IMPLEMENTASI ALGORITMA KRIPTOGRAFI *DES* DAN *WATERMARK* DENGAN METODE *LSB* PADA DATA CITRA

NASKAH PUBLIKASI

disusun oleh:

Sulidar Fitri

06.11.1009

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2010

NASKAH PUBLIKASI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI *DES* DAN *WATERMARK* DENGAN METODE *LSB* PADA DATA CITRA

disusun oleh

Sulidar Fitri

06.11.1009

Dosen Pembimbing,

Arief Setyanto, S.Si, MT
NIK. 190302036

Tanggal, 4 Februari 2010

Ketua Jurusan
Teknik Informatika

Ir. Abas Ali Pangera, M. Kom.
NIK. 190302010

ABSTRACT

Since internet comes in human life, the control of information is move so fast. Including the information that should have special sense because the value of the information is very important and secret. Nowadays live there a lot of people save the secret message on digital media and use the certain code. DES(Data Encryption Standard) is such algorithm that ever be the most famous one in US and the basic standard to secure information that use in whole world. Watermark is also one solution to protect the confidentiality and ownership. Watermark by LSB method can hide the information to such a media without known by other people. People also don't realize that media have a hiding information in it.

This Research is dividing in 3 parts. First is implementation the DES Algorithm and Watermark by LSB method in java language. The Second thing is that see the differences quality of image media before and after it's hidden by the secret information. Image media that use to hide is using 3 different image file extension, those are jpeg, gif, and png. The last is to measure the performance of the process in second that implement in those 3 different image file extension.

The result said that the implementation in Windows operation system is successful. The quality of image before and after the message was hidden cannot differentiated by human eyes directly. But we can differ it by information on histogram. The performance by processing 100 characters is relatively fast, less equal than 1 second.

***Keyword**: Cryptography, DES Algorithm, Data Encryption Standard,Watermark, LSB(Least Significant Bit),Image Watermark, Secret Information*

1. Pendahuluan

Kehadiran komputer memberi perhatian yang lebih bukan hanya dalam pengolahan data saja melainkan juga dengan keamanan data. Teknologi jaringan komputer yang saat ini berkembang, memungkinkan satu komputer dapat terhubung dengan komputer lainnya di belahan dunia ini untuk saling berbagi data dan informasi.

Semenjak kehadiran internet pada kehidupan manusia, kontrol atas informasi bergerak dengan amat cepat. Termasuk pula informasi-informasi yang harus mendapatkan “perhatian” khusus karena nilai informasi tersebut yang sangat penting semisal informasi intelijen, militer, dan berbagai macam informasi yang sering dilabeli *TOP SECRET*.

Kehidupan sekarang pun, orang-orang banyak yang menyimpan suatu pesan pada media *digital*. Terkadang ada juga pesan yang merupakan informasi rahasia yang disimpan pada media gambar namun sang pemilik pesan tersebut hanya mengizinkan beberapa orang saja yang dikehendaki untuk mengetahuinya. Tetapi ada saja pihak maupun orang yang ingin mengetahui isi pesan tersebut untuk kepentingan tertentu namun sebenarnya tidak diberi hak oleh sang pemilik pesan.

Adanya masalah di atas memunculkan ilmu baru pada dunia informatika yang disebut kriptografi yang merupakan pengembangan dari kriptologi. Berbagai pakar kriptografi telah mengembangkan berbagai macam algoritma enkripsi. *DES* merupakan algoritma yang pernah menjadi sangat terkenal di Amerika dan pernah menjadi keamanan dasar yang digunakan di seluruh dunia.

Teknologi *Watermark* juga merupakan suatu solusi didalam melindungi kerahasiaan dari tanda kepemilikan. *Watermark* dapat

menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan kecuali orang yang telah mengetahui kuncinya, karena hasil keluaran *Watermark* adalah data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia, namun berbeda apabila dilihat dengan perangkat pengolah data digital seperti komputer, sedangkan perubahan pesan dalam kriptografi dapat dilihat dan disadari langsung oleh indera manusia.

Penggunaan teknik *Watermark* dan kriptografi secara bersamaan dimaksudkan untuk memberikan keamanan berlapis dalam pengamanan pesan sebagai tanda kepemilikan. Pada skripsi ini akan dibahas mengenai penyisipan data yang sudah di enkripsi dengan kriptografi algoritma *DES* ke dalam sebuah citra dengan metode penyisipan *LSB*.

