

**APLIKASI PENYEMBUNYIAN DAN PENGAMANAN PESAN
MENGUNAKAN NEW BLOCK CIPHER DAN DYNAMIC
STEGANOGRAPHY**

TUGAS AKHIR

Oleh:

JOKO HERMAWAN

NIM. 11.111.2514

MUHAMMAD NURAZMY BAKTI

NIM. 11.111.2557



**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
MIKROSKIL
MEDAN
2016**

**APPLICATION FOR HIDING AND SECURING MESSAGE
USING NEW BLOCK CIPHER AND DYNAMIC
STEGANOGRAPHY**

FINAL RESEARCH

By:

JOKO HERMAWAN

ID. 11.111.2514

MUHAMMAD NURAZMY BAKTI

ID. 11.111.2557



**STUDY PROGRAM OF INFORMATICS ENGINEERING
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
MIKROSKIL
MEDAN
2016**

LEMBARAN PENGESAHAN

APLIKASI PENYEMBUNYIAN DAN PENGAMANAN PESAN MENGUNAKAN NEW BLOCK CIPHER DAN DYNAMIC STEGANOGRAPHY

TUGAS AKHIR

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Sarjana Strata Satu
Program Studi Teknik Informatika

Oleh:

JOKO HERMAWAN

NIM. 11.111.2514

MUHAMMAD NURAZMY BAKTI

NIM. 11.111.2557

Disetujui Oleh:

Dosen Pembimbing I,

Kristian Telaumbanua S.T, M.T

Dosen Pembimbing II,

Andrew Sagitta Jauhari S.Kom, M.T

Medan, 24 Februari 2016

Diketahui dan Disahkan oleh

Ketua Program Studi
Teknik Informatika,

Hardy S.Kom, M.Sc.

Wakil Ketua I,

Djoni S.Kom, M.T.I

ABSTRAK

Seiring dengan semakin berkembangnya teknologi *internet*, terdapat banyak informasi yang perlu untuk dirahasiakan, namun tidak menarik perhatian dari pihak lain, yang berarti pihak lain tidak mengetahui bahwa telah terjadi komunikasi rahasia. Proses pengamanan data dengan metode enkripsi akan mengakibatkan pihak lain mengetahui bahwa agen rahasia tersebut telah mengirimkan suatu informasi rahasia kepada pihak lain.

Metode steganografi LSB dapat digunakan untuk menyelesaikan permasalahan diatas. Namun, metode LSB rentan terhadap penyerangan sehingga dilakukan modifikasi dengan menggabungkannya dengan metode *new block cipher*. Posisi penyisipan bit juga ditentukan secara dinamis pada saat penyisipan sehingga metode ini bersifat dinamis.

Penelitian ini menghasilkan beberapa informasi yaitu nilai MSE berbanding lurus dengan panjang pesan dan nilai PSNR berbanding terbalik dengan panjang pesan, nilai MSE dan PSNR untuk citra berbeda berukuran sama hanya sedikit mempengaruhi kualitas citra, nilai MSE untuk citra berbeda ukuran berbeda berbanding terbalik dengan ukuran citra sampel, perubahan warna piksel yang bukan pada daerah penyimpanan pesan tidak akan mempengaruhi pesan yang terekstrak keluar dan kunci stego tidak boleh memiliki pola yang berulang.

Kata kunci : steganografi, kriptografi, metode LSB, *ciphertext*, citra digital

UNIVERSITAS
MIKROSKIL

KATA PENGANTAR

Puji dan syukur kehadiran Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **“Aplikasi Penyembunyian dan Pengamanan Pesan menggunakan *New Block Cipher* dan *Dynamic Steganography*”** sebagai salah satu syarat menyelesaikan pendidikan Strata Satu Program Studi Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer Mikroskil.

