

Pengamanan Pesan Menggunakan Kombinasi Kriptografi dan Steganografi Audio Berbasis Transformasi Wavelet Diskrit

Ahmad Ulul Albab dan Darmaji

Departemen Matematika, Institut Teknologi Sepuluh Nopember (ITS)

e-mail: darmaji@matematika.its.ac.id.

Abstrak—Teknologi saat ini berkembang sangat pesat dan berpengaruh pada keseharian kita dalam berkomunikasi, dampak perkembangan teknologi saat ini, mengirim dan menerima pesan dapat dilakukan dengan mudah dan cepat. Selain itu, perkembangan teknologi juga berdampak pada berkembangnya penyadapan pesan ilegal yang dilakukan oleh pihak yang tidak seharusnya mendapatkan pesan. Salah satu solusi untuk masalah tersebut adalah kriptografi dan steganografi. Kriptografi sendiri adalah ilmu menyandikan pesan, sedangkan steganografi adalah ilmu menyembunyikan pesan ke dalam media lain. Pada penelitian ini menerapkan pengamanan pesan menggunakan kombinasi kriptografi dan steganografi audio. Proses diawali dengan menyandikan pesan dengan algoritma RSA, pesan yang sudah disandikan akan disembunyikan ke dalam audio dengan Transformasi Wavelet Diskrit (DWT). Hasil uji coba menunjukkan bahwa pesan dapat diamankan dengan baik. Pada uji coba dengan sampel audio file WAV berdurasi 17 detik disisipi 50.107 karakter pesan, hanya 8,7% responden yang berpendapat bahwa audio asli dan audio yang sudah disisipi pesan rahasia keduanya berbeda.

Kata Kunci—Kriptografi, Steganografi, Audio, Transformasi Wavelet Diskrit, RSA.

I. PENDAHULUAN

PERKEMBANGAN teknologi yang pesat memudahkan manusia dalam berkomunikasi. Mengirim dan menerima pesan adalah bentuk komunikasi yang sederhana dan sering digunakan. Semakin berkembangnya teknologi, semakin mudah juga meretas atau menyadap pesan-pesan yang harusnya memiliki privasi yang terjaga. Terdapat dua cara yang bisa membantu menyelesaikan permasalahan tersebut, yaitu Kriptografi dan steganografi. Kriptografi adalah ilmu yang mempelajari bagaimana cara menjaga agar data atau informasi tetap aman dari pihak ketiga dengan cara mengubah data tersebut menjadi bentuk lain[1]. Sedangkan steganografi adalah ilmu yang mempelajari bagaimana cara menyembunyikan data atau pesan rahasia sehingga tidak seorang pun yang mencurigai keberadaan pesan tersebut. Di dalam steganografi, pesan teks, gambar, maupun file bisa disembunyikan kedalam sebuah gambar, video, maupun audio[2].

Kedua cara pengamanan data tersebut memiliki beberapa metode yang bisa digunakan untuk mengoptimalkan fungsinya. Dalam kriptografi salah satunya terdapat algoritma asimetri RSA, kepanjangan RSA adalah gabungan inisial nama penemunya, yaitu Rivest, Shamir, Adleman. Dengan RSA siapapun dapat mengenkripsi dengan kunci publik, tetapi dekripsi hanya dapat dilakukan oleh pemilik

kunci pribadi[3]. Sedangkan dalam steganografi salah satunya menggunakan DWT (*Discrete Wavelet Transform*) dimana merupakan metode yang dapat membagi informasi dari suatu sinyal menjadi pendekatan sinyal dan detail sinyal[4].

Penelitian terhadap analisa sinyal menggunakan Transformasi Wavelet semakin bertambah, dikarenakan beberapa penelitian mendapatkan hasil bagus. Salah satu penelitian tentang analisa sinyal menggunakan Transformasi Wavelet yang dilakukan oleh Fera Putri Ayu Lestari dimana sinyal EEG (Elektroensefalografi) dikenai Transformasi Wavelet sehingga didapat sinyal alpha untuk mendeteksi tingkat relaksasi seseorang[5]. Ada juga penelitian tentang pengelompokan musik menurut genre dan emosi, dimana sebelum dikelompokkan semua musik dikenai Transformasi Wavelet[6].

