IMPLEMENTASI APLIKASI STEGANOGRAFI BERBASIS WEB MENGGUNAKAN ALGORITMA LSB DAN BPCS

Laily Farkhah Adhimah[1], Isti Nurhafiyah[2],
Adnan Aditya Muntahar[3], Fandi Kristiaji[4] , Dinar Mustofa[5]

[1,2,3,4,5] Informatika, Universitas Amikom Purwokerto
Jl. Letjend Pol. Soemarto No.127, Watumas, Purwanegara,
Kec. Purwokerto Utara, Kabupaten Banyumas, Jawa Tengah 53127
E-mail :lailyfarkhaha@gmail.com[1], istinurhafiyah15@gmail.com[2], adnanadityam9@gmail.com[3]
fkristiaji15@gmail.com[4] , dinar.mustofa@amikompurwokerto.ac.id[5]

Abstrak

Steganografi merupakan teknik yang digunakan untuk menyembunyikan data yang berisi informasi rahasia dalam data yang tampak normal. Dalam beberapa tahun terakhir, penggunaan steganografi dalam aplikasi web telah menjadi populer karena kemudahan akses dan kemampuannya untuk menyembunyikan data dalam berbagai jenis media. Tujuan penelitian ini yaitu untuk mengimplementasikan sebuah aplikasi steganografi berbasis web yang menggunakan algoritma *Bit-Plane Complexity Segmentation* (BPCS) dan *Least Significant Bit* (LSB). Dalam tahap perancangan, sistem dikembangkan menggunakan bahasa, seperti CSS, HTML, dan JavaScript agar pengguna dapat mengakses aplikasi melalui browser. Algoritma LSB dan BPCS digunakan sebagai metode untuk menyisipkan data rahasia ke dalam gambar yang dipilih oleh pengguna. LSB adalah metode steganografi yang sederhana di mana bit terakhir dari setiap piksel gambar digunakan untuk menyimpan bit informasi rahasia. Sementara itu, BPCS merupakan metode steganografi yang lebih kompleks, yang menggabungkan analisis domain spasial dan frekuensi untuk menyembunyikan data dalam gambar dengan kualitas yang tinggi. Hasil penelitian ini menunjukkan bahwa aplikasi steganografi berbasis web menggunakan algoritma LSB dan BPCS dapat berhasil mengimplementasikan metode penyembunyian data rahasia dalam gambar secara efektif.
Kata Kunci: Steganografi, aplikasi web, LSB, BPCS, penyisipan data, gambar steganografi.

Abstract

Steganography is a method for concealing sensitive information in seemingly unremarkable data. In recent years, the use of steganography in web applications has become popular due to its accessibility and ability to conceal data in various types of media. Implementing a web-based steganography program that makes use of the Bit-Plane Complexity and Least Significant Bit algorithms is the aim of this project. To enable users to access the application through a browser, the system is constructed utilizing web technologies like HTML, CSS, and JavaScript during the design phase. The LSB and BPCS algorithms are employed as methods to embed secret data into user-selected images. The least significant bit of each image pixel is utilized to hold a secret piece of information using the straightforward steganography technique known as LSB. On the other hand, BPCS is a more complex steganography method that combines spatial and frequency domain analysis to hide data within high-quality images. The findings of this study show that the technique of hiding sensitive information within photos is successfully implemented by the web-based steganography program employing the LSB and BPCS algorithms.
Keywords: *Steganography, web application, LSB, BPCS, data embedding, steganographic images.*

1. PENDAHULUAN

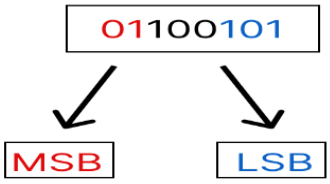
Kehidupan manusia sangat dipengaruhi oleh teknologi yang sangat maju dalam bidang informasi dan komunikasi, berbagai media sekarang dapat digunakan dengan mudah untuk menyampaikan informasi. Pengembangan yang pesat dalam teknologi pengiriman proses data memiliki konsekuensi yang sangat signifikan, hal ini meliputi masalah pengiriman dalam keamanan data . Karena proses pengiriman data melalui media biasanya dilakukan secara tidak aman atau tanpa pengamanan, data dikirmkan harus dilindungi dengan cara yang berbeda, salah satunya adalah enkripsi file [1].

