PENGAMANAN PESAN PADA CITRA DIGITAL DENGAN METODE KOMBINASI LSB, IWT DAN RSA

SKRIPSI

Disusun Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer
pada Departemen Ilmu Komputer/Informatika

Disusun Oleh :

RAHMAT HIDAYAT

24010313120001

DEPARTEMEN ILMU KOMPUTER/ INFORMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

2018

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama : Rahmat Hidayat

NIM : 24010313120001

Judul : Pengamanan Pesan pada Citra Digital dengan Metode Kombinasi LSB, IWT dan RSA

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, 24 Januari 2018

Rahmat Hidayat

24010313120001

HALAMAN PENGESAHAN

Judul : Pengamanan Pesan pada Citra Digital dengan Metode Kombinasi LSB, IWT dan RSA

Nama : Rahmat Hidayat

NIM : 24010313120001

Telah diujikan pada sidang tugas akhir pada tanggal 24 Januari 2018 dan dinyatakan lulus pada tanggal 24 Januari 2018.

Semarang, 24 Januari 2018

Mengetahui,

Ketua Departemen Ilmu Komputer/ Informatika
FSM UNDIP

Dr. Retno Kusumaningrum, S.Si, M.Kom
NIP. 197810042020050012001

Panitia Penguji Tugas Akhir
Ketua

Drs. Suhartono, M.Kom
NIP. 195504071983031003

HALAMAN PENGESAHAN

Judul : Pengamanan Pesan pada Citra Digital dengan Metode Kombinasi LSB, IWT dan RSA

Nama : Rahmat Hidayat

NIM : 24010313120001

Telah diujikan pada sidang tugas akhir pada tanggal 24 Januari 2018.

Semarang, 24 Januari 2018

Pembimbing,

Helmie Arif Wibawa, S.Si, M.Cs

NIP. 197805162003121001

ABSTRAK

Perkembangan teknologi informasi digital memungkinkan penyimpanan data dan informasi secara digital. Data dan informasi ini ada yang dapat dipublikasikan dan ada yang harus dijaga kerahasiannya. Untuk menjaga kerahasiannya, maka dibutuhkan suatu cara untuk mengaburkan makna data dan informasi tersebut serta menghilangkan keberadaannya. Kriptografi dan steganografi adalah cara yang dapat digunakan untuk mengaburkan makna dan menghilangkan keberadaan data dan informasi (pesan). Kriptografi RSA merupakan kriptografi dimana panjang kunci menjadi penentu tingkat keamanannya. Steganografi LSB, sebagai salah satu metode pada steganografi menghasilkan citra stego yang tidak tahan terhadap berbagai serangan. Untuk mengatasi hal tersebut, dibutuhkan transformasi citra *Integer Wavelet Transform* (IWT) untuk meningkatkan ketahanan citra steganografi LSB. Oleh karena itu, penelitian ini berfokus kepada mengkombinasikan Steganografi LSB, Kriptografi RSA dan IWT untuk meningkatkan keamanan pesan serta mengetahui kinerja dari kombinasi tersebut. Hasil yang didapat menunjukan bahwa IWT dapat menjaga kualitas citra stego lebih baik dibandingkan tanpa IWT. Hasil ini ditunjukan oleh nilai PSNR citra stego dengan IWT yang cenderung stabil dibandingkan dengan tanpa IWT. Disisi lain, kualitas pesan dipengaruhi komposisi bit modulus kunci RSA yang digunakan. Kualitas pesan semakin baik jika bilangan modulus tersebut mendekati nilai maksimal untuk panjang kunci yang sesuai.

Kata kunci : Steganografi LSB, Kriptografi RSA, IWT

ABSTRACT

The development of digital information technology allows the storage of data and information digitally. This data and information is there that can be published and there is to be kept confidential. To maintain confidentiality, it takes a way to obscure the meaning of data and information and eliminate its existence. Cryptography and steganography are ways that can be used to obscure meaning and eliminate the existence of data and information (messages). RSA cryptography is cryptography where the key length becomes the determinant of its security level. LSB steganography, as one method of steganography produces stego images that can not stand the various attacks. To overcome this, we need Integer Wavelet Transform image (IWT) image transformation to improve the steganographic image resistance of LSB. Therefore, this study focuses on combining LSB Steganography, RSA Cryptography and IWT to improve message security and to know the performance of such combinations. The results show that IWT can maintain better stego image quality than without IWT. This result is shown by PSNR value of stego images with IWT are more stable than stego image without IWT. On the other hand, message quality is influenced by RSA key modulus bit composition used. The quality of the message is better if the modulus number is close to the maximum value for the corresponding key length.

