Rekayasa Hijau: Jurnal Teknologi Ramah Lingkungan Volume 9 | Nomor 2
ISSN [e]: 2579-4264 | DOI: https://doi.org/10.26760/jrh.V9i2.123-133 Juli 2025

Analisis Penyisipan Pesan Terenkripsi Algoritma RSA Pada Gambar Dengan Pengujian PSNR

Asep Rizal Nurjaman[1], Fauzan Ramadhan[2]
[1] Institut Teknologi Nasional, Bandung, Indonesia
[2] Universitas Telkom, Bandung, Indonesia
Email: aseprizal@itenas.ac.id[1]

Received 10 Mei 2025 | Revised 20 Mei 2025 | Accepted 25 Mei 2025

ABSTRAK

Keamanan data digital menjadi tantangan dalam pengembangan sistem yang akan dikembangkan. Keamanan ini akan berbanding terbalik dengan kenyamanan. kriptografi merupakan salah satu teknik untuk mengamankan/mengacak data, namun jika hanya dilakukan pengacakan/pengamanan data, maka penyerang akan dengan mudah mencoba untuk melakukan dekripsi karena mengetahui pesannya teracak. Teknik lain yang bisa digunakan untuk mengamankan pesan adalah steganografi yang merupakan sebuah teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya tampak seperti informasi normal lainnya. Penelitian ini mencoba untuk menggabungkan antara kriptografi dan steganografi sehingga pesan yang terenkripsi akan disisipkan dalam sebuah gambar. Pengujian yang dilakukan dengan metode PSNR dimana kemiripan antara gambar asli dan gambar hasil penyisipan akan dihitung. Selain pengujian PSNR, skema yang dibangun akan diujikan dengan skema MITM Attack. Hasil penelitian menunjukkan bahwa nilai PSNR dari gambar yang disisipkan pesan terenkripsi > 50dB yang berarti tingkat kualitas gambar antara gambar asli dan gambar yang disisipkan dengan pesan terenkripsi sangat tinggi. Hasil pengujian skema menunjukkan jika gambar berhasil di ekstraksi, penyerang harus melakukan dekripsi dengan menebak kunci rahasia pengirim untuk bisa mendapatkan pesan aslinya. Penelitian ini dibatasi pada gambar berekstensi .png. Ukuran gambar, panjang pesan dengan kombinasi karakter pada pesan yang sangat mempengaruhi ukuran gambar hasil penyispan pesan terenkripsi.

***Kata kunci**: Algoritma RSA, PSNR, Steganografi, Enkripsi, Dekripsi*

ABSTRACT

Digital data security is a challenge in developing the system to be developed. This security will be inversely proportional to convenience. Cryptography is one technique to secure data, but if only for securing data, the attacker will try to decrypt it. Another technique that can be used to secure messages is steganography which is a technique to hide personal information with something that looks like other normal information. This study tries to combine cryptography and steganography so that the encrypted message will be inserted into an image. Testing is done using the PSNR method where the similarity between the original image and the embedded image will be calculated. In addition to PSNR testing, the scheme that was built will be tested with the MITM Attack scheme. The results of the study showed that the PSNR value of the image inserted with the encrypted message was > 50dB which means the level of image quality between the original image and the image inserted with the encrypted message is very high. The results of the scheme test show that if the image is successfully extracted, the attacker must decrypt it by guessing the sender's secret key to be able to get the original message. This research is limited to images with the extension .png. Image size, message length with character combination in the message which greatly affects the size of the image resulting from the embedded encrypted message.

***Keywords**: RSA Algorithm, PSNR, Steganography, Encryption, Decryption*

1. PENDAHULUAN

Peningkatan kebutuhan manusia akan informasi mendorong teknologi informasi yang berkembang dengan pesat, informasi dalam bentuk fisik telah bertransformasi ke dalam bentuk digital. Keamanan pada data digital menjadi tantangan dalam pengembangan sistem atau aplikasi yang akan dikembangkan. Keamanan ini akan berbanding terbalik dengan kenyamanan. Kriptografi merupakan sebuah Teknik untuk mengamankan / mengacak data, baik data yang dikirim atau data yang disimpan. Kriptografi merupakan seni untuk menyandikan pesan [1]. Dengan konsep kriptografi maka data yang disimpan akan terlihat acak. Hal ini menjadi pemicu peretas untuk mencari tahu informasi dari data yang diacak. Teknik lain yang bisa digunakan untuk mengamankan data digital adalah steganografi yang merupakan sebuah teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya tampak seperti informasi normal lainnya [2]. Pada umumnya steganografi ini merupakan proses untuk menyembunyikan data dalam berbagai media (media citra digital, audio, atau video) dengan teknik tertentu sehingga tidak ada seorang pun yang mengetahui bahwa ada suatu pesan rahasia selain pengguna yang diberikan hak akses. Menyisipkan pesan pada sebuah media gambar merupakan sebuah pilihan yang tepat dan efektif. Sebab pesan yang disisipkan dalam sebuah gambar secara kasat mata hanya terlihat sebuah gambar biasa. Hal ini mampu menjaga kerahasiaan informasi dan tidak menimbulkan kecurigaan bagi pihak lain karena gambar masih terlihat seperti aslinya. Contoh sederhananya adalah seseorang menyisipkan informasi berupa pesan pada sebuah gambar, pihak lain akan melihat bahwa foto yang dikirimkan merupakan sebuah foto yang biasa, namun bagi si penerima, foto ini merupakan sebuah media yang sudah disisipkan informasi berupa teks. Walaupun metode ini sederhana, namun efektif dalam menyamarkan informasi rahasia, sehingga pesan yang disisipkan dalam media gambar sulit terdeteksi secara langsung oleh orang lain, mempersulit proses membaca pesan secara kasat mata [3], [4]. LSB (Least Significant Bit) merupakan sebuah metode yang paling sering digunakan pada steganografi. LSB bekerja dengan cara menyembunyikan bit pesan rahasia ke dalam bit terakhir dari setiap elemen citra digital [5]. Least Significant Bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil, letaknya adalah paling kanan dari barisan bit [6].

