Vol. 5, No. 1, April 2024, hal. 36-41

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital

Aqilah Syaima' Fadel[1], Rianto David Saputra[2], Risky Nanda Putra[3], Yulia Fatma[4]
Email: [1]210401119@student.umri.ac.id, [2]210401114@student.umri.ac.id, [3]210401260@student.umri.ac.id

[1234]Teknik Informatika, Ilmu Komputer, Universitas Muhammadiyah Riau

Diterima:06 Februari 2024 | Direvisi: - | Disetujui: 28 April 2024

Abstrak
Perkembangan teknologi yang cepat membuka kemungkinan bagi pihak-pihak tidak berkepentingan untuk mengekstraksi pesan dari media cover. Oleh karena itu, diperlukan langkah-langkah keamanan tambahan untuk melindungi pesan yang disembunyikan. Penelitian sebelumnya telah mengusulkan penggabungan teknik steganografi dan kriptografi. Kriptografi, sebagai teknik untuk mengamankan pesan, dapat diklasifikasikan menjadi modern dan klasik berdasarkan waktu kemunculannya. Jenis kuncinya meliputi kriptografi simetris dan asimetris dengan beberapa algoritma populer seperti Rivest Cipher 4 (RC4), Data Encryption Standard (DES), dan Advanced Encryption Standard (AES). Steganografi yang merupakan seni dan ilmu menyembunyikan pesan, menjadi penting untuk menjaga kerahasiaan dan keamanan data dan informasi. Meskipun kelebihan pengiriman data melalui internet, terdapat kelemahan seperti kejahatan siber, termasuk penyadapan dan perubahan data. Metode Least Significant Bit (LSB) adalah strategi terkenal dalam steganografi, terutama dengan menggunakan LSB dari data piksel gambar. Metode ini memberikan keamanan tinggi dan dapat menyesuaikan teknik penyematan tanpa kehilangan informasi akibat kompresi dan perubahan yang tidak terlihat dalam steganografi gambar. Pentingnya menggunakan format kompresi tanpa kehilangan (lossless) saat menggunakan metode LSB diilustrasikan dalam kompresi stego image. Penggunaan format kompresi yang mengalami kehilangan (lossy) dapat mengakibatkan kehilangan pesan rahasia. Meskipun steganografi LSB umum digunakan karena kesederhanaannya, metode ini rentan terhadap deteksi oleh algoritma analisis steganografi yang canggih. Penelitian ini menyoroti keterbatasan dalam kapasitas penyembunyian informasi dan risiko keamanan yang perlu mendapatkan perhatian.
Kata kunci: *lsb, steganografi, kriptografi*

Security analysis of text steganography using the least significant bit (lsb) method in digital images.

Abstract
The rapid development of technology makes it possible for unauthorized parties to extract messages from cover media. Therefore, additional security measures are required to protect the hidden message. Previous research has proposed combining steganography and cryptography techniques. Cryptography, as a technique for securing messages, can be classified into modern and classical based on the time it emerged. The key types include symmetric and asymmetric cryptography with some popular algorithms such as Rivest Cipher 4 (RC4), Data Encryption Standard (DES), and Advanced Encryption Standard (AES). Steganography, which is the art and science of hiding messages, is important for maintaining the confidentiality and security of data and information. Despite the advantages of sending data over the internet, there are disadvantages such as cybercrime, including eavesdropping and data alteration. The Least Significant Bit (LSB) method is a well-known strategy in steganography, mainly by using the LSBs of image pixel data. This method provides high security and can customize embedding techniques without information loss due to compression and invisible changes in image steganography. The importance of using a lossless compression format when using the LSB method is illustrated in stego image compression. The use of compression formats that suffer from loss (lossy) can result in the loss of the secret message. Although LSB steganography is commonly used due to its simplicity, it is vulnerable to detection by sophisticated steganographic analysis algorithms. This research highlights the limitations in information hiding capacity and security risks that need attention.
Keywords: *lsb, steganography, cryptography*

1. PENDAHULUAN

Perkembangan teknologi yang sangat cepat tidak menutup kemungkinan pihak-pihak yang tidak berkepentingan dapat mengekstraksi pesan dari media cover. Oleh karena itu, diperlukan pengamanan lebih pada pesan yang disembunyikan. Pada beberapa penelitian sebelumnya telah banyak diusulkan kombinasi teknik steganografi dan kriptografi [1].

