

**PROTOTYPE KEAMANAN PESAN RAHASIA DENGAN
TEKNIK KRIPTOGRAFI DAN STEGANOGRAFI
MENGUNAKAN ALGORITMA LSB, RSA, CRT DAN
HUFFMAN**

TESIS



Oleh:

MOH. SOFJAN

1311600173

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2015

**PROTOTIPE KEAMANAN PESAN RAHASIA DENGAN
TEKNIK KRIPTOGRAFI DAN STEGANOGRAFI
MENGUNAKAN ALGORITMA LSB, RSA, CRT DAN
HUFFMAN**

TESIS

Diajukan untuk memenuhi salah satu persyaratan
Memperoleh gelar Magister Ilmu Komputer (MKOM)



Oleh:

MOH. SOFJAN

1311600173

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

JAKARTA

2015



PROGRAM STUDI MAGISTER ILMU KOMPUTER (MIKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini,

Nama Mahasiswa : MOH. SOFJAN
Nomor Induk Mahasiswa : 1311600173
Program Studi : MAGISTER ILMU KOMPUTER (MIKOM)
Konsentrasi : REKAYASA KOMPUTASI TERAPAN

menyatakan bahwa TESIS yang berjudul :
PROTOTYPE KEAMANAN PESAN RAHASIA DENGAN TEKNIK
KRIPTOGRAFI DAN STEGANOGRAFI MENGGUNAKAN
ALGORITMA LSB, RSA, CRT DAN HUFFMAN.

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, Agustus 2015



(MOH. SOFJAN)



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

LEMBAR PENGESAHAN

Nama Mahasiswa : Moh. Sofjan
Nomor Induk Mahasiswa : 1311600173
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul TESIS : PROTOTIPE KEAMANAN PESAN RAHASIA
DENGAN TEKNIK KRIPTOGRAFI DAN
STEGANOGRAFI MENGGUNAKAN
ALGORITMA LSB, RSA, CRT DAN HUFFMAN

Jakarta, 31 Agustus 2015

Tim Penguji :

Tanda tangan :

Penguji I (Ketua)
Prof. Dr. Moedjiono, M.Sc

Penguji II
Ir. Wendi Usino, MM., M.Sc., Ph.D

Pembimbing,
Dr., Ir. Nazori Az, M.T

Ketua Program Studi

(Dr., Ir. Nazori Az, M.T)

ABSTRAK

Kriptografi dan Steganografi merupakan metode pengiriman pesan secara rahasia. Pada kriptografi pesan yang dikirim tetap terlihat oleh pihak lain tapi dalam bentuk yang tersandi. Sementara pada steganografi pesan yang dikirim disembunyikan di balik media lain. Kombinasi keduanya akan memberikan tingkat keamanan pesan yang lebih tinggi. LSB merupakan salah satu metode steganografi yang cukup dikenal luas. Metode ini akan menggantikan bit-bit tertentu pada citra dengan pesan yang akan disembunyikan. Sementara RSA merupakan salah satu metode kriptografi bertipe tidak simetris yang banyak digunakan. Kriptografi tidak simetris adalah kriptografi yang terdiri atas kunci publik dan kunci *private*. Kunci publik akan disebar luaskan sementara kunci *private* hanya dimiliki oleh yang berhak. Sebuah pesan yang dienkripsi dengan kunci publik hanya dapat dibuka dengan kunci *private* yang berkaitan. Penelitian ini menggabungkan kriptografi RSA 1024 bit 8 faktor prima yang telah dimodifikasi dengan steganografi LSB. Pada proses enkripsi digunakan metode RSA yang digabungkan dengan metode *Huffman* untuk mengurangi jumlah bit yang akan disisipkan pada citra penampung. Sementara pada proses dekripsi digunakan metode *Huffman* yang dilanjutkan dengan modifikasi algoritma RSA dengan menggunakan *Chinese Remainder Theorem*, untuk mengurangi proses komputasi terhadap bilangan yang sangat besar. Hasil penelitian ini berupa citra gambar yang telah disisipi pesan rahasia yang terenkripsi, yang selanjutnya citra tersebut dibuka dengan menggunakan metode tersebut di atas. Pengujian dilakukan untuk membandingkan kecepatan dekripsi metode RSA standard an RSA CRT, tingkat keamanan pesan citra tersebut dan pengujian aplikasi.

Kata kunci: Citra, Kriptografi, Steganografi, RSA, LSB, CRT, *Huffman*.

