Jurnal Nasional Komputasi dan Teknologi Informasi
Vol. 4 No. 1, Februari 2021
P-ISSN 2620-8342
E-ISSN 2621-3052

Steganografi Penyisipan Pesan Pada File Citra Menggunakan Metode LSB (Least Significant Bit)

Buha Johannes Simbolon
STMIK Pelita Nusantara
Jl. Iskandar Muda No. 1 Medan 20154 Indonesia
Corresponding author's e-mail: simbolon19.js19@gmail.com

Abstrak—Perkembangan teknologi yang sangat pesat tidak hanya memberikan dampak positif, namun juga dapat memberikan dampak negatif bagi para pengguna teknologi tersebut. Salah satunya adalah berkembangnya cyber crime yang menyebabkan pesan menjadi tidak aman untuk dilindungi. Keamanan pesan dapat dilindungi dengan menggunakan steganografi untuk mengubah pesan menjadi sandi rahasia. Agar sandi rahasia lebih aman maka digunakan teknik steganografi. Steganografi merupakan teknik penyembunyian pesan dengan menyisipkan pesan ke dalam wadah lain. Pada penelitian ini digunakan kombinasi dari dua algoritma, yaitu algoritma Kriptografi RC4 dan Base, yang lebih dikenal dengan algoritma Super Enkripsi dan teknik steganografi menggunakan metode Least Significant Bit (LSB) dengan penyisipan pixel secara acak menggunakan pseudorandom number generator (PRNG). Penggunaan algoritma. ruang lingkup masalah adalah media penyisipan informasi yang digunakan, proses pembuatan data menjadi informasi dan pengiriman kepada penerima pesan, metode yang digunakan dalam penulisan skripsi menggunakan LSB (Least Significant Bit) dan bahasa pemrograman yang digunakan dalam membangun sistem ini adalah PHP (Hypertext Preprocessor) dengan Database MySQL *(My Structured Query Language)* pada *PhpMyAdmin.*
Kata kunci: Metode LSB, Penyisipan Informasi, File Citra, Steganografi

Abstract — The rapid development of technology not only has a positive impact, but can also have a negative impact on the users of this technology. One of them is the development of cyber crime which causes messages to be unsafe to protect. Message security can be protected by using steganography to convert messages into secret passwords. To make the secret password more secure, steganography techniques are used. Steganography is a technique for hiding messages by inserting messages into other containers. In this study, a combination of two algorithms is used, namely the RC4 and Base Cryptography algorithm, which is better known as the Super Encryption algorithm and the steganography technique using the Least Significant Bit (LSB) method with random pixel insertion using a pseudorandom number generator (PRNG). Algorithm use. the scope of the problem is the information insertion media used, the process of making data into information and sending to message recipients, the method used in writing the thesis using LSB (Least Significant Bit) and the programming language used in building this system is PHP (Hypertext Preprocessor) with MySQL database (My Structured Query Language) on PhpMyAdmin.
Keywords: LSB Method, Information Insertion, Image Files, Steganography

1. Pendahuluan

Salah satu tehnik yang digunakan dalam mengamankan informasi adalah kriptogafi. Teknik ini melakukan proses pengacakan data asli sehingga dihasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya. Tindakan pengamanan menggunakan cara tersebut ternyata dianggap belum cukup dalam mengamankan suatu informasi karena adanya peningkatan kemampuan komputasi.

Berbeda dengan teknik kriptografi, steganografi menyembunyikan pesan rahasia agar orang awam tidak menyadari keberadaan dari pesan yang disembunyikan [1]. Caranya dengan menyembunyikan informasi rahasia di dalam suatu wadah penampung informasi dengan sedemikian rupa sehingga keberadaan informasi rahasia yang ditempelkan tidak terlihat. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut.

Steganografy dan kriptogarfy adalah saudara sepupu dalam spycraft. Perbedaan mendasar antara steganografi dan kriptografi terletak pada proses penyembunyian data dan hasil akhir dari proses dimana pada kriptografi pesan yang sudah disisipi pesan rahasia akan sangat berbeda dengan pesan sebelum disisipi pesan rahasia, sedangkan pada steganografi, pesan yang sudah disisipi pesan rahasia akan tampak sama (dengan kasat mata) dengan pesan sebelum disisipi pesan rahasia (pesan rahasia tersamarkan dalam cover text). *Steganografy* yang berbasis *computer – based* diterapkan menggunakan berbagai media *cover* (media penyisipan) [2]. Beberapa contoh media penyisipan pesan rahasia yang digunakan dalam teknik steganografy dalah teks, audio

(suara), citra (gambar) dan vidio.

