# IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN ENKRIPSI RSA UNTUK KEAMANAN DATA

**S.E.Retnosari[1], Ramadhan Renaldy[2] dan P.R.Sari[3]**

[1,2,3]*Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*

*Gedung Pusat Lantai 6, Kampus 1 Jl. Sidodadi Timur 24, Semarang*

E-mail : septianiekar@gmail.com[1], ramadhanrenaldy@upgris.ac.id[2], pujiratnasari611@gmail.com[3]

***Abstrak***

*Metode kejahatan seperti perusakan dan pencurian data semakin berkembang seiring dengan kemajuan teknologi. Banyak pihak yang tidak berwenang menggunakan berbagai metode untuk mendapatkan informasi secara ilegal, yang memungkinkan mereka untuk mendapatkan data yang tidak mereka miliki. Dalam komunikasi digital, keamanan data menjadi masalah utama, terutama ketika data sensitif disimpan atau dikirim melalui media yang rentan terhadap ancaman. Tujuan penelitian ini adalah untuk memecahkan masalah ini dengan menggunakan steganografi yang menggunakan metode Least Significant Bit (LSB) yang dikombinasikan dengan enkripsi RSA. Metode LSB memungkinkan penambahan pesan ke bitbit terakhir dari piksel citra digital tanpa mengurangi kualitas visual gambar secara signifikan. Algoritma RSA digunakan untuk mengenkripsi pesan sebelum disisipkan, memberikan lapisan perlindungan tambahan. Hasil uji dengan perhitungan Mean Squared Error (MSE) menunjukkan bahwa kualitas gambar tetap terjaga dengan perubahan yang tidak terlihat oleh mata manusia. Kombinasi LSB dan RSA terbukti efektif sebagai solusi keamanan data dalam komunikasi digital tanpa merusak kualitas media yang digunakan*

***Kata Kunci*:** Steganografi LSB, Enkripsi RSA, Mean Squared Error (MSE)

## I. PENDAHULUAN

Pertukaran informasi di era sekarang ini menjadi sangat mudah. Menurut Badan Pusat Statistik (BPS) hasil dari pendataan Survei Susenas pada tahun 2022, sebanyak 66,48 persen penduduk Indonesia telah mengakses internet pada tahun 2022 dan 62,10 persen di tahun 2021. Tingginya penggunaan internet ini mencerminkan iklim keterbukaan informasi dan penerimaan masyarakat terhadap perkembangan teknologi dan perubahan menuju masyarakat informasi. Berdasarkan tingginya persentase tersebut, tidak hanya memberikan dampak yang baik tetapi juga memberikan dampak yang buruk.

Seiring dengan kemajuan teknologi, metode kejahatan seperti perusakan dan pencurian data juga semakin berkembang. Banyak pihak yang tidak berwenang menggunakan berbagai teknik untuk mengakses informasi secara ilegal, sehingga mereka dapat mengakses data yang bukan hak mereka(Hafiz, 2019). Keamanan informasi adalah aspek terpenting dalam proses pertukaran informasi seperti mengirim pesan melalui media elektronik. Tanpa adanya keamanan sering kali terjadi penyalahgunaan informasi yang dapat merugikan sumber tersebut. Dengan demikian, keamanan informasi yang dipertukarkan turut menjadi hal yang sangat penting untuk dijaga. Oleh karena itu,berbagai upaya dapat dilakukan untuk melindungi keamanan dan kerahasiaan data serta informasi.

Beberapa cara dapat digunakan sebagai upaya dalam mengamankan suatu data yang penting. Salah satu teknik pengamanan data yang sering digunakan adalah kriptografi dan steganografi. Penggunaan teknik steganografi dapat diperkuat dengan mengombinasikannya dengan enkripsi kriptografi sebelum pesan disembunyikan di dalam gambar. Dalam



E-ISSN: 2985-3532

kriptografi, terdapat proses enkripsi yang mengubah teks asli menjadi kode tak terbaca (ciphertext), sementara proses dekripsi dapat mengembalikan ciphertext menjadi teks asli, algoritma ini juga dapat memanfaatkan kunci yang dimasukkan dari luar. Teknik kriptografi dapat menimbulkan kecurigaan pada pihak ketiga yang tidak berhak menerima informasi karena pesan disamarkan dengan cara mengubah pesan yang asli menjadi seolah-olah tidak terbaca. Selanjutnya pihak ketiga tersebut akan memiliki keinginan untuk mengetahui isi pesan rahasia tersebut dan berusaha memecahkan informasi yang sebenarnya.

