MENINGKATKAN KEAMANAN DATA MENGGUNAKAN METODE STEGANOGRAFI LSB DAN KRIPTOGRAFI DES PADA CITRA DIGITAL

Restu Maulunida*, Dhimas Widrayato†, dan Memed Sumaedi‡
Fakultas Teknologi Informasi
Universitas Budi Luhur
Jakarta, Indonesia
Email: *vandalz12@gmail.com, †dhimas.buing@gmail.com, ‡memedsumaedi@gmail.com

Abstract—This paper discusses safety data using steganography and cryptography. Advances in information technology have a positive impact to help complete the work and exchange of information very quickly, where one can perform mutual communication and exchange of information in just seconds. Unfortunately, the exchange of information that occurs over the Internet does not guarantee the security of that information. If there is a third party manages to get such information when data exchange is running this can be damaging to the parties concerned; as it is highly confidential information. The information is encrypted using the DES algorithm, and then it will be hidden into an image. Therefore, the confidential information will be difficult to disclose. As conclusion, an application of steganography and cryptography can improve the security of information when any communications take place.

Index Terms—Steganografi, Kriptografi, DES, LSB

1 Pendahuluan

Internet mengijinkan seseorang untuk melakukan komunikasi dan pertukaran informasi dengan orang lain walaupun jarak lokasi antara mereka sangat jauh. Pekerjaan ini dapat dilakukan dengan sangat cepat dan juga lebih murah. Dimana tidak seperti metode konvensional sebelum adanya teknologi informasi, seseorang harus mengirim pesan secara manual kepada tujuannya.

Bagaimanapun, pertukaran informasi melalui internet memiliki masalah dalam keamanan. Permasalahan terjadi ketika informasi sedang dikirim ke tujuan, dikarenakan informasi tersebut dikirim dalam bentuk teks asli, yang berarti dapat dibaca oleh orang lain. Jika informasi tersebut sangat penting dan rahasia seperti strategi bisnis suatu perusahaan, jika terdapat pihak ketiga dengan niat jahat dan berhasil mendapatkan informasi tersebut, maka akan merugikan pihak yang bersangkutan.

Penelitian ini mengajukan keamanan data dengan menggunakan metode steganografi LSB dan kriptografi DES. Dimana suatu data sebelum dikirim ke tujuan akan di enkripsi terlebih dahulu, kemudian hasil enkripsi data akan disembunyikan ke dalam media gambar. Melalui penerapan ini, dapat menjamin tingkat keamanan data menjadi dua tingkat, jika pihak ketiga mengetahui suatu pesan yang disembunyikan pada media gambar dan berhasil mendapatkannya, maka dia harus melakukan enkripsi terlebih dahulu dengan kunci yang sesuai sebelum dapat mengetahui isi dari informasi yang dikirim.

2 Penelitian Terkait

Keamanan data merupakan salah satu aspek terpenting dari sebuah komunikasi untuk berbagi suatu informasi. Keamanan sering terletak pada kerahasiaan keberadaannya dan/atau kerahasiaan bagaimana untuk memecahkan kode itu. Teknik kriptografi sering digunakan untuk mengamankan suatu data, tetapi teknik ini hanya memenuhi satu dari dua kondisi dalam keamanan data. Banyak metode telah dikembangkan untuk enkripsi dan dekripsi data dengan tujuan untuk mengamankan data. Tetapi, itu tidak cukup untuk menjaga data tetap aman, mungkin juga diperlukan untuk menjaga kerahasiaan keberadaan dari suatu data. Teknik yang digunakan untuk mengimplementasikan ini disebut dengan steganografi [1].

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut teminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain [2]. Dengan penerapan kirptografi data yang akan dikirim akan diacak terlebih dahulu sehingga menjadi sulit untuk diterjemahkan makna dari pesan tersebut.

