

BAB I

PENDAHULUAN

I.1. Latar Belakang

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang penting dari Sistem Informasi, informasi tidak akan berguna lagi bila telah disadap atau dibajak orang lain. Tuntutan keamanan menjadi semakin kompleks, apalagi bila data itu dikirimkan, dan data itu merupakan data yang sangat rahasia, maka harus dijaga agar tidak dibajak orang lain.

Ada berbagai cara yang digunakan untuk melindungi data misalnya pemberian *password*, tetapi cara ini dapat dibobol oleh para pembajak, karena *user* dapat membuat kemungkinan-kemungkinan kata yang digunakan sebagai *password* oleh pihak yang menguncinya. Cara lain yaitu dengan *Chipertext*, dengan cara ini data yang hendak disimpan disandikan terlebih dahulu, akan tetapi cara ini dapat menarik kecurigaan oleh pihak yang tidak bertanggung jawab, sehingga *user* akan berusaha memecahkan kode-kode penyandiannya, sehingga data tersebut dapat dibajak. Oleh karena itu dibutuhkan suatu cara yang mampu membuat para pembajak tidak curiga dan pemakai tidak langsung mengetahui bahwa ada data yang tersimpan, dan cara itu adalah Steganografi.

Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga

tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung. Media penampung yang banyak digunakan untuk menyembunyikan informasi yaitu citra digital. Penyisipan informasi pada media citra digital dilakukan pada bit-bit *pixel* yang terdapat pada citra. Penggunaan citra digital sebagai media penampung mempunyai kelebihan karena indera penglihatan manusia memiliki keterbatasan terhadap warna, sehingga dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipkan pesan rahasia.

Metode *Pixel Value Differencing (PVD)* merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi. Metode ini menawarkan kapasitas penyimpanan pesan yang lebih besar, dengan kualitas citra yang lebih baik dibandingkan dengan metode lain. Untuk menambah tingkat keamanan dari informasi yang akan disisipkan kedalam citra, steganografi dapat dikombinasikan dengan enkripsi, sehingga informasi yang disisipkan tidak akan mudah dibaca oleh orang yang tidak bertanggung jawab. Salah satu enkripsi yang dapat digunakan yaitu algoritma *Caesar Cipher*. Metode *caesar cipher* berasal dari *Julius Caesar*, yang merupakan kaisar Roma, ia menggunakan *cipher* substitusi untuk mengirim pesan ke panglima perangnya. *Caesar Cipher* dikenal dengan beberapa nama seperti : *Shift Cipher*, *Caesar's Code*, atau *Caesar Cipher Shift*. Metode Enkripsi ini berjenis *cipher* substitusi, dimana setiap huruf pada plainteksnya digantikan dengan huruf lain.

Berdasarkan uraian diatas, maka penulis tertarik untuk menyusunnya dalam bentuk skripsi dengan judul “**Perancangan Aplikasi Steganografi dengan Algoritma Caesar Cipher dan Pixel Value Differencing**”.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah yang ada yaitu sebagai berikut:

1. Pentingnya sebuah aplikasi steganografi agar pesan yang penting tidak bisa dibaca oleh pihak yang tidak bertanggung jawab.
2. Steganografi tersebut dibuat dengan menggunakan kombinasi algoritma *pixel value differencing* dan metode *caesar cipher* agar data tersebut tidak mudah diganggu isi aslinya dari seseorang yang tidak diizinkan.

I.2.2. Perumusan Masalah

Berdasarkan uraian latar belakang terhadap masalah diatas, maka yang menjadi perumusan masalah adalah :

1. Bagaimana menyembunyikan dan mengekstraksi pesan dengan menggunakan steganografi?
2. Bagaimana mengimplementasi steganografi dengan metode *pixel value differencing* pada citra berwarna?
3. Bagaimana melakukan enkripsi pada pesan yang akan disisipkan menggunakan metode *Caesar cipher* ?
4. Bagaimana melakukan kombinasi 2 (dua) algoritma yang berbeda?

I.2.3. Batasan Masalah

Mengingat keterbatasan waktu dalam penulisan dan pengumpulan data maka penulis memberikan batasan masalah untuk mempermudah penyusunan laporan yang sistematis agar mudah dipahami oleh pembaca yaitu :

1. Penyisipan hanya dilakukan pada berkas gambar dengan format BMP.
2. Pada implementasi perangkat lunak, pesan yang akan disisipkan dienkripsi terlebih dahulu baru disisipkan pada *file* gambar.
3. Tidak membahas perubahan kapasitas pada *file* yang akan dijadikan media penyisipan.
4. Pada metode *Caesar Cipher* hanya bisa menggunakan huruf A sampai Z saja, angka dan simbol tidak bisa.
5. Bahasa pemrograman yang digunakan adalah *Borland Delphi 7*.

