Jurnal Elektronik Ilmu Komputer Udayana
Volume 11, No 3. February 2023

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Pengamanan Audio Menggunakan Metode RSA dan Steganografi *Spread spectrum* Berbasis Android

I Ketut Kusuma Merdana[a1], I Komang Ari Mogi[a2], I Gede Arta Wibawa[a3], Agus Muliantara[a4], I Ketut Gede Suhartana[a5], I Putu Gde Hendra Suputra[a6]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Badung, Bali, Indonesia
[1]ketutkusuma0910@gmail.com
[2]arimogi@unud.ac.id
[3]gede.arta@unud.ac.id
[4]muliantara@unud.ac.id
[5]ikg.suhartana@unud.ac.id
[6]hendra.suputra@unud.ac.id

Abstract

Audio is a multimedia element whose function is the same as text, video or images, but for the recipient it can only be heard through human hearing, which is 20 to 20,000 Hz. Audio can also be in the form of a song that is often listened to and has a high selling power, therefore audio is also often traded or rented. In this study, the application was developed using the Spread spectrum method, Rivest Shamir Adleman and assisted also by the Standard Advanced Encryption method to secure audio to protect against data theft by unauthorized parties. This application is based on Android which can be further developed to run more flexibly and make it easier for users to use it. From the test results the application can process input and output as expected. For testing the results of image quality, which is an audio password insertion container, in this test, the PSNR value with an average of 56,851 is obtained, and the MSE value with an average value of 0.124 which is a good result for testing image quality.

Keywords: *Steganography, RSA, Spread spectrum, PSNR*

1. Pendahuluan

Saat ini, meningkatnya penggunaan teknologi komputasi dan telekomunikasi mengubah pandangan masyarakat tentang komunikasi. Kemajuannya di bidang jaringan komunikasi seluler dengan konsep sistem terbuka yang memudahkan seseorang untuk membobol jaringan adalah data yang tidak aman karena dapat digunakan oleh pihak yang tidak bertanggung jawab untuk mengambil data penting yang berujung pada proses pengiriman informasi [1]. Melindungi informasi sangat penting sehingga ada dua cara untuk melindunginya: enkripsi dan stenografi. Enkripsi pada umumnya adalah ilmu penyandian data, menggunakan kunci enkripsi untuk mengacak data [2]. Stegnografi adalah ilmu menulis pesan tersembunyi atau tersembunyi sehingga hanya pengirim dan penerima yang dapat mengenalinya [3]. Kriptografi memiliki banyak algoritma untuk melindungi informasi. Salah satunya adalah algoritma RSA yang merupakan algoritma enkripsi asimetris. Keuntungan utama dari algoritma RSA adalah menggabungkan teknik keamanan informasi, atau stenografi, untuk meningkatkan keamanan. Stegnografi *spread spectrum* membutuhkan proses penyisipan melalui proses propagasi dan modulasi, yang mengacak pesan propagasi *spread spectrum* di seluruh media penampung. Untuk pesan dan informasi yang dikirim secara acak.

Pada penelitian sebelumnya [2] tentang kombinasi enkripsi RSA dan stenografi *spread spectrum* untuk melindungi data teks, penelitian ini menggunakan enkripsi RSA dan stenografi *spread spectrum* sebagai file teks pada sebuah gambar, saya berhasil menggabungkannya dengan. Penelitian selanjutnya tentang implementasi stenografi SMS pada audio menggunakan metode *spread spectrum* [4] menguji PSNR dan MSE penelitian ini dan membandingkan file asli dengan file hasil stagnografi.

Pengujian 3x menghasilkan rata-rata MSE sebesar 2.2692E-06 dengan nilai PSNR rata-rata sebesar 111.9842 dB. Jumlah karakter atau ukuran file yang disisipkan berpengaruh signifikan terhadap nilai MSE dan PSNR. Berdasarkan referensi di atas, sebuah penelitian yang berjudul "Implementasi *Spread spectrum* RSA Algorithms and Stegnography for Installing Text Messages in Speech" telah diusulkan. Penelitian ini mengimplementasikan transaksi atau aplikasi keamanan audio yang dapat digunakan untuk bertransaksi. Data audio dalam aplikasi ini menggunakan audio terenkripsi dan audio berformat .wav terenkripsi RSA. Format WAV dipilih karena dapat menyimpan file audio terkompresi dan tidak terkompresi. Pembeli yang memutar audio harus menggunakan aplikasi keamanan audio ini untuk memutar audio setelah proses dekripsi dan ekstraksi.