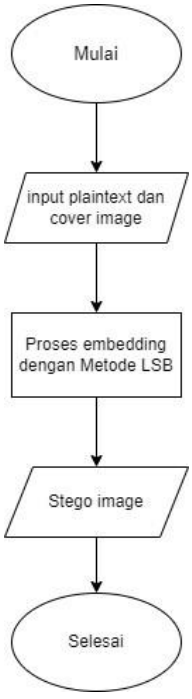
Kriptografi adalah salah satu teknik yang dapat digunakan untuk mengamankan pesan melalui penerapan algoritma. Algorita kriptografi dapat diklasifikasikan berdasarkan waktu kemunculannya yaitu modern dan klasik. Menurut jenis kunci, kriptografi terbagi menjadi bentuk kriptografi simetris dan asimetris. Beberapa algortima yang populer dalam kirptografi adalah Rivest Cipher 4 (RC4), Data Encryption Standard (DES), Advanced Encryption Standard (AES) [2].

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga tidak ada pihak ketiga selain si pengirim dan si penerima yang mengetahui adanya suatu pesan rahasia. Masalah kerahasiaan dan keamanan merupakan komponen penting dari suatu data dan informasi. Pengiriman dan penerimaan data dan informasi melalui jaringan internet memang memiliki banyak kelebihan salah satunya adalah kecepatan dalam proses transmisi, akan tetapi dilain sisi pengiriman melalui jaringan internet mempunyai kelemahan yaitu kejahatan internet (cyber-crime) seperti penyadapan, perubahan data dan lainnya [3]

2. METODE PENELITIAN

2.1 Tahapan penelitian

Metode penelitian adalah proses yang dilakukan untuk dapat menghasilkan sebuah penelitian yang terstruktur dan sistematis serta memberikan hasil penelitian yang sesuai.

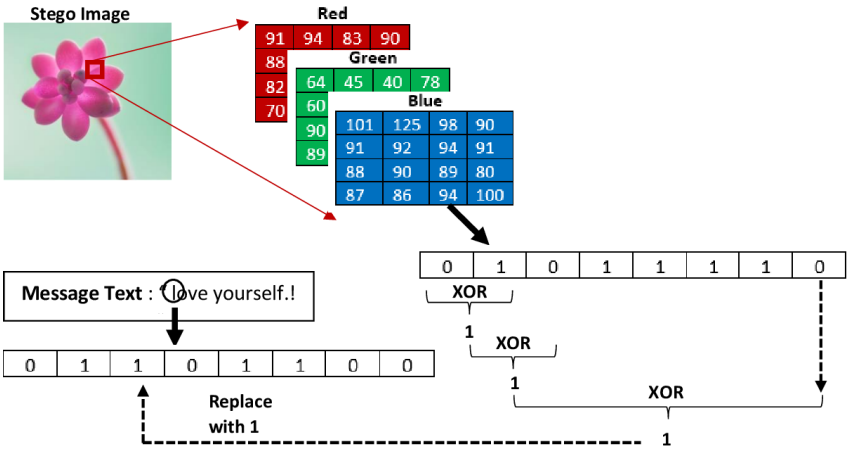


- Input plaintext dan cover image
  Tahapan ini adalah proses awal untuk melakukan steganografi dengan memasukkan sebuah teks atau file teks yang kemudian akan di sisipkan kedalam cover image
- Proses *embedding* dengan metode LSB
  Tahapan ini adalah proses perhitungan LSB yang dilakukan pada cover image yang telah disisipi teks atau file teks sebagai data inputan.
- Stego Image
  Tahapan ini adalah output akhir pada proses steganografi yang dilakukan dengan metode LSB. Stego image merupakan gambar yang menjadi cover Dimana gambar tersebut berisi pesan teks yang telah disisipkan sebelumnya.
- Kesimpulan
  Kesimpulan adalah tahapan akhir yang berisi hasil dari penelitian yang dilakukan. Kesimpulan menjelaskan apakah penelitian tersebut efektif atau tidak.

