

**TEKNIK STEGANOGRAFI MENGGUNAKAN METODE
LEAST SIGNIFICANT BIT (LSB) INTERPOLASI DAN
ADVANCED ENCRYPTION STANDARD (AES)
UNTUK PENGAMANAN DATA**

(Studi Kasus: Soal ujian Universitas Singaperbangsa Karawang)

TESIS



Oleh:

GARNO

1411600990

**PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2016**

**TEKNIK STEGANOGRAFI MENGGUNAKAN METODE
*LEAST SIGNIFICANT BIT (LSB) INTERPOLASI DAN
ADVANCED ENCRYPTION STANDARD*
UNTUK PENGAMANAN DATA**

(Studi Kasus: Soal ujian Universitas Singaperbangsa Karawang)

TESIS

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



Oleh:

GARNO

1411600990

**PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2016**



PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini

Nama Mahasiswa

: Barrio

Nomor Induk Mahasiswa

: 14.11.600990

Konsentrasi

: Rekayasa komputasi terapan

Program Studi

: Magister Ilmu komputer (Mkom)

Fakultas/Program

: Pascasarjana

Menyatakan bahwa Tesis yang berjudul :

Teknik steganografi menggunakan metode least significant bit (LSB) Interpolasi dan advanced encryption standard (AES) untuk pengamanan data
Studi Kasus : Soal Ujian Universitas Singaperbangsa Karawang

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 yang berlaku apabila dikemudian hari pernyataan ini tidak benar.

Jakarta, 13, Agustus 2016





PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Garno
Nomor Induk Mahasiswa : 1411600990
Konsentrasi : Rekayasa Komputasi Terapan
Program Studi : Magister Ilmu Komputer (MKOM)
Judul Proposal Tesis : Teknik Steganografi Menggunakan *Metode Least Significant Bit* (LSB) Interpolasi dan *Advanced Encryption Standard* (AES) untuk Pengamanan Data (Studi kasus: Soal ujian Universitas Singaperbangsa Karawang)

Jakarta, Senin 1 Agustus 2016

Tim Penguji

Tanda Tangan

Ketua,

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

Anggota,

Arief Wibowo, M. Kom

Pembimbing Utama,

Dr. Ir. Nazori AZ, MT

Ketua Program Studi
Magister Ilmu Komputer

(Dr. M. Syafrullah, M.Kom, M.Sc)

ABSTRACT

The research discussed today is about steganography, Reviewed steganographic techniques there are various, but most are of such techniques have not yet inserted a large file and is given the security system of encryption techniques, then in this study will propose steganographic techniques by the method of least significant bit (LSB), but as the cover to do the interpolation process beforehand, so as to insert large amounts of data and are given security encryption techniques advanced encryption standard (AES) as double security. Contributions given to research is the application of double security and the level of accuracy of the data capacity of the image bigger secret without affecting the quality of the original image imperceptibility stegoimage, but studies have not considered the estimated speed of the process, the success of steganography and encryption techniques can be used for embedding files doc, docx, pdf and compress files and zip winrar. PSNR accuracy rate is still below 40dB, the accuracy of the average PSNR a maximum of up to 38 dB with an average MSE 1.02 s / d 7.42

Keywords: *Steganography, Least Significant Bit (LSB), Interpolation, cryptography, advanced encryption standard (AES), stego image, file embedding, encryption, decryption, double security, imperceptibility image.secret stego data. compress files*

ABSTRAK

Penelitian yang dibahas sekarang adalah tentang steganografi, pada teknik steganografi ada berbagai macam, namun kebanyakan yang dari teknik tersebut belum menyisipkan *file* yang besar dan di berikan sistem *security* dari teknik enkripsi, maka pada penelitian ini akan mengusulkan teknik steganografi dengan metode *least significant bit* (LSB), namun sebagai *covernya* dilakukan proses interpolasi terlebih dahulu sehingga dapat menyisipkan data yang besar dan diberikan enkripsi dengan teknik *security advanced encryption standard* (AES) sebagai keamanan ganda. Kontribusi yang diberikan pada penelitian yaitu penerapan *double security* dan tingkat akurasi daya tampung *image* terhadap data *secret* lebih besar tanpa mempengaruhi kualitas *imperceptibility stegoimage* terhadap *image* asalnya, namun penelitian belum mempertimbangkan estimasi kecepatan proses, keberhasilan teknik steganografi dan enkripsi dapat digunakan untuk *embedding file doc, docx, pdf* dan *kompres file winrar dan zip* dengan tingkat akurasi PSNR masih dibawah 40dB, yaitu akurasi PSNR rata-rata maksimal hanya mencapai 38 dB dengan MSE rata-rata 1,02 s/d 7,42

