

**IMPLEMENTASI STEGANOGRAFI DAN KRIPTOGRAFI
DALAM MELINDUNGI PESAN CITRA DIGITAL**



SKRIPSI

**Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
Pada Jurusan Ilmu Komputer/Informatika**

**Disusun oleh:
Hafidh Wahyu Wibowo
J2F008030**

**JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2015**

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya menyatakan bahwa dalam tugas akhir / skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di Perguruan Tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis yang diacu pada naskah ini dan disebutkan dalam daftar pustaka.

Semarang, 20 Agustus 2015



Hafidh Wahyu Wibowo

J2F008030

HALAMAN PENGESAHAN

Judul : Implementasi Steganografi dan Kriptografi dalam Melindungi Pesan Citra Digital

Nama : Hafidh Wahyu Wibowo


NIM : J2F008030

Telah diujikan pada sidang Tugas Akhir tanggal 13 Agustus 2015 dan dinyatakan lulus pada tanggal 20 Agustus 2015.

Semarang, 20 Agustus 2015

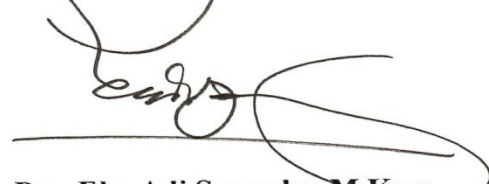
Mengetahui,

Ketua Jurusan Ilmu Komputer/Informatika
FSM Universitas Diponegoro,



Nurdin Baktiar, S.Si, M.T
NIP. 19790720 200312 1 002

Panitia Penguji Tugas Akhir
Ketua,



Drs. Eko Adi Sarwoko, M.Kom.
NIP. 19651107 199203 1 003

HALAMAN PENGESAHAN

Judul : Implementasi Steganografi dan Kriptografi dalam Melindungi Pesan Citra Digital
Nama : Hafidh Wahyu Wibowo
NIM : J2F008030

Telah diujikan pada sidang Tugas Akhir pada tanggal 13 Agustus 2015

Pembimbing I,

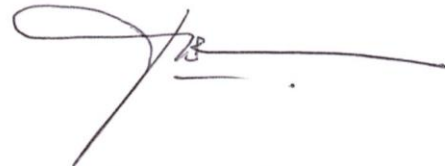


Aris Sugiharto, S.Si., M.Kom.

NIP. 19710811 199702 1 004

Semarang, 20 Agustus 2015

Pembimbing II,



Indra Waspada, S.T, M.TI

NIP. 19790212 200812 1 002

ABSTRAK

Perkembangan teknologi informasi dalam beberapa dekade terakhir telah mengalami kemajuan yang cukup pesat. Pertukaran informasi dan data dalam sebuah jaringan dapat menimbulkan suatu masalah dalam hal keamanan. Permasalahan tersebut harus mendapatkan perhatian serius karena menyangkut kerahasiaan informasi dan data yang cukup berharga bagi beberapa orang. Salah satu cara yang sering digunakan untuk menjaga kerahasiaan data atau informasi tersebut adalah dengan kriptografi, sedangkan metode yang lain adalah steganografi. Tugas akhir ini mengembangkan Sistem gabungan antara steganografi dan kriptografi. Adapun metode yang digunakan steganografi dengan metode transformasi wavelet diskrit haar dan kriptografi dengan metode vigenere *cipher*. Sistem steganografi dan kriptografi diharapkan dapat menghasilkan citra stego yang mirip dengan citra cover asli dan citra pesan hasil ekstraksi mirip dengan pesan citra digital (citra pesan asli). Setelah dilakukan beberapa pengujian diperoleh hasil bahwa sistem steganografi dan kriptografi memiliki nilai PSNR antara 37 sampai 80 dan nilai NC di atas 0,9. Sistem steganografi dan kriptografi tahan terhadap berbagai macam serangan antara lain: *flipping*, kompresi, rotasi dan *cropping*.