Ada juga penelitian yang menggabungkan kriptografi dan steganografi sehingga keamanan pesan lebih terjamin dan pembajakan data rahasia akan semakin sulit karna harus menemukan pesan rahasia lalu perlu memecahkan pesan rahasia tersebut. Salah satunya penelitian tentang kombinasi kriptografi dan steganografi berbasis Transformasi Wavelet Diskrit Haar, di mana menggunakan citra sebagai media penampung dan pesan rahasia berupa text[1].

Berdasarkan latar belakang dan penelitian-penelitian terdahulu, keamanan informasi menjadi perhatian utama akhir-akhir ini, selain itu kriptografi dan steganografi dengan media penampung audio merupakan salah satu penyelesaian masalah tersebut, sedangkan untuk metode steganografi yang akan digunakan adalah DWT, karena dalam penelitian sebelumnya terbukti bahwa DWT dapat menghasilkan nilai PSNR lebih besar dari beberapa metode lain[4]. Maka dalam penelitian ini penulis mengajukan kombinasi kriptografi dan steganografi audio berbasis Transformasi Wavelet Diskrit di mana pesan teks sebagai pesan rahasia dan audio sebagai media penampung.

II. DASAR TEORI

A. Pesan

“Dalam proses komunikasi, pengertian pesan adalah sesuatu yang disampaikan pengirim kepada penerima. Pesan dapat disampaikan dengan cara tatap muka atau melalui media komunikasi. Isinya bisa berupa ilmu pengetahuan, hiburan, informasi, nasihat atau propaganda.” Pernyataan dari Hafied Cangara dalam bukunya *Pengantar Ilmu Komunikasi*.

Dapat disimpulkan bahwa pesan adalah suatu gagasan (ide) yang dituangkan dalam lambang-lambang oleh komunikator[7]. Lambang-lambang tersebut bisa berupa teks, gambar, atau suara. Dalam penelitian ini pesan yang digunakan adalah pesan teks sebagai pesan rahasia dan pesan suara atau audio sebagai wadah penampung.

B. Kriptografi

“Kriptografi adalah disiplin ilmu sekaligus seni untuk menjaga keamanan pesan.” Definisi kriptografi menurut Schneier pada buku karangannya yang berjudul “Applied Cryptography”. Untuk menjaga keamanan pesan tersebut, pesan akan dirubah menjadi *cipherteks* atau pesan yang disandikan. Tujuannya adalah agar pesan tidak dapat dibaca oleh pihak yang bukan dituju. Proses menyandikan pesan menjadi *cipherteks* disebut enkripsi, sedangkan proses mengembalikan *cipherteks* menjadi pesan asli disebut dekripsi[2].

C. Algoritma RSA

Algoritma RSA adalah salah satu algoritma kriptografi modern yang mempunyai tingkat kerumitan yang tinggi. Keamanan dari algoritma ini terletak pada sulitnya memfaktorkan bilangan besar menjadi factor - faktor prima. Jadi dapat disimpulkan bahwa jika tidak ada algoritma yang dengan cepat memfaktorkan bilangan bulat besar menjadi faktor - faktor primanya, maka selama itu pula keamanan algoritma RSA masih terjamin[2].

Terdapat 3 runtutan dalam algoritma RSA, yaitu pembangkitan / pembuatan kunci, enkripsi, dan dekripsi. Proses enkripsi dan dekripsi sendiri dapat dijalankan dengan persamaan (1) untuk enkripsi dan (2) untuk dekripsi.

$$E_e(m) = c = m^e \text{ mod } n \quad (1)$$

$$D_d(c) = m = c^d \text{ mod } n \quad (2)$$

D. Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia pada wadah penampung sehingga keberadaan pesan tidak terdeteksi oleh indera manusia. Dalam steganografi, membutuhkan dua properti, yaitu wadah penampung dan pesan rahasia yang akan disembunyikan. Dalam konteks digital, pesan rahasia dan wadah penampung dapat berupa citra, suara, teks, maupun video. Pesan rahasia akan disembunyikan di dalam wadah penampung dengan tidak mengubah stuktur asli dari wadah penampung[2]. Wadah penampung yang sudah dimasuki oleh pesan rahasia biasa disebut dengan stego file, misalkan wadah penampung berupa audio maka jika sudah dimasuki pesan rahasia disebut audio stego.