ABSTRACT

Cryptography and Steganography are methods of sending secret messages. In the cryptographic sent message is remain visible by others but in encrypted form. Meanwhile in steganography sent messages is hidden behind other media. Both combination would provide higher level security. LSB is one of the steganographic methods which quite well known. This method will replace certain bits of the image with the messages that will be hidden. While RSA is asymmetric cryptography method that is widely used. Asymmetric Cryptography is the cryptography which consist of public key and private key. The public key will be disseminated while the private key is only held by eligible. A message encrypted with the public key can only be opened with the associated private key. This research combines a 1024-bit 8 prime factors RSA Cryptography that have been modified with LSB Steganography. At the encryption process, we use RSA method that combining with the Huffman method to reduce the number of bits that will be inserted into cover image. Meanwhile in the decryption process, we use modified RSA algorithm using Chinese Remainder Theorem to reduce the computation process time to the very large number. Results of this research is an image that have been inserted an encrypted secret message, and then this stego image is opened by using the method above. The test will be conducted to compare decryption speed of standard RSA and RSA CRT, stego image security level and application testing.

Keywords : Image, Cryptography, Steganography, RSA, LSB, Huffman.

KATA PENGANTAR

Assalamu 'alaikum Warohmatullohi Wabarokatuh.

Segala puji dan syukur senantiasa terpanjatkan ke hadirat Allah SWT yang telah memberikan taufiq dan hidayah-Nya sehingga penulis dapat menyelesaikan proposal tesis yang berjudul “**Prototipe keamanan pesan rahasia dengan teknik kriptografi dan steganografi menggunakan algoritma LSB, RSA, CRT dan Huffman**”. Shalawat serta salam senantiasa tercurah pada Rasulullah Muhammad SAW beserta keluarga shahabat dan umatnya yang setia hingga akhir zaman.

Dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah memberikan bantuan atas penyelesaian penulisan proposal tesis ini, dengan segala ketulusan hati penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Orang tua serta keluargaku yang tercinta yang senantiasa memberikan kasih sayang, nasihat, dorongan serta doa yang tak pernah berhenti mengalir.
2. Bapak Prof. Dr. Moedjiono, M.Sc. sebagai Direktur Program Pascasarjana Universitas Budi Luhur.
3. Bapak Dr., Ir. Nazori AZ, M.T. sebagai Ketua Program Studi Magister Komputer Universitas Budi Luhur sekaligus sebagai pembimbing yang telah banyak memberikan saran dan masukan penyusunan proposal tesis ini. Terima kasih juga kepada beliau yang mengajarkan ilmu steganografi dan kriptografi kepada penulis selama perkuliahan Komputasi Terapan.
4. Bapak Prof. Dr. Moedjiono, M.Sc sebagai dosen penguji
5. Bapak Ir. Wendi Usino, MM., M.Sc., Ph.D sebagai dosen penguji
6. Bapak Mardi Hardjianto M.Kom yang mengajarkan metode *Huffman* kepada penulis selama perkuliahan Keamanan Sistem dan Jaringan Komputer.

7. Bapak Ir. Teddy Mantoro M.sc.,Ph.D yang mengajarkan metode RSA dan pemrograman Android kepada penulis selama perkuliahan *Mobile Computing*.
8. Seluruh dosen, staff karyawan dan karyawan Universitas Budi Luhur yang telah memberikan bantuannya.
9. Seluruh rekan-rekan kuliah MKOM Universitas Budi Luhur.

Penulis menyadari penulisan tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun demi tercapainya penulisan yang lebih baik. Saran dan kritik dapat dikirimkan ke alamat e-mail msofjan70@gmail.com

Wassalamu'alaikum Warohmatullohi Wabarokatuh.

Jakarta, Agustus 2015

Moh. Sofjan

DAFTAR ISI

	Halaman
Abstrak	i
Kata Pengantar	iii
Daftar Isi	v
Daftar Gambar	viii
Daftar Tabel	ix
Daftar Lampiran	xi
 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 Penelitian dan Manfaat Penelitian	3
1.3.1. Tujuan Penelitian	3
1.3.2. Manfaat Penelitian	4
1.4.Sistematika Penulisan	5
1.5.Daftar Pengertian	5
 BAB II LANDASAN PEMIKIRAN	
2.1. Tinjauan Pustaka	7
2.1.1. Teori Bilangan	7
2.1.2. Kode ASCII	13
2.1.3. Kriptografi	13
2.1.4. Kriptografi RSA	18
2.1.5. <i>Chinese Remainder Theorem</i> (CRT)	27
2.1.6. Pemampatan Huffman	31

