

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

SKRIPSI



disusun oleh:

Sulidar Fitri

06.11.1009

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

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta,

Sulidar Fitri
NIM. 06.11.1009

KATA PENGANTAR

Assalaamu'alaykum Wr.Wb

Maha besar Allah penguasa sekalian alam, segala puja dan puji syukur adalah milikMU “Allah Subhanahu Wata’ala”, hanya karena izin-Mu lah penulis mampu menyelesaikan kewajiban sebagai mahasiswi. Sanjungan kebaikan hanya penulis tunjukan kepada Habibullah Muhammad Salallahu Alaihi Wassalam yang telah menaburkan kilau Al-Qur’anulkarim dan mutiara sunnah-Nya.

Penyusunan dan penulisan skripsi dengan judul “*Implementasi Algoritma Kriptografi DES dan Watermark dengan Metode LSB Pada Data Citra*” ini bertujuan untuk memenuhi syarat kelulusan perguruan tinggi program studi Strata-1 Teknik Informatika dan mendapatkan gelar kesarjanaan dalam bidang computer di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Dalam proses penyusunan dan penulisan skripsi, penulis menyadari bahwa kemampuan penulis terbatas. Oleh karena itu, penulis menyampaikan terimakasih kepada pihak-pihak yang turut terlibat dari awal proses hingga akhir, antara lain:

1. Bapak Prof.Dr.M.Suyanto,MM selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Bapak Ir.Abas Ali Pangera,M.Kom selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Bapak Arief Setyanto, S.Si, MT selaku Dosen Pembimbing, yang telah banyak meluangkan waktu untuk membimbing dan mengarahkan sehingga skripsi ini dapat terselesaikan.

4. Bapak Erik Hadi Saputra, S.Kom dan Bapak Melwin Syafrizal, S.Kom, M.Eng selaku Dosen Penguji, terimakasih atas saran dan kritiknya yang merupakan langkah awal penyempurnaan skripsi ini.
5. Seluruh Dosen STMIK AMIKOM Yogyakarta yang telah memberikan ilmunya pada penulis.
6. Semua pihak yang telah memberikan bantuan kepada penulis yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari sepenuhnya bahwa dalam penyusunan skripsi ini masih jauh dari kesempurnaan dan tidak akan pernah mencapai kesempurnaan, namun yang dapat kita lakukan adalah hanya membuat agar mendekati kesempurnaan yaitu dengan cara mengevaluasi dan mengoreksi jika ada yang kurang ataupun salah. Untuk itu, penulis mengharapkan adanya kritik ataupun saran yang bersifat membangun demi mendekati kesempurnaan laporan ini.

Akhir kata penulis mengharapkan semoga penyusunan dan penulisan skripsi ini dapat memberikan manfaat dan ruang yang lebar bagi pembaca untuk berkreasi lebih sempurna dalam menuangkan sebuah karya.

