PROCEEDINGS

knastik 2012

UKDW YOGYAKARTA 29 MAY 2012

PROCEEDINGS

Business Intelligence:
Extending Your Business

DUTA WACANA

UKDW
YOGYAKARTA
29 MAY 2012

ISBN 978-602-95792-0-8

The KNASTIK International Conference is an annual conference that aims at gathering some researchers, academicians, and practitioners who meet and discuss ideas and innovations in the implementations of information technology. This year the conference explores issues related to developing Business Intelligence in Indonesia.
These proceedings are the compilation of the papers presented in the 2012 KNASTIK International Conference.

Committee

Patron	:	Rektor UKDW
Wardens	:	Head of Informatics Department of UKDW
		Head of Information System of UKDW
Chief Executive	:	Katon Wijana, S.Kom, M.T.
Vise Chief Executive	:	Antonius Rachmat C., S.Kom., M.Cs.
Secretary	:	Dave GSM Fernandez, S.Kom
		Ignatia Dhian, S.Kom
Treasurer	:	Dra. Widi Hapsari, M.T.
Division of Seminar and Program	:	Lucia Dwi Krisnawati, S.Si, MA
		Rosa Delima, M.Kom
		Jeanny Dhewayani, Ph.D.
		Willy Sudiarto R, S.Kom, M.Cs
		Yuan Lukito, S.Kom
		Drs. Djoni Dwijana, Akt., M.T.
Division of Material and Publication	:	Fransisca Endang L, S.Pd., M.Hum
		Dra. Endah Setyowati, M.Si., M.A.
		Erick Kurniawan, S.Kom, M.Kom
Division of Publication and Documentation	:	Aditya Wikan Mahastama, S.Kom
		Paulus Widiatmoko, M.A.
		Budi Susanto, S.Kom, MT
Division of Equipment and Accommodation	:	Hendro Setiadi, ST, MM, M.Eng.Sc
		Restyandito, S.Kom, MSIS
		Eka Nugraha
		Ronny Kuncoro
Division of Refreshments	:	Dra. Emy Suryawati

Reviewer

- Dr. Volker Müller (Université du Luxembourg)
- Gloria Virginia, S. Kom. MAI (University of Warsaw, Poland)
- Ir. P. Insap Santosa, Ph.D (Universitas Gadjah Mada)
- Dr. Sri Kusumadewi, S.Si., MT (Universitas Islam Indonesia)
- Drs. R. Gunawan Santosa, M.Si (Universitas Kristen Duta Wacana)
- Restyandito, S.Kom, MSI (Universitas Kristen Duta Wacana)
- Drs. Jong Jek Siang, M.Sc (Universitas Kristen Duta Wacana)

Secretariat

KNASTIK 2012
Universitas Kristen Duta Wacana
Jl. Dr. Wahidin Sudirohusodo 5 - 25
Yogyakarta 55224
Telp. 0274 - 563929 ext. 322
URL : http://knastik.ukdw.ac.id
E-mail : info@knastik.ukdw.ac.id

Table of Content

REMARKS OF THE CHAIRMAN OF EXECUTIVE COMMITTEE 2012
International Conference KNASTIK
Harun Room, UKDW, Tuesday, May 29, 2012

Dear Chairman Kopertis Yogyakarta Region V or the representative,
Dear Christian University Board Rectorate Discourse Duta Yogyakarta,
Dear Mrs. Prof. Anne Laurent,
Dear Mr. Dr. Gilbert Ooi,
Dear Mr. Prof. Dr. Richardus Eko Indrajit,
Invited guests esteemed gentlemen,
The honorable the speakers International Conference 2012,
And seminar participants 2012 International Conference of the blessed,

Good morning, ladies and gentlemen. First of all, I would like to extend a sincere welcome to all of you joining us today for this international seminar hosted by the Information Technology Faculty of Duta Wacana Christian University. In addition, I greatly appreciate the participation of our keynote speakers and the panelists at the International Conference KNASTIK 2012 on May 29, 2012

