Jurnal Quancom
Vol.x, No.x, Juli 202x, pp. xx~xx
e-ISSN: -
P-ISSN: -

IMPLEMENTASI STEGANOGRAFI DENGAN METODE ALGORITMA LEAST SIGNIFICANT BIT UNTUK MENYISIPKAN PESAN TEKS PADA GAMBAR

Lamria Sitorus [1], William Panjaitan [2], Inggrid Pardede [3]
[1,2,3] Teknologi Rekayasa Perangkat Lunak, Institut Teknologi Del
lamriaa04@gmail.com[1] , 20williampanjaitan@gmail.com[2] , inggridpardede72@gmail.com [3]

* Corresponding

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

Digital Image, Embedding, Extraction, Least Significant Bit, Steganography.

ABSTRACT

Steganography is an art in hiding data information in a media that is not suspicious where only the intended person knows the information. One of the popular steganography techniques is the Least Significant Bit (LSB) which is often used to hide confidential information into digital files such as images, audio, and even video. This research will produce an implementation of steganography with the LSB method to insert text into images that will provide protection for secret messages without reducing or damaging the visual quality of the image. This technique will take the least important bit which will then be given a text message insertion. In the process of inserting messages with this method, binary message data will be inserted into the bits on each color component (Red, Green, Blue) in the image pixels sequentially. Then the extraction process will be carried out in retrieving the message that was previously inserted into the digital image. Based on the implementation results, it shows that the LSB method has a high success rate in inserting text messages without any difference between the original image and the steganography results. Then the text can also be extracted as long as there has been no modification process on the image. The results of this implementation will further provide an overview that steganography techniques can be the best solution for simple but efficient data protection.

PENDAHULUAN

Perkembangan teknologi dan komunikasi di jaman ini begitu pesat, salah satu manfaat yang terasa adalah saling bertukar data maupun informasi begitu cepat. Data atau informasi ada yang bersifat umum, yang artinya bisa dilihat atau diakses oleh banyak orang. Ada juga informasi yang bersifat pribadi atau rahasia, yang artinya tidak boleh dilihat oleh banyak orang, hanya orang tertentu yang bisa mengaksesnya [1]. Saat ini sudah banyak ancaman yang terjadi terhadap privasi dan keamanan data maka dari itu kebutuhan untuk melindungi informasi menjadi semakin penting dan harus dilakukan penerapannya. Keamanan data menjadi salah satu hal yang perlu disorot, terutama dalam mencegah pengaksesan informasi yang sensitif oleh pihak yang tidak berkepentingan.

Beberapa modus kejahatan terkait dengan keamanan komputer dan kerahasiaan dalam pertukaran data informasi secara elektronik atau media internet cukup banyak, diantaranya modus tersebut adalah: interruption dimana serangan dilakukan dengan merusak data, interception dimana ancaman dari pihak yang tidak berhak memperoleh akses untuk mengambil data atau informasi [2]. Ancaman seperti ini menimbulkan kekhawatiran saat mengirimkan dan menerima pesan rahasia. Oleh karena itu, faktor keamanan dan kerahasiaan menjadi aspek utama dalam suatu proses mengirim dan menerima pesan, data, atau informasi.

Sebagai solusi dari permasalahan ini, penerapan sistem keamanan data akan dibangun dengan menggunakan steganografi dengan metode LSB.

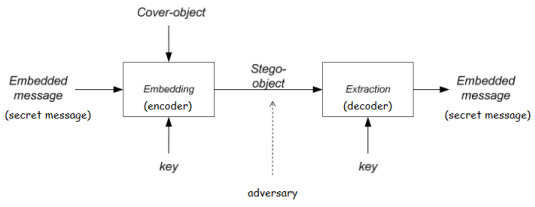
METODE

Pada bagian ini akan dijelaskan langkah sistematis yang digunakan dalam pengimplementasian algoritma least significant bit (LSB) sebagai metode steganografi dalam menyisipkan pesan teks pada gambar digital.

