Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)
Vol.1, No.2, December 2018, pp. 65~74
ISSN (print): 2655-2183, ISSN (online): 2655-7290
DOI: https://doi.org/10.33173/jsikti.16

Sistem Keamanan Data Text dengan Data Encryption Standard (DES) dan Metode Least Significant Bit (LSB)

Indra Pratistha*[1], Paholo Iman Prakoso[2]
[1]Prodi S2 Ilkom, Departemen Ilmu Komputer dan Elektronika, FMIPA UGM, Yogyakarta
[2]Information Technology, Computer and Sciences Association (INFOTEKS), Indonesia
e-mail: *[1]**indra.pratista@mail.ugm.ac.id**, [2]info@infoteks.org

Abstrak

Informasi dapat dikirimkan dengan cepat tanpa mengenal batas-batas geografis mengguanakan media internet. Namum demikian, informasi yang dikirimkan dapat disadap ditengah jalan oleh pihak yang tidak diinginkan, maka keamanan data benar-benar menjadi permasalahan yang sangat penting. Perkembangan sistem Komputer dan dan interkoneksinya melalui jaringan internet telah meningkat, tentu saja membutuhkan keamanan data dan message yang handal agar terhindar dari serangan. Untuk mengamankan data atau message dijaringan internet diperlukan kriptografi dengan metode enkripsi, salah satunya metode enkripsi data yang ada adalah metode data encryption standard (DES) dan selanjutnya disisipkan ke sebauh citra digital (steganografi) menggunakan metode least significant bit (LSB).

Kata kunci*— Kriptografi, Steganografi, Encryption*

Abstract

Current information can be delivered quickly without knowing the geographical boundaries using the internet. However, the information transmitted can be intercepted by the middle of the road which is not desired, then the security of the data actually becomes a very important issue. The development of computer systems and networks and the interconnection through the Internet has increased, of course, require data security and reliable message in order to avoid the attack. To secure internet data or message network necessary cryptographic encryption methods, one method of data encryption that there is a method of data encryption standard (DES) and subsequently inserted into the Lakeside digital images (steganography) using the method of least significant bit (LSB).

Keywords— *cryptographic, steganography, encryption*

1. PENDAHULUAN

Saat ini informasi dapat dikirimkan dengan cepat tanpa mengenal batas-batas geografis mengguanakan media internet. Namum demikian, informasi yang dikirimkan dapat disadap ditengah jalan oleh pihak yang tidak diinginkan. Ada banyak teknik untuk mencegat informasi yang dikirimkan melalui jaringan publik seperti Internet. Hal ini sangat berbahaya, bila informasi yang dikirimkan tersebut dinilai sensitif, seperti rahasia negara atau perusahaan.

Masalah keamanan dan kerahasian merupakan salah satu aspek penting dari suatau data, pesan dan informasi lainnya, perpindahan data atau informasi yang sangat penting membutuhkan tingkat keamanan yang tinggi, dengan perkembangan teknologi informasi

Received December 5th,2018; Revised December 15th, 2018; Accepted December 30th, 2018

sekarang ini yang sangat pesat, dimana setiap orang akan mudah untuk mendapakan suatau data dan informasi[1], [2]. Berbagai cara dilakukan orang untuk mendapakan data dan informasi tersebut, mulai dari tingkatan yang paling mudah sampai cara-cara yang lebih rumit, dan berbagai cara pula orang berusaha untuk melindungi pesan data ataupun informasi tersebut agar tidak dapat diketahui oleh orang yang tidak memiliki hak atas data dan informasi tersebut. Seiring dengan kemajuan teknologi informasi,Teknik kejahatan dunia maya juga meningkat. Ada beberapa bentuk serangan terhadap data dan informasi, seperti peretas, cracker, Trojans, dll[2], [3]. Edisi laporan Symantec Intelligence [4] mengindikasikan bahwa penyerang memilih target serangan. Teknik yang paling umum digunakan untuk keamanan dalam pengiriman data adalah enkripsi simetris [5][6]. Inti dari keamanan data adalah bagian penting dari proses enkripsi dan menyediakan lalu lintas data yang aman di antara pengirim dan penerima [7]. Untuk masyarakat modern, keamanan dan kelengkapan data sangat penting [8][9].