Kriptografi, sebagai ilmu yang digunakan untuk mengamanan data, mungkin dapat menyelesaikan masalah tersebut. Salah satu cara untuk melindungi informasi yang sangat penting dalam sebuah file adalah dengan menggunakan kriptografi. Ini terjadi ketika data yang ada di dalam file disandikan atau dienkripsi, yang berarti bahwa yang dapat mengetahui isi file tersbut adalah orang tertentu saja [2]. Banyak algoritma yang telah dikembangkan selama kemajuan ilmu kriptografi saat ini yang dapat digunakan sebagai pengubahah menjadi ciphertext atau symbol tertentu dari data asli (plaintext) [3].

Steganografi membuat kecurigaan lebih sedikit karena data pesan yang disamarkan dan disembunyikan dalam file pesan lainnya. Ini memungkinkan seseorang untuk menyamarkan file pesan ke dalam media tanpa diketahui orang lain bahwa pesan tersebut telah dimasukkan ke dalamnya [4][5]. Hal ini disebabkan fakta bahwa data yang dihasilkan oleh steganografi memiliki bentuk visual yang sama dengan data aslinya jika dilihat oleh panca indera manusia. Pada saat yang sama, perubahan dalam teknologi enkripsi pesan dapat diamati dan dirasakan langsung oleh panca indera manusia. Steganografi menghasilkan objek steganografi setelah data rahasia digabungkan dengan objek penutup. Dalam steganografi, media penyimpanan biasanya adalah suara, gambar, teks, dan video. Data juga bisa berupa suara, gambar, teks, video, atau pesan lainnya. Penelitian ini menggunakan steganografi gambar [6].

Ada beberapa ketidaksamaan penggunaan steganografi dengan kriptografi. Kriptografi mengubah atau mengacak karakter pesan menjadi bentuk lain yang tidak berguna. Karena ketidak bermaknaannya, pesan yang disampaikan dalam kriptografi menjadi mencurigakan. Disebabkan steganografi, pesan terlihat seperti pesan biasa, sehingga sangat tidak mungkin untuk dicurigai. Namun, ini tidak berarti steganografi ini tidak memiliki kelemahan. Apabila format pesan diubah, steganografi ini mengalami kelemahan, karena pesan rahasia hilang.

Pada penelitian ini, kami menggunakan penerapan algoritma Least Significant Bit (LSB), Spread Spectrum Steganography, dan Bit-Plane Complexity Segmentation (BPCS).



Gambar 1. Metode LSB

Angka 0 yang berada di depan disebut Most Significant Bit (MSB) Maka bit LSB pada biner tersebut yaitu angka 1 yang paling kanan atau paling belakang. Ketika bit paling akhir LSB disisipi atau diubah dengan 0 hal tersebut tidak akan mempengaruhi tampilan warna secara jelas (tidak terlihat jelas perbedaannya). Namun jika bit yang disisipi dengan bit yang berbeda maka akan terlihat perbedaan pada citra [7].

Metode steganografi yang paling umum adalah Less Significant Bit (LSB). Karena metode ini tidak akan mengubah gambar digital secara signifikan, maka file yang telah terenkripsi dengan file dalam bentuk dokumen akan disisipkan dengan mengganti bit terkecil (terakhir) dari pixel gambar dengan bit pesan [8]. Upaya yang dapat dilakukan yaitu dengan meminimalisir kemungkinan serangan dengan menggabungkan metode LSB dan algoritma kriptografi untuk penyandian pesan. Sehingga hanya yang memiliki kunci yang dapat mengetahui isi dari pesan tersebut.

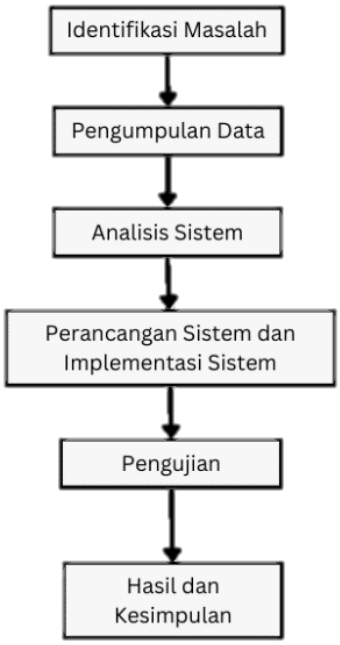
Steganografi umumnya banyak diimplementasikan pada file berupa citra digital. Karena citra digital atau yang biasa disebut gambar adalah format yang paling mudah disebarluaskan melalui web dan komunitas online [9].

