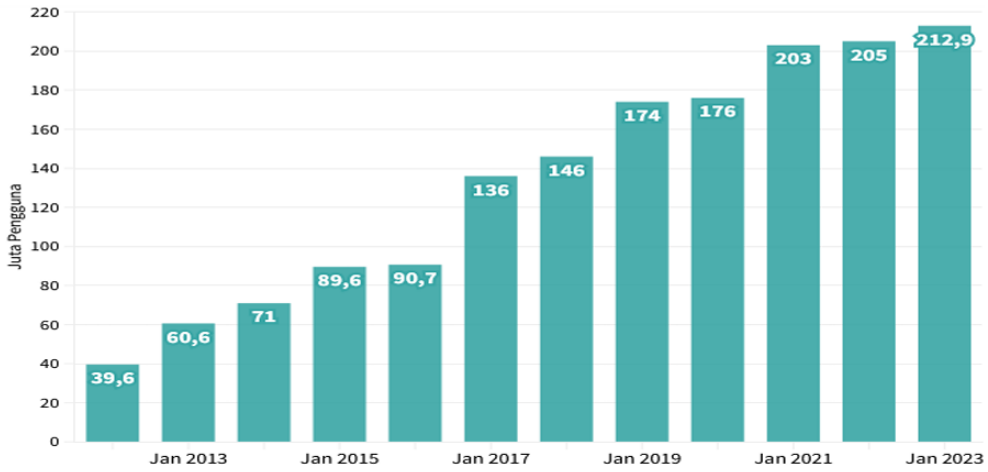
BAB I
PENDAHULUAN

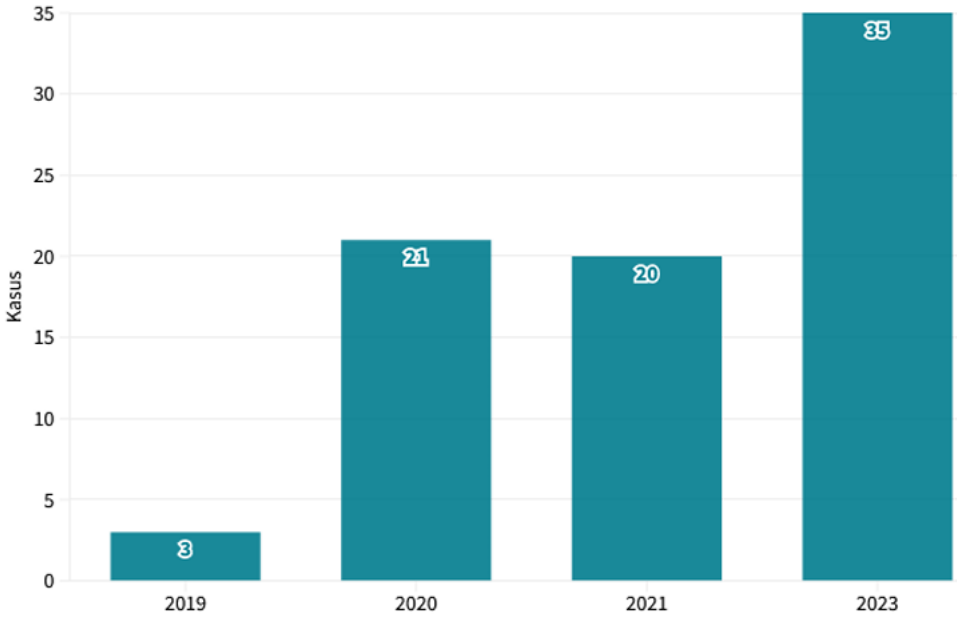
1.1 Latar Belakang Penelitian

Perkembangan teknologi saat ini berlangsung sangat pesat, memungkinkan akses data dan informasi yang cepat bagi manusia. Hal ini didukung oleh peningkatan signifikan jumlah pengguna internet di Indonesia setiap tahunnya, seperti yang terlihat pada data dalam gambar 1.1. Jumlah pengguna internet di Indonesia mengalami peningkatan sejak 2013 hingga 2023, bersamaan dengan semakin tingginya kebutuhan masyarakat terhadap teknologi informasi dalam kehidupan sehari-hari.



