**BAB II**

**LANDASAN TEORI**

* 1. **Kajian Ilmiah**

Dalam penelitian ini, kami menggunakan gambar sebagai media digital. Kami memodifikasi *Least Significant Bit* (LSB) yang merupakan teknik yang paling umum digunakan dalam steganografi. Oleh karena itu, penting untuk memodifikasi algoritma LSB untuk memastikan aspek keamanannya. Perbaikan teknik LSB disarankan dengan memilih hanya piksel ganjil dan mengabaikan piksel genap dalam implementasi steganografi. Kami berhasil menerapkan algoritma LSB yang dimodifikasi dengan menggunakan gambar RGB dan citra *grayscale* sebagai media steganografi. *Mean Squared Error* (MSE) dan *Peak Signal-to-noise Ratio* (PSNR) digunakan untuk mengevaluasi kualitas *stego*-*image*. Perhitungan kami menunjukkan bahwa algoritma LSB yang dimodifikasi memberikan hasil yang lebih baik daripada LSB konvensional. Algoritma LSB konvensional memberikan 1.98 10-5 untuk MSE dan 95.20893 dB untuk perhitungan PSNR, sedangkan LSB yang dimodifikasi memberikan nilai masing-masing 1.80 10-5 dan 95.6101 dB untuk MSE dan PSNR. (Putri, dkk, 2017).

Dari penelitian yang telah dilakukan oleh (Amin, 2014) yang berjudul “*Image* *Steganography* dengan Metode *Least Significant Bit* (LSB)” didapatkan hasil bahwa *cover-image* pertama dengan teks pesan yang paling panjang didapatkan nilai 1.3967 dB untuk MSE dan 46.68 dB untuk PSNR, pada gambar kedua dengan panjang teks lebih sedikit dari gambar pertama didapatkan nilai 0.86916 dB untuk nilai MSE dan 48.74 dB untuk nilai PSNR, sedangkan pada gambar ketiga dengan panjang teks paling sedikit didapatkan nilai 0.4955 dB untuk nilai MSE dan 51.18 dB untuk nilai PSNR. dari hasil perhitungan tersebut dapat dikatakan bahwa penyisipan sebuah teks pesan dengan ukuran yang berbeda-beda akan menghasilkan nilai MSE dan PSNR yang berbeda pula. Semakin besar ukuran *file* pesan maka nilai MSE akan semakin besar dan nilai PSNR semakin kecil, begitu pula sebaliknya semakin kecil ukuran *file* pesan maka nilai MSE semakin kecil dan nilai PSNR akan semakin besar. Jika nilai PSNR tersebut kecil maka dapat dikatakan kualitas citra semakin buruk itu artinya kualitas citra secara fisik buruk pula. Sedangkan apabila nilai PSNR besar maka kualitas citra tetap bagus, yang artinya kerusakan pada citra relatif sedikit.

Penelitian yang telah dilakukan oleh (Pardosi I. A., dkk, 2015) yang berjudul “Aplikasi Penyembunyian Pesan pada Citra dengan Metode AES Kriptografi dan *Enhanced* LSB Steganografi” mendapat kesimpulan untuk pengujian dengan jumlah karakter bervariasi bahwa jumlah karakter pesan yang telah disisipkan pada setiap gambar penampung berpengaruh terhadap nilai PSNR yang dihasilkan atau dengan kata lain semakin banyak karakter pesan yang disisipkan ke dalam gambar penampung, maka semakin berkurang kualitas gambar yang dihasilkan. Sedangkan hasil pengujian untuk kriteria *fidelity* dan *recovery* disimpulkan bahwa algoritma *Enhanced* LSB memenuhi kriteria steganografi untuk *fidelity* dan *recovery*. Tidak terjadi perubahan mutu dan ukuran penampung pada saat gambar penampung sudah disisipkan pesan dan pesan yang disisipkan sebelumnya dapat diekstrak tanpa kehilangan isi pesan.

