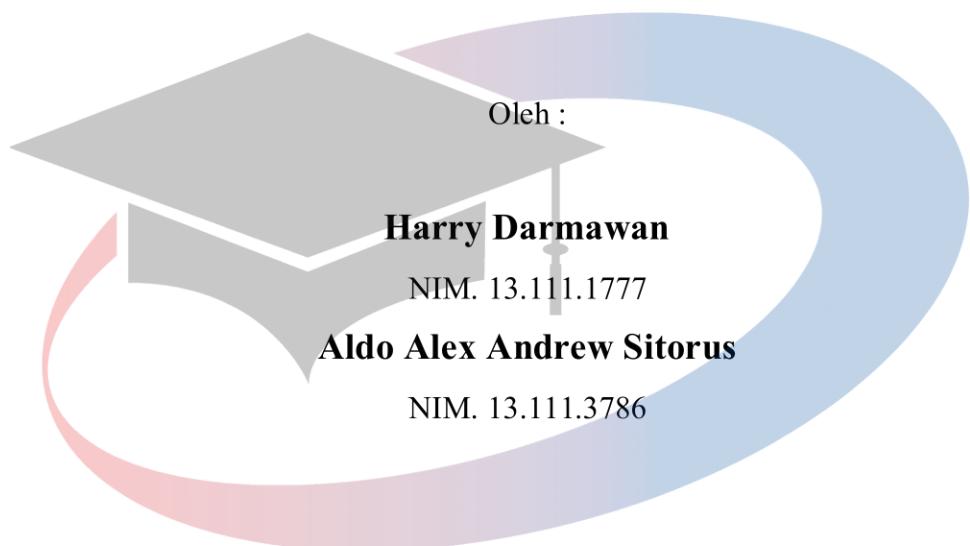


**PENGAMANAN DATA TEKS DENGAN NTRU DAN METODE
STEGANOGRAFI MODULUS FUNCTION PADA KOEFISIEN
IHWT SUATU CITRA WARNA**

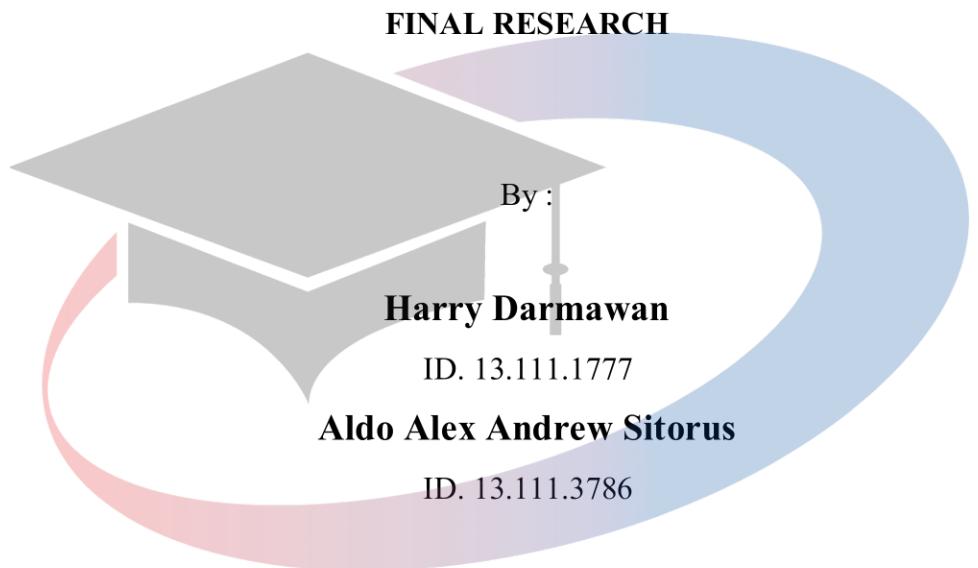
TUGAS AKHIR



**UNIVERSITAS
MIKROSKIL**

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
MIKROSKIL
MEDAN
2017**

**SECURING TEXT DATA WITH NTRU AND MODULUS
FUNCTION STEGANOGRAPHY METHOD ON
COEFFICIENT IHWT A COLOR IMAGES**



**UNIVERSITAS
MIKROSKIL**



**STUDY PROGRAM OF INFORMATICS ENGINEERING
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
MIKROSKIL
MEDAN
2017**

LEMBAR PENGESAHAN

**PENGAMANAN DATA TEKS DENGAN NTRU DAN METODE
STEGANOGRAFI MODULUS FUNCTION PADA KOEFISIEN
IHWT SUATU CITRA WARNA**

TUGAS AKHIR

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

Oleh:

Harry Darmawan

NIM. 13.111.1777

Aldo Alex Andrew Sitorus

NIM. 13.111.3786

Disetujui Oleh:

Dosen Pembimbing I,


Dr. Ronsen Purba, M.Sc.