Gambar 1. 1 Jumlah Pengguna Internet di Indonesia (Rizaty, 2023)

Peningkatan ini mencerminkan pesatnya perkembangan teknologi informasi serta kebutuhan yang meningkat akan konektivitas digital. Namun, kemajuan ini juga meningkatkan risiko terhadap keamanan pesan, terutama yang bersifat rahasia, yang rentan diketahui oleh pihak tidak bertanggung jawab. Informasi sensitif seperti data pribadi, data pelanggan, rahasia bisnis, dan data keuangan adalah target yang sangat menguntungkan bagi pelaku kejahatan digital (Kurnianingrum, 2023). Grafik dalam gambar 1.2 menunjukkan kasus kebocoran data di Indonesia pada periode Januari 2019 hingga Januari 2023.



Gambar 1. 2 Kasus Kebocoran Data di Indonesia (Widi, 2023)

Berdasarkan gambar 1.2 tersebut penyebab kasus kebocoran data disebabkan oleh beberapa hal diantaranya minimnya sistem keamanan dan serangan yang disengaja dari pihak lain. Banyak perusahaan dan organisasi besar telah mengalami insiden kebocoran data yang merugikan baik secara finansial maupun reputasi. Kebocoran data juga dapat menimbulkan dampak negatif bagi individu yang mengalaminya, seperti pencurian identitas, penipuan keuangan, atau bahkan ancaman keamanan fisik (Yudistira & Ramadhan, 2023). Oleh karena itu menjaga keamanan data, informasi, dan platform adalah tanggung jawab dan kesadaran bersama (Pradeka dkk., 2023).

Salah satu langkah penting untuk mencegah kebocoran data adalah dengan menjaga keamanan pesan dengan menggunakan teknik kriptografi dan steganografi. Steganografi dan kriptografi adalah dua metode yang dapat digunakan untuk berbagi informasi secara tersembunyi (Susanto & Mulyono, 2020). Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Metode kriptografi dapat digunakan untuk merubah teks menjadi bentuk yang tidak bermakna dengan melakukan perhitungan matematika (Rambe dkk., 2018).

Salah satu metode kriptografi adalah *Caesar Cipher,* yaitu teknik kriptografi sederhana yang digunakan untuk mengenkripsi dan mendekripsi teks (Ardiansyah dkk., 2023). Algoritma ini mengombinasikan substitusi dan transposisi data dengan

rumus matematika sederhana hingga kompleks. *Caesar Cipher* yang diterapkan dengan tepat dapat meminimalkan kebocoran dan meningkatkan keamanan data secara keseluruhan (Febrianingsih & Hafiz, 2019).

Namun perubahan bentuk tersebut menimbulkan kecurigaan oleh pihak lain. Metode steganografi hadir untuk menyembunyikan teks ke dalam sebuah media agar teks tersebut tidak diketahui oleh orang lain (Rambe dkk., 2018). Salah satu metode steganografi yang efektif adalah penggunaan teknik *Least Significant Bit* (LSB), yang memungkinkan penyisipan pesan tanpa memengaruhi kualitas visual video. LSB menggantikan bit paling tidak signifikan pada piksel media dengan bit pesan. LSB dapat diaplikasikan pada berbagai jenis media, antara lain gambar, audio, dan video (Minarni & Redha, 2020). Pada penelitian yang dilakukan oleh Mellynda & Nasution (2024) diperoleh hasil bahwa penerapan teknik steganografi menggunakan algoritma LSB pada aplikasi berjalan dengan baik. Aplikasi yang dihasilkan mampu melakukan penyisipan pesan teks ke dalam video. Pesan teks yang digunakan berasal dari file berformat *.txt*, sedangkan video yang digunakan sebagai media penyisipan memiliki format *.mp4*. Aplikasi ini dapat diakses melalui web browser, dan dikembangkan menggunakan *Visual Studio Code* dengan bahasa pemrograman HTML dan *Javascript*.