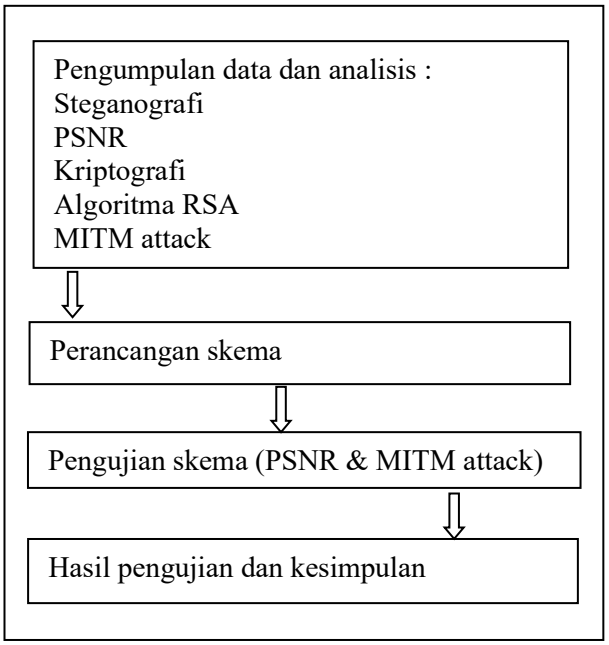
Penelitian terkait steganografi sudah pernah dilakukan oleh Lasarus [10], dimana pada penelitiannya menyembunyikan suatu informasi ke dalam *file* multimedia dengan memanfaatkan Microsoft Visual Basic 6.0. produk yang dikembangkan menggunakan teknik steganografi dengan metode *simple least significant bit substitution*. Pada penelitian Dewi Laksmiati [7], menyimpulkan bahwa *file* asli dan hasil penyisipan secara kasat mata terlihat sama, ukuran gambar membatasi kemampuannya untuk menampung pesan yang disisipkan. Pada penelitian Ravansa dkk [8], mengemukakan jika kombinasi LSB dan One Time Pad dapat menjadi metode yang efektif untuk meningkatkan keamanan email. Pada penelitian Zaim dkk [9], menghasilkan sebuah kesimpulan bahwa Semakin besar kapasitas untuk disisipkan pesan maka kualitas gambar dengan perhitungan PSNR terlihat kurang baik.

Penelitian ini bertujuan untuk mengombinasikan antara steganografi dan kriptografi sehingga data yang disisipkan pada gambar tidak mudah dibaca oleh pengguna yang tidak sah saat gambar tersebut berhasil di ekstraksi karena data yang disisipkan sudah di amankan dengan menggunakan algortima RSA sehingga hanya pengguna yang memiliki akses (pengguna yang sah) yang bisa melakukan ekstraksi dan dekripsi pesan yang disisipkannya. Pada penelitian ini juga akan di bandingkan antara penyisipan pesan pada gambar dan penyisipan pesan yang di enkripsi algoritma RSA pada gambar. Pengujian yang dilakukan dengan melakukan perbandingan antara kualitas citra asli dengan citra yang telah disisipkan teks dan citra yang sudah disisipkan dengan teks terenkripsi (kriptstego).

2. METODOLOGI

2.1 Metodologi Penelitian

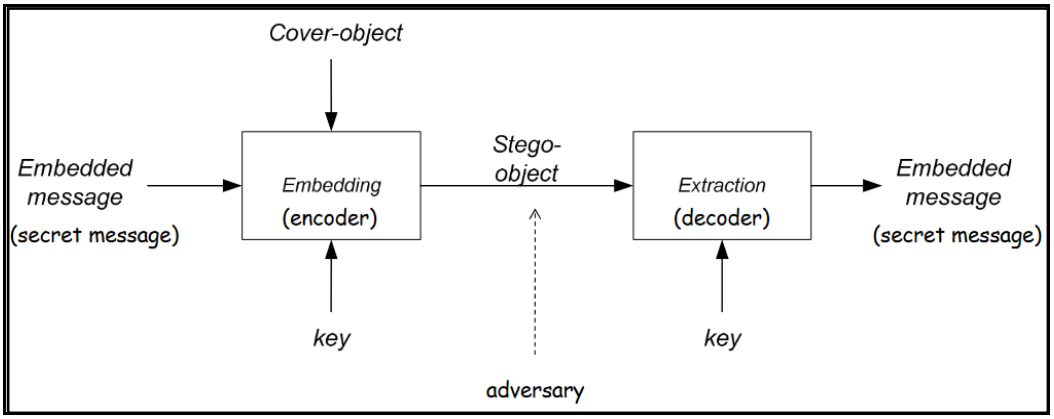
Pada penelitian ini dilakukan beberapa langkah proses dimulai dari pengumpulan data dan analisis sampai dengan proses akhir berupa pengujian dan kesimpulan. Proses penelitian dapat dilihat pada Gambar 1.