Tujuan dari penelitian ini yaitu untuk mengiimplementasikan steganografi berbasis web yang menggunakan algoritma *Bit-Plane Complexity Segmentation* (BPCS) *dan Least Significant Bit* (LSB) dalam menyembunyikan pesan mengguanakan citra digital serta sejauh mana perubahan kualitas pada citra dengan membandingkan kualitas citra hasil (stego image) dengan citra awal (cover image) berdasarkan ukuran filenya. [10]

2. METODOLOGI

2.1. Skema Alur Penelitian

Tahapan penelitiannya adalah sebagai berikut :



Gambar 2. Tahapan Penelitian

1. Identifikasi Masalah

   Pengiriman data tanpa pengamanan menjadi masalah signifikan dalam era teknologi informasi saat ini. Kebutuhan akan keamanan data semakin mendesak, terutama untuk melindungi informasi sensitif. Kriptografi, sebagai ilmu pengamanan data, menyediakan solusi dengan mengubah data menjadi bentuk tidak terbaca tanpa kunci dekripsi. Namun, steganografi juga menjadi alternatif yang menarik dengan kemampuannya untuk menyamarkan pesan dalam media lain tanpa menimbulkan kecurigaan. Oleh karena itu, kriptografi dan steganografi memiliki peran penting dalam memastikan keamanan dan integritas data sensitif. Dalam tahap ini, peneliti mengidentifikasi masalah yang dihadapi dalam konteks steganografi. Fokus pada kebutuhan untuk mengembangkan sebuah aplikasi steganografi berbasis web menggunakan algoritma LSB dan BPCS untuk memenuhi kebutuhan dan tuntutan keamanan informasi.

2. Pengumpulan Data

   Data dikumpulkan melalui Tinjauan Pustaka (Library Research) dan dokumentasi, seperti membaca buku dan jurnal tentang steganografi dan keamanan data. Steganografi terdiri dari dua proses umum: embedding, yang digunakan untuk menyisipkan pesan dan ekstraksi yang digunakan untuk mengekstraksi pesan yang disisipkan.

3. Analisis Sistem

   Dalam tahap analisis sistem, peneliti memeriksa sistem yang akan diimplementasikan dengan mempertimbangkan penggunaan algoritma BPCS dan LSB. Hal ini mencakup evaluasi kebutuhan fungsional dan non-fungsional khusus yang terkait dengan penggunaan kedua algoritma ini. Selain itu, peneliti juga menetapkan batasan dan tujuan dari aplikasi steganografi berbasis web dengan mempertimbangkan integrasi yang tepat antara algoritma BPCS dan LSB untuk memastikan keamanan dan efektivitas sistem secara keseluruhan.

4. Perancangan Sistem dan Implementasi Sistem

   Peneliti merancang arsitektur aplikasi steganografi berbasis web, termasuk antarmuka pengguna (UI) untuk unggah gambar dan pesan teks. Selain itu, peneliti mengimplementasikan algoritma LSB dan BPCS sesuai dengan desain yang telah disusun.

5. Pengujian

Peneliti melakukan pengujian fungsionalitas dan keamanan aplikasi. Ini mencakup verifikasi bahwa algoritma LSB dan BPCS berfungsi dengan benar dalam konteks aplikasi web. Selain itu, kinerja aplikasi juga dievaluasi.

6. Hasil dan Kesimpulan

Pada tahap terakhir, peneliti menyimpulkan hasil dari implementasi aplikasi steganografi. Ini mencakup penilaian terhadap kinerja sistem, keefektifan algoritma yang digunakan, dan kesesuaian aplikasi dengan tujuan dan kebutuhan awal.

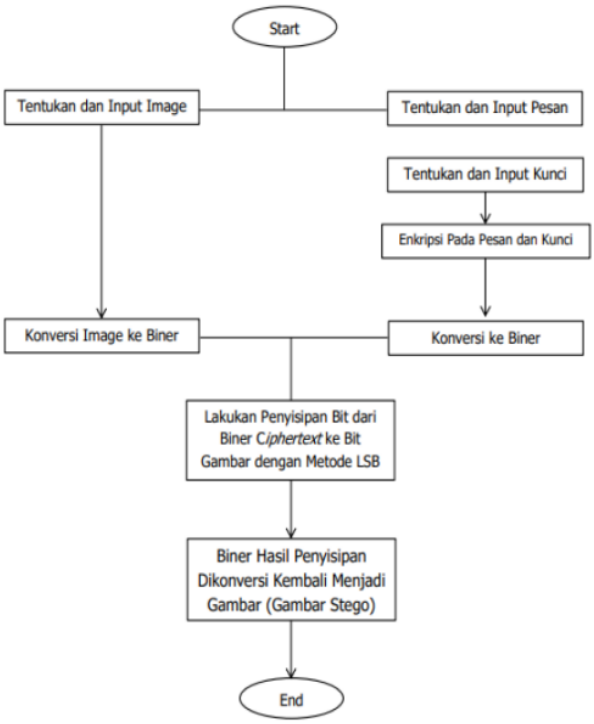
3. HASIL DAN PEMBAHASAN.

