

**PENGGABUNGAN TEKNIK STEGANOGRAFI DAN
KRIPTOGRAFI UNTUK KEAMANAN DATA
MENGUNAKAN MICROSOFT ACCESS:
STUDI KASUS PT. PANASONIC INDUSTRIAL DEVICES INDONESIA (PIDID)**

TESIS



Oleh :

**MUHAMMAD RIFQI
1111601488**

**PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2013**

**PENGGABUNGAN TEKNIK STEGANOGRAFI DAN
KRIPTOGRAFI UNTUK KEAMANAN DATA
MENGUNAKAN MICROSOFT ACCESS:
STUDI KASUS PT. PANASONIC INDUSTRIAL DEVICES INDONESIA (PIDID)**

TESIS

**Diajukan Untuk Memenuhi Salah Satu Persyaratan Memperoleh
Gelar Magister Ilmu Komputer (M.Kom)**



Oleh :

**MUHAMMAD RIFQI
1111601488**

**PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2013**



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

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Muhammad Rifqi
Nomor Induk Mahasiswa : 1111601488
Program Studi : Magister Ilmu Komputer
Konsentrasi : Rekayasa Komputasi Terapan
Fakultas/Program : Strata 2

menyatakan bahwa TESIS yang berjudul :

Penggabungan Teknik Steganografi Dan Kriptografi Untuk
Keamanan Data Menggunakan Microsoft Access :
Studi Kasus PT Panasonic Industrial Devices Indonesia
(PIDIO).

1. Merupakan hasil karya tulis ilmiah 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 aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta,


(MUHAMMAD RIFQI)



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

LEMBAR PENGESAHAN

Nama : Muhammad Rifqi
Nomor Induk Mahasiswa : 1111601488
Konsentrasi : Teknologi Ilmu Terapan
Jenjang Studi : Strata 2
Judul : Penggabungan Teknik Steganografi dan Kriptografi
Untuk Keamanan Data Menggunakan Microsoft
Access: Studi Kasus PT Panasonic Industrial Devices
Indonesia.

Jakarta, 04 September 2013

Tim Penguji:

Tanda tangan :

Ketua.
Dr. Moedjiono, M.Sc

Anggota,
Dr. Ir. Wendi Usino, M.Sc, MM

Pembimbing Utama,
Dr. Ir. Nazori, AZ, MT

Ketua Program Studi

Dr. Ir. Nazori, AZ, MT

ABSTRAK

Steganografi dan kriptografi adalah dua teknik yang berbeda yang menjaga kerahasiaan dan integritas data. Dalam dunia teknologi modern, pesan rahasia dapat disembunyikan di balik citra (image), misalnya pesan dapat dikodekan dalam low-order bit sehingga tidak mengganggu media gambar yang di kirimkan, metode ini di sebut dengan metode steganografi. Sedangkan kriptografi melindungi pesan dari individu yang tidak sah dengan mengubah artinya. Penerapan Sistem Metode Steganografi Bit *Least* signifikan bertujuan untuk menyediakan fasilitas keamanan data, terutama dalam hal menyembunyikan data yang ditujukan untuk perusahaan, bisnis maupun pribadi. Penelitian ini didasarkan pada peningkatan arus lalu lintas data paket pengiriman melalui email atau media lain yang berdampak langsung terhadap meningkatnya ancaman dan pencurian data. Penelitian ini dibentuk dengan metode penelitian eksperimental teknik pengumpulan data menggunakan literatur dan dokumentasi. Pendekatan pemecahan masalah dengan menggunakan identifikasi masalah untuk mencari solusi. Desain metode yang digunakan adalah rapid *Application Development* dengan menerapkan desain 5-langkah, yaitu pemodelan bisnis, pemodelan data, pemodelan proses, generasi dan pengujian aplikasi. Perangkat lunak ini dibangun dengan menggunakan Microsoft Access yang dapat menyembunyikan teks rahasia (*encrypt*) dan menampilkan teks (*decrypt*) pada gambar untuk keamanan data. Dengan menggunakan penggabungan teknik steganografi dan kriptografi pada pengiriman informasi rahasia dengan mengembangkan algoritma Caesar Chiper dapat menjamin kerahasiaan yang lebih baik dari ancaman dan pencurian data.