A. Metode yang digunakan

Salah satu metode yang digunakan untuk melindungi informasi atau data adalah menggunakan metode steganografi. Kata steganografi (steganography) berasal dari bahasa yunani steganos yang berarti "tersembunyi/terselubung" dan graphien "menulis" sehingga kurang lebih artinya "menulis (tulisan) terselubung" [3]. Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan informasi di dalam sebuah gambar. Steganografi membutuhkan dua properti yaitu media penampung dan data rahasia yang akan disembunyikan [4]**.** Steganografi sudah digunakan sejak dahulu kala sekitar 2500 tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi [5]. Sekarang steganografi sudah terdiri atas beberapa bagian dimana penyisipannya sudah dapat dilakukan pada gambar, teks, audio, video, bahkan jaringan. Steganografi adalah cara komunikasi rahasia dengan menyembunyikan pesan pada objek yang tidak terlihat mencurigakan atau berbahaya.

Tujuan dari steganografi adalah untuk merahasiakan atau menyembunyikan keberadaan sebuah teks penting yang bahkan yang bersifat rahasia. Maka akan membutuhkan dua aspek yaitu media penyimpan dan informasi rahasia yang akan disembunyikan [6]. Pada pengimplementasian kebanyakan teks tersebut akan disembunyikan dengan hanya terjadi sedikit perubahan sehingga tidak akan menimbulkan kecurigaan para penyerang. Komponen dari sistem penyisipan ini yaitu terdapat komponen untuk menuliskan pesan yang dipakai untuk menempatkan penulisan pesan rahasia [7]. Steganografi melibatkan dua buah proses utama yaitu penyisipan (*embedding*) dan penguraian (*extraction*) [8]. Proses *embedding* adalah langkah menyisipkan pesan ke dalam media *cover*, sedangkan *extraction* adalah proses untuk mengambil kembali pesan dari media *stego*.



Gambar 1. Proses embedding dan extraction

Steganografi merupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya [9]. Kelebihan steganografi dibandingkan dengan kriptografi bahwa semua pesan yang telah disisipkan atau disembunyikan tidak akan menarik perhatian orang lain. Teknik ini sering digunakan untuk meningkatkan keamanan informasi dalam komunikasi, terutama dalam situasi di mana deteksi pesan tersembunyi dapat mengakibatkan risiko besar. Dengan menjaga tampilan media penampung tetap terlihat normal, steganografi menjadi alat yang efektif dalam perlindungan data rahasia. Dalam perkembangan ilmu steganografi sekarang ini, terdapat berbagai macam metode yang dapat digunakan untuk menyembunyikan pesan tersebut [10]**.** Salah satu contohnya adalah metode least significant bit (LSB).

Pada penelitian ini penyisipan pesan dalam steganografi dapat menggunakan teknik least significant bit (LSB). Dimana teknik ini menggunakan bit bit terkecil dalam representasi digital pada setiap komponen warna (red, green, dan blue) dari piksel gambar dengan data biner dari pesan yang akan disisipkan. Proses ini dilakukan secara berurutan sehingga pesan tersembunyi dapat disimpan secara efisien tanpa mengurangi kualitas visual dari gambar tersebut. Proses penyisipan juga membutuhkan sebuah perhitungan menggunakan metode dan harus memiliki jenis objek yang akan dijadikan wadah penyisipan data teks [11] seperti gambar digital.

Hasil dari implementasi ini menunjukkan bahwa metode LSB mampu menyisipkan pesan teks dengan tingkat keberhasilan yang tinggi. Gambar hasil steganografi hampir tidak dapat dibedakan dari gambar asli, sehingga membuat teknik ini sangat efektif untuk menjaga kerahasiaan pesan. Selain itu, pesan yang disisipkan juga dapat diekstraksi kembali selama gambar tidak mengalami proses modifikasi. Pada penelitian ini juga terdapat beberapa metode pengukuran kualitas gambar.

Least significant bit (LSB)

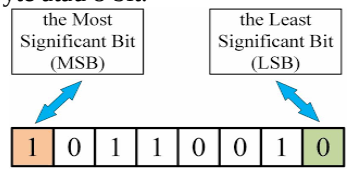
Metode yang digunakan yaitu least significant bit (LSB). Metode ini banyak digunakan karena tidak terlalu kompleks dan pesan yang disembunyikan cukup aman. [12]

Least significant bit (LSB) adalah metode steganografi yang menyembunyikan data rahasia dengan merubah bagian dari bit terendah dari komponen data digital seperti gambar, audio, dan juga video. Steganografi membutuhkan dua properti, yaitu data dan wadah penampung data. Wadah penampung yang umumnya digunakan berupa teks, suara, gambar, atau video. Sedangkan data yang disembunyikan dapat berupa teks, gambar, atau data yang lainnya. [13]**.**

