

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi di era saat ini, memudahkan masyarakat bertukar informasi dalam media digital seperti teks, audio, video, dan citra. Perkembangan Informasi dan Komunikasi menjadikan kegiatan penyampaian informasi maupun data menjadi lebih efisien. Perkembangan teknologi saat ini yang sangat signifikan memberikan dampak bagi masyarakat dalam bertukar informasi maupun melakukan komunikasi. Secara umum informasi dikategorikan menjadi dua, yaitu informasi yang bersifat rahasia dan informasi yang tidak bersifat rahasia. Informasi yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Informasi bersifat rahasia yaitu setiap informasi yang ada didalamnya sangat berharga bagi pihak yang membutuhkan karena informasi tersebut dapat dengan mudah digandakan. (Desimeri Laoli, 2020).

Saat ini telah banyak cara yang dapat dilakukan untuk penyembunyian pesan dalam pengiriman data dengan merubah data menjadi yang tidak dimengerti oleh pihak yang tidak memiliki akses untuk menerima pesan tersebut. Salah satu cara penyembunyian pesan dalam pengiriman yaitu dengan penyandian dan penyisipan menggunakan teknik kriptografi dan steganografi. Maka dari itu penulis menggabungkan metode kriptografi yaitu algoritma *Hill Cipher* dan metode steganografi yaitu *Least Significant Bit (LSB)*. (Jane Irma Sari, 2017). Tujuan untuk dapat menjaga dan memberikan keamanan yang berlapis tanpa mengurangi atau merusak pesan teks pada citra digital yang akan dikirim.

Seiring dengan majunya perkembangan teknologi, menyebabkan adanya cara-cara terbaru, yang digunakan dengan tidak bertanggung jawab oleh beberapa oknum yang menyalahgunakan fungsi keamanan akan sebuah sistem informasi. Ini sangat berisiko karena kemudahan dalam mendapatkan informasi saat ini memudahkan oknum dalam mendapatkan informasi pribadi milik seseorang

sehingga sangat merugikan dan meresahkan. .karena Informasi tersebar ke tangan okum lain dapat menimbulkan efek negatif untuk pemilik informasi dan disalah gunakan seperti merubah di bagian-bagian tertentu sehingga banyak terjadi perubahan. Pihak yang tidak bertanggung jawab menggunakan data tersebut untuk kepentingan tertentu yang tidak ada kaitannya dengan pemilik informasi tersebut. Kemudian Data-data yang penting jika tidak dilindungi secara optimal maka rentan akan pencurian atau kehilangan data. Pencurian atau kehilangan data tentunya akan merugikan seseorang.

Mengacu pada permasalahan yang dibahas maka diperlukan untuk merancang sebuah sistem keamanan yang dapat melindungi data yang dianggap penting dengan penyandian data, serta membuat kunci rahasia untuk dapat membuka data tersebut yang sulit untuk dideteksi oleh pihak yang tidak berhak. Gabungan dari metode kriptografi yakni algoritma *Hill Cipher* untuk enkripsi pesan dengan metode steganografi yaitu *Least Significant Bit (LSB)* dapat menambah keamanan dalam sebuah pesan (Desimeri Laoli, 2020).

Kriptografi merupakan salah satu ilmu maupun seni untuk menjaga kerahasiaan sebuah pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa alur kerja dari proses enkripsi. Algoritma yang dipakai pada penyusunan skripsi berikut ini yaitu *Hill Cipher* (Fresly Nandar Pabokory, 2015). Algoritma *Hill Cipher* menggunakan matriks berukuran $m \times m$ sebagai kunci untuk melakukan enkripsi dan dekripsi. Satu cara untuk mendapatkan kembali naskah asli tentunya dengan menerka kunci dekripsi, jadi proses menerka kunci dekripsi harus menjadi sesuatu yang sulit. memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan.

Sedangkan steganografi adalah seni untuk menyisipkan pesan rahasia kedalam suatu media, dimana pesan rahasia yang akan disembunyikan tidak diubah bentuknya, melainkan disisipkan pada sebuah citra digital, sehingga orang lain tidak mengetahui bahwa di dalam citra digital tersebut ada pesan rahasia.

Setelah dibubuhi pesan rahasia, setiap pixel dibangun kembali menjadi gambar yang utuh menyerupai dengan media gambar semula (Desimeri Laoli, 2020). Metode steganografi yang digunakan adalah metode *Least Significant Bit (LSB)*. Metode ini merupakan penyembunyian pesan yang dilakukan mengganti bit-bit data yang kurang berarti dalam segmen citra dengan bit-bit rahasia pada bit terakhir (Jane Irma Sari, 2017).

Beberapa penelitian terdahulu yang terkait dengan pengembangan implementasi penggabungan algoritma *hill cipher* dan metode *least significant bit (LSB)* yaitu penelitian dari (Ardiansyah dan Kurniasih, 2018) dengan judul *Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit* berdasarkan pengembangan sistem yang telah dibuat menghasilkan beberapa fitur diantaranya *add file, add text, cover image, set password, embed*. Kemudian penelitian dari (Agustinus Noertjahyana dkk, 2012) dengan judul *Aplikasi Metode Steganography Pada Citra Digital Dengan Menggunakan Metode LSB (Least Significant Bit)* dari pengembangan sistem yang telah dibuat menghasilkan beberapa fitur diantaranya *home, embed, help, dan exit*. Lalu penelitian dari (Hasugian, 2013) *Implementasi Algoritma Hill Cipher Dalam Penyandian Data* dari pengembangan sistem yang telah dibuat menghasilkan beberapa fitur diantaranya enkripsi dan dekripsi.

