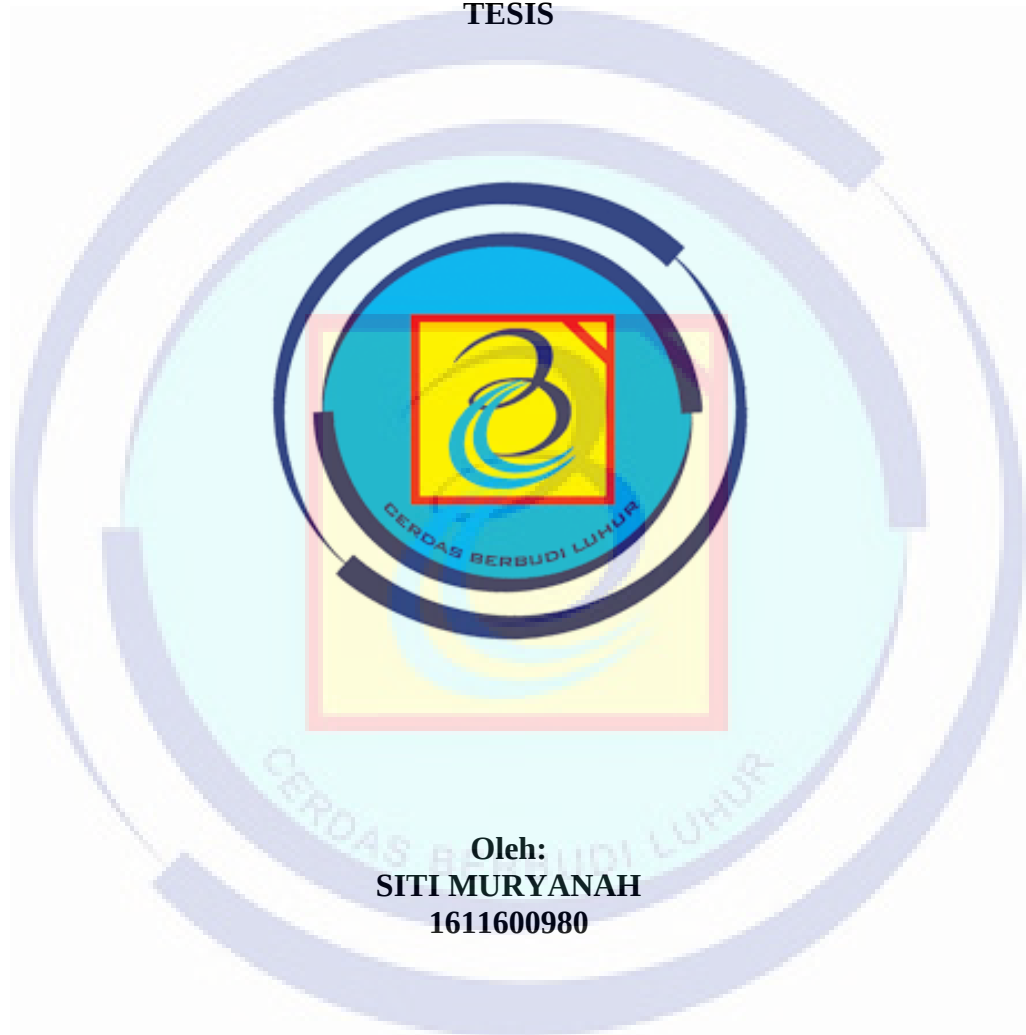


**SISTEM PENGAMANAN DATA MENGGUNAKAN
ALGORITMA AES DAN BLOWFISH DENGAN METODE LSB
PADA CITRA PNG**

TESIS



**Oleh:
SITI MURYANAH
1611600980**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2018**

SISTEM PENGAMANAN DATA MENGGUNAKAN ALGORITMA AES DAN BLOWFISH DENGAN METODE LSB PADA CITRA PNG

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)



Oleh:
SITI MURYANAH
1611600980

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2018



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini

Nama Mahasiswa : Siti Muryanah
NIM : 1611600980
Konsentrasi : Teknologi Sistem Informasi

Menyatakan bahwa Tesis yang berjudul :
Sistem Pengamanan Data Menggunakan Algoritma AES
dan Blowfish dengan Metode LSB Pada Citra PNG

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik 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 tanggungjawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila dikemudian hari pernyataan ini tidak benar.