2.2 *Least Significant Bit (LSB)*

Metode Least Significant Bit (LSB) adalah salah satu strategi yang terkenal dan banyak diterapkan untuk steganografi. Selain itu, teknik teknik yang menonjol untuk steganografi saat ini adalah dengan menggunakan LSB dari data piksel gambar. Dalam steganografi berbasis LSB itu adalah diperlukan untuk mengganti semua bit rahasia dengan bit piksel LSB dari objek cover, baik itu gambar, audio, video, dan lainnya. LSB menyematkan panjang xed-length bit rahasia dalam LSB piksel dengan panjang xed-length komparatif [4]. LSB sebagai cara sederhana untuk menyematkan bit yang memberikan keamanan tinggi dan mengubah teknik penyematan tinggi tanpa takut kehilangan informasi akibat kompresi dan perubahan yang tidak terlihat dalam steganografi gambar [5].

Metode LSB harus menggunakan format *lossless compression* Ketika melakukan kompresi pada stego image, karena metode ini menggunakan bit-bit pada setiap piksel pada image. Jika digunakan format *lossy compression*, pesan rahasia yang disembunyikan dapat hilang. Jika digunakan image 24 bit color sebagai cover, sebuah bit dari masing-masing komponen Red, Green, dan Blue, dapat digunakan sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah image 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 bytes) data rahasia [6].



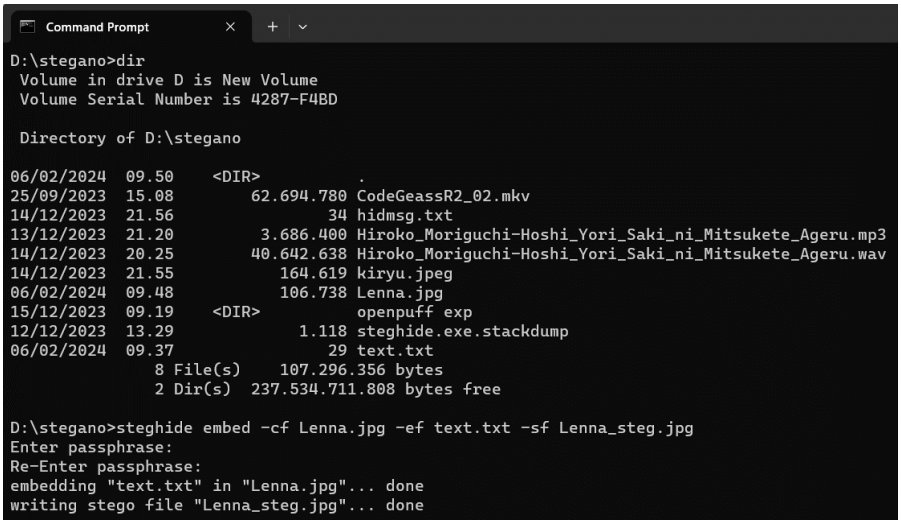
Gambar 1. Perhitungan LSB

3. HASIL DAN PEMBAHASAN

Hasil yang diperoleh didapat dari pengujian terhadap tools steganografi '*Steghide'*.Caranya dengan menyisipkan pesan atau text pada *cover image* melalui commandprompt pada laptop. Untuk Teknik steganografi ini dilakukan dengan algoritma kriptografi Rijndael.

3.1. Penyisipan pesan

Dengan menggunakan metode LSB pada teknik Steganografi, berikut contoh inputan pesan dan proses penyisipan pesan pada gambar. Perhatikan gambar dibawah ini.