Penelitian yang telah dilakukan oleh (Darmayanti, & Awang Harsa.K., 2016) yang berjudul “Sistem Steganografi pada Citra Digital Menggunakan *Least Significant Bit*” mendapat kesimpulan bahwa algoritma LSB memberikan nilai MSE Red 47.715, Green 67.46, Blue 92.768. Sedangkan untuk nilai PSNR *Red* 16.76, *Green* 11.866, *Blue* 7.9777. Dari perhitungan tersebut didapatkan bahwa metode LSB ini memenuhi kriteria, yaitu secara kasat mata hasil citra akhir tidak banyak berubah dari citra awal. Hasil yang diuji semuanya bisa disisipkan dengan baik, meskipun pada hasil outputnya ukuran gambar tidak sama dibandingkan dengan citra awal.

Metode *Least Significant Bit* (LSB) digunakan untuk menyisipkan pesan ke dalam media penyisipan citra warna 24 bit (*cover image*) pada setiap 2 bit yang tidak paling signifikan dari setiap warna citra (*Red, Green, dan Blue*) sehingga setiap piksel citra warna dapat menampung 6 bit pesan teks. Metode LSB 2 bit, bit yang disisipi adalah bit ke-7 dan bit ke-8 untuk setiap *byte*. Sehingga perubahan nilai pada 2 bit terakhir berkisar antara nol sampai dengan tiga dari nilai *byte* sebelum terjadi penyisipan. Dalam menentukan letak piksel citra warna yang akan disisipi pesan, digunakan algoritma pembangkit bilangan acak semu, yaitu *Linear Congruential Generator* (LCG). Hasil eksperimen menunjukkan Secara kasat mata kualitas *stego-image* tidak berbeda dengan *cover-image*. Proses ekstraksi pesan dari *stego-image* menghasilkan pesan teks yang sama dengan pesan teks asli. Untuk ukuran panjang pesan rahasia yang maksimal, penyisipan pesan menggunakan metode LSB 2 bit memberikan kualitas *stego-image* yang termasuk tinggi, yaitu di atas 40 dB. Dalam implementasi algoritma LCG untuk membangkitkan bilangan acak semu, nilai konstanta m sebaiknya tidak sama dengan jumlah piksel *cover-image*, sehingga nilai ini yang juga merupakan nilai *stego-key* akan lebih tahan terhadap serangan *bruteforce attack*. (Djuwitaningrum & Apriyani, 2016)

## Dasar Teori

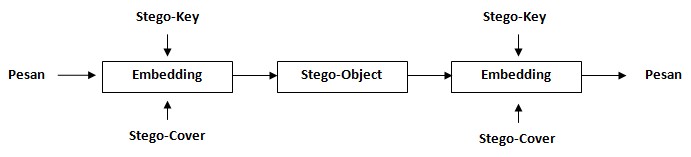
### Steganografi

Steganografi adalah ilmu, teknik atau seni menyembunyikan pesan rahasia atau tulisan rahasia sehingga keberadaan pesan tidak terdeteksi orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi berasal dari bahasa yunani yaitu *steganos* yang artinya tersembunyi atau menyembunyikan dan *graphy* yang artinya tulisan.

Catatan pertama tentang steganografi ditulis oleh Herodotus, yaitu seorang sejarawan yunani. Herodotus mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Caranya dengan menuliskan pesan diatas kepala budak yang telah dibotaki, ketika rambut telah tumbuh, budak tersebut diutus untuk membawa pesan rahasia dibalik rambutnya.

Bangsa romawi sendiri melakukannya dengan menggunakan tinta tak-tampak (*invisible ink*) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan diatas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Kini, istilah steganografi termasuk penyembunyian data digital dalam *file* komputer. Untuk menyisipkan data yang ingin disembunyikan membutuhkan dua unsur. Unsur pertama adalah media penampung seperti citra, suara, video dan sebagainya yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia. Unsur kedua adalah pesan yang ingin disembunyikan yaitu media penampungnya berupa citra yang disebut cove*r*-*object* dan citra yang telah disisipi pesan disebut stego-*object*.



