

BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi saat ini sudah berkembang begitu pesat. Akan tetapi, perkembangan teknologi tersebut tidak sebanding dengan tingkat keamanan pada suatu data. Oleh karena itu, sejalan dengan berkembangnya teknologi informasi juga harus dibarengi dengan perkembangan keamanan pada suatu data. Khususnya kasus yang dialami oleh Elfa Furniture dalam penyimpanan file yang bersifat rahasia. Elfa Furniture merupakan salah satu perusahaan penyedia jasa yang bergerak di bidang kontraktor, *furniture* dan *design interior*, perusahaan tersebut belum mempunyai system yang dapat mengamankan file secara efisien. File-file tersebut mempunyai beberapa poin penting yang harus dijaga kerahasiaannya, yaitu perjanjian kerja sama kepada *client* yang berisi kontrak kerja serta penawaran harga. Menurut perusahaan, poin-poin tersebut bersifat rahasia, karena hanya pihak tertentu pada perusahaan dan *client* saja yang mengetahui isi dari file tersebut. Oleh karena itu, dibutuhkannya suatu system yang dapat mengamankan file tersebut agar tidak dapat disalahgunakan oleh pihak yang tidak memiliki hak akses untuk mengakses file tersebut. Dengan demikian, untuk mengatasi hal di atas, dapat dilakukan dengan mengenkripsi file tersebut menggunakan algoritma kriptografi.

Kriptografi adalah ilmu yang digunakan untuk mengamankan pesan yang bersifat rahasia. Cara kerja kriptografi adalah dengan menyandikan isi dari file, penyandian file tersebut melalui proses enkripsi yaitu mengubah file asli menjadi bentuk tersandi yang tidak bermakna. Pada penelitian ini penulis memilih algoritma kriptografi twofish, karena algoritma ini merupakan salah satu kandidat AES (*Advanced Encryption Standard*) yang memenuhi kriteria yang dibutuhkan NIST (*National Institute of Standards and Technology*) yaitu membuat algoritma yang efisien. Penelitian yang dilakukan oleh Izzat Shulhan (2018), menjelaskan bahwa algoritma twofish memiliki keunggulan dari segi ketahanan, hal ini dikarenakan algoritma ini membutuhkan proses yang lebih lama untuk memecahkannya.

Dini Nursafitri, 2021

PENERAPAN STEGANOGRAFI DENGAN METODE LSB (LEAST SIGNIFICANT BIT) DAN ALGORITMA KRIPTOGRAFI TWOFISH UNTUK PENGAMANAN FILE

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Program Studi Informatika
[www.upnvj.ac.id – www.library.upnvj.ac.id – www.repository.upnvj.ac.id]

Selain menggunakan kriptografi, teknik lain yang dapat digunakan untuk menjaga rahasia dari suatu file adalah teknik steganografi. Steganografi merupakan ilmu yang digunakan untuk menyembunyikan pesan ke dalam suatu media lain sebagai *cover* sehingga terlihat menjadi samar. Dengan steganografi maka file yang disembunyikan ke dalam suatu media tersebut tidak menarik perhatian serta tidak menimbulkan kecurigaan oleh pihak lain. Media *cover* yang dapat digunakan sebagai media penampung berupa media gambar, audio atau video. Akan tetapi, dalam proses penyisipan tersebut dapat memengaruhi kualitas media cover. Oleh karena itu, hal yang dilakukan untuk mengurangi terjadinya perubahan kualitas pada media penampung adalah dengan metode penyisipan bit terakhir atau LSB (*Least Significant Bit*). Pada penelitian yang dilakukan oleh Pandapotan dan Taronisokhi (2016), menjelaskan bahwa dengan metode LSB citra yang dihasilkan setelah dilakukan penyisipan pesan hanya mengalami sedikit penurunan kualitas yang tidak berpengaruh secara signifikan oleh indera penglihatan manusia.

Berdasarkan uraian diatas, maka penulis ingin membuat sebuah aplikasi untuk keamanan file dengan menerapkan steganografi menggunakan metode LSB dan algoritma kriptografi twofish agar keamanan yang dihasilkan menjadi lebih baik.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka penulis merumuskan perumusan masalah sebagai berikut:

- a. Bagaimana membantu mengamankan file penawaran harga pada perusahaan Elfa Furniture?
- b. Bagaimana waktu yang dibutuhkan untuk melakukan proses penyisipan dan ekstrasi pada metode LSB dalam mengamankan file penawaran harga?