Kata kunci : Kriptografi, Steganografi, Transformasi wavelet diskrit haar, Vigenere *cipher*, PSNR, NC, Pesan citra digital

ABSTRACT

The development of information technology in recent decades progressed quite rapidly. Transmission of information and data in a network can create a problem in terms of security. Those problems should get serious attention because the confidentiality of information or data that was valuable enough for some people. Cryptography was often used to maintain the confidentiality of data or information, whereas the other was a method of steganography. The final task was to develop combination applications between steganography and cryptography. The development of system was used steganography method with discrete haar wavelet transformation and cryptography method with vigenere cipher. Steganography and cryptography system was expected to produce a stego image similar to the original cover image and the image of the extracted message similar to the message of digital image (the image of the original message). After doing some test of the obtained results that steganography and cryptography systems have PSNR values between 37 and 80 and the NC value above 0.9. Steganography and cryptography system was resistant to various kinds of attacks include: flipping, compressing, rotating and cropping.

Keywords : Cryptography, Steganography, Discrete haar wavelet transformation, Vigenere cipher, PSNR, NC, Message of digital image

KATA PENGANTAR

Segala puji syukur penulis panjatkan kehadirat Allah SWT karena atas izin, rahmat, dan karunia-Nya tugas akhir ini dapat terselesaikan. Tugas akhir yang berjudul “Implementasi Steganografi dan Kriptografi dalam Melindungi Pesan Citra Digital”, disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer/Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Sebagai pelaksanaan penyusunan Laporan Tugas Akhir ini, penulis banyak mendapat bimbingan, arahan dan bantuan dari berbagai pihak yang sangat mendukung. Oleh karena itu dengan segala kerendahan hati, penulis ingin mengucapkan terima kasih dengan tulus kepada:

1. Prof Dr. Widowati, M.Si selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Bapak Nurdin Bahtiar, S.Si, M.T. selaku Ketua Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
3. Bapak Aris Sugiharto, S.Si, M.Kom. selaku dosen pembimbing I.
4. Bapak Indra Waspada, S.T, M.TI. selaku dosen pembimbing II.
5. Bapak dan Ibu dosen Jurusan Ilmu Komputer / Informatika atas semua ilmu yang telah diberikan.
6. Ibu serta keluarga saya yang telah mendoakan dan memberikan semua fasilitas untuk penyusunan Tugas Akhir ini.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki kekurangan, untuk itu penulis mengharapkan kritik dan saran yang bersifat membangun demi kesempurnaan Tugas Akhir ini. Semoga Tugas Akhir ini dapat membawa manfaat bagi penulis sendiri khususnya dan bagi para pembaca pada umumnya.

Semarang, Agustus 2015

Penulis

DAFTAR ISI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
DAFTAR KODE	xiii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan dan Manfaat	2
1.4. Ruang Lingkup	2
1.5. Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA	4
2.1. Citra Digital.....	4
2.2. Kriptografi.....	6
2.3. <i>Vigenere Cipher</i>	9
2.4. Steganografi	10
2.5. Transformasi Wavelet Diskrit	11
2.6. <i>Peak Signal to Noise Ratio</i>	16
2.7. <i>Normalized Crosscorellation</i>	17
2.8. <i>Software Requirement Spesification</i>	17
2.9. <i>Data Flow Diagram</i>	18
2.10. <i>Flowchart</i>	18
2.11. Matlab	19
BAB III ANALISIS DAN PERANCANGAN.....	21
3.1. Definisi Kebutuhan	21