Perubahan pada bit setiap gambar hampir tidak terlihat oleh manusia karena menggunakan bit paling tidak signifikan terhadap nilai keseluruhan data. Ini merupakan metode yang tidak terlalu kompleks, penyimpanan pesan pada cover object juga cukup besar. Dasar metode ini adalah bilangan berbasis biner yaitu angka 0 dan 1, karena pada data digital merupakan susunan [3]. Selain itu, proses penyisipan dan ekstraksi dari

metode ini juga relatif cukup cepat. [14]. Pengguna pertama (pengirim pesan) dapat mengirim media yang telah disisipi informasi rahasia tersebut melalui jalur komunikasi publik, hingga dapat diterima oleh pengguna kedua (penerima pesan). Penerima pesan dapat mengekstraksi informasi rahasia yang ada di dalamnya [3].

Pada susunan bit di dalam sebuah byte, terdapat bit yang paling berarti *most significant* bit atau msb dan bit yang paling kurang berarti *least significant* bit atau LSB. Kemudian LSB yang akan digunakan dalam steganografi untuk menyisipkan data rahasia karena perubahan kecil sulit terdeteksi. Gambar 2 menjelaskan posisi msb dan LSB dalam susunan bilangan biner pada 1 byte atau 8 bit.



Gambar 2. Posisi msb dan LSB pada bilangan biner 8 bit

Pengujian PSNR (*peak signal to noise ratio*)

Adapun pengujian yang dilakukan untuk mengukur kualitas gambar adalah menggunakan metode PSNR (peak signal to noise ratio). Dimana PSNR adalah ukuran perbandingan antara nilai piksel cover image dengan nilai piksel pada citra stego yang dihasilkan. Pengukuran dilakukan dengan rumus sebagai berikut [3].

Sebelum melakukan pengujian PSNR, terlebih dahulu dilakukan pengujian MSE (*mean square error*). Pengujian MSE (mean square error) dilakukan untuk menentukan nilai rata – rata kuadrat dari jumlah kuadrat absolute error antara cover image dengan citra stego. Terdapat rumus dalam menghitung MSE, rumus MSE adalah sebagai berikut:

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{3}$$

Keterangan:
MSEavg = nilai rata-rata MSE cover image.
MSEr = nilai MSE warna merah.
MSEg = nilai MSE warna hijau.
MSEb = nilai MSE warna biru.

Kemudian dapat dilakukan pengujian PSNR (*peak signal to noise ratio*) digunakan untuk mengukur kualitas citra yang dihasilkan. Metode PSNR adalah ukuran perbandingan antara nilai piksel cover image dengan nilai piksel pada citra stego yang dihasilkan. Berikut rumus, hasil perhitungan dan grafik hasil perhitungan PSNR yang telah dilakukan.

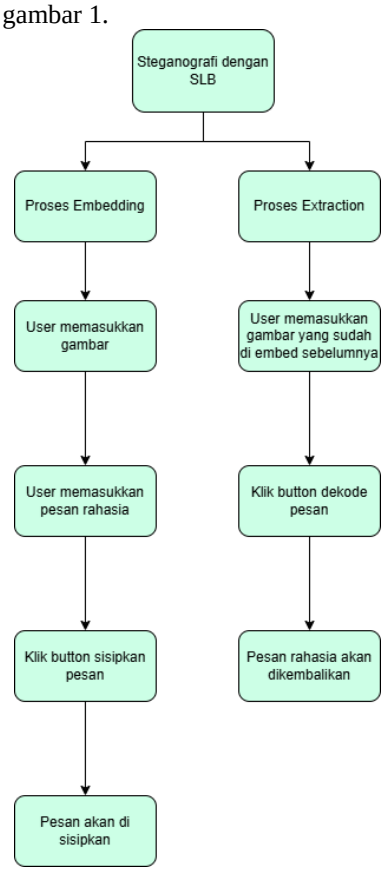
$$PSNR = 10_{log10}\left(\frac{255^2}{MSE}\right)$$

Keterangan:
Pnsr = nilai PSNR citra digital.
MSE = nilai mean square error dari citra.

Dengan demikian, penelitian ini memberikan gambaran bahwa steganografi, khususnya dengan metode LSB, dapat menjadi solusi sederhana namun efisien dalam melindungi data rahasia.

