# Simulasi Dan Analisis Performansi Teknik Rivest Shamir Adleman (RSA) Pada Steganografi *Least Significant* Bit (LSB)

1st Amanda Nabila Alya
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
amandanabilaalya@student.telkomuniversity.ac.id

2nd Ida Wahidah Hamzah
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
wahidah@telkomuniversity.ac.id

3rd M. Faris Ruriawan
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
Muhammad.faris.rusiawan@telkomuniversity.ac.id

**Abstrak--- Proses transmisi data sangat penting dan bersifat privasi, dalam perjalanan menuju penerima untuk dijaga dan dilindungi kerahasiaan data informasinya dengan aman agar data tidak bocor kepada pihak ketiga yang tidak bertanggung jawab Sistem keamanan yang kompatibel sangat diperlukan agar data terlindungi dari ancaman-ancaman serangan. Dalam penelitian Tugas Akhir ini, penulis memilih menganalisis salah-satu metode teknik keamanan data (security) kriptografi sebagai proses enkripsi data yang nantinya dilakukan penyisipan data melalu teknik steganografi dengan metode least significant bit (LSB) yang diterapkan pada sampel data citra medis. Berdasarkan hasil pengujian, waktu komputasi lebih banyak dipengaruhi oleh ukuran citra, dimana semakin besar ukuran citra, semakin besar pula waktu komputasi yang dibutuhkan dalam pengujian. Panjang karakter pesan dan besarnya angka prima yang dipilih tidak terlalu berpengaruh terhadap lamanya waktu komputasi. Waktu komputasi tercepat pada proses enkripsi-embedding yang dibutuhkan adalah 5.533 detik, sedangkan waktu komputasi terlama yang dibutuhkan adalah 95.12 detik. Pada proses ekstraksi-dekripsi yang paling cepat sebesar 3.49 detik dengan waktu komputasi terlama membutuhkan waktu sebesar 56.2167 detik.**

***Kata kunci: Kriptografi, Steganografi, RSA, Rivest Shamir Adleman, LSB, Least Significant Bit.***

## I. PENDAHULUAN

Teknologi yang sudah berkembang pesat sangat dibutuhkan dari berbagai aspek kehidupan. Proses pengiriman dan penerimaan data semakin familiar di kalangan masyarakat atau biasa disebut sebagai proses transmisi data. Proses transmisi data ini terjadi di berbagai kalangan profesi masyarakat. Proses transmisi data sangat penting dan bersifat privasi, dalam perjalanan menuju penerima untuk dijaga dan dilindungi kerahasiaan data informasinya dengan aman agar data tidak bocor kepada pihak ketiga yang tidak bertanggung jawab.

Sistem keamanan yang kompatibel sangat diperlukan agar data terlindungi dari ancaman-ancaman serangan. Dalam penelitian Tugas Akhir ini, penulis memilih menganalisis salah-satu metode teknik keamanan data (security) kriptografi sebagai proses enkripsi data yang nantinya dilakukan penyisipan data melalu teknik steganografi dengan metode least significant bit (LSB) yang diterapkan pada sampel data citra medis. Teknik kriptografi secara garis besar berguna untuk menjaga kerahasiaan data informasi yang dikirimkan. Sedangkan, teknik steganografi secara garis besar adalah suatu teknik untuk menyembunyikan suatu pesan rahasia ke dalam suatu media lain, sehingga antara citra asli dan citra stego tidak terlihat jauh perbedaannya secara kasat mata. Penulis dalam hal ini menganalisis performansi metode RSA (Rivest Shamir Adleman) sebagai teknik kriptografi enkripsi. Hasil simulasi pada metode ini akan dilihat bagaimana analisis dari metode yang telah dilakukan penyisipan oleh steganografi LSB. Berdasarkan penelitian terkait yang menggabungkan antara kriptosistem RSA dan steganografi least significant bit menghasilkan mutu data citra digital yang telah disisip pesan tidak mengalami perubahan berarti dan data yang berada dalam citra digital dapat diekstrasi kembali [15]. Dari uraian di atas, maka pada penelitian tugas akhir ini dilakukan penelitian dengan metode kriptograsi enkripsi RSA yang dikombinasikan dengan teknik penyisipan dengan algoritma steganografi LSB.