Pada penelitian terdahulu yang dilakukan oleh Watimena & Mufti (2020) dilakukan penelitian terkait pengamanan data dengan menggunakan metode *steganografi* dengan teknik *Least Significant Bit (LSB)* untuk menyisipkan pesan pada citra *bitmap*. Pesan tersebut dienkripsi menggunakan algoritma *Vigenere* untuk menjaga kerahasiaanya. Penelitian tersebut menunjukan bahwa ukuran citra yang lebih besar dapat meningkatkan kapasitas penyimpanan data. Namun dari penelitian tersebut masih memiliki kekurangan dalam keamanan algoritma kriptografi *vigenere* klasik seperti penelitian terdahulu yang dilakukan oleh Hidayatullah dkk. (2024), dalam penelitiannya tesebut menyimpulkan bahwa *vigenere cipher* memiliki kerentanan terhadap analisis kasar seperti *brute force attack* jika panjang kunci tidak terlalu panjang dan pola berulang. Jika panjang kunci relatif pendek dan berulang, pola pergeseran huruf dapat ditemukan dengan metode kriptanalisis yang lebih canggih. Adapun menurut Aiman & Brisbane (2021) dalam hasil penelitiannya menjelaskan kriptoanalisis *vigenere cipher*

memberikan pengetahuan untuk menentukan panjang kunci menggunakan *Index of Coincidence* (IC), menetukan karakter kunci membagi teks sandi menjadi beberapa kelompok dan membandingkan frekuensi huruf dengan frekuensi bahasa inggris normal, menggunakan program *cryptool.* Berdasarkan kekurangan dari penelitian tersebut, pada penelitian ini mempertimbangkan dengan menggunakan algoritma *Caesar Cipher* termodifikasi yang sederhana tetapi cukup *powerfull* dalam melakukkan enkrirpsi karena merupakan penghulu dari semua algoritma enkripsi yang ada di dunia sampai saat ini (Irwansyah dkk., 2020).

Pemilihan bahasa pemrograman Go (*Golang*) yang dikembangkan oleh *Google*, semakin populer sebagai bahasa pemrograman untuk pengembangan web dan aplikasi lain karena kesederhanaan, efisiensi, dan dukungan kuat untuk konkurensi (Uzayr, 2022). Analisis kinerja telah menunjukkan bahwa *Golang* mengungguli *JavaScript* dan PHP dalam hal pemanfaatan CPU, waktu respons, dan skalabilitas, menjadikannya pilihan yang sangat baik untuk proyek pengembangan web (Nabiil dkk., 2023).

Berdasarkan pemaparan sebelumnya, penelitian ini bertujuan untuk mengembangkan sistem steganografi video yang mengintegrasikan LSB, *Caesar Cipher* termodifikasi, dan transposisi yang diimplementasikan dalam bahasa pemograman *Golang* sehingga dapat dilakukan proses penyisipan pesan tekstual ke dalam video tanpa mengorbankan kualitas visual secara signifikan dengan tujuan meningkatkan keamanan tanpa menambah kompleksitas yang berlebihan. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam bidang keamanan informasi, khususnya dalam konteks steganografi video dan kriptografi. Pengembangan sistem ini tidak hanya relevan dari segi akademis, tetapi juga memiliki potensi aplikasi praktis yang luas. Dalam era di mana privasi dan keamanan informasi menjadi semakin penting, sistem steganografi video yang aman dan efisien dapat memiliki implikasi signifikan dalam berbagai bidang.

1.2 Rumusan Masalah Penelitian

Berdasarkan penjelasan latar belakang sebelumnya, peneliti menyusun beberapa rumusan masalah berikut:

1. Bagaimana merancang dan mengimplementasikan aplikasi steganografi video berbasis web yang mengintegrasikan LSB, *Caesar Cipher* super enkripsi (termodifikasi, dan transposisi) dalam bahasa pemrograman *Golang*.
2. Bagaimana kinerja sistem steganografi video yang mengintegrasikan LSB, *Caesar Cipher* super enkripsi (termodifikasi, dan transposisi) dalam bahasa pemrograman *Golang.*

1.3 Tujuan penelitian

Berdasarkan rumusan masalah yang telah dirumuskan sebelumnya, maka penelitian ini bertujuan untuk memenuhi beberapa tujuan sebagai berikut:

1. Mengembangkan sistem steganografi video yang mengintegrasikan metode LSB (Least Significant Bit), *Caesar Cipher super* enkripsi (termodifikasi, dan teknik transposisi) untuk menyisipkan pesan tekstual, serta merancang aplikasi berbasis web menggunakan bahasa pemrograman Golang.
2. Mengetahui kinerja sistem steganografi penyisipan pesan tekstual ke dalam video menggunakan metode LSB untuk memaksimalkan kapasitas penyisipan serta mempertahankan kualitas visual video.