B. Desain penelitian

Desain eksperimen digunakan dengan tujuan untuk mengimplementasikan algoritma LSB dalam melakukan penyisipan teks pada sebuah gambar. Menggunakan perangkat lunak berbasis python dengan berbagai macam library untuk menjalankan fungsi dalam menguji performa metode LSB dalam berbagai skenario penyisipan dan ekstraksi pesan. Gambaran umum perangkat lunak dapat dilihat pada gambar 1.



Gambar 3. Flowchart perangkat lunak yang dibangun

C. Tahapan implementasi

Tahapan implementasi ini menggunakan langkah-langkah yang sudah disusun dengan sistematis dalam membuat sebuah algoritma least significant bit (LSB) pada gambar digital untuk menyisipkan sebuah pesan teks yang bersifat rahasia. Proses implementasi menggunakan sebuah perangkat lunak yang dikembangkan untuk menilai efektivitas algoritma tersebut dalam menyisipkan sebuah pesan teks di dalam sebuah gambar.

Pada tahapan pengembangan perangkat lunak untuk implementasi steganografi dengan metode least significant bit (LSB), digunakan python sebagai bahasa pemrograman utama dalam mengimplementasikan algoritma untuk penyisipan dan juga ekstraksi pesan rahasia pada sebuah gambar digital. Selain itu, flask berperan sebagai kerangka backend dalam membangun tampilan/antarmuka aplikasi berbasis web yang memungkinkan pengguna untuk mengunggah gambar. Sehingga kombinasi dari keduanya akan memastikan bahwa sistem yang telah dikembangkan dapat digunakan dengan baik dan mudah diakses.

Persiapan data

Setelah mengumpulkan data dengan menggunakan metode studi literatur yaitu mencari sumber dari berbagai jurnal yang terkait, maka untuk melakukan implementasi harus dimulai dengan mempersiapkan data yang diperlukan. Data yang diperlukan yaitu sebuah gambar digital dan sebuah pesan teks bersifat rahasia yang ingin disisipkan. Berikut adalah gambar yang digunakan dalam mengimplementasikan yang ditampilkan pada gambar 4.

Gambar 4. Contoh gambar yang digunakan

Teks : ini adalah pesan rahasia, jangan berikan kepada siapapun.

Proses embedding

Proses embedding, yakni proses penyembunyian pesan dimana pada bagian pertama dilakukan proses embedding hidden image yang hendak disembunyikan ke dalam stego medium sebagai media penyimpanan [15]. Setelah gambar dan juga pesan sudah siap, selanjutnya akan dilakukan penyisipan pesan kedalam gambar menggunakan algoritma LSB. Pada tahap ini, maka bit paling tidak signifikan dari komponen warna gambar, yaitu red, green, dan blue (rgb), akan dimodifikasi untuk menyisipkan pesan teks.

Proses penyisipan pesan dimulai dengan melakukan perubahan gambar ke dalam format rgb, di mana setiap piksel terdiri dari tiga komponen warna: red, green, dan blue, yang masing-masing menyimpan informasi dalam 8 bit (0-255). Kemudian setiap karakter dalam pesan akan disisipkan ke dalam bit LSB dari piksel gambar, sehingga perubahan yang terjadi pada gambar sangat kecil dan tidak terlihat oleh mata manusia. Proses penyisipan dapat dilihat pada tabel 1.

Tabel I. Proses penyisipan (embedding)

Langkah	Deskripsi
1. Masukkan gambar	Masukkan gambar yang ingin disisipkan pesan
2. Masukkan pesan	Masukkan pesan yang ingin disisipkan
3. Penyisipan LSB	Menyisipkan bit pesan pada bit paling tidak signifikan (LSB)

Proses extraction

Setelah penyisipan pesan dinilai berhasil, maka tahap selanjutnya adalah melakukan ekstraksi pesan dari gambar yang telah dimodifikasi. Tahap ekstraksi dimulai dengan mengambil kembali bit paling tidak signifikan dari setiap piksel gambar tersebut. Bit-bit ini kemudian disusun kembali menjadi pesan teks yang asli. Proses ekstraksi ini sangat penting untuk memastikan bahwa pesan yang disisipkan dapat dipulihkan tanpa kesalahan. Kemudian gambar akan ditampilkan kembali dengan pesan rahasia yang sudah disisipkan tadi. Proses ekstraksi dapat dilihat pada tabel 2.

