BAB III
METODE PENELITIAN

3.1 Masalah Keamanan Pesan

Dalam perkembangan teknologi komunikasi, keamanan dalam pengiriman pesan harus diperhatikan. Pengirim pesan harus berhati-hati jika mengirim pesan melalui pihak ketiga, terutama jika pesan tersebut bersifat rahasia. Terkadang, pihak ketiga dapat memecahkan *chipertext*. Seiring kemajuan teknologi, media sosial menjadi salah satu cara untuk bertukar pesan. Melalui media sosial pesan menjadi lebih cepat sampai, namun ada saja hal yang dapat membuat pesan tersebut diketahui oleh penerima yang bukan seharusnya. Dengan menyembunyikan pesan pada gambar maka orang lain tidak akan curiga. Salah satu cara untuk meningkatkan keamanan yaitu dengan menggunakan kriptografi yang dimodifikasi dan dikombinasikan dengan steganografi.

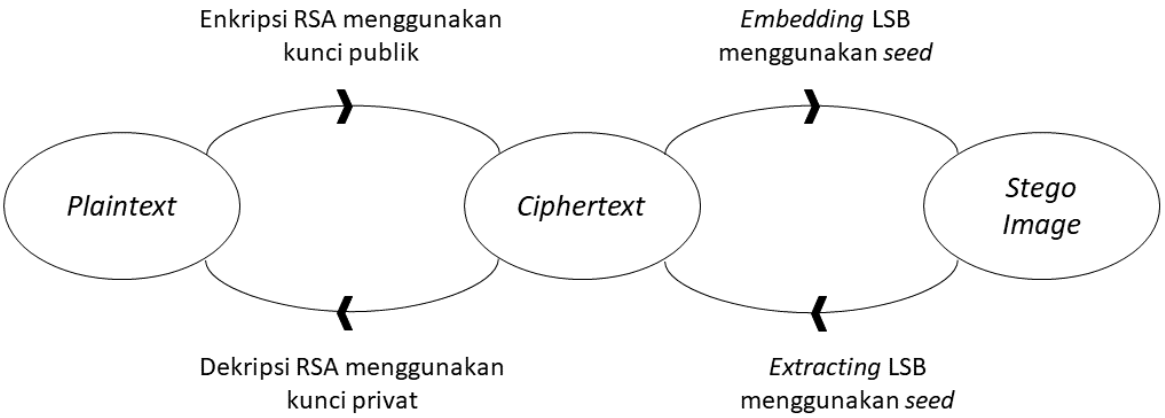
3.2 Mengkaji Model Dasar

Algoritma RSA merupakan salah satu algoritma kriptografi yang masih dianggap aman karena dalam menkriptanalis RSA terdapat proses memfaktorkan sebuah bilangan yang sangat besar menjadi dua buah bilangan prima. Walaupun ternyata sudah ada peneliti yang mengemukakan metode untuk menkriptanalis RSA namun membutuhkan waktu yang lama untuk menemukan dua buah bilangan prima tersebut.

Steganografi merupakan salah satu cara untuk meningkatkan keamanan pesan dengan menyembunyikan pesan tersebut pada suatu media. Metode *Least Significant Bit* (LSB) merupakan salah satu metode steganografi dengan cara mengganti bit terakhir dengan pesan yang sudah diubah ke dalam bentuk biner. Metode LSB ini menghasilkan gambar yang tidak jauh berbeda dengan gambar aslinya sehingga keamanan pesan akan tetap terjaga.

3.3 Pengembangan Model Dasar

Pengembangan kriptografi RSA yang ditingkatkan dan steganografi LSB adalah dengan cara menambahkan satu bilangan prima pada pembangkitan kunci sehingga total bilangan prima yang dibutuhkan adalah tiga buah bilangan, kemudian mengkombinasikannya dengan steganografi LSB, sehingga pesan yang akan disampaikan kepada penerima lebih terjamin keamanannya. Proses yang dilakukan oleh pengirim pesan yaitu *plaintext* dienkripsi menggunakan algoritma RSA yang ditingkatkan menjadi *ciphertext* dengan membangkitkan kunci publik, kemudian *ciphertext* akan disembunyikan di dalam sebuah gambar dengan menggunakan metode LSB namun untuk pemilihan lokasi *pixel* dipilih secara acak yang dapat dilakukan dengan metode *pseudorandom number generator* (PRNG) menggunakan *seed*. Proses yang dilakukan oleh penerima pesan yaitu, membangkitkan PRNG menggunakan *seed* yang sama untuk mengetahui lokasi *pixel*. Dengan mengambil bit terakhir dari setiap lokasi *pixel* kemudian bit-bit tersebut disusun sehingga mendapatkan *ciphertext*. *Ciphertext* yang diperoleh lalu didekripsi dengan menggunakan kunci privat RSA sehingga dapat menghasilkan pesan asli yang dikirim oleh pengirim.



Gambar 3.1 Skema proses Enkripsi, *Embedding*, *Extracting*, dan Dekripsi

3.4 Konstruksi Program Komputer

Pembuatan program dari penggabungan kriptografi RSA yang ditingkatkan dengan steganografi LSB menggunakan bahasa pemrograman Python versi 3.7. Bilangan prima yang digunakan untuk membangkitkan kunci berukuran 1024-bit.

Program ini akan memiliki beberapa tampilan menu (*tab*), yaitu pembangkitan kunci, enkripsi dan *embedding*, serta *extracting* dan dekripsi.

Pada menu pembangkitan kunci akan menghasilkan dua buah *file object* Python, yaitu kunci publik dan kunci privat. Pada menu enkripsi dan *embedding*, masukan (*input*) pada menu ini berupa pesan teks yang akan dienkripsi, kunci publik, serta gambar yang akan dijadikan media untuk menyembunyikan *ciphertext*, dan keluaran (*output*) dari menu ini adalah berupa gambar yang didalamnya terdapat pesan yang diacak dan *seed* yang berbentuk *file object* Python. Sementara pada menu *extracting* dan dekripsi *input* berupa kunci privat, *seed* juga gambar yang berisi *ciphertext*, dan *output* dari menu ini adalah pesan yang disembunyikan pada gambar.

3.5 Validasi

Pada tahap ini dilakukan validasi terhadap program komputer yang dirancang. Tahap validasi dilakukan untuk mengetahui apakah *ciphertext* hasil enkripsi RSA yang ditingkatkan yang kemudian disisipkan (*embedding*) pada citra dapat mengembalikan *plaintext* pada proses *extracting* LSB dan dekripsi RSA yang ditingkatkan.

3.6 Menarik Kesimpulan

Tahap terakhir yang dilakukan adalah menarik kesimpulan dari hasil penelitian yang telah dilakukan dan memberikan rekomendasi-rekomendasi untuk peneliti selanjutnya agar mendapatkan hasil penelitian yang lebih baik.