Gambar 2. CMD untuk embedding pesan

Pada instruksi di atas kita ingin menyisipkan pesan (**text.txt**) pada sebuah gambar cover (**Lenna.jpg**) yang nantinya akan disimpan dalam stegofile bernama **Lenna_steg.jpg**, pada saat encode ini kapasitas pada file gambar cover akan berubah tergantung seberapa banyak karakter pesan yang disisipkan.

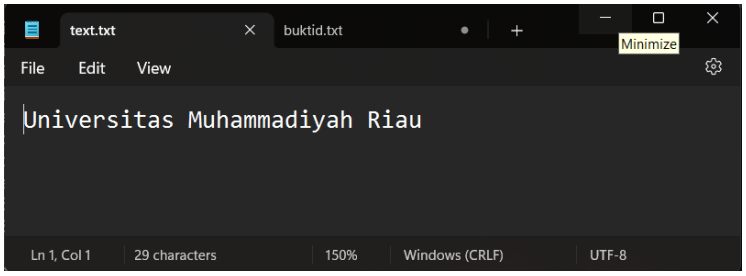
Proses penyisipan pesan berhasil, dan stego file disimpan di folder yang sama dengan gambar asli. Berikut ini adalah perbandingan gambar asli dan stego image:

Gambar 3. Gambar original (Lenna.jpg)

Gambar 4. Stego Image (Lenna_steg.jpg)

Hasil Stegano Image

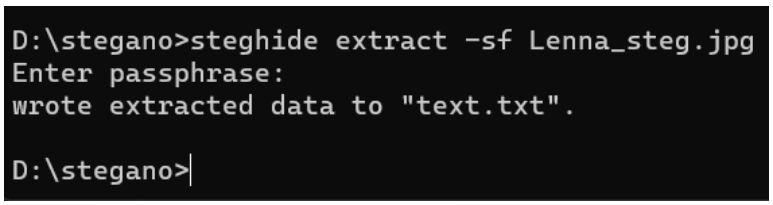
Sekilas pada gambar di atas tidak terlihat perbedaan yang kentara, namun sebelumnya kita telah menyisipkan sebuah pesan di stego image, ini adalah pesan yang disisipkan:



Gambar 5. Pesan yang disisipkan kedalam cover image

3.2. Ekstraksi pesan

Setelah kita meng-encode pesan kedalam cover image, lalu kita akan men-decode pesan tersebut

