Indonesian Journal of Data and Science (IJODAS) ISSN: 2715-9930
Vol 2, No 2, July 2021, pp. 91-102

Modifikasi *Least Significant Bits* pada Gambar sebagai Data *Hiding Steganography*

A.Muh.Ramadhani.S[a,1], Tasrif Hasanuddin[a,2]

[a] *Universitas Muslim Indonesia, Jl. Urip Sumoharjo KM.05, Makassar dan 90231, Indonesia*
[1] *13020150072@umi.ac.id;* [2] *tasrif_hasanuddin@umi.ac.id;*

INFORMASI ARTIKEL

Diterima : 08 – 05 – 2021
Direvisi : 18 – 06 – 2021
Diterbitkan : 31 – 07 – 2021

Kata Kunci:
Steganography
Cryptography
LSB
Image encryption
Data Security

ABSTRAK

Penelitian ini menghasilkan kombinasi teknik steganografi dan kriptografi dengan metode LSB. merupakan teknik kriptografi yang populer dapat diterapkan pada citra digital. Nilai piksel citra digital hanya berkisar 0 sampai 255, Dalam penelitian ini diusulkan untuk mengkonversi nilai piksel citra menjadi 16bit sehingga kunci yang digunakan dapat lebih bervariasi. Hasil eksperimen membuktikan adanya peningkatan keamanan serta nilai *imperceptibility* yang tetap terjaga. Hal ini dibuktikan dengan hasil PSNR 77,79dB, MSE 0.0005dB.

I. Pendahuluan

Munculnya teknologi internet dan multimedia telah mendorong berbagai macam usaha untuk melindungi, mengamankan dan menyembunyikan data pada *file* digital dari pihak-pihak yang tidak mempunyai otoritas mengakses *file-file* tersebut[1], [2]. Pengiriman data/pesan dari suatu tempat ke tempat lain banyak terkendala dengan permasalahan keamanan.[3], [4] Apalagi jika pesan tersebut merupakan pesan yang sangat rahasia, sehingga tidak sembarang orang dapat membacanya. Banyak cara yang dapat dilakukan untuk mengamankan pesan yang akan dikirim[5]. Salah satu usaha untuk mengamankan data diantaranya dengan menggunakan kriptografi[6]. Selain kriptografi juga terdapat *steganography* (steganografi) sebagai alternatif untuk mengamankan data.[7], [8]

Steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan suatu informasi.[9] Steganografi dapat digolongkan sebagai salah satu bagian dari ilmu komunikasi.[10] Kata steganografi berasal dari bahasa Yunani yang berarti "tulisan tersembunyi". Pada era informasi digital, steganografi merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak kelihatan.[11]

Dalam pengembangan *steganography* terdapat dua algoritma penting yaitu untuk melakukan *embedding* dan satu lagi untuk melakukan *extracting*[12]–[16]. Proses *embedding* merupakan proses untuk menyisipkan pesan rahasia (*secret message*) ke dalam *cover work* yang berupa *file image*, video, audio maupun teks sebagai media untuk menyisipkan pesan.[17] *Output* dari proses *embedding* disebut sebagai *Stegograme* yang berisi *cover work* dan pesan tersembunyi. Sedangkan *extracting* adalah proses untuk memunculkan kembali pesan yang tersembunyi dari *cover work*. Hal tersebut merupakan keseluruhan proses dalam *steganography*.[18]

Steganografi mempunyai keunggulan yaitu tidak ada perbedaan secara kasat mata antara *Cover-Image* dengan *Stego-Image*.[19] Media yang dapat disisipkan oleh informasi. Rahasia dapat berupa teks, citra, audio maupun video. Jumlah pertukaran data media yang besar membuat kemungkinan kecurigaan adanya informasi rahasia yang pertukarkan melalui pertukaran media digital menjadi kecil.[20]

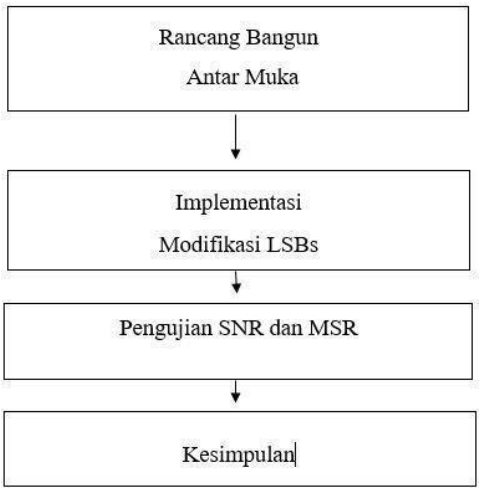
Teknik steganografi yang paling paling sederhana sekaligus paling populer adalah teknik LSB (*Least Significant Bit*) yaitu posisi *bit* pada bilangan biner yang memberikan nilai unit yaitu menentukan apakah nomor genap atau ganjil.[21] Teknik ini mengganti *bit* terakhir dari media steganografi dengan *bit* dari pesan. Supaya tidak menyebabkan perubahan besar, penggantian *bit* ini hanya boleh dilakukan pada informasi yang sifatnya redundan dan memiliki toleransi terhadap perubahan kecil.[22], [23]