Penelitian ini menggunakan dokumen berupa file gambar sebagai citra *cover* dan teks pesan yang akan diamankan menggunakan teknik enkripsi untuk kemudian menggabungkan teks ke dalam file gambar dengan penggunaan algoritma LSB dan BPCS.

Metode steganografi(penyembunyian pesan) menggunkan algoritma LSB. Di bagian pertama, gambar tersembunyi dimasukkan ke dalam stegomedium sebagai media penyimpanan dengan menggunakan kunci tertentu, sehingga stegoimage, atau media dengan data tersembunyi, dihasilkan [11]. berikut langkah-langkahnya:

1.) Konversi gambar menjadi biner.
2.) Memilih dan menentukan pesan teks (plaintext).
3.) Memilih dan menentukan kunci (key).
4.) Melakukan enkripsi pada pesan dan kunci menggunakan metode vigenere cipher.
5.) Ciphertext selanjutnya dikonversi menjadi biner.
6.) Selanjutnya melakukan penyisipan biner ciphertext pada biner gambar dengan metode LSB, setiap bit dari ciphertext disisipkan pada bit terakhir dari gambar.
7.) Lalu biner dari hasil dari penyisipan tersebut dikonversi kembali menjadi gambar.

Proses encode atau embedding pada kedua teknik ini berfokus pada penyisipan bit-bit data teks ke dalam file gambar. Dalam algoritma LSB, bit-bit data teks disisipkan ke bit terakhir setiap piksel secara langsung. Sedangkan dalam algoritma BPCS, bit-bit data teks disisipkan ke dalam blok-blok citra yang memiliki kompleksitas bit-plane yang cukup tinggi.



Gambar 3. Proses Encode / Embedding

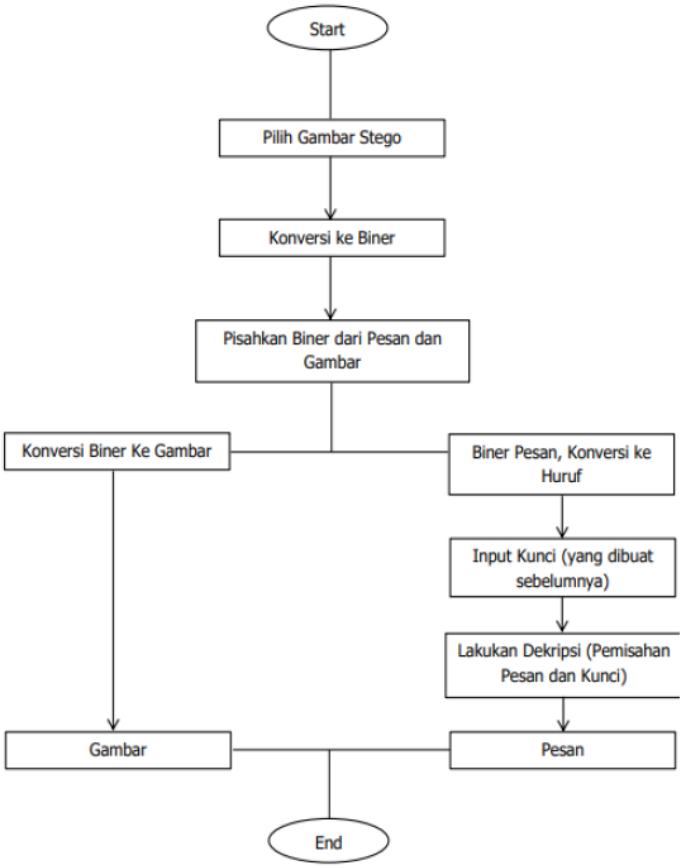
Pada akhir proses encode, file citra akan menjadi citra terenkripsi yang mengandung file teks yang disembunyikan. Proses enkripsi ini harus dilakukan dengan hati-hati perlu mempertimbangkan kecepatan, keamanan, dan integritas data. Selanjutnya ada proses decode/ekstraksi, yaitu langkah untuk mengambil kembali data yang telah disembunyikan atau disisipkan ke dalam file gambar.

