BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era teknologi yang terus berkembang, keamanan informasi menjadi sangat penting. Salah satu dampak dari perkembangan teknologi adalah ancaman diretasnya informasi yang bersifat rahasia (Humaira dkk., 2023). Berdasarkan kemungkinan tersebut, individu, lembaga, atau pun perusahaan akan melindungi informasi rahasia agar tidak diretas dan disalahgunakan oleh pihak yang tidak berwenang. Seseorang harus tetap waspada saat memberikan kepercayaan kepada satu orang untuk mengetahui informasi rahasia, karena ada kemungkinan terjadi penyimpangan atas perjanjian dan peraturan dari kedua belah pihak. Jika seseorang mempercayakan informasi rahasia pada satu pihak saja, ada kemungkinan pihak tersebut akan menyalahgunakan wewenang yang diberikan kepadanya, yang dapat merugikan pihak lain yang terlibat dengan informasi rahasia tersebut (Daniel, 2017).

Contoh dari permasalahan tersebut adalah ketika seseorang memiliki informasi rahasia yaitu sebuah *password* untuk mengakses akun *mobile banking*. Ia ingin mempercayakan *password* tersebut kepada orang lain tetapi informasi tersebut tetap terjamin keamanannya. Hal itu dapat dilakukan dengan memodifikasi informasi rahasia sebelum menyerahkannya sehingga orang yang dititipkan tidak tahu informasi rahasia secara langsung, atau dengan membuat kode rahasia untuk membuka informasi rahasia tersebut (Daniel, 2017).

Berdasarkan pemaparan tersebut, terdapat cara untuk menyelesaikan masalah tersebut, yaitu dengan menggunakan teknik kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan (informasi) dengan cara menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya (Kurniasih dkk., 2023). Untuk mengamankan pesan dibutuhkan proses enkripsi yaitu mengubah pesan asli (plainteks) menjadi pesan tersamar (cipherteks), dan juga proses dekripsi yaitu pengembalian cipherteks menjadi plainteks (Munir, 2019).

Cabang dari ilmu kriptografi yang dapat menjadi solusi dari permasalahan tersebut adalah skema pembagian data rahasia (*secret sharing schemes*). Konsep dari *secret sharing schemes* adalah memecah rahasia menjadi potongan-potongan informasi (*share)* yang diberikan kepada sekelompok orang sehingga orang-orang tersebut harus dikumpulkan jika ingin mendapatkan kembali rahasia tersebut (Daniel, 2017). Skema pembagian data rahasia ditemukan oleh Shamir pada tahun 1979 dinamakan *Shamir Secret Sharing* atau lebih dikenal dengan Skema Ambang Shamir (*Shamir Threshold Scheme*) (Munir, 2019).

Untuk meningkatkan keamanan informasi rahasia, teknik kriptografi dapat digabungkan dengan teknik steganografi. Teknik steganografi yang merupakan metode menyembunyikan informasi ke dalam sebuah media, dapat berupa media gambar, *audio* maupun video, sehingga informasi rahasia tersebut tidak dapat diketahui keberadaannya oleh orang lain (Kurniasih dkk., 2023). Salah satu metode steganografi yang sering digunakan adalah *Least Significant Bit* (LSB).

Humaira dkk. (2023) melakukan penelitian dengan judul "Penggabungan Kriptografi Skema Pembagian Data Rahasia dan Steganografi *Audio Least Significant Bit* (LSB)". Penelitian tersebut menghasilkan program *Shamir Threshold Scheme* dengan Skema (3,4) yang berarti program dapat mengkonstruksi *share* untuk 4 partisipan dan membutuhkan 3 partisipan untuk merekonstruksi *secret*. Kemudian Skema (3,4) digabungkan dengan steganografi LSB menggunakan media *cover* berupa *audio*. Pesan rahasia yang diproses dalam penelitian tersebut berupa PIN angka 6 digit dengan digit pertama tidak sama dengan nol. Pada proses konstruksi *share* program akan menghasilkan 4 buah *share* berupa file *audio*.

Chuang dkk. (2010) melakukan penelitian dengan judul "*A Novel Secret Sharing Techniques Using QR Code*". Penelitian tersebut menghasilkan program untuk mengkonstruksi *share* dan merekonstruksi *secret* menggunakan metode *Shamir Threshold Scheme* dengan *input* dan *output* berupa *QR Code*. Pada tahun 2024, Az-zahra dkk. melakukan penelitian dengan judul "Implementasi *QR Code* dengan Algoritma SHA-256 dan RSA yang Ditingkatkan untuk Autentikasi Dokumen Digital". Penelitian tersebut membuat tanda tangan elektronik dengan

menggabungkan algoritma RSA yang ditingkatkan dan algoritma hashing SHA-256. Tanda tangan tersebut diubah menjadi *QR Code* untuk mempermudah autentikasi dokumen digital. *QR Code* dapat memuat tautan yang merujuk kepada pesan teks, gambar, video, audio, alamat *email*, dan lainnya.