I.3 Ruang Lingkup

Penulis memfokuskan penelitian ini dibatasi oleh ruang lingkup pembahasan agar dalam penulisan penelitian ini lebih terarah, berikut ini ruang lingkup pembahasannya yaitu:

Dini Nursafitri, 2021

PENERAPAN STEGANOGRAFI DENGAN METODE LSB (LEAST SIGNIFICANT BIT) DAN ALGORITMA KRIPTOGRAFI TWOFISH UNTUK PENGAMANAN FILE

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Program Studi Informatika.

[www.upnvj.ac.id – www.library.upnvj.ac.id – www.repository.upnvj.ac.id]

- a. Data yang digunakan pada proses penyisipan pesan berupa file dengan format pdf.
- b. Data yang digunakan sebagai media cover berupa gambar dengan format jpeg.
- c. Menyembunyikan suatu file yang telah dienkripsi dengan menyisipkan file tersebut ke dalam sebuah gambar menggunakan metode LSB.
- d. Proses enkripsi dan dekripsi pada file yang dilakukan menggunakan algoritma kriptografi twofish.

I.4 Tujuan Penelitian

Berdasarkan latar belakang, perumusan masalah dan ruang lingkup yang telah diberikan, maka tujuan penelitian dari penelitian ini yaitu sebagai berikut:

- a. Mengamankan file penawaran harga yang disimpan oleh pihak perusahaan.
- b. Mencegah pihak yang tidak bersangkutan mengetahui isi dari file tersebut.

I.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini yaitu sebagai berikut:

- a. Dapat menjadi alternative untuk mengamankan file penawaran harga yang disimpan oleh pihak perusahaan.
- b. Dapat dijadikan sebagai bahan referensi terhadap penelitian mengenai kriptografi menggunakan algoritma twofish.

I.6 Luaran yang Diharapkan

Luaran yang diharapkan dalam penelitian ini adalah menghasilkan sebuah system pengaman file untuk menjaga isi dari file tersebut dengan penerapan algoritma kriptografi twofish dan teknik steganografi, hal ini bertujuan untuk membantu perusahaan dalam mengamankan file yang disimpan yang bersifat rahasia dari pihak yang tidak berhak untuk mengetahuinya.

I.7 Sistematika Penulisan

Dini Nursafitri, 2021

PENERAPAN STEGANOGRAFI DENGAN METODE LSB (LEAST SIGNIFICANT BIT) DAN ALGORITMA KRIPTOGRAFI TWOFISH UNTUK PENGAMANAN FILE

UPN Veteran Jakarta, Fakultas Ilmu Komputer, Program Studi Informatika.

[www.upnvj.ac.id – www.library.upnvj.ac.id – www.repository.upnvj.ac.id]

Sistematika penulisan tugas akhir ini dibagi menjadi beberapa bab dan setiap bab terdiri dari beberapa sub bab. Adapun sistematika penulisannya sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi penjelasan mengenai Latar Belakang, Perumusan Masalah, Ruang Lingkup, Tujuan Penelitian, Manfaat Penelitian, Luaran yang Diharapkan, dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Bab ini berisi uraian mengenai berbagai macam literatur yang berkaitan dengan teori, konsep serta proses yang digunakan sebagai referensi dalam penulisan tugas akhir. Selain itu, dalam bab ini juga terdapat riset atau penelitian terdahulu yang sudah pernah dilakukan sebelumnya yang sejenis dengan topik penelitian yang akan dibahas.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan mengenai metodologi yang digunakan dalam penelitian ini yang menguraikan langkah-langkah dalam melakukan penelitian mulai dari identifikasi masalah hingga langkah penyusunan tugas akhir.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan mengenai implementasi system aplikasi seperti uji coba pada aplikasi dan penerapan serta hasil analisis pengamanan pada file dalam aplikasi yang telah dibangun.

BAB V PENUTUP

Bab ini merupakan bagian penutup yang berisi mengenai hasil kesimpulan dari pembahasan pembuatan tugas akhir dan aplikasi serta saran untuk proses pengembangan selanjutnya.

DAFTAR PUSTAKA

LAMPIRAN