Pada penelitian ini mencoba melakukan modifikasi pada metode LSB yaitu dengan mencoba menambahkan *bit* sisipan yang akan disembunyikan pada setiap *pixel* yang kemudian pada penelitian ini

disebut dengan modifikasi *least significant bits*. Pengujian yang akan dilakukan pada hasil steganografinya adalah *Signal to Noise Ratio* dan *Means Sequence Error*. Berdasarkan penelitian terdahulu maka tujuan peneliti yaitu dengan mencoba melakukan modifikasi metode LSB (*Least Significant Bits*) pada gambar sebagai data hiding steganografi serta mengujinya menggunakan PSNR dan MSE.

II. Metode

Pada bagian ini akan dibahas terkait dengan metode penelitian yang digunakan pada penelitian ini, berikut langkah-langkah penelitian:

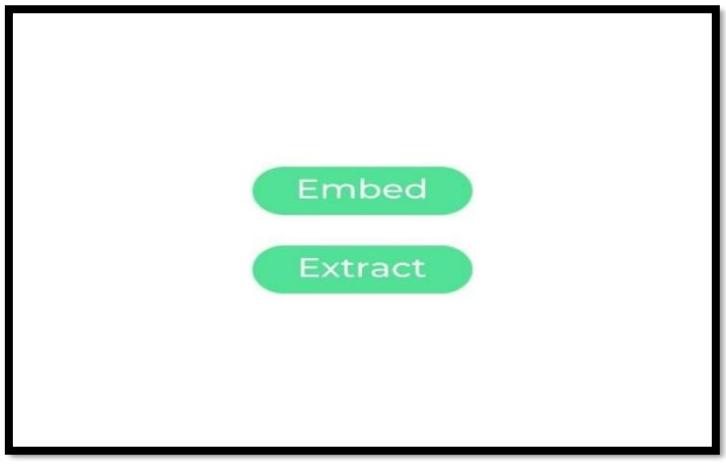


Gambar 1. Tahapan Penelitian

Metode pada penelitian ini di uraikan menjadi 4 tahapan:

1) Rancang Bangun Antar Muka

Antar muka yang akan di rancang menggukan bahasa pemrograman java yang terdiri dari tiga *form* yaitu *form* menu utama, *form embedding* dan *form extract* dimana ditujukan pada Gambar 2, Gambar 3, dan Gambar 4.

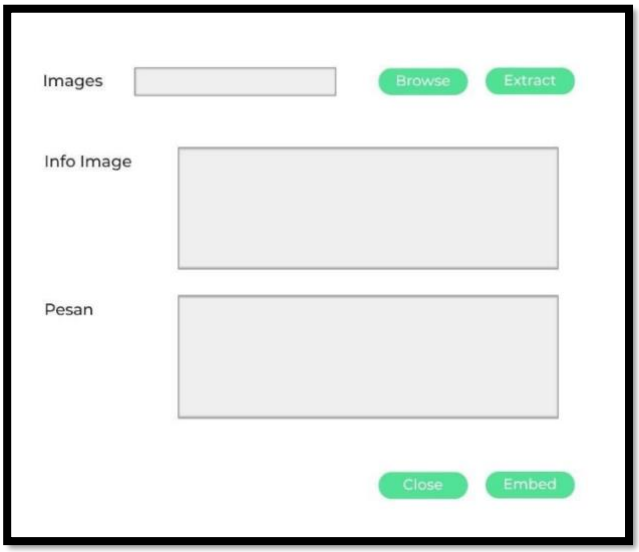


Gambar 2. *Form* Menu Utama

Gambar 2. Menunjukka *form* utama yang memiliki 2 tombol, dimana tombol *embed* untuk masuk ke *form* proses *embedding text* kedalam *image*, sedangkan *extract* untuk masuk ke *form* proses mengeluarkan *text* dari gambar

Gambar 3. Menunjukkan *form embedding*, tahapan yang dilakukan pada *form* tersebut adalah memilih gambar yang akan digunakan sebagai *image* penampung *text*, tombol proses digunakan untuk menunjukkan informasi gambar tersebut, informasi utama yang ditampilkan pada gambar tersebut adalah jumlah karakter yang dapat ditampung oleh gambat tersebut. Sedangkan tombol *embed* berfungsi untuk memasukkan semua pesan pada *textbox* pesan kedalam gambar.