Berdasarkan penelitian terdahulu, penulis tertarik melakukan penelitian penggabungan kriptografi *Shamir Secret Sharing* dan steganografi *Least Significant Bit* dengan *QR Code*. Pada penelitian ini, *input* dari proses konstruksi *share* yaitu pesan teks dapat berupa angka, huruf, simbol, maupun kombinasi ketiganya. Setiap *share* dari metode *Shamir Secret Sharing* akan disembunyikan pada media *cover* berupa citra RGB menggunakan metode *Least Significant Bit* sehingga menghasilkan *stego image*. *Output* akhir dari program berupa *QR Code* yang berisi *stego image* tersebut. Kemudian *input* pada proses rekonstruksi *secret* yaitu *QR Code* dan *output*-nya yaitu pesan semula. Penulis tetap menggunakan steganografi LSB karena LSB dilakukan dengan dengan mengganti *bit* terakhir dari setiap *pixel* pada citra digital dan menggantikannya dengan *bit* pesan yang akan disembunyikan. Hasil akhir metode LSB tidak akan jauh berbeda dengan citra yang belum disisipkan pesan, bahkan tidak terlihat perbedaanya secara kasat mata (Mufadilah, 2019). Oleh karena itu, penulis melakukan penelitian dengan judul "Penggabungan Kriptografi *Shamir Secret Sharing* dan Steganografi Citra RGB *Least Significant Bit* dengan *QR Code*".

1.2 Rumusan Masalah

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

1) Bagaimana skema dan algoritma penggabungan kriptografi *Shamir Secret Sharing* dan steganografi citra RGB *Least Significant Bit* dengan *QR Code*?
2) Bagaimana merancang program aplikasi penggabungan kriptografi *Shamir Secret Sharing* dan steganografi citra RGB *Least Significant Bit* dengan *QR Code* menggunakan Python?
3) Bagaimana validasi program aplikasi penggabungan kriptografi *Shamir Secret Sharing* dan steganografi citra RGB *Least Significant Bit* dengan *QR Code*?

1.3 Tujuan Penelitian

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

1. Mengkonstruksi skema dan algoritma penggabungan kriptografi *Shamir Secret Sharing* dan steganografi citra RGB *Least Significant Bit* dengan *QR Code*.
2. Merancang program aplikasi penggabungan kriptografi *Shamir Secret Sharing* dan steganografi citra *Least Significant Bit* dengan *QR Code* dalam program aplikasi menggunakan Python.
3. Memvalidasi program aplikasi penggabungan kriptografi *Shamir Secret Sharing* dan steganografi citra RGB *Least Significant Bit* dengan *QR Code.*

1.4 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut:

1) Pesan teks sebagai pesan asli maksimal 8 karakter berupa karakter ASCII dari 32 sampai 126.
2) *Shamir Secret Sharing* yang akan digunakan adalah Skema (t, w), dengan $w \leq 10$ dan $2 \leq t \leq w$. Input dari w dan t berdasarkan sudut pandang *user*.
3) Citra RGB yang digunakan pada penelitian ini yaitu *file* gambar dengan format png.
4) *Stego key* yang digunakan pada penelitian ini yaitu bilangan acak yang diperoleh dari metode *Pseudo Random Number Generator* (PRNG) yang dibangkitkan oleh algoritma *Linear Congruential Generator* (LCG).

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1) Secara praktis, penelitian ini menghasilkan program aplikasi penggabungan kriptografi *Shamir Secret Sharing* dan steganografi citra metode *Least Significant Bit* dengan *QR Code* dengan bahasa pemograman Python yang diharapkan dapat digunakan oleh *user* untuk mempermudah membagikan pesan rahasia.
2) Penelitian ini diharapkan dapat memberi pemahaman mengenai implementasi kriptografi *Shamir Secret Sharing Scheme* dan steganografi *Least Significant Bit.*

3) Penelitian ini diharapkan dapat digunakan sebagai bahan referensi bagi peneliti lain untuk mengembangkan topik yang terkait penggabungan kriptografi dan steganografi.