**Gambar 2.1** Cara Kerja Steganografi

Secara umum, terdapat dua proses didalam steganografi, yaitu proses *embedding* untuk menyisipkan pesan ke dalam *cover*-*object* dan proses *decoding* untuk ekstraksi pesan dari *stego*-*object*. Kedua proses ini mungkin memerlukan kunci rahasia yang dinamakan *stego*-*key* agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Dalam steganografi terdapat istilah-istilah yang sering digunakan. Beberapa istilah yang digunakan tersebut adalah sebagai berikut:

1. *Cover*-*Object*

*Cover*-*Object* adalah suatu objek atau media yang digunakan sebagai wadah penyisipan pesan.

1. *Stego*-*Object*

*Stego*-*object* adalah hasil dari steganografi tersebut yakni *cover*-*object* yang telah dimasukkan informasi rahasia di dalamnya.

1. *Stego*-*Key*

*Stego* *key* adalah kunci steganografi yang digunakan untuk embedding message atau mengekstraknya sehingga informasi dapat dipisahkan dari *cover*-*object*.

1. *Embedding*

*Embedding* merupakan proses menyembunyikan pesan ke dalam berkas atau media yang disebut *cover*. kemudian *cover* dan pesan yang mengandung pesan rahasia disebut *Stego*-*Object.*

1. *Extraction*

*Extraction* adalah proses menguraikan pesan yang tersembunyi dalam *Stego*-*Object*.

Beberapa kriteria yang harus diperhatikan dalam penyembunyian data adalah :

* + - 1. Tidak dapat dipersepsi *(Imperceptibility)*

Keberadaan pesan rahasia tidak dapat dipersepsi oleh indera manusia. Jika pesan disispkan kedalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli saat dilihat dengan mata.

* + - 1. Ketepatan *(Fidelity)*

Kualitas citra penampung tidak jauh berubah setelah penyisipan data rahasia. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

* + - 1. Kapasitas *(Capacity)*

Berhubungan dengan jumlah informasi yang dapat disisipkan ke dalam media penampung.

* + - 1. Ketahanan *(Robustness)*

Data yang disembunyikan harus tahan terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung.

* + - 1. Tidak terdeteksi *(Undetecability)*

Kemampuan untuk menghindari deteksi oleh indra manusia maupun analisis statistik.

* + - 1. Pemulihan *(Recovery)*

Data yang disembunyikan harus dapat diungkapkan kembali.

Untuk melakukan penyisipan pesan baik itu pada pesan teks, gambar, suara dan video dibutuhkan masukan berupa *file* digital yang akan disisipkan pesan, pesan yang akan disisipkan (*message*), dan kunci (*key*).

Beberapa contoh *cover-object* atau media penyembunyian informasi rahasia yang digunakan dalam teknik steganografi menurut (Rohayah dkk., 2015) antara lain adalah :

Teks

Dalam algoritma steganografi yang menggunakan teks sebagai media penyisipannya biasanya digunakan teknik *NLP (Natural Language Processing)* sehingga teks yang telah disisipi pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya.

1. Gambar

Format gambar paling sering digunakan, karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma steganografi untuk media penampung yang berupa citra.

1. Suara

Format suara sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar. Sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula.

1. Video

Format video memang merupakan format dengan ukuran *file* yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.

