BAB I
PENDAHULUAN

1.1. Latar Belakang

Kriptografi visual adalah teknik pengamanan citra dimana proses enkripsi dilakukan dengan membagi citra asli menjadi beberapa *share* sehingga dapat didekripsi oleh sistem visual manusia. Skema (*k,n*) *secret sharing* membentuk *n share* menggunakan angka acak sehingga dapat direkonstruksi dengan menyusun minimal *k shares*. Kelemahan skema ini yaitu proses rekonstruksi citra dapat dilakukan oleh siapa saja yang memiliki minimal *k share* dan masih memperlihatkan pola citra aslinya. Untuk memperkuat pengamanan dan menghilangkan pola citra asli pada *chiper image*, maka dapat digunakan teknik enkripsi. AES adalah algoritma standar dalam berbagai *platform* yang masih dianggap aman sampai saat ini. *Chiper image* hasil pengacakan kemudian dibagi menjadi *n shares*. Kelemahan teknik ini yaitu *shares* yang dihasilkan dapat menimbulkan kecurigaan pihak lain.

Untuk menghilangkan kecurigaan pihak lain maka dapat digunakan metode steganografi untuk menyembunyikan *shares* ke citra amplop (*cover image*). Cara yang umum digunakan adalah metode LSB dengan memanfaatkan *least significant bit* dari citra amplop dengan menyisipkan sejumlah *bit shares* secara sekuensial. Algoritma Triple-A yang ditemukan oleh (Gutub, dkk.,2009), memanfaatkan AES dan penggunaan bilangan acak untuk menentukan saluran (R,G,B) yang digunakan sebagai tempat penyisipan dan jumlah bit sisip untuk membuat penyisipan *bit share image* ke citra amplop menjadi lebih bervariasi. Namun algoritma tersebut masih menggunakan penempatan sekuensial. Kelemahan tersebut dapat diatasi dengan menentukan titik awal, arah pergerakan dan titik akhir penyisipan yang dikenal dengan *layout management*. Selanjutnya, generator modulo *p* (*p* adalah bilangan prima) dapat juga digunakan untuk menghasilkan posisi penyisipan yang acak. Dengan memanfaatkan *layout management* dan generator modulo, maka penyerang akan sulit mengetahui posisi yang digunakan sebagai tempat penyimpanan bit-bit *share images* karena tergantung pada nilai kunci, *k* dan *n* serta ukuran citra sampul.

Selanjutnya, untuk mengimplementasikan otoritas yang berbeda bagi pihak pemilik *share*, maka ditambahkan pembobotan yang berbeda pada masing-masing *share*. Dengan demikian terdapat pilihan berdasarkan jumlah *share* minimum, atau jumlah bobot minimum atau gabungan keduanya untuk mendapatkan kembali citra warna yang dirahasiakan. Penelitian ini dilakukan untuk mengetahui pengaruh parameter masukan terhadap serta kualitas *stego images*. Kemudian untuk menguji pengaruh gangguan pada satu *stego image* terhadap hasil ekstraksi, maka dilakukan bentuk gangguan dengan pemberian *noise* terhadap satu *stego image*.

Berdasarkan uraian di atas, maka topik ini diangkat sebagai tugas akhir dengan judul ***"Pengamanan Citra Warna Menggunakan Modifikasi Kriptografi Visual Skema (K,N) Dan Algoritma Triple – A+".***

1.2. Rumusan Masalah

Sesuai dengan latar belakang yang diuraikan di atas yang menjadi permasalahan adalah :

1. Bagaimana pengaruh parameter masukan yang digunakan dalam proses penyisipan terhadap *imperceptability* dan *capacity.*
2. Bagaimana parameter nilai *k* pada saat rekonstruksi mempengaruhi *recovery rate.*
3. Bagaimana pengaruh *noise Salt and Pepper* yang diberikan pada satu *stego images* dalam hal *recovery rate.*

1.3. Tujuan dan Manfaat

Tujuan penyusunan Tugas akhir ini adalah membuat sebuah perangkat lunak pengamanan citra warna dengan memodifikasi kriptografi visual skema (k,n) dengan Algoritma Triple-A+ dengan mode penyisipan berbeda untuk menghindarkan penyisipan sekuensial.

Sedangkan manfaat yang diharapkan dari tugas akhir ini, adalah:

1. Sistem dapat digunakan sebagai alternatif untuk mengamankan pesan rahasia (citra) pada *file* gambar.

2. Perangkat lunak dapat digunakan sebagai aplikasi alternatif untuk mengamankan citra.
3. Laporan Tugas Akhir dapat digunakan sebagai referensi untuk pengembangan sistem kriptografi visual.