2.1.7. Citra	35
2.1.8. Steganografi	41
2.1.9. Steganografi LSB	43
2.2. Tinjauan Studi	45
2.3. Tinjauan Obyek Penelitian	46
2.3.1. Perangkat Lunak	46
2.3.2. Perangkat Keras	46
2.4. Pola Pikir Pemecahan Masalah	47
2.5. Hipotesis	47

BAB III METODOLOGI PENELITIAN

3.1. Metodologi Penelitian	48
3.1.1. Pendekatan Teori	48
3.1.2. Pendekatan Abstraksi	49
3.1.3. Pendekatan Desain Produk atau Sistem	49
3.2. Desain Penelitian	50
3.2.1. Metode Enkripsi dan Deskripsi RSA MF-8 1024 bit	51
3.2.2. Metode Kompresi dan Dekompresi Huffman	55
3.2.3. Metode LSB 2 Bit	56
3.3. Pemilihan Sampel	58
3.4. Metode Pengumpulan Data	58
3.5. Instrumentasi	58
3.6. Pengujian	59
3.7. Langkah – langkah Penelitian	60

BAB IV PEMBAHASAN HASIL PENELITIAN

4.1. Analisis dan Perancangan Sistem	62
4.1.1. Diagram <i>Use Case</i>	62
4.1.2. Diagram <i>Activity</i>	64
4.1.3. Diagram <i>Class</i>	65
4.1.4. Diagram <i>Sequence</i>	66
4.1.5. <i>Prototype GUI</i>	69
4.2. Sampel Data	70

4.3.Pendekatan Teori	71
4.3.1. Perhitungan Faktor Kompresi Kombinasi RSA dan Huffman	71
4.3.2. Perbandingan Waktu Eksekusi RSA CRT dan Standar	75
4.4.Pendekatan Abstraksi	78
4.4.1. Pengujian Citra <i>Cover Image</i> dan <i>Stego Image</i> Dengan parameter PSNR	79
4.4.2. Pengujian Citra <i>Cover Image</i> dan <i>Stego Image</i> dengan aplikasi <i>steganalysis</i> dan <i>cryptanalysis</i> ...	82
4.5.Pendekatan Disain Produk atau Sistem	86
4.5.1. Kategori ISO 9126 dan Hasil Angket	86
4.5.2. Uji Skor Aktual	94
4.6.Implikasi Penelitian.....	97
4.7.Rencana Implementasi	97
 BAB V PENUTUP	
5.1.Kesimpulan	98
5.2.Saran	99
 DAFTAR PUSTAKA	100
LAMPIRAN – LAMPIRAN	101
RIWAYAT HIDUP	123