Gambar 1. Alur proses penelitian

Tahap pertama pada metodologi penelitian ini adalah fase pengumpulan data dan analisis, di mana terdapat beberapa kajian teori yang dibahas, yaitu :

a. Steganografi
   Steganografi merupakan ilmu dan seni menyembunyikan pesan rahasia dengan suatu cara sehingga tidak seorang pun yang mencurigai keberadaan pesan tersebut. Diagram proses steganografi dapat dilihat pada Gambar 2.



Gambar 2. Diagram proses steganografi

b. Kriptografi
   Kriptografi merupakan bidang keilmuan dalam mengamankan data / pesan. Pada umumnya kriptografi membuat pesan atau data menjadi tidak terbaca dengan menggunakan teknik enkripsi dan

data yang terlihat acak itu bisa di kembalikan ke data atau pesan semula dengan teknik dekripsi. Pada penelitian ini, kriptografi digunakan untuk mengacak pesan dan pesan acak tersebut disisipkan dalam sebuah gambar.

c. Algoritma RSA

Algoritma RSA merupakan algoritma asimetris di mana dibutuhkan kunci publik dan kunci rahasia untuk melakukan enkripsi / dekripsi. Pada penelitian ini, algortima RSA digunakan untuk mengenkripsi pesan sebelum pesannya disisipkan dalam sebuah gambar. Algoritma RSA merupakan algoritma asimetris yang digunakan untuk mengamankan pesan yang digunakan dalam penelitian ini yaitu algoritma RSA. Proses pembangkitan pasangan kunci pada RSA yaitu :

1. Ambil dua buah bilangan prima sembarang, p dan q.
2. Hitung $r = p*q$ (1)
   Di mana, p != q, sebab jika p = q maka $r = p^2$ (2)
   sehingga p dapat diperoleh dengan menarik akar pangkat dua dari r.
3. Hitung $\Phi(r) = (p - 1)(q - 1)$ (3)
4. Pilih kunci publik, PK, yang relatif prima terhadap $\Phi(r)$.
5. Bangkitkan kunci rahasia dengan menggunakan $SK . PK \equiv 1 \pmod{\Phi(r)}$. (4)

Perhatikan bahwa $SK*PK \equiv 1 \pmod{\Phi(r)}$ ekuivalen dengan $SK*PK = 1 + m\Phi(r)$, sehingga SK dapat dihitung dengan persamaan 5.

$SK = (1 + m\Phi(r)) / PK$ (5)

Proses enkripsi pada algoritma RSA dapat dilihat pada persamaan 6.

$y_i = x_i^{PK} \bmod r$ (6)

Di mana x_i merupakan *index* dari karakter pada pesan yang diubah ke dalam tabel ASCII.

Proses dekripsi algoritma RSA dapat dilihat pada persamaan 7.

$x_i = y_i^{SK} \bmod r$ (7)

Blok-blok m1, m2, m3, ..., diubah kembali ke bentuk huruf dengan melihat kode ASCII hasil dekripsi.

d. MITM attack

Serangan *Man-in-the-Middle* merupakan sebuah strategi yang digunakan oleh penyerang untuk memanipulasi komunikasi antara dua pihak tanpa sepengetahuan mereka. Konsep dasar serangan ini melibatkan tiga entitas: pengirim, penerima, dan penyerang yang berada di tengah-tengah keduanya. Dalam dunia digital, serangan ini dapat menyusup ke segala bentuk komunikasi *online*, dari pesan email hingga transaksi finansial. Pada penelitian ini, penyerang akan menyadap komunikasi antara keduanya lalu akan coba mengekstrak gambar yang didapatkan. Jikalau gambar berhasil di ekstraksi, karena pesan yang disisipkan terenkripsi maka penyerang harus menebak kunci untuk bisa membuka pesannya.

e. PSNR

PSNR (Peak-Signal-to-Noise-Ratio) merupakan metrik untuk mengukur kualitas (*fidelity*) citra setelah proses manipulasi. Pada PSNR membandingkan gambar asli dengan gambar yang dimanipulasi. Satuan PSNR adalah desibel (dB).

Cara melakukan pengujian PSNR:

1. Baca gambar ke dalam ruang kerja
2. Buat objek dlarray yang tidak diformat dengan data gambar
3. Tambahkan noise pada gambar
4. Buat objek dlarray yang tidak diformat dengan data gambar yang berisik
5. Hitung SNR puncak dan SNR data berisik terhadap data asli

Nilai PSNR yang lebih tinggi berarti kualitas gambar yang lebih baik. Namun, skor PSNR tidak selalu berkorelasi dengan kualitas yang dirasakan. PSNR yang dapat diterima/ditoleransi adalah jika > 30 dB.