Untuk melakukan steganografi terdapat banyak metode yang dapat digunakan. Berikut adalah beberapa metode yang dapat digunakan dalam steganografi, antara lain:

1. *Least Significant Bit* (LSB)

LSB adalah bagian dari barisan data biner yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Metode LSB merupakan metode yang sangat populer dimana LSB dari setiap *byte* dalam sebuah citra dapat digunakan untuk menyimpan data. LSB juga merupakan metode paling sederhana dan pesan yang disembunyikan cukup aman. Selain itu, metode LSB memiliki kelebihan-kelebihan seperti mudah dan cepat secara algoritma, semua jenis *file* digital dapat dijadikan *sampling* dan pesan yang disembunyikan dapat memiliki ukuran yang besar.

1. *End Of File* (EOF)

Metode *End Of File* (EOF) merupakan salah satu teknik untuk menyisipkan data pada akhir *file* dan merupakan pengembangan daripada metode *Least Significant Bit* (LSB). Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran *file* asli (sebelum disisipkan data) ditambah dengan ukuran data yang akan disisipkan ke *file* tersebut. Dalam teknik EOF, data yang disisipkan pada akhir diberi tanda khusus sebagai pengenal *start* dari data tersebut dan pengenal akhir dari data tersebut.

Teknik EOF tidak akan mengubah isi awal dari *file* yang disisipi. Sebagai contoh, jika akan menyisipkan sebuah pesan ke dalam sebuah *file* audio, maka file audio tidak berubah, tidak rusak dan dapat diputar seperti *file* audio asli. Ini yang menjadi salah satu keunggulan metode EOF dibandingkan dengan metode steganografi yang lain. Karena disisipkan pada akhir *file*, pesan yang disisipkan tidak bersinggungan dengan isi *file*, hal ini menyebabkan integritas data dari *file* yang disisipi tetap dapat terjaga. Namun, metode EOF akan mengubah besar ukuran *file* sesuai dengan ukuran pesan yang disisipkan ke dalam *file* awal, namun tidak mengubah format file dari media yang dipakai sebagai tempat penyisipan pesan tersebut. (Fauzi Achmad & Putri, 2017).

1. *Discrete Cosine Transform* (DCT)

*Discrete Cosine Transform* (DCT) adalah sebuah teknik untuk mengubah sinyal ke dalam komponen frekuensi dasar. Dengan menggunakan fungsi gelombang *cosinus diskrit*, konsep yang digunakan pada metode DCT adalah mengganti koefisien DCT pada citra asli menjadi koefisien baru. Pemilihan koefisien yang diganti tergantung pada pemilihan frekuensi. Jika frekuensi yang dipilih adalah frekuensi tinggi dan koefisien yang dihasilkan bernilai rendah, maka citra yang dihasilkan tidak mengalami perubahan sehingga tidak terlihat oleh indera penglihatan manusia atau bisa disebut nilai *invisibility* tinggi. Tetapi penggunaan frekuensi ini menyebabkan citra lemah terhadap perubahan atau bisa disebut nilai *robustness* rendah. Sebaliknya jika yang dipilih adalah koefisien bernilai rendah dan koefisien yang dihasilkan tinggi, maka citra hasil proses ini tahan terhadap perubahan atau bisa disebut nilai *robustness* tinggi namun perubahan pada citra ini mudah terlihat atau bisa disebut nilai *invisibility* rendah. (Choirunnisa, dkk, 2018).

1. *Discrete Wavelet Transform* (DWT)

Metode DWT melakukan dekomposisi suatu gambar menjadi empat bagian yaitu subband koefisien aproksimasi (LL), detil horisontal (HL), detil vertikal (LH), dan detil diagonal (HH). Proses penyisipan teks dilakukan pada subband LL menggunakan metode *Lempel Ziv Welch* (LZW). Induk wavelet yang digunakan adalah *Daubechies* 4 (Db4). Kelebihan dari metode DWT yaitu kualitas gambar yang menjadi tempat penyisipan teks tidak jauh berubah dari kualitas media asli (Prawirawan dkk., 2012).

* 1. **Format Citra Digital**

Dalam citra digital terdapat dua format gambar berdasarkan jenis kompresinya yaitu *lossless* dan *lossy*.

