

BAB I

PENDAHULUAN

1.1. Latar Belakang

Data digital merupakan representasi informasi dalam bentuk angka atau simbol-simbol yang dapat diolah oleh komputer atau perangkat elektronik lainnya. Macam-macam data digital yang umum ditemui meliputi data teks, gambar, audio, video, spreadsheet, presentasi, dan basis data. Data teks terdiri dari karakter, huruf, angka, dan simbol lainnya, seperti dokumen teks atau pesan teks. Data gambar adalah representasi digital dari gambar atau grafik, seperti foto atau ilustrasi. Data audio merupakan representasi digital dari suara, seperti file musik atau rekaman suara. Data video adalah representasi digital dari gambar bergerak dan suara, seperti file video atau film. Video merupakan salah satu jenis media audio visual yaitu media yang mengandalkan indera pendengaran dan indera penglihatan, setiap jenis video memiliki ekstensi file yang umum digunakan seperti .mp4, .avi, .mov, dan .wmv, tergantung pada format dan kebutuhan penggunaannya. Data spreadsheet terstruktur dalam bentuk tabel atau lembar kerja, digunakan untuk menyimpan data yang terorganisir. Data presentasi digunakan untuk membuat dan menyajikan materi presentasi. Sedangkan data basis data terorganisir dalam struktur yang terdefinisi dan digunakan untuk menyimpan dan mengelola informasi dalam suatu sistem. Macam-macam data digital ini memiliki format dan jenis yang beragam, tergantung pada sifat dan penggunaannya.

Data atau informasi memiliki dua jenis, yaitu yang bersifat publik yang dapat diakses oleh banyak orang, dan yang bersifat pribadi atau rahasia yang hanya dapat diakses oleh orang-orang tertentu (Yusup et al., 2020). Ketika mengirimkan informasi rahasia melalui internet, keamanan harus diprioritaskan agar informasi tersebut tidak jatuh ke tangan yang salah. Salah satu cara untuk menyembunyikan informasi rahasia adalah dengan menyelipkannya ke dalam berkas citra digital menggunakan teknik steganografi. Dengan cara ini, informasi tersembunyi dalam

citra digital tidak akan menarik perhatian pihak yang mencoba mencuri informasi saat pengiriman melalui internet (Muadzani et al., 2016).

Keamanan pengiriman informasi melalui internet merupakan hal vital yang harus diperhatikan dikarenakan banyak terjadi kebocoran data/informasi dalam berbagai sektor, perusahaan telekomunikasi asal Amerika Serikat Verizon dalam laporan risetnya menyebutkan sepanjang tahun 2021 ada 5.212 kasus kebocoran data (Annur, 2022) Badan Siber dan Sandi Negara (BSSN) juga melaporkan ada 311 kasus kebocoran data yang terjadi di Indonesia pada tahun 2022. (Mustajab, 2023).

Penelitian ini bertujuan untuk mengatasi masalah keamanan pengiriman informasi melalui internet dengan memanfaatkan algoritma Caesar Cipher dan Metode Least Significant Bit (LSB). Caesar Cipher adalah salah satu teknik enkripsi klasik yang digunakan untuk mengubah teks menjadi teks sandi dengan menggeser setiap huruf dalam teks asli sejumlah langkah tertentu. Algoritma tersebut digunakan untuk menambahkan tingkat keamanan dari penenkripsian yang akan dilakukan. (Yusup et al., 2020). Selain itu, metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai coverttext. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling depan (most significant bit atau MSB) dan bit yang paling akhir (least significant bit atau LSB). (Novianto & Setiawan, 2019). Metode LSB juga tidak mengganggu visual secara signifikan karena hanya menggunakan bit-bit yang kurang berarti didalam suatu citra.

Pada Penelitian sebelumnya (Yusup et al., 2020) menyimpulkan bahwa dari total 5 file dokumen semuanya dapat dienkripsi dengan baik, namun pada saat penyematan hanya 2 dari 5 file dokumen yang dapat disematkan. Dalam penelitian yang dilakukan (Novianto & Setiawan, 2019) menyimpulkan penyisipan informasi berjalan dengan baik dimana informasi yang disisipkan dapat diambil kembali secara penuh dan citra berwarna tidak menunjukkan perubahan yang signifikan.

Tantangan utama dalam penelitian ini adalah menggabungkan kedua metode ini sehingga teks dapat diamankan dengan baik tanpa mengorbankan kualitas

visualnya. Selain itu, perlu mempertimbangkan juga kecepatan pengolahan video agar pengguna dapat mengunggah dan mengunduh video dengan mudah.

Berdasarkan pemahaman terhadap konteks sebelumnya serta hasil penelitian yang telah dilakukan, peneliti berencana untuk menjalankan sebuah penelitian dengan judul " Penerapan Algoritma Caesar Cipher dan Least Significant Bit Untuk Mengamankan Teks di dalam Video". Diharapkan bahwa penelitian ini akan memberikan kontribusi yang berharga dan dapat menjadi sumber referensi bagi penelitian-penelitian mendatang.

1.2. Identifikasi Masalah

Berdasarkan uraian latar belakang yang telah disampaikan sebelumnya, masalah-masalah yang dapat diidentifikasi dalam penelitian ini termasuk:

1. Kebocoran data/informasi yang marak terjadi pada saat proses pengiriman.
2. Potensi kerusakan visual pada video akibat proses enkripsi dan penyisipan data/informasi.

1.3. Rumusan Masalah

Setelah melalui proses identifikasi masalah, masalah yang akan dibahas dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana mengamankan proses pengiriman data/informasi dengan memanfaatkan Algoritma Caesar Cipher dan Metode Least Significant Bit?
2. Bagaimana mengamankan data/informasi kedalam video dengan mempertimbangkan kualitas video dan keamanan data?

1.4. Tujuan Penelitian

Dengan mempertimbangkan masalah yang telah diuraikan sebelumnya, tujuan penelitian yang akan dicapai adalah sebagai berikut:

1. Membuat Website yang dapat mengamankan informasi berupa teks didalam sebuah video menggunakan Algoritma Caesar Cipher dan Metode Least Significant Bit.
2. Mengamankan pengiriman informasi berupa teks dengan tetap mempertimbangkan kualitas visual dari video.

1.5. Batasan Masalah

Dari identifikasi masalah yang telah dilakukan, batasan masalah dan cakupan permasalahan yang luas telah ditetapkan, oleh karena itu peneliti dibatasi sebagai berikut:

1. Pengamatan akan difokuskan pada implementasi algoritma dan metode tersebut untuk mengamankan teks kedalam vidio yang memiliki format AVI.
2. Penelitian ini akan berfokus pada penerapan algoritma Caesar Cipher dan metode Least Significant Bit (LSB) untuk mengamankan teks kedalam sebuah vidio.

1.6. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan solusi teknis untuk mengamankan pengiriman informasi berupa teks didalam vidio dengan mempertimbangkan kualitas visual, sehingga pengguna tetap dapat menikmati vidio yang baik.
2. Menyediakan dasar untuk penelitian lebih lanjut dalam pengembangan metode pengamanan teks di dalam vidio.

