

**KRIPTOGRAFI CITRA DIGITAL DENGAN KOMBINASI
TRANSFORMASI WAVELET DAN ALGORITMA *ONE TIME PAD***



SKRIPSI

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

Disusun Oleh:

ADIB ADIPRADITYA

24010311130043

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

2015

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini,

Nama : Adib Adipraditya

NIM : 24010311130043

Judul : Kriptografi Citra Digital dengan Kombinasi Transformasi *Wavelet* dan Algoritma
One Time Pad

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

Semarang, 28 Desember 2015



Adib Adipraditya

NIM. 24010311130043

HALAMAN PENGESAHAN

Judul : Kriptografi Citra Digital dengan Kombinasi Transformasi *Wavelet* dan Algoritma
One Time Pad

Nama : Adib Adipraditya

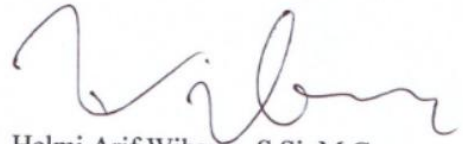
NIM : 24010311130043

Telah diujikan pada sidang tugas akhir pada tanggal 15 Desember 2015 dan dinyatakan
lulus pada tanggal 28 Desember 2015.



Semarang, 28 Desember 2015

Panitia Penguji Tugas Akhir
Ketua,



Helmi Arif Wibawa, S.Si, M.Cs.
NIP. 19780516 200312 1 001

HALAMAN PENGESAHAN

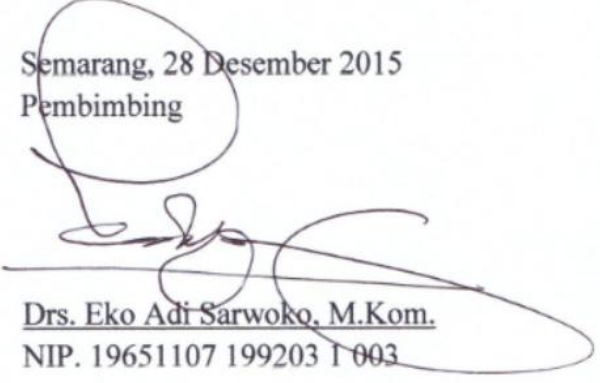
Judul : Kriptografi Citra Digital dengan Kombinasi Transformasi *Wavelet* dan Algoritma
One Time Pad

Nama : Adib Adipraditya

NIM : 24010311130043

Telah diujikan pada sidang tugas akhir pada tanggal 15 Desember 2015.

Semarang, 28 Desember 2015
Pembimbing



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

ABSTRAK

Citra merupakan salah satu bentuk informasi visual yang tidak lepas dari ancaman seperti modifikasi dan duplikasi. Oleh karena itu keamanan citra harus terjaga agar citra dapat terjamin kerahasiaannya, keasliannya, dan keutuhannya sehingga tidak terjadi penyalahgunaan informasi yang akan merugikan pihak tertentu. Tugas akhir ini membahas tentang kriptografi citra digital dengan kombinasi transformasi *Wavelet* dan algoritma *One Time Pad*. Algoritma *One Time Pad* dipilih karena relatif lebih cocok dalam mengenkripsi citra. Citra relatif memiliki volume yang besar sehingga untuk mengenkripsi citra dibutuhkan algoritma enkripsi yang efisien. Algoritma *One Time Pad* dikombinasikan dengan transformasi *Wavelet* untuk menyebar piksel yang dienkripsi sehingga citra terenkripsi lebih sulit dipecahkan. Analisis histogram antara citra asli dengan citra hasil enkripsi didapatkan hasil yang berbeda yang mengindikasikan bahwa algoritma enkripsi memiliki tingkat keamanan yang bagus. Pengujian citra asli dan citra hasil dekripsi menghasilkan nilai *Peak Signal to Noise Ratio* (PSNR) nilai rata-rata sebesar 38,4 dB.

Kata Kunci : Citra, Algoritma *One Time Pad*, Transformasi *Wavelet*, *Peak Signal to Noise Ratio* (PSNR)

ABSTRACT

Image is a part of visual information that can not be separated from threats such as modification and duplication. Therefore, the security of image must be maintained so that the image can be guaranteed confidentiality, authenticity and integrity so there is no misuse of the information. The final project discusse about digital image cryptography with *Wavelet* transform and *One Time Pad* algorithm combination. *One Time Pad* algorithms been relatively better in encrypting image and relatively simple. Image has large volume so as to encrypt the image needed an efficient encryption algorithm. *One Time Pad* algorithm combined with *Wavelet* transform can spread the encrypted pixels so encrypted image is more difficult to solve. Histogram analysis between the original image with encrypted image obtained different results, indicating that the encryption algorithm has a good level of security. Testing of the original image and the decrypt image generate Peak Signal to Noise Ratio (PSNR) value in average of 38.4 dB.