2. Metode Penelitian

2.1 *Riverst Shamir Adleman*

Rivest Shamir Adleman (RSA) adalah algoritma enkripsi asimetris yang menggunakan dua angka acak sebagai kunci untuk menghasilkan dua kunci untuk enkripsi pesan. Proses dekripsi plaintext (P) dan ciphertext (C) dari algoritma RSA menggunakan persamaan berikut [5]:

$$C = P^e \ mod \ n \quad (1)$$

$$P = C^d \ mod \ n \quad (2)$$

Proses pencarian kunci publik (e,n) dan kunci privat (d,n) tidak gratis. Untuk menentukan kunci publik dan kunci privat: (Rudiyanto,.

1. Pilih 2 buah bilangan prima p dan q yang mana nilainya harus berbeda.
2. Menghitung n = p*q
3. Mencari nilai dari persamaan m = (p-1)*(q-1)
4. Menda[atkan nilai e, yang mana berasal dari nilai e yang merupakan bilangan relative prima dari m
5. Mendapatkan nilai d, yang berasal dari persamaan e.d mod m = 1.

Untuk mendapatkan nilai d yang memenuhi persamaan pada langkah 5 digunakan algoritma extended Euclidean pada langkah selanjutnya.

1. Mengubah persamaan e.d dalam mode m = 1 menjadi (m.x) + (e.y) = 1 yang merupakan persamaan Euclidean
2. Mentukan nilai a dan b yang memenuhi persmaan m = (a.e) + b
3. Menyimpan persamaan yang ditemukan dan mengganti nilai m dan nilai e dengan nilai e dan nilai b
4. Mengulangi hingga nilai b menjadi 1 untuk langkah 2 dan 3
5. Mengubah menjadi b = m – (a.3) untuk semua persamaan yang tersimpan
6. Pada setiap persamaan yang nilainya b = e, ubah nilai e
7. Mengubah agar menjadi mirip dengan persamaan yang dibuat pada langkah 1 untuk setiap persamaan
8. Pada setiap persamaan yang telah diubah tersebut, variable y merupakan kunci privat yang dapat digunakan untuk proses dekripsi. Kunci merupakan bilangan positif karenanya jika y bernilai negatif maka kunci dekripsi akan menggunakan persamaan m – y.

2.2 *Spread spectrum*

Metode *spread spectrum* adalah teknologi transmisi yang menggunakan kode semu yang tidak bergantung pada data informasi sebagai modulator bentuk gelombang dan menyebarkan energi sinyal pada jangkauan yang lebih luas dari jalur komunikasi asli (bandwidth). Melalui penerima, sinyal dikumpulkan kembali dalam replika *encoder pseudo-noise* yang disinkronkan. Metode *spread spectrum* memerlukan cakupan sebagai *noise* atau sebagai upaya untuk menambahkan pseudo-noise ke cakupan. Penyisipan menggunakan metode ini memiliki tiga proses: difusi pesan, modulasi, dan penyisipan amplop, dan ekstraksi memiliki tiga proses: akuisisi pesan, demodulasi, dan *despreading* [6].

Penyisipan *Spread Spectrum* memiliki langkah-langkah utama sebagai berikut.

1. Gunakan kata kunci untuk menghasilkan kebisingan pseudo-acak.
2. Proses penyebaran untuk setiap pesan yang akan disisipkan.
3. Modulasi antar pesan hasil penyebaran dengan pseudo-acak yang telah menghasilkan kebisingan.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

4. Menyisipkan kebisingan ke dalam setiap LSB pada penampung yang mana pesan rahasia akan disisipkan.

Untuk langkah ekstrasi yang merupakan langkah untuk mengambil data yang disisipkan terdiri dari langkah-langkah sebagai berikut [7].