Dosen Pembimbing II,


Irpan Adiputra Pardosi, S.Kom, M.TI

Medan, 12 Desember 2017
Diketahui dan Disahkan Oleh:

Ketua Program Studi
Teknik Informatika,


Sunario Megawan, S.Kom, M.Kom.

ABSTRAK

Perkembangan informasi *digital* telah menyebabkan meningkatnya teknologi informasi keamanan untuk melindungi suatu data teks yang mengandung kerahasiaan. Steganografi merupakan salah satu solusi untuk pengamanan data teks dengan melakukan proses penyembunyian data teks pada suatu gambar (citra) sehingga orang lain tidak mengetahui keberadaan data teks tersebut. Kriteria steganografi yang baik adalah *imperceptibility, fidelity, robustness* dan *recovery*.

Salah satu metode steganografi adalah CD (*Coefficient Difference*) yang diadopsi dari PVD (*Pixel Value Differencing*) yang melakukan penyembunyian pada domain spasial menggunakan selisih dari 2 nilai piksel sehingga menghasilkan jumlah modifikasi nilai piksel yang besar, membuat tingkat *imperceptibility* menurun. Metode *modulus function* digunakan untuk mengatasi kelemahan pada CD dengan menggunakan fungsi modulus pada penyisipannya sehingga dapat memperkecil modifikasi nilai piksel pada penyisipan sehingga meningkatkan tingkat *imperceptibility*. Dalam penelitian ini digunakan metode IHWT (*Integer Haar Wavelet Transform*) untuk menjaga tingkat *imperceptibility*. Untuk meningkatkan keamanan, metode kriptografi NTRU digunakan terhadap pesan rahasia sebelum pesan rahasia disembunyikan pada citra.

Hasil pengujian menunjukkan bahwa penggabungan metode NTRU, IHWT dan *modulus function* menghasilkan nilai *imperceptibility* yang baik dengan melihat nilai PSNR diatas 40dB dan citra stego tahan terhadap serangan *noise salt and pepper* nilai maksimal 0,002% dan serangan kontras dengan nilai maksimal 1.

Kata kunci: pengamanan data teks, imperceptibility dan transformasi

UNIVERSITAS
MIKROSKIL

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadiran Tuhan Yang Maha Esa atas segala berkat dan kasih karunia-Nya sehingga penulis dapat menyelesaikan penelitian Tugas Akhir Skripsi yang berjudul “Pengamanan Data Teks dengan NTRU dan Metode Steganografi Modulus Function pada Koefisien IHWT suatu Citra Warna”.

Tugas Akhir Skripsi ini disusun untuk memenuhi persyaratan kelulusan Sarjana Strata Satu (S1) Program Studi Teknik Informatika dengan konsentrasi bidang Komputasi Ilmiah di STMIK Mikroskil Medan.

Adapun keberhasilan dan kelancaran dalam penyusunan dan penulisan skripsi ini tidak lepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini peneliti ingin mengucapkan terima kasih kepada:

1. Bapak Dr. Ronsen Purba, M.Sc., selaku Dosen Pembimbing I (satu) yang telah meluangkan waktu untuk memberikan bimbingan, saran serta motivasi di saat menempuh studi maupun penyusunan skripsi.
2. Bapak Irpan Adiputra Pardosi, S.Kom, M.TI., selaku Dosen Pembimbing II (dua) yang telah meluangkan waktu untuk memberikan bimbingan, saran serta motivasi di saat menempuh studi maupun penyusunan skripsi.
3. Bapak Sunario Megawan, S.Kom., M.Kom., selaku Ketua Program Studi Teknik Informatika STMIK Mikroskil.
4. Bapak Felix, S.Kom., M.Kom., selaku Sekretaris jurusan Program Studi Teknik Informatika STMIK Mikroskil.
5. Bapak Dr. Mimpin Ginting, M.S., selaku Ketua STMIK Mikroskil.
6. Bapak Djoni, S.Kom., M.T.I., selaku Wakil Ketua I STMIK Mikroskil.
7. Bapak Paulus, S.Kom., M.T., selaku Wakil Ketua II STMIK Mikroskil.
8. Bapak Saliman, S.T., selaku Wakil Ketua III STMIK Mikroskil.