Jakarta, 08 Agustus 2018



Siti Muryanah



**PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PENGESAHAN TESIS

Nama Mahasiswa : Siti Muryanah
NIM : 1611600980
Konsentrasi : Teknologi Sistem Informasi
Judul Tesis : Sistem Pengamanan Data Menggunakan
Algoritma AES dan Blowfish Dengan Metode
LSB Pada Citra PNG

Jakarta, 08 Agustus 2018

Tim Penguji
Ketua,

Tanda Tangan

Ir. Wendi Usino, MM., M.Sc., Ph.D
Anggota,

Dr. Goenawan Brotosaputro, S.Kom., M.Sc
Pembimbing,

Dr. Ir. Nazori Az, M.T

Ketua Program Studi

Dr. M. Syafrullah, M.Kom., M.Sc

ABSTRAK

Di era internet sekarang ini transaksi online hampir setiap detik terjadi dan keamanan informasi menjadi suatu tantangan yang harus diselesaikan. Pada tahun 2014-2016 terdapat 36.6 juta insiden serangan *cyber* di Indonesia termasuk pencurian data). Kriptografi menjadi salah satu solusi dalam keamanan tersebut yaitu dengan membuat informasi menjadi tidak dimengerti oleh orang lain. Namun dengan kriptografi dinilai kurang cukup, sehingga diperlukan keamanan berlapis dengan metode lainnya seperti steganografi agar pesan tidak dicurigai oleh pihak yang tidak bertanggung jawab, karena hasil kriptografi disisipkan kedalam media digital sehingga informasi tersebut tidak akan menimbulkan kecurigaan oleh orang lain. Algoritma kriptografi yang digunakan adalah AES dan Blowfish dan metode steganografi dengan LSB (*least significant bit*). Pengujian citra dengan *mean square error* dan *peak signal to noise ratio*, yaitu dengan nilai hasil MSE masing-masing 1.814 dan 1.817 serta nilai PSNR 42.29. Untuk pengujian keamanan menggunakan tools *StegSpy 2.1* dengan mendeteksi keberadaan pesan dalam *stegoimage* yang hasilnya tidak terdeteksi di citra PNG.

Kata kunci: kriptografi, steganografi, AES, Blowfish, *least significant bit*, *mean square error*, *peak signal to noise ratio*, *stegoimage*.

ABSTRACT

In today's internet world, online transactions almost every second occur and information security is a challenge that must be resolved. In 2014-2016 there were 36.6 million incidents of cyber attacks in Indonesia including data theft. Cryptography is one of the solutions in security that is by making information not understood by others. However, with cryptography is considered insufficient, so there is a need for layered security with other methods such as steganography so that messages are not suspected by irresponsible parties, because cryptographic results are inserted into digital media so that information will not cause suspicion by others. Cryptographic algorithms used are AES and Blowfish and the steganography method with LSB (least significant bit). Image testing with mean square error and peak signal to noise ratio, namely with the MSE results of 1,814 and 1,817 and PSNR 42.29. For security testing use StegSpy 2.1 tools by detecting the presence of messages in stegoimage whose results are not detected in PNG images.

Keywords: cryptography, steganography, AES, Blowfish, least significant bit, mean square error, peak signal to noise ratio, stegoimage.

KATA PENGANTAR

Assalamu 'alaikum Wr. Wb.