This International Conference KNASTIK is designed to be held every year to celebrate our University anniversary, but in the 2011 we suspend the event to greet the 50th anniversary of our university in this year. The theme of International Conference KNASTIK this year is "Business Intelligence: Extending your business". The purpose of this seminar is to bring together experts in field of Information Systems, Information Technology and Communications to discuss and display the the works of research on the use of information technology to be utilized especially in business. In this year we also invite Professor Anne Laurent from Paris, France and Dr. Gilbert Ooi from HELP University College Kuala Lumpur, Malaysia as the Intelligent Business experts who will be the seminar speaker and keynote speaker at the event.

On this occasion, as the committee of the International Conference 2012, we specifically would like to express our sincere gratitude to Professor Anne Laurent, who is willing to come from a very far away, Paris, France, taking special time to come to Yogyakarta, Indonesia, also Dr. Gilbert Ooi, who is honored to be the keynote speaker at this seminar. We are also thankful to the Kopertis, the rectorate of Duta Wacana Christian University, the faculty of Information Technology, PT Telkom Indonesia, and all the supporters of other parties, and all the committee who have fought and worked hard during the preparation and execution of this event.

As the Indonesian saying, there is no ivory that is not cracked. Although the committee has tried to prepare everything as well as possible to organize this seminar, we would like to apologize profusely for any inconvenience or shortage. Criticism and suggestions are our hope for improvement in the coming years.

Thank you

Chairman of the Committee of International Conference 2012,

Katon Wijana, S.Kom, M.T. &
Antonius Rachmat Chrismanto, S.Kom, M.Cs.

Remarks of The Dean of The Information Technology Faculty
The International Conference KNASTIK 2012

Welcome to Yogyakarta, the city known as a city of culture, education and tolerance. Warmest welcome to Duta Wacana Christian University, especially to our guest speakers and participants of the International Conference KNASTIK 2012. This International Conference is the third scientific conference organized by the Faculty of Information Technology. This conference is usually being held at the national level. However, this year is special, as it is the fiftieth anniversary (Jubelium) of Duta Wacana Christian University.

The theme of International Conference KNASTIK 2012 is "Business Intelligence: Extending your business" which aims to bring together experts in the field of Information Communication Technology to discuss and present the works of research on the utilization of information technology to be utilized primarily in the business world. In this conference the commitee invited Professor Anne from Paris, France and also Dr. Gilbert Ooi from HELP University College in Kuala Lumpur, Malaysia as a Senior Researcher in the areas of Databases and Business Intelligence as the keynote speakers. In addition to the two experts, the third keynote speaker is Prof. Dr. Richardus Eko Indrajit, who is the chairman of the Indonesian Association of Computer Universities and Colleges (APTIKOM).

I am pleased that this conference is attended by many speakers from different universities and also from various regions in Indonesia. I hope that seminars and discussions in this conference will broaden our knowledge and generate new knowledge for the ICT world, especially in Business world. Finally, on behalf of the Faculty of Information Technology, as the dean of Information Technology Faculty, I wish to thank you very much for the presence of the keynote speakers, speakers of the article and participants. Have a good conference and seminar.

Wimmie Handiwidjojo, Drs. MIT
Dean Of Information Technology Faculty

TEKNIK PENGAMANAN PESAN DENGAN ALGORITMA RC4 DAN METODA LSB

R. Kristoforus J. Bendi[(1)]
kristojb@gmail.com

Erwin Budiman[(2)]
win_ns.zone@yahoo.co.id

Abstract

Issues of security and confidentiality are one important aspect of messages, data or information. By using various techniques, many people are trying to access information that they are should not have access to. With the development of science, the application of information security techniques and data that have been used in ancient times can be an alternative in securing data communications. Cryptography is a science and art to maintain the security of messages sent from one place to another. RC4, one cryptographic algorithm, is widely applied to encrypt information. Cryptography can still be broken even if the process takes time, cost and effort. Other data security techniques are also quite popular is steganography. In contrast to cryptographic techniques, steganography can reduce suspicion because the message is disguised is hidden in another file. LSB is one of steganographic methods. LSB widely applied to insert a secret message into a digital image.This software is made in order to secure the secret message into a digital image using the RC4 algorithm and the method of LSB. The software is built using the waterfall model of software development.The results of the development of this software has been able to secure the secret message in the form of text into a digital image with a BMP format using RC4 algorithm and the method of LSB.