E. Kriteria Steganografi yang Baik

Penyembunyian pesan rahasia ke dalam wadah penampung akan mengubah kualitas wadah tersebut, sehingga perlu kriteria-kriteria yang harus diperhatikan dalam penyembunyian data. Kriteria tersebut adalah *Imperceptibility* (keberadaan pesan rahasia tidak dapat diketahui secara indrawi), *Fidelity* (kualitas dari wadah penampung tidak jauh berubah), *Payload* (pesan yang disembunyikan kalau bisa sebanyak mungkin), dan *Recovery* (data yang disembunyikan harus dapat diungkapkan kembali)[2].

Imperceptibility dapat diukur dengan memperdengarkan audio asli dan audio stego untuk diukur secara indrawi, *Fidelity* dapat diukur dengan menghitung MSE (*Mean Square Error*), atau PSNR (*Peak Signal to Noise Ratio*) pada audio asli dan audio stego, *Payload* dapat dipenuhi dengan menyisipkan pesam sebanyak atau semaksimal mungkin, Sedangkan *Recovery* dapat diukur dengan menghitung perbedaan pesan hasil ekstraksi dan pesan asli.

F. Transformasi Wavelet Diskrit

Transformasi Wavelet Diskrit (DWT) menggambarkan sebuah sinyal digital berdasarkan skala waktu yang didapatkan dengan menggunakan teknik *filtering* digital. Sebuah sinyal harus dilewatkan dalam dua *filter* DWT, yaitu *highpass filter* dan *lowpass filter* agar frekuensi dari sinyal dapat dianalisis. Analisis sinyal dilakukan terhadap hasil *filtering*. Dimana *highpass filter* digunakan untuk menganalisa frekuensi tinggi dan *lowpass filter* digunakan untuk menganalisa frekuensi rendah. Pembagian sinyal menjadi frekuensi tinggi dan frekuensi rendah melalui proses *filtering* tersebut disebut sebagai dekomposisi sinyal[5]. Berikut gambaran dekomposisi dua tingkat ditunjukkan pada Gambar 1.

G. Parameter Kuantitatif

Untuk melihat keberhasilan dari tujuan penelitian ini diperlukan alat ukur atau biasa disebut dengan parameter dalam pengujian hasil penelitian. Pada penelitian ini akan digunakan 2 parameter, yaitu parameter kuantitatif dan parameter kualitatif. Untuk parameter kuantitatif akan menggunakan *Mean Square Error* (MSE) pada audio asli dan audio stego.

MSE adalah parameter yang digunakan untuk menganalisis performansi sistem dengan meninjau hasil kualitas dari audio stego. Metode ini dilakukan dengan menghitung nilai rata-rata error antara audio asli dengan audio stego. Semakin besar nilai MSE, maka kualitas dari audio stego semakin buruk, sebaliknya semakin kecil nilai MSE maka kualitas dari audio stego semakin baik atau mendekati audio asli. Rumus untuk mencari MSE sebagai berikut[1], [6].

$$MSE = \frac{1}{m \times n} \sum_{i=1}^n \sum_{j=1}^m [f(i, j) - g(i, j)]^2 \quad (3)$$

Dengan:

- m = Panjang sinyal audio asli
- n = Panjang sinyal audio stego
- $f(i, j)$ = nilai ke (i, j) pada audio asli
- $g(i, j)$ = nilai ke (i, j) pada audio stego

H. Parameter Kualitatif

Parameter kualitatif pada penelitian ini adalah variable yang digunakan untuk mengukur seberapa besar perbedaan antara audio asli dan audio stego menurut pendengar (orang). Pendengar sendiri akan memberikan penilaian setelah mendengarkan langsung kedua audio yang disiapkan (audio asli dan audio stego). Berikut kriteria parameter penilaian seberapa besar perbedaan audio asli dan audio stego :

1. Tidak ada/sama persis (0% perbedaan), tidak ada perbedaan sama sekali antara kedua audio,

2. Mirip (1-25% perbedaan), sekilas terdengar sama, tetapi Ketika dicermati terdapat perbedaan tipis antara kedua audio,
3. Sedikit berbeda (26-50% perbedaan), ada beberapa perbedaan (noise) yang jelas tetapi hanya sedikit (kurang dari 5x),
4. Berbeda (51-75% perbedaan), banyak terdengar perbedaan (noise) pada kedua audio (6-10x),
5. Sangat berbeda (76-100% perbedaan), terlalu banyak perbedaan yang terdengar pada kedua audio (lebih dari 10x).