Metode LSB *(Least Significant Bit)* merupakan salah satu metode dalam teknik steganography pengisipan pesan informasi kedalam file citra [3][4]. Least Significant Bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil, letaknya adalah paling kanan dari barisan bit. Contohnya adalah bilangan biner dari 255 adalah 11111111 (kadang-kadang diberi huruf b pada akhir bilangan menjadi 11111111b). Bilangan tersebut dapat berarti: 1*27+1*26+1*25+1*23+1*22+1*21+1*20=128+64+32+16+84+2+1=255, dimana dari barisan angka 1 diatas, angka 1 paling kanan bernilai 1, dan itu adalah yang paling kecil, bagian tersebut disebut dengan *Least Significant Bit* (bit yang paling tidak berarti). *Least Significant Bit* digunakan untuk kepentingan penyisipan data kedalam suatu media digital lain, salah satu yang memanfaatkan metode Least Significant Bit ini sebagai metode penyembunyian data adalah *steganography* [5]. Peneliti sebelumnya dalam Jurnal TAM *(Technology Acceptance Model)*, yang berjudul Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image, yaitu pada penelitian ini sistem yang dibangun hanya dapat di akses di komputer itu sendiri dan tidak berbasis *web*. [6]

2. Tinjauan Pustaka

2.1. Steganografi *(Steganography)*

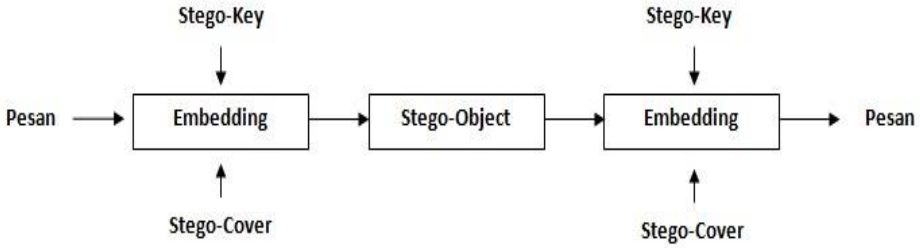
Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain sipengirim dan sipenerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Contoh singkat yang dapat dijelaskan adalah pengirim memilih gambar yang ingin dititipi informasi, kemudian mengatur setiap warna *pixel* ke-100 untuk menyesuaikan huruf dalam *alphabet*. Setiap perubahan yang terjadi diamati dan dicatat, perubahan yang begitu halus atau tanpa cacat dalam kondisi fisik gambar tersebut sehingga tidak ada pihak lain yang menyadarinya bahwa didalam gambar tersebut terdapat sebuah informasi yang bersifat rahasia jika pihak lain tidak benar-benar memperhatikannya menggunakan aplikasi untuk mendeteksi informasi tersembunyi dalam gambar digital [7]. Pulung Nurtantio Andono, T. Sutojo dan Muljono berpendapat bahwa steganografi (*Steganography*) adalah merupakan seni untuk menyembunyikan pesan didalam media digital sedemikian rupa, sehingga orang lain tidak menyadari ada suatu pesan didalam media tersebut [8]. Jubilee Enterprise mengatakan bahwa steganografi adalah paduan antara seni dan ilmu pengetahuan yang mempelajari cara menuliskan pesan tersembunyi. Pulung Nurtantio Andono, T. Sutojo dan Muljono menjelaskan bahwa 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 cover-object dan citra yang telah disisipi pesan disebut *stego-object* [9].

2.2. Teknik Steganografi *(Steganography)*

Teknik dalam penyisipan pesan pada media digital yaitu sebagai berikut [10] [11] :

1. Injection merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut embedding.
2. Substitusi, Data normal digantikan dengan data rahasia. Biasanya, hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
3. Transformasi Domain, teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada transform space.
4. Spread Spectrum, Spread spectrum merupakan teknik pentransmisian menggunakan pseudo-noise code, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (bandwith) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika pseudo-noise code tersinkronisasi.
5. Statistical Method, teknik ini disebut juga skema steganographic 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. Distortion, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.

