BAB III
METODE PENELITIAN

3.1 Identifikasi Masalah

Dalam pekembangannya teknologi dan telekomunikasi yang semakin pesat, maka keamanan informasi dalam pengiriman pesan harus diperhatikan. Pengirim pesan perlu berhati-hati dalam mengirim pesan yang bersifat pribadi atau rahasia supaya pihak ketiga tidak dapat memecahkan *ciphertext*. Seiring dengan kemajuan teknologi, banyak cara untuk mengamankan pesan supaya tidak mudah dikriptanalisis. Dengan menyembunyikan pesan pada gambar maka orang lain tidak akan curiga. Untuk meningkatkan keamanan informasi salah satunya dapat dilakukan dengan cara menggabungkan kriptografi dan steganografi.

3.2 Model Dasar

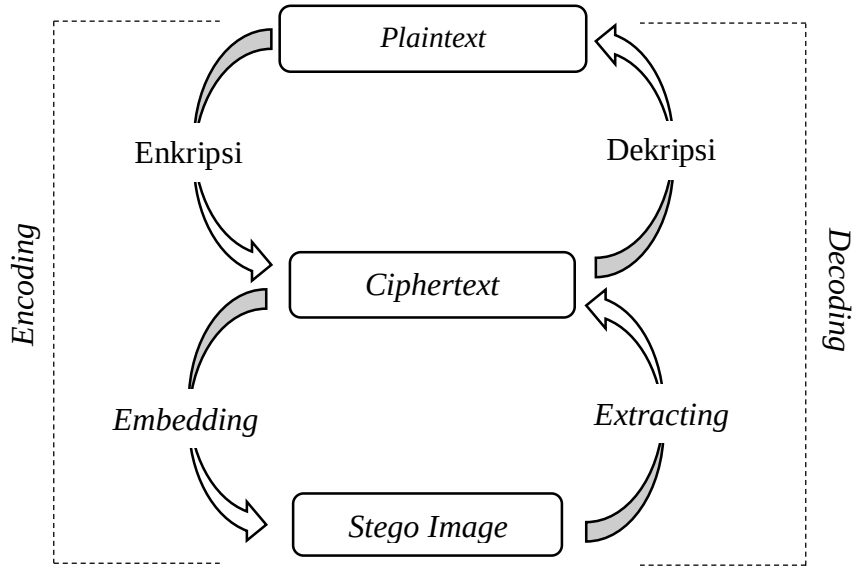
Algoritma AES merupakan algoritma yang masih dianggap aman karena pada prosesnya membutuhkan pengulangan dan membangkitkan kunci untuk setiap pengulangan, sehingga membutuhkan waktu yang cukup lama untuk menemukan kuncinya.

Untuk lebih meningkatkan keamanan pesan, akan menggunakan steganografi untuk menyembunyikan pesan rahasia pada suatu media. Metode steganografi yang digunakan yaitu LSB secara terurut, mengganti bit terakhir pada *byte* sebuah *pixel* dengan bit *ciphertext*.

3.3 Penggabungan Kriptografi AES dan Steganografi LSB

Pada penelitian ini akan menggabungkan kriptografi AES dan steganografi LSB dengan tujuan untuk meningkatkan keamanan pesan. Langkah pertama yang dilakukan adalah membangkitkan kunci dari 128 bit menjadi 1.408 bit, selanjutnya *plaintext* dienkripsi dengan kriptografi AES sehingga diperoleh *ciphertext*. *Ciphertext* yang didapat akan disembunyikan pada citra menggunakan metode LSB sehingga menghasilkan *stego image*. Untuk proses dekripsi, pertama mengeluarkan *ciphertext* dari *stego image*. Kemudian mengubah kembali *ciphertext* menjadi pesan

menggunakan kunci yang didapat dari pengirim pesan. Skema proses enkripsi dan dekripsi dapat dilihat pada gambar berikut:



Gambar 3. 1 Rancangan Proses Enkripsi dan Dekripsi AES

3.4 Kontruksi Program

Program Penggabungan Kriptografi AES dan steganografi LSB ini akan dibuat menggunakan *Python*. Program tersebut bertujuan untuk memudahkan proses pembangkitan kunci, enkripsi, dekripsi, *embedding*, dan *extracting*.