* + 1. *Lossless*

Metode *lossless* merupakan algoritma kompresi data yang memungkinkan data asli direkonstruksi secara tepat dari data yang terkompresi. Kompresi data *lossless* digunakan dalam perangkat lunak kompresi seperti format Zip, PKZIP dan WinZip, dan program Unix bzip2 dan gzip. Beberapa format *file* gambar yang menggunakan metode ini antara lain PNG dan GIF.

Dalam teknik kompresi *lossless* terdapat beberapa algoritma, diantaranya algoritma *Run Length Encoding* (RLE), *Adaptive Dictionary Based* (*Lempel-Ziv-Welch* disingkat LZW), dan *Entropy Encoding* (*Huffman Encoding* dan *Arithmetic Encoding*). Jika algoritma *Run Length Encoding* (RLE) yang diimplementasikan maka akan dihasilkan citra digital dengan format file *Bitmap Picture* (BMP), kemudian algoritma *Adaptive Dictionary Based* (*Lempel-Ziv-Welch* disingkat LZW) akan menghasilkan citra digital dengan format *file* *Graphic Interchange Format* (GIF), dan yang terbaru algoritma *Adaptive Dictionary Based* (*Lempel-Ziv-Welch* disingkat LZW) dikombinasikan dengan algoritma *Huffman Encoding* akan dihasilkan citra digital dengan format *file* *Portable Network Graphics* (PNG). (Wiryawan, dkk, 2019)

* + 1. *Lossy*

*Lossy* kompresi adalah suatu metode untuk mengkompresi data dan mendekompresinya, data yang diperoleh mungkin berbeda dari yang aslinya tetapi cukup dekat perbedaaanya. *Lossy* kompresi ini paling sering digunakan untuk kompres data multimedia (Audio, gambar diam). Sebaliknya, kompresi *lossless* diperlukan untuk data teks dan *file*, seperti catatan bank, artikel teks dll.

Format kompresi *lossy* mengalami *generation* *lossy* yaitu jika melakukan berulang kali kompresi dan dekompresi file akan menyebabkan kehilangan kualitas secara progresif. Hal ini berbeda dengan kompresi data *lossless*. ketika pengguna yang menerima file terkompresi secara *lossy* (misalnya untuk mengurangi waktu download) *file* yang diambil dapat sedikit berbeda dari yang asli dilevel bit ketika tidak dapat dibedakan oleh mata dan telinga manusia untuk tujuan paling praktis. Metode ini menghasilkan ratio kompresi yang lebih besar daripada metode *lossless*. Misal terdapat *image* asli berukuran 12,249 bytes, kemudian dilakukan kompresi dengan JPEG kualitas 30 dan berukuran 1,869 bytes berarti *image* tersebut 85% lebih kecil dan ratio kompresi 15%. Contoh metode *lossy* adalah metode CS&Q (*coarser sampling and/or quantization*), JPEG, dan MPEG. Ada dua skema dasar *lossy* kompresi :

1. *Lossy transform codec*, sampel suara atau gambar yang diambil, di potong kesegmen kecil, diubah menjadi ruang basis yang baru, dan kuantisasi. hasil nilai kuantisasi menjadi *entropy coded*.
2. *Lossy predictive codec*, sebelum dan/atau sesudahnya data di-*decode* digunakan untuk memprediksi sampel suara dan *frame picture* saat ini. kesalahan antara data prediksi dan data yang nyata, bersama-sama dengan informasi lain digunakan untuk mereproduksi prediksi, dan kemudian dikuantisasi dan kode.

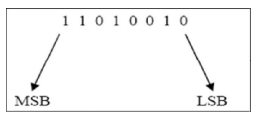
Dalam beberapa system kedua teknik digabungkan, dengan mengubah kode yang digunakan untuk mengkompresi kesalahan sinyal yang dihasilkan dari tahapan prediksi.(Sembiring, 2018)

* 1. **Algoritma *Least Significant Bit* (LSB)**

Teknik steganografi dengan menggunakan metode *Least Significant Bit* (LSB) adalah teknik yang paling sederhana untuk menyisipkan informasi di dalam suatu citra digital.