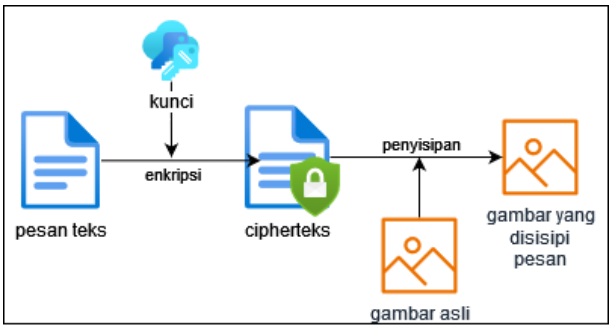
Pengujian hasil penyisipan dan enkripsi dilakukan dengan menggunakan metode PSNR. Pada gambar yang sudah disisipi pesan terenkripsi akan dibandingkan dengan gambar asli. Rumus dari PSNR bisa dilihat pada persamaan 8, sementara rumus MSE (*Means square root error*) bisa dilihat pada persamaan 9.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \tag{8}$$

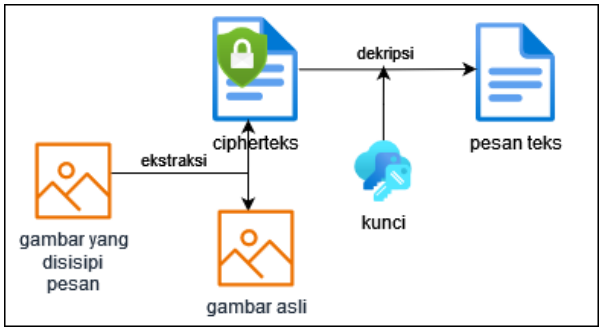
$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i,j) - g(i,j)]^2 \tag{9}$$

MSE tidak memiliki satuan sedangkan satuan dari PSNR adalah desibel (dB). Semakin mirip kedua citra maka nilai MSE semakin mendekati nilai nol. Sedangkan pada PSNR, dua buah citra dikatakan memiliki tingkat kemiripan yang rendah jika nilai PSNR di bawah 30 dB.

Tahap kedua pada metodologi penelitian ini adalah perancangan skema dari penggabungan antara kriptografi dan steganografi yang diharapkan dapat memperkuat keamanan pesan tanpa membuat kecurigaan bagi penyerang karena pesan yang terenkripsi disisipkan pada sebuah gambar. Gambaran proses antara kriptografi dan steganografi untuk enkripsi dan penyisipan dapat dilihat pada gambar 3. Sementara proses ekstraksi dan dekripsi bisa dilihat pada gambar 4.



Gambar 3. Proses penyisipan pesan terenkripsi pada gambar



Gambar 4. Proses ekstraksi dan dekripsi pesan dari gambar

Tahap ketiga merupakan pengujian skema dengan menggunakan Pengujian PSNR (*Peak Signal to Noise Ratio*) yang akan mengukur kualitas gambar dengan menghitung rasio sinyal terhadap derau puncak. Pengujian ini sering digunakan untuk mengukur kualitas rekonstruksi *codec kompresi lossy*, seperti kompresi gambar. Pada pengujian PSNR ini gambar yang digunakan dengan format .png dengan ukuran *file* 6830KB, 47KB. Percobaan dilakukan dengan berbagai panjang pesan dari 128 karakter, 256 karakter, 512 karakter, 1024 karakter dan lebih dari 1024 karakter. Pesan yang digunakan pada percobaan penelitian ini bisa dilihat pada Tabel 1.

Tabel 1. Pesan yang digunakan pada percobaan

No	Kategori	Karakteristik isi pesan
1	Pesan 1	Kombinasi huruf, angka, spesial karakter [30 karakter]
2	Pesan 2	Kombinasi alafabet dengan spasi [26 karakter]
3	Pesan 3	Kombinasi huruf, angka, spesial karakter [127 karakter]
4	Pesan 4	Kombinasi huruf, angka, spesial karakter dalam sebuah paragraf [1495 karakter]
5	Pesan 5	Kombinasi huruf, angka, spesial karakter dalam sebuah paragraf [1024 karakter]

No	Kategori	Karakteristik isi pesan
6	Pesan 6	Kombinasi huruf, angka, spesial karakter dalam sebuah paragraf [512 karakter]
7	Pesan 7	Kombinasi huruf, angka, spesial karakter dalam sebuah paragraf [256 karakter]
8	Pesan 8	Kombinasi huruf, angka, spesial karakter dalam sebuah paragraf [128 karakter]

Pada tahap ini skema yang dibangun akan diujikan dengan *Mitm attack*, dimana akan dilihat probabilitas *attack* dari penyerang yang akan berada di antara pengirim dan penerima dengan tujuan untuk mencari tahu kunci rahasia dari pengirim yang nantinya akan digunakan untuk memanipulasi data dokumen.

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

Desain dari skema yang dikembangkan terdiri dari dua *user*, yaitu pengirim dan penerima. Pada skema yang dibangun, penerima dan pengirim sudah memiliki kunci publik dari kunci *private* yang di-*generate* dari kunci publik.

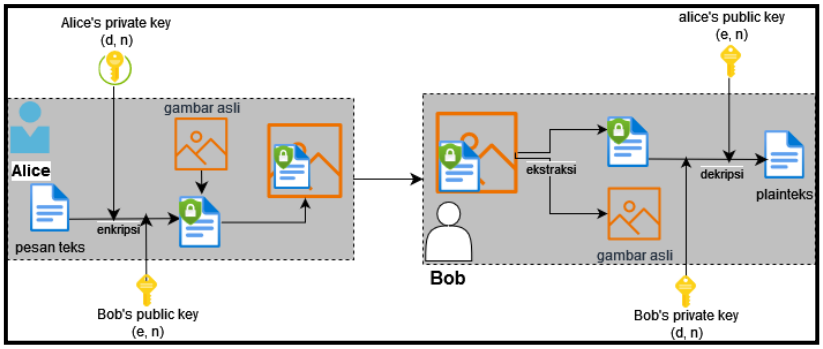
Proses yang terjadi di pengirim yaitu :

a. Pengirim membuat pesan teks dan mengenkripsinya dengan kunci *private* pengirim dan kunci publik penerima.
b. Hasil dari proses enkripsi pesan (*ciphertext*) pada poin b akan disisipkan dalam sebuah gambar.
c. Hasil dari penyisipan pesan akan dikirim ke penerima.