Key words : LSB Steganography, RSA Cryptography, IWT

KATA PENGANTAR

Segala puji syukur bagi Tuhan Yang Maha Esa atas karunia-Nya yang diberikan kepada penulis sehingga dapat menyelesaikan laporan tugas akhir yang berjudul "Pengamanan Pesan pada Citra Digital dengan Metode Kombinasi LSB, IWT dan RSA". Laporan tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Departemen Ilmu Komputer/ Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan laporan ini penulis banyak mendapat bimbingan dan bantuan dari berbagai pihak. Untuk itu, pada kesempatan ini penulis mengucapkan rasa hormat dan terima kasih kepada:

1. Dr. Retno Kusumaningrum, S.Si, M.Kom selaku Ketua Departemen Ilmu Komputer/ Informatika.
2. Helmie Arif Wibawa, S.Si, M.Cs, selaku Koordinator Tugas Akhir dan dosen pembimbing.
3. Semua pihak yang telah membantu kelancaran dalam penyusunan tugas akhir, 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 dan penulis pada umumnya.

Semarang, 24 Januari 2018

Rahmat Hidayat

24010313120001

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, serta ruang lingkup tugas akhir mengenai metode kombinasi Steganografi *Least Significant bit*, Kriptografi RSA dan *Integer Wavelet Transform* pada citra digital.

1.1. Latar Belakang

Perkembangan teknologi informasi digital memungkinkan penyimpanan data dan informasi secara digital. Data dan informasi tersebut ada yang dapat dipublikasikan secara umum dan ada yang harus dijaga kerahasiannya. Untuk dapat menjaga kerahasiannya, dibutuhkan suatu cara agar data dan informasi tidak dapat dibaca secara langsung serta tidak dirasakan keberadaannya. Hal itu dapat meningkatkan keamanan dan privasi data dan informasi yang dirahasiakan.

Data dan informasi (pesan) dapat diubah menjadi bentuk yang tidak dapat dibaca (sulit dipahami maknanya) dengan cara menyandikan pesan tersebut. Pesan yang disandikan pun harus dapat diterjemahkan kembali dengan suatu algoritma untuk mendapatkan pesan asli. Salah satu algoritma yang dapat memenuhi hal tersebut adalah algoritma RSA.

Algoritma RSA adalah algoritma dalam kriptografi yang tergolong pada kriptografi kunci asimetris. Kriptografi kunci asimetris adalah algoritma kriptografi dimana kunci untuk menyandikan pesan berbeda dengan kunci untuk mengembalikan pesan dari bentuk sandinya. Panjang kunci yang digunakan pada algoritma RSA menjadi penentu tingkat keamanan pesan yang disandikan. Semakin panjang kunci yang digunakan, semakin tinggi tingkat keamanan pesan yang disandikan.

Berbagai penelitian telah menunjukan kehandalan dari algoritma RSA. Santomo (2016) menjelaskan bahwa RSA memberikan keamanan yang handal dan efisien karena sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima. Tujuannya adalah untuk mencari berbagai kemungkinan kombinasi kunci yang sesuai untuk memecahkan pesan yang disandikan. Cara memecahkan pesan dengan mencoba semua kemungkinan kunci yang digunakan disebut sebagai metode *brute force* (Wicaksono,2004). Semakin panjang kunci yang digunakan, maka kemungkinan kombinasi kunci pun semakin banyak. Hal ini mengakibatkan waktu

untuk yang dibutuhkan untuk memecahkan pesan yang disandikan juga semakin tinggi, sehingga tingkat keamanan pesan yang disandikan pun semakin tinggi (Triorizka, 2010).

Untuk semakin meningkatkan privasi, pesan yang telah disandikan disembunyikan ke dalam suatu host untuk membuat pesan tersebut tidak dapat disadari keberadaannya. Penyembunyian pesan tersebut dapat dilakukan dengan steganografi. Sederhananya, steganografi adalah penulisan pesan secara rahasia, baik berupa ditulis dengan menggunakan tinta tak terlihat di atas kertas maupun berupa informasi hak cipta yang disembunyikan ke dalam suatu berkas digital (Cole, 2003). Pada steganografi, pesan disembunyikan ke dalam suatu host. Pengaplikasian teknik ini dapat meningkatkan keamanan pesan tersebut. Saat ini, terdapat berbagai jenis algoritma yang merupakan bagian dari steganografi, salah satunya adalah algoritma LSB.