9. Bapak/Ibu Dosen yang telah mengajar dan memberikan bimbingan selama kuliah di STMIK Mikroskil.
10. Keluarga terkhususnya kedua orangtua saya yang telah memberikan kasih sayang yang tulus, materi, perhatian dan dukungan yang kuat serta doa kepada penulis.
11. Kepada rekan mahasiswa, teman-teman, dan orang-orang yang terdekat yang turut memberikan dorongan dan partisipasi hingga tugas akhir ini dapat diselesaikan dengan baik.

Doa dan ucapan syukur yang dapat penulis panjatkan, semoga Tuhan Yang Maha Kuasa senantiasa membala kebaikan yang telah Bapak, Ibu, Saudara, Keluarga, Teman dan Semua pihak yang memberikan dukungan.

Akhir kata, peneliti menyadari bahwa skripsi ini masih sangat memerlukan kritik dan saran yang membangun dari pembaca. Serta peneliti memohon maaf kepada seluruh pihak apabila terdapat kesalahan dalam penulisan skripsi ini. Semoga skripsi ini dapat menjadi sumbangan bagi pengembangan ilmu informatika khususnya di bidang komputasi ilmiah dan dapat bermanfaat bagi pihak yang berkepentingan.

UNIVERSITAS
MIKROSKIL

Medan, Agustus 2017

Harry Darmawan

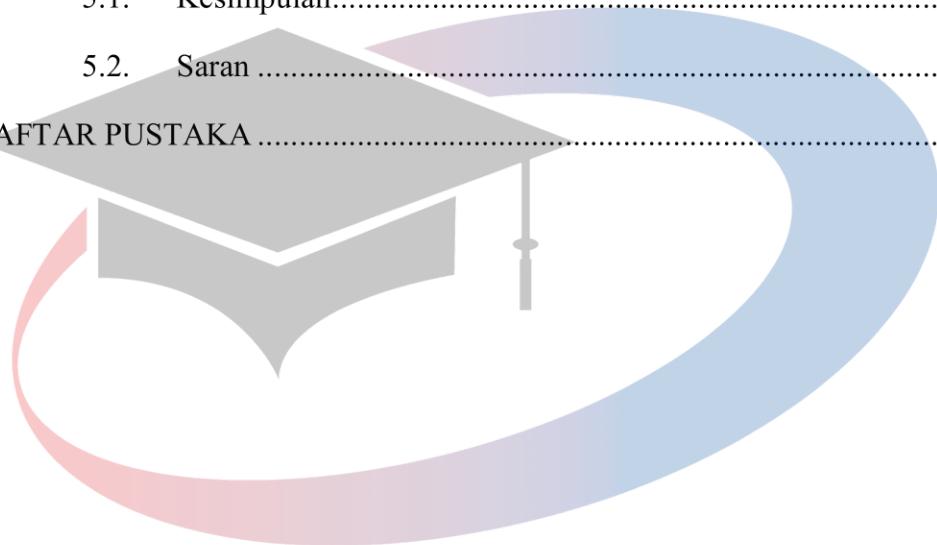
Aldo Alex Andrew Sitorus

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI	iv
DAFTAR GAMBAR	vii
DAFTAR TABEL	xii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	2
1.3. Tujuan	3
1.4. Manfaat	3
1.5. Ruang Lingkup	3
1.6. Metodologi Penelitian.....	4
BAB II TINJAUAN PUSTAKA.....	6
2.1 Kriptografi.....	6
2.1.1. Pengenalan Kriptografi	6
2.1.2. Kriptografi Kunci Simetris	6
2.1.3. Kriptografi Kunci Asimetris	7
2.2. NTRU.....	7
2.2.1. Pengenalan NTRU.....	7
2.2.2. Polinomial Pada NTRU	8
2.2.3. Proses pada NTRU	9
2.3. Wavelet Transform	11
2.3.1. Discrete Wavelet Transform (DWT).....	11

