

**PROTOTYPE "PENGAMANAN GANDA"
PESAN RAHASIA DENGAN MENGGUNAKAN TEKNIK
STEGANOGRAFI METODE LSB DAN KRIPTOGRAFI
METODE *VIGENERE CIPHER***

TESIS



Oleh:

AGUNG WIBOWO

1111600787

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR**

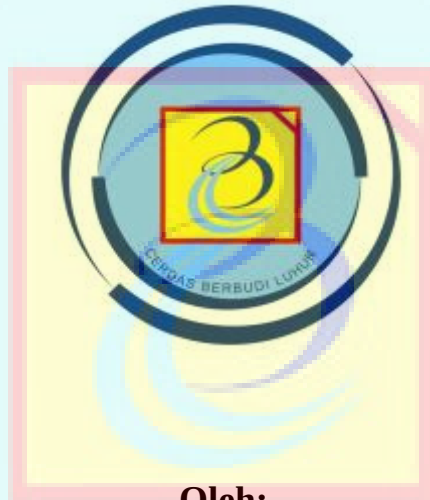
JAKARTA

2014

**PROTOTYPE "PENGAMANAN GANDA"
PESAN RAHASIA DENGAN MENGGUNAKAN TEKNIK
STEGANOGRAFI METODE LSB DAN KRIPTOGRAFI
METODE VIGENERE CIPHER**

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelas Magister Ilmu Komputer (MKom)



Oleh:

AGUNG WIBOWO

1111600787

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR**

JAKARTA

2014



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

LEMBAR PENGESAHAN

NAMA MAHASISWA : AGUNG WIBOWO
NIM : 1111600787
PROGRAM STUDI : MAGISTER ILMU KOMPUTER
JENJANG STUDI : S2

MENYATAKAN BAHWA TESIS YANG BERJUDUL :

PROTOTYPE "PENGAMANAN GANDA" PESAN RAHASIA DENGAN
MENGUNAKAN TEKNIK **STEGANOGRAFI METODE LSB** DAN KRIPTOGRAFI
METODE VIGENERE CIPHER

Jakarta, 22 Februari 2014

Tim Penguji :

Ketua

Penguji I,

Ir. Dana Indra Sensuse, Ph.D

Penguji II,

Samidi, MM, M.Kom

Moderator

Dr. Ir. Nazori Az, M.T

Tanda Tangan :

Ketua Program Studi

Dr. Ir. Nazori Az, M.T



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

LEMBAR PERNYATAAN

NAMA MAHASISWA : AGUNG WIBOWO

NIM : 1111600787

PROGRAM STUDI : MAGISTER ILMU KOMPUTER

FAKULTAS / PROGRAM : REKAYASA KOMPUTASI TERAPAN

MENYATAKAN BAHWA TESIS YANG BERJUDUL :

PROTOTYPE "PENGAMANAN GANDA" PESAN KAHASIA
DENGAN MENGGUNAKAN TEKNIK SAE SANDSKAEI METODE
LSB DAN KRIPTOGRAFI METODE VIGENERE CIPHER

1. Merupakan hasil karya tulis sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya ijin 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 dengan aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 22 Februari 2014



KATA PENGANTAR

Assalamu'alaikum wr, wb.

Segala puji hanya milik Allah SWT dan sudah selayaknya pujian itu kita sampaikan hanya kepadaNya. Dengan izinNya pula, tesis yang berjudul **“PROTOTYPE "PENGAMANAN GANDA" PESAN RAHASIA DENGAN MENGGUNAKAN TEKNIK STEGANOGRAFI METODE LSB DAN KRIPTOGRAFI METODE VIGENERE CIPHER”** ini dapat diselesaikan. Dalam penyusunan naskah akhir tesis ini, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Allah SWT, atas segala rahmat dan izinNya;
2. Kedua orang tua, Bpk. H. Suropto dan Ibu HJ. Nunung Suningsih, Kedua saudaraku, Setyo Dwi Nugroho S.Kom dan Bayu Nurahman serta istri tercinta Nidaul Chasanah S.E. atas semua dukungan serta doanya;
3. Bapak Dr. Setyawan Widyarto, M.Sc., Ph.D, selaku pembimbing yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
4. Bapak Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
5. Serta semua pihak yang tidak dapat dituliskan.