Gambar 3. *Form Embedding*

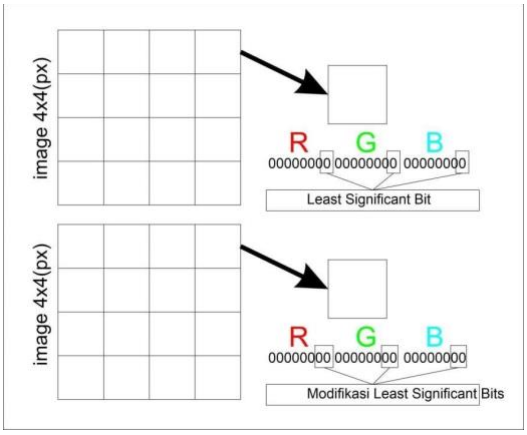


Gambar 4. *Form Extract*

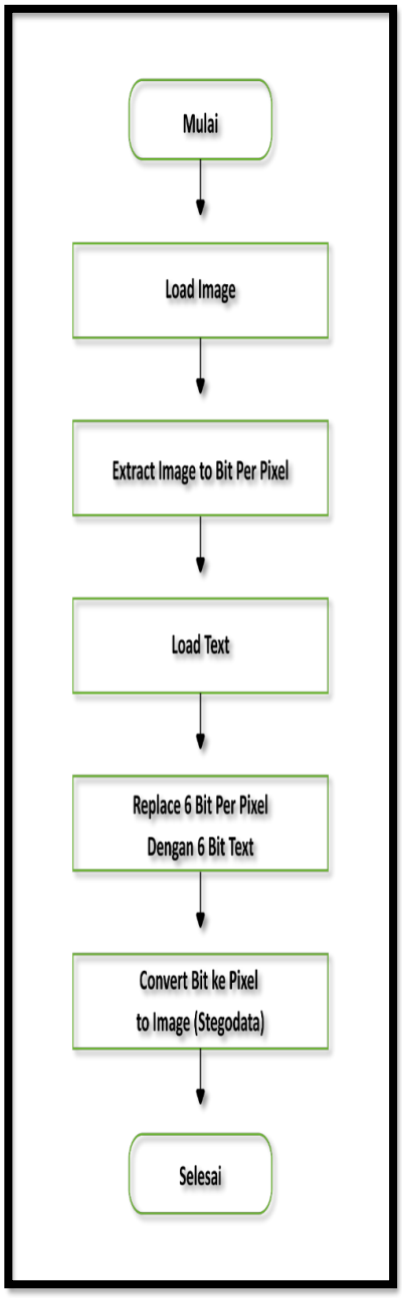
Gambar 4. menunjukkan *form extract*, dimana form ini berfungsi untuk mengeluarkan *text* yang ada pada gambar yang sebelumnya telah disisipkan *text*.

2) Implementasi Modifikasi LSBs

Modifikasi LSBs pada penelitian ini yaitu dengan menyisipkan lebih dari satu bit dibanding *default* metode LSB. Dimana metode dasar dari LSB sebelumnya adalah menyisipkan 3*bit* disetiap nilai *pixel* yang memiliki nilai *Red*, *Green*, dan *Blue* (RGB), sedangkan modifikasi LSB yang dilakukan pada penelitian ini adalah menyisipkan 6*bit* disetiap *pixel* yang memiliki nilai RGB. Gambar 5 menunjukkan perbedaan metode LSB dan modifikasi LSBs yang dilakukan pada penelitian ini.