7. Cover Generation, metode ini lebih unik daripada metode lainnya karena cover object dipilih untuk menyembunyikan pesan.ilmiah lainnya.



Gambar 1. Prinsip atau Cara Kerja Steganografi

3. Metode Penelitian

Dalam menganalisa masalah yang perlu dilakukan adalah identifikasi masalah, merumuskan masalah dan menentukan manfat dan tujuan sistem yang akan dibangun. Tahapan penelitian :

a. Mengidentifikasi Masalah

Merupakan tahap yang dilakukan dalam penelitian untuk mencari, menemukan, mengumpulkan, meneliti, mendaftarkan, mencatat data dan informasi yang dibutuhkan dalam membangun aplikasi penyisipan informasi kedalam file citra dengan menggunakan metode steganogafi.

b. Pengumpulan Data

Referensi ini dapat dicari dari buku, jurnal, artikel laporan penelitian, dan situs-situs di internet. Output dari studi literatur ini adalah terkoleksinya referensi yang relevan dengan perumusan masalah, tujuannya adalah untuk memperkuat permasalahan serta sebagai dasar teori dalam melakukan studi dan juga menjadi dasar untuk melakukan desain kendali dan simulasi alur dalam aplikasi penyisipan informasi kedalam file citra dengan menggunakan metode steganografi.

c. Proses Steganografi Menggunakan Metode LSB (Least Siginificant Bit)

Setelah dilakukan pengumpulan data dan data telah terkumpul, maka tahap selanjutnya adalah dilakukan analisa atau proses terhadap data yang telah dikumpulkan sebelumnya dengan menggunakan metode least siginificant bit dengan tujuan agar rumusan masalah dapat teratasi sehingga aplikasi penyisipan informasi kedalam file citra dengan menggunakan metode steganografi ini dapat bermanfaat.

d. Perancangan sistem adalah merupakan tahapan setelah dilakukan proses analisa data menggunakan metode steganografi. Perancangan sistem ini bertujuan untuk menggambarkan sistem yang akan dibangun nantinya.

e. Implementasi merupakan kegiatan akhir dari proses penerapan sistem baru dimana tahap ini merupakan tahap meletakkan sistem supaya siap untuk dioperasikan dan dapat dipandang sebagai usaha untuk mewujudkan sistem yang telah dirancang.

4. Hasil dan Pembahasan

Permasalahan yang berkaitan dengan aplikasi Steganografi untuk penyisipan pesan yaitu pada penyisipan pesan pada teks, gambar, suara dan video. Adapun penyisipan pada pesan teks berformat (pdf dan doc), pada file gambar berformat (jpg, png, bmp dan gift), pada file suara berformat (mp3, wav dan wma), serta pada file video berformat 3gp. Dalam pengumpulan data aplikasi ini menggunakan cara studi pustaka yakni mengumpulkan data dan informasi dari buku teks dan internet yang berkaitan dengan pembuatan aplikasi Steganografi tersebut. Untuk keamanan pesan, Steganografi memiliki tiga cara kerja yaitu hidden text, algoritma penyisipan dan algoritma pendeteksian. Sesuai dengan tujuan Steganografi itu sendiri yaitu menyembunyikan isi pesan, maka dibutuhkan sebuah aplikasi Steganografi untuk penyisipan pesan.

Analisis Steganografi dilakukan dengan memodifikasi bit-bit yang termasuk bit pada setiap byte warna pada sebuah pixel. Bit-bit ini akan dimodifikasi dengan menggantikan setiap bit yang ada dengan bit bit informasi lain yang ingin disembunyikan. Setelah semua bit informasi lain menggantikan bit di dalam file tersebut, maka informasi telah berhasil disembunyikan. Ketika informasi rahasia tersebut ingin kembali dibuka, maka bit-bit yang sekarang ada, diambil satu per satu kemudian disatukan kembali menjadi sebuah informasi yang utuh seperti semula. Penentuan bit-bit dilakukan secara berurutan, mulai dari byte awal sampai byte terakhir sesuai panjang dari data rahasia yang akan disembunyikan. Mengubah bit hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya tidak berpengaruh terhadap persepsi visual/auditori. Untuk proses analisis penyisipan pesan informasi pada media citra menggunakan metode steganografi terdapat dua proses

analisis yaitu embedding dan ekstraksi. Analisis Ekstraksi Citra Stego Menggunakan Metode LSB (*Least Siginificant Bit*)

