

IMPLEMENTASI STEGANOGRAFI MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* (LSB) DALAM PENGAMANAN INFORMASI PADA CITRA DIGITAL

SKRIPSI

*Diajukan Untuk Memenuhi Salah Satu Persyaratan Menyelesaikan Program Studi
S1 Pendidikan Teknik Informatika Departemen Teknik Elektronika
Fakultas Teknik Universitas Negeri Padang*



OLEH :

**FITRI YANTI
2018/18076022**

**PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK ELEKTRONIKA
FAKULTAS TEKNIK
UNIVERSITAS NEGERI PADANG
2023**

HALAMAN PERSETUJUAN SKRIPSI


IMPLEMENTASI STEGANOGRAFI MENGGUNAKAN *METODE LEAST SIGNIFICANT BIT* (LSB) DALAM PENGAMANAN INFORMASI PADA CITRA DIGITAL

Nama : Fitri Yanti
NIM/TM : 18076022/2018
Program Studi : Pendidikan Teknik Informatika
Departemen : Teknik Elektronika
Fakultas : Teknik

Padang, Mei 2023

Disetujui Oleh :

Dosen Pembimbing

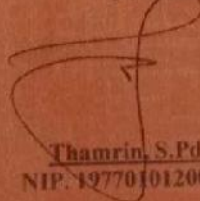


Khairi Budayawan, S.Pd., M.Kom
NIP. 197608102003121002

Mengetahui,

Ketua Departemen Teknik Elektronika

FT-LNR



Thamrin, S.Pd., MT.
NIP. 197701012008121001

HALAMAN PENGESAHAN

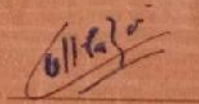
Dinyatakan lulus setelah dipertahankan Skripsi di depan Tim Penguji
Program Studi Pendidikan Teknik Informatika Departemen Teknik Elektronika
Fakultas Teknik Universitas Negeri Padang

Judul : Implementasi Steganografi Menggunakan Metode
Least Significant Bit (LSB) dalam Pengamanan
Informasi Pada Citra Digital
Nama : Fitri Yanti
NIM : 18076022
Departemen : Teknik Elektronika
Program Studi : Pendidikan Teknik Informatika
Fakultas : Teknik

Padang, Mei 2023

Tim Penguji

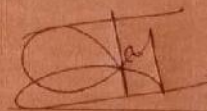
1. Ketua : Vera Irma Delianti, S.Pd., M.Pd.T



2. Anggota 1 : Khairi Budayawan, S.Pd., M.Kom



3. Anggota 2 : Hadi Kurnia Saputra, S.Pd., M.Kom



SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Fitri Yanti
TM/NIM : 2018/18076022
Program Studi : Pendidikan Teknik Informatika
Jurusan : Teknik Elektronika
Fakultas : Teknik

Dengan ini menyatakan bahwa Skripsi saya yang berjudul "**Implementasi Steganografi Menggunakan Metode *Least Significant Bit* (LSB) dalam Pengamanan Informasi pada Citra Digital**" adalah benar merupakan karya saya sendiri. Sepanjang pengetahuan saya tidak terdapat pendapat atau karya orang lain yang ditulis dan diterbitkan kecuali sebagai acuan ilmiah atau kutipan dengan mengikuti tata penulisan karya ilmiah yang lazim.

Padang, Maret 2023

Yang Menyatakan,



Fitri Yanti

NIM : 18076022

ABSTRAK

Fitri Yanti (18076022) : Implementasi Steganografi Menggunakan Metode *Least Significant Bit* (LSB) dalam Pengamanan Informasi Pada Citra Digital.

Berbagai metode untuk menyembunyikan pesan rahasia telah banyak digunakan salah satunya adalah steganografi. Steganografi adalah teknik penyembunyian pesan atau informasi rahasia pada suatu media penampung (*cover object*), sehingga pihak yang tidak berhak mengaksesnya (orang ketiga) sulit menyadari pesan tersebut. Pada penelitian ini metode steganografi yang digunakan dalam penyembunyian pesan yaitu *Least Significant Bit* (LSB) yang dikombinasikan dengan kriptografi *vigenere cipher*. Metode ini merupakan salah satu metode yang sering digunakan, sederhana, cepat dalam proses ekstraksi, serta memiliki daya tampung penyisipan yang cukup besar. Pesan akan disisipkan dengan cara mengganti bit terakhir pada citra *cover* dengan bit pesan, dengan catatan jumlah bit pada pesan tidak melebihi bit citra *cover*. Dari hasil pengujian yang dilakukan pada beberapa citra digital bahwa nilai PSNR citra rata-rata diatas 30 dB. Hal ini menunjukkan bahwa steganografi cukup baik digunakan dalam proses penyisipan pesan, karena citra *stego* (hasil steganografi) tidak mengalami perubahan yang signifikan dari citra *cover*.