Untuk mencegah jatuhnya informasi penting ke tangan yang salah, maka digunakanlah teknik kriptografi, yaitu proses mengubah (*encrypt*) suatu informasi (*plaintext*) dengan suatu algoritma khusus (*cipher*) dengan tujuan agar informasi tersebut tidak dapat dibaca (*decrypt*) tanpa bantuan kunci (key) khusus[10]. Teknik enkripsi memiliki beberapa kelemahan, salah satunya yaitu mengundang perhatian. Algoritma enkripsi diklasifikasikan menjadi dua jenis; algoritma simetris tempat kunci digunakan oleh semua pengguna dan algoritma asimetris di mana ada kunci pribadi yang dimiliki oleh salah satu sistem pengguna. Standar Pemrosesan Informasi Federal memberikan deskripsi lengkap untuk standar enkripsi data (DES) pada tahun 1977 [11]. DES adalah cipher blok 64 bit yang artinya mengenkripsi data 64 bit pada a waktu [12]. Implementasi yang diusulkan mewakili satu tahap dari algoritma DES yang dikembangkan dengan penggunaan xor operan. Putaran DES terdiri dari teknik enkripsi tradisional yang dikenal sebagai substitusi diikuti oleh tahap transposisi. Data Encryption Standard (DES) adalah algoritma kunci simetris modern dan paling populer pertama yang digunakan untuk enkripsi dan dekripsi data digital [13].

Citra digital adalah citra yang dapat diolah oleh komputer, citra digital dapat juga diilustrasikan dengan sebuah gambar. Gambar ini memiliki bagian-bagian yang biasanya disebut dengan piksel [14]. Piksel adalah elemen terkecil dari sebuah citra, piksel dalam hal ini adalah sebuah titik digital yang merupakan elemen dari sebuah image, baik itu dari layar komputer maupun pada hasil cetakkannya [14], [15]. Setiap piksel memiliki bagian-bagian yang dapat diubah atau dimanipulasi. Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima tidak ada pihak lain yang mengetahuinya. Berbeda dengan enkripsi, steganografi tidak mengundang kecurigaan karena pesan rahasia disembunyikan dalam file yang normal seperti citra digital.

Dari lantar belakang permasalahan, maka akan dibuat sebuah aplikasi untuk menyembunyikan data text ke dalam citra digital (steganografi) menggunakan metode *Least Significant Bit* (LSB) dan *Data Encyption Standard* (DES).

.

2. METODE PENELITIAN

2.1 State Of The Arts

Penulisan pada jurnal "Kombinasi Kriptografi dengan Hillcipher dan Steaganografi dengan LSB untuk Keamanan Data Text karya Esti Suryanti dan Titin Sri Martini program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Magelang . Dimana membahas tentang keamanan data text yang sangat penting, perkembangan sistem komputer dan interkoneksinya melalui jaringan internet telah meningkat, tentu saja hal in membutuhkan keamanan data dan message yang sangat handal agar terhindar dari serangan (attack). Untuk merahasiakan pesan yang dikirim, yang dapat dilakukan dengan proses kriptografi, serta

sekaligus menghindarkan pesan tersebut dari kecurigaan, yang dapat dilakukan dengan proses steganografi.

Pesan yang digunakan dalam jurnal tersebut berupa text. Pada proses kriptografi, pesan yang berupa text tersebut akan dienkrip dengan metode Hillcipher, dan selanjutnya pesan yang telah terenkripsi tersebut akan dilakukan proses steaganografi pada citra digital grayscale 8 bit dengan skala 0-255, dengan metode *Least Significant Bit* (LSB)

Perbandingan dengan penelitian ini adalah jika dalam jurnal berjudul "Kombinasi Kriptografi dengan Hillciher dan Steaganografi dengan LSB untuk Keamanan Data Text karya Esti Suryanti dan Titin Sri Martini. Merupakan implementasi penyenbunyian data rahasia menggunkan metode HillChiper, dimana data tersebut di enkripsi, sedangkan dalam penelitian ini merupakan perancangan metode DES dan selanjutnya di sembunyikan pada sebuah citra atau gambar menggunkan metode LSB.

Dari jurnal yang berjudul "Penyenbunyian Pesan pada Citra Terkompresi JPEG menggunkan Metode Spread Spectrum" karya Winda Winanti Jurusan Teknik Informatika". Dimana dalam jurnal ini membahas keamanan dalam pengiriman informasi yang bersifat rahasia, pada makalah ini dilakukan studi mengenai bagaimana steganografi pada media citra digital, dimna citra digital yang digunakan adalah citra terkompresi dengan format file JPEG, dengan menggunakan metode Spread Spectrum.