Semakin banyak respon dengan kriteria parameter nomor kecil (1 dan 2) maka dapat dikatakan audio stego yang dihasilkan baik secara kualitatif. Begitupun sebaliknya, semakin banyak respon dengan kriteria parameter nomor besar (4 dan 5) maka dapat dikatakan audio stego yang dihasilkan kurang baik.

III. ANALISIS DAN PEMBAHASAN

A. Analisis Sistem

Perancangan perangkat lunak dimulai dengan merancang algoritma untuk perangkat lunak dilanjut desainnya. Karena langkah pertama adalah pembangkitan kunci RSA. maka akan dibuat 2 *EditText* untuk bilangan prima, tombol pembangkit kunci, dan *EditText* nilai n , sedangkan *EditText* kunci public dan kunci pribadi berada disebelah tombol enkripsi dan dekripsi.

Langkah selanjutnya yang berhubungan dengan pengirim pesan termasuk enkripsi dan penyisipan pesan. Maka akan dibuat *EditText* pesan asli, tombol enkripsi yang disebelahnya terdapat kunci public, *EditText chipertext*, tombol penyisipan, dan 2 *EditText* untuk nama audio asli dan audio stego. Selanjutnya yang berhubungan dengan penerima pesan termasuk ekstraksi pesan dan dekripsi. Maka akan dibuat *EditText* nama audio stego, tombol ekstraksi, *EditText chipertext*, tombol dekripsi yang bersebelahan dengan *EditText* kunci pribadi, dan *EditText* pesan asli.

Untuk tambahannya dibuat 2 tombol tambahan dibawah yaitu tombol 'Bersih' untuk mengosongkan semua *EditText* yang ada dan tombol 'Keluar' untuk keluar dari perangkat lunak. Desain dan perancangan perangkat lunak pada penelitian ini dapat dilihat pada Gambar 2.

B. Data Uji Coba

Dalam Penelitian ini, data uji coba yang diperlukan adalah data audio dengan *file wav*. sebagai wadah penampung untuk menyembunyikan pesan, dan juga pesan teks. Data yang digunakan akan terdapat beberapa kondisi, berikut kondisi data yang digunakan dalam uji coba :

1. Ukuran audio
2. Isi dari audio
3. Panjang pesan teks

Di mana audio yang diuji disini ada 9 audio dengan 3 jenis isi audio dan dengan ukuran yang berbeda-beda, di mana 3 jenis isi audionya adalah suara seseorang berbicara / monolog, musik bergenre rock, dan suara alam (suara air mengalir di hutan dan burung). Sedangkan pesan teks yang diuji disini ada 23 macam pesan dengan panjang karakter yang berbeda.

C. Hasil Uji Coba

Pada Penelitian ini parameter yang digunakan ada dua, yaitu parameter kuantitatif dan parameter kualitatif. Maka uji coba yang dilakukan juga secara kuantitatif dan kualitatif.

Hasil Uji Coba Kuantitatif

Proses uji coba kuantitatif dijalankan dengan 9 sampel audio (dengan rincian 3 sampel monolog, 3 sampel musik, 3 sampel suara alam) dan akan dipasangkan dengan setiap 23 macam pesan teks yang panjangnya berbeda dan diuji coba menggunakan perangkat lunak yang dikembangkan dengan menggunakan bilangan prima (71) dan (157) untuk membangkitkan kunci RSA. Dan dari uji coba tersebut didapatkan MSE dari setiap uji coba. Hasil uji sampel audio monolog, hasil uji sampel audio musik, dan hasil uji sampel audio suara alam dapat dilihat pada Tabel 1, Tabel 2, dan Tabel 3.

