.

Domain wavelet

Audio steganografi berdasarkan Discrete Wavelet Transform (DWT) merupakan data yang tertanam di dalam LSB dari koefisien wavelet yang mencapai kapasitas tinggi 200 kbps dalam sinyal audio 44,1 kHz. Meningkatkan data imperceptibilitas yang tertanam dengan menggunakan ambang pendengaran ketika menanamkan data dalam wavelet integer koefisien, sambil menghindari data tersembunyi di bagian sunyi dari sinyal audio.

Haider Ismael Shahadi dan Razali Jidin mengusulkan, steganografi audio berkapasitas tinggi dan tidak terdengar skema. Algoritma ini didasarkan pada transformasi paket wavelet diskrit dengan persembunyian adaptif bit yang paling tidak signifikan. Di sini sinyal input tersegmentasi ke dalam segmen G. Pesan rahasia juga tersegmentasi ke dalam segmen G.

Sinyal penutup didekomposisi menjadi koefisien wavelet dan setiap sinyal detail diskalakan sesuai dengan nilai maksimum dan jumlah bit per sampel. Untuk setiap sampel, algoritma menentukan jumlah bit yang bisa disembunyikan dengan aman. Pada langkah selanjutnya tombol stegano tertanam pada sinyal detail frekuensi terendah yang mana membuat stegano-key lebih tahan terhadap distorsi. Algoritma yang telah mendapatkan kapasitas persembunyian yang tinggi dan kualitas output yang sangat baik.

Dora M. Ballesteros L dan Juan M Moreno A mengusulkan sebuah makalah dalam domain wavelet berdasarkan Efisien Masking wavelet (EWM). EWM adalah model steganografi yang mengadaptasi pesan rahasia ke sinyal host. Ia menggunakan dua prinsip: adaptasi yang efisien dan properti masking dari Sistem Audit Manusia (HAS). Metode ini juga menggunakan kunci rahasia yang menambah keamanan tambahan. Dalam ujung pemancar output akan mirip dengan pembawa dengan pesan rahasia yang tertanam di dalamnya. Peretas itu akan dibutakan oleh sinyal yang ditransmisikan.

Domain enkoder

Saat mempertimbangkan penyembunyian data untuk komunikasi waktu nyata, codec ucapan seperti: AMR, ACELP, SILK menggunakan tingkat pengkodean masing-masing. Melewati salah satu codec, sinyal yang ditransmisikan diberi kode dan dikompres sesuai dengan laju codec kemudian didekompresi pada akhir decoder. Ketika mempresentasikan teknik steganografi lossless untuk juru kode telepon G.711-PCMU. Satu bit tertanam di dalam 8 bit data ucapan yang amplitudo absolutnya nol. Tergantung pada jumlah sampel yang mutlakdari setiap amplitudo adalah 0, tingkat persembunyian potensial mulai dari 24 - 400 bps.

Analisis Teganografi Audio

Untuk mengevaluasi kinerja teknik yang ditinjau, maka harus menggunakan rasio signal-to-noise SNR. Nilai SNR menunjukkan jumlah distorsi yang disebabkan oleh data yang disematkan dalam cover sinyal audio sc (m, n). Berdasarkan persamaan yang diperoleh, Nilai SNR sebagai berikut:

$$SNR_{dB} = 10\log_{10}\left(\frac{\sum_{n=1}^{N}|s_c(m,n)|^2}{\sum_{n=1}^{N}|s_c(m,n)-s_s(m,n)|^2}\right)$$

Di mana ss (m, n) adalah sinyal stego-audio seperti: m = 1 ... M dan n = 1 .... N, di mana M adalah jumlah frame dalam milidetik (ms) dan N adalah jumlah sampel dalam setiap bingkai.

Untuk mengontrol distorsi yang disebabkan oleh proses embedding, sebagian besar metode steganografi audio didasarkan pada domain frekuensi dengan menggunakan model perseptual untuk menentukan jumlah data tanpa embedding yang diizinkan mendistorsi sinyal audio.

Banyak algoritma steganografi audio yang menggunakan masking dan frekuensi masking pendengaran sebagai model persepsi untuk embed steganografi. Selain itu, adanya beberapa domain frekuensi pendekatan, antara lain: fase embedding secara implisit mewarisi sifat fase yang meliputi ketahanan terhadap manipulasi sinyal linier seperti: amplifikasi, redaman, pemfilteran, resampling, dll. Kinerja dari metode ini dianalisis dalam hal MSE (Mean Squared Error), PSNR (Peak Signal-to-Noise Ratio) dan SNR (Rasio Signal-to-Noise). Evaluasi kualitas subjektif dari metode ini dapat dilakukan dengan mendengarkan tes dan membandingkan sumber asli dengan sinyal audio dan sinyal audio stego yang sesuai.

Tabel 1. Ringkasan Teknik Steganography Audio

Method	Strength	Weakness
LSB	Simple	Easy to extract
Parity coding	More robust than LSB	Easy to extract
Echo hiding	Avoids problem with additive noise	Low capacity
Tone insertion	Exploits masking property	Low embedding capacity
Phase coding	Robust	Low capacity
Spread spectrum	Increases transparency	Occupies more bandwidth
Wavelet domain	High hiding capacity and transparency	Lossy data retrieval

Kesimpulan

Hingga saat ini tantangan utama dalam steganografi audio digital adalah steganografi audio ke audio dengan efisiensi tinggi, lossless adalah teknik keamanan terbaik. Makalah ini menyajikan tinjauan tentang teknik dan pendekatan steganografi audio digital. Kami membahas potensi dan keterbatasan dalam memastikan komunikasi yang aman. Dari sudut pandang, perbandingan dan evaluasi untuk teknik yang ditinjau juga telah diberikan. Keuntungan menggunakan satu teknik dibandingkan teknik lainnya sangat tergantung pada jenis aplikasi dan urgensi seperti kasitas persembunyian atau jenis serangan yang mungkin menemukan sinyal yang ditransmisikan.

Referensi

Fatiha Djebbar, Beghdad Ayady, Habib Hamamzand Karim Abed-Meraim, “A view on latest audio stegnography”, International Conference on Innovations in Information Technology, 2013, pages 409-414.

F. Djebbar, H. Hamam, K. Abed-Maraim, D. Guerchi, ”Controlled Distortion for High Capacity Data-in-speech Spectrum Steganography”, 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP’06), Germany, Oct 2011.

Haider Ismael Shahadi and Razali Jidin, “High capacity and inaudibility audio steganography scheme”, 7th International Conference n Information Assurance and Security (IAS), IEEE, 2012.

Jayaram P. , Ranganatha H R. , Anupama H S, “ Information hiding using audio steganography – a survey” , International Journal of Multimedia

& its applications ,Vol.3, No.3, August 2012.

K. Gopalan and S. Wenndt, "Audio steganography for covert data transmission by imperceptible tone insertion", Proceedings of Communications Systems and Applications, IEEE, 2005.

Muhammad Asad, Junaid Gilani, Adnan Khalid , " An enhanced least significant bit modification technique for audio steganography ", International Conference on Computer Networks and Information Technology (ICCNIT), 2012.

M. Nutzinger and J. Wurzer, "A novel phase coding technique for steganography in auditive media", 2012 Sixth International Conference on Availability, Reliability and Security (ARES), IEEE, 2012.