Keywords : cryptography, steganography, RC4, LSB.

1. Pendahuluan

Saat ini *internet* sudah berkembang menjadi salah satu media yang sangat populer di berbagai belahan dunia (Bunyamin dan Andrian, 2009). Namun dengan semakin berkembangnya *internet*, semakin berkembang pula kejahatan dalam penyalahgunaan informasi. Dengan menggunakan berbagai teknik, banyak orang yang mencoba untuk mengakses informasi yang bukan haknya.

Keamanan suatu informasi pada zaman global ini menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan (Anna *et. al.*, 2009). Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut tentang aspekaspek keputusan bisnis, keamanan, ataupun kepentingan umum.

Dengan berkembangnya ilmu pengetahuan, penerapan teknik-teknik pengamanan informasi dan data yang sudah pernah dipakai pada zaman dulu dapat menjadi alternatif dalam pengamanan komunikasi data melalui jaringan *internet* (Sukrisno, 2007). Sebagai contoh adalah kriptografi, yaitu suatu ilmu dan seni untuk

[1] *Dosen, Jurusan Teknik Informatika, Sekolah Tinggi Teknik Musi*
[2] *Staf TI, Bank Ekonomi Palembang*

menjaga keamanan pesan yang dikirim dari suatu tempat ke tempat yang lain. Teknik pengamanan data lain yang juga cukup populer adalah teknik steganografi. Berbeda dengan teknik kriptografi yang dapat menimbulkan kecurigaan karena pesan disamarkan dengan cara mengubah pesan yang asli menjadi seolah-olah tidak terbaca, steganografi justru lebih bisa mengurangi kecurigaan karena pesan yang disamarkan disembunyikan dalam *file* lain. Dalam penerapannya, steganografi membutuhkan dua properti, yaitu media penampung dan data rahasia yang akan disembunyikan (Anggraini dan Utami, 2007).

Melalui penelitian ini, kedua teknik pengamanan data tersebut akan digabungkan. Kasus yang dibahas dalam penelitian ini adalah pengamanan pesan rahasia dengan menggunakan algoritma RC4 dan metoda LSB. Media penampung pesan rahasia yang digunakan adalah citra digital. Hal ini karena adanya batasan kepekaan manusia dalam hal sistem visualisasi (Anggraini dan Utami, 2007). Sedangkan algoritma kriptografi RC4 dan metoda steganografi LSB dipilih karena keduanya paling sederhana dan paling mudah diimplementasikan (Munir, 2006).

2. Tinjauan Pustaka

Bruce Schneier (1996) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ("*Cryptography is the art and science of keeping messages secure"*). Sistem kriptografi *(cryptosystem)* adalah kumpulan yang terdiri dari algoritma kriptografi, semua *plaintext*, *ciphertext*, dan kunci yang mungkin. *Plaintext* atau pesan adalah data yang dapat dibaca dan dimengerti maknanya, sedangkan *ciphertext* adalah bentuk pesan yang tersandi ke bentuk lain yang tidak dapat dipahami.

Steganografi adalah teknik yang digunakan untuk menyembunyikan pesan rahasia ke dalam media yang lebih besar sedemikian rupa sehingga orang lain tidak dapat melihat keberadaan atau isi dari pesan rahasia tersebut (Stallings, 2005; Schneier, 1996). Steganografi bermanfaat bagi orang yang ingin mengirimkan pesan rahasia kepada orang lain.