Kata kunci : Keamanan Data, Steganografi, Kriptografi, *Encryption*, *Decryption*, *Least Significant Bit (LSB)*

ABSTRACT

Steganography and cryptography are two different techniques that maintain the confidentiality and integrity of data. In the world of modern technology, secret message can be hidden behind the image, for example, a message can be encoded in the low-order bit so it doesn't interfere with media images as it travels, this method is called Steganography method. Whereas cryptography protects messages from unauthorized individuals by changing its meaning. Application of System Least Significant Bit Steganography Method aims to provide security for the data, especially in terms of hiding the data directed to the company, business or personal. The study was based on an increase in traffic flow packet data transmission via email or other media that directly impact on the increasing of threat and of data stealing. This research formed by experimental research method of data collection techniques using literature and documentation. Using a problem-solving approach to the identification of problems to find solutions. Design method used is Rapid Application Development by applying the 5-step design, the business modeling, data modeling, process modeling, generation and test application. The software is built using Microsoft Access that can hide a secret text (encrypt) and display text (decrypted) on the image for data security. By using steganography and cryptography combined techniques on transferring confidential information with developing a Caesar Cipher algorithm, it can guarantee better confidentiality of the threat and data stealing.

Keywords : Data Security, Steganography, Cryptography, Encryption, Decryption, Least Significant Bit (LSB).

KATA PEGANTAR



Alhamdulillahirobbil ‘alamiin, Segala puji dan syukur ke hadirat Allah yang telah melimpahkan rahmat dan karunia-Nya, shalawat dan salam semoga senantiasa tercurah kepada junjungan dan tauladan kita Muhammad Rasulullah, keluarga dan para sahabatnya.

Selesainya penyusunan tesis ini dengan Judul **“PENGGABUNGAN TEKNIK STEGANOGRAFI DAN KRIPTOGRAFI UNTUK KEAMANAN DATA MENGGUNAKAN MICROSOFT ACCESS STUDI KASUS : PT. PANASONIC INDUSTRIAL DEVICES INDONESIA (PIDID)”** tak luput dari peran serta dari Allah SWT juga dari peran serta ibu sebagai orang tua yang saya sayangi dan cintai, istri, anak-anak yang saya cintai dan juga para dosen pembimbing tentunya yang saya hormati. Ijinkan saya mengucapkan terima kasih dan penghargaan yang tinggi kepada :

1. Allah SWT, yang saya sadari sepenuhnya segala sesuatu atas izin dan ridho dari Allah Subhanallah Wa Ta ‘ala.
2. Kepada Ibunda Hj. Achyani yang saya cintai dan sayangi atas do’a dan dukungan nya kepada saya.
3. Istri tercintaku Misriyani, SSi, Apt. atas dorongan semangat yang tak pernah surut memotivasi sehingga selesainya tesis ini.
4. Anak-anak tercinta Rifani Nur Shabrina, Muhammad Raiyan Sani dan Muhammad Raihan yang memberikan arti tersendiri bagi saya yang tak ternilai harganya yang berperan ikut menyemangati saya dalam perkuliahan hingga selesai.
5. Bapak DR. Moedjiono, M.Sc, selaku Direktur Program Pasacarjana Universitas Budi Luhur.
6. Bapak. Dr. Ir. Nazori AZ, MT selaku Ketua Program Studi Magister Ilmu Komputer sekaligus pembimbing, yang telah meluangkan waktunya untuk membimbing sehingga penulis dapat menyelesaikan Tesis ini dengan tepat waktu.
7. Bapak Sutedy, selaku jajaran Manager pada PT Panasonic Industrial Devices Indonesia.
8. Teman-teman seperjuangan tentunya yang tidak saya sebutkan satu persatu yang tentunya tidak mengurangi rasa cinta dan hormat saya.

Semoga jasa baiknya dibalas pahala yang setimpal oleh Allah SWT.
Dengan penulisan tesis ini, semoga membawa manfaat bagi kita dan dapat memperkaya khasanah keilmuan kita, penghargaan tulus bagi anda apabila dapat memberikan saran, masukan dan kritik yang membangun guna penyempurnaan tulisan ini melalui email rifqi_muh99@yahoo.co.id karena tidak ada gading yang tidak retak.

