PROTOTIPE VALIDASI DAN PROTEKSI DATA PADA FILE IMAGE DENGAN MENGGUNAKAN ADVANCED ENCRYPTION STANDARD DAN LEAST SIGNIFICANT BIT BERBASIS ANDROID

TESIS

Oleh:

Akbar Muchbarak
1211601677

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2015

PROTOTIPE VALIDASI DAN PROTEKSI DATA PADA FILE IMAGE DENGAN MENGGUNAKAN ADVANCED ENCRYPTION STANDARD DAN LEAST SIGNIFICANT BIT BERBASIS ANDROID

TESIS

Diajukan untuk memenuhi salah satu persyaratan memperoleh gelar

Magister Ilmu Komputer (MKOM)

Oleh:
Akbar Muchbarak
1211601677

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2015

PROGRAM STUDI:MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini,

Nama	: Akbar Muchbarak
NIM	: 1211601677
Program Studi	: Magister Ilmu Komputer
Konsentrasi	: Rekayasa Komputasi Terapan
Fakultas/ Program	: Pasca Sarjana

Menyatakan bahwa TESIS yang berjudul :

PROTOTIPE VALIDASI DAN PROTEKSI DATA PADA FILE IMAGE DENGAN MENGGUNAKAN ADVANCED ENCRYPTION STANDARD DAN LEAST SIGNIFICANT BIT BERBASIS ANDROID

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan hasil karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta, 20 Februari 2015

METERAI TEMPEL 6000 ENAM RIBU RUPIAH

(Akbar Muchbarak)

PROGRAM STUDI:MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama	:	Akbar Muchbarak
NIM	:	1211601677
Konsentrasi	:	Rekayasa Komputasi Terapan
Jenjang Studi	:	Strata 2
Judul	:	Prototipe Validasi Dan Proteksi Data Pada File *Image* Dengan Menggunakan *Advanced Encryption Standard* Dan *Least Significant Bit* Berbasis Android

Jakarta, 7 Maret 2015

Tim Penguji :	Tanda tangan :
Ketua, Prof. Dr. Moedjiono, M.Sc	.....
Anggota / Pembimbing Utama, Dr. Ir. Nazori Az, M.T	.....
Pembimbing Pendamping, Mardi Hardjianto, M.Kom	.....

Ketua Program Studi

Dr. Ir. Nazori Az, M.T

ABSTRAK

Dalam sebuah *image* kita dapat menyimpan beberapa informasi seperti waktu dan lokasi pengambilan gambar. Informasi yang secara otomatis tersimpan saat mengambil sebuah gambar salah satunya yaitu *geolocation. Geolocation* dapat kita gunakan untuk mengetahui dimana posisi kita saat mengambil gambar tersebut. Informasi tersebut disimpan dalam metadata yang biasa disebut EXIF, namun informasi yang dapat disimpan sangat terbatas. Selain terbatasnya informasi yang dapat disimpan, keamanan data juga menjadi masalah. Teknik untuk penyimpanan dan pengamanan pesan yang lebih baik dapat menggunakan steganografi. Sedangkan salah satu cara pengamanan data pesan dapat dilakukan dengan kombinasi teknik keamanan kriptografi dan steganografi. Dengan kombinasi tersebut, pesan rahasia berupa teks atau *file* terlebih dahulu dienkripsi dengan algoritma AES, kemudian hasil enkripsi menggunakan AES tersebut disembunyikan ke dalam media citra digital dengan metode LSB. Penerapan metode steganografi ditambah dengan penerapan algoritma kriptografi bertujuan untuk lebih meningkatkan proteksi pesan rahasia dari akses yang tidak berhak. Penelitian ini menghasilkan sebuah prototipe aplikasi penyimpanan informasi dan pesan rahasia berbasis Android menggunakan metode LSB dan AES.

Kata Kunci : Steganografi, *Least Significan Bit (LSB)*, Kriptografi, *Advanced Encryption Standard (AES), Geolocation*

ABSTRACT

In an image we may store some information such as the time and location of the image. The information is automatically stored while taking a picture of one of them is geolocation. Geolocation can be used to find out where we are currently taking these pictures. Such information is stored in a so-called EXIF metadata, but the information can be kept very limited. In addition to the limited information that can be stored, data security is also an issue. Storage and security techniques for better message can use steganography. While one way of securing data messages can be done with a combination of cryptography and steganography security techniques. With that combination, the secret message in the form of text or file first encrypted with the AES algorithm, then encrypted using the AES hidden into media digital image with the LSB method. Application of steganography method coupled with the implementation of cryptographic algorithms aim to further improve the protection of secret messages from unauthorized access. This study produced a prototype application information storage and Android-based secret message using the LSB and AES

Keyword : Steganography , Least Significan Bit (LSB), Cryptoraphy, Advanced Encryption Standard (AES), Geolocation

KATA PENGANTAR

Puji dan Syukur yang sedalam-dalamnya kepada Allah SWT, karena hanya dengan rahmat dan karunia-Nya-lah naskah tesis yang berjudul "Prototipe Validasi Dan Proteksi Data Pada File Image Dengan Menggunakan *Advanced Encryption Standard* Dan *Least Significant Bit* Berbasis Android" dapat diselesaikan. Shalawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu.