Perbandingan dengan penelitian ini adalah jika dalam jurnal yang berjudul "Penyenbunyian Pesan pada Citra Terkompresi JPEG menggunkan Metode Spread Spectrum" karya Winda Winanti Jurusan Teknik Informatika". Dimana membahas keamanan dengan menyisipkan data rahasia ke dalam sebuah citra digital, tanpa merubah (enkripsi) data tersebut, sedangankan penelitian dimna data rahasia tersebut di ekripsi terlebih dahulu sebelum disisipkan ke dalam sebuah citra digital.

2. 2 Kriptografi (cryptography)

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu "kriptos" dan "graphia". Arti kata "kriptos" artinya sesuatu yang disembunyikan, tidak dikenal, terselubung, rahasia atau misterius. Sedangkan "graphia" artinya tulisan. Jadi, kriptografi dapat dijelaskan secara harfiah sebagai tulisan rahasia atau terkadang disebut sebagai seni dan ilmu tulisan rahasia [16]. Menurut buku yang berjudul "*Applied Cryptography*" karangan Bruce Schneider [17], kriptografi merupakan seni atau ilmu untuk menjaga keraasiaan dari sebuah tulisan agar tetap aman, tanpa diketahui pihak yang tidak berkepentingan. Pakar ilmu kriptografi dikenal sebagi kriptografer[16], [18]. Selain kriptografi, ada kripnalisis yang merupakan kebalikan dari proses kriptografi dalam kriptologi. Kriptologi ini termasuk salah satu cabang ilmu algoritma di bidang matematika. Para pelaku kriptologi dikenal sebagai kriptologis. Pada kripnalisis, penganalisa dan pemecah kode chipertext menjadi plaintext tanpa melalui proses dekripsi yang wajar disebut kripnalisis. Algoritma kriptografi dan seluruh kemungkinan *chippertext*, *plaintext*, dan key (kunci-kunci lainya) disebut kriptosistem. Plaintext adalah pesan/data asli yang dapat dibaca. Chippertext adalah pesan/data yang acak, yang sulit diartikan. key adalah nilai yang digunakan mengubah chippertext menjadi plaintext.

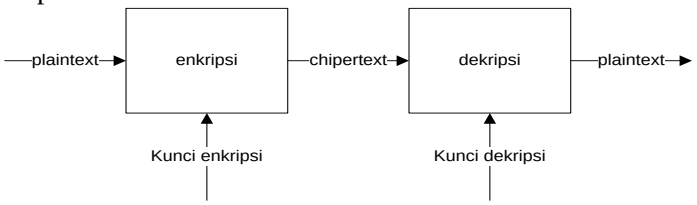
Dalam ilmu kriptografi terdapat aspek-aspek keamanan meliputi :

1. *Confidelity* (Kerahasiaan) adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun keculai yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.
2. *Data integrity* (Integritas data) adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, system harus memiliki kemampuan untuk mendeteksi manipulasi oleh pihak-pihak yang tidak berhak, antara lain penyisipan, pengapusan, dan pensubsitusian data lain ke dalam data sebenarnya.
3. *Authentication* (Keontentikan) adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan system maupun informasi itu sendiri. Dua pihak yang

saling beromunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentifikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

4. *Non-repudiation* (anti-penyangkalan) adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan, atau harus dapat membuktikan bahwa suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim informasi tersebut.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah plaintext menjadi chipertext (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti. Seperti pada Gambar 1.



Gambar 1. Diagram proses enkripsi dan dekripsi

2. 3 Data Encryption Standar (DES)

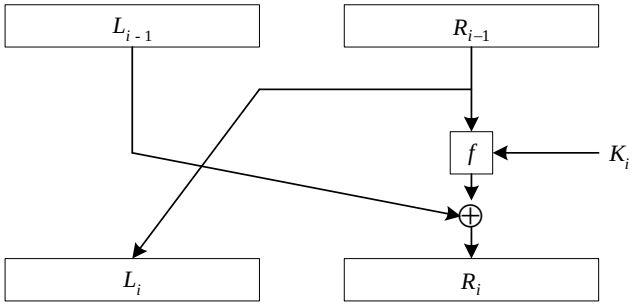
DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau upa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.Skema global dari algoritma DES adalah sebagai berikut [19]:

1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).
2. Hasil permutasi awal kemudian di-enciphering- sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipherteks.