Wassalamu'alaikum wr, wb.

Jakarta, Februari 2014

Agung Wibowo

DAFTAR ISI

	Hal
ABSTRAK	i
KATA PENGANTAR.....	iii
DAFTAR ISI	iv
DAFTAR GAMBAR.....	vii
DAFTAR TABEL.....	ix
BAB I. PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Masalah Penelitian	2
1.2.1 Identifikasi Masalah	2
1.2.2 Pembatasan Masalah	3
1.2.3 Rumusan Masalah	3
1.3 Tujuan dan Manfaat Penelitian	3
1.3.1 Tujuan Penelitian	3
1.3.2 Manfaat Peneliti	4
1.4 Tata Urut Penulisa	4
1.5 Daftar Pengertian.....	5
BAB II . LANDASAN PEMIKIRAN	
2.1 Tinjauan Pustaka	6
2.1.1 Steganografi	6
2.1.1.1 Pesan	7
2.1.1.2 Citra digital	8
2.1.2 LSB (<i>Least Significant Bit</i>)	12
2.1.3 Kriptografi	14
2.1.4 Vigenere Cipher.....	17
2.1.5 Pengamanan Ganda	19
2.1.6 Pengembangan Prototype	21
2.1.7 ISO 9126	23

2.2	Tinjauan Studi	24
2.3	Tinjauan Objek Penelitian	31
2.4	Pola Pikir	32
2.5	Hipotesis	34
BAB III	. METODELOGI PENELITIAN.....	35
3.1	Metode Penelitian	35
3.2	Metode Pengumpulan Data	35
3.3	Instumentasi	36
3.4	Teknik Analisis Data	36
3.5	Langkah Langkah Penelitian.....	36
3.6	Jadwal Penelitian	42
BAB IV	. ANALISIS, INTERPETASI, DAN IMPLIKASI PENELITIAN	
4.1	Analisis Sistem.....	44
4.1.1	Actor	44
4.1.2	Use Case Diagram	45
4.1.3	Activity Diagram	50
4.2	Perancangan Sistem	53
4.2.1	Perancangan Teknik	53
4.2.2	Perancangna Layar Aplikasi	55
4.3	Instumentasi Sistem.....	58
4.3.1	Spesifikasi Perangkat Keras	58
4.3.2	Spesifikasi Perangkat Lunak	59
4.3.3	Implementasi Program	59
4.4	Pengujian Sistem ..	68
4.4.1	Pengujian Black Box	68
4.4.2	Pengujiann PSNR dan MSE	73
4.4.3	Pengujian ISO 9126	77
4.5	Implikasi Penelitian	82
4.5.1	Aspek Sistem	82
4.5.2	Aspek Manajerial	83

4.5.3 Aspek Penelitian Lanjutan	83
4.6 Rencana Implementasi.....	85
BAB V . PENUTUP	87
5.1 Kesimpulan.....	87
5.2 Saran	88
5.3 Rencana Implementasi	88
DAFTAR PUSTAKA	90
LAMPIRAN	93