Kata Kunci: *Steganografi, Least Significant Bit (LSB), Interpolasi, kriptografi, advanced encryption standard (AES), stego image, embedding file, enkripsi, dekripsi, double security, imperceptibility stegoimage. secret data. kompres file.*

KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang senantiasa memberikan nikmat dan karunia-Nya, sehingga penulisan dapat menyelesaikan penelitian berjudul “Teknik Steganografi menggunakan metode *least significant bit* (LSB) interpolasi dan *advanced encryption standard* (AES) untuk pengamanan data studi kasus soal ujian Universitas Singaperbangsa Karawang”. Shalawat dan salam tidak lupa penulis ucapkan pada baginda Nabi Muhammad Saw, keluarganya, para sahabatnya, serta semua para umatnya yang selalu melakukan kebaikan dimuka bumi hingga hari ini.

Penulis menyadari untuk menghasilkan tulisan yang baik tidak mudah, kerana banyak menyita waktu. Berkat keuletan dan kegigihan penulis, sehingga penulisan penelitian tesis ini dapat diselesaikan, dan penulis menyadari sepenuhnya bahwa dalam penulisan penelitian ini, mendapatkan bantuan dari berbagai pihak, maka penulis mengucapkan terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Prof. Ir. Suryo Hapsono Tri Utomo, Ph.D selaku Rektor Universitas Budi Luhur.
2. Dr. Sugiharto, M.Sc., M.Fin selaku direktur program pascasarjana Universitas Budi Luhur
3. Prof. Dr. Moedjiono, M.Sc selaku mantan direktur pascasarjana Universitas Budi Luhur.
4. Dr. M. Syafrullah, M.Sc selaku kepala program studi magister ilmu komputer dan sebagai penguji 1 pada sidang proosal dan sidang tesis.
5. Dr. Ir. Nazori Az, M.T selaku pembimbing satu dan sebagai dosen matakuliah Rekayasa Komputasi Terapan.
6. Arif Wibowo, M.Kom sebagai penguji 2 pada sidang proposal dan sidang tesis.
7. Rusdah, M.Kom., selaku Pembimbing dua dan sebagai dosen matakuliah Keamanan Sistem dan Jaringan Komputer.

8. Prof. Dr. Setyawan Widyarto selaku dosen matakuliah Pengolahan Citra Digital.
9. Prof Ki-Hyun Jung, Department of Cyber Security, Kyungil University, 50 Gamasil-Gil, Hayang-Eup, Gyeongsan-Si, Gyeongbuk 38428, Republic of Korea, yang mengajarkan teknik *image* interpolasi.
10. Khan Muhammad., Phd, Department of Computer Science, Islamia College Peshawar, K.P.K, Pakistan, yang bekerja di Research Associate Intelligent Media Laboratory Department of Digital contents Sejong University, Seoul, South Korea, yang mengajarkan teknik steganografi pada citra berwarna dengan metode random.
11. Asoke Nath, Associate Professor, Dept. of Computer Science, St. Xavier's College (Autonomous), Kolkata, India, yang mengajarkan teknik hiding file dan enkripsi dengan *advanced encryption standard* (AES)
12. Ashish Soni, Assistant Professor, ECE Dept. Acropolis Technical Campus, Indore, Rajiv Gandhi University, yang mengajarkan teknik LSB system metode selek bit.
13. Habibullah Akbar, Ph.D, Universitas Bina Nusantara, yang mengajarkan Matlab step-bystep.
14. Para Dosen Program Studi Magister Ilmu Komputer yang telah memberi bekal ilmu pengetahuan kepada penulis, semoga ilmunya menjadi amal sholeh yang berkesinambungan di dunia hingga akhirat.
15. Staff Tata Usaha Universitas Budi Luhur yang telah melayani administrasi akademik.
16. Oman Komarudin, S. Si., M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang yang telah memberikan ijin sebagai tempat penelitian.
17. Ade Andri Hendriadi, S.Si., M.Kom selaku Wakil Dekan Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang yang telah memberikan ijin sebagai tempat penelitian.
18. Aris Suharso, S.Si.,M.Kom selaku Kaprodi Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang yang telah memberikan ijin sebagai tempat penelitian.