Segala puji dan syukur senantiasa terpanjatkan ke hadirat Allah SWT yang telah memberikan rahmat dan ridho-Nya sehingga penulis dapat menyelesaikan **MENGUNAKAN ALGORITMA AES DAN BLOWFISH DENGAN METODE LSB PADA CITRA PNG**".

Sholawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu.

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

1. Bapak dan Ibu yang senantiasa memberikan kasih sayang, nasihat, dukungan, semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
2. Suamiku tercinta Muhammad Amin S.Sos dan anak-anakku Muhammad Luthfi Abdullah dan Muhammad Yusuf Abdullah yang menjadi penyemangat dalam menyelesaikan tesis ini
3. Bapak Prof. Dr. sc. agr. Ir. Didik Sulistyanto selaku Rektor Universitas Budi Luhur.
4. Bapak Dr.Suhartono, MBA, M.A selaku Direktur Program Pascasarjana Universitas Budi Luhur.
5. Bapak Dr. M. Syafrullah, M.Kom, M.Sc selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
6. Bapak Dr. Ir. Nazori Az, M.T, selaku dosen pembimbing yang telah membimbing dan memotivasi penulis dalam mengerjakan tesis ini.
7. Seluruh Bapak dan Ibu Dosen pengampu mata kuliah di Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang telah sabar memberikan ilmu pengetahuan, pencerahan, dan bimbingan dalam belajar.
8. Sahabat dan teman terbaikku Ismatul Maula S.Kom, yang selalu ada dan membantu dalam penyusunan proposal tesis ini.
9. Intan dan kawan-kawan MKOM UBL Kelas XC, XM di semester 1, 2 dan Kelas SI di semester 3.

"Tiada gading yang tak retak". 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
st.muryanah@gmail.com.

Wassalamu 'alaikum. Wr. Wb.

Jakarta, Agustus 2018

Siti Muryanah



DAFTAR ISI

LEMBAR PERNYATAAN	i
HALAMAN PENGESAHAN TESIS	ii
ABSTRAK	iii
ABSTRACT.....	iv
KATA PENGANTAR	v
DAFTAR ISI.....	vii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xii
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Masalah Penelitian.....	2
1.2.1 Identifikasi Masalah.....	2
1.2.2 Batasan Masalah.....	3
1.2.3 Rumusan Masalah.....	3
1.3 Tujuan dan Manfaat penelitian.....	4
1.3.1 Tujuan Penelitian	4
1.3.2 Manfaat Penelitian	4
1.4 Tata Urut Penulisan.....	5
1.5 Daftar Pengertian	6
BAB II	8
LANDASAN TEORI DAN KERANGKA KONSEP	8
2.1 Kriptografi.....	8

2.2	Blowfish	13
2.3	Advanced Encryption Standard (AES)	16
2.4	Steganografi	22
2.5	<i>Least significant Bit</i>	26
2.6	<i>Peak Signal to Noise Ratio</i> dan <i>Mean Square Error</i>	28
2.7	Tinjauan Studi	29
2.8	Kerangka Konsep/Pola Pikir Pemecahan Masalah	38
2.9	Hipotesis.....	39
BAB III		40
METODOLOGI DAN RANCANGAN PENELITIAN		40
3.1.	Metode Penelitian.....	40
3.2.	Metode Pengumpulan Data.....	42
3.3.	Sumber dan Instrumen Data.....	42
3.4.	Teknik Analisis, Rancangan, dan Pengujian Sistem.....	43
3.4.1.	Teknik Analisis	43
3.4.2.	Teknik Perancangan.....	43
3.4.3.	Teknik Pengujian Keamanan Pesan dan Sistem	44
3.5.	Langkah-langkah Penelitian.....	44
3.6.	Jadwal Penelitian.....	46
BAB IV		48
PEMBAHASAN DAN HASIL PENELITIAN		48
4.1.	Analisis Algoritma Kriptografi dan Steganografi	48
4.2.	Hasil Implementasi.....	48
4.2.1.	Halaman Menu Utama	49
4.2.2.	Halaman Menu Enkripsi dan <i>Encode</i>	49