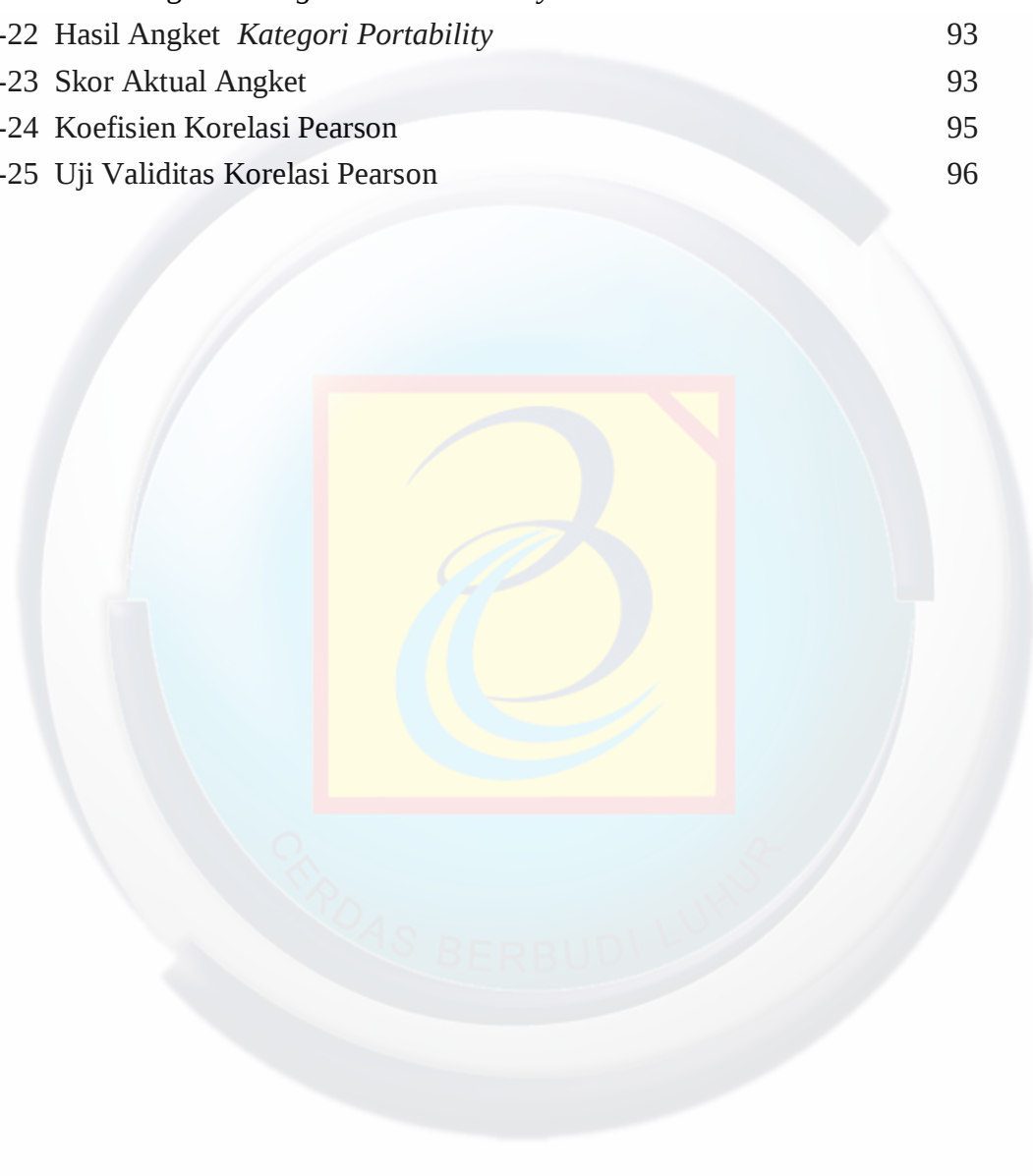
DAFTAR GAMBAR

Gambar	Halaman
II-1 Proses Enkripsi dan Dekripsi	14
II-2 Citra Biner atau Hitam Putih	36
II-3 Citra Keabuan	37
II-4 Citra RGB	38
II-5 RGB dan CMYK	38
II-6 Kombinasi warna RGB (sumber:Microsoft Excel)	39
II-7 Proses Steganografi	42
II-8 Pola Pikir	47
III-1 Algoritma Penyisipan Pesan pada Citra	50
III-2 Algoritma Pengambilan Pesan dari Citra	51
III-3 Proses Enkripsi RSA dan kompresi Huffman	55
III-4 Proses Dekripsi RSA dan dekompresi Huffman	56
III-5 Proses Penyisipan pesan pada metode LSB	57
III-6 Proses Pengambilan pesan dengan metode LSB	57
IV-1 Diagram <i>Use Case</i>	63
IV-2 Diagram <i>Activity</i>	64
IV-3 Diagram <i>Class</i>	65
IV-4 Diagram <i>Sequence</i> – Memasukkan <i>Cover Image</i>	66
IV-5 Diagram <i>Sequence</i> -Memasukkan pesan rahasia	68
IV-6 Diagram <i>Sequence</i> -Memasukkan <i>stego image</i>	69
IV-7 <i>Prototype GUI</i>	69
IV-8 Banyak karakter angka <i>plaintext</i> dan <i>ciphertext</i>	72
IV-9 Rasio karakter angka <i>plaintext</i> dan <i>ciphertext</i>	73
IV-10 Banyak angka biner <i>plaintext</i> dan <i>ciphertext</i>	74
IV-11 Perbandingan angka biner <i>plaintext</i> dan <i>ciphertext</i>	74
IV-12 Waktu dekripsi RSA (detik)	77
IV-13 Perbandingan waktu dekripsi RSA	77
IV-14 Sampel citra	79
IV-15 Nilai PSNR citra uji untuk beberapa variasi pesan	81
IV-16 Enkripsi dengan aplikasi RSAmake	83
IV-17 Dekripsi dengan aplikasi RSAmake	84
IV-18 Dekripsi pesan aplikasi tesis dengan aplikasi RSAmake	85