Patel et al. [3] mendisain teknik steganografi berdasarkan koefisien DCT, jika koefisien DCT berada dibawah nilai yang sudah ditentukan, LSB dari media gambar akan digantikan dengan MSB dari data. Gupta et al. [4] mendisain teknik steganografi hanya menggunakan metode LSB pada media gambar. Singla et al. [5]

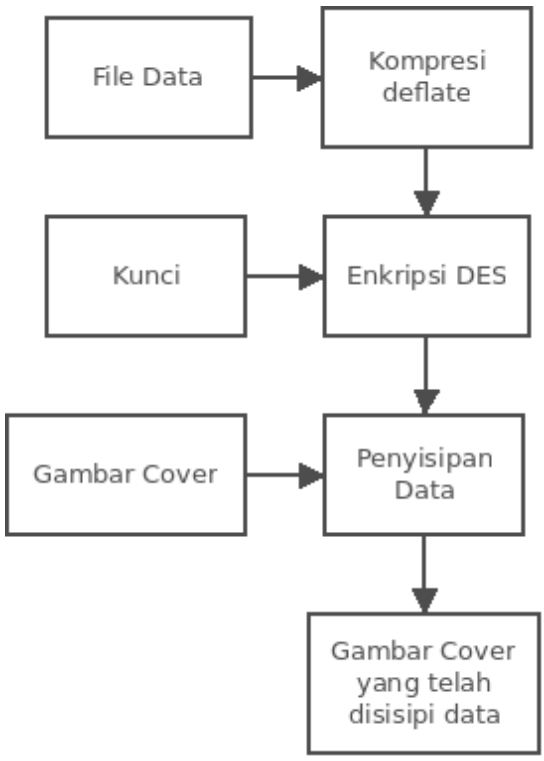
mendisain teknik steganografi menggunakan LSB dan DCT untuk menyembunyikan data dan sebelum data tersebut disembunyikan, data tersebut dienkripsi terlebih dahulu menggunakan algoritma RSA.

Kami mengajukan keamanan data menggunakan kriptografi DES dan metode steganografi LSB pada gambar. DES merupakan suatu sistem kriptografi simetri dan tergolong jenis blok kode, DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plaintext menjadi 64 bit chipertext dengan menggunakan 56 bit kunci internal, kemudian chipertext tersebut disembunyikan ke dalam media gambar.

Tujuan penelitian ini ditujukan untuk membantu menyelesaikan masalah pada keamanan data. Terdapat dua tujuan utama dalam penelitian ini: Tujuan pertama adalah untuk mendesain dan mengembangkan algoritma untuk mengamankan data. Tujuan kedua adalah menerapkan algoritma DES untuk enkripsi dan metode LSB untuk menyembunyikan data pada media gambar.

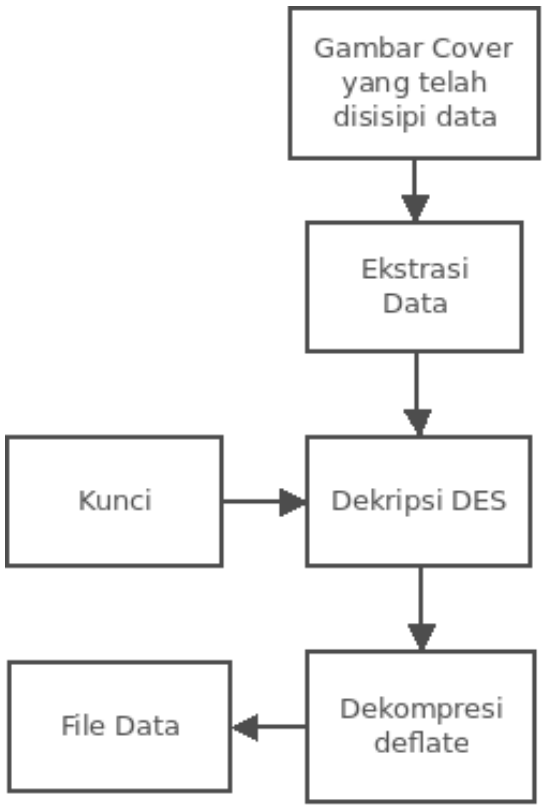
3 METODOLOGI

Proses menyembunyikan data pada media gambar yang diusulkan terdiri dari dua tahap: (1) data dienkripsi menggunakan algoritma DES sebelum data disembunyikan pada media gambar. (2) setelah data didapatkan chipertext dari hasil enkripsi menggunakan algoritma DES, chipertext disembunyikan ke dalam media gambar menggunakan metode LSB, dua bit LSB pada masing-masing channel RGB pada pixel gambar akan digantikan dengan dua bit pada chipertext, hasil gambar yang sudah disisipi oleh data disebut dengan stego image. Proses menyembunyikan ini disebut dengan proses embedding. Gambar 1 menunjukkan proses embedding data ke dalam media gambar.