Selanjutnya melakukan proses ekstraksi stegoimage dilakukan dengan menggunakan tombol yang sama. Ini menghasilkan gambar yang tersembunyi kembali. [12]

Berikut langkah-langkah proses ekstraksi:

1.) Pilih dan tentukan gambar (stego image).
2.) Lalu gambar stego dikonversi menjadi biner.
3.) Melakukan pemisahan biner ciphertext dan biner gambar.
4.) Melakukan dekripsi (pemisahan pesan dan kunci) dapat dilakukan dengan cara menginputkan kunci yang telah dibuat sebelumnya kemudian diproses dengan perintah dekripsi.
5.) Biner gambar diubah menjadi desimal kemudian dipetakan menjadi gambar.
6.) Biner plaintext dan kunci diubah menjadi bilangan desimal serta dikonversi ke bentuk huruf.

Karena tidak ada pencatatan pada kondisi awal dari stegomedium yang digunakan pada penyimpanan saat file disimpan, pada metode penyisipan pesan, tahap ekstraksi file dokumen dalam bentuk teks tidak akan mengembalikan stegomedium pada kondisi awal sama persis dengan stegomedium setelah tahap ekstraksi, bahkan mungkin saja mengalami kehilangan data.



Gambar 4. Proses Decode / Ekstraksi

Algoritma BPCS melakukan penyisipan pada bit-plane dengan sistem CGC (Canonical Gray Code). Oleh sebab itu, selama proses penyisipan berlangsung bit-plane dengan representasi PBCM diubah menjadi bit-plane dengan representasi CGC. Penyisipan pesan dilakukan pada segmen yang memiliki kompleksitas tinggi atau disebut sebagai wilayah suara, dan penyisipan dilakukan pada seluruh bitplane yang terdiri dari wilayah suara. Oleh karena itu, dalam teknik BPCS kapasitas data yang disisipkan dapat mencapai 50% dari ukuran cover objek [14].

Saat menyisipkan data, algoritma BPCS mengikuti langkah-langkah berikut:

1.) Objek penutup yang menggunakan sistem PBC perlu diubah menjadi sistem CGC, lalu gambar dipecah menjadi bit-plane dalam bentuk gambar biner, dengan bit yang digambarkan oleh bit-plane pada setiap piksel gambar.
2.) Dengan menggunakan nilai batas/batas (α0), setiap bit-plane cover-object dibagi menjadi wilayah yang informatif dan mirip suara. Nilai batas umum = 0,3.
3.) Menyusun pesan rahasia menjadi rangkaian blok yang terdiri dari beberapa byte.
4.) Jika blok (S) kurang kompleks daripada nilai batas, maka perlu dilakukan konjugasi terhadap S agar blok konjugasi (S*) menjadi lebih kompleks. Nilai batas harus lebih kompleks daripada blok konjugasi (S*).
5.) Jika blok S adalah blok pesan rahasia, masukkan setiap blok ke bit-plane yang menyerupai area suara. Alternatif, gantikan semua bit dengan area suara.