Dalam pelaksanaan penelitian ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah sebagai berikut :

1. Bagaimana mengimplementasikan teknik kriptografi *DES*(*Data Encryption Standard*) dan *Watermarking* metode *LSB(Least Significant Bit)* pada data citra RGB?
2. Bagaimana kualitas dan perbedaan citra sebelum dan sesudah disisipkan teks?
3. Bagaimana performa teknik kriptografi *DES* dan *watermark* dengan metode *LSB*?

2. Landasan Teori

2.1. Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan

rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan Kerahasiaan (*confidentiality*), integritas data(*data integrity)*, otentikasi(*authentication)*, dan penyangkalan(*non-repudiation).*

Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Kata “seni” berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia pesan mempunyai nilai estetika tersendiri.

Kriptografi berkembang menjadi sebuah seni merahasiakan pesan (kata “*graphy*” di dalam “*cryptography*” itu sendiri sudah menyiratkan sebuah seni). Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

2.2. Enkripsi dan Dekripsi

Enkripsi adalah hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga

kerahasiaannya. Pesan asli disebut plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bias diartikan dengan cipher atau kode.

Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya(teks asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.

Keamanan dari kriptografi modern didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri. Kunci memiliki fungsi yang sama dengan password. Jika keseluruhan keamanan algoritma tergantung pada kunci yang dipakai, maka algoritma ini bisa dipublikasikan dan dianalisa orang lain.

2.3. Algoritma Kunci Simetris

Algoritma kunci simetris adalah algoritma kriptografi yang memiliki kunci yang sama untuk proses enkripsi dan dekripsinya. Kunci tersebut merupakan satu-satunya jalan untuk proses dekripsi (kecuali mencoba membobol algoritma tersebut), sehingga kerahasiaan kunci menjadi nomer satu.

2.4. Algoritma DES(Data Encryption Standard)

2.4.1. Sejarah *DES*

Pada sekitar akhir tahun 1960, IBM melakukan riset pada bidang kriptografi yang pada akhirnya disebut *Lucifer*. *Lucifer* dijual pada tahun 1971 pada sebuah perusahaan di london. *Lucifer* merupakan algoritma berjenis Block Cipher yang artinya bahwa input maupun output dari algoritma tersebut merupakan 1 blok yang terdiri dari banyak bit seperti 64 bit atau 128 bit.Lucifer beroperasi pada blok input 64 bit dan menggunakan key sepanjang 128 bit.

Lama-kelamaan *Lucifer* semakin dikembangkan agar bisa lebih kebal terhadap serangan analisis cypher tetapi panjang kuncinya dikurangi menjadi 56 bit dengan masksud supaya dapat masuk pada satu chip. Di tempat yang lain, biro standar amerika sedang mencari-cari sebuah algoritma enkripsi untuk dijadikan sebagai standar nasional.IBM mencoba mendaftarkan algoritmanya dan di tahun 1977 algoritma tersebut dijadikan sebagai *DES* (*Data Encryption Standard*).

2.5. Proses Kerja DES(Data Encryption Standard)

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 (lihat Gambar 2.3):

a. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
b. Hasil permutasi awal kemudian di-*enciphering*- sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
c. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP^{-1}) menjadi blok cipherteks.

2.6. WATERMARKING

Istilah *watermarking* ini muncul dari salah satu cabang ilmu yang disebut dengan *steganography*. *Stegranography* merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi “rahasia” di dalam suatu

informasi lainnya. Perbedaan stegranograpy dengan cryptography terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses tersebut. *Cryptography* melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar- benar acak / seolah-olah berantakan (tetapi dapat dikembalikan ke bentuk semula) dan berbeda dengan aslinya, sedangkan stegranography menyembunyikan dalam data lain yang akan ditumpanginya tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir sama. Dengan kata lain keluaran stegranography ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi disini oleh indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya.

Watermarking (tanda air) dapat diartikan sebagai suatu teknik penyembunyian data atau informasi “rahasia” kedalam suatu data lainnya untuk “ditumpangi” (kadang disebut dengan host data), tetapi orang lain tidak menyadari kehadiran adanya data tambahan pada data host-nya. Jadi seolah-olah tidak ada perbedaan antara data host sebelum dan sesudah proses *watermarking*.