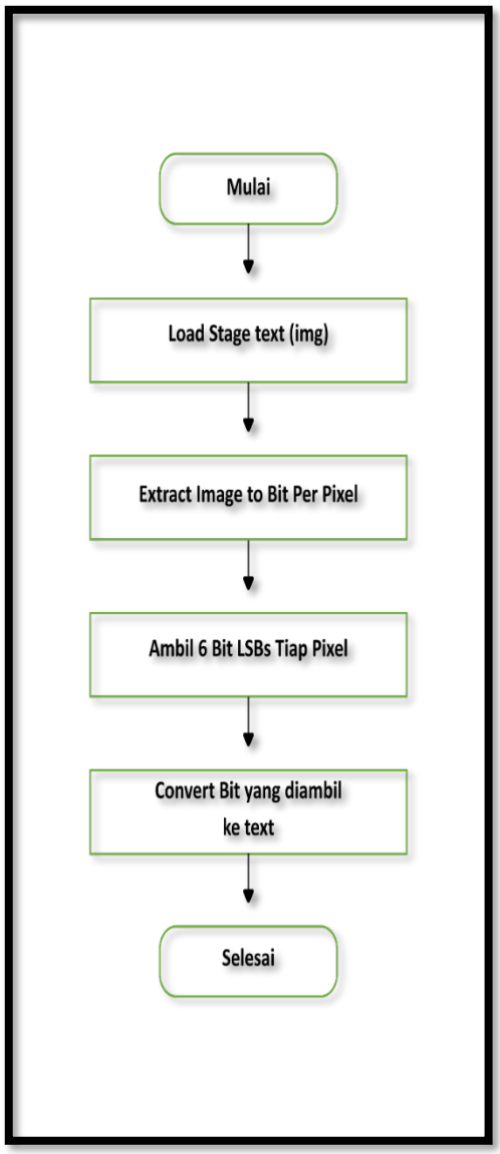


Gambar 5. Perbandingan metode LSB dan LSBs



Gambar 6. *Flowchart* MLSB (*embed*)

Gambar 6. Menunjukkan *flowchart* proses enkripsi dan *embedding* pada pengiriman pesan. Dimulai menginput gambar lalu gambar akan dimuat, kemudian gambar akan di ekstrak dari *bit* ke *pixel*, lalu akan memuat teks, selanjutnya dilakukan proses *embedding cipher image* ke citra *cover* menggunakan metode MLSB yang output-nya berupa citra *stego*.



Gambar 7. *Flowchart* MLSBS (*extract*)

Gambar 7. menunjukkan *flowchart* proses ekstraksi pada penerima pesan. Proses ekstraksi diawali dengan penginputan citra *stego* dan kunci, selanjutnya proses ekstraksi dilakukan dengan menggunakan metode MLSB yang *output* berupa *cipher image*.

Pengujian PSNR dan MSE

Pengujian yang akan dilakukan pada penelitian ini akan menggunakan PSNR dan MSE menggunakan persamaan 1 dan 3 pada objek gambar yang telah disisipi *text* menggunakan metode Modifikasi LSBs.

Pengambilan Kesimpulan

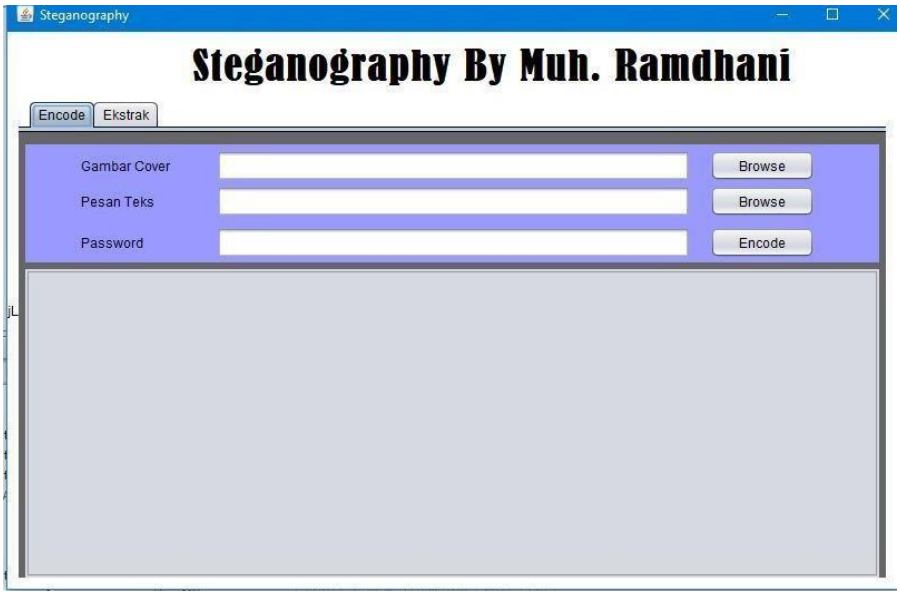
Kesimpulan yang diambil pada penelitian ini mengacu pada hasil pengujian PSNR dan MSE, melihat perbandingan perubahan nilai pada gambar asli dan gambar hasil yang telah disisipi teks.

III. Hasil dan Pembahasan

A. Hasil Penelitian

1) Halaman Utama Aplikasi

Halaman utama aplikasi merupakan halaman awal yang ditampilkan saat aplikasi steganalisis dijalankan. Pada halaman ini terdapat beberapa menu yang tersedia yaitu menu *File*, menu *steganography*, menu ekstraksi dan Menu *About*. Gambar 8 menunjukkan tampilan halaman utama aplikasi *steganography* LSB.