Sementara proses yang terjadi pada penerima yaitu :

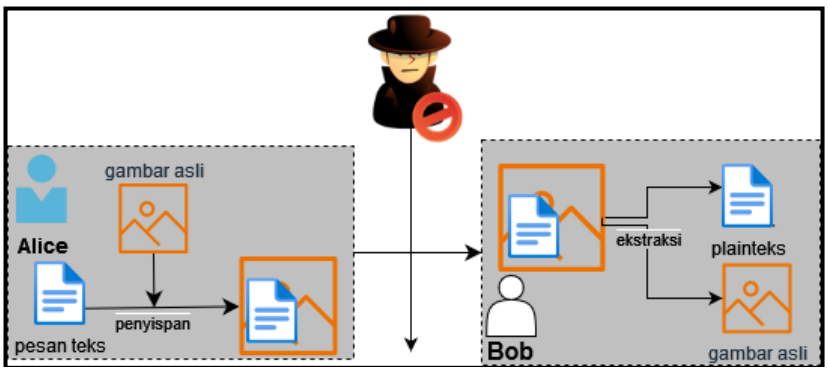
a. Penerima menerima pesan teks lalu mengekstraksi pesan sehingga menghasilkan pesan terenkripsi dan gambar sebagai media penyisipan.
b. Penerima mendekripsi pesan terenkripsi menggunakan kunci *private* penerima dan kunci publik pengirim.
c. Jika hasil pesan ter-dekripsi berhasil dipecahkan, maka penerima ter-autentikasi sebagai penerima yang sah dari pengirim yang sah.

Dari proses yang terjadi antara pengirim dan penerima, maka pada skema penyisipan pesan ini akan terjadi *mutual* autentikasi antara pengirim dan penerima yang sah. Desain skema bisa dilihat pada gambar 5



Gambar 5. Skema penyisipan dan ekstraksi pesan terenkripsi pada gambar

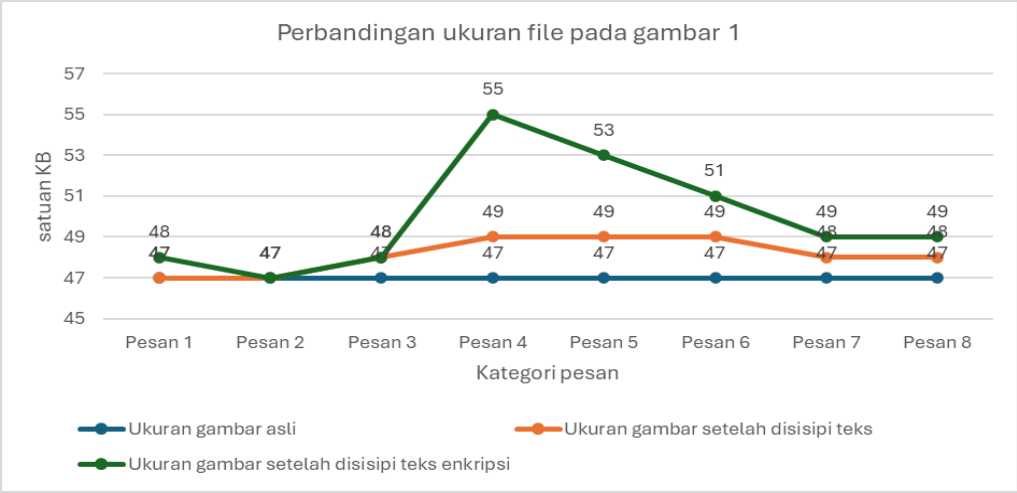
Skema *MITM attack* dapat dilihat pada gambar 6, di mana pengirim menyisipkan pesan dan di ekstraksi oleh penerima. Saat penyerang menyadap komunikasi antara pengirim dan penerima dan berhasil mengekstraksi pesan maka pesan bisa dibaca oleh penyerang dengan mudah.



Gambar 6. Skema *MITM attack* pada steganografi

3.2 Hasil

Setelah diujikan dua gambar dengan ukuran *file* yang berbeda, baik saat dilakukan penyisipan pesan dan penyisipan pesan terenkripsi. Beberapa parameter yang ditinjau diantaranya ukuran *file* sebelum dan sesudah disisipi pesan dan pesan terenkripsi, waktu penyisipan pesan dan pesan terenkripsi, waktu ekstraksi dari gambar dengan pesan dan pesan terenkripsi, dan perhitungan PSNR dari perbandingan gambar asli dengan gambar yang disisipi pesan dan gambar asli dengan gambar yang disisipi pesan terenkripsi. Gambar 7 merupakan grafik perbandingan ukuran antara gambar asli, gambar yang disisipi pesan, dan gambar yang disisipi pesan terenkripsi di mana ukuran gambar asli sebesar 47 KB. Ukuran gambar setelah disisipi pesan dan pesan terenkripsi meningkat, namun peningkatan terbesar ada pada gambar yang disisipi pesan terenkripsi sebesar 15% dengan panjang pesan lebih dari 1024 karakter.