Watermarking ini memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Jadi *watermaking* merupakan suatu cara untuk penyembunyian atau penanaman data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) kedalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran), dan mampu menghadapi proses-proses pengolahan sinyal digital yang tidak merusak kualitas data yang ter-*watermark* sampai pada tahap tertentu. Disamping itu data yang ter-watermark harus tahan (*robust*) terhadap serangan-serangan baik secara

sengaja maupun tidak sengaja untuk menghilangkan data *watermark* yang terdapat didalamnya.

2.6.1. Sejarah Watermark

Watermarking sudah ada sejak 700 tahun yang lalu. Pada akhir abad 13, pabrik kertas di Fabriano Italia, membuat kertas yang diberi *watermark* atau tanda air dengan menekan bentuk cetakan gambar atau tulisan pada kertas yang baru setengah jadi. Ketika kertas dikeringkan, terbentuklah suatu kertas yang ber-*watermark*. Kertas itu biasanya digunakan oleh seniman atau sastrawan untuk menuliskan karya mereka. Kertas yang sudah dibubuhi tanda-air tersebut sekaligus dijadikan identifikasi bahwa karya seni di atasnya adalah milik mereka.

Ide *watermarking* dalam data *digital* (sehingga disebut *digital watermarking*) dikembangkan di Jepang pada tahun 1990 dan Swiss pada tahun 1993. *Digital watermarking* semakin berkembang seiring semakin meluasnya penggunaan internet.

Mutu dari teknik *watermarking* meliputi beberapa parameter-parameter utama yang berikut ini

a. *Fidelity* : Merupakan suatu istilah perubahan yang disebabkan oleh tanda (*mark*) semestinya tidak mempengaruhi nilai isi, idealnya tanda harusnya tidak dapat dilihat, sehingga tidak dapat dibedakan antara data yang ter-watermark dan data yang asli.

b. *Robustness* : *watermark* di dalam *host* data harus tahan terhadap beberapa operasi pemrosesan digital yang umum seperti pengkonversian dari digital ke analog dan dari analog ke digital, dan manipulasi data.

c. *Security* : *Watermarking* harus tahan terhadap usaha segaja memindahkan/mencopy watermark dari satu multimedia data ke

multimedia data lainnya. Pada ketiga kriteria diatas, *fidelity* merupakan kriteria paling tinggi.

2.6.2. Tujuan Penggunaan *Watermark*

Ada beberapa jenis penggunaan watermaking yang umum dalam kehidupan sehari-hari adalah:

a. Perlindungan (*copyright*), Memberi label kepemilikan (*ownership*) dalam file digital.
b. Autentikasi atau *tamper proofing*: untuk membuktikan apakah file masih asli atau sudah berubah.
c. *Fingerprinting*, menjadi identitas dari file yang didistribusikan.

2.6.3. Tipe Watermark

Tipe watermark pada dasarnya terbagi menjadi dua, yakni *visible* dan *invisible*. Disibut visible jika suatu *watermark* bias dilihat dengan mata telanjang. Sedangkan *invisible watermark* tidak dapat dilihat dengan mata telanjang.

Ada beberapa alasan pemakaian *invisible watermark*, antara lain:

a. *Proof of Ownership* (bukti kepemilikan): selain bisa digunakan sebagai tanda pengenal kepemilikan (*owner identification*), juga bisa digunakan sebagai pembuktian kepemilikan bila ada dua orang atau lebih yang memperebutkan hak kepemilikan.
b. Pendistribusian lebih aman: keamanan dalam pendistribusian. Oleh karena watermark tidak bisa dilihat dengan mata telanjang, kemungkinan untuk dicurigai sangatlah kecil.

2.7. Metode LSB(Least Significant Bit)

Metode ini menggunakan teknik domain spatial dan merupakan metoda yang paling sederhana tetapi yang paling tidak tahan terhadap segala proses yang dapat mengubah nilai-nilai intensitas pada citra. Metoda ini akan mengubah nilai *LSB* (*Least Significant* Bit) bit warna menjadi bit yang bersesuai dengan bit label yang akan disembunyikan. Memang metoda ini akan menghasilkan citra rekonstruksi yang sangat mirip dengan aslinya, karena hanya mengubah nilai bit terakhir dari data. Tetapi sayang tidak tahan terhadap proses-proses yang dapat mengubah data citra terutama kompresi JPEG.