19. Ahmad Fauzi, S. Kom., M. Kom selaku Dekan Fakultas Teknologi dan Ilmu Komputer Universitas Buana Perjuangan Karawang yang telah memberikan dispensasi waktu untuk mengerjakan penelitian tugas akhir.
20. Hanny Hikmayanti H, S. Kom., M. Kom selaku Kaprodi Fakultas Teknologi dan Ilmu Komputer Universitas Buana Perjuangan Karawang yang telah memberikan bimbingan penelitian bidang komputasi terapan.
21. Slamet Abadi, S.Si., M.Si selaku Kaprodi Fakultas Agro Teknologi Universitas Singaperbangsa Karawang yang selalu support dan memberikan motivasi dan bimbingan penelitian.
22. Istri dan anak atas segala kasih sayang, perhatian, dukungan dan doa yang senantiasa tercurah tanpa henti.
23. Bapak dan Ibu, Kakak dan Adik atas segala kasih sayang, perhatian, dukungan dan doa yang senantiasa tercurah tanpa henti.
24. Rekan-rekan Karawang Team Deden Wahiddin, Carudin, Jamaludin Indra, Nono Heryana, Arif Sholehudin dan Rini Mayasari yang selalu support dan kekompakan.
25. Seluruh rekan-rekan S2 Universitas Budi Luhur angkatan 2014 dan seluruh pihak yang telah membantu, yang tidak dapat Penulis sebutkan satu per satu.

dalam penulisan ini masih banyak kekurangan yang perlu diperbaiki, maka penulis mengharapkan masukan dalam bentuk kritikan dan saran yang sangat berari untuk membangun tulisan penelitian ini, demi menghasilkan bentuk hasil penelitian yang lebih baik, harapan penulis, penelitian dan penulisan laporan ini dapat bermanfaat dan memberikan kontribusi positif bagi penulis khususnya dan masyarakat pada umumnya dan Semoga Allah SWT melimpahkan karunia-Nya kepada kita semua, amin.

Karawang, juni 2016

Penulis

DAFTAR ISI

ABSTRACT	i
ABSTRAK	ii
KATA PENGANTAR.....	iii
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	ix
DAFTAR LAMPIRAN	x
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Masalah Penelitian.....	3
1.3 Tujuan dan Manfaat Penelitian	4
1.4 Tata Urut Penulisan	5
1.5 Daftar Pengertian	7
BAB II LANDASAN TEORI DAN KERANGKA PEMIKIRAN	9
2.1 Tinjauan Pustaka.....	9
2.2 Tinjauan Studi	39
2.3 Perbedaan Penelitian Sebelumnya.....	41
2.4 Tinjauan Objek Penelitian	42
2.5 Pola Pikir.....	42
2.5 Hipotesis.	44
BAB III METODOLOGI DAN DESAIN PENELITIAN	45
3.1 Metode Penelitian	45
3.2 Metode Pemilihan Sampel.....	63
3.3 Metode Pengumpulan Data.	63
3.3 Sumber dan Instrumen Data.....	64
3.4 Teknik Analisis, Perancangan dan Pengujian Sistem.....	64
3.5 Langkah-langkah Penelitian	67
3.7 Jadwal Penelitian	69
BAB IV PEMBAHASAN DAN HASIL PENELITIAN	70
4.1 Pengelompokan Data, Analisis dan Temuan-Temuan.....	70

4.2 Perancangan Sistem.....	73
4.3 Konstruksi Model	83
4.4 Pengujian Sistem (<i>Testing</i>).....	84
4.5 Implikasi Penelitian.....	94
4.6 Rencana Implementasi Sistem.	97
BAB V PENUTUP.....	99
5.1 Kesimpulan.....	99
5.2 Saran.....	99
DAFTAR PUSTAKA.....	101
LAMPIRAN-LAMPIRAN.....	105
RIWAYAT HIDUP SINGKAT	140