3.1.1.	Gambaran Umum.....	21
3.1.2.	Analisis Kebutuhan.....	24
3.1.3.	<i>Software Requirement Spesification</i>	24
3.1.4.	Pemodelan Fungsional.....	25
3.2.	Perancangan Proses Analisis	28
3.2.1.	<i>Discrete Haar Wavelet Transformation</i>	28
3.2.2.	Enkripsi.....	30
3.2.3.	<i>Embedded</i>	31
3.2.4.	<i>Ekstracted</i>	33
3.2.5.	Dekripsi.....	34
3.2.6.	<i>Invers Discrete Haar Wavelet Transformation</i>	35
3.3.	Perancangan Antarmuka Sistem.....	37
3.3.1.	Rancangan <i>Form</i> Menu Utama.....	38
3.3.2.	Rancangan <i>Form</i> Stego <i>Embedded</i>	39
3.3.3.	Rancangan <i>Form</i> Stego <i>Ekstracted</i>	41
3.3.4.	Rancangan Menu Bantuan.....	43
BAB IV IMPLEMENTASI DAN PENGUJIAN		44
4.1.	Implementasi Antarmuka	44
4.1.1.	Implementasi Antarmuka Menu Utama.....	44
4.1.2.	Implementasi Antarmuka Stego <i>Embedded</i>	46
4.1.3.	Implementasi Antarmuka Stego <i>Ekstracted</i>	49
4.2.	Implementasi Fungsi	52
4.2.1.	Stego <i>Embedded</i>	52
4.2.2.	Stego <i>Ekstracted</i>	59
4.3.	Pengujian	66
4.3.1.	Lingkungan Pengujian	66
4.3.2.	Pelaksanaan Pengujian.....	66
4.3.3.	Evaluasi Pengujian.....	76
BAB V PENUTUP		78
5.1.	Kesimpulan.....	78
5.2.	Saran.....	78
DAFTAR PUSTAKA.....		80

DAFTAR GAMBAR

Gambar 2. 1. Proses Enkripsi-dekripsi Kunci Simetris	8
Gambar 2. 2. Proses Enkripsi-dekripsi Kunci Asimetris.....	8
Gambar 2. 3. Proses Steganografi	11
Gambar 2. 4. Dekomposisi Wavelete Diskrit pada Sinyal 1 Dimensi.....	12
Gambar 2. 5. Langkah Dekomposisi Transformasi Wavelet Diskrit	13
Gambar 2. 6. Hasil Dekomposisi Transformasi Wavelet Diskrit.....	13
Gambar 3. 1. Deskripsi Umum Sistem Stegkrip – Stego <i>Embedded</i>	21
Gambar 3. 2. Deskripsi Umum Sistem Stegkrip – Stego <i>Ekstracted</i>	21
Gambar 3. 3. Alur Proses Stego <i>Embedded</i>	22
Gambar 3. 4. Alur Proses Stego <i>Ekstracted</i>	23
Gambar 3. 5. DCD Sistem Stegkrip	25
Gambar 3. 6. DFD Sistem Stegkrip.....	27
Gambar 3. 7. <i>Flowchart</i> Proses Stego <i>Embedded</i> (kiri) dan Stego <i>Ekstracted</i> (kanan).....	28
Gambar 3. 8. <i>Flowchart</i> Proses HWT	29
Gambar 3. 9. <i>Flowchart</i> Proses Enkripsi.....	31
Gambar 3. 10. <i>Flowchart</i> Proses <i>Embedded</i>	32
Gambar 3. 11. <i>Flowchart</i> Proses <i>Ekstracted</i>	34
Gambar 3. 12. <i>Flowchart</i> Proses Dekripsi	35
Gambar 3. 13. <i>Flowchart</i> Proses IHWT.....	36
Gambar 3. 14. Rancangan <i>Form</i> Pembuka.....	38
Gambar 3. 15. Rancangan <i>Form</i> Stego <i>Embedded</i>	40
Gambar 3. 16. Rancangan <i>Form</i> Stego <i>Ekstracted</i>	42
Gambar 3. 17. Rancangan Menu Bantuan	43
Gambar 4. 1. <i>Form</i> Menu Utama	44
Gambar 4. 2. Kotak Dialog “Keluar”	45
Gambar 4. 3. <i>Form</i> Menu Bantuan.....	46
Gambar 4. 4. <i>Form</i> Stego <i>Embedded</i>	46
Gambar 4. 5. Kotak Dialog “Buka <i>File</i> Citra”	47
Gambar 4. 6. <i>Form</i> Stego <i>Embedded</i> setelah Proses Buka	47
Gambar 4. 7. <i>Form</i> Stego <i>Embedded</i> setelah Proses HWT.....	47