DAFTAR TABEL

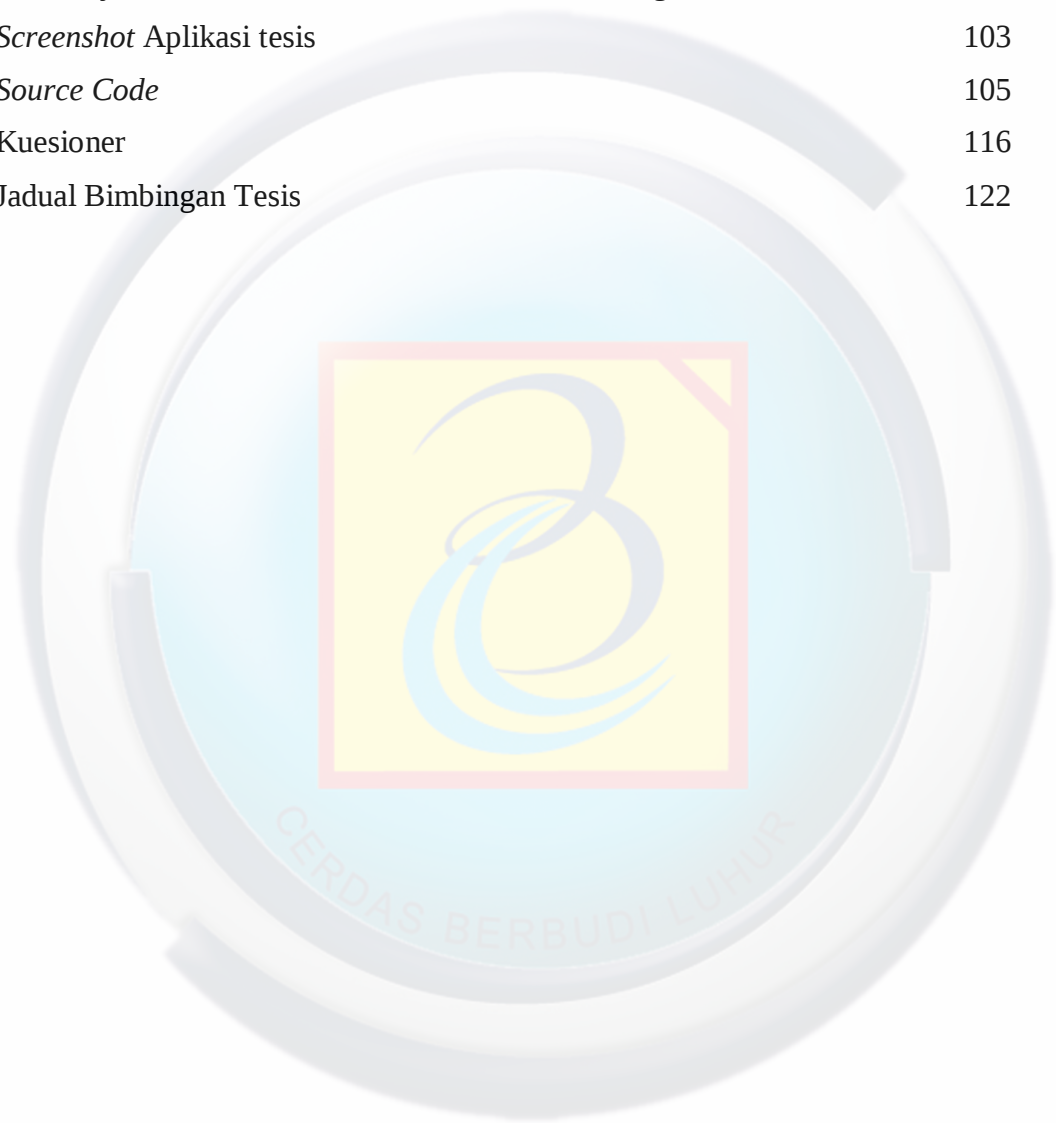
Tabel	Halaman
II-1 Sifat Aritmatika Modulo	10
II-2 Enkripsi Pesan dengan RSA 1 variabel	20
II-3 Dekripsi Pesan dengan RSA 1 variabel	21
II-4 Parameter RSA Standar	22
II-5 Enkripsi Pesan dengan RSA 2 faktor prima	23
II-6 Dekripsi Pesan dengan RSA 2 faktor prima	25
II-7 Contoh Perhitungan RSA per karakter	27
II-8 Contoh Perhitungan RSA dengan CRT	29
II-9 Contoh Perhitungan RSA CRT per kelompok karakter	30
II-10 9 variasi warna dasar merah	39
II-11 Kombinasi 3 warna RGB	40
II-12 Penerapan Steganografi LSB 2 bit	44
II-13 Literatur penelitian lain yang berkaitan	45
III-1 Kombinasi 2 dan 8 faktor prima	52
III-2 Jadual Penelitian	61
IV-1 Deskripsi peran aktor	62
IV-2 Daftar <i>Use Case</i>	63
IV-3 Nama Kelas	65
IV-4 Aksi aktor dan sistem-Memasukkan <i>cover image</i>	66
IV-5 Aksi aktor dan sistem-Memasukkan pesan rahasia	67
IV-6 Aksi aktor dan sistem-Memasukkan <i>stego image</i>	68
IV-7 Sebagian Sampel Pengujian	70
IV-8 Perbandingan jumlah angka <i>plaintext</i> dan <i>ciphertext</i>	72
IV-9 Bilangan biner <i>plaintext</i> dan <i>ciphertext</i>	73
IV-10 Perbandingan waktu (detik) dekripsi RSA standar dan CRT	75
IV-11 Rasio RSA standar dan CRT	76
IV-12 Hasil perhitungan PSNR 3 buah citra	80
IV-13 Hasil perhitungan PSNR 2 buah citra	81
IV-14 Hasil uji dengan aplikasi stego expose	82
IV-15 Persentase pesan terhadap kapasitas <i>cover image</i>	82
IV-16 Sub Kategori Adaptasi ISO 9126	87
IV-17 Hasil Angket <i>Kategori Functionality</i>	88