Dalam steganografi, media penampung (*cover-object*) dibutuhkan untuk menyisipkan pesan rahasia (*embedded message*) (Anderson dan Petitcolas, 1998 dalam Shreelekshmi dan Wilscy, 2010). Citra digital, audio, video maupun *file* komputer lainnya dapat digunakan sebagai media penampung untuk menyembunyikan pesan rahasia.

Terdapat beberapa penelitian mengenai kriptografi dan steganografi pada citra digital yang telah dilakukan sebelumnya. Sarmah dan Bajpai (2010) membahas tentang sistem penyembunyian data menggunakan kriptografi dan steganografi. Penelitian ini mengembangkan sebuah sistem dengan teknik baru di mana kriptografi dan steganografi digunakan sebagai bagian yang terintegrasi bersama. Algoritma kriptografi yang digunakan untuk mengenkripsi pesan adalah algoritma AES (*Advanced Encryption Standard*) sedangkan metode steganografi yang digunakan untuk menyisipkan pesan ter-enkripsi ke dalam citra digital adalah DCT (*Discrete Cosine Transform*).

Swain dkk. (2010) mengusulkan teknik yang dapat digunakan untuk ber-komunikasi secara aman antara dua pihak. Teknik yang digunakan merupakan gabungan dari kriptografi dan steganografi. Citra digital dipilih sebagai media penampung dalam

metoda steganografi. Pesan rahasia akan dienkripsi dengan menggunakan *cipher* substitusi *Two Square Reverse*. Metode steganografi yang digunakan adalah metode LSB. Setelah penyisipan pesan ke dalam citra digital maka citra digital tersisipi akan dikirim ke penerima, penerima akan menerapkan operasi sebaliknya untuk mendapatkan pesan rahasia yang diinginkan.

Dalam penelitian lain, Narayana dan Prasad (2010) memperkenalkan dua metode baru dimana kriptografi dan steganografi digabungkan untuk mengenkripsi data serta untuk menyembunyikan data ter-enkripsi dalam media lain sehingga keamanan data lebih terjaga. Pesan rahasia yang digunakan dalam penelitian ini berupa citra digital yang akan dienkrispi lebih dulu menggunakan algoritma S-DES. Kemudian citra digital terenkrispi tersebut akan disisipkan ke dalam citra digital lain dengan metoda steganografi. Metoda steganografi yang digunakan berupa metoda LSB.

Pada penelitian ini akan dilakukan proses penyembunyian pesan ke dalam citra digital dengan menggunakan algoritma RC4 (*Ron 's Code* 4) dan metoda LSB (*Least Significant Bit*). Media penampung yang digunakan berupa citra digital bitmap berekstensi BMP 24 bit. Penggunaan wadah penampung berupa citra digital karena adanya batasan kepekaan manusia dalam hal sistem visualisasi (Anggraini dan Utami, 2007). Sedangkan algoritma kriptografi RC4 dan metoda steganografi LSB dipilih karena keduanya paling sederhana dan paling mudah diimplementasikan (Munir, 2006).