## II. KAJIAN TEORI

### A. Kriptografi

Kriptografi (cryptography) merupakan ilmu dan seni untuk melindungi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan [1]. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa, sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut. Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

### B. *Rivest Shamir Adleman* (RSA)

*Rivest Shamir Adleman* (RSA) merupakan salah satu metode enkripsi yang paling banyak digunakan dan termasuk algoritma pada enkripsi kunci publik. RSA

dikembangkan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman di MIT dan pertama kali diterbitkan pada tahun 1978 . Skema *Rivest-Shamir-Adleman* (RSA) sejak saat itu menjadi yang tertinggi sebagai pendekatan tujuan umum yang paling banyak diterima dan diterapkan untuk enkripsi kunci publik [5]. RSA hanya menggunakan satu operasi aritmatika (eksponensial modular) yang membuatnya secara konseptual menjadi skema asimetris sederhana.

- Enkripsi dan Dekripsi

Operasi RSA dilakukan pada ring bilangan bulat $Z_n$ (yaitu, aritmatika modulo n) di mana $n = p * q$, dengan $p, q$ adalah bilangan prima besar. Enkripsi dan dekripsi secara sederhana adala eksponensial di atas ring [6].
Diberikan kunci publik $(n,e) = k_{pub}$ dan kunci privat $d = k_{pr}$ kita tulis

$y = e_{kpub}(x) \equiv x^e \bmod n$

$x = d_{kpr}(y) \equiv y^d \bmod n$

dimana $x, y \varepsilon Z_n$, dengan $e_{kpub}$ () enkripsi dan $d_{kpr}$ () operasi dekripsi. (2.1)

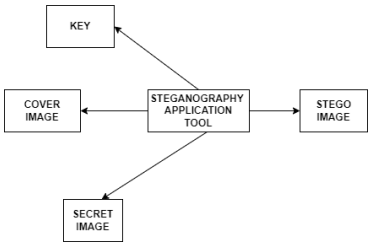
1.Pembangkitan Kunci

Sebagai algoritma asimetris kriptografi, RSA membutuhkan dua kunci yang berbeda. Bilangan prima yang besar dipilih sebagai syarat nilai kunci yang akan digunakan, dengan alasan pemfaktoran sebuah bilangan hasil perkalian dari dua bilangan prima yang besar menjadi dua bilangan prima yang sesuai akan sangat sulit sehingga keamanan dari RSA dapat terjamin. Seperti semua skema asimetris, RSA memiliki fase set-up di mana kunci privat dan publik dihitung.
Keluaran: kunci publik $(n,e) = k_{pub}$ dan kunci privat $d = k_{pr}$

1. Pilih dua bilangan prima besar $p, q$
2. Hitung $n = p * q$
3. Hitung $\Phi(n) = (p-1) * (q-1)$
4. Pilih eksponen publik $e \varepsilon \{1, 2, ..., \Phi(n)-1\}$ sehingga $gcd(e, \Phi(n)) = 1$
5. Hitung kunci privat sehingga $d * e \equiv 1 \bmod \Phi(n)$ Kembali $(n,e) = k_{pub}$ dan kunci privat $d = k$

C. Steganografi

Steganografi adalah seni menyembunyikan informasi dalam cara yang mencegah pendeteksian terhadap pesan tersembunyi. Steganografi, berasal dari bahasa Yunani, secara harfiah berarti “tulisan tertutup.” Ini mencakup sejumlah besar metode komunikasi rahasia yang menyembunyikan keberadaan pesan itu sendiri. Metode ini termasuk tinta tak terlihat (*invisible inks*), *microdots*, pengaturan karakter, tanda tangan digital, saluran rahasia, dan komunikasi spektrum tersebar (*spread spectrum communications*). Berikut adalah blok diagram sederhana dari steganografi [7] :




GAMBAR 2.1
BLOK DIAGRAM STEGANOGRAFI [7]

Steganografi dan kriptografi adalah algoritma yang saling berkaitan. Kriptografi mengacak pesan sehingga itu tidak dapat dipahami. Steganografi menyembunyikan pesan sehingga tidak dapat dilihat. Sebuah pesan dalam ciphertext, misalnya, dapat menimbulkan kecurigaan pada pihak penerima sementara sebuah pesan "tidak terlihat" dibuat dengan metode steganografi yang tidak akan menimbulkan kecurigaan [8].