1.4 Batasan penelitian

1. Tipe Video Input: Aplikasi dirancang untuk menerima format video dari pengguna dalam format AVI.
2. Format Video Output: Setiap video yang diproses oleh aplikasi akan dikonversi menjadi format AVI (*Audio Video Interleave*). Pemilihan format AVI sebagai output standar bertujuan untuk menjaga konsistensi dan kompatibilitas lintas platform, serta memudahkan proses penyisipan dan ekstraksi pesan.
3. Teknik Enkripsi dan Penyisipan:
    a) Enkripsi: Aplikasi mengimplementasikan *Caesar Cipher* yang telah dimodifikasi, dikombinasikan dengan teknik transposisi cipher.

Modifikasi ini bertujuan untuk meningkatkan keamanan pesan dibandingkan dengan *Caesar Cipher* tradisional.

b) Penyisipan: Metode Least Significant Bit (LSB) digunakan untuk menyisipkan pesan terenkripsi ke dalam frame-frame video. Teknik ini dipilih karena kemampuannya menyembunyikan informasi dengan dampak visual minimal.

4. Bahasa pemograman Go (*Golang*): Dipilih sebagai bahasa pemrograman utama untuk pengembangan aplikasi. Go menawarkan performa tinggi dan kemampuan konkurensi yang baik, ideal untuk pemrosesan video dan integrasi komponen yang berbeda.
5. Aplikasi Web:
    a) Aplikasi berbasis web akan dikembangkan untuk memungkinkan pengguna mengunggah video, memasukkan pesan yang akan dienkripsi, dan mengunduh video yang telah dihasilkan.
    b) Aplikasi web harus menyediakan antarmuka pengguna yang intuitif dan menampilkan hasil validasi secara langsung.

1.5 Manfaat penelitian

1.5.1 Manfaat Teoritis

Manfaat teoritis dari penelitian ini adalah sebagai berikut:

1. Pengembangan konsep steganografi video: Penelitian ini berkontribusi pada pengembangan teori steganografi, khususnya dalam konteks media video, memperluas pemahaman tentang teknik penyembunyian informasi dalam konten multimedia.
2. Integrasi metode kriptografi klasik: Studi ini mendemonstrasikan penerapan dan modifikasi *Caesar Cipher* dalam konteks modern, memberikan wawasan baru tentang adaptasi algoritma kriptografi klasik untuk keamanan digital kontemporer.
3. Eksplorasi teknik LSB dalam video: Penelitian ini memperdalam pemahaman tentang aplikasi metode *Least Significant Bit* (LSB) dalam konteks steganografi video, potensial mengungkapkan batasan dan peluang baru dalam teknik ini.

4. Pengembangan model keamanan berlapis: Studi ini berkontribusi pada teori keamanan informasi dengan menggabungkan steganografi dan kriptografi, memberikan model untuk sistem keamanan multi-layer dalam konteks digital.
5. Inovasi dalam transposisi data: Penelitian ini mengeksplorasi teknik transposisi baru, potensial memperkaya teori pengacakan data dalam konteks keamanan informasi.
6. Kontribusi pada pengembangan aplikasi *Golang*: Studi ini menambah pengetahuan tentang implementasi algoritma keamanan kompleks menggunakan *Golang*, memperkaya literatur tentang penggunaan bahasa pemrograman modern dalam pengembangan sistem keamanan.

1.5.2 Manfaat Praktis

Manfaat praktis dari penelitian ini adalah sebagai berikut:

1. Manfaat bagi peneliti adalah memperoleh pengalaman dalam penerapan algoritma *Caesar Cipher* termodifikasi, transposisi, dan *steganografi* LSB untuk penyisipan pesan tekstual dalam video, serta mendapatkan keterampilan dalam merancang dan mengimplementasikan sistem *steganografi* video ini menggunakan bahasa pemrograman *Golang.*
2. Manfaat bagi pengguna dan masyarakat umum, penelitian ini memberikan solusi nyata untuk meningkatkan kerahasiaan pesan pribadi maupun data sensitif melalui teknik penyisipan dan ekstraksi pesan pada video yang sulit terdeteksi, sehingga privasi dan informasi rahasia dapat terlindungi dengan baik dari pihak yang tidak berwenang. Sistem *steganografi* video ini menggabungkan metode LSB, *Caesar Cipher* termodifikasi, dan transposisi untuk meningkatkan keamanan pesan yang disisipkan.