Keyword: Image, *One Time Pad* Algorithm, *Wavelet* Transform, Peak Signal to Noise Ratio (PSNR)

KATA PENGANTAR

Segala puji bagi Allah SWT atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul “Kriptografi Citra Digital dengan Kombinasi Transformasi *Wavelet* dan Algoritma *One Time Pad*” ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer/ Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan laporan ini tentulah banyak mendapat bantuan dan dukungan dari berbagai pihak. Untuk itu pada kesempatan ini penulis mengucapkan rasa hormat dan terimakasih kepada :

1. Ragil Saputra, S.Si, M.Cs. selaku Ketua Jurusan Ilmu Komputer / Informatika FSM Universitas Diponegoro.
2. Helmi Arif Wibawa, S.Si, M.Cs. selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika FSM Universitas Diponegoro.
3. Drs. Eko Adi Sarwoko, M.Kom. selaku dosen Pembimbing.
4. Semua pihak yang telah membantu kelancaran dalam pelaksanaan tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajiannya karena keterbatasan kemampuan dan pengetahuan penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan. Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya.

Semarang, Desember 2015

Penulis

DAFTAR ISI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	ii
HALAMAN PENGESAHAN	iii
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
DAFTAR KODE.....	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	2
1.3. Tujuan dan Manfaat	3
1.4. Ruang Lingkup	3
1.5. Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	5
2.1. Citra Digital	5
2.2. Kriptografi	5
2.3. Algoritma <i>One-Time Pad</i>	6
2.4. <i>Logistic Map</i>	7
2.5. Transformasi <i>Wavelet</i> Diskrit (DWT)	8
2.6. <i>Peak Signal to Noise Ratio</i>	10
2.7. Proses Pengembangan Perangkat Lunak	11
2.8. UML.....	13
2.8.1. <i>Things</i>	13
2.8.2. <i>Relationship</i>	14
2.8.3. Diagram	17
2.9. Pengujian Perangkat Lunak	19
BAB III ANALISIS DAN PERANCANGAN.....	21
3.1. Analisis Kebutuhan.....	21

3.1.1. Deskripsi Umum.....	21
3.1.2. Arsitektur Aplikasi	22
3.1.3. Kebutuhan Fungsional.....	22
3.1.4. <i>Use Case</i> Modeling	23
3.1.4.1. Daftar Aktor	23
3.1.4.2. Daftar Use Case.....	23
3.1.4.3. Diagram Use Case.....	23
3.1.4.4. Detail Use Case	24
3.1.5. <i>Class</i> Diagram	25
3.2. Perancangan Aplikasi	26
3.2.1. Perancangan Fungsi.....	26
3.2.1.1. Flowchart Enkripsi	26
3.2.1.2. Flowchart Dekripsi.....	27
3.2.1.3. Flowchart Uji Citra	28
3.2.2. Perancangan Antarmuka.....	28
3.2.2.1. Rancangan Antarmuka Halaman Depan	28
3.2.2.2. Rancangan Antarmuka Enkripsi	29
3.2.2.3. Rancangan Antarmuka Dekripsi	30
3.2.2.4. Rancangan Antarmuka Uji Citra.....	31
BAB IV IMPLEMENTASI, PENGUJIAN DAN ANALISIS HASIL	33
4.1. Implementasi.....	33
4.1.1. Implementasi Fungsi	33
4.1.2. Implementasi Antarmuka	36
4.2. Pengujian	40
4.2.1. Pengujian Fungsional Aplikasi.....	40
4.2.2. Rencana Pengujian Fungsional Aplikasi	41
4.2.3. Kasus Uji dan Hasil Uji.....	41
4.3. Analisis Hasil.....	41
4.3.1. Proses Enkripsi	41
4.3.2. Proses Dekripsi.....	45

4.3.3. Proses Uji Citra.....	46
BAB V KESIMPULAN	48
5.1. Kesimpulan	48
5.2. Saran	48
DAFTAR PUSTAKA.....	49
LAMPIRAN-LAMPIRAN	51