Gambar 8. Tampilan Halaman Utama Aplikasi

2) Halaman Menu *Extract*

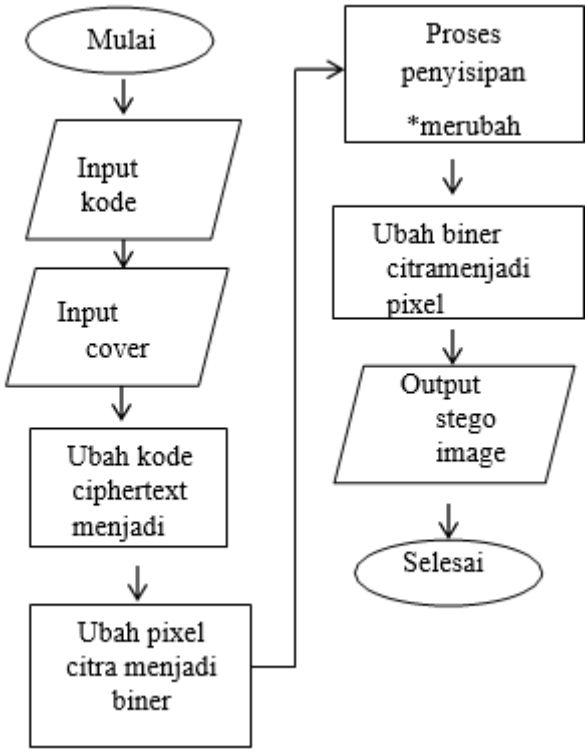
Untuk dapat mengakses halaman ekstraksi pesan, pengguna hanya perlu memilih menu *Ekstract* pada menubar aplikasi. Juga terdapat *textarea* yang digunakan untuk melihat hasil pesan yang ingin di eksraksi. Gambar *Stegano* dipilih oleh pengguna melalui menu *File* - *Open* Gambar akan ditampilkan pada *scrollpane* Gambar. Gambar 9 menunjukkan tampilan halaman pesan hasil ekstraksi.

Gambar 9. Tampilan Halaman *Extract* Aplikasi

B. Pembahasan

1) Proses Penyisipan Metode LSB

Pembahasan Proses penyisipan metode LSB dapat diketahui dengan *flowchart* berikut:



Gambar 10. *Flowchart* metode LSB

Berdasarkan Gambar 10 Proses penyisipan metode LSB dengan langkah menginputkan kode *ciphertext* dan *cover image*, kemudian kode *ciphertext* di konversi menjadi bilangan biner, selain kode *ciphertext*, konversi *cover image* menjadi bilangan biner, setelah keduanya terkonversi, maka dilakukan proses penyisipan dengan mengubah *bit* terakhir dengan *bit* kode *ciphertext* sampaisemua *bit* kode *ciphertext* tersisipkan, kemudian konversi kembali menjadi matriks dan *output*nya berupa *stego image*.

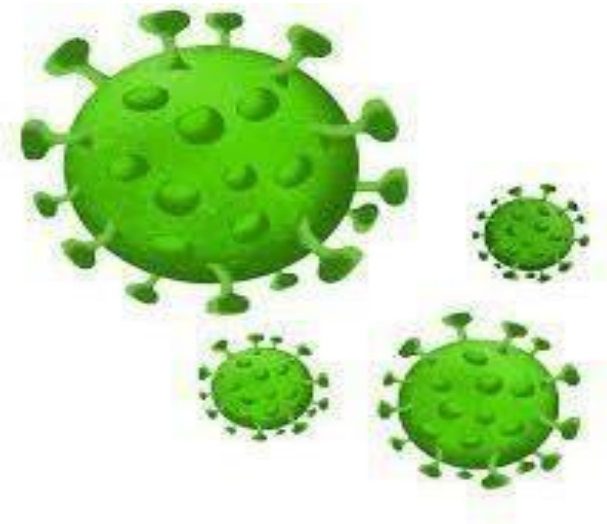
Adapun contoh penyisipan metode LSB seperti berikut:

a) Konversikan terlebih dahulu kode ciphertext dan cover image menjadi bilangan biner seperti ditunjukkan pada Tabel 1:

Tabel 1. Konversi kode *Ciphertext* ke Biner (2)

43 = 00010101	0 = 00000000	1 = 00000001	102 = 01100110
62 = 00111110	12 = 00001100	75 = 01001011	52 = 00110100
126 = 01111110	0 = 00000000	43 = 00101011	138 = 10001010

b) Inputkan cover image dan konversi ke dalam bentuk matriks seperti ditunjukkan pada Tabel 2:



Gambar 11. *Cover Image* metode LSB

didapatkan sebagian matriks dari Gambar 11. seperti yang ditunjukkan pada Gambar 12:

```
 163  163  16 3 162  162  162  162  162  162  162  162  163
F163  163  16 3 162  162  162  162  164  164  164  164  164 1
I164  164  16 4 164  164  164  164  164  164  163  163  163 '
1163  163  16 3 163  163  163  163  162  162  163  163  163 1
                                                          I
I163  164  16 4 164  164  164  164  164  164  163  163  163 I
I163  163  16 4 162  162  164  163  162  162  163  164  164 I
 I163 164  164 162  162  163  164  164  164  163  163  163I
 [162 163  162 163  163  164  164  164  164  164  ...  ... ]
```

Gambar 12. .

c) Kemudian matriks tersebut diubah menjadi bilangan biner seperti yang ditunjukkan pada Gambar 13

```
┌ 10100011  10100011  10100011  10100010  10100010  10100010
  10100010  10100010  10100010  10100010  10100010  10100011  1
  10100011  10100011  10100011  10100010  10100010  10100010
  10100010  10100010  10100100  10100100  10100100  10100100

I 10100100  10100100  10100100  10100100  10100100  10100100  I
[ 10100100  10100100  10100100  10100100  ...       ...       ]
```

Gambar 13. .

d) Kemudian dilakukan proses penyisipan dengan metode LSB yaitu dengan mengganti bit terakhir dari *cover image* dengan *bit* kode *ciphertext*, sampai semuan *bit* kode tersisipkan seperti yang ditunjukkan pada Gambar 14:

```
⌜ 10100010  10100010  10100010  10100011  10100010  10100011  ⌝
  10100010  10100011  10100010  10100010  10100010  10100010
  10100010  10100010  10100010  10100010  10100010  10100010
  10100010  10100010  10100100  10100100  10100100  10100101

⌊ 10100100  10100101  10100101  10100101  10100100  10100100  ⌋
  10100101  10100101  10100100  10100100  ...       ...       ⌉
```

Gambar 14. .

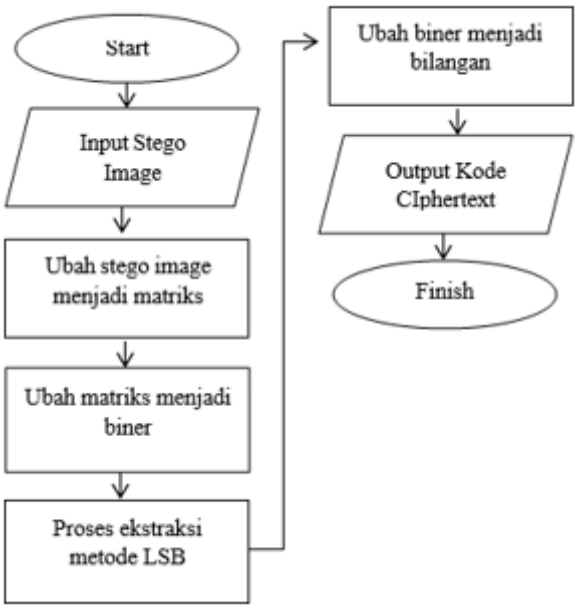
e) Kemudian konversi kembali ke bentuk matriks seperti ditunjukkan pada Gambar 15:

```
⌜ 162 162 162 163 162 163 162 163 162 162 162 162 ⌝
  162 162 162 162 162 162 162 164 164 164 165 164
  165 165 165 164 164 164 164 164 164 163 163 163
  163 163 163 163 163 163 163 162 162 163 163 163
  163 164 164 164 164 164 164 164 164 163 163 163
  163 163 164 162 162 164 163 162 162 163 164 164
  163 164 164 162 162 163 164 164 164 163 163 163
⌊ 162 163 162 163 163 164 164 164 164 164 ... ... ⌋
```

Gambar 15. .

2) Proses Ekstraksi Metode LSB

Proses ekstraksi metode LSB dapat diketahui dengan *flowchart* dibawah ini:

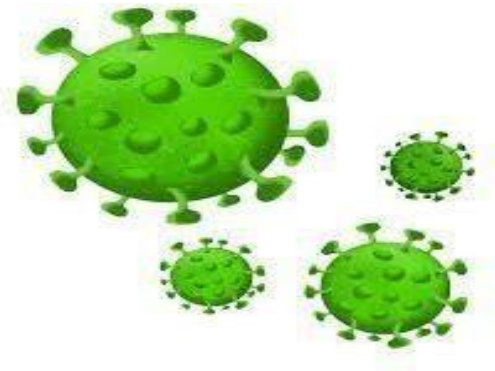


Gambar 16. *Flowchart* proses ekstraksi metode LSB

Berdasarkan Gambar 16. proses ekstraksi metode LSB dengan menginputkan *stego image*, kemudian ubah *stego image* menjadi matriks, setelah itu konversi matriks dari *stego image* menjadi bilangan biner, kemudian dilakukan proses ekstraksi metode LSB dengan cara mengambil setiap *bit* terakhir dari *stego image* dan rangkai menjadi 8 *bit*, setelah itu konversi bilangan biner menjadi desimal dan *output*nya merupakan kode *ciphertext*.