Pada uji coba sampel audio suara alam dengan ukuran 2.92MB tidak maksimal dengan penyisipan 50107 karakter, karena dengan besar audio tersebut maksimal hanya dapat menyisipkan 47868 karakter dengan perangkat lunak yang digunakan.

Hasil Uji Coba Kualitatif

Proses uji coba kualitatif dilakukan dengan menyebarkan kuesioner penelitian ke beberapa orang secara acak, dimana dalam kuesioner berisi pertanyaan tentang identitas responden yaitu nama, Pendidikan terakhir atau yang sedang dijalani, dan nama sekolah atau kampus terakhir. Setelah pengisian identitas responden akan diberikan 2 audio untuk didengarkan, setelah mendengarkan kedua audio yang diberikan responden akan diberikan pertanyaan tentang seberapa besar perbedaan pada kedua audio yang baru didengarkan dan diberikan beberapa pilihan seperti yang sudah dijelaskan pada sub bab *parameter kualitatif*.

Kuesioner penelitian ini disebar sebanyak dua kali, pertama dengan audio asli sampel sebesar 3.14 MB dan stego audio yang disisipi pesan teks 33 karakter dan penyebaran kedua dengan audio asli sebesar 3.14 MB dan stego audio yang disisipi pesan teks 50107 karakter. Ringkasan hasil dari kuesioner dapat dilihat pada Gambar 3, Gambar 4, Gambar 5, dan Gambar 6.

D. Pembahasan

Hasil uji coba yang didapatkan dari uji coba kuantitatif menggunakan parameter MSE untuk mengukur kualitas audio stego yang dihasilkan. Dapat dilihat pada Tabel 1 sampai Tabel 3 bahwa nilai MSE akan semakin naik / bertambah jika semakin banyak jumlah karakter pesan yang diamankan dengan ukuran audio tetap.

Dari hasil uji coba kuantitatif yang dilakukan didapatkan nilai MSE terendah yaitu 0,0013. Kondisi ini didapatkan pada sampel audio musik bergenre rock dengan ukuran 3,46 MB dengan jumlah pesan 15 karakter pesan teks. Sedangkan nilai MSE tertinggi yaitu 0.6248 di mana kondisi ini didapatkan pada sampel audio suara alam dengan ukuran 7.7 MB dengan jumlah pesan 50107 karakter pesan teks.

Dari hasil uji coba kuantitatif didapati juga jumlah karakter error yang menunjukkan jumlah karakter yang berbeda dengan pesan aslinya, di mana apabila jumlah karakter errornya adalah 0 maka tingkat keberhasilan dalam

pengamanan dan kemiripan pesan mencapai 100% pada uji coba tersebut.

Dari hasil uji coba yang dilakukan, dilihat dari jumlah karakter errornya, didapatkan bahwa uji coba dengan audio monolog menghasilkan hasil terbaik dengan 65 uji coba menghasilkan 0 error, sedangkan dari uji coba dengan audio musik didapat 17 uji coba, dan audio suara alam didapat 8 uji coba dengan 0 error. Dari semua uji coba kuantitatif yang dilakukan tingkat keberhasilan dalam pengamanan dan kemiripan pesan > 97%.

Dari hasil uji coba kualitatif yang dijalankan dengan menyebarkan kuesioner penelitian, dapat dilihat pada gambar 3 sampai 6, bahwa pada penyebaran kuesioner pertama dengan sampel audio ukuran 3,14 MB disisipi 33 karakter pesan teks memiliki perbedaan lebih kecil dari pada penyebaran kuesioner kedua dengan sampel audio ukuran 3,14 MB disisipi 50107 karakter pesan teks. Dari 57 responden kuesioner pertama 57,9% menjawab tidak menemukan perbedaan, sedangkan dari 46 responden kuesioner kedua 34,8% menjawab tidak menemukan perbedaan. Sedangkan respon responden tentang seberapa besarkah perbedaan stego audio dengan audio asli dari 57 responden kuesioner pertama tidak ada yang menjawab berbeda dan sangat berbeda, semua menjawab tidak ada, mirip, atau sedikit berbeda. Sedangkan dari 46 responden kuesioner kedua 8,7% menjawab berbeda, dan sisanya menjawab tidak ada, mirip, atau sedikit berbeda.