Kata Kunci : Penyisipan Pesan, Steganografi, *Least Significant Bit* (LSB), Kriptografi, *Vigenere Cipher*

KATA PENGANTAR

Alhamdulillah rabbil'alamin, puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat dan karunianya sehingga penulis dapat menyelesaikan skripsi penulis yang berjudul "**Implementasi Steganografi Menggunakan Metode *Least Significant Bit (LSB)* dalam Pengamanan Informasi Pada Citra Digital.**" Skripsi ini dibuat sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Pendidikan Strata Satu (S1) di program Studi Pendidikan Teknik Informatika Fakultas Teknik Universitas Negeri Padang. Penyelesaian skripsi ini tidak terlepas dari bimbingan, bantuan, serta dukungan dari berbagai pihak. Oleh karena itu pada kesempatan kali ini, penulis mengucapkan terimakasih kepada:

1. Orang Tua tercinta dan kedua adik yang senantiasa memberikan dukungan, kasih sayang, dan do'a yang tiada hentinya kepada penulis
2. Bapak Dr. Fahmi Rizal, M.Pd.,M.T selaku Dekan Fakultas Teknik Universitas Negeri Padang
3. Bapak Thamrin, S.Pd., M.T selaku Ketua Jurusan Teknik Elektronika Fakultas Teknik Universitas Negeri Padang
4. Bapak Hadi Kurnia Saputra,S.Pd., M.Kom selaku Pembimbing Akademik
5. Bapak Khairi Budayawan, S.Pd., M.Kom selaku Dosen Pembimbing yang telah membimbing dalam perencanaan, pelaksanaan, dan pelaporan skripsi ini
6. Ibuk Vera Irma Delianti, S.Pd., M.Pd.T dan Bapak Hadi Kurnia Saputra, S.Pd., M.Kom selaku penguji yang telah memberikan arahan, bimbingan, dan motivasi dalam menyelesaikan skripsi ini

7. Rekan – rekan PTI 18 senasib dan seperjuangan yang telah memotivasi dan mendukung penulis dalam menyelesaikan Tugas Akhir ini.

Penulis menyadari bahwa tak ada gading yang tak retak, begitu juga dengan penulisan skripsi ini yang tak luput dari kekurangan. Untuk itu penulis mengharapkan saran dan kritik yang membangun untuk menyempurnakan skripsi. Semoga Allah SWT menilai ibadah yang penulis kerjakan dan skripsi ini dapat bermanfaat bagi pembaca, Aamiin.

Padang, Februari 2023

Penulis

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI	iv
DAFTAR TABEL	vi
DAFTAR GAMBAR	vii
DAFTAR LAMPIRAN	viii
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah.....	1
B. Identifikasi Masalah.....	4
C. Rumusan Masalah.....	5
D. Pembatasan Masalah.....	5
E. Tujuan Penelitian.....	5
F. Manfaat Penelitian.....	5
BAB II KAJIAN PUSTAKA	7
A. Kajian Teori.....	7
1. Steganografi.....	7
2. Kriptografi.....	10
3. Metode <i>Least Significant Bit</i> (LSB).....	11
4. Algoritma <i>Vigenere Cipher</i>	14
5. Informasi.....	26
6. Citra Digital.....	26
7. Citra Bitmap.....	27
8. MSE dan PNSR.....	29
B. Penelitian Yang Relevan.....	30
C. Kerangka Konseptual.....	32
BAB III METODE PENELITIAN	33
A. Desain Penelitian.....	33
B. Objek Penelitian.....	33
C. Teknik Pengumpulan Data.....	33
D. Perangkat Yang Digunakan.....	33