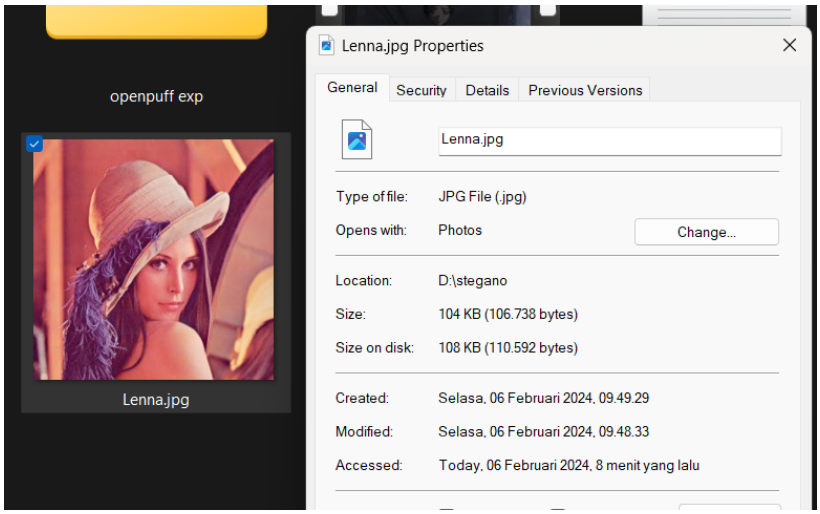


Gambar 6. Proses decode pesan dari stego image

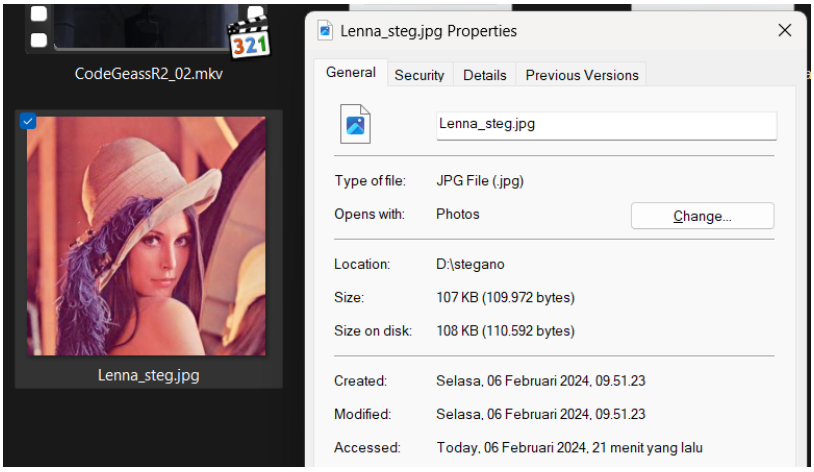
Pesan berhasil di ekstrak.

3.3 Perbandingan Citra

Perbandingan citra dilakukan dengan melihat ukuran gambar yang asli dengan gambar yang sudah dilakukan steganografi. Berikut gambar dibawah merupakan perbandingan metadata antara gambar original dengan stego image.



Gambar 7. Ukuran byte pada gambar original



Gambar 8. Ukuran byte pada stego image

Gambar 7 adalah gambar asli yang belum dilakukan embedding teks, jika dibandingkan dengan Gambar 8 ukurannya berubah dari 106.738 bytes menjadi 109.972 bytes. Hal ini menunjukkan bahwa setiap karakter pesan yang di sisipkan kedalam sebuah gambar akan mempengaruhi ukuran gambar tersebut meski tidak terlalu signifikan.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan penulis mengenai steganografi LSB pada citra digital ialah bisa menyisipkan pesan rahasia kedalam sebuah gambar. Steganografi LSB adalah teknik penyembunyian informasi dalam media digital dengan memanfaatkan bit-bit paling tidak signifikan dalam data, seperti gambar. Dengan mengganti nilai-nilai bit paling tidak signifikan

dalam piksel-piksel gambar, informasi tambahan dapat disisipkan tanpa mengganggu penampilan visual secara signifikan. Meskipun umum digunakan karena sederhana, metode ini rentan terhadap deteksi oleh algoritma analisis steganografi yang canggih, serta memiliki keterbatasan dalam kapasitas penyembunyian informasi dan risiko keamanan yang perlu diperhatikan

DAFTAR PUSTAKA

[1] I. Riadi, S. Sunardi, and D. Aryanto, "Steganografi Video Digital dengan Algoritma LSB (Least Significant Bit) dan Rijndael," *J. Innov. Inf. Technol. Appl.*, vol. 2, no. 02, pp. 127–134, 2020, doi: 10.35970/jinita.v2i02.361.

[2] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher," *J. Masy. Inform.*, vol. 14, no. 1, pp. 16–28, 2023, doi: 10.14710/jmasif.14.1.51484.

[3] M. O. Abdillah, O. A. Pane, and F. R. A. Lubis, "Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB)," *J. Sains dan Teknol.*, vol. 3, no. 1, pp. 40–46, 2023, doi: 10.47233/jsit.v3i1.482.

[4] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method," *IEEE Access*, vol. 10, no. November, pp. 124053–124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

[5] S. D. Muyco and A. A. Hernandez, "Least significant bit hash algorithm for digital image watermarking authentication," *ACM Int. Conf. Proceeding Ser.*, pp. 150–154, 2019, doi: 10.1145/3330482.3330523.

[6] Irfan, "Penyembunyian Informasi (steganography) Gambar Menggunakan Metode LSB (Least Significant Bit)," *Rekayasa Teknol.*, vol. 5, no. 1, 2017, doi: 10.1088/0031-9120/20/3/307.