Di dalam proses enciphering, blok plainteks terbagi menjadi dua bagian, kiri (L) dan kanan (R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi yang disebut f. Pada fungsi f, blok R dikombinasikan dengan kunci internal Ki. Keluaran dai fungsi f di-XOR-kan dengan blok L untuk mendapatkan blok R yang baru. Sedangkan blok L yang baru langsung diambil dari blok R sebelumnya. Ini adalah satu putaran DES. Secara matematis, satu putaran DES dinyatakan seperti Rumus 1

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i \quad (1)$$

Gambar 2 menunjukan skema algoritma DES, dalam jaringan *feistel*.

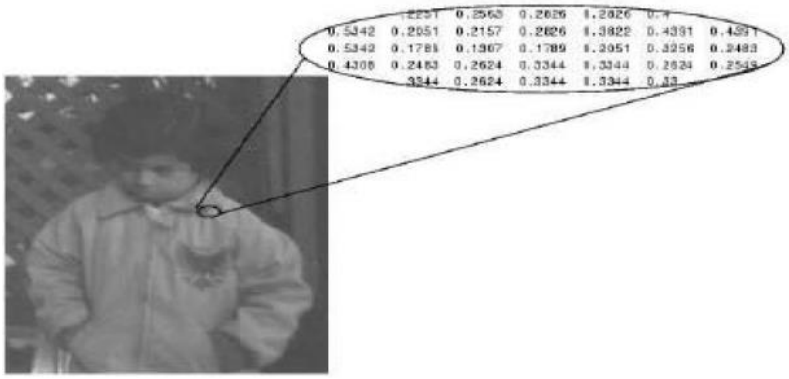


Gambar 2. Diagram proses enkripsi dan dekripsi

DES termasuk dalam algoritma enkripsi yang sifatnya cipher block, yang berarti DES mengubah data masukan menjadi blok-blok 64-bit dan kemudian menggunakan kunci enkripsi sebesar 56-bit. Setelah mengalami proses enkripsi maka akan menghasilkan output blok 64-bit.

2. 4 Citra Digital

Citra digital adalah citra yang dinyatakan secara diskrit (tidak kontinu), baik untuk posisi koordinatnya maupun warnanya. Dengan demikian, citra digital dapat digambarkan sebagai suatu matriks, dimana indeks baris dan indeks kolom dari matriks menyatakan posisi suatu titik di dalam citra dan harga dari elemen matriks menyatakan warna citra pada titik tersebut. Dalam citra digital yang dinyatakan sebagai susunan matriks seperti ini, elemen–elemen matriks tadi disebut juga dengan istilah piksel yang berasal dari kata picture element. Citra juga dapat didefenisikan fungsi dua variabel, f(x,y), di mana x dan y adalah koordinat spasial sedangkan nilai f(x,y) adalah intensitas citra pada koordinat tersebut. Ilustrasi citra digital dapat dilihat pada Gambar 4 [20], seperti pada Gambar 3.



Gambar 3. Ilustrasi Citra Digital

Citra digital merupakan suatu matriks dimana indeks baris dan kolomnya menyatakan suatu titik pada citra tersebut dan elemen matriksnya (yang disebut sebagai elemen gambar/ piksel/ pixel/ picture element) menyatakan tingkat keabuan/ warna pada titik tersebut. Citra digital dinyatakan dengan matriks berukuran N x M (baris/ tinggi = N, kolom/ lebar = M)

2. 5 Metode Penyisipan Pesan LSB (Least Significant Bit)

Dalam satu Ada banyak cara untuk menyisipkan pesan ke dalam media penyimpan pesan, antara lain metode LSB (Least Significant Bit), marking, dan filtering, metode Spread Spectrum, dan lain-lain. Pada bagian ini kita membahasi steganografi menggunkan metode LSB saja. Perhatikan contoh untuk menyisipkan sebuah karakter A ke dalam citra grayscale. Sebuah pesan huruf A akan disisipkan ke dalam citra grayscale 8 bit ukuran 10 x 10 piksel.