2.3.2. Integer Wavelet Transform (IWT)	11
2.3.3. Integer Haar Wavelet Transform (IHWT)	12
2.4. Steganografi.....	14
2.4.1. Pengenalan Steganografi.....	14
2.4.2. Kriteria Steganografi yang baik	14
2.4.3. Metode Steganografi.....	15
2.4.4. Proses Steganografi	23
2.5. Noise	25
2.5.1. Gaussian Noise	25
2.5.2. Noise Salt and Pepper	26
2.6. Peak Signal to Noise Ratio (PSNR).....	26
BAB III METODOLOGI PENELITIAN.....	28
3.1. Pengembangan Aplikasi.....	28
3.1.1. Analisis Sistem	28
3.2. Perancangan Sistem	65
3.2.1. Perancangan Form Menu Utama	65
3.2.2. Perancangan Form Penyisipan	66
3.2.3. Perancangan Form Ekstraksi.....	68
3.2.4. Perancangan Form Pengujian Imperceptibility	69
3.2.5. Perancangan Form Pengujian Robustness	71
BAB IV IMPLEMENTASI DAN PENGUJIAN.....	75
4.1. Implementasi	75
4.1.1. Form Menu Utama	75
4.1.2. Form Enkripsi Penyisipan.....	75
4.1.3. Form Ekstraksi Dekripsi	85

4.1.4. Form Pengujian	91
4.2. Pengujian.....	113
4.2.1. Pengujian Terhadap Imperceptibility	114
4.2.2. Pengujian Terhadap Robustness.....	119
BAB V KESIMPULAN DAN SARAN.....	131
5.1. Kesimpulan.....	131
5.2. Saran	131
DAFTAR PUSTAKA	133



UNIVERSITAS MIKROSKIL

DAFTAR GAMBAR

Gambar 2.1. Ilustrasi kriptografi kunci simetris (Odeh, A., dkk, 2015)	6
Gambar 2.2. Ilustrasi kriptografi kunci asimetris (Odeh, A., dkk, 2015)	7
Gambar 2.3. Dekomposisi tingkat 1 (Adi, P, W., dkk, 2015)	12
Gambar 2.4. Dekomposisi tingkat 2 (Adi, P, W., dkk, 2015)	13
Gambar 3.1. Flowchart proses penyisipan dan enkripsi data teks	29
Gambar 3.2. Flowchart pembangkitan kunci enkripsi dan kunci dekripsi.....	29
Gambar 3.3. Flowchart enkripsi data teks dengan NTRU	33
Gambar 3.4. Flowchart penyisipan data teks dengan modulus function	35
Gambar 3.5. Proses Transformasi IHWT tingkat 1	38
Gambar 3.6. Flowchart ekstraksi kunci dekripsi dan pesan acak dengan modulus function	46
Gambar 3.7. Flowchart dekripsi pesan acak dengan NTRU	49
Gambar 3.8. Use case diagram	52
Gambar 3.9. Perancangan menu utama.....	65
Gambar 3.10. Perancangan <i>form</i> penyisipan.....	66
Gambar 3.11. Perancangan <i>form</i> ekstraksi.....	68
Gambar 3.12. Perancangan form pengujian imperceptibility	70
Gambar 3.13. Perancangan form pengujian robustness terhadap noise.....	71
Gambar 3.14. Perancangan form pengujian robustness terhadap kontras	73
Gambar 4.1. Form menu utama	75
Gambar 4.2. Form Enkripsi Penyisipan	76
Gambar 4.3. Pembangkitan kunci dekripsi dan kunci enkripsi di form enkripsi penyisipan.....	77
Gambar 4.4. Enkripsi data teks di form enkripsi penyisipan	78
Gambar 4.5. Messagebox saat tidak ada dimasukkan pesan	78
Gambar 4.6. Messagebox panjang pesan yang dimasukkan melebihi standar panjang pesan dari parameter set	79