Tabel II. Proses ekstraksi

Langkah	Deskripsi
1. Masukkan gambar	Masukkan gambar yang ingin dilakukan ekstraksi.
2. Decode pesan	Pesan yang telah disisipkan akan dikembalikan lagi.

HASIL DAN PEMBAHASAN

Berdasarkan hasil implementasi penerapan metode LSB pada steganografi, dapat disimpulkan bahwa metode LSB memiliki kemampuan yang baik dalam menyisipkan pesan teks kedalam sebuah gambar digital tanpa mengubah atau mengurangi kualitas dari gambar tersebut. Pengujian ini dilakukan pada beberapa gambar dengan resolusi yang berbeda-beda.

A. Kualitas visual gambar

Secara visual gambar hasil steganografi tidak memiliki perbedaan yang signifikan, gambar tersebut sekilas akan terlihat sama seperti gambar aslinya. Hal ini dikonfirmasi

melalui pengukuran nilai PSNR (peak signal-to-noise ratio), yang pada pengujian menunjukkan nilai-rata rata 30db. Nilai ini menunjukkan bahwa gambar yang dihasilkan memiliki kualitas tinggi serta keberadaan pesan di dalam gambar semakin sulit untuk diketahui.
Hasil perhitungan MSE dan PSNR dalam format gambar jpg yang dilakukan dalam penelitian ini, dapat dilihat pada tabel 3.

Tabel III. Tabel pengujian MSE dan PSNR dengan format gambar jpg

	Nama gambar	Ukuran gambar	Ukuran *stego image*	MSE	PSNR
1	Image1.jpg	300 x 300	66,4 kb	0,0001	86,42
2	Image2.jpg	500 x 500	314 kb	5,3333	90,86
3	Image3.jpg	700 x 700	591 kb	2,7210	93,78
4	Image4.jpg	1000 x 1000	920 kb	1,3333	96,88
5	Image5.jpg	1200 x 1200	690 kb	9.2592	98,46

Hasil percobaan menunjukkan bahwa meskipun nilai MSE tidak konsisten, nilai PSNR meningkat seiring bertambahnya ukuran gambar, menandakan kualitas gambar tetap baik. Ukuran stego image yang lebih besar tidak memengaruhi kualitas visual secara signifikan, sehingga metode penyisipan pesan dapat menjaga kualitas gambar dengan baik.

Hasil perhitungan MSE dan PSNR dalam format gambar jpeg yang dilakukan dalam penelitian ini, dapat dilihat pada tabel 4.

Tabel IV. Tabel pengujian MSE dan PSNR dengan format gambar jpeg

	Nama gambar	Ukuran gambar	Ukuran *stego image*	MSE	PSNR
1	Image1.jpeg	300 x 300	66,3 kb	0,0001	87,97
2	Image2.jpeg	500 x 500	314 kb	3,7333	92,40
3	Image3.jpeg	700 x 700	592 kb	1,9047	95,33
4	Image4.jpeg	1000 x 1000	921 kb	9,3333	98,43
5	Image5.jpeg	1200 x 1200	692 kb	6.4814	100,01

B. Efisiensi penyisipan pesan

Metode LSB memungkinkan penyisipan pesan pada setiap bit paling tidak signifikan dari komponen warna (red, green, blue) di setiap piksel gambar. Dengan memanfaatkan struktur ini, kapasitas penyimpanan pesan akan semakin meningkat. Pada pengujian ini, kapasitas maksimum pesan yang dapat disisipkan bergantung pada jumlah bit yang digunakan untuk mempresentasikan warna dalam satu piksel gambar digital.

C. Keberhasilan saat mengekstrak pesan

Ekstraksi pesan berhasil dilakukan dengan tingkat akurasi 100% selama tidak ada modifikasi pada gambar hasil steganografi. Penggunaan metode ini memberikan jaminan bahwa pesan rahasia dapat diambil kembali (extraction) dengan akurat apabila gambar tetap dalam kondisi asli setelah penyisipan pesan..

D. Keamanan

Teknik LSB menawarkan solusi sederhana namun efisien untuk melindungi pesan rahasia. Meskipun tidak sepenuhnya aman dari serangan seperti ancaman analisis pola warna pada histogram gambar, teknik ini dapat digunakan untuk kebutuhan perlindungan data sederhana yang memerlukan kecepatan implementasi dan efisiensi penyimpanan.

Berikut akan dibahas langkah - langkah dan hasil dari pengimplementasian metode LSB dalam steganografi.

