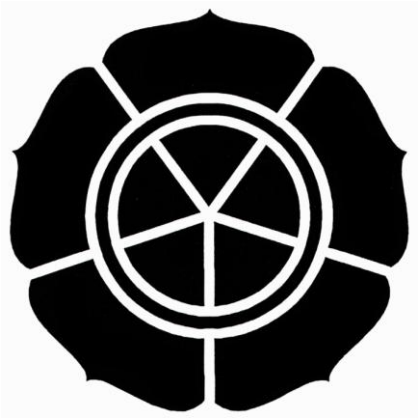
IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN WATERMARK DENGAN METODE LSB PADA DATA CITRA

SKRIPSI



disusun oleh

Joko Tri Purwanto

10.11.4561

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN WATERMARK DENGAN METODE LSB PADA DATA CITRA

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Joko Tri Purwanto

10.11.4561

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013

PERSETUJUAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN WATERMARK DENGAN METODE LSB PADA DATA CITRA

yang dipersiapkan dan disusun oleh

Joko Tri Purwanto

10.11.4561

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 23 Februari 2013

Dosen Pembimbing,

Ema Utami, Dr., S.Si, M.Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN WATERMARK DENGAN METODE LSB PADA DATA CITRA

yang dipersiapkan dan disusun oleh

Joko Tri Purwanto

10.11.4561

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 November 2013

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Bayu Setiaji, M.Kom. **NIK. 190302216**	
Ferry Wahyu Wibowo, S.Si., M.Cs. **NIK. 190302207**	
Ema Utami, Dr., S.Si, M.Kom. **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjanah Komputer
Tanggal 25 November 2013

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN KEASLIAN

Saya yang bertanda tanggan 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 atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan desebutkan dalam daftar pustaka.

Yogyakarta, 2 Desember 2013

Joko Tri Purwanto

NIM. 10.11.4561

MOTTO

“ Kemenangan dan atau keberhasilan hanya dapat di capai dengan kesabaran”

“Penghargaan tertinggi manusia adalah manusia yang selalu menghargai usaha dan jerih payah orang lain”

“Kegagalan hanya terjadi bila kita menyerah *(Lessing)”*

“Pendidikan merupakan perlengkapan paling baik untuk hari tua. *(Aristoteles)”*

“Berusahalah jangan sampai terlengah walau sedetik saja, karena atas kelengahan kita tak akan bisa dikembalikan seperti semula.”

PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dengan mengucap syukur Alhamdulillah, kupersembahkan karya kecilku ini untuk orang-orang yang kusayangi :

1. Ayah dan Ibuku tercinta, motivator terbesar dalam hidupku yang tak pernah jemu mendo'akan dan menyayangiku, atas semua pengorbanan dan kesabaran mengantarku sampai kini. Tak pernah cukup ku membalas cinta ayah dan Ibu padaku.
2. Mas Eko Agus Harianto dan Mbak Retno Widiastuti yang tiada henti memberikan dorongan serta mendo'akanku sampai skripsi ini selesai.
3. Sahabat terbaikku Aerton Sena P yang selama ini mendukungku
4. Teman-teman ku yang selalu kubanggakan

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Ucapan puji syukur kepada Allah Azza Wa'Jala atas semua karunia yang diberikan sehingga dengan inayahnya serta bimbingannya dapat terselesaikan skripsi ini. Shalawat serta salam diucapkan kepada baginda Nabi Agung Muhammad SAW semoga Allah selalu memberikan safaat kepada beliau berserta keluarga dan para sahabatnya. Atas petunjuk Allah Skripsi yang berjudul "Implementasi Algoritma Kriptografi AES dan Watermak Dengan Metode LBS Pada Data Citra" ini dapat terselesaikan dengan baik.

Adapun tujuan penyusunan laporan skripsi ini adalah untuk untuk menganalisis kinerja dan perfoma algoritma AES dan Watermark metode LBS dengan data terbatas. Laporan ini juga disusun sebagai salah satu syarat kelulusan Program Studi Teknik Informatika Jejang S-1 STMIK Amikom Yogyakarta.

