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 Alloh penguasa sekalian alam, segala puja dan puji sykur adalah milikMU "Alloh 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 tingi 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 hinga 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 idak 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

DAFTAR TABEL

DAFTAR GAMBAR

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 pemrograma 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 disispi 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*