Salah satu algoritma yang memanfaatkan kriptografi sebagai sistem keamanan adalah algoritma RSA (Ron Rivest,Shamir, dan Leonard Adleman). RSA mempunyai dua kunci, yaitu kunci publik dan kunci privat. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci enkripsi bersifat terbuka dan dapat diakses oleh umum (disebut kunci publik), sedangkan kunci dekripsi bersifat rahasia (kunci privat). Untuk menemukan kunci dekripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah hal yang mudah, Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA(Fitriani, 2020).

Steganografi bisa digunakan juga untuk menyampaikan pesan yang bersifat rahasia, karena sifat dari steganografi yaitu sulit dideteksi keberadaannya karena tersembunyi. Tujuan dari steganografi adalah memanipulasi sebuah objek untuk menyembunyikan pesan kedalamnya. Untuk sistem keamanan komputer, steganografi dapat digunakan untuk menyembunyikan data rahasia pada saat proses enkripsi tidak dapat dilakukan atau bersamaan dengan proses enkripsi itu sendiri(Handoyo et al., 2018). Metode yang digunakan dalam steganografi ini adalah metode RSA (Ron Rivest,Shamir, dan Leonard Adleman) dalam pengacakan pesan dan menggunakan metode Modifikasi LSB (Least Significant Bit) dalam menyisipkan pesan rahasia ke media citra digital. Penyembunyian pesan dengan menggunakan metode LSB ini sangat sederhana karena hanya mengubah nilai bit terakhir dengan bit pesan. Namun, Teknik ini dapat menghasilkan citra yang sangat mirip dengan citra aslinya sehingga indra penglihatan manusia tidak dapat mendeteksi perubahan pada citra dan mustahil untuk mengartikan pesan secara langsung.

Citra digital menggunakan format *.bmp lebih baik dibandingkan dengan menggunakan gambar dengan format *.tiff, *.jpg dan *.png. Hal ini dikarenakan gambar dengan format *.bmp terdiri dari piksel yang berdiri sendiri dan mempunyai warna sendiri(Sekarwati & Budiman, 2017). Berdasarkan hal tersebut penggunaan gambar dengan format *.bmp lebih baik untuk melakukan encoding atau penyisipan karena ukuran gambar asli dengan gambar yang telah disisipi sama sehingga tidak terlihat kecurigaan.

Dari hasil penelitian sebelumnya kami dapat mengambil dasar dan teori-teori yang bisa dijadikan sebagai data pendukung. Salah satu data pendukung yang kami jadikan acuan adalah penelitian terdahulu yang relevan dan permasalahan yang di bahas. Permasalahan yang dibahas pada penelitian (Jatmoko dkk., 2018) membandingkan metode LSB dan MSB. Data yang digunakan citra cover grayscale ukuran 256*256. Sedangkan citra pesan juga menggunakan citra grayscale dengan ukuran 128*64. Berdasarkan hasil uji komparasi pada penelitian ini dapat disimpulkan bahwa metode LSB memiliki keunggulan pada kualitas citra



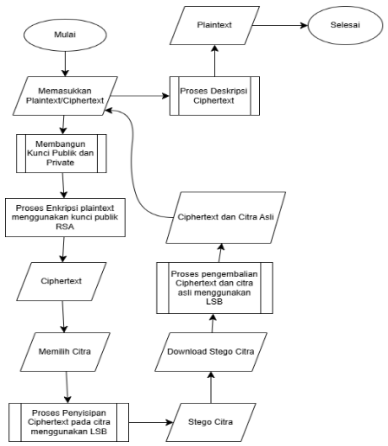
E-ISSN: 2985-3532

stego. Terbukti bahwa nilai PSNR yang mencapai lebih dari 54 dB, nilai PSNR juga stabil(Jatmoko et al., 2018).