Metode *LSB* menyembunyikan data rahasia dalam pixel – pixel tak signifikan (*least significant pixel*) dari berkas wadah (*cover*). Pengubahan nilai pixel – pixel tidak signifikan pada dasarnya memberikanpengaruh terhadap berkas wadah, tetapi karena perubahan yang terjadi sangat kecil, sehingga tidak tertangkap oleh indra manusia. Kenyataan inilah yang akhirnya dimanfaatkan sebagai teknik penyembunyian data atau pesan.

Sebagai ilustrasi cara penyimpanan data dengan metode *LSB*, misalnya pixel-pixel wadah berikut

```
01001101 00101110 10101110 10001010 10101111
10100010 00101011 101010111
```

Digunakan untuk menyimpan karakter ‘H’ (01001000), maka pixel – pixel wadah tersebut akan dirubah menjadi

```
01001100 00101111 10101110 10001010 10101111
10100010 00101010 101010110
```

2.8. TIPE FILE GAMBAR

2.8.1. JPEG (Joint Photographic Experts Group)

Adalah format gambar yang banyak digunakan untuk menyimpan gambar-gambar dengan ukuran lebih kecil. Ada beberapa karakteristik gambar dalam JPEG yang tentu kita tahu pasti memiliki ekstensi .jpg atau .jpeg. Selain itu JPEG juga mampu menayangkan warna dengan kedalaman 24-bit true color.

File JPG cocok digunakan untuk gambar yang memiliki banyak warna, misalnya foto wajah dan pemandangan. Dan tidak cocok digunakan untuk gambar yang hanya memiliki sedikit warna seperti kartun atau komik.

2.8.2. GIF (Graphics Interchange Format)

Merupakan salah satu format gambar yang banyak digunakan. Salah satu ciri khas tipe gambar berekstensi GIF adalah bisa memainkan animasi gambar sederhana. Beberapa karakteristik lain format gambar GIF adalah mampu menayangkan maksimum sebanyak 256 warna karena format GIF menggunakan 8-bit untuk setiap pixel-nya. Selain itu GIF juga mampu mengkompresi gambar dengan sifat lossless dan mendukung warna transparan.

File GIF cocok digunakan untuk gambar dengan jumlah warna sedikit (dibawah 256), gambar yang memerlukan perbedaan warna yang tegas seperti logo tanpa gradien, gambar animasi sederhana seperti banner-banner iklan, header, dan sebagainya. Dan tidak cocok digunakan untuk gambar yang memiliki banyak warna seperti pemandangan, gambar yang didalamnya terdapat warna gradien atau semburat.

2.8.3. PNG (Portable Network Graphics)

Adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra

tersebut. Secara umum PNG dipakai untuk Citra Web (Jejaring jagad Jembar – en:World Wide Web). Citra dengan format PNG mempunyai faktor kompresi yang lebih baik dibandingkan dengan GIF (5%-25% lebih baik dibanding format GIF).

Kelebihan file PNG adalah adanya warna transparan dan alpha. Warna alpha memungkinkan sebuah gambar transparan, tetapi gambar tersebut masih dapat dilihat mata seperti samar-samar atau bening.

3. Analisis

3.1. Proses Perputaran *DES*

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 sebagai

$$L_i = R_{i-1}$$

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

Sebelum putaran pertama, terhadap blok plainteks dilakukan permutasi awal (*initial permutation* atau IP). Tujuan permutasi awal adalah mengacak plainteks sehingga urutan bit-bit di dalamnya berubah.

Karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah. Kunci-kunci internal ini dapat dibangkitkan sebelum proses

enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter.

Dalam permutasi ini, tiap bit kedelapan (*parity bit*) dari delapan *byte* kunci diabaikan. Hasil permutasinya adalah sepanjang 56 bit, sehingga dapat dikatakan panjang kunci DES adalah 56 bit. Selanjutnya, 56 bit ini dibagi menjadi 2 bagian, kiri dan kanan, yang masing-masing panjangnya 28 bit, yang masing-masing disimpan di dalam C0 dan D0.

Selanjutnya, kedua bagian digeser ke kiri (*left shift*) sepanjang satu atau dua bit bergantung pada tiap putaran. Operasi pergeseran bersifat *wrapping* atau *round-shift*. Misalkan (Ci, Di) menyatakan penggabungan Ci dan Di. (Ci+1, Di+1) diperoleh dengan menggeser Ci dan Di satu atau dua bit.