Gambar 4. 8. <i>Form Stego Embedded</i> setelah Proses Enkripsi	48
Gambar 4. 9. <i>Form Stego Embedded</i> setelah Proses Penyisipan dan IHWT	48
Gambar 4. 10. Kotak Dialog “Menyimpan <i>File Citra</i> ”	49
Gambar 4. 11. <i>Form Stego Ekstracted</i>	50
Gambar 4. 12. <i>Form Stego Ekstracted</i> setelah Proses Buka	50
Gambar 4. 13. <i>Form Stego Ekstracted</i> setelah Proses HWT.....	50
Gambar 4. 14. <i>Form Stego Ekstracted</i> setelah Proses Ekstrak	51
Gambar 4. 15. <i>Form Stego Ekstracted</i> setelah Proses Dekripsi	51
Gambar 4. 16. <i>Form Stego Ekstracted</i> setelah Proses IHWT	52
Gambar 4. 17. barbaraGray.jpg	67
Gambar 4. 18. rahasia.jpg.....	67
Gambar 4.19. Serangan Horizontal <i>Flip</i>	70
Gambar 4.20. Serangan Vertical <i>Flip</i>	70
Gambar 4. 21. Serangan Kompresi.....	71
Gambar 4. 22. Serangan Kompresi Rasio 50%	71
Gambar 4. 23. Serangan Kompresi Rasio 25%	71
Gambar 4. 24. Serangan Rotasi 10°	72
Gambar 4. 25. Serangan Rotasi 20°	72
Gambar 4. 26. Serangan Rotasi 30°	72
Gambar 4. 27. Serangan Rotasi 40°	73
Gambar 4. 28. Serangan Rotasi 50°	73
Gambar 4. 29. Serangan Rotasi 60°	73
Gambar 4. 30. Serangan Rotasi 70°	73
Gambar 4. 31. Serangan Rotasi 80°	73
Gambar 4. 32. Serangan Rotasi 90°	73
Gambar 4. 33. Serangan <i>Copping</i> 100 Piksel di bagian kiri.....	75
Gambar 4. 34. Serangan <i>Copping</i> 100 Piksel di bagian atas.....	75

DAFTAR TABEL

Tabel 2. 1. Simbol-simbol pada DFD.....	18
Tabel 2. 2. Simbol-simbol pada <i>Flowchart</i>	19
Tabel 3. 1. SRS Sistem Steganografi dan Kriptografi.....	24
Tabel 4. 1. Nilai PSNR dan NC dari <i>barbaraGray.jpg</i> dan <i>rahasia.jpg</i>	68
Tabel 4. 2. Nilai NC Citra Pesan sebelum dan setelah Serangan <i>Flipping</i>	70
Tabel 4. 3. Nilai NC Citra Pesan sebelum dan setelah Serangan <i>Kompresi</i>	72
Tabel 4. 4. Nilai NC Citra Pesan sebelum dan setelah Serangan Rotasi.....	73
Tabel 4. 5. Nilai NC Citra Pesan sebelum dan setelah Serangan <i>Cropping</i>	76

DAFTAR KODE

Kode 4. 1. Fungsi Buka <i>File</i>	53
Kode 4. 2. Fungsi HWT.....	53
Kode 4. 3. Fungsi Buka Kunci	54
Kode 4. 4. Fungsi Enkripsi	56
Kode 4. 5. Fungsi Penyisipan	57
Kode 4. 6. Fungsi IHWT	58
Kode 4. 7. Fungsi Buka <i>File</i>	59
Kode 4. 8. Fungsi HWT.....	60
Kode 4. 9. Fungsi Ekstraksi.....	61
Kode 4. 10. Fungsi Buka Kunci	62
Kode 4. 11. Fungsi Dekripsi.....	64
Kode 4. 12. Fungsi IHWT	65

BAB I

PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, serta ruang lingkup penelitian tugas akhir mengenai Implementasi Steganografi dan Kriptografi dalam Melindungi Pesan Citra Digital.

1.1. Latar Belakang

Perkembangan teknologi informasi yang terjadi dalam beberapa dekade terakhir ini telah mengalami kemajuan yang cukup pesat. Pertukaran informasi dan data dalam sebuah jaringan dapat menimbulkan suatu masalah dalam hal keamanan informasi dan data tersebut memiliki aspek kerahasiaan yang cukup berharga dan tidak boleh diakses oleh sembarang orang yang tidak berhak. Permasalahan tersebut membuat aspek keamanan dalam bidang komunikasi data merupakan hal yang harus mendapatkan perhatian yang cukup serius karena menyangkut kerahasiaan suatu informasi dan data yang cukup berharga bagi beberapa orang.