Dari hasil uji coba kuantitatif dan kualitatif keduanya mendapati bahwa semakin banyak jumlah karakter pesan teks yang disisipkan maka stego audio yang dihasilkan akan semakin memiliki perbedaan dari audio aslinya.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

1. Telah berhasil menerapkan pengamanan pesan dengan kombinasi kriptografi RSA dan steganografi audio berbasis Transformasi Wavelet Diskrit, di mana proses pengamanan pesan dilakukan dengan membangkitkan kunci RSA dilanjutkan mengenkripsi pesan dengan kunci yang dibangkitkan dan hasil enkripsi diamankan dalam sinyal audio hasil Transformasi Wavelet yaitu sinyal frekuensi tinggi.
2. Kinerja perangkat lunak yang mengimplementasikan kombinasi kriptografi RSA dan steganografi audio berbasis Transformasi Wavelet Diskrit sebagai berikut:
 - a. Perangkat lunak berhasil menjalankan semua proses uji coba pengamanan pesan dengan cukup baik dengan

tingkat keberhasilan dalam pengamanan dan kemiripan pesan > 97%.

- b. Pada 69 kali uji coba yang dijalankan pada sampel audio monolog, 65 kali didapat kemiripan pesan 100%, sedangkan pada sampel audio musik hanya 17 kali, dan pada sampel audio suara alam hanya 8 kali. Dari hasil tersebut sangat disarankan penggunaan audio monolog pada pengamanan pesan.
- c. Pada uji coba kualitatif didapat bahwa Perangkat lunak bekerja baik dalam penyembunyian pesan, uji coba dengan sampel audio 3,14 MB disisipi 50107 karakter pesan, dari 46 responden hanya 4 responden (8,7%) yang berpendapat bahwa audio stego dan audio asli keduanya berbeda (memiliki perbedaan pada kisaran 51-75%).
- d. Dari hasil uji coba kuantitatif yang dilakukan didapatkan nilai MSE terendah yaitu 0,0057. Kondisi ini didapatkan pada sampel audio dengan ukuran 3,14 MB dengan jumlah pesan 15 karakter pesan teks.

B. Saran

1. Menggunakan metode penyisipan dengan mengubah pesan ke dalam biner dan dengan pesan teks yang sedikit, untuk mendapatkan hasil penyisipan pesan yang maksimal.
2. Melakukan penelitian tentang steganografi audio berbasis Wavelet dengan audio berisikan suara monolog agar dapat menyembunyikan pesan yang maksimal.

DAFTAR PUSTAKA

- [1] U. M. Nuchan, "Kombinasi Kriptografi dan Steganografi Berbasis Transformasi Wavelet Diskrit Untuk Pengamanan Data Departemen," Institut Teknologi Sepuluh Nopember, 2020.
- [2] R. Munir, *Kriptografi*. Bandung, Indonesia: Informatika Bandung, 2019.
- [3] B. J. Santhosh Kumar, R. V. K. Roshni, and A. Nair, "Comparative study on AES and RSA algorithm for medical images," in *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017*, 2018, vol. 2018-January, pp. 501–504. doi: 10.1109/ICCSP.2017.8286408.
- [4] P. Batarius and M. Maslim, "Perbandingan metode dalam teknik steganografi," in *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012 (Semantik 2012)*, 2012, p. INFRM 303-INFRM 306.
- [5] F. P. A. Lestari, "Deteksi dan Analisa Gelombang Alpha Pada Sinyal EEG Terhadap Rangsang Suara Musik Menggunakan Transformasi Wavelet," Institut Teknologi Sepuluh Nopember, 2018.
- [6] N. Anastasya, "Pengelompokan Musik Berdasarkan Emosi Menggunakan Metode Transformasi Haar Wavelet," Universitas Brawijaya, Malang, Indonesia, 2020.
- [7] D. Nurhidayah, "Representasi Makna Pesan Sosial Dalam Film Bulan Terbelah di Langit Amerika," Universitas Tadulako, 2017.