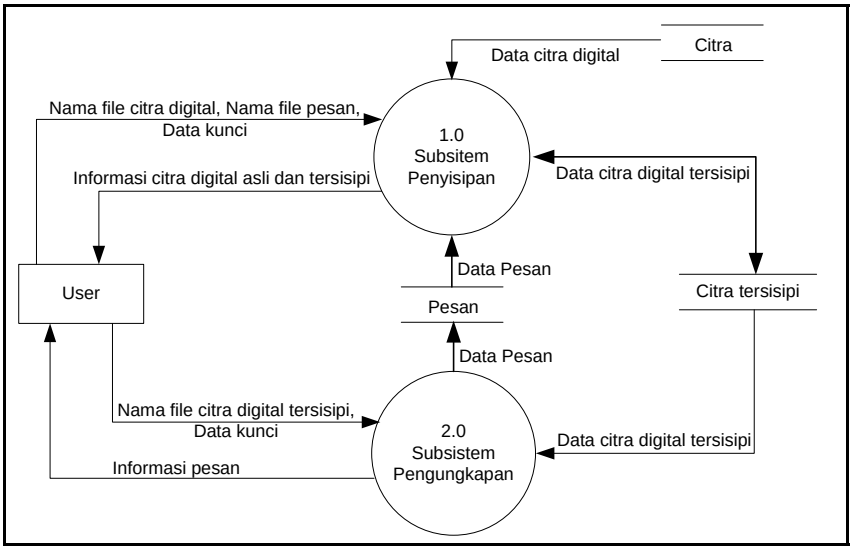
Menurut Munir (2006) RC4 adalah *cipher* aliran yang digunakan secara luas pada sistem keamanan seperti protokol SSL (*Secure Socket Layer*). Algoritma kriptografi ini sederhana dan mudah diimplementasikan. RC4 dibuat oleh Ron Rivest dari laboratorium RSA (RC adalah singkatan dari *Ron 's Code*). RC4 membangkitan aliran kunci (*keystream*) yang kemudian di-*XOR*-kan dengan *plaintext* pada waktu enkripsi (atau di-*XOR*-kan dengan bit-bit *ciphertext* pada waktu dekripsi). Tidak seperti *cipher* aliran yang memproses data dalam bit, RC4 memproses data dalam ukuran *byte*.

Metoda LSB (*Least Significant Bit*) merupakan metode steganografi yang paling sederhana dan paling mudah diimplementasikan (Munir, 2006). Untuk menjelaskan teknik penyembunyian LSB yang dipakai ini, digunakan citra digital sebagai media penampung. Setiap *pixel* yang ada di dalam *file* citra berukuran 1 sampai 3 *byte*. Pada susunan bit dalam setiap *byte* (1 byte = 8 bit), ada bit yang paling berarti (*Most Significant Bit* atau MSB) dan bit yang paling kurang berarti (*Least Significant Bit* atau LSB).

Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Hal ini karena mata manusia tidak dapat membedakan perubahan warna yang kecil ini.

3. Analisis

Secara umum perangkat lunak pengamanan pesan rahasia ini berfungsi untuk menyembunyikan pesan rahasia di balik media penampung citra digital. Agar kerahasiaan informasi yang terkandung dalam citra digital lebih terjaga maka digunakan sebuah algoritma kriptografi yang bermanfaat untuk melakukan proses enkripsi dan dekripsi pesan rahasia.