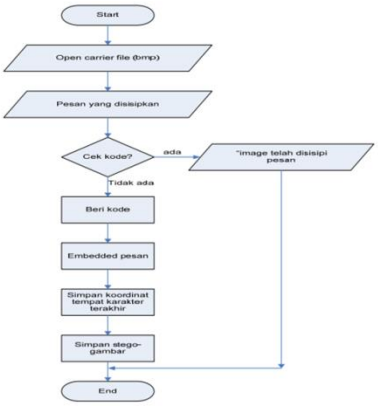
Setelah dilakukan penyisipan pesan kedalm file citra gambar, maka sipenerima pesan melakukan ekstraksi pada sebuah citra steganografi yang berukuran 4x4 piksel, sehingga pesan yang terkandung didalamnya adalah dengan menggunakan beberapa langkah berikut ini :

Ambil pesan dari citra steganografi,

105 (GANJIL), maka bit pesan = 1
200 (GENAP), maka bit pesan = 0
56 (GENAP), maka bit pesan = 0
69 (GANJIL), maka bit pesan = 1
179 (GANJIL), maka bit pesan = 1
144 (GENAP), maka bit pesan = 0
49 (GANJIL), maka bit pesan = 1
22 (GENAP), maka bit pesan = 0

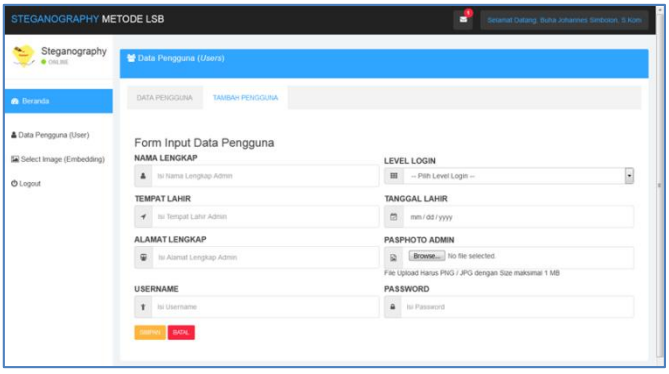
$$\begin{bmatrix} 105 & 200 & 56 & 69 \\ 179 & 144 & 49 & 22 \\ 143 & 211 & 54 & 68 \\ 153 & 174 & 58 & 98 \end{bmatrix}$$

Urutkan bit pesan dimulai dari MSB (*Most Siginifacnt Bit*) : pesan = 1 0 0 1 1 0 1 0. Sehingga setelah di urutkan pesan, maka pesan yang terkandung didalam file citra adalah : Pesan = 154. Gambar 2 menjelaskan diagram alir proses embedding pesan ke media file citra.



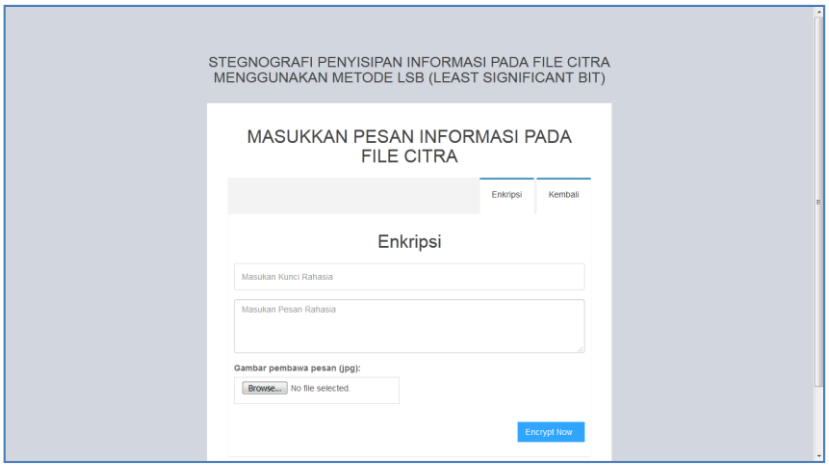
Gambar 2. Diagram Alir Proses Embedding Pesan Pada Media File Citra

Sebelum menjalankan program sistem informasi steganografi penyisipan pesan pada file citra dengan menggunakan metode LSB (Least Significant Bit) ini, maka terlebih dahulu program di hosting ke server agar bisa di akses. Misalnya di server localhost : http://localhost/steganografi-lsb/, setelah di hosting maka buka browser internet, misalnya : Mozila Firefox, Internet Explorer, Opera dan Chrome, maka tampillah halaman utama website steganografi penyisipan pesan pada file citra dengan menggunakan metode LSB (Least Significant Bit).