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Dekripsi.....	6
Gambar 2.2 Contoh Transformasi <i>Wavelet</i> pada Citra.....	8
Gambar 2.3. Contoh Citra 1 Dimensi	9
Gambar 2.4. Hasil Proses Transformasi Perataan dan Pengurangan.....	9
Gambar 2.5. Proses Rekonstruksi Citra Hasil Dekomposisi	9
Gambar 2.6. Contoh Hasil Dekomposisi Citra 2 Dimensi	10
Gambar 2.7. Proses Metode Waterfall.....	12
Gambar 2.8. Dependency Antara Class ‘Filmclip’ dan ‘Channel’	14
Gambar 2.9. Contoh Penggunaan Name Asosiasi Class ‘Person’ dan ‘Company’	14
Gambar 2.10. Contoh Penggunaan Role Asosiasi Class ‘Person’ dan ‘Company’	15
Gambar 2.11. Contoh Penggunaan Multiplicity Asosiasi Class ‘Person’ dan ‘Company’ .	15
Gambar 2.12. Contoh Penggunaan Aggregation Class ‘Company’ dan ‘Department’	16
Gambar 2.13. Generalization: Class ‘Rectangle’, ‘Circle’, ‘Polygon’	16
Gambar 2.14. Contoh Class Diagram Pemesanan Barang	17
Gambar 2.15. Simbol Use Case.....	18
Gambar 2.16. Simbol Actor.....	18
Gambar 2.17. Contoh Sequence Diagram untuk Proses Pemesanan Barang	19
Gambar 3.1. Arsitektur Aplikasi	22
Gambar 3.2. Diagram <i>Use Case</i>	23
Gambar 3.3. <i>Class Diagram</i>	25
Gambar 3.4. Flowchart Enkripsi	26
Gambar 3.5. Flowchart Dekripsi	27
Gambar 3.6. Flowchart Uji Citra.....	28
Gambar 3.7. Rancangan Antarmuka Halaman Depan.....	29
Gambar 3.8. Rancangan Antarmuka Enkripsi	30
Gambar 3.9. Rancangan Antarmuka Dekripsi.....	31
Gambar 3.10. Rancangan Antarmuka Uji Citra	32
Gambar 4.1. Implementasi Antarmuka Halaman Depan.....	37
Gambar 4.2. Implementasi Antarmuka Enkripsi	38
Gambar 4.3. Implementasi Antarmuka Dekripsi.....	39

Gambar 4.4. Implementasi Antarmuka Uji Citra	40
Gambar 4.5. Histogram Citra 'boat' Terenkripsi.....	43
Gambar 4.5. Histogram Citra 'lena512warna' Terenkripsi	44

DAFTAR TABEL

Tabel 2.1. Nilai PSNR	11
Tabel 2.2. Jenis <i>Relationship</i> pada <i>Use Case</i> Diagram	18
Tabel 3.1. Kebutuhan Fungsional.....	22
Tabel 3.2. Daftar Aktor.....	23
Tabel 3.3. Daftar <i>Use Case</i>	23
Tabel 3.4. Detail <i>Use Case</i> Enkripsi Data	24
Tabel 3.5. Detail <i>Use Case</i> Deskripsi Data	24
Tabel 3.6. Detail <i>Use Case</i> Deskripsi Citra.....	25
Tabel 4.1. Rencana Pengujian Aplikasi.....	41
Tabel 4.2. Hasil Enkripsi Citra	42
Tabel 4.3. Hasil Dekripsi Citra.....	45
Tabel 4.4. Uji Citra.....	46

DAFTAR KODE

Kode 1. Fungsi Enkripsi	33
Kode 2. Fungsi Dekripsi	34
Kode 3. Fungsi Uji Citra	35

BAB I

PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup serta sistematika penulisan penelitian tugas akhir mengenai kriptografi citra digital dengan kombinasi transformasi *Wavelet* dan algoritma *One Time Pad*.

1.1. Latar Belakang

Informasi memiliki peranan besar bagi kehidupan dalam berbagai bidang, seperti politik, ekonomi, sosial, budaya, pertahanan dan lain sebagainya. Informasi tidak hanya disajikan dalam bentuk teks, tetapi juga dapat berupa citra, audio, dan video. Keempat macam data atau informasi ini sering disebut multimedia. Citra sebagai salah satu komponen multimedia sangatlah penting sebagai bentuk informasi visual. Sebuah citra dapat memiliki banyak informasi, berbeda halnya dengan teks.

Seiring dengan kemajuan teknologi tersebut, ancaman-ancaman terhadap informasi seperti modifikasi dan duplikasi menyebabkan dibutuhkannya keamanan informasi. Nilai informasi yang digunakan dalam transaksi *online* sangatlah vital, sehingga memerlukan penanganan yang serius dalam pengamanan informasinya. Pengamanan informasi tersebut sangat dibutuhkan untuk menjaga privasi (*confidentiality*) informasi, memastikan identitas atau otentikasi (*authentication*), menjaga keutuhan atau integritas (*integrity*) informasi, dan menjamin ketersediaan (*availability*).

Begitu pula dengan citra sebagai bagian dari informasi. Citra digunakan dalam berbagai bidang seperti keamanan, medis, ilmu, teknik, seni, hiburan, iklan, pendidikan serta pelatihan. Oleh karena itu keamanan citra harus terjaga agar citra dapat terjaga kerahasiannya, keasliannya dan keutuhannya.