Gambar 4.7. Tampilan keseluruhan dari proses enkripsi data teks pada form enkripsi penyisipan	79
Gambar 4.8. Pembangkitan threshold acak pada form enkripsi penyisipan	80
Gambar 4.9. Pembangkitan kunci stego pada form enkripsi penyisipan	81
Gambar 4.10. Form dialog penyimpanan kunci stego di form enkripsi penyisipan	81
Gambar 4. 11. Messagebox penyimpanan kunci stego berhasil.....	82
Gambar 4.12. Form dialog mengambil citra sampul	82
Gambar 4.13. Form enkripsi penyisipan setelah dimasukkan citra sampul	83
Gambar 4.14. Tampilan keseluruhan proses enkripsi dan penyembunyian pada form enkripsi penyisipan	84
Gambar 4.15. Form dialog penyimpanan citra stego.....	84
Gambar 4.16. Messagebox untuk penyimpanan citra berhasil.....	85
Gambar 4.17. Form ekstraksi dekripsi	85
Gambar 4.18. Form dialog cari citra stego.....	86
Gambar 4. 19. Form ekstraksi dekripsi setelah citra stego dipilih oleh pengguna	86
Gambar 4. 20. Form dialog mencari kunci stego	87
Gambar 4.21. Form ekstraksi dekripsi setelah kunci stego dipilih pengguna.....	87
Gambar 4.22. Tampilan keseluruhan dari proses ekstraksi pada form ekstraksi dekripsi.....	88
Gambar 4. 23. Pemisahan kunci dekripsi dan pesan acak.....	89
Gambar 4.24. Tampilan keseluruan pada form ekstraksi dan dekripsi.....	90
Gambar 4.25. Form pengujian imperceptibility	91
Gambar 4.26. Mencari citra sampul pada form pengujian imperceptibility	92
Gambar 4. 27. Form pengujian imperceptibility setelah citra sampul dipilih pengguna	92
Gambar 4.28. Mencari citra stego pada form dialog untuk pengujian imperceptibility.....	93
Gambar 4.29. Form pengujian imperceptibility setelah citra stego dipilih pengguna	94

Gambar 4.30. Hasil perhitungan MSE dan PSNR di form pengujian imperceptibility	95
Gambar 4.31. Memasukkan nilai perhitungan MSE dan PSNR ke tabel pada form pengujian imperceptibility.....	96
Gambar 4.32. Microsoft excel yang berisi data pengujian dari tabel aplikasi di form pengujian imperceptibility.....	96
Gambar 4.33. Form pengujian robustness.....	97
Gambar 4.34. Mencari citra stego pada form dialog untuk pengujian robustness	98
Gambar 4.35. Form pengujian robustness terhadap noise setelah citra stego dipilih pengguna	98
Gambar 4.36. Form pengujian robustness setelah ditambahkan noise	99
Gambar 4.37. Messagebox saat pengguna menambahkan noise tetapi tidak memasukkan persentase noise	99
Gambar 4. 38. Form dialog untuk memilih tempat penyimpanan dari citra noise	100
Gambar 4.39. Form dialog untuk memilih kunci stego	100
Gambar 4.40. Form pengujian robustness dengan textbox kunci stego sudah terisi kunci stego.....	101
Gambar 4.41. Messagebox citra telah di simpan.....	101
Gambar 4.42. Hasil ekstraksi citra stego dengan citra stego setelah diberi noise pada form pengujian robustness	102
Gambar 4.43. Hasil perhitungan persentase pesan kembali pada form pengujian robustness.....	103
Gambar 4.44. Memasukkan nilai perhitungan persentase pesan kembali ke tabel pada form pengujian robustness	104
Gambar 4.45. Microsoft excel yang berisi data pengujian dari tabel aplikasi di form pengujian robustness terhadap noise.....	104
Gambar 4.46. Gambar form pengujian terhadap kontras.....	105
Gambar 4.47. Mencari citra stego pada form dialog untuk pengujian robustness	105