E. Prosedur Penelitian	34
F. Pengujian dan Analisis	37
BAB IV HASIL DAN PEMBAHASAN	38
A. Embedding dan Ekstraksi	38
B. Pengujian	61
BAB V KESIMPULAN DAN SARAN	66
A. KESIMPULAN	66
B. SARAN	66
DAFTAR PUSTAKA	68

DAFTAR TABEL

Tabel 1. ASCII Printable Character 32-126	25
Tabel 2. Kriteria <i>Stego Image</i>	30
Tabel 3. Enkripsi dengan <i>Vigenere Cipher</i>	40
Tabel 4. <i>Pixel</i> RGB	40
Tabel 5. Konversi desimal <i>pixel</i> ke biner	41
Tabel 6. Desimal <i>Ciphertext</i>	41
Tabel 7. Biner <i>Ciphertext</i>	41
Tabel 8. Penyisipan biner <i>ciphertext</i> pada citra <i>cover</i>	42
Tabel 9. <i>Pixel</i> citra <i>stego</i>	43
Tabel 10. Dekripsi <i>vigenere cipher</i>	45
Tabel 11. Pesan (<i>plaintext</i>)	46
Tabel 12. Kunci (<i>key</i>)	46
Tabel 13. Enkripsi dengan <i>vigenere cipher</i>	50
Tabel 14. Desimal <i>ciphertext</i>	51
Tabel 15. Biner <i>ciphertext</i>	52
Tabel 16. Penyisipan biner <i>ciphertext</i> pada biner citra <i>cover</i>	52
Tabel 17. Dekripsi <i>vigenere cipher</i>	59
Tabel 18. Pesan (<i>plaintext</i>)	60
Tabel 19. Kunci (<i>key</i>)	60
Tabel 20. Kriteria pengamatan	61
Tabel 21. Implementasi pada citra digital	62
Tabel 22. Perbandingan ukuran citra	64
Tabel 23. Nilai PSNR	65

DAFTAR GAMBAR

Gambar 1. Proses <i>Embedding</i>	9
Gambar 2. Ekstraksi Citra	9
Gambar 3. Proses Steganografi dengan Metode LSB	12
Gambar 4. Proses Penggunaan Kunci	12
Gambar 5. Metode LSB	13
Gambar 6. Tabel <i>Vigenre Cipher</i>	15
Gambar 7. Huruf dan angka	15
Gambar 8. Hasil penukaran huruf dan angka	16
Gambar 9. Proses <i>Embedding</i> (Menyisipkan Pesan)	35
Gambar 10. Proses <i>Ekstraksi</i> (Memisahkan Pesan)	36
Gambar 11. mushroom 4x4.bmp	38
Gambar 12. Tampilan Proses <i>Encoding</i> pada Matlab	42
Gambar 13. mushroom 4x4 stego.bmp	43
Gambar 14. Tampilan Ekstraksi Pesan	46
Gambar 15. mushroom 16x16.bmp	47
Gambar 16. Desimal <i>pixel</i> merah (<i>Red</i>)	51
Gambar 17. Desimal <i>pixel</i> hijau (<i>green</i>)	51
Gambar 18. Desimal <i>pixel</i> biru (<i>blue</i>)	51
Gambar 19. Tampilan proses <i>encoding</i> pada matlab	54
Gambar 20. Desimal <i>pixel</i> merah (<i>red</i>)	54
Gambar 21. Desimal <i>pixel</i> hijau (<i>green</i>)	55
Gambar 22. Desimal <i>pixel</i> biru (<i>blue</i>)	55
Gambar 23. mushroom 16x16 stego.bmp	55
Gambar 24. Tampilan Ekstraksi Pesan	60

DAFTAR LAMPIRAN

Lampiran 1. Tabel ASCII <i>printable character</i>	71
Lampiran 2. Biner citra <i>cover</i> mushroom.bmp 16x16	73
Lampiran 3. Biner citra <i>stego</i> mushroom.bmp 16x16	76
Lampiran 4. Hasil Proses <i>embedding</i> dan ekstraksi (<i>decoding</i>) citra digital	80
Lampiran 5. MSE PSNR citra <i>stego</i>	85