IV-18 Hasil Angket <i>Kategori Reliability</i>	89
IV-19 Hasil Angket <i>Kategori Usability</i>	90
IV-20 Hasil Angket <i>Kategori Efficiency</i>	91
IV-21 Hasil Angket <i>Kategori Maintainability</i>	92
IV-22 Hasil Angket <i>Kategori Portability</i>	93
IV-23 Skor Aktual Angket	93
IV-24 Koefisien Korelasi Pearson	95
IV-25 Uji Validitas Korelasi Pearson	96



DAFTAR LAMPIRAN

Lampiran	Halaman
1. Hasil Uji Validitas Korelasi Pearson ISO 9126 dengan SPSS	101
2. <i>Screenshot</i> Aplikasi tesis	103
3. <i>Source Code</i>	105
4. Kuesioner	116
5. Jadwal Bimbingan Tesis	122



DAFTAR PUSTAKA

- [Bateman 2008] Bateman, Philip, *Image Steganography and Steganalysis*, University of Surrey Guildford, United Kingdom, 2008.
- [Hardjianto 2014] Hardjianto, Mardi, *Keamanan Sistem dan Jaringan Komputer*, Universitas Budi Luhur, Jakarta, 2014.
- [Lee 2014] Lee, Holden, Oleg Muskarov, Teo Andrica, *Number Theory*, <http://web.mit.edu/holden1>, 2014.
- [Mantoro 2014] Mantoro, Teddy, *Mobile Computing*, Universitas Budi Luhur, Jakarta, 2014.
- [Marques 2011] Marques, Oge, *Practical Image and Video Processing Using Matlab*, John Wiley & Sons, Inc, New Jersey, 2011
- [Maurya 2011] Maurya, Shweta, Vishal Shrivastava, *An Improved Novel Steganographic Technique for RGB and YCbCr Colorspace*, IOSR Journal of Computer Engineering, India, 2014
- [Nazori 2014] Nazori AZ, *Komputasi Terapan Lanjutan*, Universitas Budi Luhur, Jakarta, 2014.
- [Rosen 1986] Rosen, Kenneth H, *Elementary Number Theory and Its Applications*, Addison-Wesley Publishing Company, Massachusetts, 1986.
- [Sommerville 2003] Sommerville, Ian, *Software Engineering*, Erlangga, 2003.
- [Stinson 2006] Stinson, Douglas R, *Cryptography – Theory and Practice*, Chapman & Hall/CRC, 3rd Edition, Ontario, 2006.
- [Sugiyono 2007] Sugiyono, *Metode Penelitian Administrasi*, Bandung 2007.
- [Wikipedia 2015], http://en.wikipedia.org/wiki/Great_Internet_Mersenne_Prime_Search, 2015.