Gambar. 1. Proses Embedding

Untuk mendapatkan data yang terdapat dalam stego image terdiri dari dua tahap: (1) membaca dua bit dari masing-masing channel RGB pada pixel stego image. (2) melakukan proses dekripsi dengan menggunakan algoritma DES terhadap data yang dibaca dari stego image. Proses mendapatkan kembali data dari stego image disebut dengan extracting. Gambar 2 menunjukkan proses extracting data dari stego image.



Gambar. 2. Proses Extracting

3.1 Kompresi deflate

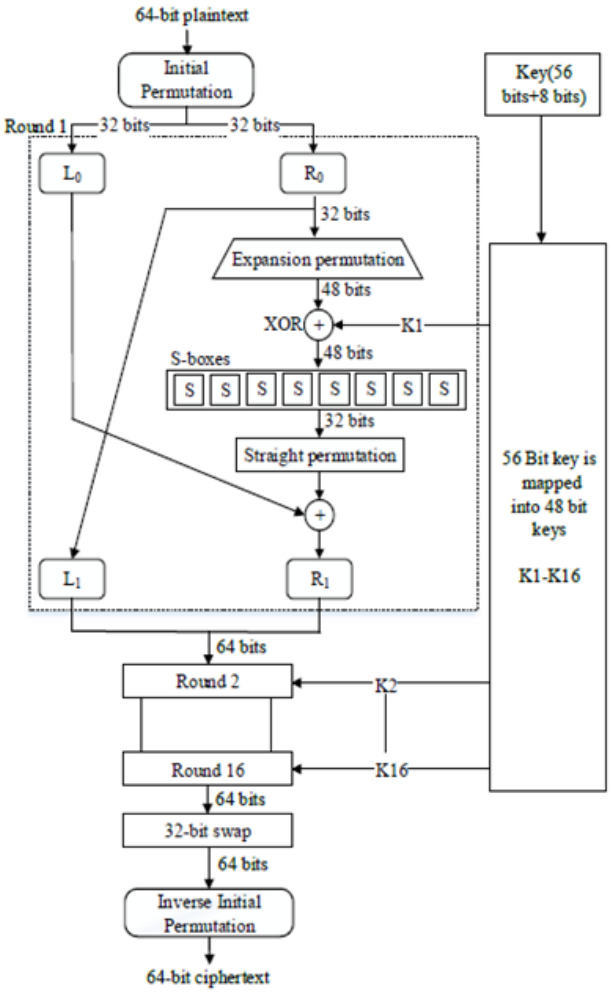
Metode kompresi Deflate merupakan kombinasi dari variant LZ77 dan metode Huffman. Adapun tahap kompresi Deflate dimulai dengan melakukan eliminasi karakter string kembar (implementasi algoritma kompresi LZ77) yang dilakukan dari hasil pembacaan tiap block yang diproses. Apabila pada awal block tidak ditemukan pola maka akan mengaktifkan mode 1 pada block tersebut, yakni mode tidak dikompresi. Ketika ditemukan pola karakter kembar maka dituliskan sebuah referensi berisi panjang sekuen dan jaraknya dari awal block. Kemungkinan panjang block adalah 2-258 Bytes dan kemungkinan jarak sliding windownya adalah 1-32768 Bytes.

Tahap berikutnya adalah penggunaan pohon Huffman, yaitu mengganti setiap data yang sering muncul dengan simbol tertentu yang memiliki bit yang lebih pendek. Mode kedua menggunakan pohon Static Huffman yang artinya karakter yang dibutuhkan untuk melakukan dekompresi file tidak disertakan dalam file terkompresi. Mode ketiga adalah menggunakan Dynamic Huffman Compression, yang artinya harus mendapatkan seluruh karakter

yang akan dilakukan untuk melakukan kompresi terhadap block. Karakter tersebut disimpan setelah data, dan sifat karakter encode ini adalah fixed. Penggolongan karakter encode Dynamic Huffman Compression dapat dilihat pada RFC 1951. Nantinya akan didapatkan hasil tiap block kompresi yang merupakan hasil teks terkompresi.