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Pada era digital ini segala sesuatu sudah menggunakan teknologi sebagai sarana pendukung salah satunya dalam penyampaian informasi. Terdapat berbagai kemungkinan ancaman yang timbul berkaitan dengan keamanan data atau informasi saat melakukan transmisi melalui media digital dan internet. Ancaman terhadap keamanan data dapat terjadi ketika informasi yang dikirimkan tidak ditujukan kepada semua orang. Saat ini telah banyak terjadi kejahatan di dunia maya, dimana informasi rahasia dengan mudahnya diambil oleh seorang *hacker* (Tri Handayani et al., 2021). Berdasarkan hasil *survey* yang dilakukan oleh *High Technology Crime Investigation Associations* (HTCIA) dari 445 responden, sekitar 14% membutuhkan peningkatan keamanan pada data, yaitu peningkatan *privacy* dan *policy* yang lebih baik dan 56,4% membutuhkan pelatihan dan pengetahuan tentang pengamanan data pada komputer atau jaringan (Ziaurrahman et al., 2019). Oleh karena itu perlunya diambil langkah-langkah dalam keamanan informasi bagi pemilik informasi rahasia.

Penerapan keamanan informasi memungkinkan sebuah organisasi untuk dapat menjaga kerahasiaan, dan ketersediaan informasi secara kontinu (Ariyus, 2013). Maka dari itu diperlukan suatu teknik penyembunyian atau penyandian dengan kode tertentu untuk seorang pemilik karya seni dalam bentuk citra digital dalam pendistribusian konten mereka yang bersifat rahasia dan terjaga, agar nantinya pesan yang diterima oleh klien tetap terjaga keasliannya. Metode dalam

penyembunyian pesan dengan media lain yang dikenal yaitu kriptografi dan steganografi.

Kriptografi adalah metode pengamanan dan penyandian pesan dari pihak ketiga dengan menerapkan teknik matematika pada algoritmanya. Pada kriptografi proses penyandiannya menggunakan algoritma kunci (Sari & Sari, 2022). Kriptografi merupakan proses penyandian pesan dengan teknik enkripsi dan dekripsi dengan kode acak.

Steganografi merupakan teknik atau seni menyembunyikan pesan rahasia (*hiding message*) atau tulisan rahasia (*covered writing*) sehingga adanya pesan tersebut tidak terdeteksi oleh orang lain yang tidak berwenang kecuali pengirim dan penerima pesan yang dapat mengetahui pesan tersebut. Teknik ini ditujukan agar pesan yang telah disembunyikan dan dimanipulasi tidak mudah terdeteksi perubahannya oleh indra penglihatan manusia. Pada dasarnya tujuan dari steganografi bukannya untuk menghindari pihak ketiga untuk *decode* (memisahkan pesan dari gambar) pesan tersembunyi, melainkan untuk mencegah pihak ketiga mengetahui keberadaan pesan tersembunyi tersebut.

Terdapat banyak metode atau teknik yang digunakan pada Steganografi diantaranya yaitu : *Least Significant Bit* (LSB) artinya mengganti bit terakhir yang tidak berpengaruh signifikan dengan bit pesan, *Most Significant Bit* (MSB) yaitu mengganti bit awal pada citra dengan bit pesan, *Metode End of File* (EOF) merupakan teknik penyisipan pada akhir file *cover*, *Spread Spectrum*, *Discrete Cosine Transform* (DCT), *Discrete Wavelet Transform* (DWT) dan *Bit-Plane Complexity Segmentation* (BPCS). Masing-masing metode mempunyai kelebihan

dan kekurangan, sehingga tidak ada metode yang sempurna dan penggunaannya tergantung kebutuhan (Ratnasari & Dwiyanto, 2020).

Pada penelitian ini penulis menggunakan metode *Least Significant Bit* (LSB). Metode ini merupakan salah satu teknik steganografi yang sering digunakan. Metode LSB merupakan metode yang paling sederhana, cepat dalam mengekstrak pesan, serta memiliki kapasitas penyisipan yang cukup besar (Lubis et al., 2015). Pada metode ini pesan akan disisipkan dengan cara mengganti bit terkecil (terakhir) dari *pixel* citra dengan bit pesan, karena tidak akan memberikan pengaruh atau perubahan yang signifikan terhadap citra digital (Supardi et al., 2021). Namun metode LSB dinilai sederhana dan mudah diimplementasikan sehingga rentan terjadinya serangan. Upaya yang dapat dilakukan yaitu dengan meminimalisir kemungkinan serangan dengan menggabungkan metode LSB dan algoritma kriptografi untuk penyandian pesan. Algoritma kriptografi yang penulis gunakan yaitu *vigenere cipher*.