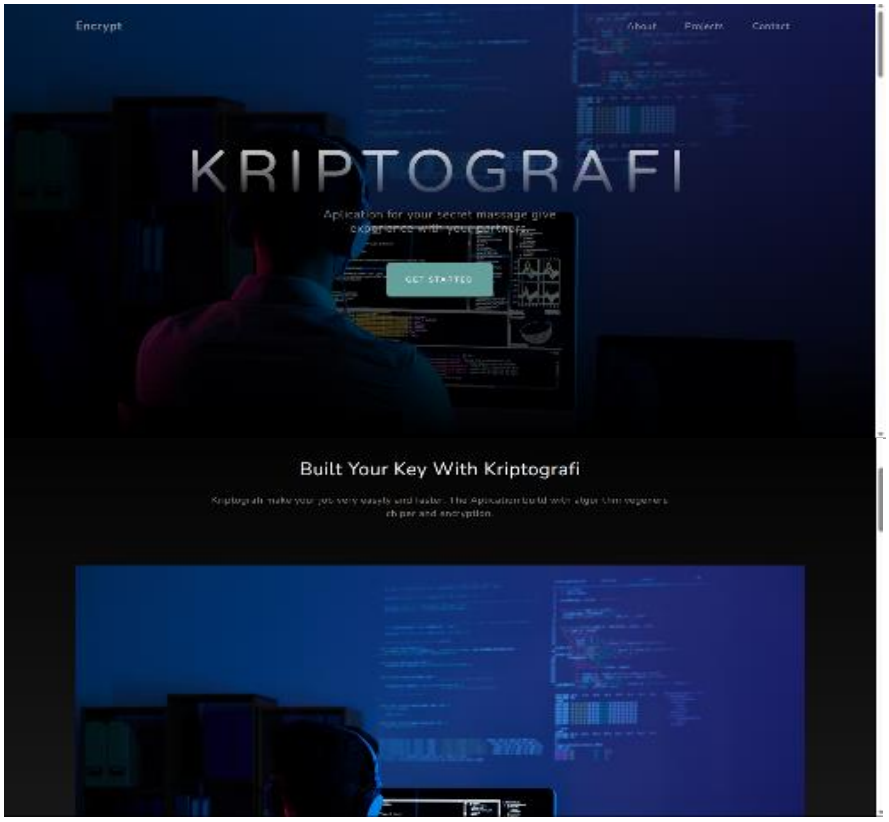
Proses decode menggunakan algoritma LSB dan BPCS. Dalam algoritma LSB, proses decode melibatkan pengambilan bit terakhir dari setiap piksel untuk mengembalikan urutan bit data yang tersembunyi. Hasil penelitian ini yaitu mencoba mengimplementasikan algotritma *Bit-Plane Complexity Segmentation* (BPCS) dan *Least Significant Bit* (LSB) untuk menenyembunyikan pesan dengan teknik *steganografi* kedalam sebuah gambar atau citra digital serta dapat digunakan untuk pengamanan sebuah data file berbasis website dengan menggunakan algoritma LSB dan BPCS.

3.1 Desain Antarmuka

3.1.1 Tampilan Halaman Utama

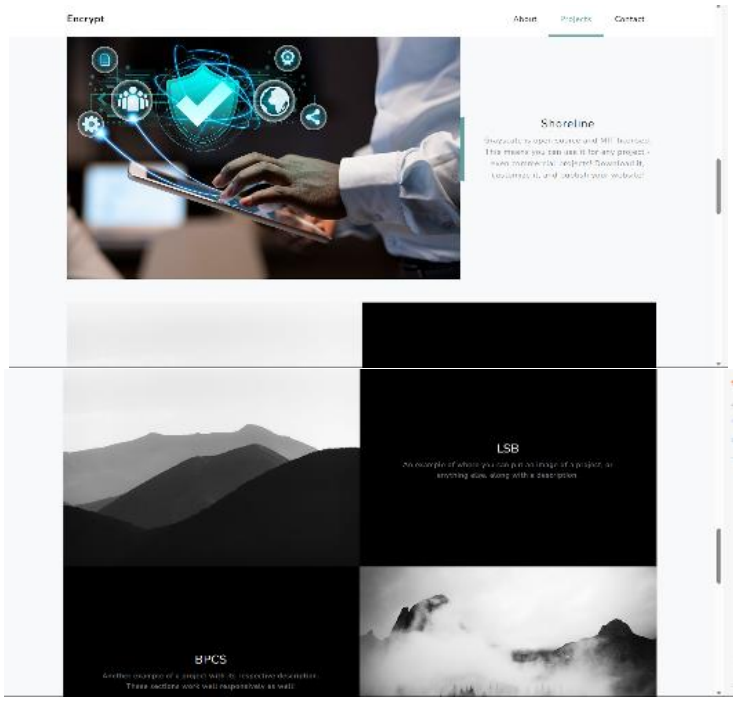
Halaman Utama dari aplikasi website dapat dilihat pada gambar berikut :

a. Halaman Utama ‘About’