Dengan segala kerendahan hati, penulis menyadari bahwa dalam menyelesaikan tugas akhir ini tidak lepas dari peran berbagai pihak yang telah banyak memberikan bantuan dan bimbingannya. Pada kesempatan ini penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Bapak Kristian Telaumbanua S.T, M.T., selaku dosen Pembimbing I yang telah memberikan banyak bimbingan dan pengarahan kepada penulis selama penulisan tugas akhir ini.
2. Bapak Andrew Sagitta Jauhari S.Kom, M.T., selaku dosen Pembimbing II yang telah memberikan banyak bimbingan dan pengarahan kepada penulis selama penulisan tugas akhir ini.
3. Bapak Dr. Mimpin Ginting, M.S., selaku ketua STMIK Mikroskil Medan.
4. Bapak Djoni S.Kom, M.T.I., selaku wakil ketua I STMIK Mikroskil Medan.
5. Bapak Hardy S.Kom., M.Sc., selaku ketua Program Studi Teknik Informatika STMIK Mikroskil Medan.
6. Bapak dan Ibu Dosen STMIK Mikroskil, Khususnya Dosen Teknik Informatika dan staf yang telah memberikan ilmu kepada penulis selama empat tahun lamanya, dan dukungan untuk menyelesaikan penulisan tugas akhir ini.
7. Teristimewa kepada kedua orang tua dan keluarga yang banyak memberikan dukungan, semangat dan doa dalam menyelesaikan tugas akhir.
8. Dan kepada sahabat-sahabat, kaka, abang dan semua pihak yang telah memberikan dukungan baik berupa moril maupun material dan semangat selama penulis mengikuti perbaikan hingga selesainya tugas akhir ini.

Penulis menyadari sepenuhnya bahwa masih terdapat banyak kekurangan dalam penyusunan tugas akhir ini. Oleh karena itu, penulis sangat mengharapkan dan menghargai saran dan kritik dari pembaca serta semua pihak yang bersifat membangun. Akhir kata, penulis berharap semoga tugas akhir ini dapat bermanfaat bagi kita semua.