Jakarta, Maret 2013
Penulis



LEMBAR PERSEMBAHAN

Karya ini ku persembahkan teruntuk ibunda ku tercinta, istriku yang kusayangi serta anak-anakku. Ibundaku yang tak pernah berhenti menyayangi dan menyemangati ku untuk terus belajar dan belajar hingga kini, walaupun terbaring lemah di tempat tidur karena di makan usia tidak menyurutkan beliau untuk memberikan support kepada anak-anaknya untuk terus maju, seperti halnya dengan diriku sebagai anak bungsu. Semua ke delapan anak-anaknya di perlakukan sama tanpa pandang bulu, jerih payah beliau sejak di tinggal ayah tidak sia-sia, Alhamdulillah berkat do'a dan pengorbanan beliau mengantarkan kesemua anak-anaknya seperti sekarang ini, juga tak lupa juga kepada istriku Misriyani yang dengan setia mendampingi dan juga menyemangatiku serta buah hatiku Rifani, Raiyan dan juga Raihan yang dengan kalian semualah menjadikan pemacu semangat untuk menggapai cita-cita dan impian.

Do'a dan harapanku padamu ya Allah, semoga Allah membalas segala kebaikan ibu ku lebih dari apa yang telah beliau berikan kepada anak-anaknya serta menyayanginya seperti beliau menyayangi anak-anaknya sewaktu kecil dan semoga ibundaku tercinta dapat mendampingi ku di acara wisuda strata sarjanaku nanti, diberikan kesembuhan atas penyakitnya serta diberikan kesehatan, demikian pula untuk istriku semoga dapat mendampingi dan menyaksikannya kelak. Peluk cium untuk kalian semua.

Jakarta, Maret 2013

DAFTAR ISI

Lembar Judul	
Lembar Pernyataan	
Lembar Pengesahan	
ABSTRAK.....	i
KATA PENGANTAR.....	iii
LEMBAR PERSEMBAHAN.....	iv
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	vii
DAFTAR TABEL.....	ix
DAFTAR LAMPIRAN.....	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Masalah Penelitian.....	7
1.2.1 Identifikasi Masalah.....	7
1.2.2 Batasan Masalah.....	8
1.2.3 Rumusan Masalah.....	9
1.3 Tujuan dan Manfaat Penelitian.....	9
1.3.1 Tujuan Penelitian.....	9
1.3.2 Manfaat Penelitian.....	10
1.4 Tata Urut Penulisan.....	10
1.5 Daftar Pengertian.....	11
BAB II LANDASAN TEORI.....	13
2.1 Tinjauan Pustaka.....	13
2.1.1 Pengertian Steganografi.....	13
2.1.2 Pengertian Kriptografi.....	15
2.1.2.1 Japanese Purple Machine.....	19
2.1.2.2 The German Enigma Machine.....	20
2.1.2.3 Enkripsi Kunci Rahasia.....	23
2.1.2.4 Substitusi.....	24
2.1.2.5 Transposisi.....	25
2.1.2.6 Vernam Cipher.....	25
2.1.2.7 Book Key Cipher.....	25
2.1.2.8 Codes.....	25
2.1.2.9 Pola-pola penyaringan Data.....	26
2.1.2.9.1 Interruption.....	26
2.1.2.9.2 Interception.....	26
2.1.2.9.3 Modification.....	26
2.1.2.9.4 Fabrication.....	26
2.2 Tinjauan Studi.....	29
2.3 Tinjauan Obyek Penelitian.....	36
2.4 Kerangka Konsep/Pola Pikir Pemecahan Masalah.....	38
2.5 Hipotesis.....	39
BAB III METODOLOGI DAN PERANCANGAN PENELITIAN.....	40

