BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Komunikasi antara dua pihak, terutama komunikasi jarak jauh telah menjadi kebutuhan yang tidak dapat dipisahkan pada kehidupan modern. Namun, komunikasi seperti ini seringkali memiliki risiko yang tinggi terhadap penyadapan oleh pihak ketiga. Hal ini menimbulkan kebutuhan akan metode untuk mengamankan isi pesan agar tidak dapat diakses oleh pihak ketiga atau pihak yang tidak berwenang (Klemm R. & Chen B., 2024). Salah satu metode yang digunakan untuk menjawab permasalahan tersebut adalah steganografi. Steganografi memiliki fungsi atau kemampuan untuk menyembunyikan keberadaan sebuah pesan (Zhou, X dkk., 2022).

Steganografi berbeda dengan enkripsi. Jika enkripsi mengubah pesan menjadi bentuk yang tidak dapat dimengerti yang biasa disebut dengan *ciphertext*, maka steganografi bekerja dengan menyimpan pesan rahasia ke dalam sebuah media yang biasa disebut dengan *cover object*. Sehingga keberadaan pesan tersebut menjadi sulit dideteksi (Majeed M. A dkk., 2021). Kombinasi antara enkripsi dan steganografi dapat memberikan keamanan yang lebih tinggi, karena selain menyembunyikan isi pesan, metode gabungan keduanya dapat menyamarkan keberadaan pesan tersebut (Thabit R dkk., 2022).

Cover object pada steganografi memiliki banyak jenis yaitu gambar, video dan teks. Di antara media steganografi tersebut, *cover object* pada teks khususnya PDF (*Portable Document Format*) memiliki beberapa kelebihan. Salah satunya adalah PDF merupakan format dokumen yang fleksibel dan banyak digunakan untuk bertukar informasi karena memiliki sifat yang tidak bergantung pada perangkat lunak, perangkat keras dan sistem operasi. Hal tersebut menjadikan PDF salah satu *cover object* yang populer digunakan sebagai *cover object* (Thabit R dkk., 2022; Dhawan S & Gupta R, 2020).

Akan tetapi, steganografi pada media PDF memiliki berbagai kekurangan. Salah satunya adalah kurangnya ruang dalam *file* berbasis teks seperti PDF, yang menyebabkan kapasitas penyimpanan pesan rahasia menjadi lebih kecil jika

dibandingkan dengan *cover object* seperti gambar atau video (Dhawan S. dan Gupta R., 2020). Selain itu, jika terdapat struktur PDF yang kompleks maka akan membutuhkan teknik khusus untuk menyimpan pesan rahasia tanpa merusak format aslinya. Salah satu teknik yang dapat digunakan adalah *Least Significant Bit (LSB) substitution*, di mana teknik tersebut dapat memanfaatkan operator dalam PDF seperti *Tj*, *Tw*, dan *Tc* untuk menyimpan pesan rahasia (Khosravi B dkk., 2019). Teknik LSB ini memiliki kelebihan jika dibandingkan dengan metode lainnya, seperti penyimpanan pesan rahasia di antara kata atau di antara karakter. Karena teknik LSB ini tidak menambahkan komponen baru dalam *file* PDF dan hanya menggunakan operator yang sudah ada di dalam PDF tersebut. Sehingga tidak menimbulkan kecurigaan bahkan ketika *file* dibuka menggunakan aplikasi PDF *reader* biasa (Sofian N dkk., 2020).

Meskipun memiliki peluang sukses yang besar, penelitian steganografi pada media PDF masih jarang dilakukan jika dibandingkan dengan steganografi pada *cover object* lain seperti gambar atau audio. Hal ini menjadi peluang untuk mengembangkan sistem yang dapat memanfaatkan kelebihan PDF sebagai *cover object*, sekaligus mengatasi keterbatasan kapasitasnya. Salah satu cara untuk meningkatkan keamanan steganografi pada media PDF adalah dengan menggunakan enkripsi pada pesan rahasia sebelum menyimpannya ke dalam *file* PDF, contohnya adalah dengan menggunakan *Advanced Encryption Standard* (AES) dengan mode operasi *Cipher Block Chaining* (CBC) (Sofian N dkk., 2020).

AES-256 menawarkan tingkat keamanan yang sangat tinggi dengan panjang kunci 256-bit, menjadikannya standar yang kuat dan direkomendasikan untuk melindungi data sensitif dari serangan *brute-force* dan kriptanalisis modern (Alfani dkk., 2020). Keandalan dan efisiensi AES telah diakui dalam berbagai aplikasi keamanan data, mulai dari pengamanan transaksi digital hingga *e-voting*, memberikan fondasi kuat untuk kerahasiaan pesan yang akan disembunyikan. Kekuatan AES-256 ini memastikan bahwa meskipun pesan yang disisipkan dalam PDF berhasil ditemukan oleh pihak yang tidak berwenang, isi pesan tersebut tetap tidak dapat dipecahkan tanpa kunci dekripsi yang benar.