Wassalaamu'alaykum wr.wb

Yogyakarta, 1 Februari 2010

Penulis

SULIDAR FITRI

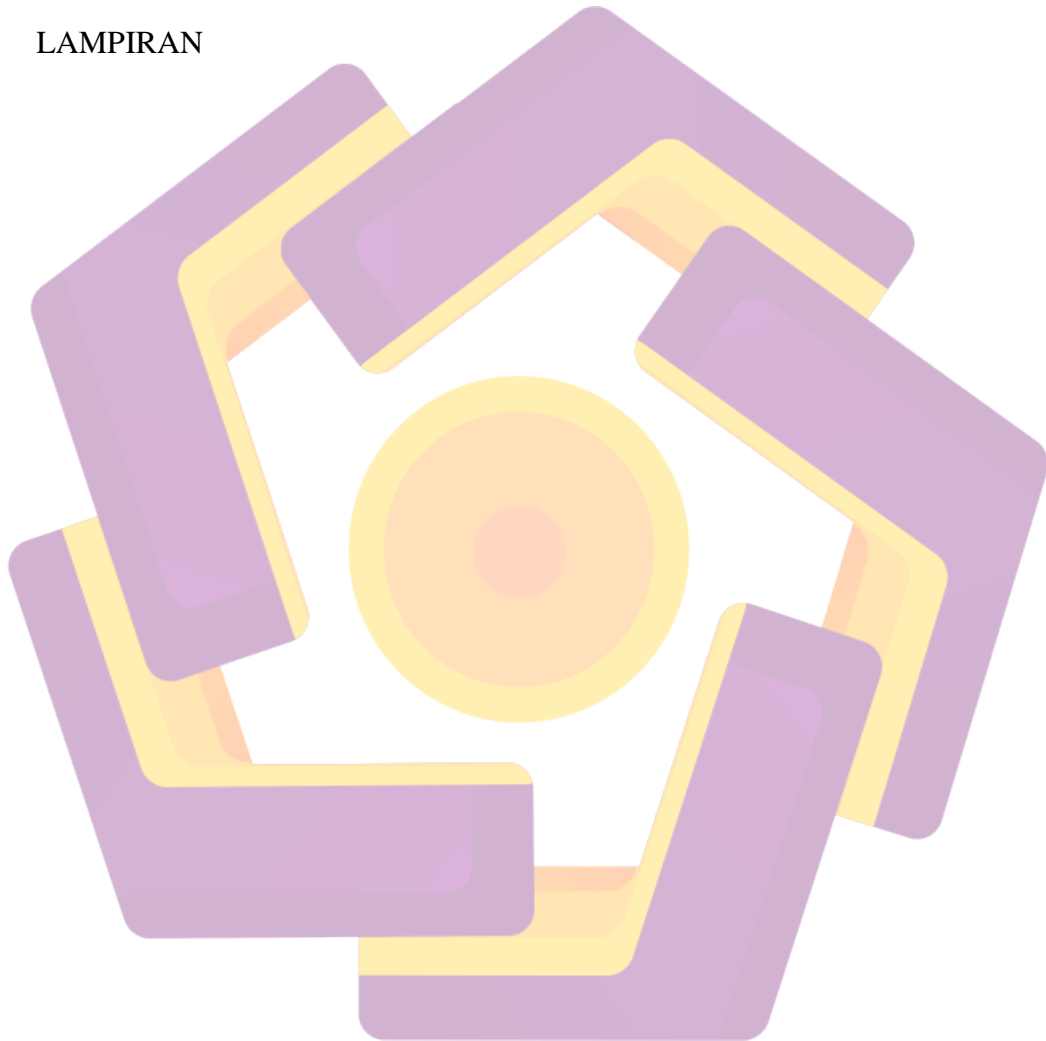
DAFTAR ISI

SAMPUL DEPAN	i
JUDUL	ii
PERSETUJUAN	iii
PENGESAHAN	iv
PERNYATAAN	v
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
INTISARI	xvii
ABSTRACT	xviii
BAB I	1
PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah	3
1.4. Tujuan Penelitian	4
1.5. Manfaat Penelitian	4
1.6. Metode Pengumpulan Data	4
BAB II	6
DASAR TEORI	6
2.1. Kriptografi	6
2.2. Enkripsi dan Dekripsi	7

2.3. Algoritma Kunci Simetris	8
2.4. Algoritma <i>DES(Data Encryption Standard)</i>	8
2.4.1. Sejarah <i>DES</i>	8
2.4.2. Proses Kerja <i>DES</i>	9
2.5. <i>Watermarking</i>	12
2.5.1. Sejarah <i>Watermark</i>	13
2.5.2. Tujuan Penggunaan <i>Watermark</i>	15
2.5.3. Tipe <i>Watermark</i>	15
2.6. Metode <i>LSB(Least Significant Bit)</i>	16
2.7. Tipe File Gambar	18
2.7.1. <i>JPEG (Joint Photographic Experts Group)</i>	18
2.7.2. <i>GIF (Graphics Interchange Format)</i>	19
2.7.3. <i>PNG (Portable Network Graphic)</i>	19
2.8. Perangkat Lunak Yang Digunakan	20
2.8.1. <i>J2SE (Java Standard Edition)</i>	20
2.8.2. Net Beans IDE 6.5	21
2.9. Pemrograman Java	21
2.9.1. Pernyataan Dalam Java	22
2.9.2. Statement if	22
2.9.3. Statement if-else	23
2.9.4. Statement if-else-if	24
2.9.5. Statement Switch	24
2.9.6. While Loop	25
2.9.7. do-while-loop	26
2.9.8. for loop	26
BAB III	27
ANALISIS DAN PERANCANGAN SISTEM	27