Medan, 18 Februari 2016

Penulis



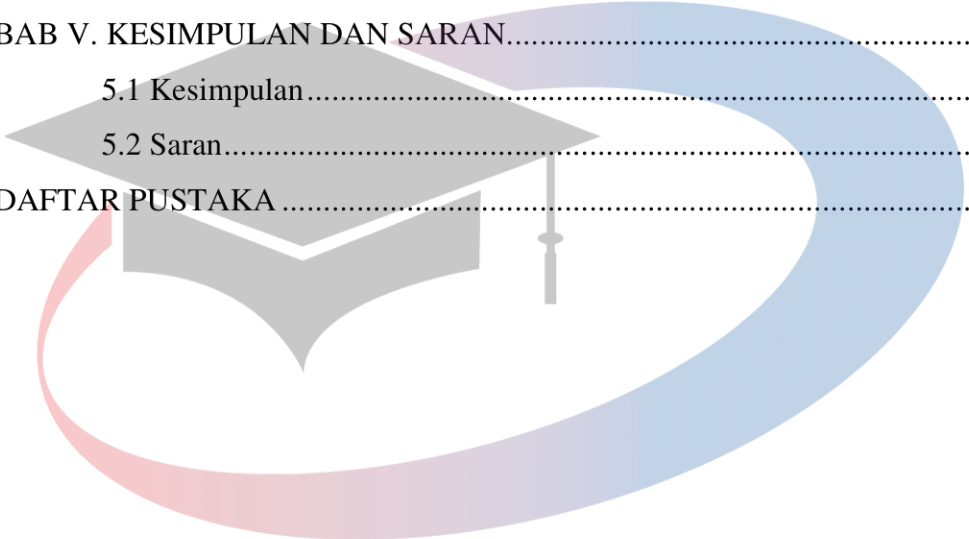
UNIVERSITAS MIKROSKIL

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI	iv
DAFTAR GAMBAR	vii
DAFTAR TABEL	xii
DAFTAR LAMPIRAN.....	xiii
BAB I. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan dan Manfaat	2
1.4 Batasan Masalah	3
1.5 Metodologi Penelitian.....	3
BAB II. TINJAUAN PUSTAKA	6
2.1 Steganografi	6
2.1.1 Metode Steganografi pada Teks	7
2.1.2 Metode Steganografi pada Gambar	9
2.1.3 Metode Steganografi pada Suara.....	11
2.2 Kriptografi	12
2.2.1 Algoritma Simetris	16
2.2.2 Algoritma Asimetri.....	17
2.2.3 Fungsi Hash.....	18
2.3 Citra Digital.....	18
2.3.1 Definisi Pengolahan Citra	18
2.3.2 Format Citra	25
2.3.3 Jenis Citra.....	27
2.3.4 Pengukuran Kualitas Citra	30
2.4 Block Cipher Baru dengan 256 Bit Kunci	31
2.4.1 Metode Hill Cipher	32
2.4.1 Algoritma Block Cipher Baru	32

2.5 Metode Dynamic Steganography	35
2.5.1 Teknik Penyisipan (Embedding) Dynamic Steganography	36
2.5.2 Teknik Penemuan Kembali Dynamic Steganography	37
2.5.3 Algoritma Skema New Block Cipher dengan Dynamic Steganography	38
BAB III. ANALISIS DAN PERANCANGAN	40
3.1 Analisis	40
3.1.1 Analisis Proses	40
3.1.1.1 Proses pada bagian Pengirim	40
3.1.1.2 Proses pada bagian Penerima.....	85
3.1.2 Analisis Kebutuhan.....	104
3.1.2.1 Analisis Kebutuhan Fungsional	104
3.1.2.2 Analisis Kebutuhan Non Fungsional	105
3.1.3 Pemodelan Sistem	106
3.2 Perancangan	111
3.2.1 Perancangan Form ‘Main’	111
3.2.2 Perancangan Form ‘Penyisipan’	112
3.2.2.1 Input Citra Sampul	112
3.2.2.2 Input Pesan Rahasia dan Enkripsi	113
3.2.2.3 Proses Enkripsi	114
3.2.2.4 Sisipkan Ciphertext ke Citra Sampul	115
3.2.3 Perancangan Form ‘Ekstraksi’	116
3.2.3.1 Input Citra Stego	116
3.2.3.2 Ekstrak Ciphertext dan Input Kunci	117
3.2.3.3 Dekripsi Ciphertext	118
3.2.4 Perancangan Form ‘Pengujian’	119
3.2.4 Perancangan Form ‘Mengenai Pembuat’	120
BAB IV. HASIL DAN PENGUJIAN	121
4.1 Hasil	121
4.1.1 Spesifikasi Perangkat Keras dan Perangkat Lunak.....	121
4.1.2 Hasil Eksekusi.....	121

4.2 Pengujian	129
4.2.1 Pengujian Berdasarkan Panjang Pesan	129
4.2.2 Pengujian Berdasarkan Citra Berbeda Berukuran Sama.....	136
4.2.3 Pengujian Berdasarkan Citra Berbeda Berukuran Berbeda ..	143
4.2.4 Pengujian Ekstraksi Pesan Setelah Menambahkan <i>Noise</i>	150
4.2.5 Pengujian Terhadap Stego Key yang Memiliki Pola yang Berulang	155
BAB V. KESIMPULAN DAN SARAN.....	160
5.1 Kesimpulan.....	160
5.2 Saran.....	161
DAFTAR PUSTAKA	162