	3.1 Metode Penelitian.....	40
	3.2 Instrumentasi.....	40
	3.2.1 Hardware yang Digunakan.....	40
	3.2.2 Software yang Digunakan.....	41
	3.3 Langkah Penelitian.....	42
	3.4 Jadwal Penelitian.....	46
BAB IV	ANALISIS DAN PEMBAHASAN.....	47
	4. Gambaran Umum.....	47
	4.1 Klasifikasi Data/Informati PT Panasonic.....	48
	4.2 Hambatan/Kendala yang di hadapi.....	48
	4.3 Analisa Kebutuhan Implementasi Pengamanan Pesan Rahasia.....	48
	4.4 Rancangan Sistem.....	49
	4.4.1 Rancangan Menu Aplikasi.....	49
	4.4.2 Rancangan <i>Flowchart</i>	50
	4.4.4 Rancangan Antar Muka.....	51
	4.4.4.1 Modul Enkripsi.....	51
	4.4.4.2 Modul Dekripsi.....	52
	4.4.4.3 Modul <i>Check Character</i>	53
	4.4.5 Rancangan Siklus Pengembangan Sistem.....	53
	4.5 Simulasi dan Pengujian Keamanan Informasi Data.....	55
	4.5.1 Hasil Pengujian.....	56
	4.5.1.1 Pengujian Modul Enkripsi/ <i>encode</i>	57
	4.5.1.2 Pengujian Modul Dekripsi/ <i>decode</i>	59
	4.5.1.3 Pengujian Modul <i>Check Character</i>	60
	4.5.1.4 Pengujian Modul <i>New</i>	62
	4.5.2 Implementasi Sistem.....	62
	4.6 Implikasi Penelitian.....	74
	4.6.1 Aspek Sistem.....	74
	4.6.2 Aspek Manajerial.....	76
	4.6.3 Aspek Penelitian Lanjutan.....	78
	4.7 Rencana Implementasi Program.....	79
BAB V	KESIMPULAN DAN SARAN.....	82
	5.1. Kesimpulan.....	82
	5.2 Saran-saran.....	83
	DAFTAR PUSTAKA.....	85
	LAMPIRAN-LAMPIRAN.....	88

DAFTAR GAMBAR

Gambar		Halaman
I – 1	Statistik Penggunaan Internet di Dunia Tahun 2012.....	2
I – 2	Tren Lubang Kerawanan pada Perangkat Lunak.....	3
I – 3	Jenis-jenis Proteksi Menurut Profesor Eko Indrajit.....	4
II – 1	Skema Embedding dan Ektrraction Data.....	14
II – 2	ROT 13 Pada Sandi Caesar.....	27
II – 3	Struktur Organisasi pada PT Panasonic Devices Ind.....	38
II – 4	Kerangka Konsep Pemecahan Masalah	39
III – 1	Langkah-langkah Penelitian.....	51
III – 2	Pengujian dengan Pengembangan Algoritma.....	53
III – 3	Hasil Setelah Memasukan Variabel dengan Benar.....	54
IV – 1	Struktur Organsasi PT Panasonic Industrial Devices Indonesia	56
IV – 2	Menu aplikasi pengamanan informasi pesan rahasia.....	58
IV – 3	Alur Program enkripsi dan dekripsi.....	59
IV – 4	Menu Utama.....	60
IV – 5	Penjelasan Menu Utama.....	65
IV – 6	Menu Pengujian Modul Enkripsi.....	66
IV – 7	Skip steganografi untuk proses <i>encode</i>	67
IV – 8	Menu Pengujian Modul Dekripsi.....	68
IV – 9	Skip steganografi untuk proses <i>decode</i>	69
IV – 10	Menu Pengujian Panjang Karakter.....	70
IV – 11	Modul untuk pengecekan jumlah karakter.....	70
IV – 12	Menu Pengujian Modul New.....	71
IV – 13	Contoh Pengembangan Algoritma Caesar Cipher.....	73
IV – 14	Bagian inti dari pengembangan algoritma baru.....	73
IV – 15	Algoritma pengembangan Caesar Cipher dengan Jam, menit detik, mili detik dan mikro detik.....	74
IV - 16	Fungsi Pengambilan <i>Login User</i> Secara Otomatis.....	75

IV – 17	Menu Utama.....	76
IV – 18	Tabel Login User.....	77
IV – 19	Menu <i>Check Password</i>	78
IV - 20	<i>Script</i> untuk konversi karakter dan spesial karakter.....	78
IV - 21	Menu Registrasi eMail.....	79
IV - 22	Informasi eMail ke User.....	79
IV - 23	Informasi <i>Password</i> pada <i>Report</i>	80
IV - 24	Grafik “ <i>pie</i> ” Menyatakan <i>password</i> untuk <i>private key</i>	80
IV - 22	Tabel <i>time</i> untuk merumuskan <i>private key</i>	81
IV - 26	Contoh <i>private key</i>	81
IV - 27	Proses dekripsi yang sudah berhasil.....	82