Dalam penulisan laporan ini penulis banyak mendapatkan sumbangan pikiran, fasilitas, dorongan moril dan spiritual serta arahan dan bimbingan dari berbagai pihak. Pada kesempatan ini penulis ingin mengucapkan terimakasih kepada :

1. Ayah, Ibu Mas Agus, Mbak Nani, Mbak Retno, Mas Sigityang telah memberikan semangat serta tuntunan, bimbingan dan kasih saying kepadaku. Semoga Allah SWT memberikan kepada kalian kebahagiaan di dunia dan menyiapkan indahnya syurga.
2. Ibu Ema Utami Dr.,S.Si., M.Kom. yang telah membantu dan mendampingi sampai pendadaran, memberikan saran, masukan dan revisi sampai skripsi ini terselesaikan.
3. Bapak dan ibu Dosen Teknik Informatika yang telah memberikan semangat dan dorongan.
4. Sahabat sejatiku Aerton Sena P yang selalu memberikan dorongan motivasi serta mendoakan dan semangat tiada henti.
5. Teman-teman kulianku S1TI-12 yang selalu memberikan dorongan serta mendoakanku.

6. Teman-teman Organisasi PPA, Veri, Erwan, Fendy, doharma, Irfan, Ryan, Badri, Ardian, Tegar, Aditya, Rimo, Dava, Faizal yang selalu memberikan masukan dan bantuan serta dorongan untuk terus semangat mengerjakan skripsi ini. Semoga kalian semua menuji hari esok yang lebih baik.
7. Serta semua pihak yang tidak bisa penulis sebutkan satu persatu. Terimakasih atas semuanya. Penulis tidak akan berarti apa-apa tanpa kalian semua.

Terakhir penulis ingin memanjatkan doa, semoga laporan ini bermanfaat bagi semua pihak yang membutuhkan.

Wassalamu'alaikum Wr. Wb

Magelang, 2 Desember 2013

Penulis

Joko Tri Purwanto

NIM. 10.11.4561

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

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.

Adanya masalah di atas memunculkan ilmu baru pada dunia informatika yang disebut kriptografi. Berbagai pakar kriptografi telah mengembangkan berbagai macam algoritma enkripsi. AES (*Advanced encryption standar)* merupakan algoritma yang pernah menjadi sangat terkenal di Amerika dan pernah menjadi keamanan dasar yang digunakan di seluruh dunia. Kelemahan AES sendiri pesan yang sudah disandikan bisa dilihat dengan kasat mata. Sedangkan teknik Watermak dengan metode LBS (*Least Significant Bit)* merupakan suatu solusi didalam melindungi kerahasiaan dengan cara menyembunyikan pesan pada gambar. Keunggulan teknik Watermak sendiri pesan tidak dapat dilihat dengan kasat mata.

Pesan yang di acak mengunakan algoritma AES dan sembunyikan/ disisipkan pada gambar merupakan pengaman data yang berlapis. Perbandingan file gambar yang disisipi pesan dengan file gambar yang belum disisipi pesan hampir tidak bisa dibedakan dengan kasat mata. Tidak membutuhkan waktu yang cukup lama dalam penyisipan pesan. Oleh karena itu perfoma penggabungan teknik kriptografi algoritma AES dan Watermaking dengan metode LBS merupakan alternative dalam pengamanan pesan.

Kata Kunci : Kriptografi, Algoritma AES, Watermark, Metode Least Significant Bit

ABSTRACT

The presence of computers give more attention not only in data processing but also the security of data . Computer network technologies currently evolving , allowing one computer to connect to other computers in different parts of the world to share data and information .

The above problems led to new knowledge on the world of informatics is called cryptography . Various experts have developed a wide range of cryptographic encryption algorithms . AES (Advanced Encryption Standard) is an algorithm that never became very well known in America and has been the basis of security that is used throughout the world . AES own weaknesses that have been encoded message can be seen with the naked eye . Meanwhile, the watermark technique LBS method (Least Significant Bit) is a solution in protecting confidentiality in a way to hide messages in images . The advantages of the technique itself watermark message can not be seen with the naked eye .

The message at random using the AES algorithm and hide / pasted the image is layered data security . Comparison of image files inserted message with an image that has not been inserted messages could hardly be distinguished with the naked eye . It did not take long in the insertion of the message . Therefore performer merging algorithm AES cryptographic techniques and Watermaking with LBS is an alternative method of securing messages .

***Keyword** : Kriptografi, Algoritma AES, Watermark, Metode Least Significant Bit*