Gambar 3. Tampilan Form Input Data Pengguna

Tampilan Form Input Data Pengguna (User) merupakan implementasi tampilan antarmuka form input data pengguna (user). Tampilan form ini berfungsi untuk menambahkan data pengguna (user) dan tampilan form ini hanya bisa di akses di halaman utama pengirim pesan informasi steganografi.



Gambar 4. Tampilan Form Input Data Enkripsi Pesan Informasi Steganografi

Tampilan Form Input Data Enkripsi Pesan Informasi Steganografi merupakan implementasi tampilan antarmuka form input data enkripsi pesan infomasi steganografi pada file citra menggunakan metode LSB (Least Siginificant Bit). Tampilan form ini berfungsi untuk menambahkan data enkripsi pesan informasi steganografi pada file citra dan tampilan form ini hanya bisa di akses di halaman utama pengirim pesan informasi steganografi.


Gambar 5. Citra Belum Disisipi Pesan


Gambar 6. Citra Disisipi Pesan

5. Kesimpulan

Kesimpulan dari penelitian :

1. Steganografi penyisipan pesan pada file citra menggunakan metode LSB (Least Significant Bit) dapat digunakan oleh seseorang dalam melindungi dan menyembunyikan pesan rahasia dari cyber crime.
2. Dengan menggunakan aplikasi steganografi ini dalam menyisipkan pesan pada file citra maka bisa menghasilkan hasil yang maksimal dalam mengamankan pesan rahasia, terbukti dengan hasil penerapan menggunakan metode LSB (Least Significant Bit) sesuai dengan perancangan sistem yang dibangun.
3. Aplikasi dapat menyediakan informasi hasil analisa penyisipan pesan pada file citra menggunakan metode LSB (Least Significant Bit).

Daftar Pustaka

[1] Aldo and L. Hakim, "Implementasi Steganografi Pada Citra Digital dan Kriptografi Algoritma Hill Cipher Untuk Pengamanan Informasi Berupa Text," *J. Ilm. Teknol. Inf. Terap.*, vol. V, no. 1, pp. 6–17, 2018.

[2] U. A. Anti, A. H. Kridalaksana, and D. M. Khairina, "Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF)," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 12, no. 2, p. 104, 2017.

[3] Bakir and Hozairi, "Implementasi Metode Least Significant Bit (LSB) Dengan Enkripsi Cipher Caesar Pada Steganografi Menggunakan Image Processing," pp. 75–81, 2018.

[4] R. Islamadina and B. Baihaqi, "Analisa Steganografi untuk Citra Bewarna (RGB) Menggunakan Metode

Less Significant Bit (LSB)," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 2, no. 1, pp. 55–64, 2019.
[5] 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.
[6] L. M. Jannah, I. Santoso, and Y. Christyono, "Kinerja Steganografi Metode End of File Pada Data Citra Digital," *Transient*, vol. 7, no. 1, p. 34, 2018.
[7] L. P. Malese, "Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (Lsb)..," vol. XIII, no. November, pp. 96–101, 2020.
[8] Novelius Buulolo and A. Sindar, "Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard)," *J. Ilm. Teknol. Inf.*, vol. XV, no. November, pp. 61–65, 2020.
[9] B. Purnama and I. S. Wijaya, "Perancangan Aplikasi Steganografi Teknik LSB (Least Significant Bit) Dalam Keamanan Komputer," *J. Ilm. Media Process.*, vol. 9, no. 1, pp. 77–88, 2014.
[10] A. S. R. Sinaga and E. Marpaung, "Segmentasi Warna HSV Telapak Tangan Untuk Deteksi Bakteri Pada Pendemi Covid 19," *Fountain Informatics J.*, vol. 5, no. 3, p. 1, 2020.
[11] B. Sitohang and A. Sindar, "Analisis Dan Perbandingan Metode Sobel Edge Detection Dan Prewit Pada Deteksi Tepi Citra Daun Srilangka," vol. 3, no. 3, pp. 314–322, 2020.