LSB (*Least Significant Bit*) adalah bit-bit pada suatu rangkaian bit yang tidak memiliki pengaruh besar jika mengalami perubahan. Algoritma subtitusi LSB di dalam steganografi adalah dengan mengubah bit LSB pada host dengan bit pesan yang disembunyikan. Pada host citra, secara visual perubahan nilai LSB tidak terlalu terlihat, sehingga dapat mengelabui mata manusia bahwa citra yang dilihat telah disisipi pesan.

Hingga saat ini, terdapat berbagai penelitian yang menggunakan algoritma LSB, seperti penelitian yang dilakukan oleh Syahrul (2010), Utomo (2012), Alamsyah (2015), Wijaya dkk (2012), dan lain sebagainya. Pada penelitian-penelitian tersebut, ditunjukan bahwa penyembunyian pesan dengan algoritma subtitusi LSB tidak mengubah ukuran host yang digunakan. Kualitas host yang digunakan pun tidak mengalami penurunan yang begitu besar dibanding dengan sebelum disisipi pesan.

Tetapi, pada penelitian yang dilakukan oleh Alamsyah (2015), penggunaan algoritma subtitusi LSB pada citra tidak dapat bertahan pada uji ketahanan citra. Citra yang telah disisipkan dilakukan perubahan kontras, kecerahan, rotasi, maupun perubahan ukuran. Citra yang telah mengalami perubahan tersebut tidak dapat diekstrak pesannya dengan baik. Sehingga diperlukan suatu cara agar citra stego – citra yang telah disisipi pesan – dapat bertahan dari perubahan tersebut.

Salah satu cara agar citra stego dapat bertahan dari perubahan adalah dengan melakukan transformasi terhadap citra tersebut. Saat ini, terdapat berbagai jenis transformasi, salah satunya adalah *Integer Wavelet Transform* (IWT).

IWT adalah transformasi suatu sinyal dalam sederetan gelombang pendek pada basis waktu yang berbeda dengan hasil berupa bilangan bulat. IWT memetakan dari bilangan integer ke bilangan integer. IWT sendiri memiliki sifat *invertible*. Sifat *invertible* adalah istilah yang berarti citra yang telah mengalami transformasi dapat dikembalikan menjadi bentuk citra semula.

Hingga saat ini, terdapat berbagai penelitian yang menunjukan kelebihan dan kelemahan penggunan IWT di dalam steganografi. Jayasudha (2013) menjelaskan bahwa menggunakan transformasi tersebut memberikan toleransi yang tinggi terhadap *noise* citra. Tetapi, disisi lain menggunakan IWT menyebabkan komputasi yang dibutuhkan relatif lebih lama.

Oleh karena itu, pada penelitian ini dilakukan pengkombinasian steganografi LSB, algoritma RSA dan IWT ke dalam suatu aplikasi. Penelitian ini juga meneliti berapa banyak bit pada suatu rangkaian bit yang dapat digunakan untuk menyimpan pesan tanpa memberikan perubahan yang besar pada citra host. Tujuannya adalah agar dapat mengetahui berapa jumlah maksimal bit yang dapat digunakan untuk menyimpan pesan.

1.2. Rumusan Masalah

Adapun rumusan masalah yang menjadi topik penelitian ini adalah bagaimana meningkatkan keamanan pesan pada citra digital dengan kombinasikan metode LSB, algoritma RSA dan IWT.

1.3. Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menghasilkan sebuah kombinasi antara metode LSB, algoritma RSA dan IWT untuk meningkatkan keamanan pesan yang disembunyikan.
2. Mengetahui kinerja kombinasi tersebut.

1.4. Manfaat

Adapun manfaat yang diharapkan dari penelitian ini adalah untuk meningkatkan privasi dan keamanan pesan yang harus dijaga kerahasiannya dengan menggunakan metode LSB, algoritma RSA dan IWT.

1.5. Ruang Lingkup

Ruang lingkup yang dibahas dalam penilitian ini adalah sebagai berikut:

1. Citra yang digunakan pada penelitian ini adalah citra dengan format bitmap (*.bmp).
2. Pesan yang disisipkan berupa berkas citra.
3. Penelitian ini fokus pada implementasi steganografi metode LSB, kriptografi RSA dan transformasi citra IWT.