UNIVERSITAS
MIKROSKIL

DAFTAR GAMBAR

Gambar 2.1 Plainteks berupa Teks dan Cipherteksnya.....	13
Gambar 2.2 Plainteks berupa Gambar dan Cipherteksnya.....	14
Gambar 2.3 Ilustrasi Algoritma Kunci Simetris	16
Gambar 2.4 (a) Citra burung nuri yang gelap, (b) Citra burung nuri yang telah diperbaiki kontrasnya sehingga terlihat jelas dan tajam.....	19
Gambar 2.5 Tiga bidang studi yang berkaitan dengan citra.....	20
Gambar 2.6 (a) Citra Lena asli, (b) Citra Lena setelah ditajamkan	21
Gambar 2.7 Kiri: Citra Lena yang kabur (blur), kanan: Citra Lena setelah deblurring.....	22
Gambar 2.8 (a) Citra boat.bmp (258 KB) sebelum dimampatkan, (b) citra boat.jpg (49 KB) setelah dimampatkan	22
Gambar 2.9 Contoh dari segmentasi citra	23
Gambar 2.10 (a) Citra camera, (b) Citra hasil pendeteksian seluruh tepi	23
Gambar 2.11 Citra biner.....	27
Gambar 2.12 Citra <i>grayscale</i>	28
Gambar 2.13 Citra warna 8 bit dengan palet.....	29
Gambar 2.14 Citra warna 16 bit.....	29
Gambar 2.15 Citra 24 bit.....	30
Gambar 3.1 <i>Flowchart</i> Proses pada Bagian Pengirim	41
Gambar 3.2 <i>Flowchart</i> Proses Enkripsi	42
Gambar 3.3 <i>Flowchart</i> Proses Penyisipan	44
Gambar 3.4 <i>Flowchart</i> Proses pada Bagian Penerima.....	85
Gambar 3.5 <i>Flowchart</i> Proses Dekripsi	86
Gambar 3.6 <i>Flowchart</i> Proses Ekstraksi	87
Gambar 3.7 <i>Use Case Diagram</i> dari Sistem	106
Gambar 3.8 Rancangan <i>Form</i> ‘Main’	111
Gambar 3.9 Rancangan <i>Form</i> ‘Proses Penyisipan – Input Citra Sampul’	112
Gambar 3.10 Rancangan <i>Form</i> ‘Penyisipan – Input Pesan Rahasia dan Kunci’	113
Gambar 3.11 Rancangan <i>Form</i> ‘Penyisipan – Proses Enkripsi’	114

Gambar 3.12 Rancangan <i>Form</i> ‘Penyisipan – Sisipkan <i>Ciphertext</i> ke Citra Sampul’	115
Gambar 3.13 Rancangan <i>Form</i> ‘Ekstraksi’	116
Gambar 3.14 Rancangan <i>Form</i> Penemuan Kembali <i>Ciphertext</i>	117
Gambar 3.15 Rancangan <i>Form</i> Dekripsi <i>Ciphertext</i>	118
Gambar 3.16 Rancangan <i>Form</i> Pengujian	119
Gambar 3.17 Rancangan <i>Form</i> tentang Aplikasi	120
Gambar 4.1 Tampilan <i>Form</i> Utama	122
Gambar 4.2 Tampilan <i>Form</i> Penyisipan	122
Gambar 4.3 Tampilan Kotak Dialog <i>Open</i>	123
Gambar 4.4 Tampilan <i>Form</i> Penyisipan Setelah Pemilihan Gambar	123
Gambar 4.5 Tampilan <i>Form</i> Penyisipan Setelah Pengisian Semua Data	124
Gambar 4.6 Tampilan <i>Form</i> Enkripsi	124
Gambar 4.7 Tampilan <i>Form</i> Penempelan Setelah Proses Penyisipan	125
Gambar 4.8 Tampilan Kotak Dialog <i>Save</i>	125
Gambar 4.9 Tampilan <i>Form</i> Setelah Proses Pemilihan Lokasi Penyimpanan Citra Stego	126
Gambar 4.10 Tampilan <i>Form</i> setelah proses penyimpanan citra stego berhasil	126
Gambar 4.11 Tampilan <i>Form</i> Ekstraksi	127
Gambar 4.12 Tampilan Kotak Dialog <i>Open</i>	127
Gambar 4.13 Tampilan <i>Form</i> Ekstraksi Setelah Pemilihan <i>File</i> Citra Stego ..	128
Gambar 4.14 Tampilan <i>Form</i> Ekstraksi Setelah Pengisian kunci dan Ekstraksi <i>Ciphertext</i>	128
Gambar 4.15 Tampilan <i>Form</i> Ekstraksi Setelah Proses Dekripsi	129
Gambar 4.16 (a) Pengujian dengan panjang pesan 1 karakter	130
Gambar 4.16 (b) Pengujian dengan panjang pesan 10 karakter	130
Gambar 4.16 (c) Pengujian dengan panjang pesan 100 karakter	130
Gambar 4.16 (d) Pengujian dengan panjang pesan 300 karakter	131
Gambar 4.16 (e) Pengujian dengan panjang pesan 500 karakter	131
Gambar 4.16 (f) Pengujian dengan panjang pesan 750 karakter	131
Gambar 4.16 (g) Pengujian dengan panjang pesan 1000 karakter	132