Gambar 5. Tampilan awal aplikasi

Gambar diatas merupakan tampilan awal ketika aplikasi diakses. Pada halaman ini tersedia kolom untuk mengupload gambar yang akan disisipkan pesan teks.

Gambar 6. Encode pesan ke gambar

Pada halaman ini pengguna dapat memilih gambar yang ingin disisipkan pesan rahasia, dengan cara drag and drop atau pilih gambar dari directory.

Gambar 7. Tampilan menyisipkan pesan

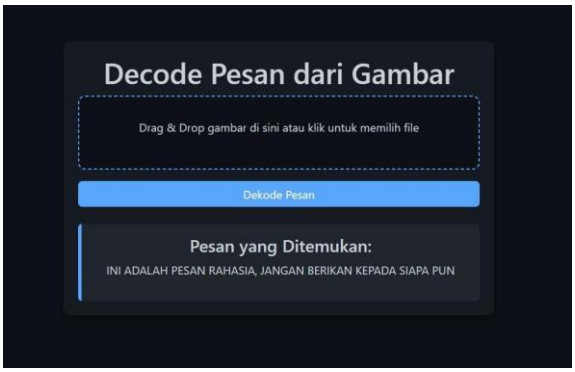
Setelah berhasil mengupload gambar, pengguna dapat menginputkan pesan yang akan disisipkan lalu sistem akan memproses penyisipan pesan rahasia tersebut pada gambar yang telah dipilih sebelum nya.

Gambar 8. Tampilan pesan sudah berhasil disisipkan

Apabila penyisipan pesan berhasil maka sistem akan menampilkan data seperti gambar diatas. Ketika pengguna ingin mengetahui pesan yang disisipkan pada gambar, pengguna wajib mengunduh gambar terlebih dahulu, lalu mengakses halaman decode.

Gambar 9. Tampilan untuk ekstraksi pesan

Untuk mengetahui pesan pada suatu gambar, pengguna dapat drag and drop atau pilih gambar dari directory gambar yang memiliki pesan rahasia.



Gambar 10. Tampilan pesan sudah di decode

Lalu sistem akan mengecek dan menampilkan pesan yang ada pada gambar tersebut dan menampilkan output seperti pada gambar diatas. Sistem berhasil menampilkan pesan yang disisipkan pada gambar digital tanpa mengubah gambar.

Hasil implementasi menunjukkan bahwa sistem berhasil menampilkan pesan yang disisipkan pada gambar digital tanpa mengubah kualitas gambar. Hal ini membuktikan bahwa metode LSB dapat menjadi solusi efektif dan efisien dalam melindungi data rahasia.

SIMPULAN

Mengimplementasikan steganografi dengan algoritma least significant bit (LSB) merupakan metode yang cukup efektif dalam melakukan penyisipan pesan teks ke dalam gambar digital dengan menggunakan bit yang paling tidak signifikan (LSB). Dengan menggunakan steganografi maka gambar tidak akan berubah dan keaslian gambar juga tetap terjaga. Oleh karena itu, pesan yang disisipkan dalam gambar akan tetap terjaga pesan juga dapat diekstraksi dengan akurasi yang tinggi, sehingga kerahasiaan dan integritas pesan akan tetap terjamin selama proses transmisi. Format gambar yang digunakan mempengaruhi hasil pengujian dari MSE dan PSNR.

Untuk semakin meningkatkan efektivitas dan keamanan metode least significant bit (LSB) disarankan untuk tidak menggunakan hanya menggunakan atau bergantung pada format gambar lossless seperti png, tetapi juga mengimplementasikan mekanisme penyisipan yang lebih adaptif. Sebaiknya menggunakan format gambar yang lain seperti jpg atau jpeg untuk melihat hasil pengujian dan menjadi perbandingan untuk menentukan tipe gambar yang paling baik. Pengembangan lebih lanjut diharapkan dapat membuat metode LSB yang lebih kompleks dengan mengkombinasikannya dengan algoritma atau metode lain

sehingga dapat meningkatkan daya tahan apabila terjadis erangan saat melakukan kompresi. Sehingga metode LSB dapat dimanfaatkan untuk berbagai aplikasi yang lebih nyata seperti penyisipan metadata dan melindungi hak cipta konten visual.