Penelitian (Kuncoro & Aditama, 2019) menggunakan kombinasi RSA dan LSB menunjukan waktu proses lebih banyak dipengaruhi oleh ukuran citra. Pada citra berukuran 250x250 piksel dibutuhkan waktu proses rata-rata 0.139 detik dan terus meningkat hingga 1.2 detik pada citra berukuran 1000x1000 piksel, sedangkan panjang pesan tidak terlalu berpengaruh terhadap lamanya waktu proses. Nilai PSNR tertinggi adalah 66.2185 dB sedangkan nilai PSNR terendah adalah 53.0696 dB. Sama seperti pada waktu proses, ukuran citra juga paling berpengaruh terhadap nilai PSNR dibandingkan data lain(Kuncoro & Aditama, 2019).

Pada penilitian ini, kami megimplementasikan steganografi pada citra digital menggunakan metode LSB dan enkripsi RSA untuk keamanan data, disini kami menggunakan pengujian kualitas citra MSE. Adapun bagian yang akan dijadikan bahan penelitian adalah media penampung yaitu citra pada proses enkripsi dan dekripsi. Tujuan dari penelitian ini untuk mengetahui pengaruh variabel citra terhadap tingkat keamanan pesan.

## II. METODOLOGI PENELITIAN




Gambar 22. Flowchart Enkripsi dan Deskripsi

Proses dimulai dengan pengguna memasukkan teks biasa (plaintext) yang ingin dikirim atau pesan yang telah terenkripsi sebelumnya (ciphertext). Selanjutnya, sistem akan membuat dua kunci rahasia, yaitu kunci publik yang digunakan untuk mengenkripsi pesan, dan kunci privat yang digunakan untuk mendekripsi pesan. Teks biasa akan dienkripsi menggunakan kunci publik sehingga berubah menjadi pesan rahasia (ciphertext). Pesan yang telah terenkripsi ini kemudian siap untuk langkah berikutnya.

Pengguna kemudian memilih gambar yang akan digunakan untuk menyembunyikan pesan rahasia. Proses penyembunyian pesan dilakukan dengan teknik *Least Significant Bit* (LSB), yang memungkinkan pesan rahasia disisipkan ke dalam gambar. Hasilnya adalah sebuah gambar baru yang terlihat normal tetapi sebenarnya berisi pesan tersembunyi. Setelah itu, pengguna dapat mengunduh gambar tersebut untuk digunakan lebih lanjut.

Jika pesan rahasia perlu diambil kembali dari gambar, sistem akan menggunakan teknik LSB yang sama untuk mengambilnya. Setelah pesan rahasia berhasil diambil, pengguna akan mendapatkan kembali pesan terenkripsi (ciphertext) beserta gambar asli tanpa perubahan. Untuk membaca pesan tersebut, pengguna dapat mendekripsinya menggunakan kunci privat



E-ISSN: 2985-3532

yang telah dibuat sebelumnya. Proses dekripsi ini akan mengembalikan pesan ke bentuk aslinya sebagai teks biasa. Akhirnya, pesan yang tersembunyi berhasil ditampilkan, dan seluruh proses dinyatakan selesai.

### 39. Least Significant Bit (LSB)

Metode Least Significant Bit (LSB) adalah salah satu teknik steganografi yang paling sederhana dan mudah diterapkan. Teknik ini bekerja dengan memodifikasi bit paling tidak signifikan dalam sebuah file, seperti gambar digital. Karena bit yang diubah adalah bagian terkecil dari data, perubahan yang dihasilkan hampir tidak memengaruhi tampilan atau kualitas file aslinya. Hal ini membuat metode LSB ideal untuk menyembunyikan pesan rahasia secara halus dan tidak terdeteksi oleh mata manusia(Mido & Ujianto, 2022).