Jadi, setiap kunci internal Ki mempunyai panjang 48 bit. Bila jumlah pergeseran bit-bit pada Tabel 1 dijumlahkan semuanya, maka jumlah seluruhnya sama dengan 28, yang sama dengan jumlah bit pada Ci dan Di. Karena itu, setelah putaran ke-16 akan didapatkan kembali C16 = C0 dan D16 = D0.

E adalah fungsi ekspansi yang memperluas blok Ri – 1 yang panjangnya 32-bit menjadi blok 48 bit. Selanjutnya, hasil ekpansi, yaitu E(Ri – 1), yang panjangnya 48 bit di-XOR-kan dengan Ki yang panjangnya 48 bit menghasilkan vektor A yang panjangnya 48-bit:

$$E(R_{i-1}) \oplus K_i = A$$

Vektor A dikelompokkan menjadi 8 kelompok, masing-masing 6 bit, dan menjadi masukan bagi proses substitusi. Proses substitusi dilakukan dengan menggunakan delapan buah kotak-S (S-box), S1 sampai S8. Setiap kotak-S menerima masukan 6 bit dan menghasilkan keluaran 4 bit. Kelompok 6-bit pertama menggunakan S1, kelompok 6-bit kedua

menggunakan S2, dan seterusnya. Keluaran proses substitusi adalah vektor B yang panjangnya 48 bit. Vektor B menjadi masukan untuk proses permutasi. Tujuan permutasi adalah untuk mengacak hasil proses substitusi kotak-S.

Bit-bit P(B) merupakan keluaran dari fungsi f.
Akhirnya, bit-bit P(B) di-XOR-kan dengan Li – 1 untuk mendapatkan Ri

$$R_i = L_{i-1} \oplus P(B)$$

Jadi, keluaran dari putaran ke-i adalah: $(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus P(B))$

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Keluaran pada setiap putaran *deciphering* adalah

$$L_i = R_{i-1}$$

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

Dalam hal ini, (R16, L16) adalah blok masukan awal untuk *deciphering*. Blok (R16, L16) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP-1. Pra-keluaran dari *deciphering* adalah adalah (L0, R0). Dengan permutasi awal IP akan didapatkan kembali blok plainteks semula.

Selama *deciphering*, K16 dihasilkan dari (C16, D16) dengan permutasi PC-2. Tentu saja (C16, D16) tidak dapat diperoleh langsung pada permulaan *deciphering*. Tetapi karena (C16, D16) = (C0, D0), maka K16 dapat dihasilkan dari (C0, D0) tanpa perlu lagi melakukan pergeseran bit. Catatlah bahwa (C0, D0) yang merupakan bit-bit dari kunci eksternal K yang diberikan pengguna pada waktu dekripsi.

Selanjutnya, K15 dihasilkan dari (C15, D15) yang mana (C15, D15) diperoleh dengan menggeser C16 (yang sama dengan C0) dan D16 (yang sama dengan C0) satu bit ke kanan. Sisanya, K14 sampai K1 dihasilkan

dari (C14, D14) sampai (C1, D1). (Ci – 1, Di – 1) diperoleh dengan menggeser Ci dan Di dengan cara yang sama seperti sebelumnya, tetapi pergeseran kiri (*left shift*) diganti menjadi pergeseran kanan (*right shift*).

3.2. Alur Metode LSB

Proses diawali dengan melakukan perulangan sebanyak tinggi dari citra digital, setelah itu dilakukan pembacaan baris dan data warna yang dilanjutkan oleh perulangan sebanyak lebar citra digital. Proses utama dalam diagram alir ini terdapat pada pengambilan nilai bit-bit warna dari citra digital untuk diproses kemudian digabungkan dengan bit-bit data.

Proses ini dilakukan pada setiap warna yang ada (merah, hijau dan biru) dengan melakukan operasi AND dengan nilai bilangan 254 yang memiliki nilai biner 11111110, hal ini dilakukan untuk membuang 1 bit belakang dari warna pada citra digital. Proses dilanjutkan dengan melakukan operasi OR dengan bit data yang telah dimasukan ke dalam variabel penampung, hasil dari operasi ini merupakan satu nilai byte warna yang telah disisipi data pada 1 bit belakang dari total 8 bit untuk masing-masing warna pada citra digital. Perulangan dilakukan terus menerus hingga seluruh titik warna(pixel) pada citra digital selesai diproses.

