

BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi memberikan manfaat khususnya dalam pertukaran data. Oleh karena itu, keamanan dalam pertukaran data melalui jaringan perlu diperhatikan untuk menghindari tindak kejahatan seperti pencurian data pribadi ataupun perusahaan. Kriptografi adalah salah satu solusi yang dapat mengatasi keamanan dalam pertukaran data. Kriptografi merupakan ilmu yang mempelajari cara mengamankan data atau *plaintext* yang dipertukarkan antara pihak pengirim dan penerima agar tetap aman tanpa ada gangguan dari pihak lainnya (Antoni, 2021). Kriptografi telah lama digunakan untuk melindungi suatu data yang bersifat rahasia dan menjadi semakin penting karena semakin banyak data yang disimpan dan dikirim melalui jaringan.

Algoritma RSA merupakan algoritma kriptografi asimetris modern yang mengenkripsikan *plaintext* dengan melakukan transformasi pada *plaintext* menjadi blok-blok. Algoritma RSA menggunakan dua bilangan bulat prima untuk menghitung nilai *public key* dan *private key* yang akan digunakan dalam proses enkripsi serta dekripsi. Algoritma RSA merupakan algoritma enkripsi kunci publik pertama di dunia dan bertahan hingga saat ini dengan uji waktu yang sangat baik (Smart, 2003). Beberapa peningkatan dapat dilakukan untuk menambah keamanan algoritma RSA, salah satunya dapat berupa penambahan banyaknya bilangan bulat prima yang digunakan (Firdaus, 2018). RSA yang ditingkatkan dapat diimplementasikan pada autentikasi dokumen digital (Az-Zahra, 2024) ataupun pada pengamanan aplikasi pengirim email (Putri, 2023).

Ciphertext yang dihasilkan dari proses enkripsi pada suatu algoritma kriptografi memiliki bentuk yang dapat dilihat sehingga kecurigaan bahwa terdapat suatu pesan rahasia dapat ditimbulkan. Terdapat metode pengamanan data dengan cara menyembunyikan data ke dalam media lain yang disebut dengan steganografi. Steganografi adalah ilmu untuk melakukan pertukaran data dengan cara

menyembunyikan data pada suatu media berupa citra digital, audio, video, dan lain sebagainya. Berbeda dengan kriptografi, data yang disembunyikan pada suatu media menggunakan steganografi hanya akan diketahui keberadaannya oleh pihak-pihak yang terlibat dan pihak lain tidak akan mengetahui keberadaannya (Ashok, dkk., 2010). Media citra digital merupakan media yang paling banyak digunakan untuk menyembunyikan data. Data dapat diubah menjadi *bit stream* dan disisipkan pada citra digital. Proses menyisipkan data (*embedding*) pada citra digital (*cover-image*) akan menghasilkan *stego-image*. Proses mengembalikan data yang disisipkan (*extracting*) akan menghasilkan *plaintext* apabila data berupa teks. Salah satu contoh algoritma steganografi yang dapat menyembunyikan data teks pada gambar adalah algoritma *Spread Spectrum*.

Algoritma *Spread Spectrum* merupakan metode komunikasi yang menyebar sinyal informasi pada seluruh frekuensi yang tersedia dengan memilih tempat untuk menyisipkan data pada frekuensi yang rendah yang disertai dengan *pseudo-noise* (Nasution, 2020). *Embedding* data pada algoritma *Spread Spectrum* dilakukan dengan cara menyebarkan data yang akan disisipkan melalui operasi hitung ataupun logika. Meskipun demikian, *stego-image* yang dihasilkan oleh algoritma *Spread Spectrum* tidak akan berbeda secara signifikan dengan *cover-image* sehingga keberadaan data yang disisipkan tidak akan diketahui keberadaannya. Algoritma *Spread Spectrum* dapat menyisipkan *ciphertext* yang dihasilkan dari enkripsi suatu *plaintext* ke dalam gambar (Daud, 2023).

Berdasarkan uraian di atas, penelitian ini mengimplementasikan algoritma kriptografi RSA yang ditingkatkan dengan algoritma steganografi *Spread Spectrum* untuk mengamankan data teks dengan cara mengenkripsi data teks (*plaintext*) menggunakan algoritma RSA yang ditingkatkan kemudian menyembunyikan *ciphertext* yang dihasilkan pada citra berwarna. Perlu diperhatikan jika implementasi dari kombinasi algoritma RSA yang merupakan algoritma enkripsi kunci publik pertama di dunia dengan algoritma *Spread Spectrum* yang menyebar data pada tempat tertentu dapat menjaga kerahasiaan data dan menyembunyikan keberadaannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, permasalahan yang dapat dirumuskan adalah sebagai berikut:

1. Bagaimana skema penggabungan algoritma kriptografi RSA yang ditingkatkan dengan steganografi *Spread Spectrum* pada citra berwarna?
2. Bagaimana implementasi penggabungan algoritma kriptografi RSA yang ditingkatkan dengan steganografi *Spread Spectrum* dalam bentuk program aplikasi dengan bahasa pemrograman Python?
3. Bagaimana kualitas *stego-image* yang dihasilkan dari penggabungan algoritma RSA yang ditingkatkan dengan steganografi *Spread Spectrum*?

1.3 Tujuan Penelitian

Tujuan dilakukannya penelitian ini berdasarkan rumusan masalah tersebut adalah sebagai berikut:

1. Mengetahui proses penggabungan algoritma kriptografi RSA yang ditingkatkan dengan steganografi *Spread Spectrum* pada citra berwarna.
2. Memberikan gambaran dari implementasi kriptografi RSA yang ditingkatkan dan steganografi *Spread Spectrum* dalam bentuk program aplikasi dengan bahasa pemrograman Python.
3. Mengetahui kualitas *stego-image* yang dihasilkan dari penggabungan algoritma RSA yang ditingkatkan dengan steganografi *Spread Spectrum* berdasarkan perbandingan hasil uji kualitas citra antara *cover-image* dengan *stego-image*.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat dalam beberapa hal, di antaranya adalah sebagai berikut:

1. Memberikan kontribusi dalam bidang kriptografi, khususnya dalam perkembangan kriptografi dan steganografi melalui penggabungan algoritma kriptografi RSA yang ditingkatkan dan steganografi *Spread Spectrum*.
2. Aplikasi yang dikembangkan dapat dimanfaatkan untuk pengamanan dan penyembunyian *plaintext* dengan menggunakan penggabungan algoritma kriptografi RSA yang ditingkatkan dan steganografi *Spread Spectrum*.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. *Plaintext* berupa data teks yang terdiri dari karakter ASCII yang dapat dicetak dalam rentang 0 hingga 255.
2. Citra berwarna yang digunakan sebagai *cover-media* dalam format '.png'.