Pengamanan informasi atau pesan yang biasa dipakai adalah kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya (Ariyus, 2008). Dunia kriptografi modern saat ini telah menerapkan berbagai metode untuk penyandian data berupa multimedia salah satunya adalah citra.

Salah satu algoritma kriptografi yang bisa diterapkan untuk kriptografi citra adalah algoritma *one-time pad*. *One-time pad* adalah *stream cipher* yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Dibandingkan dengan algoritma *blockcipher*, algoritma *stream cipher* relatif lebih cocok dalam mengenkripsi citra, karena *stream cipher* tidak menggunakan perulangan dan relatif sederhana karena hanya menggunakan operasi XOR. Data citra (atau video) umumnya bervolume relatif sangat besar, sehingga proses enkripsi citra dengan *blockcipher* memerlukan komputasi lebih lama (Munir, 2011).

Pada umumnya untuk melakukan pengkodean suatu citra, menentukan domain yang lebih sesuai untuk proses pengkuantisasian harus melakukan transformasi (Zaki, 2012). Metode yang banyak digunakan dalam transformasi ini antara lain Transformasi Cosinus diskrit, Transformasi *Fourier* dan Transformasi *Wavelet*. Dari ketiga jenis transformasi tersebut, transformasi *Wavelet* dianggap paling baik hasilnya (Putra, 2010).

Pengembangan aplikasi enkripsi citra dengan metode *One Time Pad* menggunakan sistem *chaos* sebelumnya telah diteliti oleh Munir. Pada penelitian ini, peneliti mengembangkan aplikasi enkripsi dengan metode *One Time Pad* yang dikombinasikan dengan kompresi citra. Sebagian besar penelitian mengenai enkripsi citra menyimpulkan bahwa, enkripsi dan transformasi citra dapat dikombinasikan atau dilakukan secara bersamaan.

Dalam hal ini, metode yang digunakan peneliti untuk transformasi citra adalah transformasi *Wavelet*. Sifat transformasi *Wavelet* yang *reversible* atau dapat dibalik dinilai cocok untuk dikombinasikan dengan kriptografi, dengan mengkombinasikan transformasi *Wavelet* dan algoritma *One Time Pad* maka hasil dari enkripsi citra menjadi lebih sulit untuk dipecahkan.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yaitu bagaimana membuat aplikasi kriptografi citra digital dengan mengkombinasikan transformasi *Wavelet* dan algoritma *One Time Pad*.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan suatu aplikasi kriptografi citra digital dengan kombinasi transformasi *Wavelet* dan algoritma *One Time Pad*.

Manfaat dari penelitian tugas akhir ini adalah dapat mengenkripsi citra sehingga citra terjaga kerahasiaan, keutuhan dan keasliannya.

1.4. Ruang Lingkup

Ruang lingkup pada penelitian tugas akhir mengenai kriptografi citra digital dengan kombinasi transformasi *Wavelet* dan algoritma *One Time Pad* adalah sebagai berikut:

1. Input berupa citra diam *grayscale* atau citra warna.
2. Input citra berukuran $2^n \times 2^n$.
3. Level transformasi *Wavelet* yang digunakan maksimal level 2.
4. Untuk mengetahui perbandingan kualitas citra asli dan citra hasil dekripsi dengan menghitung nilai PSNR.
5. Bahasa pemrograman yang digunakan adalah C#.

1.5. Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup serta sistematika penulisan penelitian tugas akhir mengenai kriptografi citra digital dengan kombinasi transformasi *Wavelet* dan algoritma *One Time Pad*.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang teori-teori yang digunakan dalam penyusunan tugas akhir ini. Teori yang digunakan pada penyusunan tugas akhir ini meliputi pengertian citra digital, kriptografi, algoritma *one-time pad*, *logistic map*, transformasi *Wavelet* diskrit, *peak signal to noise ratio* (PSNR), proses pengembangan perangkat lunak, permodelan fungsional dan pengujian perangkat lunak.

BAB III ANALISIS DAN PERANCANGAN

Bab ini membahas tentang analisis masalah dan rancangan penyelesaiannya. Bab ini berisi antara lain rancangan solusi permasalahan, gambaran arsitektur aplikasi, rancangan alur program dalam bentuk *flowchart*, rancangan algoritma program, serta rancangan antar muka.

BAB IV IMPLEMENTASI, PENGUJIAN DAN ANALISIS HASIL

Bab ini menguraikan implementasi algoritma dan antarmuka yang telah dirancang serta langkah-langkah pengujiannya. Bab ini juga membahas tentang analisis hasil dari penelitian tugas akhir ini.

BAB V PENUTUP

Penutup berisi kesimpulan dari pengerjaan penelitian tugas akhir ini dan saran-saran dari penulis untuk pengembangan lebih lanjut dari penelitian serupa.