Untuk membaca datanya, dilakukan suatu pengambilan nilai data yang telah disembunyikan dengan metode *LSB*, langkah yang dilakukan pertama kali yaitu pembacaan *byte-byte* warna pada citra digital, kemudian dilakukan suatu proses yang menggunakan operasi AND dengan bilangan 1 yang memiliki nilai biner 00000001, hal ini bertujuan untuk mengambil nilai 1 bit dari belakang *byte* warna yang merupakan data yang disembunyikan pada proses penyisipan data, setelah itu data yang telah berhasil dibaca dimasukan ke dalam variabel penampung yang akan dikembalikan dalam bentuk semula.

4. Hasil Penelitian dan Pembahasan

Tujuan pengujian berdasarkan file gambar ini adalah untuk melihat hasil dari perbandingan gambar yang telah disisipkan pesan dengan file aslinya. Selain itu, hasil pengujian ini juga akan diketahui lama waktu proses yang dilalui. Untuk pengujian menggunakan file gambar yang berekstensi *.GIF, *.JPEG, *.PNG, data yang dipakai menggunakan 100 karakter.

Tabel 4.1. Perbandingan Ukuran hasil Proses Penyisipan Pesan

	GIF	**JPEG**	**PNG**
File Asli	51 KB	31 KB	280 KB
Data yg Disisipkan	100 karakter	100 karakter	100 karakter
File yang telah disisipi	59 KB	44 KB	342 KB
Selisih	8 KB	13 KB	62 KB

Pengujian kecepatan terhadap proses pengolahan sangat diperlukan untuk mengetahui perbandingannya.

Tabel 4.2. Perbandingan Waktu Proses Kriptografi *DES*

Jenis	10 kar	50 kar	100 kar
Enkripsi	0.1 dt	0.2 dt	0.3 dt
Dekripsi	0.1 dt	0.2 dt	0.3 dt

Tabel 4.3 Perbandingan Waktu Proses *Watermark*

Jenis / File	GIF	JPEG	PNG
Sisip	00:00.8	00:01.0	00:00.7
Ekstrak	00:00.5	00:00.6	00:00.4

5. Kesimpulan

Dari hasil penelitiah yang telah dilakukan, maka dapat disimpulkan bahwa implementasi algoritma kriptografi DES dan watermark dengan metode LSB yang dijalankan pada Sistem Operasi Windows, cukup berhasil. Terbukti dengan:

1. Aplikasi ini mempunyai performa yang cukup bagus dengan waktu relatif cepat dengan menggunakan 100 karakter. Untuk enkripsi dan dekripsi membutuhkan waktu 0,3 dt. Untuk penyisipan teks ke dalam gambar pada file GIF=0,8 dt, JPEG= 1,0 dt, dan PNG=0.7 dt. Sedangkan pengekstrakan pada file GIF=0,5 dt, JPEG=0.6 dt , dan file PNG=0,4 dt. Hasil ini mengacu pada gambar 4.7 dan 4.8
2. Kualitas citra yang disisipi teks sebanyak 100 karakter atau sekitar 100 byte masih belum bisa dilihat secara visual.
3. Walaupun tidak bisa dilihat secara visual, perbedaan citra bisa dilihat dengan histogram

DAFTAR PUSTAKA

Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi.Yogyakarta: Penerbit ANDI

Ariyus, Dony. 2009. Keamanan Multimedia. Yogyakarta: Penerbit ANDI

A. Suhendra, S.Si dan Hariman Gunadi, S.Si, M.T. Visual Modeling Menggunakan UML dan Rational Rose, Informatika Bandung.

Hook, David.2005. *Beginning Cryptography with Java*. Wrox Press www.wrox.com (e-book). Tanggal akses: 5 Nov 09 jam 15:15

Mengenal Tipe File Gambar

http://www.file-extensions.org/filetype/extension/name/vector-graphic-files. Tanggal akses: 25 Oktober 09 jam 13:25

Modul Pemrograman Java. http://www.dosen.amikom.ac.id Tanggal akses: 27 Okt 09 jam 08:30

Steganografi Dan Kriptografi

http://www.informatika.org/~rinaldi/Kriptografi/20062007/bahankuliah2006.htm

Tanggal akses: 29 Oktober 09 jam 10:15

Watermarking dan Kriptografi

http://jurnal.bl.ac.id/wp-content/uploads/2007/01/TELTRON-v3-n1-artikel4-april2006.pdf Tanggal akses : 29 Okt 09 jam 10:25