1. Mengambil data pada setiap LSB data gambar.
2. Hasilkan kebisingan pseudo-acak dengan menggunakan kata kunci yang sama seperti proses penyisipan.
3. Melakukan proses de-modulasi antara bit pesan yang telah diekstrak dengan deret bilangan pseudo-acak.
4. Proses penyebaran balik yang bertujuan untuk mendapatkan pesan rahasia yang sudah disisipkan.

2.3 *Advanced Encryption Standar (AES)*

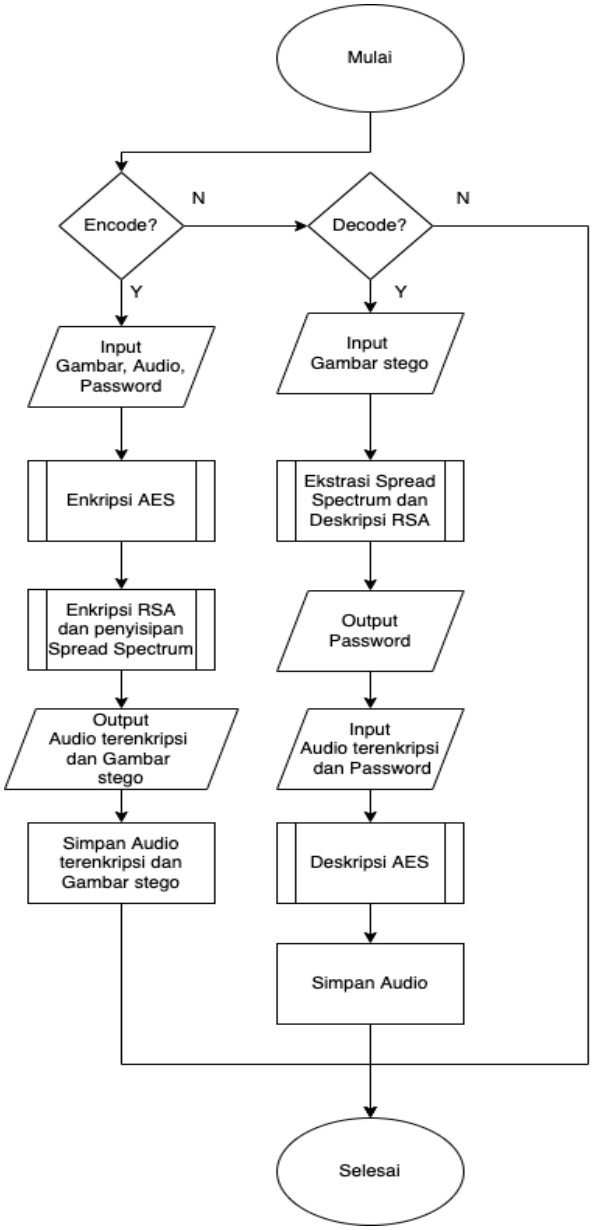
Algoritma AES (*Advanced Encryption Standard)* merupakan algoritma enkripsi yang dapat digunakan untuk melindungi data atau informasi. Algortima AES adalah sebuah *block ciphertext* simetris yang dapat mengenkripsi (encrypt) dan mendekripsi (decrypt) informasi. Kunci enkripsi AES terdiri dari kunci panjang 128-bit, 192-bit atau 256-bit. Perbedaan panjang kunci mempengaruhi jumlah putaran yang diimplementasikan oleh algoritma AES. Pada daarnya, operasi AES dilakukan pada *array byte* dua dimensi yang disebut status. Ukuran bagian adalah NRowXNCol, pada awal enkripsi, data input, disalin ke *array* keadaan dalam format in0, in2, in3, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15. Status ini akan dilakukan kemudian oleh operasi enkripsi/dekripsi. Kemudian *output* dilangkahkan ke dalam *array output*[8].