DAFTAR GAMBAR

Gambar II-1	: Proses Steganografi.....	12
Gambar II-2	: Proses Umum Penyisipan dan Ekstraksi Pesan.....	13
Gambar II-3	: Kategori Metode Steganografi Citra Digital.....	15
Gambar II-4	: Proses Enkripsi AES.....	26
Gambar II-5	: Ilustrasi Proses <i>SubByte</i>	28
Gambar II-6	: Ilustrasi pergeseran pada proses <i>ShiftRow</i>	29
Gambar II-7	: Ilustrasi Proses Dekripsi AES	31
Gambar II-8	: Ilustrasi Proses <i>InvShiftRows</i>	32
Gambar II-9	: Aspek Dasar Extreme Programing	35
Gambar II-10	: Kerangka Berfikir Steganografi.....	43
Gambar III-1	: Alur Sistem	45
Gambar III-2	: Metode Penyisipan Pesan ke dalam <i>Image</i>	49
Gambar III-3	: Metode Ekstraksi Pesan dari <i>Stego Image</i>	51
Gambar III-4	: Ilustrasi <i>state array Input</i> dan <i>Output</i>	52
Gambar III-5	: Proses enkripsi <i>plainfile</i> menjadi <i>cipherfile</i>	53
Gambar III-6	: Proses Dekripsi.....	60
Gambar III-7	: Tahapan Penelitian.....	68
Gambar IV-1	: <i>Use case diagram</i> aplikasi.....	74
Gambar IV-2	: Arsitektur aplikasi Steganografi.....	75
Gambar IV-3	: <i>Flowchart</i> Enkripsi dan Dekripsi dengan AES.....	76
Gambar IV-4	: <i>Flowchart Encode</i> dan <i>Decode</i> Steganografi LSB.....	77
Gambar IV-5	: Proses Sistem <i>Encode</i> Steganografi.....	78
Gambar IV-6	: Proses Sistem <i>Decode</i> Steganografi.....	79
Gambar IV-7	: Diagram alir <i>encode/embedding file</i> informasi ke <i>cover image</i>	80
Gambar IV-8	: Diagram alir <i>decode</i> ekstrak <i>file secret</i> dari <i>stego image</i>	81
Gambar IV-9	: Perancangan Antarmuka Aplikasi Steganografi.....	82
Gambar IV-10	: <i>Interface</i> Aplikasi Steganografi. <i>fig</i> LSB.....	84
Gambar IV-11	: <i>Interface</i> Run Aplikasi Steganografi LSB.....	84

DAFTAR TABEL

Tabel I-1	: Daftar Pengertian Istilah.....	7
Tabel II-1	: Perbandingan Jumlah <i>Round</i> dan <i>Key</i>	23
Tabel II-2	: S – BOX.....	27
Tabel II-3	: <i>Rcon[i]</i>	31
Tabel II-4	: <i>Inverse S-Box</i>	33
Tabel II-5	: Tinjauan Studi.....	39
Tabel III-1	: Jadwal Penelitian.....	68
Tabel IV-1	: Daftar <i>file</i> uji.....	72
Tabel IV-2	: Daftar <i>Image</i> Uji	72
Tabel IV-3	: Pengujian enkripsi AES.....	85
Tabel IV-4	: Pengujian Interpolasi <i>cover image</i>	85
Tabel IV-5	: Pengujian <i>encode</i> steganografi	86
Tabel IV-6	: Pengujian <i>decode</i> steganografi	87
Tabel IV-7	: Pengujian dekripsi AES.....	87
Tabel IV-8	: Hasil Pengujian Kriteria <i>Imperceptibility</i>	88
Tabel IV-9	: Hasil Pengujian Kriteria <i>Fidelity</i>	89
Tabel IV-10	: Hasil Pengujian Kriteria <i>Robustness</i>	90
Tabel IV-11	: Hasil Pengujian Kriteria <i>Recovery</i>	91
Tabel IV-12	: Hasil Pengujian Performansi	91
Tabel IV-13	: Daftar <i>User</i>	92
Tabel IV-14	: Daftar pernyataan fungsionalitas aplikasi	93
Tabel IV-15	: Daftar pernyataan pengujian usability aplikasi.....	93