Langkah pertama adalah mengubah kedua data tersebut (huruf A dan citra) menjadi biner. Nilai biner untuk A adalah 10000011. Karena jumlah digit biner huruf A hanya 8 bit maka jumlah piksel citra grayscale yang dibutuhkan cukup 8 piksel saja. Perhatikan 8 piksel pertama dari citra biner yang diubah menjadi biner, ditunjukan pada Gambar 4.

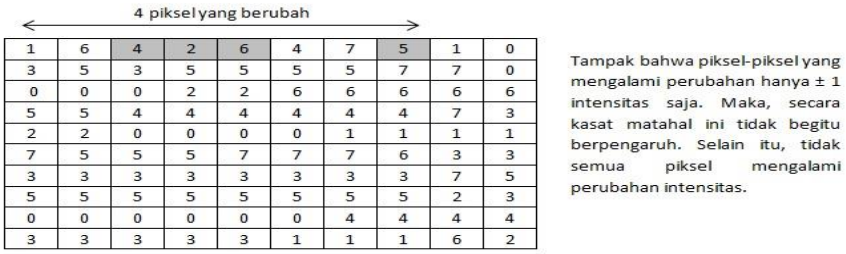
8 piksel pertama diambil

1	6	5	3	7	4	7	4	1	0
3	5	3	5	5	5	5	7	7	0
0	0	0	2	2	6	6	6	6	6
5	5	4	4	4	4	4	4	7	3
2	2	0	0	0	0	1	1	1	1
7	5	5	5	7	7	7	6	3	3
3	3	3	3	3	3	3	3	7	5
5	5	5	5	5	5	5	5	2	3
0	0	0	0	0	0	4	4	4	4
3	3	3	3	3	1	1	1	6	2

Piksel Citra	Huruf A
1 = 00000001	1
6 = 00000110	0
5 = 00000101	0
3 = 00000011	0
7 = 00000111	0
4 = 00000100	0
7 = 00000111	1
4 = 00000100	1

Gambar 4. mengubah kedua data tersebut (huruf A dan citra) menjadi biner

Perhatikan bit-bit yang ditandai dengan kotak. Bit-bit piksel citra mengalami perubahan (dalam hal ini yang berubah hanya 4 piksel saja) sehingga citra berubah menjadi :



Gambar 5. bit-bit piksel citra mengalami perubahan

Ukuran data maksimum yang bisa disembunyikan dengan metode LSB, seperti yang ditunjukan pada Gambar 5
Contoh :

Media penampungan : Citra grayscale 8-bit berukuran 64x32 piksel
Ukuran media penampung = 64 × 32 × 8 bit
= 16384 bit
1 piksel media penampung = 8 bit

Untuk menampung 1 bit data pesan diperlukan 1 piksel citra media penampung berukuran 8 bit karena setiap bit hanya menyembunyikan satu bit di LSB-nya. Oleh karena itu, citra ini hanya mampu menampung data pesan sebesar maksimum 16384/8 = 2048 bit dikurangi panjang nama filenya karena penyembunyian data rahasia tidak hanya menyembunyikan isi data tersebut, tetapi juga nama filenya. Semakin besar data yang disembunyikan di dalam citra, semakin besar pula kemungkinan data tersebut rusak akibat manipulasi pada citra penampung.

2. 6 Rancangan Sistem

Pada penelitian ini data text di enkripsikan menggunakan algoritma DES dan disembunyikan kedalam citra digital menggunkan algoritma LSB, pada Gambar 6 merupakan skema alur atau tahapan-tahapan program dari sisi pengirim dan penerima.

Flowchart diawali dengan mengimputkan data text, dan citra bmp, selanjutnya apabila file text dan file citra bmp tidak mencukupi, akan terjadi proses perulangan, insert tesxt maupun insert citra bmp, dan apabila mencukupi maka akan terjadi proses enkripsi dengan metode DES dan LSB seperti pada Gambar 7, selanjutnya terjadi proses penyimpanan file citra bmp, dimana user akan menyimpan citra bmp yang sudah dienkrip, dan proses selesai [21].