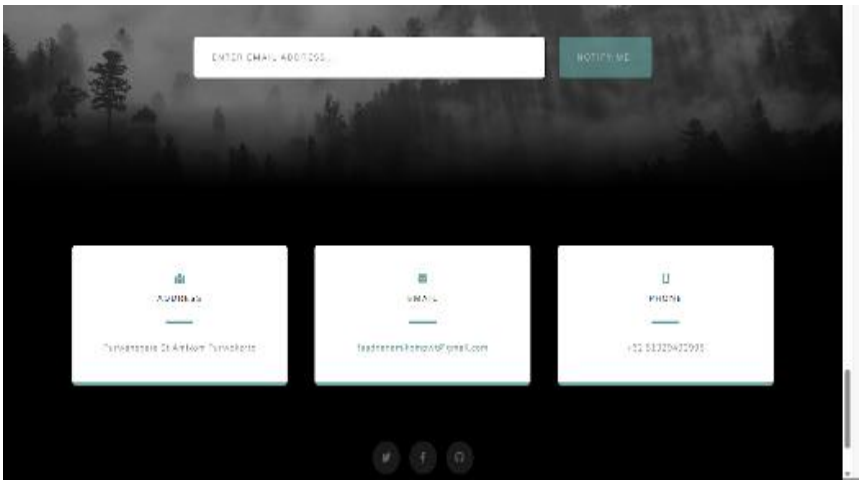
Gambar 5. Halaman About

b. Halaman Utama ‘Project’



Gambar 6. Halaman Project

c. Halaman Utama ‘Contact’



Gambar 7. Halaman Contact

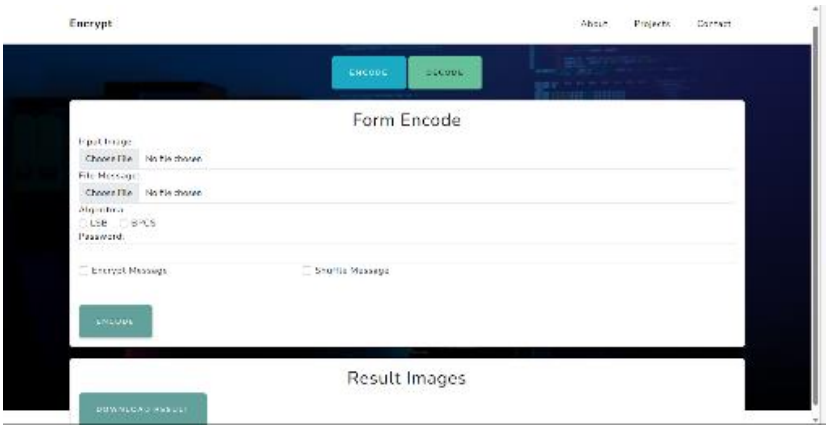
3.1.2 Tampilan Halaman Encode dan Decode

Halaman Encode digunakan untuk mengubah format gambar (*image*) biasa menjadi gambar (*image*) yang berisi pesan dan kunci(key) yang disisipkan. Proses yang pertama dilakukan yaitu Proses Embedding.

a. Dalam penelitian ini, pesan yang digunakan berupa teks, baik plaintext maupun pesan yang disisipkan, dan kunci berisi empat hingga enam karakter.
b. Pesan dan kunci tersebut kemudian digabungkan (dienkripsi) menggunakan algoritma vigenere cipher modifikasi. Hasil penggabungan pesan dan kunci disebut ciphertext.
c. *Ciphertext* dikonversi ke dalam biner, dan selanjutnya akan disisipkan pada citra *cover*.
d. Proses penukaran bit (steganografi dengan metode LSB), yaitu menyisipkan pesan pada citra cover yang dapat dilakukan apabila citra *cover* mampu menampung jumlah biner pada pesan yang disisipkan berdasarkan kriteria perhitungan jumlah pixel dibagi 8 bit. *Ciphertext* akan disisipkan

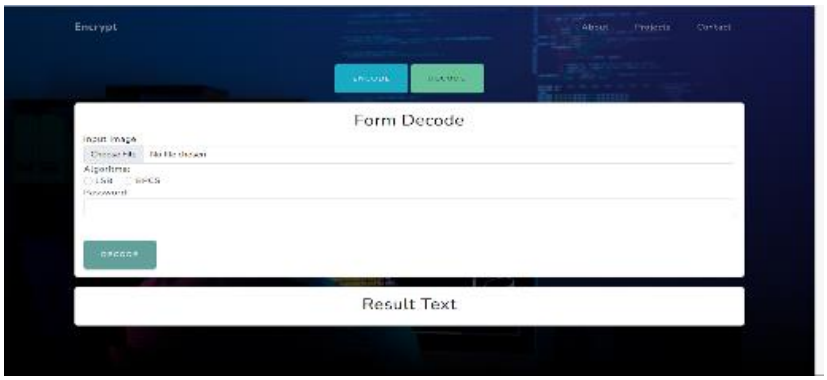
pada biner *pixel* citra *cover* berdasarkan metode LSB menggunakan perulangan pada baris dan kolom, yaitu masing-masing bit pada *ciphertext* disisipkan secara bergiliran pada *pixel* warna *red, green* dan *blue*. Biner terakhir *cover* diganti dengan biner *ciphertext* 0 atau 1.

a. *Ciphertext* akan disisipkan pada biner *pixel* citra *cover*, berdasarkan metode LSB yaitu masing-masing bit pada *ciphertext* disisipkan pada bit terakhir citra *cover*.
b. Konversi nilai biner cover baru ke bentuk angka.
c. Desimal selanjutnya dipetakan atau dikelompokkan menjadi stuego image, yaitu sebuah citra baru.