4.2.3. Halaman Menu Dekripsi dan <i>Decode</i>	52
4.2.4. Menu PSNR dan MSE	55
4.3. Pengujian dan Hasil Pengujian.....	56
4.3.1 Pengujian Keamanan Pesan	56
4.3.2 Pengujian Sistem.....	65
4.3.3 Hasil Pengujian Keamanan Pesan.....	72
4.3.4 Hasil Pengujian Sistem	73
4.4. Implikasi Penelitian.....	79
4.4.1 Aspek Sistem.....	79
4.4.2 Aspek Manajerial	79
4.4.3 Aspek Penelitian Lanjutan	79
4.5. Rencana Implementasi Sistem	80
BAB V	82
PENUTUP.....	82
5.1 Kesimpulan	82
5.2 Saran.....	82
DAFTAR PUSTAKA	83
DAFTAR RIWAYAT HIDUP SINGKAT	86

DAFTAR GAMBAR

Gambar II 1 Proses Enkripsi dan Dekripsi dalam kriptografi.....	9
Gambar II- 2 Jenis teknik kriptografi dan algoritmanya.....	10
Gambar II- 3 Fungsi Putaran (Fungsi Feistel) dalam Blowfish.....	13
Gambar II- 4 Skema jaringan Feistel Algoritma Blowfish.....	15
Gambar II- 5 Enkripsi Algoritma AES.....	17
Gambar II- 6 Ilustrasi transformasi <i>SubByte</i>	18
Gambar II- 7 Ilustrasi pergeseran pada proses <i>shiftrows</i>	19
Gambar II- 8 Ilustrasi proses Mixcolumns.....	19
Gambar II- 9 Ilustrasi Proses <i>AddRoundKey</i>	20
Gambar II- 10 Ilustrasi proses Invers Shift Rows.....	21
Gambar II- 11 Dekripsi Algoritma AES.....	22
Gambar II- 12 Penggolongan Steganografi berdasarkan tujuan.....	23
Gambar II- 13 Skema umum dari Steganografi.....	24
Gambar II- 14 Kerangka Konsep.....	38
Gambar III-1 Konsep metodologi penelitian dengan pendekatan DSR.....	40
Gambar III-2 Tahapan Penelitian.....	44
Gambar IV- 1 Menu Utama.....	49
Gambar IV. 2 Menu Enkripsi dan <i>Encode</i> AES/Blowfish.....	50
Gambar IV- 3 Notifikasi Proses <i>encode</i> sukses.....	51
Gambar IV- 4 Detail hasil proses enkripsi dan <i>encode</i> algoritma AES/Blowfish.....	52
Gambar IV- 5 Menu Dekripsi dan <i>Decode</i> AES/Blowfish.....	53
Gambar IV- 6 Notifikasi Sukses Proses <i>Decode</i>	54
Gambar IV- 7 Detail informasi Dekripsi dan <i>decode</i> AES/Blowfish.....	55
Gambar IV- 8 Menu perhitungan MSE dan PSNR.....	56
Gambar IV-9 Tools StegSpy V2.1.....	57
Gambar IV -10 Grafik Perbandingan Waktu Proses <i>Encode</i>	74
Gambar IV- 11 Grafik Perbandingan Waktu Proses <i>Decode</i>	75
Gambar IV- 12 Grafik Pengujian Nilai MSE.....	77