Ukuran data yang dapat disembunyikan bergantung pada ukuran data penampung. Misalkan saja pada *file* citra 8-bit yang berukuran 256x256 piksel memiliki potensi untuk menyembunyikan 65536 bit (65536/8 = 8192 *bytes*) informasi.

Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti (*Most Significant Bit* atau MSB) dan bit yang paling kurang berarti (*Least Significant Bit* atau LSB).



**Gambar 2.2** MSB dan LSB

Sebagai contoh, akan dilakukan proses penyembunyian karakter ‘H’ (ASCII 72) pada *file* *carrier* yang berukuran 8 *byte*. LSB dari *file* *carrier* ditandai dengan garis bawah. Berkas *carrier* berukuran 8 *byte* dalam biner pada Gambar 2.3.

1001010**1** 0000110**1** 1100100**1** 1001011**0**

0000111**1** 1100101**1** 1001111**1** 0001000**0**

**Gambar 2.3** *file carrier* 8 *byte*

Pesan yang akan disisipkan adalah karakter “H” (ASCII 72), yang nilai binernya adalah 01001000, Kedelapan bit kemudian dimasukkan dari tiap-tiap *byte* pada *file* *carrier* menjadi seperti berikut :

1001010**0** 0000110**1** 1100100**0** 1001011**0**

0000111**1** 1100101**0** 1001111**0** 0001000**0**

**Gambar 2.4** Stego *file carrier* 8 *byte*

Pada contoh di atas, perubahan hanya terjadi pada bit-bit paling terakhir dari *file* *carrier* (ditandai dengan karakter berwarna merah). Bedasarkan teori maka didapatkan bahwa ukuran *file* asli tidak mengalami perubahan yang begitu besar sehingga sulit terdeteksi oleh indra manusia.

Metode LSB memiliki kelebihan-kelebihan diantaranya adalah mudah dan cepat secara algoritma, semua jenis *file* digital dapat dijadikan *sampling*, pesan yang disembunyikan dapat memiliki ukuran yang besar, dan ukuran citra yang mengandung pesan rahasia tidak berubah atau sama seperti aslinya.

* 1. **MSE dan PSNR**

Kualitas gambar yang baik dari *file* citra steganografi adalah syarat penting kesuksesan algoritma steganografi. Salah satu cara untuk menghitung nilai kualitas dari *file* citra steganografi menggunakan persamaan *Means Square Error (MSE)* dan *Peak Signal to Noise Ratio (PSNR). Means Square Error (MSE)* adalah rata-rata kuadrat nilai kesalahan antara citra asli dengan citra manipulasi. Secara matematis dapat ditulis seperti persamaan 2.1:

...................................(2.1)

Keterangan:

M = panjang citra *stego*

N = lebar citra *stego*

f(x,y) = nilai piksel dari citra *cover*

g(x,y) = nilai piksel pada citra *stego*

Semakin rendah nilai MSE maka akan semakin baik. Setelah diperoleh nilai MSE maka nilai *Peak Signal to Noise Ratio (PSNR)* dapat dihitung, yang dimana PSNR adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya nilai eror yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan desibel, PSNR digunakan untuk mengetahui perbandingan kualitas *cover-image* sebelum dan sesudah disisipkan pesan. Secara matematis dapat ditulis seperti persamaan 2.2:

..........................................................................(2.2)

Keterangan:

MSE = nilai MSE

c = nilai maksimum dari piksel citra

Semakin besar nilai PSNR maka akan semakin baik kualitas citra steganografi. Kualitas citra dapat disimpulkan cukup baik jika nilai PSNR memenuhi standar yaitu di atas 30dB – 40dB (Lubis, dkk, 2015).