D. *Least Significant Bit* (LSB)

*Least Significant Bi*t (LSB) adalah teknik yang digunakan untuk menyematkan pesan rahasia ke dalam sampul gambar. Piksel citra dapat diubah menjadi bentuk biner dan pesan rahasia [9]. Dalam pengimplementasiannya, dibutuhkan beberapa tahapan kerja yaitu [10] :

1. Proses Penyandian dan *Embedding* Citra Pesan

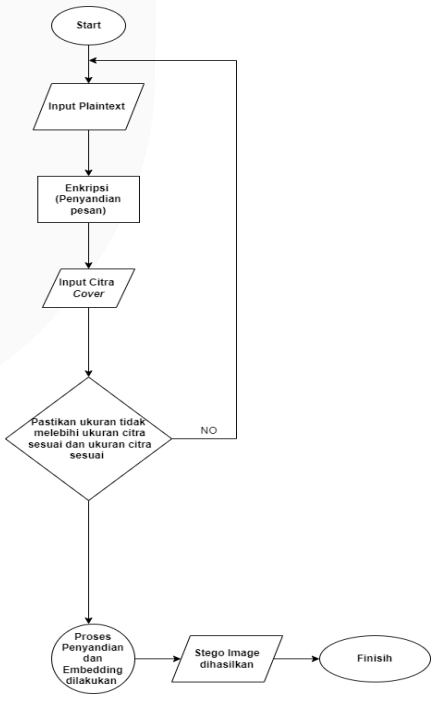
   Langkah-langkah penyembunyian citra pesan adalah sebagai berikut:

   • Citra pesan yang berukuran x × y piksel dienkripsi menggunakan metode RSA dengan kunci enkripsi yang sudah diperoleh pada tahap pembangkitan kunci RSA.

   • Dalam proses enkripsi dengan memperbanyak jumlah bit menjadi 16-bit yang membuat ukuran citra pesan berubah menjadi 2x × y piksel. 3. Dalam proses enkripsi RSA, nilai maksimal tiap pikselnya berukuran 255. Jika nilai di dalam 11 sebuah piksel melebihi 255 nilai, maka sisa tersebut akan dimasukkan ke dalam bit selanjutnya

   • Citra hasil enkripsi yang berukuran 2x × y piksel disisipkan ke dalam citra cover menggunakan metode LSB. Dengan menyisipkan bit citra pesan pada bit terakhir citra cover.

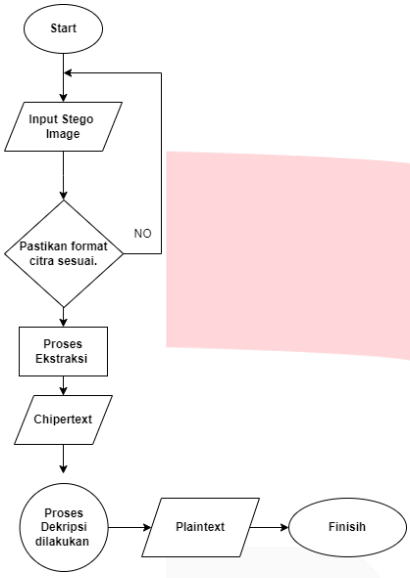
   • Hasil akhir nantinya berupa citra embedding yang sudah berisikan pesan rahasia tersandi.




GAMBAR 2.2
DIAGRAM ALUR PENYANDIAN DAN *EMBEDDING* CITRA PESAN

2. Proses Ekstraksi dan Dekripsi Citra Pesan

Proses Ekstraksi dan Dekripsi Citra Pesan Pada tahap ini bertujuan untuk mengambil citra pesan tersandi yang disembunyikan di dalam sebuah citra cover. Proses ini dilakukan untuk pengembaliak pesan ke bentuk awal, stego image akan diekstrak kembali untuk mendapatkan chipertext yang tersembunyi yang nantinya akan didekripsi untuk mendapatkan pesan rahasia kembali. Berikut adalah diagram alur proses ekstraksi dan dekripsi citra pesan:




GAMBAR 2.3
DIAGRAM ALUR EKSTRAKSI DAN DEKRIPSI CITRA PESAN

D. *Mean Absolute Error* (MAE)

*Mean Absolute Error* (MAE) adalah rata-rata dari semua error mutlak yang dihasilkan, yang dirumuskan sebagai berikut [11] :

$$\mathrm{MAE} = \frac{1}{n}\sum_{i=1}^{n} |\boldsymbol{x}_i - \boldsymbol{x}|$$

(2.2)

Dimana: • n = jumlah error,

• Σ = simbol penjumlahan

(yang berarti “jumlahkan semuanya”),

• |xi – x| = the absolute errors.