Implementasi steganografi umumnya banyak menggunakan citra digital sebagai *cover image* (citra penampung). Hal ini dikarenakan sebuah citra digital (*image*) yang berisi informasi atau pesan rahasia di dalamnya cenderung lebih mudah disebarluaskan melalui web atau forum. Namun yang perlu diperhatikan yaitu ketika informasi disisipkan pada citra digital dengan format tertentu kemudian diubah ke bentuk format lain maka informasi rahasia yang terdapat pada format tersebut akan hilang (Painem, 2016). Alasan lainnya kenapa umumnya menggunakan format citra digital sebagai media penampung karena ukuran dari file yang tidak terlalu besar selain itu terdapat banyak algoritma

steganografi yang digunakan untuk media penampung berformat citra (Permana et al., 2022).

Terdapat banyak penelitian yang membahas mengenai implementasi teknik steganografi salah satu contohnya yaitu **Implementasi Steganografi dengan Metode End of File (EOF) untuk Menyisipkan Pesan Teks Pada Gambar** (Tri Handayani et al., 2021). Metode EOF tersebut merupakan teknik penyisipan bit pesan pada akhir file penampung.

Berdasarkan uraian diatas, penulis tertarik untuk mengambil judul penelitian yang berkaitan dengan implementasi steganografi **“Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam Pengamanan Informasi Pada Citra Digital.”** Metode LSB nantinya akan dikombinasikan dengan algoritma kriptografi *vigenere cipher* untuk proses penyandian. Hasil dari penelitian ini nantinya dapat diketahui bagaimana cara mengimplementasikan metode tersebut dan keefektifannya pada pengamanan informasi.

B. Identifikasi Masalah

Berdasarkan uraian pada latar belakang masalah, maka dapat diidentifikasi beberapa permasalahan sebagai berikut:

1. Sering terjadinya serangan dalam pertukaran informasi, sehingga perlu dilakukan antisipasi agar informasi tetap aman
2. Pentingnya penerapan keamanan informasi agar tidak terjadi manipulasi data
3. Pentingnya mengamankan informasi dari pihak-pihak yang tidak memiliki wewenang

C. Rumusan Masalah

Berdasarkan identifikasi masalah yang telah ditemukan, maka dapat dirumuskan masalah dalam penelitian ini, yaitu : “Bagaimana Mengimplementasikan Steganografi Menggunakan Metode *Least Significant Bit* (LSB) dalam Pengamanan Informasi Pada Citra Digital?”

D. Pembatasan Masalah

Berdasarkan rumusan masalah, maka masalah dalam penelitian ini dibatasi pada:

1. Media penampung yang digunakan untuk menyembunyikan informasi berupa citra digital (gambar), informasi yang disembunyikan berupa teks
2. Metode steganografi yang digunakan *Least Significant Bit* (LSB)
3. Algoritma kriptografi yang digunakan *vigenere cipher*

E. Tujuan Penelitian

Tujuan yang ingin dicapai dan diperoleh dari pembuatan penelitian ini yaitu:

1. Menyembunyikan informasi pesan berupa citra digital dengan metode steganografi *Least Significant Bit* (LSB)
2. Mengetahui keefektifan metode yang digunakan dalam steganografi

F. Manfaat Penelitian

1. Bagi Pembaca

Menambah pengetahuan mengenai bagaimana mengimplementasikan steganografi menggunakan metode *Least Significant Bit* (LSB) dalam pengamanan informasi pada citra digital.

2. Bagi Peneliti Lain

Sebagai referensi untuk materi yang berhubungan untuk dikembangkan penelitian lebih lanjut di kemudian hari, serta menumbuhkan budaya meneliti sehingga terciptanya inovasi dalam pembelajaran.

3. Bagi Penulis

Menambah pengetahuan berkaitan dengan bagaimana implementasi steganografi menggunakan metode *Least Significant Bit* (LSB) dalam pengamanan informasi pada citra digital, bagaimana membuat aplikasi untuk pengujian steganografi pada software Matlab sehingga dapat menyembunyikan pesan pada media penampung citra digital.