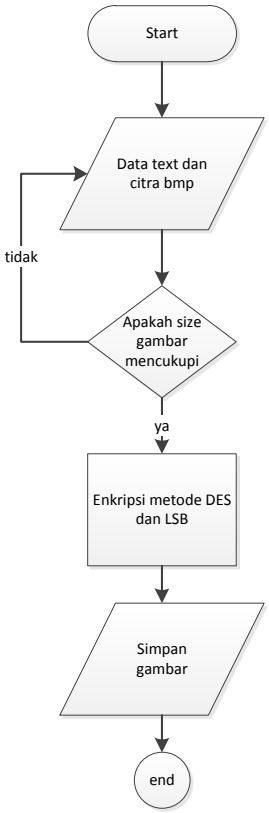
2. 7 Algoritma Enkripsi DES

Proses dari permutasi inisial (IP) teks-asli ada tiga :

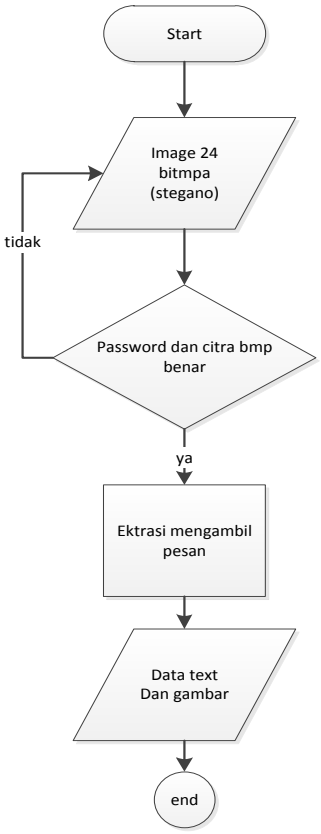
1. Teks-asli 64 bit diproses di permutasi inisial (IP) dan menyusun kembali bit untuk mengasilkan permutasi masukan.
2. Langkah untuk melakuakan fungsi yang sama, yang mengasilakan fungsi subsitusi , yang mana keluaran akhir dari awal tersebut berisi 64-bit (fungsi dari teks-teks dan kunci) masuk ke swap dan mengasilkan pre-output.
3. Pre-output dan permutasi diinversi dari permutasi inisial yang akan mengasilkan teks-teks kode 64-bit.

Proses dari kunci 56-bit :

1. Kunci melewati fungsi permutasi .
2. Pergeseran kunci, yang mana akan dipilih perulangan-perulangan permutasi kunci sebanyak 16 kali yang mengasilkan upa-kunci (ki) yang diproses dengan kombinasi permutasi.

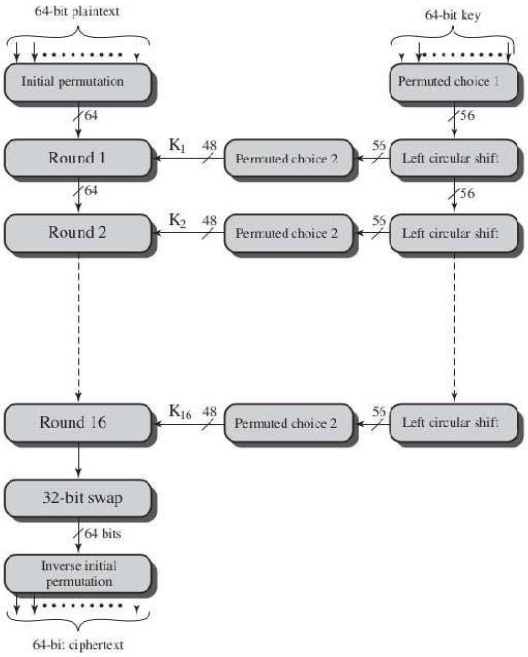


Gambar 6. Skema alur dari sisi pengirim



Gambar 7. Skema alur dari sisi penerima

3. Perbedaan dari upa-kunci (ki) akan dilakukan pergeseran kunci yang mengasilkan kombinasi teks asli 64-bit dengan kunci 56-bit. Seperti yang ditunjukan Gambar 8.



