

BAB 1

PENDAHULUAN

Pada bab ini akan dibahas mengenai latar belakang, perumusan masalah, tujuan, pembatasan masalah, dan sistematika penulisan dari Tugas Akhir ini.

1. 1. Latar Belakang

Di era revolusi informasi ini, manusia di seluruh dunia semakin memanfaatkan teknologi informasi dalam aktivitas hidupnya sehari-hari. Seiring perkembangan teknologi informasi, kebutuhan terhadap keamanan informasi semakin tinggi^[2]. Oleh karena itu dengan berkembangnya teknologi informasi, ilmu kriptografi menjadi semakin dibutuhkan untuk melakukan penyandian informasi yang semakin kuat dan aman. Salah satu teknik kriptografi yang paling mudah digunakan yaitu kriptografi visual.

Kriptografi visual adalah teknik enkripsi gambar yang membuat pesan citra rahasia (*hidden image*) ke dalam beberapa transparansi gambar (*share*) yang tidak memiliki arti. Teknik kriptografi visual juga sangat aman dari serangan kriptanalisis karena *share* yang dikirim benar-benar acak. Metoda yang digunakan dalam mengenkripsi dan mengdeskripsi merupakan modifikasi metoda pertukaran kunci *Diffie-Hellman*. Metoda pertukaran kunci *Diffie-Hellman*^[2] merupakan metoda yang memanfaatkan perhitungan modulus bilangan prima sehingga perhitungan akan menjadi mudah dalam mengenkripsi namun sulit untuk dideskripsi.

1. 2. Perumusan Masalah

Perumusan masalah dalam tugas akhir ini meliputi:

1. Bagaimana cara membuat program visual kriptografi menggunakan pendekatan pertukaran kunci *Diffie-Hellman*?
2. Bagaimana cara mengolah data dari perhitungan menggunakan pendekatan pertukaran kunci *Diffie-Hellman*?

1. 3. Tujuan

Dapat menerapkan pendekatan pertukaran kunci *Diffie-Hellman* dalam menyusun program visual kriptografi.

1. 4. Pembatasan Masalah

1. Perancangan dan realisasi menggunakan aplikasi berbasis Matlab.
2. Perhitungan modulus menggunakan bilangan prima.
3. Pengujian hasil percobaan menggunakan metoda SSIM.

1. 5. Sistematika Penulisan

Laporan Tugas Akhir ini disusun dengan sistematika sebagai berikut :

- **BAB 1 : Pendahuluan**

Merupakan bab yang menjelaskan mengenai latar belakang masalah, rumusan masalah, tujuan dan sistematika penulisan dari Tugas Akhir ini.

- **BAB 2 : Landasan Teori**

Merupakan bab yang disusun untuk memberikan penjelasan dan teori-teori penunjang tentang citra digital, *Cryptography*, *Visual Cryptography*, *Key exchange Diffie-Hellman*.

- **BAB 3 : Perancangan Perangkat Lunak**

Merupakan bab yang berisi penjelasan desain yang akan dilakukan untuk membuat Realisasi *Visual Cryptography* Pendekatan *Key exchange Diffie-Hellman*.

- **BAB 4 : Data Pengamatan dan Analisis**

Merupakan bab yang berisi data pengamatan yang diperoleh dari penelitian dan analisis yang diperoleh melalui Tugas Akhir ini.

- **BAB 5 : Simpulan dan Saran**

Merupakan bab yang berisi simpulan dan saran yang dapat diambil untuk melakukan pengembangan terhadap hasil dan sistem yang telah dibuat.