2.4 Analisis Masalah

Dalam penelitian ini mencoba mengembangkan aplikasi yang dapat mengenkripsi dan mendekripsi audio menggunakan metode RSA, tetapi setelah membaca dan menjalankan eksperimen itu sendiri, peneliti tidak dapat melakukannya. Hal ini juga diperkuat dengan penelitian sebelumnya yang gagal mendekripsikan audio yang terenkripsi RSA. Masalah utama dengan dekripsi adalah bahwa RSA tidak cocok untuk mengenkripsi data dalam jumlah besar. Semakin besar data yang akan dienkripsi, semakin panjang kunci yang dihasilkan oleh RSA harus mengikuti panjang data. Untuk itu peneliti menggunakan metode enkripsi yang lebih sederhana yaitu metode AES. Ini unggul dalam mengenkripsi dan mendekripsi data dalam jumlah besar. Penggunaan metode atau algoritma akan dilanjutkan pada penelitian ini dengan menggabungkan *spread spectrum steganography*. Oleh karena itu, dienkripsi menggunakan metode RSA dan dimasukkan ke dalam wadah sebelum Anda memasukkan kunci atau kata sandi untuk membuka audio.

2.5 Desain Perancangan Sistem

Desain perancangan sistem berisikan langkah pada rancangan pembuatan perangkat lunak, yang bertujuan untuk mempermudah untuk pengembangan sistem aplikasi yang dibangun. Sesuai dengan Gambar 1, sistem memiliki dua fungsi utama, enkoding dan dekoding, dimana fungsi enkoding memasukkan gambar, audio dan password. Gambar-gambar ini dienkripsi menggunakan metode AES audio dan enkripsi RSA, dan ketika dimasukkan dengan *Spread spectrum*, audio dihasilkan. Gambar terenkripsi dan gambar yang disisipkan. Fungsi dekoding pertama memasukkan gambar yang disisipkan, pertama-tama mengekstraknya dengan *Spread spectrum*, dan kemudian mendekodekannya dengan RSA. Setelah mendapatkan kata sandi, itu akan dimasukkan dengan audio terenkripsi yang didekripsi menggunakan AES.



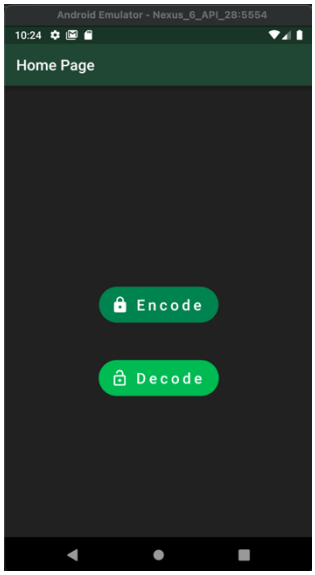
Gambar 1. Alur umum sistem

3. Hasil dan Pembahasan

3.1 Tampilan Antarmuka Sistem Pengamanan Audio

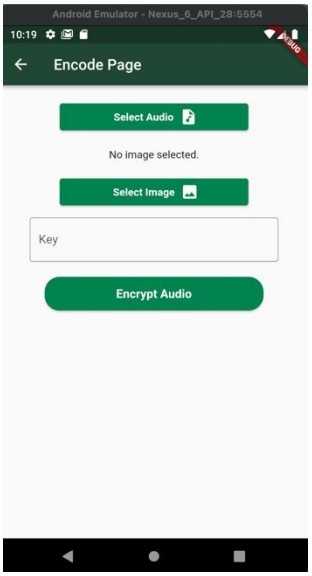
Tampilan antarmuka sistem terdapat tiga halaman yang difokuskan, yaitu halaman utama, halaman enkode, dan halaman dekode. Pada saat aplikasi dibuka maka akan ditujukan kepada halaman utama yang mana berisikan dua fitur seperti yang ditujukan pada Gambar 2.