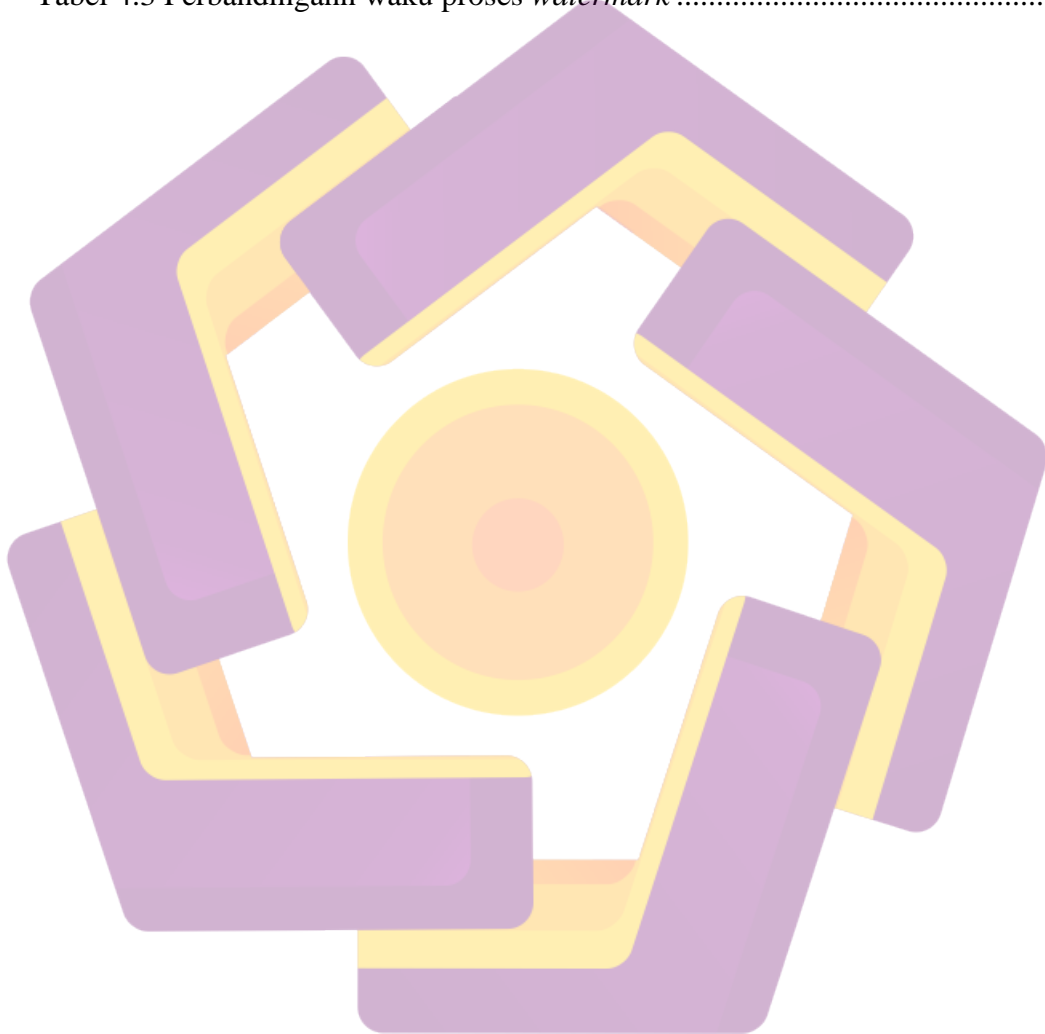
3.1. Analisis	27
3.1.1. Identifikasi Masalah	27
3.1.2. Analisis Kebutuhan Sistem	27
3.2. Perancangan Sistem	30
3.2.1. <i>Use Case</i> Diagram	30
3.2.2. <i>Class</i> Diagram	30
3.2.3. <i>Flowchart</i> Sistem	32
3.2.3.1. <i>Flowchart</i> Penyisipan Pesan	32
3.2.3.2. <i>Flowchart</i> Ekstrak Pesan	34
3.2.4. <i>Flowchart</i> Program	36
3.2.4.1. Enkripsi dan Dekripsi <i>DES</i>	36
3.2.4.2. Meode <i>LSB</i>	43
BAB IV	45
PEMBAHASAN	45
4.1. Pengujian Berdasarkan File Gambar	45
4.1.1. Pengujian Pada File *.gif	45
4.1.2. Pengujian Pada File *.jpeg	47
4.1.3. Pengujian Pada File *.png	49
4.2. Pengujian Kecepatan Berdasarkan Proses	52
4.3. Grafik Perbandingan Waktu	53
4.4. Pembahasan Kode Program	54
4.4.1. Algoritma <i>DES</i>	54
4.4.2. <i>Watermark LSB</i>	55
4.5. Petunjuk Penggunaan Aplikasi	58
4.5.1. Menyisipkan Data ke File Gambar	59
4.5.2. Membaca Pesan Dari File Gambar	63