Pengembangan sistem keamanan data ini memerlukan platform aplikasi web yang robust dan efisien. *Framework* Laravel dikenal luas akan kemampuannya dalam mempercepat proses *coding* dan pengembangan aplikasi web yang efisien (Arimbi dkk., 2022). *Framework* ini menyediakan berbagai fitur-fitur keamanan bawaan yang esensial, seperti perlindungan terhadap serangan *cross-site scripting* (XSS) dan *SQL injection*, serta sistem autentikasi dan otorisasi yang kokoh (Sari D. P. & Wijanarko R., 2019). Selain itu, Laravel mengadopsi arsitektur *Model-View-Controller* (MVC) yang terstruktur, memudahkan pengelolaan kode, skalabilitas, dan kolaborasi dalam tim pengembangan. Dengan menggunakan Laravel, pengembangan sistem dapat dilakukan secara lebih efisien, modular, dan menghasilkan aplikasi yang *robust* dengan *user interface* yang interaktif (Arimbi dkk., 2022).

Oleh karena itu, penulis mengusulkan pengembangan sebuah *website* berbasis Laravel yang dapat melakukan proses steganografi pada media PDF. Sistem steganografi pada media PDF ini akan menyimpan pesan ke dalam objek *stream* pada PDF, dengan keamanan tambahan melalui proses enkripsi menggunakan AES-256 sebelum penyimpanannya. Dengan sistem ini, diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan pertukaran informasi digital melalui media *file* PDF.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah yang dapat diajukan dalam penelitian ini adalah:

1. Bagaimana merancang dan mengimplementasikan aplikasi website berbasis Laravel yang mengintegrasikan kriptografi *AES-256* dan steganografi pada dokumen PDF untuk mengamankan data?
2. Bagaimana hasil implementasi website berbasis Laravel dan tingkat keamanan kriptografi *AES-256* serta steganografi pada dokumen PDF untuk keamanan data?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk:

1. Merancang dan mengimplementasikan aplikasi website berbasis Laravel yang mengintegrasikan kriptografi *AES-256* dan steganografi pada dokumen PDF untuk mengamankan data.
2. Menganalisis pengaruh penyisipan data pada file PDF terhadap ukuran file, kualitas dokumen, dan performa website dalam melakukan pengamanan data untuk memastikan efektivitas dan efisiensi sistem yang dikembangkan.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik dari sisi teoritis maupun praktis, sebagai berikut:

1.4.1 Manfaat Teoritis

1. Memberikan kontribusi pada pengembangan teknik steganografi pada dokumen PDF dengan integrasi kriptografi *AES-256*.
2. Menambah referensi penelitian dalam bidang keamanan data dengan memanipulasi *stream* dan *metadata* PDF.
3. Memberikan *insight* baru tentang efektivitas kombinasi kriptografi dan steganografi dalam pengamanan data digital

1.4.2 Manfaat Praktis

1. Menghasilkan sebuah aplikasi berbasis web yang dapat digunakan untuk melindungi informasi rahasia dalam dokumen PDF.
2. Memberikan solusi praktis untuk menjaga kerahasiaan pesan dalam komunikasi digital, terutama untuk sektor-sektor seperti pemerintah, pendidikan, dan perusahaan.
3. Menyediakan website yang dapat digunakan untuk penelitian lebih lanjut dalam bidang keamanan informasi berbasis steganografi pada media PDF.

1.5 Ruang Lingkup Penelitian

Berdasarkan tujuan penelitian diatas, maka ruang lingkup penelitian ini yaitu:

1. Penelitian ini hanya menguji PDF umum yang dapat diakses oleh semua orang.
2. Teknik steganografi pada penelitian ini terbatas di penyisipan pada *Metadata* dan objek *Stream* pada file PDF baik untuk penyisipan teks serta file rahasia.

3. Kapasitas penyisipan pada file *cover* PDF untuk pesan teks tergantung pada besarnya size file *cover*, namun berdasarkan spesifikasi device yang digunakan data yang dapat disisipkan kurang lebih 671.180 *bytes* atau 500.000 huruf.
4. Lingkungan pengujian sistem dilakukan pada Windows 11, server lokal 127.0.0.1:5000 dan penyimpanan lokal.

1.6 Struktur Organisasi Skripsi

Sistematika penulisan penelitian disusun berdasarkan pedoman penulisan karya ilmiah UPI 2024 sebagai berikut:

1. BAB I PENDAHULUAN

   Bab I berupa Pendahuluan yang berisi latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan ruang lingkup penelitian.
2. BAB II TINJAUAN PUSTAKA

   Bab II berupa Tinjauan Pustaka yang berisi uraian teori dan penelitian terdahulu yang relevan sebagai dasar untuk mendukung penelitian. Bagian ini juga mencakup kerangka teori dan konsep yang menjadi landasan penelitian..
3. BAB III METODE PENELITIAN

   Bab III berisi uraian Metode Penelitian untuk menjelaskan metode yang digunakan dalam penelitian.
4. BAB IV HASIL DAN PEMBAHASAN

   Bab IV berisi hasil implementasi dan pengujian aplikasi website berbasis Laravel yang mengintegrasikan kriptografi AES-256 dan steganografi PDF.
5. BAB V SIMPULAN DAN SARAN

   Bab V berupa Simpulan dan Saran yang berisi simpulan dari hasil penelitian yang telah dilakukan dan saran untuk pengembangan penelitian selanjutnya dalam bidang keamanan data berbasis steganografi dan kriptografi.