p-ISSN: 2301-5373
e-ISSN: 2654-5101



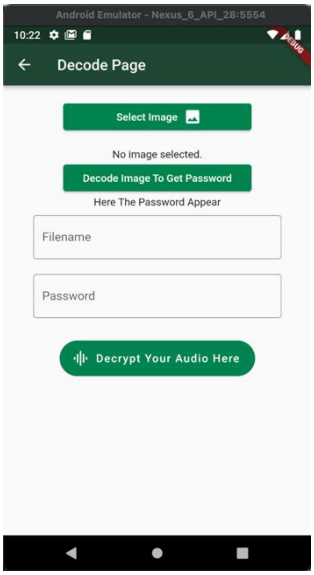
Gambar 2. Halaman utama

Gambar 2 menunjukan halaman utama yang mana merupakan halaman pertama yang ditampilkan kepada pengguna yang di dalamnya terdapat fitur encode dan decode. Fitur-fitur tersebut merupakan fitur utama yang ada pada aplikasi. Oleh karenanya halaman utama sangat penting dan harus ada.



Gambar 3. Halaman Enkode

Gambar 3 menunjukkan halaman Enkode yang digunakan untuk enkoding. Pertama, ada tombol *"Select Audio"* yang digunakan pengguna untuk memilih audio. Dengan fungsi pemilihan audio ini, *. Hanya file audio format wav yang dapat dibaca. Di bawahnya terdapat tombol *Select Image*, yang digunakan untuk memilih gambar yang akan digunakan sebagai pengganti password terenkripsi. Lalu ada area entri teks untuk memasukkan kata sandi. Ini harus berisi 8 karakter.



Gambar 4. Halaman Dekode

Selanjutnya halaman decode yang merupakan halaman dimana fungsi dekripsi dan ekstrasi berlangsung pada sistem. Tampilan halaman dekode bisa dilihat pada Gambar 4 yang mana dilihat bahwa pada halaman dekode akan menerima masukan berupa gambar yang telah disisipkan yang akan mengambil kunci untuk membuka audio. Setelah mendapatkan kunci maka kunci akan digunakan untuk membuka audio terenkripsi yang sebelumnya sudah dipilih oleh pengguna.

3.2 Pengujian Kualitas Gambar Tersisipkan

Pada penelitian ini, untuk menguji apakah gambar yang sudah disisipkan memiliki kualitas yang bagus agar tidak dapat diketahui oleh pengguna asing bahwa gambar tersebut sudah memiliki data rahasia. Maka dilakukan pengujian PSNR dan MSE yang merupakan pengujian terhadap kualitas gambar yang disisipkan kunci audio. Hasil pengujian tersebut dapat dilihat pada Tabel 1.

Tabel 1. Hasil Pengujian Kualitas Gambar Dengan PSNR dan MSE

No.	Berkas Gambar	Ukuran Gambar (Steganografi)	MSE	PSNR
1.	Gambar 1	11,6 MB	0.11664017220786	57.462322087 dB
2.	Gambar 2	7,2 MB	0.15389515817901	56.258554045 dB
3.	Gambar 3	5,11 MB	0.0880213131703	58.6849251745 dB
4.	Gambar 4	3,5 MB	0.12594370659722	57.1290389017 dB
5.	Gambar 5	9,4 MB	0.13714898003472	56.758877787 dB
6.	Gambar 6	4,9 MB	0.17089168495418	55.8035942902 dB
7.	Gambar 7	6,7 MB	0.06488634478788	60 dB
8.	Gambar 8	9,6 MB	0.16076400945216	56.068915319 dB

Pada Tabel 1 dapat dibandingkan dan diuji dengan MSE dan PSNR untuk menentukan kualitas gambar yang baik. Semakin kecil nilai MSE, semakin baik kualitas gambarnya. Untuk PSNR, gambar berkualitas tinggi adalah gambar dengan PSNR besar. Pada pengujian PSNR dan MSE rata-rata PSNR untuk pengujian ini adalah 56,851 dB dan nilai MSE rata-rata 0,124 dB. Pengujian ini dilakukan untuk menguji bagaimana kualitas gambar setelah proses *embedding* atau penyisipan dibandingkan dengan rata-rata skor PSNR 56,851 dan rata-rata skor MSE 0,124. Hal ini menunjukkan bahwa proses steganografi menggunakan *Spread spectrum* dapat berhasil menyisipkan data ke dalam citra.