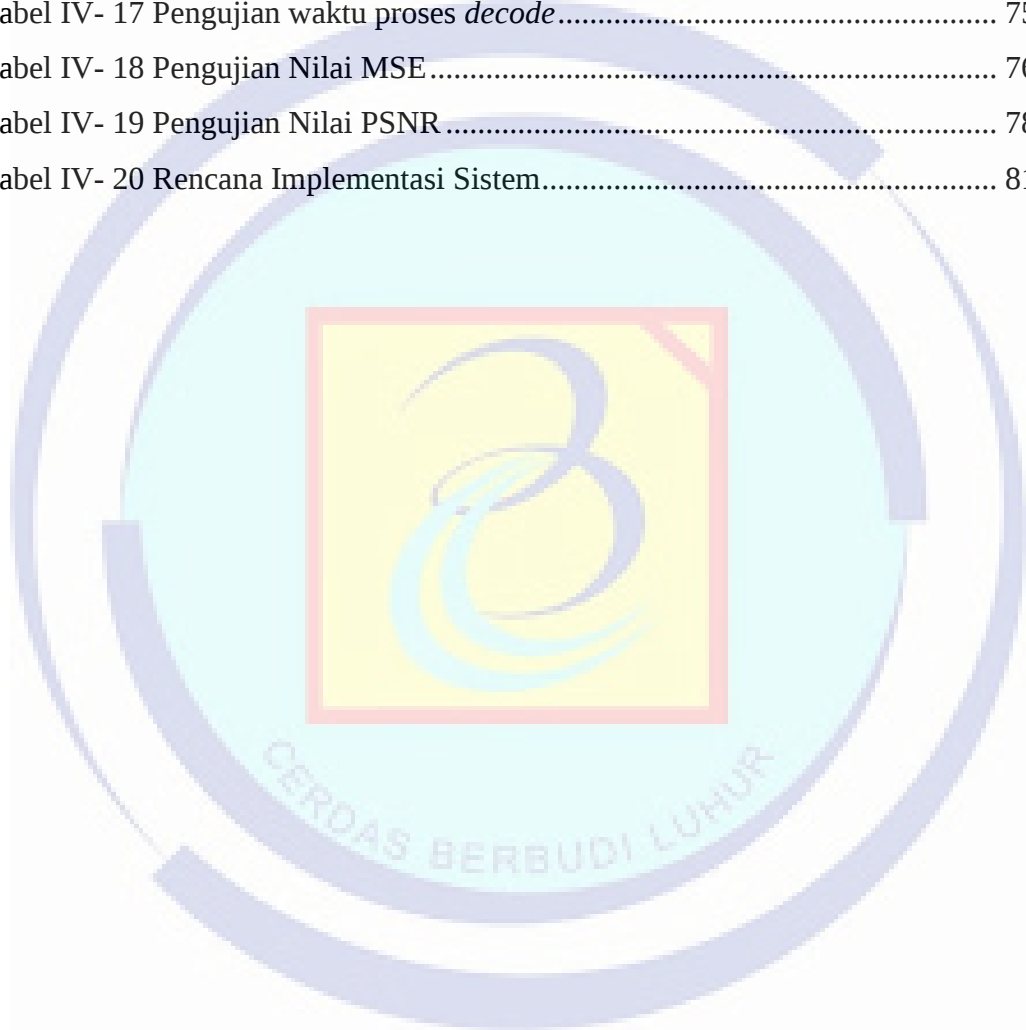
Gambar IV- 13 Pengujian Nilai PSNR	78
--	----



