BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital, keamanan data menjadi perhatian utama karena semakin tingginya ancaman terhadap privasi dan integritas informasi. *QR Code* (*Quick Response Code*) merupakan teknologi yang banyak digunakan untuk menyimpan dan menyampaikan informasi dalam berbagai bentuk, termasuk teks, URL, hingga data biner. Meskipun praktis dan efisien, *QR Code* memiliki kelemahan dalam aspek keamanannya, terutama jika data di dalamnya tidak dilindungi dengan baik. Hal ini membuka peluang bagi pihak yang tidak bertanggung jawab untuk mencuri, memanipulasi, atau menyalahgunakan data tersebut.

Salah satu pendekatan untuk meningkatkan keamanan data adalah dengan mengadopsi teknik kriptografi dan steganografi. Kriptografi adalah seni dan ilmu untuk menjaga kerahasiaan data dengan cara mengubahnya menjadi bentuk yang tidak dapat dimengerti tanpa kunci tertentu. Di sisi lain, steganografi adalah teknik menyembunyikan informasi di dalam media lain sehingga keberadaan informasi tersebut tidak terdeteksi (Johnson & Katzen, 2000).

Salah satu metode steganografi yang banyak digunakan adalah *Least Significant Bit* (LSB). Teknik ini menyembunyikan data dengan memodifikasi Bit paling tidak signifikan pada media digital, seperti gambar, tanpa mengubah tampilan visual secara signifikan. Metode *Least Significant Bit* merupakan salah satu teknik steganografi yang paling sederhana dan banyak digunakan, di mana data disisipkan ke dalam bit paling tidak signifikan dari suatu piksel dalam citra digital. Teknik ini memiliki keunggulan karena perubahan bit pada posisi tersebut tidak menyebabkan perubahan visual yang signifikan pada gambar (Kurniasih, dkk., 2023). Namun, metode *Least Significant Bit* memiliki kelemahan, seperti potensi deteksi oleh serangan analisis statistik. Untuk mengatasi keterbatasan ini, metode kriptografi seperti Kriptografi Visual *Secret Sharing* (KVSS) dapat digunakan sebagai pelengkap. Kriptografi Visual *Secret Sharing* adalah metode membagi data menjadi beberapa share yang secara individual tidak bermakna, tetapi dapat digabungkan untuk merekonstruksi data asli (Naor & Shamir, 1994).

Penggabungan kedua metode ini memberikan solusi inovatif dalam menjaga keamanan data *QR Code*. Data biner dari *QR Code* dapat disembunyikan menggunakan teknik *Least Significant Bit*, yang efektif menyembunyikan informasi tanpa mengubah tampilan visual media secara signifikan (Zahra, dkk. 2024). Selain itu, data tersembunyi ini dilindungi lebih lanjut menggunakan metode Kriptografi Visual *Secret Sharing*, yang membagi data menjadi beberapa bagian (*share*) sehingga data hanya dapat direkonstruksi ketika seluruh *share* digabungkan. Dengan kombinasi ini, keamanan data menjadi berlapis, sehingga lebih sulit diakses tanpa otorisasi yang sah. Penelitian terkait, seperti yang dilakukan oleh Zahra, dkk. (2024), melakukan penelitian terkait autentikasi *QR Code* dan mengemukakan pentingnya pengamanan data *QR Code*, sementara penelitian yang dilakukan oleh Humaira, dkk. (2023), mengimplementasikan skema *secret sharing* dan steganografi audio *Least Significant Bit* untuk meningkatkan keamanan informasi.

Penelitian yang dilakukan oleh Sujono, dkk. (2024) membahas pengamanan citra *grayscale* dengan menggabungkan Kriptografi Visual *Secret Sharing* dan Steganografi *Enhanced Least Significant Bit*. Metode ini membagi citra menjadi beberapa bagian dengan kriptografi visual untuk meningkatkan kerahasiaan, kemudian menyembunyikannya menggunakan teknik *Enhanced Least Significant Bit* yang memodifikasi beberapa Bit terakhir citra penutup. Kombinasi kedua metode memberikan tingkat keamanan yang lebih tinggi, karena pesan hanya dapat diungkap jika semua bagian dan teknik digabungkan. Pendekatan ini efektif dalam melindungi informasi visual dari akses tidak sah. Selain itu, penelitian yang dilakukan oleh Dwi (2024), memanfaatkan Kriptografi Shamir *Secret Sharing* dan Steganografi *Least Significant Bit* untuk meningkatkan keamanan pada informasi yang akan disisipkan.

Dengan meningkatnya penggunaan *QR Code* dalam berbagai bidang, termasuk penyimpanan informasi penting, diperlukan sistem keamanan yang mampu melindungi data di dalamnya dari ancaman manipulasi dan akses tidak sah. Penelitian ini menawarkan pendekatan baru dengan menggabungkan metode steganografi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing* secara terintegrasi untuk meningkatkan keamanan *QR Code*. Berbeda dengan penelitian

sebelumnya yang hanya menerapkan salah satu metode atau menggunakannya secara terpisah, penelitian ini memadukan kedua teknik secara sistematis untuk menciptakan perlindungan berlapis. Inovasi utama dari penelitian ini terletak pada penerapan kombinasi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing* yang dirancang untuk memastikan data *QR Code* tersembunyi di dalam citra digital serta hanya dapat direkonstruksi oleh pihak yang berwenang. Dengan demikian, penelitian ini diharapkan dapat berkontribusi dalam mengembangkan metode pengamanan *QR Code* yang lebih efektif dan adaptif terhadap tantangan keamanan data di era digital yang terus berkembang.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, masalah yang dapat dirumuskan sebagai berikut:

1. Bagaimana skema implementasi Steganografi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing* untuk keamanan data *QR Code?*
2. Bagaimana program aplikasi implementasi Steganografi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing* untuk keamanan data *QR Code* menggunakan *Python*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan dari penelitian ini sebagai berikut:

1. Merancang skema dan algoritma implementasi Steganografi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing* untuk keamanan data *QR Code.*
2. Mengkonstruksi program aplikasi implementasi Steganografi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing* untuk keamanan data *QR Code* dalam program aplikasi *Python*.

1.4 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut:

1. Data yang digunakan sebagai pesan rahasia merupakan data biner yang diekstrak dari *QR Code* versi 5-10.
2. Citra yang digunakan sebagai *cover image* adalah citra *grayscale* dengan format *.png.*

3. Ukuran citra *cover image* harus sesuai dengan jumlah Bit data biner yang akan disisipkan
4. Banyak n *share* yang dihasilkan terbatas yaitu 3.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1. Secara praktis, penelitian ini menghasilkan program aplikasi implementasi Steganografi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing* dengan bahasa pemograman *Python* yang diharapkan dapat digunakan oleh *user* untuk mengamankan data dalam *QR Code.*
2. Penelitian ini diharapkan dapat menjadi alternatif implementasi Steganografi *Least Significant Bit* dan Kriptografi Visual *Secret Sharing.*