3.3 Pengujian Pengubahan Gambar

Pengujian ini menjalankan pengujian untuk menganalisis bagaimana sebuah gambar dengan tombol atau pesan mengubah atributnya berupa ukuran gambar, warna gambar, panjang dan lebar gambar.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Hal ini dilakukan untuk menguji hasil ekstraksi apakah hasilnya cocok dengan kunci yang dimasukkan sebelumnya setelah atribut diubah. Setelah dilakukan pengujian dan mendapatkan hasil yang ditunjukkan pada Tabel 2, dapat disimpulkan bahwa citra steganografi dengan atribut yang dimodifikasi tidak dapat diekstraksi.

Tabel 2. Hasil pengujian Pengubah Gambar

No	Pengujian	Hasil
1.	Ubah warna gambar	Tidak berhasil ekstrasi
2.	Ubah ukuran gambar	Tidak berhasil ekstrasi
3.	Ubah panjang dan lebar gambar	Tidak berhasil ekstrasi

4. Kesimpulan

Aplikasi yang dibangun menggunakan penyebaran spektrum dan enkripsi dengan RSA berhasil menyisipkan dan mengekstraksi teks cipher ke dalam gambar yang disiapkan dengan baik. Kualitas gambar yang telah disisipkan menerima rata-rata 56.185 dB untuk nilai PNSR dan untuk nilai MSE rata-rata dengan nilai 0,113431 yang dapat disimpulkan bahwa kualitas gambar sulit untuk dibedakan dengan yang aslinya. Namun sistem ini memiliki kelemahan berupa panjang minimum wadah format gambar yang digunakan untuk penyisipan harus sepanjang 1504 piksel, ini dapat mempersulit sistem untuk pengambilan data gambar.

Daftar Pustaka

[1] Yusfrizal, “RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID Yusfrizal 1),” *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 2, 2019.

[2] Rajamah Limbong, “KOMBINASI KRIPTOGRAFI RSA DAN STEGANOGRAFI *SPREAD SPECTRUM*,” vol. 7, no. 1, pp. 97–100, 2019.

[3] A. Septayuda, I. Bambang Hidayat, and H. Hudan Nuha, “ANALISIS STEGANOGRAFI CITRA DIGITAL MENGGUNAKAN METODE *SPREAD SPECTRUM* BERBASISANDROID ANALYSIS OF DIGITAL IMAGE STEGANOGRAPHY USING *SPREAD SPECTRUM* METHOD BASED ON ANDROID,” Bandung, Dec. 2014.

[4] M. M. Assyahid, R. Rihartanto, and D. S. B. Utomo, “Implementasi Steganografi Pesan Text ke Dalam Audio Dengan Metode *Spread spectrum*,” *Juristek*, vol. 3, no. 2, pp. 27–34, 2018.

[5] A. Hidayat and A. Faizin, “PERBANDINGAN KRIPTOGRAFI MENGGUNAKAN ALGORITMA DATA ENCRYPTION STANDART (DES) DAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK KEAMANAN DATA,” *JASIEK*, vol. 1, no. 2, 2019, doi: 10.12928/JASIEK.v13i2.xxxx.

[6] B. Oktavianto, T. W. Purboyo, and R. E. Saputra, “A Proposed Method for Secure Steganography on PNG Image Using *Spread spectrum* Method and Modified Encryption,” 2017. [Online]. Available: http://www.ripublication.com

[7] M. Iqbal, T. Zebua, and R. D. Sianturi, “Implementasi Algoritma Spritz Dan *Spread spectrum* Untuk Menyembuyikan Pesan Enkripsi Kedalam File Audio Mp3,” *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 3, no. 1, pp. 486–492, 2019, doi: 10.30865/komik.v3i1.1631.

[8] A. Fauzi, “Analisa Kombinasi Pesan Teks Ke Dalam File Audio Memanfaatkan Algoritma Data Encryption Standard Dan Metode End of File,” *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 1, pp. 1–8, 2019.

This page is intentionally left blank.