3.2 Algoritma DES

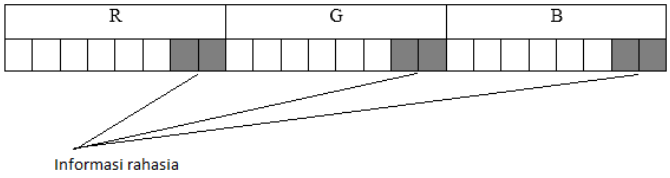
DES adalah salah satu algoritma enkripsi yang paling banyak digunakan, sistem kriptografi yang tersedia untuk umum, yang diadopsi oleh NIST (National Institute of Standards and Technology) sebagai standar pengolahan informasi federal AS. Secara umum standar enkripsi data terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi 64 bit dan dekripsi data 64 bit yang mana satu kelompok saling berinteraksi satu sama lain[6][7]. Proses algoritma enkripsi DES ditunjukkan pada gambar 3. Proses algoritma diawali dengan initial permutation, enam belas iterasi block chiper dan final permutation.



Gambar. 3. Algoritma Enkripsi DES

3.3 Metode LSB

Metode LSB (Least Significant Bit) merupakan teknik substitusi pada steganografi, biasanya arsip 24 bit atau 8 bit digunakan untuk menyimpan citra digital. Representasi warna dari pixel-pixel bisa diperoleh dari warna-warna primer, yaitu merah, hijau, dan biru. Citra 24 bit menggunakan 3 bytes untuk masing-masing pixel, di mana setiap warna primer direpresentasikan dengan ukuran 1 byte. Penggunaan citra 24 bit memungkinkan setiap pixel direpresentasikan dengan nilai warna sebanyak 16.777.216 macam. Dua bit dari saluran warna tersebut bisa digunakan untuk menyembunyikan data. Pada penelitian ini dua bit terakhir pada channel RGB pada masing-masing pixel diganti dengan dua bit pada data. Skema proses penggantian bit pada channel RGB ditunjukkan pada gambar 4.



Gambar. 4. Skema Proses Penyisipan Bit

4 Implementasi

Terdapat dua proses utama dalam suatu sistem steganografi, yaitu proses embedding dan extracting. Data yang akan disisipi ke dalam media gambar adalah berupa file, sehingga memungkinkan untuk menyembunyikan suatu dokumen ke dalam suatu gambar, sehingga membuat aplikasi ini menjadi lebih fleksibel karena data tidak dibatasi oleh apapun. Proses embedding dan extracting seperti pada langkah-langkah berikut.

4.1 Embedding

Embedding merupakan proses penyisipan data ke dalam suatu media digital dalam penelitian ini berupa gambar, berikut adalah langkah-langkah penyisipan data yang digunakan pada penelitian ini.

1) Membaca bytes data pada file yang akan disembunyikan pada media gambar.
2) Melakukan Enkripsi pada bytes data dan menghasilkan chipertext.
3) Membaca chipertext dan menyisipkan dua bit chipertext ke dalam masing-masing channel RGB pada media gambar.
4) Menghasilkan Stego Image.

4.2 Extracting

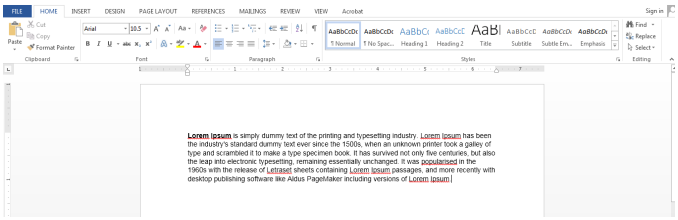
Extracting merupakan proses mengembalikan data dari stego image, dibawah adalah langkah-langkah extracting data yang digunakan pada penelitian ini.

1) Membaca nilai pixel dari stego image.
2) Membaca dua bit terakhir dari masing-maing channel RGB pada stego image.
3) Melakukan Dekripsi terhadap data yang dibaca dari stego image.
4) Menghasilkan file data.