Dengan manfaat praktis yang dihasilkan, penelitian ini berkontribusi pada peningkatan keamanan informasi dengan mengembangkan sistem steganografi video berbasis *Golang*. Menggunakan kombinasi LSB, *Caesar Cipher* termodifikasi, dan transposisi, sistem ini memungkinkan penyisipan pesan tekstual yang aman dalam video, meningkatkan perlindungan data sensitif dan privasi pengguna.

1.6 Struktur Organisasi Skripsi

Struktur organisasi skripsi ini berperan sebagai pedoman penulis dalam menyusun penulisan skripsi secara lebih terarah, maka penulis menyusun struktus organisasi skripsi berdasarkan pada Peraturan Rektor UPI (Universitas Pendidikan Indonesia) Nomor. 7867/UN40/HK/2021 tentang Pedoman penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun Akademik 2021. Sistem penulisan karya ilmiah ini terdiri dari lima bagian yaitu, pendahuluan, kajian pustaka, metode penelitian, hasil dan pembahasan, kemudian simpulan, implikasi dan rekomendasi. Adapun rincian sebagai berikut.

Pendahuluan, pada bab ini berisi tentan latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian dan struktur organisasi skripsi.

Kajian Pustaka, pada bab ini berisi tentan kajian literatur dari penelitian sebelumnya yang terkait dengan aplikasi atau Web, *RGB,* Steganografi*,* Kriptografi Super Enkripsi*,* Video digital*,* Format AVI*,* OpenCV, FFmpeg*, Golang,* MSE dan PSNR, termasuk Studi Terkait yang relavan.

Metode penelitian, pada bab ini akan menjelaskan proses penelitian dari tahap perancangan, implementasi, hingga pengujian efektivitas Pengembangan Sistem Steganografi Video dan *Caesar Cipher* Termodifikasi Berbasis *Golang.* Pemilihan metode *Design and Development* (D&D) akan dijelaskan untuk memberikan pemahaman yang jelas tentang pendekatan yang digunakan, mencakup pengumpulan data yang relevan dan akurat, proses pengembangan sistem sesuai kebutuhan pengguna, serta strategi dan teknik pengujian untuk memastikan kuaitas dan fungsionalitas sistem sebelum diimplementasikan, sehingga memebrikan gambaran umum tentang metodologi yang diadopsi dalam penelitian ini.

Temuan dan Pembahasan, pada bab ini akan menjadi wadah untuk menyampaikan hasil temuan dari rancangan dan kinerja sistem yang dikembangkan. Evaluasi pengujian kinerja sistem akan menjadi fokus utama pembahasan. Pada bagian ini, penulis akan menyoroti aspek-aspek kritis yang mucul selama penelitian dan memberikan pemahaman yang mendalam terhadap perlindungan data yang disematkan kedalam video terdapat kesentifan pada kunci

algoritma *Caesar Cipher* yang dimodifikasi. Penekanan akan diberikan pada pemahaman yang komprehensif terkait pengujian kinerja sistem, sehingga pembaca dapat memperoleh wawasan yang jelas tentang pendekatan dan hasil yang dicapau dalam evaluasi sistem.

Simpulan Implikasi dan Rekomendasi, pada bab terakhir yaitu simpulan implikasi dan rekomendasi, yang akan merangkum temuan penelitian terkait pengembangan sistem *steganografi* video untuk penyisipan pesan tekstual menggunakan metode LSB, *Caesar Cipher* termodifikasi, dan transposisi berbasia *Golang*. Simpulan dari hasil penelitian akan disajika, diikuti dengan pembahasan implikasi dari penerapan teknik-tekni enskripsi dan *steganigrafi* tersebut dalam sistem pengamanan informasi. Terakhir, penulis akan menyampaikan rekomendasi yang dapat memberikan arah bagi peneliti masa depan untuk mengembangkan lebih lanjut konsep dan aplikasi *steganografi* video serta kemananan informasi digital.