BAB V	65
PENUTUP	65
5.1. Kesimpulan	65
5.2. Saran	66
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

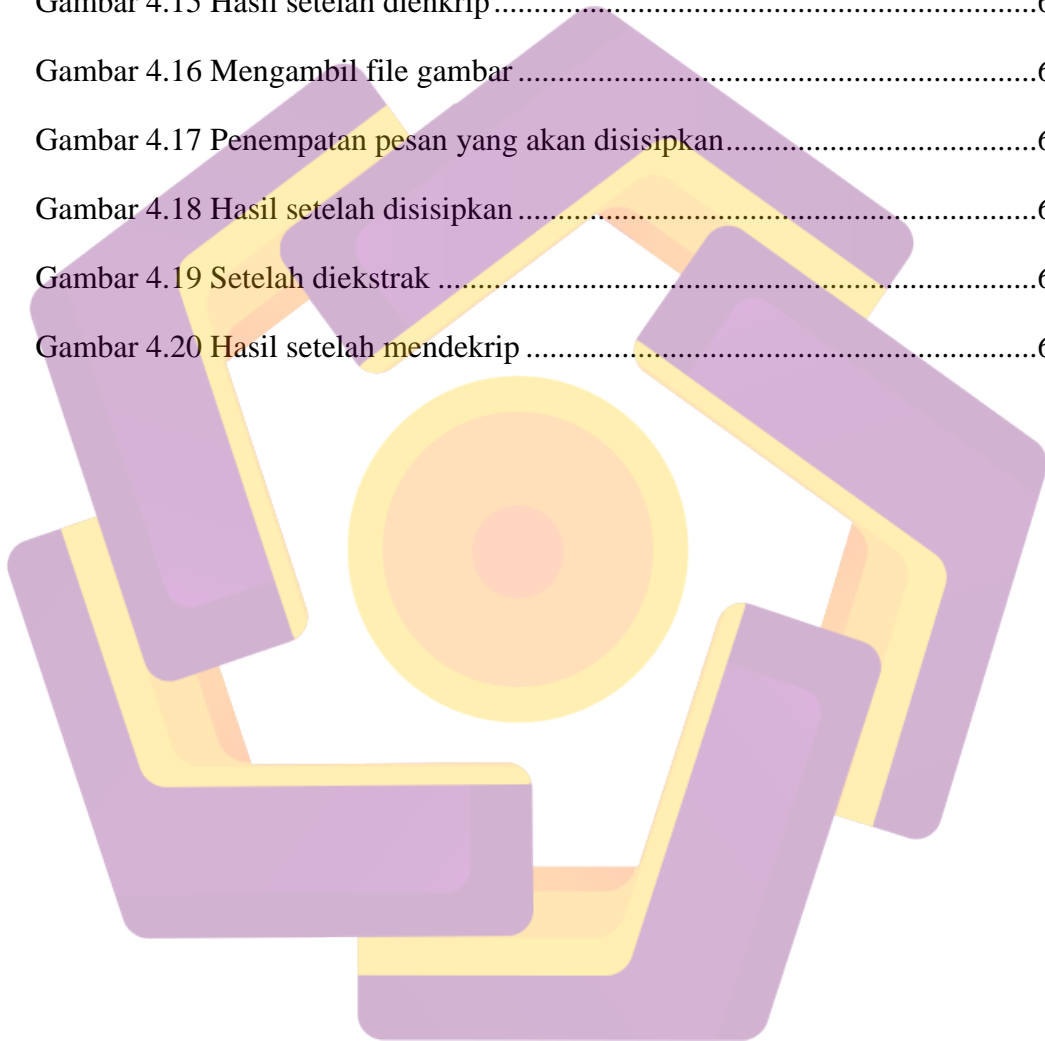
Table 4.1 Perbandingan Ukuran Hasil Proses Penyisipan Pesan.....	51
Tabel 4.2 Perbandingan waktu proses Kriptografi <i>DES</i>	52
Tabel 4.3 Perbandingann waku proses <i>watermark</i>	52