DAFTAR GAMBAR

	Hal
gambar II.1 : Contoh gambar <i>cover image</i> dan <i>stego-image</i>	7
gambar II.2 : Citra Biner	8
gambar II.3 : Representasi Citra Biner	8
gambar II.4 : Citra <i>Grayscale</i>	9
gambar II.5 : Citra Berwarna	10
gambar II.6 : Ilustrasi Dasar Konsep Steganografi LSB	11
gambar II.7 : <i>Bit</i> pada MSB dan LSB	12
gambar II.8 : Contoh <i>Tabula Recta Vigenere Cipher</i>	18
gambar II.9 : Pola Pikir	33
gambar III.1 : Langkah-langkah penelitian	37
gambar III.2: <i>Flowchart</i> Sistem yang dikembangkan	40
gambar IV.1 : <i>Encode Stegano and krypto message use case diagram</i>	37
gambar IV.2 : <i>Decode Stegano and krypto message use case diagram</i>	48
gambar IV.3 : <i>Activity diagram</i> aplikasi pesan rahasia dengan Steganografi dan kriptografi	51
gambar IV.4 : <i>Sequence diagram</i> pengirim aplikasi pesan rahasia dengan Steganografi dan kriptografi	52
gambar IV.5 : <i>Sequence diagram</i> penerima aplikasi pesan rahasia dengan Steganografi dan kriptografi	52
gambar IV.6: Proses pesan rahasia teknik Steganografi metode LSB (<i>Least Significant Bit</i>) dan teknik Kriptografi metode <i>Vigenere Cipher</i> yang dikembangkan	54
gambar IV.7 : Rancangan layar halaman depan	55
gambar IV.8: Rancangan layar “Buat pesan Rahasia”.....	56
gambar IV.9: Rancangan layar “Tampilkan Pesan Rahasia”.....	57
gambar IV.10: Tampilan halaman utama aplikasi	60
gambar IV.11: Tampilan halaman “Buat pesan Rahasia”	64
gambar IV.12: Tampilan memilih “Tampilkan pesan Rahasia”.....	67

gambar IV.13: Tampilan <i>show all</i> "	68
gambar IV.134 Tampilan <i>chart diagram PSNR dan MSE</i>	76



DAFTAR TABEL

	Hal
tabel II.1 : Karakteristik software berkualitas menurut ISO 9126	24
tabel II.2: Ringkasan Penelitian Terkait	28
tabel III.1: Jadwal Penelitian	42
tabel IV.1 <i>Encode Stegano and krypto message use case diagram.</i>	47
tabel IV.2 <i>Decode Stegano and krypto message use case diagram.</i>	49
tabel IV-3 Spesifikasi Perangkat Keras.	58
tabel IV.4 Spesifikasi perangkat lunak	58
tabel IV-5 Hasil pengujian <i>black box</i> proses <i>encode metode vigenere chipper</i>	69
tabel IV-6 Hasil pengujian <i>black box</i> proses Encode metode LSB	70
tabel IV-7 Hasil pengujian <i>black box</i> proses <i>decode metode LSB</i>	71
tabel IV-8 Hasil pengujian <i>black box</i> proses <i>decode metode vigenere chipper</i>	72
tabel IV-9 Hasil pengujian PSNR (<i>peak signal to noise rasio</i>) dan MSE (<i>mean square error</i>)	74
tabel IV-10 Hasil pengujian <i>black box</i> proses <i>decode metode LSB</i>	71
tabel IV-11 Pengujian kualitas ISO 9126 <i>functionality</i>	78
tabel IV-12 Pengujian kualitas ISO 9126 <i>Usability</i>	80
tabel IV-13 Pengujian kualitas ISO 9126 <i>Efficiency</i>	81
tabel IV-14 Pengujian kualitas ISO 9126 secara keseluruhan	81

ABSTRAK

Saat ini teknologi informasi sudah sangat berkembang menjadi salah satu media yang paling populer didunia. dengan semakin berkembangnya teknologi informasi semakin berkembang pula tindak penyalahgunaan informasi yang bukan haknya. Maka dari itu perkembangan teknologi informasi harus juga dibarengi dengan perkembangan pengaman informasi seperti pesan rahasia. Salah satu cara pengamanan data pesan dapat dilakukan dengan kombinasi Teknik keamanan kriptografi dan steganografi. Tujuannya adalah untuk merahasiakan sebuah pesan. proses kombinasi kriptografi dan steganografi diyakini sebagai cara ampuh untuk melindungi pesan yang dikirim, serta sekaligus menghindari pesan tersebut dari kecurigaan. Pesan yang digunakan dalam tesis ini berupa text. pada proses kriptografi, pesan yang berupa text akan dienkrip dengan metode *Vigenere Cipher*. selanjutnya pesan yang ter enkrip tersebut akan disembunyikan dengan proses steganografi pada citra digital dengan metode *Least Significan Bit (LSB)*. Hasil dari aplikasi ini adalah dapat menyisipkan pesan tersembunyi berupa text ke dalam berkas citra digital berformat BMP, JPG, Gif dan dapat mengekstraksi kembali pesan tersembunyi tersebut dari dalam citra (*stego-image*).