Contoh proses ekstraksi metode LSB dilakukan untuk mengungkap kembali kode *ciphertext* yang telah disembunyikan dengan cara seperti berikut:

a) *Input*kan *stego image*



Gambar 17. *Stego Image* metode LSB

Gambar 17. dikonversi ke bentuk matriks seperti yang ditunjukkan pada Gambar 18:

```
162 162 162 163 162 163 162 163 162 162 162 162
162 162 162 162 162 162 162 164 164 164 165 164
165 165 165 164 164 164 164 164 164 163 163 163
163 163 163 163 163 163 163 162 162 163 163 163
164 164 164 164 164 164 164 164 164 163 163 163
162 162 164 163 162 162 163 164 164
162 162 163 164 164 164 163 163 163
163 163 164 164 164 164 164 ... ...
```

Gambar 18. Matriks hasil konversi metode LSB

b) Kemudian matriks dari *stego image* dikonversi menjadi bilangan biner seperti ditunjukkan pada Gambar 19.

```
10100010 10100010 10100010 10100011 10100010 10100011
10100010 10100011 10100010 10100010 10100010 10100010
10100010 10100010 10100010 10100010 10100010 10100010
10100010 10100010 10100100 10100100 10100100 10100101

10100100 10100101 10100101 10100101 10100100 10100100
10100101 10100101 10100100 10100100 ... ...
```

Gambar 19. *Matriks* dari *stego image* dikonversi menjadi bilangan *biner*

c) Setelah itu, ambil setiap *bit* terakhir dari *stego image* seperti yang ditunjukkan pada Tabel 2.

Tabel 2. Biner dari kode *ciphertext* (2)

00010101	00000000	00000001	01100110
00111110	00001100	01001011	00110100
01111110	00000000	00101011	10001010

d) Setelah itu, *bit* dikonversi ke dalam bentuk *decimal* seperti yang ditunjukkan pada Tabel 3.

Tabel 3. Kode *Ciphertext* (2)

43	0	1	102
62	12	75	52
126	0	43	138

IV. Kesimpulan

Berdasarkan hasil penilitian disimpulkan bahwa *cover image* yang digunakan dengan metode LSB diperoleh *stego image* yang baik, dengan nilai eror terkecil daripada *stego image* yang lain yaitu dengan nilai MSE 0,0005 dB dan nilai PSNR 77,3737 dB, nilai PSNR tersebut menghasilkan *stego image* yang sangat baik karena tidak ada *noise* dan tidak banyak mengalami perubahan, serta tidak menimbulkan kecurigaan bagi pihak lain. Dari metode steganografi tersebut, dapat disimpulkan bahwa metode LSB yang digunakan adalah metode yang baik untuk menyembunyikan pesan tersebut, karena penyisipan dilakukan pada *bit* yang tidak terlalu berpengaruh dalam citra sehingga *cover image* tidak mengalami banyak perubahan.

Daftar Pustaka

[1] Sugiarti and Mirnawati, "Implementasi Algoritma Goverment Standard (GOST) dalam Pengamanan File Dokumen," *Indones. J. Data Sci.*, vol. 1, no. 2, pp. 52–56, 2020.

[2] H. Nursan and Muslim, "Penerapan Metode Digital Watermarking dan Privilege pada Dokumen Skripsi," *Indones. J. Data Sci.*, vol. 1, no. 1, pp. 19–22, 2020.

[3] Z. A. I. Niswati, "STEGANOGRAFI BERBASIS LEAST SIGNIFICANT BIT (LSB) Abstrak . Penelitian ini bertujuan untuk menerapkan metode LSB untuk menyisipkan pesan gambar ke gambar grayscale . Hal ini diperlukan karena sering terjadi bahwa pesan gambar dikirim adalah pesan rahasi," vol. 5, no. 2, pp. 181–191, 1979.

[4] E. Roza and M. Mujirudin, "Studi Multicast," *Rekayasa Teknol.*, vol. 5, no. 1, 2013.

[5] D. Susanti, "Analisis Modifikasi Metode Playfiar Cipher Dalam Pengamanan Data," *Indones. J. Data Sci.*, vol. 1, no. 1, pp. 1–80, 2020.