1.4. Batasan Masalah

Batasan masalah dalam tugas akhir ini, antara lain:

1. Citra awal yang di-*input* ke perangkat lunak adalah citra berwarna dengan format .bmp.
2. Ukuran citra rahasia minimal 50 x 50 pixel dan maksimal 200 x 200 pixel.
3. Jumlah *n* yang harus di-*input* oleh *user* adalah minimal 6 dan maksimal 10.
4. Jumlah *k* yang harus di-*input* oleh *user* adalah minimal 2 dan maksimal sama dengan jumlah *n* yang ada.
5. Untuk Bobot setiap *share* ($B_1 \ldots B_n$) dibatasi minimal 1 dan maksimal 7
6. Algoritma *Advanced Encryption Standard* (AES) yang digunakan adalah AES-256
7. Untuk menentukan Amplop Khusus (untuk menampung Parameter Masukan), maka ditetapkan aturan-aturan berikut :
   - Ukuran 50 x 50 pixel.
   - Parameter Masukan (PM) = $\text{Key} + \text{K} + \text{N} + B_1 \ldots . Bn + \text{Bobot Minimum} + \text{G1} + \text{G2} = 336$ bit
   - Kebutuhan Parameter Masukan (KP) $= \frac{\text{PM}}{\text{1 bit Sisip} * \text{1 Saluran}}$
   - Penyisipan dengan 1 bit di setiap pixel dan hanya pada saluran B (*blue)* dengan mode sisip menggunakan *Generator Modulo*.
8. Untuk menentukan jumlah bit sisip, saluran, dan mode sisip yang digunakan berdasarkan nilai kunci :
   - Untuk bit sisip maka karakter pertama (C1) dengan cara C1 Mod 4
   - Untuk saluran maka karakter ke dua (C2) dengan cara C2 Mod 7
   - Untuk mode sisip maka karakter ke tiga (C3) dengan cara C3 Mod 3

9. Untuk menentukan citra sampul dilakukan dengan rumus :
   - Total Bit(m) = Panjang Citra Rahasia * Lebar Citra Rahasia * 24
   - Total Pixel (R) = $\frac{\text{m}}{\text{Jlh Bit Sisip} * \text{Jh Saluran}}$
   - Ukuran Sampul (n) = $\sqrt{\frac{R}{Jlh\ Bit\ Sisip * Jlh\ Saluran}}$
10. Untuk mengetahui persentase perbedaan pada setiap citra sampul yang di uji (pada pengujian *Recovery rate*) dilakukan dengan rumus:
    - *Recovery Rate* = $\frac{Jumlah\ pixel\ sama}{Total\ Pixel\ Keseluruhan} * 100\%$
11. Skema penyembunyian yang digunakan adalah
    - *Spiral Movement Scheme*
    - *Snake Movement Scheme*
    - *Generator Modulo* (dimana *p* = Bilangan Prima < (Panjang Sampul * Lebar Sampul)

1.5. Metodologi Penelitian

Metodologi yang digunakan dalam penyusunan tugas akhir ini adalah sebagai berikut:

1. Kajian Literatur

   Pada tahap ini penulis melakukan kajian terhadap literatur untuk memahami cara kerja metode (Algoritma) yang digunakan.
2. Pengembangan sistem dengan model *waterfall*

   2.1. Analisis Kebutuhan.

   Memahami permasalahan dan merumuskan solusi yang tepat dalam pembuatan aplikasi, seperti menggabungkan algoritma *triple-A* dengan metode penyembunyian pesan dan pemodelan sistem menggunakan *Use Case Diagram*.

   2.2. Perancangan.

   a. Merancang langkah-langkah algoritma dengan *Flow Chart*.

   b. Merancang user interface dengan aplikasi *Pencil*.

   2.3. Penulisan Program.

Melakukan penulisan kode program menggunakan C#.net.

2.4. Pengujian.

a. Melakukan pengujian pada pengaruh parameter masukan terhadap kualitas stego *images* (*imperceptability* dan *capacity*).

b. Melakukan pengujian pada pengaruh nilai *k* terhadap *recovery rate* (apabila *k extract* lebih kecil dari *k embed*)

c. Melakukan pengujian kualitas pada stego *cover image* yang akan diberikan *noise* (berupa *salt and pepper)* terhadap *recovery rate*

3. Menarik kesimpulan dari hasil pengujian.
4. Menyusun laporan tugas akhir berdasarkan referensi yang diperoleh dan hasil pengujian dari perangkat lunak hasil konstruksi.