Keunggulan teknik LSB dalam steganografi adalah kemampuannya untuk mempertahankan kualitas citra stego yang baik sambil menjaga aspek *imperceptibility*, yaitu ketidakmampuan manusia untuk membedakan citra asli dan citra yang telah disisipi pesan. Selain itu, teknik ini juga efisien dalam hal proses penyisipan dan pengambilan data rahasia. Adapun Perhitungan dalam LSB mencakup:

a. Konversi data pesan ke biner.
b. Penyisipan bit pada LSB citra.
c. Evaluasi kualitas citra dengan MSE.
d. Perhitungan kapasitas penyisipan pesan.
e. Ekstraksi kembali data yang disembunyikan.

Teknik LSB digunakan embedding dan ekstraksi, konsep dasar dari subtitusi LSB adalah dengan menggantikan data rahasia di paling kanan bit (bit dengan bobot terkecil) sehingga prosedur embedding tidak signifikan mempengaruhi nilai piksel aslinya.

### 40. Mean Square Error (MSE)

Ada begitu banyak teknik kualitas gambar yang banyak digunakan untuk mengevaluasi dan menilai kualitas citra. Penelitian ini menggunakan teknik MSE (Mean Square Error). Mean Square Error (MSE) adalah penaksir paling umum untuk metrik pengukuran kualitas gambar dengan sebuah metrik referensi lengkap dan nilai yang mendekati nol adalah lebih baik. Ukuran penduga yang menunjukkan bagaimana penaksir bervariasi dari yang diperkirakan. Dalam kaitannya dengan varians dan derajat distorsi dari rahasia asli MSE mengakses kualitas gambar yang direproduksi. Persamaan MSE seperti persamaan:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\Sigma_{Y=1}^{N}\left(S_{xy} - C_{xy}\right)^2 \qquad (1)$$

Penjelasan Komponen:

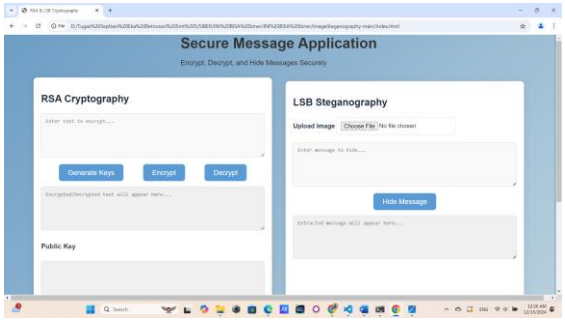
1. M: Jumlah elemen dalam dimensi horizontal (atau jumlah kolom data).
2. N: Jumlah elemen dalam dimensi vertikal (atau jumlah baris data).
3. Sxy: Nilai sebenarnya (ground truth) pada posisi (x,y).
4. Cxy: Nilai prediksi pada posisi (x,y).
5. $(Sxy-Cxy)^2$: Perbedaan kuadrat antara nilai sebenarnya dan nilai prediksi untuk elemen tertentu.

## III. HASIL DAN PEMBAHASAN

Untuk dapat membuat sistem pengamanan citra digital dengan kriptografi RSA dan metode steganografi LSB, maka implementasinya dibuat dalam bentuk program dengan menggabungkan HTML untuk struktur, CSS untuk styling, dan JavaScript untuk fungsionalitas, serta menggunakan library JavaScript untuk mendukung fitur kriptografi.



E-ISSN: 2985-3532

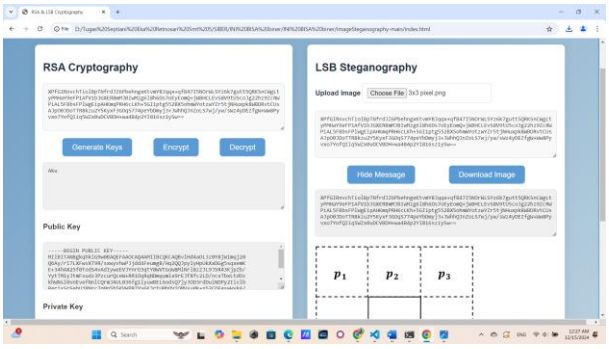



Gambar 23. Tampilan Program program Secure Message Application

Gambar di atas merupakan tampilan program *Secure Message Application* yang digunakan untuk proses enkripsi dan penyisipan pesan secara aman. Aplikasi ini memiliki dua bagian utama, yaitu modul *RSA Cryptography* dan modul *LSB Steganography*.