Gambar 8. Halaman Encode

Halaman Decode digunakan untuk mengubah gambar (*image*) yang berisi pesan/teks yang disisipkan menjadi gambar.



Gambar 9. Halaman Decode

4. PENUTUP

Hasil penelitian menghasilkan kesimpulan berikut :

a. Hasil metode steganografi LSB dan BPCS dan implementasi algoritma enkripsi *Vigenere Cipher* untuk menyisipkan dan menyembunyikan pesan pada citra digital dapat berjalan dengan baik. Gambar pesan yang ditambahkan (*stego image*) pada system tidak berbeda dengan gambar aslinya.
b. Pesan yang disematkan pada gambar dapat dikembalikan seperti semula. Kecuali jika pesan atau informasi yang disematkan dalam gambar diformat, dipotong, dan diubah ukurannya, informasi yang terkandung di dalamnya akan rusak.

DAFTAR PUSTAKA

[1] A. Rohmanu, "METODE ALGORITMA DES DAN METODE END OF FILE Ajar Rohmanu," *J. Inform.*, vol. 2, no. 1, pp. 1–11, 2017.
[2] E. dan S. Utami, "Implementasi Steganografi EoF dengan Gabungan Ekripsi Rijndael, Shift Chiper dan Fungsi Hash.," 2017.
[3] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.
[4] Stallings, Williams, *Cryptography and Network Security : Principles and Practices,* 2nd editio. Upper Saddle River : Prentice Hall Inc., 1995.
[5] Stallings, Williams, *Cryptography and Network Security : Principles and Practices,* 4th editio. Upper Saddle River : Prentice Hall Inc., 2006.
[6] M. F. Syawal, D. C. Fikriansyah, and N. Agani, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB," *J. TICOM*, vol. 4, no. 3, pp. 91–99, 2016.
[7] T. E. Putri, M. R. Al Fauzan, dan P. A. Sejati, "Perbaikan Algoritma Steganografi Teknik Least Significant Bits Untuk Aplikasi Keamanan Data," *J. Online Phys*, vol. 3, pp. 23–32, 2018, doi: 10.22437/jop.v3i1.5343.
[8] S. Supardi, A. A. Alkodri, dan B. Isnanto, "Teknik Steganografi Penyembunyian Pesan Text Rahasia Pada Citra Digital Dengan Metode Least Significant Bit," *Sisfotek Glob*, vol. 11, p. 70, 2021, doi: 10.38101/sisfotek.v11i1.351.
[9] F. Yanti and K. Budayawan, "Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb) dalam Pengamanan Informasi pada Citra Digital Penggunaan teknologi sebagai sarana dalam penyampaian informasi menimbulkan dampak terutama dari segi keamanan dan kerahasiaan informa," vol. 11, no. 1, 2023.
[10] P. Painem, "Implementasi Steganografi Metode Discrete Cosine Transform (Dct) Dan Kompresi Metode Huffman Untuk Mengamankan Dokumen Surat Keputusan Pada Yblc," *Telemat. Mkom*, vol. 8, pp. 121–126, 2016.
[11] N. F. Hasan, C. N. Dengen, dan D. Ariyus, "Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, pp. 20–29, 2020, doi: 10.31849/digitalzone.v11i1.3413.
[12] B. W. Rauf, "Kombinasi Steganografi Bit Matching dan Kriptografi Playfair Cipher, Hill Cipher dan Blowfish," *J. Teknol. Inf*, vol. 4, pp. 282–233, 2020, doi: 10.36294/jurti.v4i2.1346.
[13] I. S. Rangkuti and E. R. Siagian, "Implementasi Penyembunyian Pesan Pada Audio Dengan Metode Bit-Plane Complexity Segmentation (BPCS)," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 2, p. 285, 2020, doi: 10.30865/jurikom.v7i2.2088.
[14] Nugroho, Adi, "Rekayasa Perangkat Lunak Berbasis Objek Dengan Metode USDP," *Penerbit Andi*.
[15] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.