Gambar 4.16 (h) Pengujian dengan panjang pesan 2000 karakter.....	132
Gambar 4.16 (i) Pengujian dengan panjang pesan 3000 karakter.....	132
Gambar 4.16 (j) Pengujian dengan panjang pesan 5000 karakter.....	133
Gambar 4.17 Grafik hasil pengujian nilai MSE berdasarkan panjang pesan...	134
Gambar 4.18 Grafik hasil pengujian nilai PSNR berdasarkan panjang pesan.	134
Gambar 4.19 Grafik hasil pengujian waktu sisip dan waktu ekstrak berdasarkan panjang pesan	135
Gambar 4.20 (a) Pengujian berdasarkan citra berukuran sama dengan nama cute.jpg	136
Gambar 4.20 (b) Pengujian berdasarkan citra berukuran sama dengan nama hijabku.jpg	136
Gambar 4.20 (c) Pengujian berdasarkan citra berukuran sama dengan nama Tertawa.jpg.....	137
Gambar 4.20 (d) Pengujian berdasarkan citra berukuran sama dengan nama Apaa.jpg.....	137
Gambar 4.20 (e) Pengujian berdasarkan citra berukuran sama dengan nama Unyu.jpg	137
Gambar 4.20 (f) Pengujian berdasarkan citra berukuran sama dengan nama cipit.jpg.....	138
Gambar 4.20 (g) Pengujian berdasarkan citra berukuran sama dengan nama Ballet.jpg.....	138
Gambar 4.20 (h) Pengujian berdasarkan citra berukuran sama dengan nama Hahahaii.jpg.....	138
Gambar 4.20 (i) Pengujian berdasarkan citra berukuran sama dengan nama Hehehe.jpg.....	139
Gambar 4.20 (j) Pengujian berdasarkan citra berukuran sama dengan nama Hoaam.jpg.....	139
Gambar 4.21 Grafik hasil pengujian nilai MSE berdasarkan citra berbeda berukuran sama.....	141
Gambar 4.22 Grafik hasil pengujian nilai PSNR berdasarkan citra berbeda berukuran sama.....	141
Gambar 4.23 Grafik hasil pengujian waktu sisip dan waktu ekstrak berdasarkan citra berbeda berukuran sama	142