Untuk melakukan proses enkripsi menggunakan modul RSA Cryptography, pengguna perlu memasukkan teks yang akan dienkripsi di kolom yang tersedia, kemudian menekan tombol "Generate Keys" untuk membuat kunci publik dan privat. Setelah kunci dibuat, pengguna dapat menekan tombol "Encrypt" untuk mengenkripsi pesan dan mendapatkan hasil dalam bentuk *ciphertext*. Jika pesan ingin didekripsi kembali, pengguna cukup memasukkan *ciphertext* dan menekan tombol "Decrypt".

Pada modul LSB Steganography, proses penyisipan pesan ke dalam gambar dapat dilakukan dengan terlebih dahulu memilih file gambar (*Upload Image*) yang akan digunakan sebagai media penampung pesan. Selanjutnya, pengguna memasukkan pesan rahasia yang ingin disisipkan pada kolom "Enter message to hide". Setelah itu, dengan menekan tombol "Hide Message", aplikasi akan menyisipkan pesan ke dalam gambar menggunakan metode LSB (*Least Significant Bit*). Hasilnya adalah gambar baru yang telah berisi pesan tersembunyi, dan pesan yang telah disisipkan akan muncul di bagian hasil.




Gambar 2. Tampilan setelah memasukkan gambar yang telah dimodifikasi

Gambar yang telah dimodifikasi dapat diunduh dengan menekan tombol "Download Image". Gambar ini tampak seperti gambar biasa, tetapi di dalamnya terdapat pesan tersembunyi yang hanya dapat diakses oleh penerima yang mengetahui metode ekstraksi.

- **Analisis Perhitungan dan Evaluasi Mean Square Error (MSE) pada Sistem Steganografi LSB**

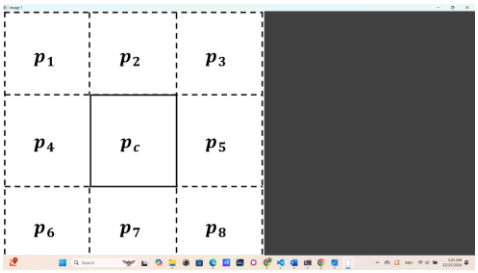
Mean Square Error (MSE) adalah metrik yang digunakan untuk mengevaluasi perbedaan antara dua data numerik, dalam hal ini adalah gambar asli (*cover image*) dan gambar hasil steganografi (*stego image*). Pada sistem steganografi berbasis LSB (*Least Significant Bit*), MSE berfungsi sebagai indikator kuantitatif untuk



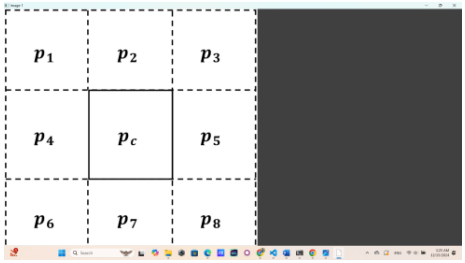
E-ISSN: 2985-3532

mengukur dampak penyisipan pesan terhadap kualitas visual gambar. Pada penelitian ini peneliti menggunakan 2 metode perhitungan MSE di antaranya sebagai berikut:

1. **Proses Perhitungan MSE Menggunakan Python**
   Hasil Output




Gambar 3. Tampilan Image 1 (Gambar asli)




Gambar 4. Tampilan Image 2 ( Gambar Steganografi)


Gambar 5. Tampilan Hasil dari Perhitungan MSE

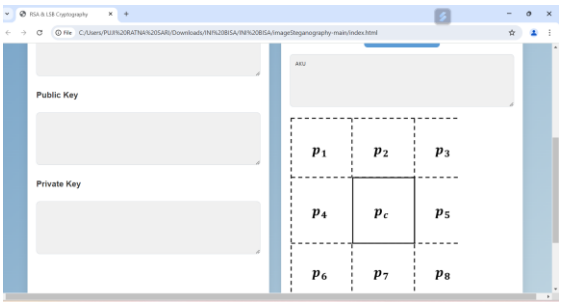
Implementasi MSE dalam Python melibatkan beberapa langkah utama, yaitu memuat gambar, menghitung perbedaan piksel, dan merata-ratakan kuadrat perbedaannya. Gambar asli (*image1*) dan gambar hasil steganografi (*image2*) diambil menggunakan pustaka OpenCV (cv2.imread). Gambar yang digunakan harus memiliki ukuran yang sama untuk memastikan perhitungan MSE dapat dilakukan. Hasil Akhir Nilai MSE yang kita dapatkan adalah: 0.000661