Langkah-langkah mudah untuk penggunaan rumus MAE adalah :

1.Temukan semua kesalahan absolut Anda, xi – x;

2.Tambahkan semuanya;

3.Bagi dengan jumlah kesalahan. Misalnya, jika memiliki 10 pengukuran, bagi dengan 10

E. *Avalanche Effect* (AE)

Dalam kriptografi, *avalanche effect* mengacu pada property yang diinginkan dari algoritma kriptografi. Biasanya dalam bentuk blok *chipper* dan fungsi *hash* kriptografis. Efek avalanche terbukti jika, ketika input sedikit diubah (misalnya, membalik satu bit) *output* berubah secara signifikan (misalnya, setengah dari bit keluaran membalik). Dalam kasus blok *chiper* berkualitas tinggi, perubahan kecil pada kunci atau *plaintext* harus menyebabkan perubahan drastis dalam teks sandi [12].

## III. METODE

A. Desain Sistem

Pada penelitian tugas akhir ini peneliti menggunakan perangkat keras (hardware) dan perangkat lunak (software) yang berfungsi untuk mendukung jalannya penelitian. Perangkat keras yang digunakan dalam penelitian ini meliputi satu unit laptop dengan spesifikasi sebagai berikut:

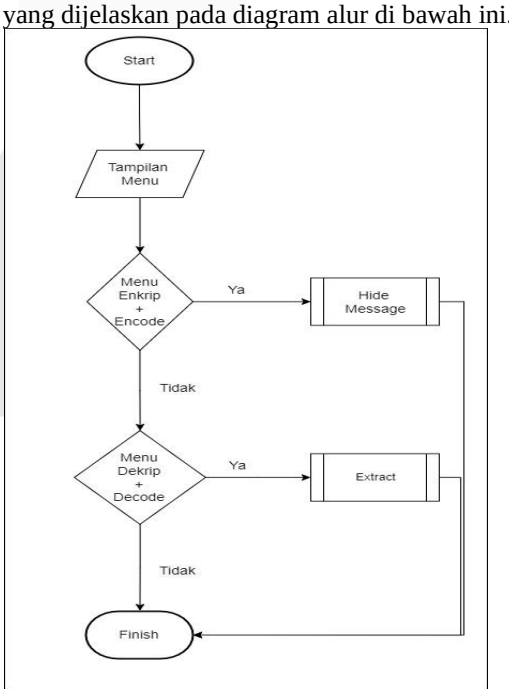
a. Processor : Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz 1.90 GHz
b. Installed RAM :8.00 GB
c. System type : 64-bit operating system, x64-based processor

Sedangkan perangkat lunak yang digunakan dalam penelitian ini meliputi:

a. Operating System : Windows 10 Pro
b. Aplikasi : Virtual Code Studio
c. Bahasa Pemrograman : python 3.10 (64 bit)

B. Rancangan Aplikasi

Perancangan aplikasi akan dilakukan dalam aplikasi Vscode untuk menjalankan fungsi dari enkripsi RSA yang dikombinasikan dengan stego LSB. System ini dibangun untuk mengetahui apakah program enkripsi berjalan sesuai ketentuan fungsi RSA-nya. Secara umum, proses alur sistem terbagi menjadi dua proses yaitu proses komputasi enkrip yang diterapkan pada gambar sampel, lalu setelah proses komputasi selesai, gambar sampel akan di kembalikan ke nilai awal sampel atau dengan kata lain sebagai proses dekrip, seperti yang dijelaskan pada diagram alur di bawah ini.




GAMBAR 3.1
*FLOWCHART* SISTEM

Gambar 3.1 merupakan flowchart yang menggambarkan saat pertama kali pengguna menjalankan simulasi. Pada halaman

tersebut terdapat dua opsi, yaitu enkripsi + encode pesan ke gambar stego, dan decode gambar stego + dekripsi pesan.

C. Parameter Performansi

Parameter yang digunakan untuk analisis adalah nilai RSA, panjang teks yang disisipkan, dan ukuran hasil keluaran gambar.

2. Pengujian Nilai RSA

Pada pengujian ini dilakukan perbandingan pengujian waktu komputasi steganografi dengan masukan hasil proses enkripsi dan dekripsi terhadap data teks yang disisipkan.

3. Pengujian Keamanan Sistem

Pengujian keamanan sistem yang diuji adalah Avalanche Effect. Suatu algoritma dikatakan memiliki nilai AE yang baik jika perubahan satu bit pada masukkan menghasilkan perubahan sekitar 50% jumlah bit pada keluarannya. Salah satu fungsi dari AE adalah untuk melihat tingkat keamanan suatu algoritma kriptografi.