Gambar 8. Gambaran umum algoritma DES

3. HASIL DAN PEMBAHASAN

Implementasi merupakan tahap dimana sistem siap dijalankan atau dioperasikan ketahap sebenarnya, sehingga akan diketahui apakah system yang dibuat benar-benar sesuai dengan yang direncanakan. Pada implementasi perangkat lunak ini dijelaskan bagaimana aplikasi bekerja. Pada aplikasi ini terdiri dari 2 form, yaitu Form Enkripsi Citra dan Form Dekripsi Citra

3.1 Proses enkripsi dan deskripsi data

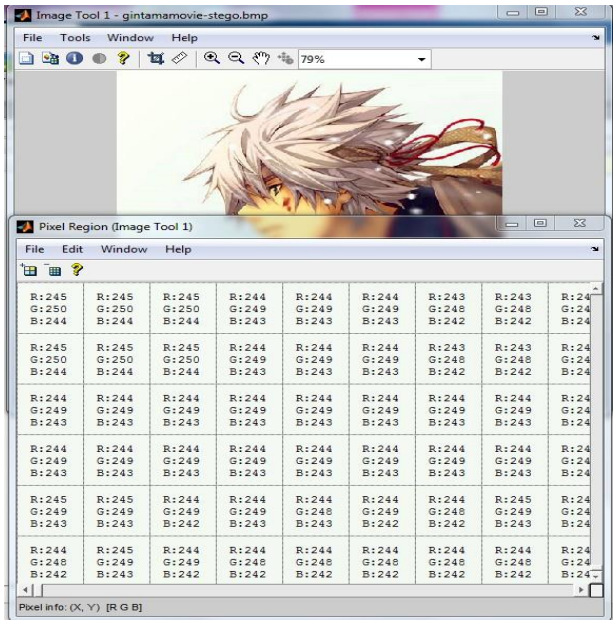
Pada button proses berfungsi sebagai proses enkripsi text dan disisipkan kedalam citra bmp. Untuk password harus lebih dari 9 karakter atau sama dengan 9 karakter, karena untuk jumlah karakter password tersebut adalah bawaan script NetBeands dimana metode DES tersebut telah diinclude dan penulis mengimplementasikannya ke dalam program, di dalam NetBeands jumlah karakter tersebut berhubungan dengan internal, dimana jumlah karakter adalah kunci internal, seperti pada Gambar 9.

Gambar 9. Proses enkripsi citra

3.2 Pengujian Sistem

Berikut ini akan dibahas mengenai pengujian sistem dan hasil uji coba analisis penyisipan data text yang sudah di enkripsikan menggunkan metode Data Encyption Standard (DES), dan disisipkan ke dalam citra digital menggunakan metode Least Significant Bit (LSB), dimana file size gambar tidak mengalami perubahan yg cukup besar.

Pada pengujian ini terdapat 2 citra bmp yang belum disisipkan text (gintama.bmp). dan yang sudah disipkan text (gintamamovie-stego.bmp), dimana dalam pengujian ini menggunkan program Matlab untuk melihat size dan informasi perubahan yang terjadi pada citra bmp, didalam Gambar 10 tidak mengalami perubahan yang terlalu besar.



Gambar 10. Piksel RGB gintamamovie-stego.bmp

Dari Gambar 10, dapat dilihat perubahan komponen RGB piksel yang berubah,perrubahan terjadi dari RGB pojok kiri bawah ke kanan bawah, perubahan yang terjadi tersebut disebabkan oleh perubahan yang terjadi karena metode Least Significant Bit (LSB), dari hasil uji coba tersebut, tidak terjadi perubahan yang terlalu besar pada citra yang sudah disisipkan maupun citra aslinya, sehingga dapat disimpulkan bahwa aplikasi sudah mampu menerapkan penyisipan pesan text yang sudah di encrypt, menggunkan metode Data Encryption Standard (DES) dan disembunyikan pada sebuah citra digital menggunakan metode Least Significant Bit (LSB).

4. KESIMPULAN

Hasil penelitian yang sudah dilakukan oleh penulis adapun kesimpulan dan saran yang diberikan sebagai berikut, Implementasi aplikasi untuk menyembunyikan pesan rahasia ke dalam citra digital (bmp) menggunkan NetBeands. Aplikasi ini bekerja dengan cara mengenkripsi pesan dengan metode DES (Data Encryption Standard), dengan menggunkan password dari pengguna sebagai kunci, aplikasi kemudian menyisipkan pesan tersebut kedalam citra digital (bmp) dengan metode LSB (Least Significant Bit), Aplikasi selain digunakan untuk menyisipkan pesan rahasia dari file, dapat berfungsi untuk mengambil kembali pesan rahasia dari file, proses pengambilan pesan dilakukan dengan cara mengektrak file pesan yang terenkripsi dari file stego, file in kemudian dideskripsi dengan meminta masukan berupa password dari pengguna. Kualitas file citra digital sebelum dan sesudah dialakukan penyisipan secara teori terjadi perubahan, namun perubahan tersebut sedemikian kecil, sehingga tidak dapat dilihat secara kasat mata.