- **Testing Program Secure Message Application**
  1. Cropping (Pemotongan Gambar)



E-ISSN: 2985-3532

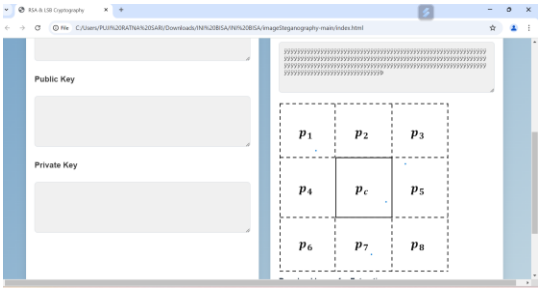
Cropping adalah manipulasi gambar dengan memotong sebagian dari area gambar, sehingga hanya bagian tertentu yang tersisa. Tujuannya Untuk menguji apakah sistem steganografi tetap bisa mengekstrak pesan ketika sebagian data gambar hilang akibat pemotongan. Uji Cropping dalam sistem menjunkan bahwa sistem berjalan dengan baik:




Gambar 12. Uji Cropping pada gambar

2. Noise (Gangguan Acak)

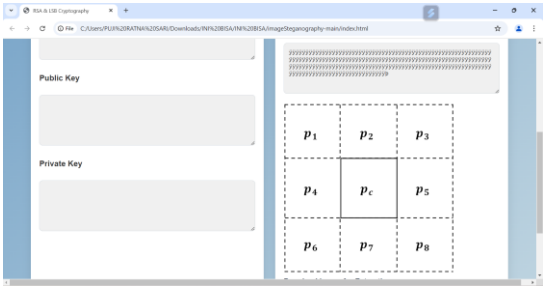
Noise adalah gangguan acak yang ditambahkan ke gambar, biasanya berupa bintik-bintik kecil (grainy effect). Noise sering digunakan untuk mensimulasikan gangguan yang terjadi pada file gambar selama transmisi atau penyimpanan. **Tujuannya** untuk menguji apakah pesan tersembunyi dalam gambar masih dapat diekstraksi setelah gambar terganggu oleh noise. Uji Noise dalam sistem menunjukkan bahwa terdapat bug dalam sistem dikarenakan ada perubahan saat gambar stegano di ekstrak:




Gambar 13. Uji Noise pada gambar

3. **Brightness (Kecerahan)**

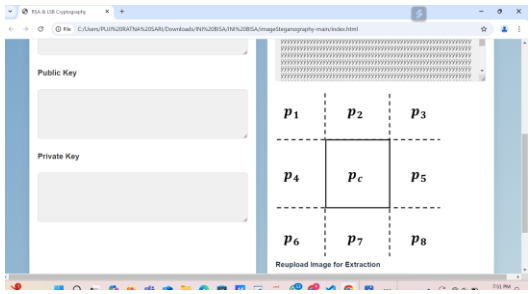
Brightness adalah manipulasi gambar dengan menambah atau mengurangi tingkat kecerahan keseluruhan gambar. Tuujiannya untuk menguji apakah data yang disisipkan di gambar masih dapat diekstraksi meskipun gambar menjadi lebih terang atau lebih gelap. Uji Brightness dalam sistem menunjukkan bahwa terdapat bug dalam sistem dikarenakan ada perubahan saat gambar stegano di ekstrak:




Gambar 14. Uji Brightness pada gambar

4. Resize (Perubahan Ukuran)

Resize adalah manipulasi gambar dengan memperbesar atau memperkecil ukuran gambar. Proses ini sering kali menyebabkan perubahan pada struktur piksel gambar. Tujuannya untuk menguji apakah data steganografi tetap utuh atau rusak ketika gambar diubah ukurannya. Uji Resize dalam sistem menunjukkan bahwa terdapat bug dalam sistem dikarenakan ada perubahan saat gambar stegano di ubah ukuran dan di ekstrak:




Gambar 15. Uji Resize pada gambar

## IV. KESIMPULAN

Penelitian ini berhasil menggabungkan dua teknik, yaitu steganografi LSB (Least Significant Bit) dan enkripsi RSA, untuk menyembunyikan pesan secara aman dalam gambar. Teknik LSB menyisipkan pesan ke dalam bit terakhir dari piksel gambar, sementara RSA mengenkripsi pesan terlebih dahulu sebelum disembunyikan, memberikan lapisan perlindungan ekstra. Hasil pengujian menunjukkan bahwa meskipun pesan berhasil disembunyikan, kualitas gambar hampir tidak berubah, yang terlihat dari nilai MSE yang rendah yaitu 0.666. Enkripsi RSA memastikan bahwa pesan hanya bisa diakses oleh penerima yang memiliki kunci privat, menambah tingkat keamanan.

Berdasarkan hasil pengujian manipulasi gambar dengan metode Cropping, Noise, Brightness, dan Resize, diketahui bahwa sistem steganografi memiliki kinerja yang baik terhadap pemotongan gambar namun menunjukkan kelemahan pada gangguan noise, perubahan kecerahan, dan perubahan ukuran yang menyebabkan pesan tersembunyi sulit diekstraksi dengan benar. Untuk meningkatkan ketahanan sistem, diperlukan pengujian lanjutan seperti variasi persentase pemotongan, intensitas dan jenis noise, skala perubahan kecerahan, serta metode interpolasi pada resize. Selain itu, penerapan algoritma berbasis transformasi domain, teknik koreksi kesalahan (ECC), serta pengujian kombinasi manipulasi dan simulasi kompresi dunia nyata dapat dilakukan untuk memperkuat keandalan sistem dalam berbagai kondisi.

.

## V. REFERENSI

Fitriani, L. A. (2020). Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA Dan Steganografi LSB. *Journal of Computer System and Informatics …*, *1*(2), 32–38. https://ejurnal.seminar-id.com/index.php/josyc/article/view/72

Hafiz, A. (2019). Steganografi Berbasis Citra Digital Untuk Menyembunyikan DataMenggunakan Metode Least Significant Bit (Lsb). *Jurnal Cendikia Vol. XVII Cendikia 2019 Bandar Lampung, April 2019* , *17*, 194–198.

Handoyo, A. E., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., & Susanto, A. (2018). Message Concealment and Encryption Technique in Digital Image with Combination of LSB and RSA Methods. *Jurnal Teknologi Dan Sistem Komputer*, *6*(1), 37–43. https://doi.org/10.14710/jtsiskom.6.1.2018.37-43

Jatmoko, C., Handoko, L. B., Sari, C. A., Ignatius, D. R., & Setiadi, M. (2018). *U Ji P Erforma P Enyisipan P Esan Dengan M Etode Lsb Dan Msb*. *14*(1), 47–56.

Kuncoro, T. R., & Aditama, R. (2019). Analisis Kombinasi Algoritma Kriptografi Rsa Dan



E-ISSN: 2985-3532

Algoritma Steganografi Least Significant Bit (Lsb) Dalam Pengamanan Pesan Digital. *Statmat : Jurnal Statistika Dan Matematika*, *1*(2), 60–82. https://doi.org/10.32493/sm.v1i2.2947

Mido, A. R., & Ujianto, E. I. H. (2022). Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan STEGANOGRAFi LSB. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *9*(2), 279. https://doi.org/10.25126/jtiik.2022914852

Sekarwati, K. A., & Budiman, A. (2017). Implementasi Algoritma Rivest-Shamir-Adleman (Rsa) Dan Metode Least Significant Bit(Lsb) Untuk Keamanan File Teks Dan Dokumen Menggunakan Visual C#. *Jurnal Teknologi Rekayasa*, *22*(1), 54–62.



E-ISSN: 2985-3532