DAFTAR GAMBAR

Gambar 2.1 Skema Algoritma Simetris	8
Gambar 2.2 Skema Global Algoritma <i>DES</i>	10
Gambar 2.3 Skema Algoritma Enkripsi <i>DES</i>	11
Gambar 2.4 Proses <i>Watermark</i>	13
Gambar 2.5 <i>Digital Image Watermark</i>	16
Gambar 3.1 Use Case Aplikasi <i>Watermark</i>	30
Gambar 3.2 Class Diagram Aplikasi <i>Watermark</i>	31
Gambar 3.3 Flowchart enkrip dan dekrip pada pesan.....	32
Gambar 3.4 Flowchart Sisip dan ekstrak pesan	32
Gambar 3.5 Flowchart enkrip dan dekrip <i>DES</i>	36
Gambar 3.6 Proses Pembangkitan kunci internal <i>DES</i>	39
Gambar 3.7 Rincian Komputasi fungsi <i>f</i>	40
Gambar 3.8 Flowchart metode <i>LSB</i>	43
Gambar 4.1 Perbandingan file *.gif	45
Gambar 4.2 Histogram file *.gif	46
Gambar 4.3 File *.gif kiri dan kanan	47
Gambar 4.4 Perbandingan file *.jpeg.....	48
Gambar 4.5 Histogram file *.jpeg.....	49
Gambar 4.6 Perbandingan file *.png.....	50
Gambar 4.7 Histogram file *.png.....	51
Gambar 4.8 File *.png kiri dan kanan.....	52
Gambar 4.9 File yang belum disisipi	53
Gambar 4.10 File yang disisipi data lebih besar dari penampung	54

Gambar 4.11 Grafik Perbandingan Waktu	56
Gambar 4.12 Aplikasi Enkrip dan Dekrip <i>DES</i>	61
Gambar 4.13 Aplikasi sisip dan ekstrak pesan	61
Gambar 4.14 Mengenkripsi pesan.....	62
Gambar 4.15 Hasil setelah dienkrip	63
Gambar 4.16 Mengambil file gambar	64
Gambar 4.17 Penempatan pesan yang akan disisipkan.....	64
Gambar 4.18 Hasil setelah disisipkan	65
Gambar 4.19 Setelah diekstrak	66
Gambar 4.20 Hasil setelah mendekrip	66



INTISARI

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 dan rahasia. Kehidupan sekarang, orang-orang banyak yang menyimpan suatu pesan pada media *digital* dan menggunakan kode-kode tertentu. *DES(Data Encryption Standard)* 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* metode *LSB(Least Significant Bit)* dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan.

Penelitian ini dibagi menjadi 3 tahap. Pertama adalah implementasi dari algoritma *DES* dan *Watermark LSB* dalam bahasa pemrograman java. Dilanjutkan dengan mengamati perbedaan media citra antara sebelum dan sesudah disisipkan pesan yang terenkripsi dengan *DES*. Media citra yang merupakan tempat penyisipan pesan menggunakan ekstensi file gambar *jpeg*, *gif*, dan *png*. Tahap terakhir adalah mengukur seberapa cepat kinerja dari proses dalam satuan detik pada beberapa ekstensi file gambar yang berbeda.

Dari hasil pengujian, didapat bahwa implementasi yang dilakukan di system operasi *Windows* berhasil. Kualitas gambar sebelum dan sesudah disisipi tidak dapat dibedakan dengan hanya dilihat mata manusia secara langsung. Tetapi bisa dibedakan dengan melihat informasi dari histogram. Kinerja proses yang didapat dengan memproses 100 karakter, rata-rata kurang dari sama dengan 1 detik.

Kata Kunci: Kriptografi, Algoritma *DES*, *Data Encryption Standard*, *Watermark*, *LSB(Least Significant Bit)*, *Watermark* gambar, informasi rahasia.

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