3.4.1 Perancangan Program Aplikasi

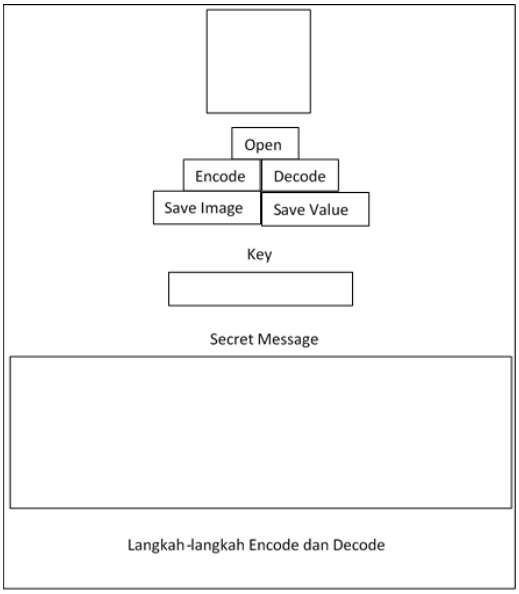
Pada bab ini dilakukan perancangan tampilan untuk program *encode* dan *decode* seperti pada Tabel 3.2. Input dari program *encode* adalah kunci, pesan teks dan gambar yang akan dijadikan media untuk menampung pesan rahasia dengan *output stego image*. Untuk proses *decode* hampir sama, hanya saja pesan sebagai *output* dan *stego image* serta kunci sebagai *input*.

Tabel 3.1 Rancangan Program *Encode* dan *Decode*

Keterangan	*Encode*	*Decode*
Input	- *Plaintext* - Kunci - Gambar	- *Stego Image* - Kunci
Output	- Stego *Image*	- *Plaintext*

3.4.2 Perancangan Tampilan

Program aplikasi komputer dibuat untuk mempermudah enkripsi dan *embedding*, *extracting* dan dekripsi, serta validasi pada gabungan kriptografi dan steganografi. Program dibuat dengan bahasa pemograman Python 3.7. Rancangan program aplikasi komputer dapat dilihat pada Gambar 3.2.



Gambar 3. 2 Rancangan Tampilan Program Aplikasi Komputer

3.4.3 Algoritma Kriptografi AES dan Steganografi LSB

3.4.3.1 Proses Pembangkitan Kunci

Pada penggabungan kriptografi AES dan steganografi LSB, pengirim akan melakukan pembangkitan kunci yang akan dikirim kepada penerima. Berikut langkah pembangkitan kunci AES.

1. Proses membangkitan kunci sesuai dengan sub-bab 2.4.2 Ekspansi Kunci.
2. Diperoleh 10 sub-kunci dan 1 kunci utama.

3.4.3.2 Enkripsi dan *Embedding*

Setelah melakukan pembangkitan kunci, pengirim kemudian melakukan enkripsi terhadap *plaintext* yang akan menghasikan *ciphertext*, kemudian melakukan *embedding* terhadap *cipertext*. Berikut langkah-langkah enkripsi dan *embedding*:

1. Pengirim menentukan *plaintext*, kunci dan gambar sebagai media penyembunyian pesan.
2. Pengirim mengubah setiap karakter pada *plaintext* dan kunci dengan bilangan *hexcadecimal* ASCII dengan aturan setiap karakter menjadi sebuah blok. Untuk setiap perhitungan, karakter ASCII dikonversikan ke dalam bentuk biner.
3. Pengirim kemudian melakukan ekpansi kunci. Selanjutnya pengirim melakukan enkripsi dengan kunci yang sudah didapat. Kemudian didapat *ciphertext*.
4. *Ciphertext* yang didapat dari proses enkripsi akan disisipkan pada sebuah gambar.
5. Untuk setiap lokasi *pixel*, dicari nilai RGB dan selanjutnya nilai RGB dikonversikan ke dalam bentuk biner.
6. Digit terakhir dari setiap *byte pixel* diganti dengan bit dari setiap karakter *ciphertext* sehingga menghasilkan nilai RGB baru. Kemudian diterapkan pada gambar.
7. Gambar yang dihasilkan adalah *stego image*.
8. Pengirim kemudian mengirimkan *stego image* dan kunci pada penerima.

3.4.3.3 *Extracting* dan Dekripsi

Setelah menerima *stego image* dan kunci, penerima kemudian melakukan *extracting* dan dekripsi untuk mengembalikan *plaintext*. Berikut langkah-langkah *extracting* dan dekripsi:

1. Penerima mencari nilai RGB dan nilai RGB tersebut dikonversikan ke dalam bentuk biner.
2. Penerima mengambil digit terakhir nilai RGB dari setiap *byte pixel*.
3. Penerima memperoleh *ciphertext*, dan dikelompokkan dalam tiap *byte*.
4. Penerima kemudian melakukan dekripsi. Bentuk biner yang didapat di konversikan pada bilangan *hexcadecimal*.

5. Penerima kemudian mengubah bilangan *hexcadecimal* menjadi karakter ASCII sehingga penerima memperoleh *plaintext*.

3.5 Validasi

Pada tahap ini dilakukan validasi terhadap program komputer yang dirancang. Tahap validasi dilakukan untuk mengetahui apakah *ciphertext* hasil dari proses penggabungan kriptografi AES yang kemudian disisipkan (*embedding*) pada gambar dapat mengembalikan *plaintext* pada proses *extracting* LSB dan dekripsi AES.

3.6 Kesimpulan

Tahap terakhir yang dilakukan adalah menarik kesimpulan dari hasil pembahasaan yang telah dilakukan dan memberikan saran-saran untuk pembahasan selanjutnya supaya mendapat hasil yang lebih baik.