Gambar 4.24 (a) Pengujian berdasarkan citra dan ukuran berbeda (citra 1)....	143
Gambar 4.24 (b) Pengujian berdasarkan citra dan ukuran berbeda (citra 2) ...	143
Gambar 4.24 (c) Pengujian berdasarkan citra dan ukuran berbeda (citra 3)....	144
Gambar 4.24 (d) Pengujian berdasarkan citra dan ukuran berbeda (citra 4) ...	144
Gambar 4.24 (e) Pengujian berdasarkan citra dan ukuran berbeda (citra 5)....	144
Gambar 4.24 (f) Pengujian berdasarkan citra dan ukuran berbeda (citra 6)	145
Gambar 4.24 (g) Pengujian berdasarkan citra dan ukuran berbeda (citra 7) ...	145
Gambar 4.24 (h) Pengujian berdasarkan citra dan ukuran berbeda (citra 8) ...	145
Gambar 4.24 (i) Pengujian berdasarkan citra dan ukuran berbeda (citra 9)	146
Gambar 4.24 (j) Pengujian berdasarkan citra dan ukuran berbeda (citra 10) ..	146
Gambar 4.25 Grafik hasil pengujian nilai MSE berdasarkan citra berbeda berukuran berbeda	148
Gambar 4.26 Grafik hasil pengujian nilai PSNR berdasarkan citra berbeda berukuran berbeda	148
Gambar 4.27 Grafik hasil pengujian waktu sisip dan waktu ekstrak berdasarkan citra berbeda berukuran berbeda.....	149
Gambar 4.28 (a) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'Z' .	150
Gambar 4.28 (b) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'S' .	150
Gambar 4.28 (c) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'Y' .	150
Gambar 4.28 (d) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'T' .	151
Gambar 4.28 (e) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'V' .	151
Gambar 4.28 (f) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'H' .	151
Gambar 4.28 (g) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'A' .	152
Gambar 4.28 (h) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'R' .	152
Gambar 4.28 (i) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'M' .	152
Gambar 4.28 (j) Pengujian ekstraksi pesan setelah menambahkan <i>noise</i> 'G' .	153
Gambar 4.29 Pengujian terhadap <i>stego key</i> yang memiliki pola yang berulang 'a' sampai dengan 32 karakter	155
Gambar 4.30 Laporan hasil perhitungan pengujian pertama <i>stego key</i>	156

Gambar 4.31 Pengujian terhadap <i>stego key</i> yang memiliki pola yang berulang ‘12345678’ sampai dengan 32 karakter.....	157
Gambar 4.32 Laporan hasil perhitungan pengujian kedua <i>stego key</i>	157
Gambar 4.33 Pengujian terhadap <i>stego key</i> yang memiliki pola yang tidak berulang ‘ini tugas akhir skripsi kami yaa’	158
Gambar 4.34 Laporan hasil perhitungan pengujian ketiga <i>stego key</i>	159



DAFTAR TABEL

Tabel 2.1 Kualitas Citra	31
Tabel 2.2 Proses Penyisipan bit pada Citra.....	37
Tabel 3.1 Narasi dari <i>Use Case</i> Meng- <i>input</i> Pesan Rahasia.....	107
Tabel 3.2 Narasi dari <i>Use Case</i> Meng- <i>input</i> Citra Sampul.....	108
Tabel 3.3 Narasi dari <i>Use Case</i> Melakukan Proses Penyisipan Pesan Rahasia, Mengkripsi pesan dengan metode <i>new block cipher</i> dan Menyisipkan bit ciphertext dengan metode <i>dynamic steganography</i>	108
Tabel 3.4 Narasi dari <i>Use Case</i> Melakukan Proses Ekstraksi Pesan Rahasia, Mengekstrak bit <i>ciphertext</i> dengan metode <i>dynamic steganography</i> dan Mendekripsi <i>ciphertext</i> dengan metode <i>new block cipher</i>	110
Tabel 4.1 Tabel Pengujian berdasarkan panjang pesan	133
Tabel 4.2 Tabel Pengujian berdasarkan citra berbeda berukuran sama	140
Tabel 4.3 Tabel Pengujian berdasarkan citra berbeda berukuran berbeda.....	146
Tabel 4.4 Tabel Pengujian berdasarkan ekstraksi pesan setelah menambahkan noise.....	153

UNIVERSITAS
MIKROSKIL

DAFTAR LAMPIRAN

Lampiran 1. Listing Program	163
Lampiran 2. Daftar Riwayat Hidup	
Lampiran 3. Berita Acara Bimbingan Tugas Akhir	