4. Pengujian Output

Pengujian output yang dihasilkan untuk selanjutnya adalah melakukan analisis terhadap keluaran dari sistem.

## IV. HASIL DAN PEMBAHASAN

A. Pengujian Sistem

Pengujian enkripsi RSA pada steganografi LSB pada Tugas Akhir ini disimulasikan pada terminal di Visual Studio Code dengan menggunakan Bahasa Python 3.10 64 bit. Terminal ini berfungsi untuk menjalankan perintah komputasi program enkripsi. Pesan yang akan dienkripsi berupa media gambar berformat .bmp.

Perintah yang dibangun pada program enkripsi ini memiliki 2 perintah yaitu perintah encoding dan decoding. Perintah 1 yaitu encoding berfungsi untuk mengubah file gambar yang telah di input ke dalam program untuk kemudian dilihat apakah terbukti enkripsi berjalan sesuai dengan nilai RSA. Sedangkan perintah decoding berguna untuk mengembalikan pesan acak yang telah diambil dari dalam gambar stego menjadi bentuk awal sehingga dapat diketahui pesan rahasianya.

B. Pengujian Enkripsi *Rivest Shamir Adleman* (RSA)

1. Program Utama

Langkah pertama pengujian yang dilakukan yaitu perintah *encode* membutuhkan beberapa parameter untuk dapat dijalankan sebagaimana fungsinya, yaitu:

a. Panjang Karakter

Jumlah yang telah ditentukan dalam Batasan Masalah yaitu maksimal 255 karakter. Pada penelitian ini, dilakukan pengujian dengan 3 jumlah karakter yang berbeda yaitu:

5. Pada 200 karakter, kalimat yang digunakan adalah, "*Far far away, behind the word mountains, far from the countries Vokalia and Consonantia, there live the blind texts. Separated they live in Bookmarksgrove right at the coast of the Semantics, a large*."
6. Pada 52 karakter, kalimat yang digunakan adalah, "*Far far away, behind the word mountains, far from th*."

Pada 20 karakter, kalimat yang digunakan adalah, "*Far far away, behind*."

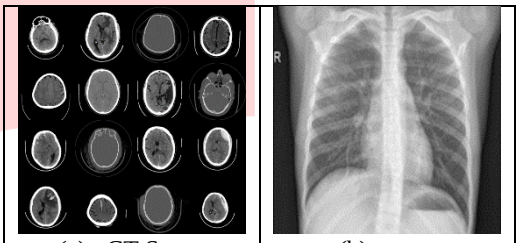
2. Nilai Pembangkitan Kunci RSA

Program enkripsi RSA dibutuhkan nilai kunci publik (*e*,*n*) dan perhitungan nilai kunci privat *d* dengan ketentuan nilai yang dihasilkan diturunkan dari bilangan prima *p* dan *q*. Dalam pengujian ini dilakukan dua kali percobaan pada dua nilai pembangkitan yang berbeda.

C. Skenario Sistem

1. Citra Digital yang Digunakan

Dalam pengujian ini digunakan lima macam ukuran sampel gambar, yaitu dengan ukuran 512x512, 720x720, 1024x1024, 1536x1536, dan 2048x2048 piksel. Sampel data yang digunakan *x-ray* dan *Computed Tomography Scan* (CT *Scan*) menggunakan citra RGB yang memenuhi kualifikasi algoritma RSA dengan format gambar .bmp karena format ini tidak mengalami pengkompresan yang signifikan.



(a) CT Scan (b) *x-ray*

GAMBAR 4.1
SAMPEL CITRA (A) CT SCAN (B) X-RAY

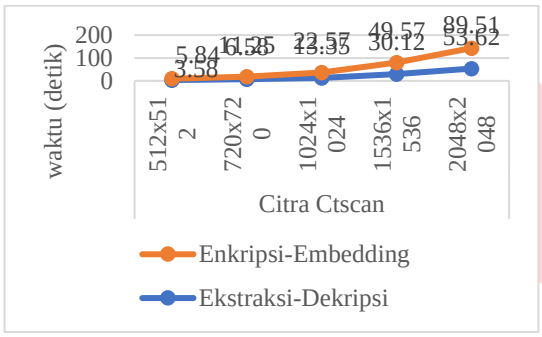
D. Analisis Waktu Komputasi

Berdasarkan pengujian yang dilakukan dari hasil rata-rata 3 kali percobaan dengan 2 nilai parameter yang berbeda, diperoleh rata-rata data hasil waktu komputasi seperti tabel di bawah ini:

TABEL 4.1
WAKTU KOMPUTASI TIPE DATA

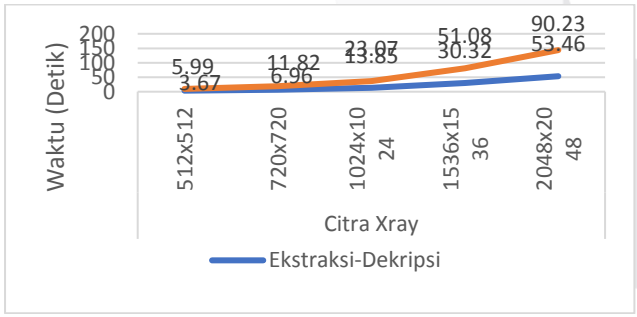
| Tipe Data | Variasi Data | Rataan Waktu Komputasi (Detik) | |
|---|---|---|---|
| | | Enkripsi-Embedding | Ekstraksi-Dekripsi |
| Citra Ctscan | 512x512 | 5.84 | 3.58 |
| | 720x720 | 11.25 | 6.58 |
| | 1024x1024 | 22.57 | 13.35 |
| | 1536x1536 | 49.57 | 30.12 |
| | 2048x2048 | 89.51 | 53.62 |
| Citra Xray | 512x512 | 5.99 | 3.67 |
| | 720x720 | 11.82 | 6.96 |
| | 1024x1024 | 23.07 | 13.85 |
| | 1536x1536 | 51.08 | 30.32 |
| | 2048x2048 | 90.23 | 53.46 |

Berdasarkan Tabel 4.1 terlihat bahwa ukuran dari citra digital sangat berpengaruh terhadap waktu komputasi, baik dalam sisi enkripsi-*embedding* maupun ekstraksi-dekripsi. Hal ini karena pada prosesnya dipengaruhi oleh jumlah piksel pada setiap gambar. Oleh karena itu, waktu komputasi citra digital jika ukuran gambar semakin besar, maka waktu komputasi akan semakin lama. Panjangnya pesan digital yang disisipkan dalam proses ini disimpulkan tidak membuat perubahan signifikan terhadap waktu prosesnya karena perbedaan waktu proses masih dalam batas toleransi kesalahan. Lalu, dari tabel yang di peroleh, dapat dilihat hasil berdasarkan grafik di bawah ini:




GAMBAR 4.2
WAKTU KOMPUTASI PADA CT *SCAN*

Citra digital CT *scan* pada grafiknya menunjukkan waktu komputasi yang dibutuhkan lebih lama pada proses enkripsi-*embedding* dengan waktu rata-rata 5.84 detik pada citra berukuran 512x512 piksel, dan pada puncaknya membutuhkan waktu sekitar 89.51 detik. Dibandingkan dengan waktu komputasi pada proses ekstraksi-dekripsi, membutuhkan waktu yang cenderung lebih cepat dengan waktu rata-rata yang dibutuhkan pada citra gambar yang berukuran 512 x 512 piksel adalah sekitar 3.58 detik, dengan puncaknya pada ukuran gambar 2048 x 2048 dengan waktu sekitar 53.62 detik.




GAMBAR 4.3
WAKTU KOMPUTASI PADA *XRAY*

Citra digital *Xray* pada grafiknya menunjukkan waktu komputasi yang dibutuhkan juga lebih lama pada proses enkripsi-*embedding* dengan waktu rata-rata 5.99 detik pada citra berukuran paling kecil pada 512 x 512 piksel, dan pada puncaknya membutuhkan waktu sekitar 90.23 detik. Dibandingkan dengan waktu komputasi pada proses ekstraksi-dekripsi, membutuhkan waktu yang cenderung lebih cepat dengan waktu rata-rata yang dibutuhkan pada citra gambar yang berukuran 512 x 512 piksel adalah sekitar 3.67 detik, dengan puncaknya pada ukuran gambar 2048 x 2048 pada waktu komputasi sekitar 90.23 detik.

E. Analisis Pengaruh Ukuran Citra Host Terhadap Ukuran Citra Stego

Berdasarkan percobaan yang sudah dilakukan, berikut adalah tampilan ringkas hasil dalam bentuk diagram.