DAFTAR TABEL

Tabel I-1 Daftar Pengertian Istilah.....	6
Tabel II-1 Perbandingan kriptografi kunci simetrik dan asimetrik.....	11
Tabel II-2 Perbandingan Block Cipher dan Stream Cipher	11
Tabel II-3 Perbandingan beberapa algoritma kriptografi.....	12
Tabel II-4 Perbandingan Jumlah <i>round</i> dan <i>Key</i>	16
Tabel II-5 S-Box dalam algoritma AES.....	18
Tabel II-6 Invers S-Box algoritma AES.....	21
Tabel II-7 Tinjauan Studi	33
Tabel III-1 Jadwal Penelitian	46
Tabel IV-1 Tabel Pengujian Keamanan file doc. Citra PNG dengan tools StegSpy 2.1.....	57
Tabel IV-2 Tabel Pengujian Keamanan file pdf. Citra PNG dengan tools StegSpy 2.1.....	59
Tabel IV- 3 Tabel Pengujian Keamanan file txt. Citra PNG dengan tools StegSpy 2.1.....	60
Tabel IV- 4 Tabel Pengujian Keamanan file doc. Citra BMP dengan <i>tools StegSpy 2.1</i>	61
Tabel IV- 5 Tabel Pengujian Keamanan file pdf. Citra BMP dengan <i>tools StegSpy 2.1</i>	63
Tabel IV- 6 Tabel Pengujian Keamanan file ptxt. Citra BMP dengan <i>tools StegSpy 2.1</i>	64
Tabel IV- 7 <i>Encode</i> AES dan Blowfish (format doc.)	65
Tabel IV-8 <i>Encode</i> AES dan Blowfish (format .pdf)	66
Tabel IV- 9 <i>Encode</i> AES dan Blowfish (format txt).....	68
Tabel IV- 10 <i>Decode</i> AES dan Blowfish (format doc).....	68
Tabel IV-11 <i>Decode</i> AES dan Blowfish (format pdf.)	69
Tabel IV-12 <i>Decode</i> AES & Blowfish (format txt.)	70
Tabel IV- 13 Pengujian <i>stegoimage</i> dengan MSE dan PSNR	71

Tabel IV- 14 Hasil Pengujian Keamanan Pesan citra PNG dengan <i>tools StegSpy</i> 2.1.....	72
Tabel IV- 15 Hasil Pengujian Keamanan Pesan citra BMP dengan <i>tools StegSpy</i> 2.1.....	72
Tabel IV- 16 Pengujian waktu <i>encode</i>	73
Tabel IV- 17 Pengujian waktu proses <i>decode</i>	75
Tabel IV- 18 Pengujian Nilai MSE.....	76
Tabel IV- 19 Pengujian Nilai PSNR.....	78
Tabel IV- 20 Rencana Implementasi Sistem.....	81



DAFTAR PUSTAKA

- Anon, 2016. A Comparative Study and Performance Evaluation of Cryptographic Algorithms : AES and A Comparative Study and Performance Evaluation of Cryptographic Algorithms : AES and Blowfish. , (December).
- Anon, SpyHunter. Available at: <http://www.spy-hunter.com/stegspydownload.htm> [Accessed September 1, 2018].
- Baby, D. et al., 2015. A Novel DWT based Image Securing Method using Steganography. *Procedia - Procedia Computer Science*, 46(Icict 2014), pp.612–618. Available at: <http://dx.doi.org/10.1016/j.procs.2015.02.105>.
- Bhardwaj, R. & Sharma, V., 2016. Image Steganography Based on Complemented Message and Inverted bit LSB. *Procedia - Procedia Computer Science*, 93(September), pp.832–838. Available at: <http://dx.doi.org/10.1016/j.procs.2016.07.245>.
- CnnIndonesia, 2018. Mark Zuckerberg Angkat Bicara Soal Skandal Pencurian Data. *cnnindonesia.com*, p.1. Available at: <https://www.cnnindonesia.com/teknologi/20180322114136-185-284972/mark-zuckerberg-angkat-bicara-soal-skandal-pencurian-data> [Accessed June 10, 2018].
- CnnIndonesia, 2016. No Title. *CnnIndonesia*. Available at: <https://www.cnnindonesia.com/teknologi/20160111102243-185-103377/jawaban-lengkap-nadiem-soal-bug-aplikasi-gojek?>
- Gupta, A. & Walia, N.K., 2014. Cryptography Algorithms : A Review. , 2(2), pp.1667–1672.
- Gyamfi, E., 2017. Using LSB Steganography Technique and 256 bits Key Length AES Algorithm for High Secured Information Hiding International Journal of Advanced Research in Using LSB Steganography Technique and 256 bits Key Length AES Algorithm for High Secured Information . , (June).