4.3 Hasil Percobaan

Penelitian ini telah dilakukan dengan menggunakan bahasa pemrograman java. Pada percobaan ini data yang akan disisipi kedalam media gambar berupa file document microsoft word. Gambar 5 merupakan media gambar sebelum disisipi oleh data. Gambar 6 merupakan data yang akan disisipi kedalam media gambar. Gambar 7 merupakan media gambar yang telah disisipi oleh file document microsoft word. Proses extracting adalah proses untuk mendapatkan

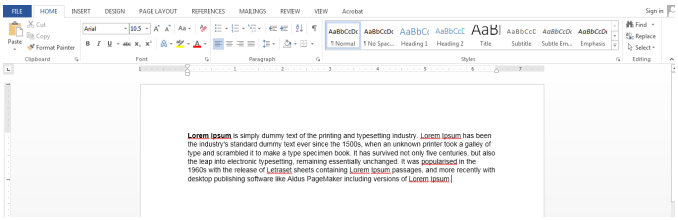
Gambar. 5. Media Gambar Sebelum Disisipi File



Gambar. 6. File Data Untuk Proses Embedding

Gambar. 7. Media Gambar Setelah Disisipi File

data yang telah disembunyikan ke dalam media gambar. Data telah berhasil didapatkan kembali dari stego image yang ditunjukkan pada gambar 7. Hasil data dari proses extracting ditunjukkan pada gambar 8.



Gambar. 8. File Data Hasil Proses Extracting

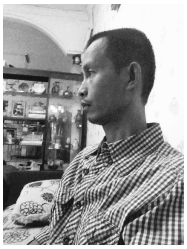
5 KESIMPULAN

Keamanan data dapat dilakukan dengan menggunakan teknik kriptografi dan steganografi. Dimana kriptografi berfungsi untuk mengacak suatu data menjadi sesuatu yang tidak dapat dibaca secara jelas tidak memiliki makna. Sedangkan steganografi berfungsi untuk menyembunyikan data kedalam suatu media digital dalam penelitian ini adalah gambar sehingga data tersebut tidak terlihat secara kasat mata. Dengan penggabungan kedua teknik ini data akan menjadi lebih sulit untuk dipecahkan, dikarenakan sebelum proses penyisipan informasi, dilakukan proses enkripsi terlebih dahulu terhadap informasi tersebut. Sehingga jika data dalam media gambar berhasil didapatkan maka data tersebut tidak langsung dapat digunakan, dikarenakan dalam kondisi terenkripsi. Pada penelitian gambar hasil output menggunakan metode lossless, file gambar yang dihasilkan berupa format png. Untuk penelitian selanjutnya dapat menggunakan teknik kompresi pada gambar, sehingga ukuran file gambar yang akan dihasilkan menjadi lebih kecil.

DAFTAR PUSTAKA

[1] D. Ariyus, *Kemanan Multimedia*. Yogyakarta, Indonesia: C.V ANDI OFFSET, 2009.
[2] A. Dony, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Yogyakarta, Indonesia: C.V ANDI OFFSET, 2008.
[3] H. Patel and P. Dave, *Steganography Technique Based on DCT Coefficients*. IJERA, Vol. 2, no. 1, 713-717, 2012.
[4] S. Gupta, G. Gujrat, and N. Aggarwal, *Enhanced Least Significant Bit algorithm For Image Steganography*. IJCEM, Vol. 15, no. 2, 2230-7893, 2012.
[5] D. Singla and R. Syal, *Data Security Using LSB & DCT Steganography In Images*. IJCER, Vol. 2, no. 2, 359-364, 2012.
[6] J. O. Grabbe, *The DES Algorithm Illustrated*. 2016. http://page.math.tu-berlin.de/ kant/teaching/hess/krypto-ws2006/des.htm. (Tanggal Akses 23/11/2016)
[7] G. Singh and Supriya, *A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security*. IJCA, Vol. 67, no. 9, 0975-8887, 2013.

Restu Maulunida lahir di Tangerang, Indonesia. Tahun 1989. Dia menyelesaikan pendidikan S1 Teknologi Informasi di Universitas Budi Luhur. Saat ini dia bekerja sebagai programmer di Jakarta.



Memed Sumaedi lahir di Tangerang, Indonesia pada tahun 1973. Menyelesaikan pendidikan S1 Mananjemen Infomatika di Universitas Bina Nusantara, Jakarta. Saat ini sedang melanjutkan studi di Universitas Budi Luhut.

Dhimas Widrayato lahir di Madiun, Indonesia pada 1990. Menyelesaikan pendidikan S1 Sistem Informasi di STMIK Insan Pembangunan dan sedang melanjutkan studi di Universitas Budi Luhur.