Gambar 4.48. Form pengujian robustness terhadap kontras setelah citra stego dipilih pengguna	106
Gambar 4. 49. Form pengujian robustness setelah ditambahkan nilai kontras ...	107
Gambar 4.50. Messagebox saat pengguna menambahkan kontras tetapi tidak memasukkan nilai kontras.....	107
Gambar 4.51. Form dialog penyimpanan citra stego yang telah diberi kontras..	108
Gambar 4.52. <i>Messagebox</i> citra stego yang telah diberi kontras telah di simpan	108
Gambar 4. 53. Form dialog untuk memilih kunci stego	109
Gambar 4.54. Form pengujian robustness dengan textbox kunci stego sudah terisi kunci stego.....	109
Gambar 4.55. Hasil ekstraksi citra stego dengan citra stego setelah ditambahkan kontras pada form pengujian robustness	110
Gambar 4.56. Hasil perhitungan persentase pesan kembali pada form pengujian robustness	111
Gambar 4.57. Memasukkan nilai perhitungan persentase pesan kembali ke tabel pada form pengujian robustness terhadap kontras.....	112
Gambar 4.58. Microsoft excel yang berisi data pengujian dari tabel aplikasi di form pengujian robustness terhadap kontras	112
Gambar 4.59. Form matrix value viewer untuk menampilkan piksel yang dilakukan penyisipan pada titik koordinat citra.....	113
Gambar 4.60. Grafik yang menunjukan nilai PSNR dan MSE pada citra peppers	118
Gambar 4. 61. Grafik yang menunjukan nilai PSNR dan MSE pada citra baboon.	118
Gambar 4. 62. Grafik yang menunjukan nilai PSNR dan MSE pada citra lena..	119
Gambar 4. 63. Grafik nilai persentase kembali pesan terhadap parameter set 401	122
Gambar 4. 64. Grafik nilai persentase kembali pesan terhadap parameter set 653	122
Gambar 4. 65. Grafik nilai persentase kembali pesan terhadap parameter set 1171	123

- Gambar 4. 66. Grafik nilai persentase kembali pesan pada citra peppers 126
Gambar 4. 67. Grafik nilai persentase kembali pesan pada citra baboon 129



DAFTAR TABEL

Tabel 2.1. Tabel standar parameter tingkat keamanan <i>NTRU</i> (Whyte, W., dkk, 2008)	10
Tabel 2.2. Ilustrasi modulus function (Wang, C. M., dkk, 2008).....	20
Tabel 2.3. Ilustrasi memecahkan permasalan penyimpangan dari batas dengan memodifikasi ulang $P_{(i,x)}$, $P_{(i,y)}$ (Wang, C. M., dkk, 2008)	21
Tabel 3. 1. Tabel hasil pencarian polinomial fp dari parameter NTRU dengan nilai $N = 7$, $p = 3$, $q = 32$ dan $df = 2$	31
Tabel 3. 2. Tabel hasil pencarian polinomial fq dari parameter NTRU dengan nilai $N = 7$, $p = 3$, $q = 32$ dan $df = 2$	31
Tabel 3.3. Nilai piksel pada citra sampul ukuran 4X4.....	36
Tabel 3.4. Nilai piksel citra pada setiap saluran setelah di modifikasi nilai piksel	37
Tabel 3.5. Nilai piksel citra pada setiap saluran setelah di modifikasi nilai piksel	38
Tabel 3.6. Nilai piksel pada citra persubband	39
Tabel 3.7. Nilai piksel citra sampul setelah transformasi	40
Tabel 3.8. Nilai piksel citra sampul setelah proses penyisipan	44
Tabel 3.9. Nilai piksel citra sampul setelah penyisipan dan IHWT invers	45
Tabel 3. 10. Nilai piksel citra stego setelah proses transformasi.....	47
Tabel 3. 11. Tabel narasi dari use case enkripsi / penyisipan data teks	52
Tabel 3.12. Tabel narasi dari use case ekstraksi / dekripsi data teks	55
Tabel 3. 13. Tabel narasi dari use case pengujian imperceptibility	57
Tabel 3. 14. Tabel narasi dari use case pengujian robustness	58
Tabel 4.1. Tabel rencana pengujian	114
Tabel 4.2. Tabel nilai PNSR dan MSE pada citra pepers	114
Tabel 4. 3. Tabel nilai PSNR dan MSE pada citra baboon	115
Tabel 4. 4. Tabel nilai PNSR dan MSE pada citra lena	116
Tabel 4. 5. Tabel nilai persentase kembali pesan pada citra <i>peppers</i>	119
Tabel 4. 6. Tabel nilai persentase kembali pesan pada citra <i>peppers</i>	123
Tabel 4. 7. Tabel nilai persentase kembali pesan pada citra baboon	126

DAFTAR LAMPIRAN

Lampiran 1. DAFTAR RIWAYAT HIDUP	214
Lampiran 2. DAFTAR RIWAYAT HIDUP	215
Lampiran 3. LISTING PROGRAM.....	135



**UNIVERSITAS
MIKROSKIL**