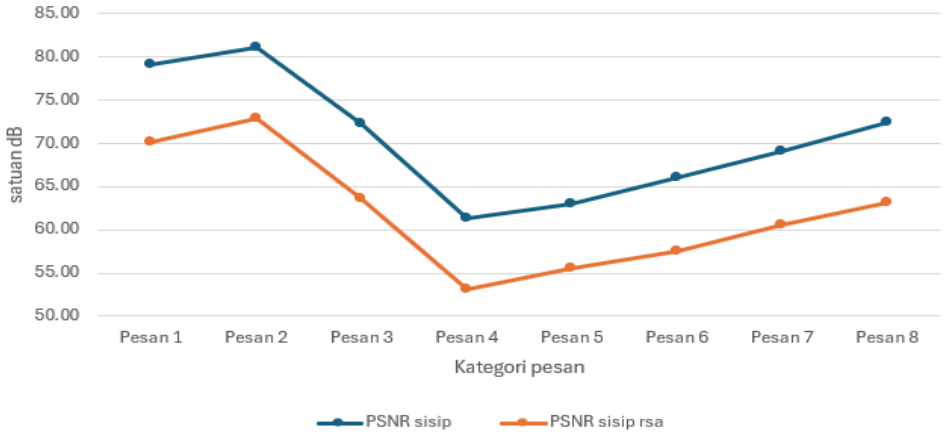


Gambar 7. Perbandingan ukuran gambar asli, dan gambar yang disisipi pada gambar pertama

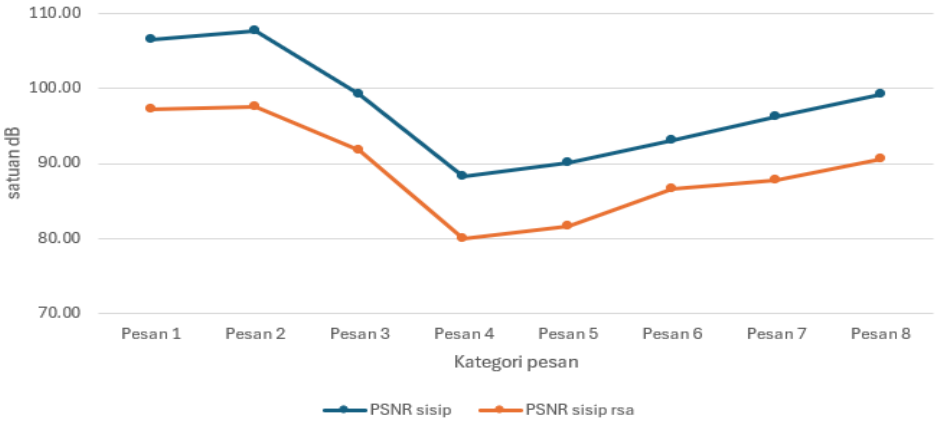
Gambar 8 merupakan grafik perbandingan ukuran antara gambar asli, gambar yang disisipi pesan, dan gambar yang disisipi pesan terenkripsi di mana ukuran gambar asli sebesar 6.830 KB. Grafik pada "Gambar 7 dan 8" menunjukkan peningkatan ukuran gambar terbesar terjadi pada penyisipan pesan terenkripsi dengan panjang karakter lebih dari 1024. Pada pengujian dengan ukuran gambar 47 KB ukuran gambar meningkat sekitar 15% dari ukuran gambar aslinya sementara pada pengujian dengan ukuran gambar 6.830 KB ukuran gambar meningkat sekitar 0.2% dari ukuran gambar aslinya. Peningkatan ukuran gambar ini dipengaruhi oleh ukuran gambar aslinya.

Gambar 8. Perbandingan ukuran gambar asli, dan gambar yang disisipi pada gambar kedua

Sementara hasil perhitungan PSNR dengan gambar berukuran 47 KB yang dapat dilihat pada "Gambar 9 dan 10" menunjukkan bahwa hasil PSNR pada penyisipan pesan terenkripsi lebih rendah dari pada penyisipan pesan. Namun nilai PSNR pada penyisipan masih lebih dari 30dB yang berarti kualitas gambar hasil penyisipan menyerupai kualitas gambar aslinya.



Gambar 9. Perbandingan PSNR pada gambar berukuran 47 KB



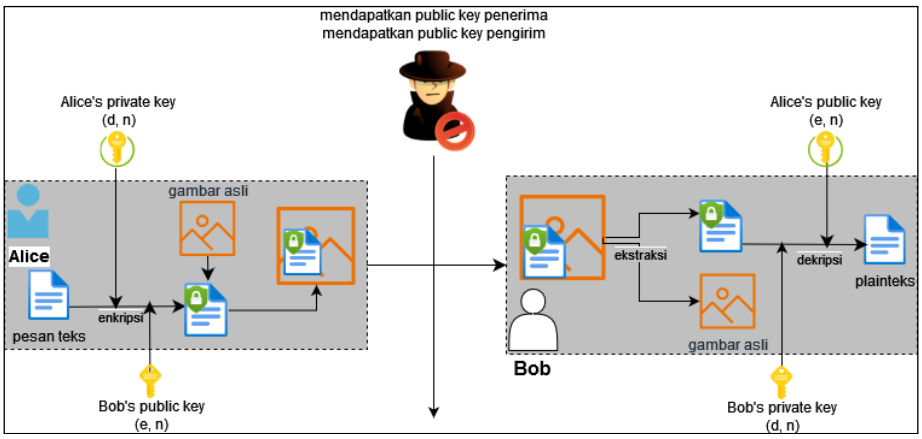
Gambar 10. Perbandingan PSNR pada gambar berukuran 6.830 KB