[6] A. I. Auliyah, "Implementasi Kombinasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman Pada File Document," *Indones. J. Data Sci.*, vol. 1, no. 1, pp. 23–28, 2020.

[7] Y. P. Dewi, "Pengembangan Teknik Steganografi Dengan Kriptografi Modifikasi dari Caesar Cipher dan SHA-256 Untuk Merahasiakan Pesan," *J. Comput. Sci. Vis. …*, vol. 5, pp. 10–21, 2020.

[8] E. Fitri Jayanti, W. Wamiliana, and R. Andrian, "Implementasi Kriptografi Dan Steganografi Pada Media Gambar Menggunakan Hill Cipher Dan Least Significant Bit (LSB)," *J. Komputasi*, vol. 5, no. 1, pp. 17–23, 2017, doi: 10.23960/komputasi.v5i1.1411.

[9] A. R. Mido and E. I. H. Ujianto, "Analysis of Image Effect on the Combination of Rsa Cryptography and," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 2, pp. 279–286, 2022, doi: 10.25126/jtiik.202294852.

[10] S. Anwar, M. I. Komputer, and U. B. Luhur, "Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi Lsb Dan Algoritma Kriptografi Aes," *Semin. Nas. Teknol. Inf. dan Multimed. 2017*, vol. 6, pp. 37–42, 2017.

[11] M. M. Amin, "Image Steganography Dengan Metode Least Significant Bit (Lsb)," *CSRID (Computer Sci. Res. Its Dev. Journal)*, vol. 6, no. 1, pp. 53–64, 2015.

[12] H. Azis and F. Fattah, "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing," *Ilk. J. Ilm.*, vol. 11, no. 2, p. 167, 2019, doi: 10.33096/ilkom.v11i2.447.167-174.

[13] Y. Salim and H. Azis, "Metode Digital Watermark Pada File Penelitian Dosen," *Ilk. J. Ilm.*, vol. 9, no. 2, pp. 161–166, 2017.

[14] F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Pros. Semin. Nas. Ilmu Komput. dan Teknol.*

Inf., vol. 3, no. 2, pp. 112–115, 2018.

[15] A. Djamalilleil, M. Muslim, Y. Salim, E. I. Alwi, H. Azis, and Herman, "Modified Transposition Cipher Algorithm for Images Encryption," *Proc. - 2nd East Indones. Conf. Comput. Inf. Technol. Internet Things Ind. EIConCIT 2018*, pp. 1–4, 2018, doi: 10.1109/EIConCIT.2018.8878326.

[16] H. Azis and R. Wardoyo, "Penerapan Network Steganography Menggunakan Metode Modifikasi LACK Dan Layanan Message Authentication Code Pada Voip Network Steganography System with modification of LACK and Message Authentication Code on VoIP," *Semin. Nas. Komun. dan Inform.*, pp. 13–19, 2015.

[17] David, A. Murtado, and U. Kasma, "Steganografi pada Citra BMP 24-Bit Menggunakan Metode Least Significant Bit," *J. Ilm. SISFOTENIKA*, vol. 2, no. 1, pp. 71–80, 2012.

[18] A. A. Gofur and U. D. Widianti, "Sistem Peramalan Untuk Pengadaan Material Unit Injection Di Pt. Xyz," *Komputa J. Ilm. Komput. dan Inform.*, vol. 2, no. 2, 2015, doi: 10.34010/komputa.v2i2.86.

[19] Irfan, "Penyembunyian Informasi (steganography) Gambar Menggunakan Metode LSB (Least Significant Bit)," *Rekayasa Teknol.*, vol. 5, no. 1, pp. 1–6, 2013.

[20] E. S. Aisyah, R. Rosdiana, and M. R. Qodri, "Implementasi Steganografi Dengan Metode Lsb Untuk Mengamankan Informasi Akun Email Pada Suatu Instansi," *SENSI J.*, vol. 1, no. 1, pp. 24–30, 2015, doi: 10.33050/sensi.v1i1.722.

[21] Bakir and Hozairi, "Implementasi Metode Least Significant Bit (LSB) Dengan Enkripsi Cipher Caesar Pada Steganografi Menggunakan Image Processing," *JUSTINDO (Jurnal Sist. Teknol. Inf. Indones.*, vol. 3, pp. 75–81, 2018.

[22] A. Muis, "Steganografi Metode Least Significant Bit pada Citra Bitmap dengan Teknik Kompres Data dan Ekspansi Wadah," UIN Alauddin Makassar, 2011.

[23] N. Rokhman and J. Maharanti, "Deteksi Steganografi Berbasis Least Significant Bit (LSB) Dengan Menggunakan Analisis Statistik," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 5, no. 2, pp. 57–62, 2013, doi: 10.22146/ijccs.2007.