DAFTAR TABEL

Tabel		Halaman
II – 2	Company Profile PT Panasonic Industrial Devices Ind.....	36
III – 1	Jadwal Penelitian.....	54
IV – 1	<i>Timeline</i> Susunan Rencana Implementasi.....	86



DAFTAR LAMPIRAN

Lampiran	Halaman
1. Menu Utama Keamanan Pesan Rahasia.....	94
2. Proses Menentukan Citra Gambar yang akan disisipkan pesan rahasia	94
3. Proses Penyisipan Pesan Rahasia pada Citra Gambar.....	95
4. Pemberian <i>Password</i> pada proses <i>Encode</i>	95
5. Menu untuk menentukan user yang akan di kirimkan pesan rahasia melalui eMail.....	96
6. Isi Pesan yang akan di sampaikan kepada <i>user</i>	96
7. Isi dari file yang dikirimkan dalam grafik garis sebagai <i>public key</i>	97
8. Pesan rahasia yang di kirimkan dalam bentuk <i>private key</i>	97
9. Isi pesan rahasia dalam bentuk <i>pie</i> sebagai <i>private key</i>	98
10. eMail yang diterima oleh user dari si pengirim pesan.....	98
11. Menu <i>Decode</i>	99
12. Isi pesan yang belum di konversi/ <i>deript</i>	99
13. Menu <i>Forgot Password</i>	100
14. Isi pesan dari <i>Public Key</i>	100
15. Proses enkripsi dalam <i>forgot password</i>	100
16. Konfirmasi <i>password</i> dalam membuka pesan rahasia.....	101
17. Rumus konversi perhitungan jam.....	101
18. <i>Password</i> yang digunakan dalam dekripsi pesan rahasia.....	101
19. Hasil dekripsi dari pesan yang disisipkan pada citra gambar.....	102
20. Listing program <i>encode</i> dan <i>decode</i>	102
21. Listng program konversi dalam <i>public key</i>	105
22. Listing program algoritma jam, menit, detik, mili detik dan mikro detik.....	106
23. <i>Hand's Over</i> aplikasi.....	108

DAFTAR PUSTAKA

- [ARUBUSMAN 2007] Arubusman, Yusrian Roman, 2007, *Audio Steganografi*,
<http://iwayan.info/File>
Mahasiswa/SkirpsiYusAudioSteganografi_2007.pdf, diakses tanggal 27
April 2012.
- [CONWAY 2003] M. Conway, *Code Wars: Steganography, Signals Intelligence, and Terrorism*, Knowledge Technology & Policy, Volume 16, Number 2, pp. 45-62, Springer, 2003.
- [DAVID 2012] David, A. Murtado, Utin Kasma, *Steganografi Pada Citra Bmp 24-Bit Menggunakan Metode Least Significant Bit*, Jurnal Ilmiah SISFOTENIKA, Vol. 2, No. 1, Januari 2012.
- [HOSMER 2006] C. Hosmer, *Discovering Hidden Evidence*, Taylor & Francis Group, Journal of Digital Forensic Practice, Vol. No.1, pp.47-56, 2006.
- [INDRAJIT 2011] Prof. Eko Indrajit, *Mencermati Fenomena Kebocoran Data dan Informasi Rahasia*,
<http://www.scribd.com/doc/73455263/139/MENCERMATI-FENOMENA-KEBOCORAN-DATA-DAN-INFORMASI-RAHASIA>,
diakses 10 Mei 2012.
- [JAJODIA 1998] N.F. Johnson and S. Jajodia, *Exploring Steganography: Seeing the Unseen*, IEEE, Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998.
- [JAMILIA AENI 2012] Aeni Jamilia, Moedjiono, Hadi Syahrial, *Rancangan Implementasi Protokol S/MIME pada Layanan E-Mail Sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi Secara Online: Studi Kasus PT. XYZ*, Jakarta, 2012.
- [JITHESH 2011] Jithesh K, A V Senthil Kumar, *Multi Layer Information Hiding -A Blend Of Steganography And Visual Cryptography*, Journal of Theoretical and Applied Information Technology, 2010.
- [KAVITHA 2012] Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dughav *Steganography Using Least Signicant Bit Algorithm*, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp. 338-341.