GAMBAR 4.4
DIAGRAM ANALISIS PENGARUH UKURAN CITRA HOST TERHADAP UKURAN CITRA STEGO

Dari data ini dapat disimpulkan bahwa ukuran citra tidak berubah setelah diberlakukan percobaan simulasis penyandian dan *embedding*, maupun setelah proses ekstraksi-dekripsi. Penyebabnya adalah, karena gambar diambil dalam format bitmap (bmp) yang telah diubah menjadi 8-bit *grayscale*, sehingga tidak ada faktor kompresi dalam prosesnya. Ini membuktikan bahwa pada percobaannya tidak mempengaruhi sama sekali besar ukuran dari citra itu sendiri.

F. Analisis Nilai *Avalanche Effect* (AE)

Di bawah ini penyajian Tabel hasil analisis *Avalanche Effect* (AE) yang telah dilakukan uji pada satu gambar dengan resolusi yang sama besar, yaitu 512x512 piksel namun diberi masukan karakter *plaintext* yang dibedakan sebanyak satu huruf.

TABEL 4.2
NILAI AE

| **Sampel Gambar** | **Plaintext 10 Karakter (far far aw)** | | |
|---|---|---|---|
| | Original | Enkripsi - *Embedding* | Ekstraksi - Dekripsi |
| CT Scan 512 | 3192ceb7d9283b015b2cf7f1f891b6457a364dd5 | 81c2d90088d748fded8adfa48e656197c13df43f | 3192ceb7d9283b015b2cf7f1f891b6457a36dd5 |

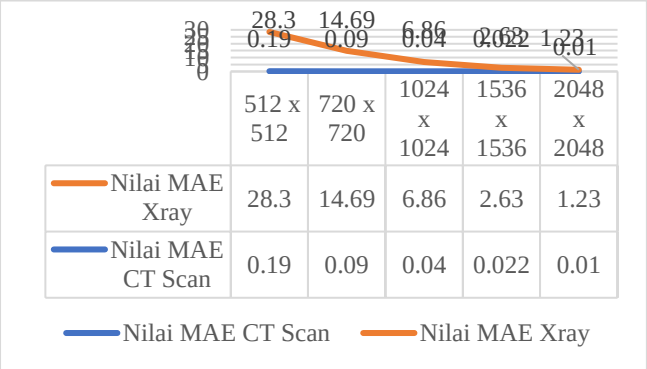
TABEL 4.3
NILAI AE

| **Plaintext 11 Karakter (far far awa)** | | |
|---|---|---|
| Original | Enkripsi – *Embedding* | Ekstraksi - Dekripsi |
| 3192ceb7d9283b015b2cf7f1f891b6457a364dd5 | 4dde4868d7ef376f22dcf8444e448c0b7b88e7f9 | 3192ceb7d9283b015b2cf7f1f891b6457a364dd5 |

Berdasarkan hasil pengujian, saat proses penyisipan gambar didapatkan bahwa *avalanche effect* terbukti berubah dari perbedaan nilai hash (SHA 1) pada proses enkripsi-*embedding*.

G. Analisis Nilai MAE Berdasarkan *Cover Image* dan Stego *Image*

Pengujian ini dilakukan menggunakan 2 citra host yang berbeda, dimana masing-masing memiliki 5 resolusi yaitu 512x512, 720x720, 1024x1024, 1536x1536, dan 2048x2048. Berikut adalah data nilai MAE dari *cover image* dan stego *image* berdasarkan data uji coba.




GAMBAR 4.5

GRAFIK NILAI MAE

Berdasarkan hasil analisis yang ditampilkan pada grafik diatas, dapat disimpulkan bahwa kriteria MAE sudah terpenuhi, sebab pada citra CT *Scan* maupun citra *xray* keduanya memiliki grafik yang semakin menurun mengikuti besarnya ukuran pada citra *host*.

## V. KESIMPULAN DAN SARAN

### A. Kesimpulan

Berdasarkan hasil analisis pengujian simulasi performansi teknik *Rivest Shamir Adleman* (RSA) pada steganografi *Least Significant Bit* (LSB), dapat diambil kesimpulan sebagai berikut:

1. Bentuk algoritma kriptografi pada steganografi dalam skripsi ini menggunakan kombinasi algoritma RSA dan steganografi LSB.
2. Waktu komputasi tercepat pada proses enkripsi-*embedding* yang dibutuhkan adalah 5.53 detik, sedangkan waktu komputasi terlama yang dibutuhkan adalah 95.12 detik. Sedangkan, waktu komputasi yang dibutuhkan pada proses ekstraksi-dekripsi yang paling cepat sebesar 3.49 detik dengan waktu komputasi terlama membutuhkan waktu sebesar 56.21 detik. Waktu komputasi lebih banyak dipengaruhi oleh ukuran citra, dimana semakin besar ukuran citra, semakin besar pula waktu komputasi yang dibutuhkan dalam pengujian.
3. Panjang karakter pesan dan besarnya angka prima yang dipilih tidak terlalu berpengaruh terhadap lamanya waktu komputasi.
4. Pada hasil pengujian nilai MAE diketahui bahwa nilai MAE antara stego *image* dengan *cover image* cenderung menurun pada citra yang memiliki ukuran lebih besar. Hal ini antara lain dipengaruhi oleh perbandingan ukuran gambar dengan jumlah bit yang diubah oleh algoritma steganografi LSB.
5. Nilai *avalanche effect*, berdasarkan hasil pengujian, saat proses penyisipan gambar didapatkan bahwa avalanche effect terbukti berubah dari perbedaan nilai hash (SHA 1) pada proses enkripsi-*embedding*.

### B. Saran

Saran pengembangan untuk penelitian selanjutnya adapun sebagai berikut:

1. Penelitian dapat menguji dengan pengkombinasian metode algoritma yang kebih bervariasi.
2. Peneliti agar dapat mencoba menambahkan parameter-parameter lain yang lebih bervariasi.
3. Sistem yang telah ada dikembangkan menjadi sebuah sistem aplikasi yang lebih kompleks sesuai kebutuhan agar dapat digunakan secara real time.

## DAFTAR PUSTAKA

[1] R. M. Supplements, T. Dip, and B. Curl, “Meal Plan Day 26,” vol. 10, no. 1, 2015.

[2] S. Wardoyo, Z. Imanullah, and R. Fahrizal, “Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android,” Setrum, vol. 3, no. 1, pp. 43–53, 2016.

[3] Y. Kurniawan and F. A. Yulianto, “Analisis Perbandingan Metode DSA dan ECDSA Pada Implementasi Tandatangan Digital,” pp. 1–6.

[4] K. Malhotra, S. Gardner, and R. Patz, “Implementation of elliptic-curve cryptography on mobile healthcare devices,” 2007 IEEE Int. Conf. Networking, Sens. Control. ICNSC’07, no. April, pp. 239–244, 2007.

[5] William Stallings, “Cryptography and Network Security Principles and Practice” Chapter 9 Public-key Cryptography and RSA.

[6] Chapter 7 of Understanding Cryptography by Christof Paar and Jan Pelzl.

[7] ]Megha S. Lahase, S. A. Dhole., 2015. “Hybrid Encryption and decryption Method Using LSB and RSA In Steganography” IJEEDC, ISSN (P): 2320-2084, (O) 2321–2950

[8] Johnson, N.F.; Jajodia, S. (1998). Exploring steganography: Seeing the unseen, 31(2), 26–34. doi:10.1109/mc.1998.4655281

[9] Ganesha Dwi A., R. Rumani M., Muhammad Nasrun, 2015. Implementasi Kriptografi dan Steganografi Pada Media Gambar Menggunakan Algoritma Blowfish dan Metode Least Significant Bit. Bandung, e-Proceeding Of Engineering : Vol.2, No.2

[10] Antonius Erick Handoyo, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari, Ajib Susant, “Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA” DOI: 10.14710/jtsiskom.6.1.2018, 37-43

[11] Stephanie Glen."Absolute Error & Mean Absolute Error (MAE)", https://www.statisticshowto.com/absolute-error/

[12] Drashti O. Vadaviya, H. Tandel "Study of avalanche effect in AES" Conference Paper · May 2015

[13] Nelson Josias Gbètoho Saho, Eugène C. Ezin. Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm. CARI 2020 – Colloque Africain sur la Recherche en Informatique et en Mathématiques Apliquées, Oct 2020, Thiès, Senegal.

[14] Dindayal Mahto and Dilip Kumar Yadav, "Performance Analysis of RSA and Elliptic Curve Cryptography" International Journal of Network Security, Vol.20, No.4, PP.625-635, July 2018 (DOI: 10.6633/IJNS.201807 20(4).04)

[15] Rajamah Limbong, "Kombinasi Kriptografi RSA dan Steganografi Spread Spectrum Untuk Mengamankan Data Teks" Jurnal Majalah Ilmiah Informasi dan Teknologi Ilmiah (INTI) ISSN 2301-9425 (Media Cetak) Volume 7, No 1, Oktober 2019 Hal: 97-100