Salah satu cara yang sering digunakan untuk menjaga kerahasiaan data atau informasi tersebut adalah dengan enkripsi informasi dan data tersebut, yang disebut dengan kriptografi. Metode lainnya yaitu dengan menyembunyikan data rahasia tersebut ke dalam data lain, teknik ini disebut dengan steganografi. Berbeda dengan teknik kriptografi yang dengan mudah dideteksi keberadaannya (walaupun sulit untuk dimengerti), steganografi menyamarkan keberadaan dari informasi dan data yang ingin disampaikan ke dalam media penyamar, misalnya media yang berbentuk multimedia (Iza, Aswin, & Mustofa, 2012).

Kelebihan dari steganografi adalah pesan yang dikirim tidak menarik perhatian. Salah satu metode steganografi adalah *Discrete Haar Wavelet Transformation* (HWT). Kelebihan dari HWT adalah mudah dalam implemetasi dan mengurangi komputasi (Banarjee & Mistry, 2013). Sedangkan kelebihan kriptografi adalah pesan yang dikirim sulit untuk dimengerti. Salah satu metode kriptografi adalah vigenere *chipper*, kelebihanannya adalah dapat mencegah frekuensi huruf-huruf di dalam chiperteks yang memiliki pola tertentu yang sama (Setyaningsih, Iswahyudi, & Widyastuti, 2011). Salah satu cara pengamanan informasi dan data dapat dilakukan

dengan mengkombinasikan kriptografi dan steganografi. Tujuannya adalah dapat menjaga informasi dan data dengan lebih baik (Martini & Esti, 2008).

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang, dapat dirumuskan permasalahan yang dihadapi, yakni bagaimana menjaga keamanan informasi dan data dengan menggabungkan steganografi dan kriptografi.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah sebagai berikut:

1. Menghasilkan sistem steganografi dengan metode *Discrete Haar Wavelet Transformation* dan kriptografi dengan metode *Vigenere Cipher* untuk menjaga keamanan informasi dan data.
2. Menguji sistem steganografi dan kriptografi untuk mengetahui kualitas citra stego dengan menggunakan PSNR dan kemiripan citra pesan hasil ekstraksi dengan citra pesan asli dengan menggunakan NC, baik tanpa serangan maupun dengan serangan.

Adapun manfaat yang diharapkan dari penelitian tugas akhir ini adalah untuk menjaga keamanan informasi dan data yang dikirim, sehingga informasi dan data tersebut tidak dapat diakses oleh orang yang tidak berhak.

1.4. Ruang Lingkup

Ruang lingkup pada Implementasi Steganografi dan Kriptografi dalam Melindungi Pesan Citra Digital adalah sebagai berikut:

- 1) Metode steganografi yang digunakan adalah metode *Discrete Haar Wavelet Transformation*.
- 2) Metode kriptografi yang digunakan adalah metode *Vigenere Cipher*.
- 3) Pembuatan sistem ini menggunakan bahasa pemrograman *Matlab*.
- 4) Penelitian dilakukan pada media berupa *file* citra digital *grayscale*.
- 5) *Input* dan *Output* berupa *file* citra digital *grayscale*.
- 6) Format *file* citra digital *input* berupa *jpg*.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi menjadi beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan singkat mengenai konsep-konsep yang mendukung pembuatan sistem seperti pengertian citra digital, steganografi, transformasi wavelet diskrit, *Peak Signal to Noise Ratio* (PSNR), *Normalized Crosscorellation* (NC), kriptografi dan vigenere cipher, *Software Requirement Spesification* (SRS), *Data Flow Diagram* (DFD), *Data Store*, *Data Flow*, *Flowchart*, Matlab.

BAB III ANALISIS DAN PERANCANGAN

Bab ini membahas proses pembuatan sistem pada tahap definisi kebutuhan, analisis dan perancangan, serta hasil yang didapat pada ketiga tahap tersebut.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas hasil pembuatan sistem pada tahap implementasi dan menerangkan rincian pengujian sistem.

BAB V PENUTUP

Bab ini berisi kesimpulan yang diambil berkaitan dengan sistem yang dibuat dan saran untuk pengembangan lebih lanjut.