Berdasarkan beberapa penelitian terdahulu saya melakukan sebuah inovasi untuk membangun sebuah sistem Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma *Hill Cipher* Dan Metode *Least Significant Bit (LSB)* berbasis website dengan beberapa fitur unggulan yang ada di dalamnya. Ini merupakan sebuah sistem yang berfokus pada pengaman pesan *text* yang terlebih dahulu dilakukan proses enkripsi lalu pesan yang telah dilakukan proses enkripsi tersebut dimasukkan ke dalam sebuah citra *digital* berupa gambar JPG dengan menggunakan metode *least significant bit (LSB)*. Adapun fitur yang ada pada aplikasi ini adalah *button encode* untuk melakukan proses penyembunyian pesan pada digital, yang kedua *button decode* untuk melakukan proses ekstraksi pada pesan dari steganografi *image*.

Berdasarkan permasalahan yang sudah dijabarkan di atas, maka saya Ramma Eka Putera selaku peneliti terkait untuk melakukan penelitian yang berjudul “IMPLEMENTASI PENYEMBUNYIAN PESAN PADA CITRA *DIGITAL* DENGAN MENGGABUNGKAN ALGORITMA *HILL CIPHER* DAN METODE *LEAST SIGNIFICANT BIT (LSB)*”. Harapannya hasil dari penelitian ini dapat membantu pengguna aplikasi untuk menyembunyikan informasi yang bersifat rahasia agar tidak mudah ditemukan atau diakses oleh orang yang tidak bertanggung jawab sehingga keamanan data atau informasi pengirim lebih terjaga.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka didapatkan rumusan masalah sebagai berikut :

- a. Bagaimana cara implementasi penyembunyian pesan pada citra *digital* dengan menggabungkan algoritma *hill cipher* dan metode *least significant bit* yang berbasis web?
- b. Bagaimana cara mengukur perbedaan citra *digital* sebelum dan sesudah steganografi menggunakan *peak signal-to-noise ratio (PSNR)* dan *Mean Square Error (MSE)*?
- c. Bagaimana cara mengevaluasi fungsionalitas sistem menggunakan metode *black box testing*?
- d. Bagaimana proses steganografi pada gambar berformat PNG sebagai format yang digunakan untuk stiker WhatsApp?
- e. Bagaimana perbedaan gambar sebelum dan sesudah dikirim melalui whatsapp?

1.3 Tujuan

Tujuan dari dilakukannya penelitian ini adalah sebagai berikut:

- a. Untuk mengembangkan aplikasi dengan mengimplementasikan penyembunyian pesan pada citra *digital* dengan menggabungkan algoritma *hill cipher* dan metode *least significant bit* yang berbasis web

- b. Untuk mengetahui apakah aplikasi penyembunyian pesan pada citra *digital* dengan menggabungkan algoritma *hill cipher* dan metode *least significant bit* fungsionalitas telah berjalan dengan baik sesuai yang diharapkan pengguna dengan melakukan *Black box testing*,
- c. Untuk mengetahui apakah aplikasi penyembunyian pesan pada citra *digital* dengan menggabungkan algoritma *hill cipher* dan metode *least significant bit* memiliki perbedaan yang signifikan pada gambar yang digunakan pada *cover image* .

1.4 Manfaat

Manfaat yang diharapkan setelah melakukan penelitian ini adalah sebagai berikut:

- a. Manfaat bagi pengguna, dapat membantu pengguna dalam menyisipkan pesan ke dalam citra *digital* sehingga isi pesan tersebut yang bersifat rahasia tidak mudah untuk disalahgunakan oleh oknum yang tidak bertanggung jawab.
- b. Manfaat bagi penulis, dapat menambah pengetahuan tentang bagaimana cara mengembangkan aplikasi *website* serta mengevaluasinya menggunakan *Black box testing*, *Peak signal-to-noise ratio (PSNR)*, dan *measure of the quality of an estimator (MSE)*.
- c. Bisa memberikan informasi yang tepat dan akurat kepada penerima pesan yang dikirim oleh pengirim pesan dengan mengurangi risiko penyalahgunaan pesan dari pihak yang tidak bertanggung jawab.

1.5 Batasan Masalah

Agar pembahasan masalah tidak terlalu melebar dan lebih terfokus, maka permasalahan dibatasi oleh beberapa hal:

- a. Penelitian ini ditujukan untuk pengguna aplikasi yang sudah melakukan proses registrasi.
- b. Aplikasi penyembunyian pesan pada citra *digital* dengan menggabungkan algoritma *hill cipher* dan metode *least significant* dibuat berbasis web.

- c. Model pengembangan aplikasi menggunakan algoritma *hill cipher* dan metode *least significant bit*.
- d. Alat evaluasi aplikasi yang digunakan adalah *Black box testing* untuk mengevaluasi fungsionalitas sistem, *Peak signal-to-noise ratio (PSNR)* dan *measure of the quality of an estimator (MSE)* untuk mengukur gambar citra sesudah dan sebelum melalui proses steganografi.
- e. Dalam penelitian ini hanya menggunakan media penyembunyian berupa citra digital gambar dengan format PNG.
- f. Aplikasi ini dibuat hanya untuk menyembunyikan data rahasia yang berupa data teks.