DAFTAR LAMPIRAN

Lampiran Scrt Program Matlab Proses Enkrip <i>File</i> Pesan.....	105
Lampiran Scrt Program Matlab Proses Dekrip <i>File</i> Pesan.....	106
Lampiran Scrt Program Matlab Proses Interpolasi <i>cover Image</i>	107
Lampiran Scrt Program Matlab Proses <i>Encode</i> Steganografi LSB.....	108
Lampiran Scrt Program Matlab Proses <i>Decode</i> Steganografi LSB.....	112
<i>Lampiran 4.1.4 Analisis dan Temuan-Temuan, File pesan berbentuk doc atau docx dan pdf dan winrar serta zip</i>	115
Lampiran 4.1.4 Analisis dan Temuan-Temuan, <i>Image</i> sebagai <i>Cover</i>	122
Lampiran 4.4.1 Pengujian Enkripsi <i>file</i> pesan.....	123
Lampiran 4.4.2 Pengujian Proses Interpolasi <i>Cover Image</i>	124
Lampiran 4.4.3 Pengujian Proses <i>Encode</i> /Steganografi dengan LSB (<i>Hidding Cipherfile</i> ke <i>Image</i> interpolasi).....	125
Lampiran 4.4.4 Pengujian Proses Ekstrak/decode Steganografi dengan LSB (<i>Cipherfile</i> dari <i>StegoImage</i>).....	126
Lampiran 4.4.5 Pengujian Proses Dekripsi <i>Cipherfile</i> menjadi <i>Plainfile</i> /file pesan.....	127
Lampiran 4.4.7 Pengujian Objektif Citra Hasil <i>Stego</i> Aspek <i>Imperceptibility</i>	128
Lampiran 4.4.8 Pengujian Objektif Citra Hasil <i>Stego</i> Aspek <i>Fidelity</i>	129
Lampiran 4.4.9 Pengujian Objektif Citra Hasil <i>Stego</i> Aspek <i>Robustness</i> ...	130
Lampiran 4.4.10 Pengujian Objektif Citra Hasil <i>Stego</i> Aspek <i>Recovery</i>	132
Lampiran 4.4.11 Angket pengujian fungsionalitas dan usability.....	133
Lampiran Teksseperempat1.docx.....	134
Lampiran Teksseperempat.pdf	135
Lampiran Tekssetengah.docx.....	136
Lampiran TekssetengahNGambar.docx.....	137
Lampiran TekssetengahNGambar.pdf.....	138
Lampiran Hasil ekstrak Channel mixer 50 % green.....	139

DAFTAR PUSTAKA

- Aditya, Y., A. Pratama, dan A. Nurlita, 2010, *Studi Pustaka untuk Steganografi dengan Beberapa Metode*, Jurnal , Fakultas Teknologi Industri UII.
- A.Joseph Raphael, V.Sundaram, *Cryptography and Steganography-A Survey*, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630, ISSN:2229-6093.
- Ariyus Dony, 2009, *Keamanan Multimedia*. Penerbit Andi. Yogyakarta. ISBN 9789792902.
- Ariyus, Dony. 2007. *Keamanan Multimedia*. Yogyakarta: Andi.
- Bakshi, Nishesh, 2007, *Steganography*. Syracuse University.
- Budi Prasetyo, Rahmat Gernowo, 2014, *Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data*, Scientific journal of informatics, vol. 1, No. 1, ISSN 2407-7658.
- Budi Raharjo, 1999, *Keamanan Sistem Informasi berbasis internet*, Infonesia Bandung.
- B. Sharmila and R. Shanthakumari, (2012) “Efficient Adaptive Steganography For Colour Images Based on LSBMR Algorithm”, ICTACT Journal on Image and Video Processing, Vol. 2, Issue:03, pp.387-392.
- C.P, S., T, S., & G, U. (2013). *A Study of Various Steganographic Techniques Used for Information Hiding*. *International Journal of Computer Science & Engineering Survey*, 4(6), 9–25. <http://doi.org/10.5121/ijcses.2013.4602>
- Channalli, S., & Jadhav, A. (2009). *Steganography An Art of Hiding Data*, 1(3), 137–141. <http://doi.org/10.3923/itj.2004.245.269>.
- Dony Ariyus, 2006, *Kriptografi: Keamanan Data dan Komunikasi*, Graha Ilmu, Yogyakarta.
- Donny Seftyanto, Mega Apriani, Tony Haryanto, 2012, *Peran algoritma caesar cipher dalam membangun karakter akan kesadaran keamanan informasi, Prosiding seminar nasional matematika dan pendidikan matematika FMIPA UNY Yogyakarta*, 10 November 2012, ISBN:978-979-16353-8-7
- Farrell, Joyce. 2012. *Java Programming*. Course Technology, United State of America.