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.

Mengetahui,
Ketua Jurusan Ilmu Komputer/Informatika
FSM UNDIP

Ragil Saputra, S.Si, M.Cs.
NIP. 19801021 200501 1 003

Semarang, 28 Desember 2015

Panitia Penguji Tugas Akhir
Ketua,

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

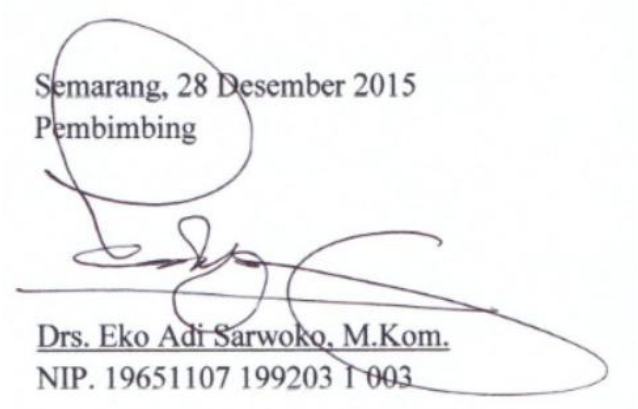
HALAMAN PENGESAHAN

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.



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

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

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 tranformasi 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 x 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 implementsi 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.