Hasil pengujian dengan skema *MITM attack* Gambar 6 menunjukkan saat penyerang menyadap komunikasi antara penerima dan pengirim lalu berhasil mendapatkan gambar yang sudah disisipi pesan, dan berhasil mengekstraksi gambarnya maka penyerang kana mendapatkan isi pesannya. Namun dengan melakukan enkripsi pada pesan yang disisipkan, saat gambar yang disisipkan pesan terenkripsi disadap oleh pihak yang tidak bertanggung jawab, maka butuh keahlian lebih untuk penyerang bisa mengetahui isi pesannya karena saat gambar bisa diekstraksi, penyerang harus melakukan dekripsi pesan agar pesan bisa terbaca. Pengujian skema *MITM attack* pada pesan terenkripsi dapat dilihat pada gambar 11.

Dengan menambahkan teknik kriptografi pada skema penyisipan pesan yang bisa dilihat pada Gambar 11, hal ini dapat mempersulit penyerang untuk mendapatkan pesan aslinya saat penyerang berhasil melakukan proses ekstraksi. Peluang untuk mendapatkan kunci rahasia pengirim dengan *brute force* adalah $1/2^{l}$ di mana l merupakan panjang kunci rahasia pengirim. Proses untuk menebak kunci rahasia pengirim bisa dilihat pada persamaan 10.

$$\text{Priv\_key'} = 1 \qquad (10)$$
$$\text{Pub\_key\_alice, Pub\_key\_bob}$$
$$\text{plainteks} = \{\{M\}_{\text{pub\_key\_alice}}\}_{\text{Priv\_key'}}$$

```
while plainteks == 0 {
        Private_key'= Private_key' + 1
        plainteks = {{M}pub_key_alice}Priv_key'
}
```



Gambar 11. Skema pengujian penyisipan pesan terenkripsi pada gambar dengan *MITM attack*

4. KESIMPULAN

Pada penelitian ini, hasil pengujian PSNR pada gambar 9 dan gambar 10 menunjukkan bahwa gambar yang disisipkan pesan terenkripsi menghasilkan nilai diatas 50 dB yang berarti tingkat kemiripan yang tinggi dari gambar hasil rekonstruksi dengan gambar aslinya. Ukuran *file* sangat berpengaruh terhadap tampungan dari penyisipan pesan yang terenkripsi, pada gambar 7 dan gambar 8 menunjukkan jika ukuran gambar meningkat baik pada gambar berukuran 47 KB dan gambar berukuran 6.830 KB saat menyiapkan *file* terenkripsi. Namun ukuran gambar meningkat 15% pada gambar yang berukuran 47 KB saat disisipi pesan terenkripsi dengan panjang karakter lebih dari 1024 karakter, namun pada gambar berukuran 6.830 KB peningkatan ukuran gambar paling besar saat disisipi pesan terenkripsi dengan Panjang karakter lebih dari 1024. Peningkatan ukuran gambar sekitar 0.2% besar ukuran gambar yang digunakan untuk menampung penyisipan pesan dan kombinasi karakter pada pesan yang disisipkan sangat berpengaruh terhadap ukuran *file* hasil penyisipan. Dari sisi keamanan skema, dengan

penambahan teknik kriptografi pada penyisipan pesan dengan algoritma RSA memberikan dampak pada peningkatan keamanan pesan yang disisipkan pada gambar di mana probabilitas penyerang untuk bisa menebak pesan terenkripsi pada gambar sebesar $1/2^{l}$ di mana l merupakan panjang kunci yang bisa ditebak pada skema yang dibangun hal ini akan mempersulit penyerang untuk mengambil isi pesan yang sudah ter-ekstraksi karena harus dilakukan proses dekripsi dengan menggunakan kunci rahasia pengirim. Untuk penelitian selanjutnya diharapkan format *file* gambar yang digunakan bisa lebih bervariasi sehingga bisa mengakomodasi kebutuhan pengguna.

DAFTAR PUSTAKA

[1] W. Stalling, *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall Press, 2013.

[2] R. Indra Perwira, D. Boedi Prasetyo, dan F. Ahmad Juni Haryanto, "Steganografi dengan AES Pada Media Suara Berbasis Internet. *Telematika: Jurnal Informatika dan Teknologi Informasi*, 2020, 17.1: 18-25.

[3] E. Saragih, D. Siregar, dan H. Dafitri, "Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB", *Jurnal SAINTIKOM (Sains Manajemen Informatika dan Komputer)*, vol. 22, no. 2, hlm. 464–473, 2023, [Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/index.php/jis/index

[4] N. Setiawan dan L. Tanti, "Kerahasiaan Teks Yang Disisipkan Ke Dalam Gambar Menggunakan Metode Porta Dan LSB", *Jurnal ITCC (Information Technology and Cyber Crime)*, vol. 1, no. 1, hlm. 52–58, 2022.