I.3. Tujuan dan Manfaat Penelitian

I.3.1. Tujuan Penelitian

Adapun yang menjadi tujuan penulisan dalam penyusunan Skripsi adalah sebagai berikut :

1. Untuk menyembunyikan dan mengekstraksi pesan dengan menggunakan steganografi.
2. Untuk mengimplementasi steganografi dengan metode *Pixel Value Differencing* pada citra.
3. Untuk melakukan enkripsi pada pesan yang akan disisipkan menggunakan metode *Caesar cipher*.

I.3.2. Manfaat Penelitian

Sedangkan manfaat dari penulisan ini adalah sebagai berikut:

1. Meningkatkan keamanan pesan dengan menggunakan dua metode, sehingga tidak menimbulkan kecurigaan terhadap orang yang tidak bertanggung jawab.
2. Dengan algoritma *Caesar Cipher* dan metode *Pixel Value Differencing* membuat pesan tidak dapat dibaca atau dimengerti orang lain.
3. Dengan menggunakan metode *Pixel Value Differencing* membuat orang lain tidak akan curiga terhadap pesan yang disembunyikan.

I.4. Metodologi Penelitian

Metode merupakan suatu cara atau teknik yang sistematis untuk memecahkan suatu kasus sehingga memberikan hasil sesuai dengan yang diharapkan.

Penulis menggunakan studi kepustakaan (*library research*), yaitu menggunakan sumber-sumber melalui buku, jurnal, tugas akhir, tesis maupun disertasi, *browsing* melalui internet, serta sumber-sumber lain yang relevan untuk digunakan dalam penelitian ini. Studi kepustakaan dalam penelitian ini adalah hal-hal yang berkaitan dengan ilmu kriptografi dan informatika komputer.

I.4.1. Pengujian/Uji Coba Sistem

Setelah melalui tahapan perancangan sistem maka pada tahap implementasi dilakukan pembangunan sistem untuk menghasilkan aplikasi. Pada tahap ini, dilakukan pemilihan bahasa pemrograman yang akan digunakan

sekaligus penerapannya sampai menghasilkan aplikasi yang diinginkan. Pengujian sistem yang dibuat antara lain adalah :

- a. Pengujian hasil gambar dilakukan dengan bantuan *software* MATLAB, untuk mencari nilai PSNR (*Peak Signal to Noise Ratio*) dan MSE (*Mean Square Error*) pada gambar.
- b. Pengujian aplikasi yang dibuat dengan menginput data teks yang akan diamankan untuk menganalisis keakuratan *output* yang dihasilkan untuk melihat sampai sejauh mana keamanan yang dibuat dapat menampilkan *output* berupa data teks yang telah dienkripsi.
- c. Pengujian aplikasi yang dibuat ini menggunakan metode steganografi *Pixel Value Differencing* dan penerapan algoritma *Caesar Cipher*.

I.5. Keaslian Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan dengan penelitian sebelumnya yang memiliki kemiripan.

1. Andreas Nicolas Tarigan, Pembuatan Aplikasi Penyisipan Pesan Pada *File Mp3* Menggunakan Metode Parity Coding Dan Enkripsi Caesar Cipher.
2. J.K. Mandal, Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain.

Untuk tabel perbandingannya dapat dilihat sebagai berikut:

Tabel I.1 Tabel Perbandingan

No	Materi Perbandingan	Instrumen
Penelitian Pertama : Pembuatan Aplikasi Penyisipan Pesan Pada File Mp3 Menggunakan Metode Parity Coding Dan Enkripsi Caesar Cipher		
1	Metode	Parity Coding dan Caesar Cipher
2	Bahasa Pemrograman	Visual Studio
3	Versi Perangkat	2008
Penelitian Kedua: Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain		
1	Metode	Pixel Value Differencing
2	Bahasa Pemrograman	C
3	Versi Perangkat	-
Penelitian yang diajukan: Perancangan Aplikasi Steganografi dengan Algoritma Caesar Cipher dan Pixel Value Differencing		
1	Metode	Pixel Value Differencing dan Caesar Cipher
2	Bahasa Pemrograman	Borland Delphi
3	Versi Perangkat	7

I.6. Sistematika Penulisan

Penulisan skripsi ini disusun secara sistematika untuk memudahkan mahasiswa dalam penyusunan skripsi. Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan membahas tentang latar belakang masalah, ruang lingkup permasalahan, tujuan dan manfaat penelitian, metode penelitian dan sistematika penulisan yang digunakan untuk menyusun laporan skripsi.

BAB II LANDASAN TEORI

Pada bab ini akan membahas tentang dasar teori mengenai kriptografi, algoritma kriptografi yang digunakan serta cara kerja enkripsi.

BAB III ANALISIS DAN DESAIN SISTEM

Bab ini akan membahas tentang analisa masalah, strategi pemecahan masalah, analisis kebutuhan aplikasi sistem keamanan, perancangan sistem dan aplikasi, *flowchart*.

BAB IV HASIL DAN UJI COBA

Bab ini akan membahas tentang hasil rancangan sistem enkripsi dan penyisipan pesan, ekstraksi pesan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan yang diperoleh dari hasil penelitian dan saran untuk menyempurnakan penelitian ini.