Kata Kunci : Kriptografi, Steganografi , *Vigenere Cipher*, *Least Significan Bit (LSB)*, Pesan rahasia.



ABSTRACT

Today information technology has growing into one of the world's most popular media. with the development of information technology is growing also acts misuse of information that is not right. then from development of information technology should also be coupled with the development of information security such as secret message. One way of securing data messages can be done with a combination of cryptography and steganography security techniques. The goal is to keep a message. the combination of cryptography and steganography believed to be a powerful way to protect messages sent and simultaneously avoid the message from suspicion. Messages are used in this thesis in the form of text. the cryptographic process , a text message will be encrypted with the Vigenere Cipher method . subsequent encrypted messages will be hidden with steganography in digital image process methods signifikan Least Bit (LSB). The results of this application is to insert hidden messages into a text file digital image format BMP , JPG , Gif and can extract the hidden message of the image (stego-images).

keywords : cryptography, steganography, Vigenere Cipher, Least Significant Bit (LSB), secret message.



DAFTAR PUSTAKA

- [A. Menezes,] A. J Menezes, P. van Oorschot and S. Vanstone - *Handbook of Applied Cryptography* UK: CRC Press.
- [Ariyus 2006] Ariyus, Dony, *Kriptografi – Keamanan Data Dan Komunikasi*, Graha Ilmu, Yogyakarta, 2006.
- [Ariyus 2008] Ariyus, Dony, *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi*. Penerbit Andi, Yogyakarta, 2008.
- [Alatas 2009] Alatas, Putri, *Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital*, Universitas Gunadarma, Jakarta, 2009.
- [B.Tjaru 2012] B.Tjaru, Setia Negara, *Modifikasi Full Vigenere Chipher dengan Pengacakan Susunan Huruf pada Bujur Sangkar Berdasarkan Kunci*, ITB Bandung, 2012.
- [Eiji 2011] Eiji Kawaguchi, *Invitation to BPCS Steganography*, 2011, <http://datahide.com/BPCSe/index.html>, (Diakses 18 Juni 2013).
- [Kamdar 2012] G. Kamdar, Dolly Patira, Dr. C. H. Vithalani, *Dual Layer Data Hiding Using Cryptography And Steganography*, *International Journal of Scientific Engineering and Technology* (ISSN : 2277-1581) www.ijset.com, Volume No.1, Issue No.4, pg :134-138, Oktober 2012
- [Leonardo 2012] Leonardo, Kevin Handoyo, *Modifikasi Vigenere Cipher dengan Metode Penyisipan Kunci pada Plaintext*, ITB, Bandung, 2012.
- [Petitcolas 1999] A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, *Information Hiding -A Survey*, *Proceeding of the IEEE*, vol. 87, Issue 7, pp. 1062-1078, Juli 1999.
- [Prasetyo 2005] Prasetyo, Bambang dan Jannah, L.M., *Metode Penelitian Kuantitatif*, Jakarta: PT. Rajagrafindo Persada, 2005.
- [Ramadhani 2006] Ramadhani, Budi, *Steganografi pada Citra GIF menggunakan bahasa pemrograman Delphi*, UII, Yogyakarta, 2006.
- [Rosziati 2012] Rosziati Ibrahim and Law Chia Kee, *MoBiSiS: An-Android based Application for Sending Stego Image through MMS*, *ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology*, 2012.