

# BAB 1

## PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang, rumusan masalah, tujuan, batasan masalah, dan sistematika penulisan.

### I.1 Latar Belakang

Dalam beberapa tahun terakhir, proses berbagi informasi dan transfer data antar pengguna telah meningkat pesat. Oleh karena itu ancaman dari pihak ketiga yang ingin mengakses informasi rahasia menjadi keprihatinan untuk para ahli. Dengan semakin majunya jaringan komunikasi, informasi ditransmisikan dengan mudah melalui Internet dan banyak data rahasia (gambar, teks dll) yang dikirimkan. Isu yang perlu dipertimbangkan adalah keamanan, karena munculnya kesempatan mencuri informasi rahasia oleh peretas karena lemahnya keamanan dalam jaringan publik. Untuk menangani masalah keamanan perlu dikembangkan algoritma yang dapat mengamankan data yang dikirim melalui internet. Dengan bantuan dari Visual Kriptografi, sistem informasi visual dapat aman melalui internet. Metode yang digunakan menggabungkan keunggulan dari Visual Kriptografi dan Kriptografi kunci publik. Dengan menggabungkan kedua metode ini akan meningkatkan keamanan dalam menjaga kerahasiaan data.

Visual Kriptografi (VC) adalah teknik enkripsi yang pertama kali diusulkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Teknik ini digunakan untuk mengenkripsi citra rahasia. Visual Kriptografi terbagi menjadi dua tahap yaitu enkripsi dan dekripsi. Enkripsi adalah mengubah citra rahasia menjadi *cipher image* sedang dekripsi merupakan tahap pengembalian *cipher image* menjadi citra rahasia. Untuk dapat bekerja, visual kriptografi membutuhkan algoritma untuk proses enkripsi dan dekripsi. Pada tugas akhir ini algoritma tersebut adalah algoritma RSA.

Algoritma RSA ditemukan oleh Rivest, Shamir dan Adleman pada tahun 1977. Algoritma RSA menggunakan pemfaktoran bilangan besar menjadi faktor-faktornya dan faktornya harus merupakan bilangan prima. Pemfaktoran dilakukan

untuk mendapat kunci rahasia. Selama belum ada algoritma untuk menemukan faktor prima bilangan besar dengan cara mudah dan cepat maka keamanan RSA terjamin.

## **I.2 Perumusan Masalah**

Rumusan masalah dalam tugas akhir ini adalah sebagai berikut :

1. Bagaimana merealisasikan kriptografi visual menggunakan metode RSA?
2. Bagaimana performansi citra awal dengan citra yang telah didekripsi?

## **I.3 Tujuan**

Tujuan dalam tugas akhir ini adalah sebagai berikut :

1. Merealisasikan kriptografi visual menggunakan metode RSA.
2. Menghitung performansi citra sebelum dienkrpsi dengan citra setelah didekripsi menggunakan metode SSIM dan MOS.

## **I.4 Pembatasan Masalah**

Batasan masalah dalam tugas akhir ini adalah sebagai berikut :

1. Citra berupa gambar dengan ukuran 400 x 400 *pixel*
2. Format gambar yang digunakan jpg
3. Program yang digunakan menggunakan perangkat lunak MATLAB 2016
4. Pengujian performansi citra menggunakan SSIM dan MOS
5. Pengujian dengan SSIM menggunakan toolbox pada MATLAB 2016

## **I.5 Sistematika Penulisan**

Dalam laporan tugas akhir ini dibagi menjadi lima bab utama, referensi dan lampiran sebagai pendukung laporan tugas akhir ini. Berikut pembahasan masing-masing bab sebagai berikut :

**BAB I** : PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang, rumusan masalah, tujuan, batasan masalah, dan sistematika penulisan.

**BAB II** : LANDASAN TEORI

Pada bab ini menjelaskan mengenai teori-teori penunjang tugas akhir. Adapun teori penunjang tersebut meliputi: Kriptografi Visual, Algoritma RSA dan Metode pengujian seperti SSIM dan MOS.

**BAB III : PERANCANGAN SISTEM**

Pada bab ini dijelaskan mengenai sistem dari Tugas Akhir ini serta perancangan perangkat lunak dengan menggunakan perangkat lunak MATLAB.

**BAB IV : HASIL DAN ANALISIS**

Bab ini berisikan percobaan-percobaan yang akan dilakukan terhadap perangkat lunak dan menampilkan data pengamatan serta analisis hasil percobaan.

**BAB V : SIMPULAN DAN SARAN**

Bab ini menjelaskan mengenai simpulan dan saran dari bab-bab yang telah dibahas sebelumnya.