[5] F. Kurniasih *dkk.*, "Penggabungan Affine Cipher dan Least Significant Bit-2 untuk Penyisipan Pesan Rahasia pada Gambar", *Jurnal Eurematika*, 2023. [Daring]. Tersedia pada: https://ejournal.upi.edu/index.php/JEM

[6] B. J. Simbolon, "Steganografi Penyisipan Pesan pada File Citra dengan Menggunakan Metode LSB (Least Significant Bit)", *Jurnal. Nasional Komputasi dan Teknologi Inf.*, vol. 4, no. 1, hlm.1–6, 2021, doi: 10.32672/jnkti.v4i1.2656.

[7] D. Laksmiati, "Implementasi Steganografi Image Processing dan Enkripsi,", *Jurnal AKRAB JUARA*, vol. 6, no. 1, hlm. 30–40, 2021.

[8] R. R. Santosa, A. R. Pamungkas, and M. K. F. Zuhri, "Pengamanan Email melalui Steganografi Penerapan One Time Pad dan Metode LSB pada Gambar Lampiran," *Pros. SAINTEK Sains dan Teknologi*, vol. 3, no. 1, hlm. 123–132, 2024.

[9] Z. Nabil, A. T. Putra, dan A. Prihanto, "Penerapan Steganografi dengan Menggunakan Metode Least Significant Bit (Lsb) Dan Pixel Value Differencing (Pvd) Pada Citra Warna". *Jurnal Informatics Computer Science*, vol. 01, no. 04, hlm. 165–173, 2020, doi: 10.26740/jinacs.v1n03.p165-173.

[10] L. P. Malese, "Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)", *Jurnal Ilmu Wahana Pendidik.*, vol. 7, no. 5, hlm. 343–354, 2021, doi: 10.38101/sisfotek.v11i1.351.

[11] Detina, Hurin In Liaf, dkk., "Steganografi: Keamanan Data Dengan Metode Least Significant Bit Menggunakan Python." *Jurnal Riset Sistem Informasi dan Teknologi Informasi (JURSISTEKNI),* vol. 6, no. 2, 439-447, 2024.

[12] G. Miftakhul Fahmi, K. Nur Isnaini, dan D. Suhartono, "SINTECH Journal | 47 Implementasi Steganografi Gambar Menggunakan Algoritma Generative Adversarial Network", [Daring]. Tersedia pada: https://doi.org/10.31598

[13] E. Saragih, D. Siregar, dan H. Dafitri, "Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer) Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB", [Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/index.php/jis/index

[14] R. Davia, A. Huday, dan S. Waluyo, "Pengamanan File Rekam Medis Pada Puskesmas Larangan Utara Menggunakan Algoritma Kriptografi Rsa Berbasis Web," 2022.

[15] A. Dharmawan dan H. Munandar, "Penerapan Algoritme Kriptografi Sha-256 Dan Aes-256 Untuk Pengamanan File Pada Pt Pelangi Sentral Kreasi", *SENAFTI*, vol. 2, no. 2, 2023. [Daring]. Tersedia pada: | https://senafti.budiluhur.ac.id/index.php/senafti/index

[16] M. Azhari, J. Perwitosari, dan F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, hlm. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[17] W. Catur, U. Putri, R. Marwati, dan S. M. Gozali, "Penggabungan Kriptografi Rivest Shamir Adleman (RSA) Dan Advanced Encryption Standard (AES) Pada Aplikasi Pengirim E-Mail," vol. 3, no. 2, hlm. 92–101, 2023.

[18] A. Hermawan, E. Iman, dan H. Ujianto, "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," vol. 5, no. 2, 2021, doi: 10.30743/infotekjar.v5i2.3585.

[19] I. A. Darmawan, "Kriptografi Algoritma RSA Untuk Pengamanan Database Berbasis Java Dekstop Pada SMA Muhammadiyah 15 Jakarta Barat," 2018.

[20] W. Catur, U. Putri, R. Marwati, dan S. M. Gozali, "Penggabungan Kriptografi Rivest Shamir Adleman (RSA) dan Advanced Encryption Standard (AES) Pada Aplikasi Pengirim E-Mail," vol. 3, no. 2, hlm. 92–101, 2023.

[21] Y. Pratama Putra, F. Nuraeni, R. Ajji Jatnika, P. Studi Teknik Informatika, dan S. Tasikmalaya, "Implementasi Kriptografi Dalam Pengamanan Database E-Voting Menggunakan Algoritma Rsa Dan Base64 Berbasis Progresive Web Apps (Studi Kasus: Pemilihan Presiden Mahasiswa STMIK Tasikmalaya)," 2021.

[22] A. Cahya Putra dan M. Simanjuntak, "Penerapan Algoritma Rivest Shamir Adleman (RSA) Untuk Mengamankan Database Program Keluarga Harapan (PKH)," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 5, no. 1, 2021.

[23] O. F. Abdelwahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, dan A. A. M. Khalaf, "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data," dalam *Procedia Computer Science*, Elsevier B.V., 2021, hlm. 5–12. doi: 10.1016/j.procs.2021.02.002.

[24] F. Farhan dan D. Leman, "Implementasi Metode Rivest Shamir Adleman (RSA) Untuk Kerahasiaan Database Perum Bulog Kanwil SUMUT," *Journal of Machine Learning and Data Analytics (MALDA)*, vol. 02, no. 01, hlm. 18–27.