UCAPAN TERIMA KASIH

Dengan penuh rasa syukur kami panjatkan puji dan syukur kepada tuhan yang maha esa atas limpahan rahmat-nya sehingga jurnal ini dapat terselesaikan dengan baik. Kami juga mengucapkan terima kasih kepada dosen pengampu yang telah memberikan arahan dan juga bimbingannya. Semoga jurnal ini dapat bermanfaat dan menjadi salah satu kontribusi dalam pengembangan ilmu pengetahuan.

Daftar pustaka

[1] i. M. Yusup, c. Carudin, and i. Purnamasari, "implementasi algoritma caesar cipher dan steganografi least significant bit untuk file dokumen," *j. Tek. Inform. Dan sist. Inf.*, vol. 6, no. 3, pp. 434–441, 2020, doi: 10.28932/jutisi.v6i3.2817.

[2] n. Endar, "penerapan steganografi file gambar menggunakan metode least significant bit (LSB) dan algoritma kriptografi advanced encryption standard (aes) berbasis android," *j. Inform. Univ. Pamulang*, vol. 5, no. 1, pp. 37–37, 2020.

[3] d. Darwis, "implementasi teknik steganografi least significant bit (LSB) dan kompresi untuk pengamanan data pengiriman surat elektronik," *j. Teknoinfo*, vol. 10, no. 2, p. 32, 2016, doi: 10.33365/jti.v10i2.8.

[4] n. A. Ramadhani and i. Susilawati, "penerapan steganografi untuk penyisipan pesan teks pada citra digital dengan menggunakan metode least significant bit," *j. Multimed. Artif. Intell.*, vol. 4, no. 1, pp. 21–27, 2020.

[5] d. Darwis, "implementasi steganografi pada berkas audio wav untuk penyisipan pesan gambar menggunakan metode low bit coding," *expert j. Manaj. Sist. Inf. Dan teknol.*, vol. 5, no. 1, 2015, doi: 10.36448/jmsit.v5i1.715.

[6] 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.

[7] a. A. Permana and h. Amna, "implementasi steganografi file citra digital menggunakan metode least significant bit," *j. Tek.*, vol. 11, no. 1, pp. 62–72, 2022, doi: 10.31000/jt.v11i1.6161.

[8] a. A. Fikhri and h. Hendrawaty, "implementasi steganografi text to image menggunakan metode one bit least significant bit berbasis android," *j. Infomedia*, vol. 3, no. 1, pp. 10–17, 2018, doi: 10.30811/jim.v3i1.623.

[9] n. Laila and a. S. R. Sinaga, "implementasi steganografi LSB dengan enkripsi vigenere cipher pada citra," *sci. Comput. Sci. Informatics j.*, vol. 1, no. 2, p. 47, 2019, doi: 10.22487/j26204118.2018.v1.i2.11221.

[10] a. Rohmanu, "metode algoritma des dan metode end of file ajar rohmanu," *j. Inform.*, vol. 2, no. 1, pp. 1–11, 2017.

[11] y. R. Nasution, m. Furqan, and m. Sinaga, "implementasi steganografi menggunakan metode spread spectrum dalam pengamanan data teks pada citra digital," *j. Sains komput. Inform. (j-sakti*, vol. 4, no. 2, pp. 351–358, 2020.

[12] s. P. Sari, w. Winarno, and d. Z. Sudirman, "implementasi steganografi menggunakan metode least significant bit dan kriptografi advanced encryption standard," *j. Ultim.*, vol. 4, no. 1, pp. 24–32, 2012, doi: 10.31937/ti.v4i1.305.

[13] a. Hafiz, "steganografi berbasis citra digital untuk menyembunyikan datamenggunakan metode least significant bit (LSB)," *j. Cendikia vol. Xvii cendikia 2019 bandar lampung, april 2019* , vol. 17, pp. 194–198, 2019.

[14] e. R. Djuwitaningrum and m. Apriyani, "teknik steganografi pesan teks menggunakan metode least significant bit dan algoritma linear congruential generator (text message steganography using least significant bit method and linear congruential generator algorithm)," *juita*, vol. Iv, no. 2, pp. 79–85, 2016.

[15] t. Alawiyah, r. Ardianto, and d. S. Purnia, "implementasi vigenere cipher sebagai pengaman pada proses deskripsi steganografi least significant bit," *j. Inform.*, vol. 7, no. 1, pp. 37–45, 2020, doi: 10.31311/ji.v7i1.6431.