Dalam penyusunan tesis ini, penulis menyampaikan terima kasih yang tulus kepada:

1. Orang tua dan keluarga yang senantiasa memberikan kasih sayang, nasihat, dukungan semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
2. Penny Purwanti yang menjadi wanita spesial dalam hidup saya, yang selalu memberi semangat dan dukungannya hingga saya lebih termotivasi untuk sesegera mungkin meyelesaikan tesis ini.
3. Bapak Prof Moedjiono, M.Sc, selaku Direktur Program Pascasarjana Universitas Budi Luhur.
4. Bapak Dr. Ir. Nazori AZ, M.T. selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur dan selaku pembimbing yang banyak membimbing dan memberi masukan dalam penyusunan tesis ini..
5. Bapak Mardi Hardjianto, M.Kom, selaku pembimbing tesis yang banyak memberikan bimbingan, bantuan dan tak henti-hentinya memberikan dukungan.
6. Teman-teman seperjuangan tesis Aam, Doli, Mas Shaka, Mba Chiquita, Amie, Ryan dan teman-teman Universitas Budiluhur yang selalu memberikan dukungan, kebahagiaan dan keceriaan.
7. Teman-teman tim Explorindo Total Solusi, Doli, Amie, Indra, Iskandar, Makin, Mas Shandy, Kang Asep, Pak Dwiana dan lainnya namun tidak bisa disebutkan satu persatu yang selalu memberikan masukan dan dukungannya selama pengerjaan tesis ini.

9. Seluruh Dosen Program Magister Ilmu Komputer Universitas Budi Luhur yang banyak memberikan ilmu selama perkuliahan.
10. Serta semua pihak yang tidak dapat dituliskan.

Penulis menyadari bahwa penulisan tesis ini jauh dari sempurna. Untuk itu penulis berharap mendapatkan kritik dan saran yang dapat berguna untuk membangun demi kesempurnaan tulisan tesis ini.

Jakarta, Februari 2015

Akbar Muchbarak

DAFTAR ISI

DAFTAR GAMBAR

Gambar **Hal**

DAFTAR TABEL

DAFTAR LAMPIRAN

Lampiran Halaman

DAFTAR PUSTAKA

[Abutaha, 2011] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh, India, "Survey Paper: Cryptography Is The Science Of Information Security", International Journal of Computer Science and Security (IJCSS), Vol. 5, 2011

[Agnes, 2014] Aryasanti Agnes dan Mardi Hardjianto, "Model Pengamanan Berkas Bank Soal dengan Metode Steganografi LSB Dan Kompresi", Jurnal TICOM Vol.2 No.2, 2014

[Ary 2012] Ary Budi Warsito, Lusi Fajarita, Nazori AZ, Maret 2012, "Proteksi Keamanan Dokumen Sertifikat File JPEG pada perguruan tinggi dengan menggunakan Steganografi dan Kriptografi", Jurnal TELEMATIKA MKOM Vol.4 No.1,Maret 2012.

[Cahyadi, 2012] Tri Cahyadi, "Implementasi Steganography dengan enkripsi Vigener Cipher pada Citra JPEG", Semarang: 2012.

[Derwin, 2012] Derwin Suhartono, Afan Galih Salman, Rojali, Christian Actavianus, April 2010, "Aplikasi Penyembunyian Pesan pada Citra JPEG dengan Algoritma F5 dalam Perangkat Mobile berbasi Android", Seminar Nasional Aplikasi Teknologi Informasi, 2012.

[Didi, 2006] Didi Surian, "Algoritma Kriptografi AES Rijndael", Jurnal Teknik Elektro, TESLA Vol.8, No.2, 97-101, Oktober 2006..

[Ekta, 2010] Dr. Ekta Walia, Payal Jaim, Navdeep, April 2010, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, 2010.

[Goel, 2013] Mukta Goel, Rohit Goel, February 2013, Technological Institute of Textile & Science, Bhiwani, Haryana India, "Current Image Steganography Techniques for Higher Compression and Robustness", International Journal of Computer Science & Information Technology, Vol.3, No.2, Februari 2013.

[Gutub, 2010] Adnan Abdul-Aziz Gutub, King Saudi University, Saudi, Arabia, "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol.2, No.1, Februari 2010.