DAFTAR PUSTAKA

[1] S. H. Hamdani, A. Suryawan, and Septiarini, "Pengujian Algoritma Rivest Code 5 Untuk Enkripsi Struktur File Dokumen," Jurnal Informatika Mulawarman," *J. Inform. Mulawarman*, vol. 8, no. 2, pp. 44–49, 2013.

[2] U. R. S. Lubis, Mesran, and T. Zebua, "Implementasi Algoritma Chua Chaotic Noise Pada Enkripsi Citra RGB," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 1, no. 1, pp. 220–224, 2017.

[3] N. Widyastuti, "Pengembangan Metode Beaufort Cipher Menggunakan Pembangkit Kunci Chaos," *J.Teknol*, vol. 7, no. 1, pp. 73–82, 2014.

[4] S. S. Ahmad, "Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm," *2016 4th Int. Conf. Cyber IT Serv. Manag.*, pp. 1–6.

[5] F. Li and P. Ming, "A simplified FPGA implementation based on an Improved DES algorithm," in *3rd International Conference on IEEE Genetic and Evolutionary Computing*, 2009, pp. 227–230.

[6] W. Stallings and L. Brown, *Computer Security Principle and Practice*. Pearson Education, 2008.

[7] S. Taherkhani, E. Ever, and O. Gemikonakli, "Implementation of Non-Pipelined and Pipelined Data Encryption Standard (DES) Using Xilinx Virtex-6 FPGA Technology," *2010 10th IEEE Int. Conf. Comput. Inf. Technol.*, no. Cit, pp. 1257–1262, 2010.

[8] J. Zhang and X. Jin, "Encryption System Design Based On DES And SHA-1," *2012 11th Int. Symp. Distrib. Comput. Appl. to Business, Eng. Sci.*, pp. 317–320, 2012.

[9] I. Marzuki, "Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux," *J. Teknol. Inf. Indones.*, vol. 2, no. 2, pp. 18–24, 2017.

[10] T. Popeea, V. Olteanu, L. Gheorghe, and R. Rughiniș, "Extension of a port knocking client-server architecture with NTP synchronization," *2011 RoEduNet Int. Conf. 10th Ed. Netw. Educ. Res.*, pp. 1–5.

[11] S.Douglas, *Cryptography: Theory and Practice*. CRC Press, 1995.

[12] N. Kumar and B. V. Gopal, "VLSI Implementation of Data Encryption Standard Algorithm," *Int. J. Innov. Technol. Explor. Eng.*, vol. 1, no. 6, pp. 106–110.

[13] S. Oukili, "FPGA implementation of Data Encryption Standard using time variable permutations," *2015 27th Int. Conf. Microelectron.*, pp. 126–129.

[14] S. T, M. Edy, S. Vincent, N. Dwi, and Wijanarto, *Teori Pengenalan Citra Digital*, 1st ed. Yogyakarta: C.V ANDI OFFSET, 2009.

[15] M. Zunaidi, "Steganografi, Menyembunyikan Pesan atau File Dalam Gambar Menggunakan Command/DOS," *J. Ilm. SAINTIKOM*, pp. 11–16, 2013.

[16] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks , Isi File Dokumen , Dan File Dokumen Menggunakan Algoritma Advanced Encryption ENCRYPTION," *J. Inform. Mulawarman*, vol. 10, no. 1, pp. 20–13, 2015.

[17] Ariyus and Dony, *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi*, 1st ed. Yogyakarta: C.V ANDI OFFSET, 2008.

[18] M. M. Amin, "Implementasi Kriptografi Klasik pada Komunikasi Berbasis Teks," *J. Pseudocode*, vol. III, no. 2, pp. 129–136, 2016.

[19] N. R. Yanti, Alimah, and D. A. Ritonga, "Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database," *J. Sains Komput. Inform.*, vol. 2, no. 1, pp. 23–32, 2018.

[20] Menezes, Oorcshot, and Vanstone, *Handbook of Applied Cryptography*. USA: CSR Press Inc., 1996.

[21] R. Munir, *Pengolahan Citra Dengan Pendekatan Algoritmik*. Bandung: Informatika, 2004.