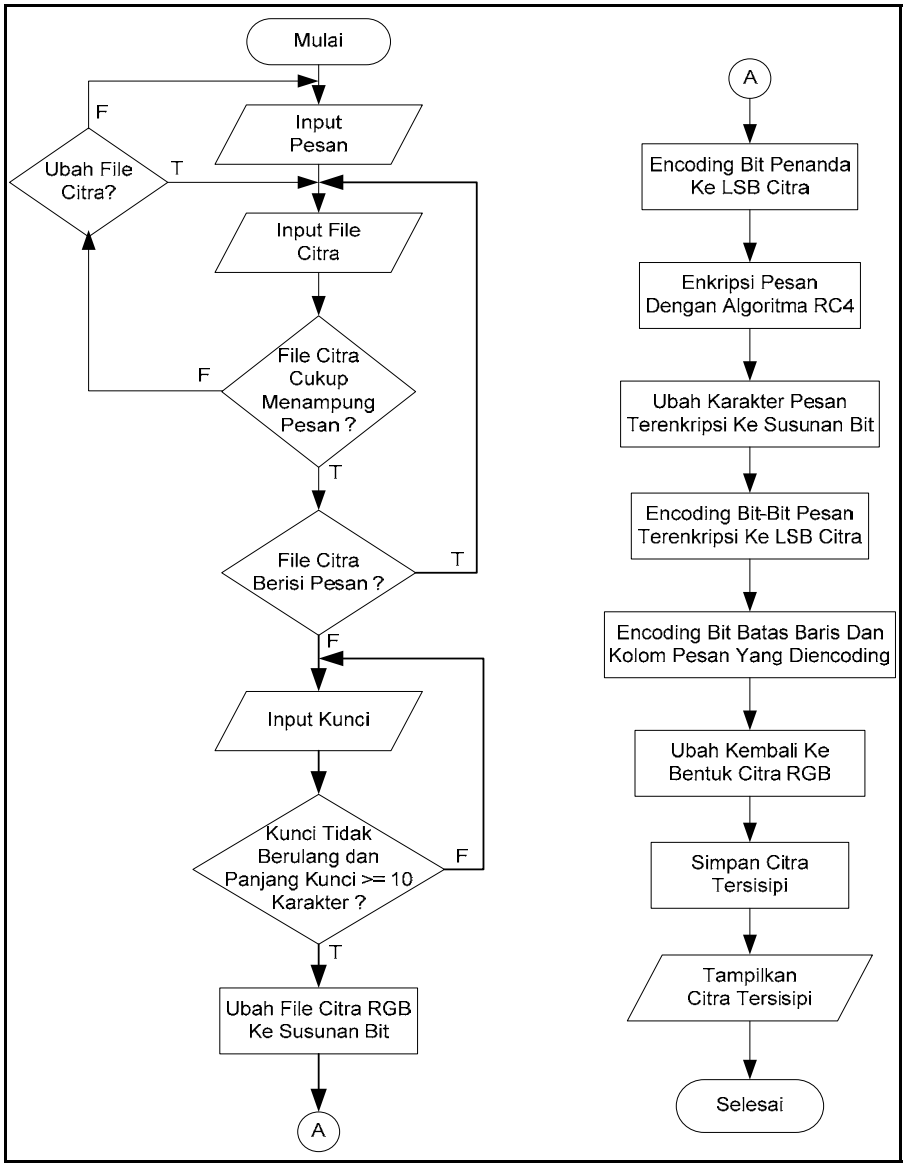


Gambar 1. Diagram Konteks Sistem Pengamanan Pesan Rahasia Yang Diusulkan

Gambar 1 merupakan Diagram Konteks dari sistem pengamanan pesan rahasia. Terminator dari sistem ini adalah *user*. Pada terminator tersebut, kita mengetahui apa yang diberikan ataupun diterima terminator dari atau pada sistem.

Proses penyisipan pesan rahasia (Gambar 2) ke dalam *file* citra digital dimulai dengan memasukkan pesan rahasia kemudian memasukkan *file* citra digital dan memasukkan kunci. Untuk *file* bitmap 24 bit maka setiap *pixel* (titik) citra digital terdiri dari susunan tiga warna, yaitu *Red*, *Green* dan *Blue* (RGB) yang masing-masing disusun oleh bilangan 8 bit dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111.

Setelah mengubah citra digital ke susunan bit, maka langkah selanjutnya yaitu menyisipkan bit-bit penanda ke dalam citra digital yang nantinya akan digunakan sebagai penanda bahwa citra digital tersebut telah berisi pesan rahasia. Pesan rahasia kemudian di-enkripsi menggunakan algoritma RC4. Karakter pesan rahasia ter-enkripsi ini lalu diubah menjadi bit-bit yang akan di-*encoding* ke dalam citra digital. Setelah proses *encoding* pesan rahasia yang ter-enkripsi ke dalam citra digital selesai, maka bit-bit batas baris dan kolom penentu lokasi penyisipan pesan rahasia ter-enkripsi akan di-*encoding* ke dalam citra digital. Kemudian citra digital yang telah berisi pesan rahasia diubah kembali ke dalam format RGB yang baru sehingga diperoleh sebuah citra digital baru yang telah berisikan pesan rahasia.

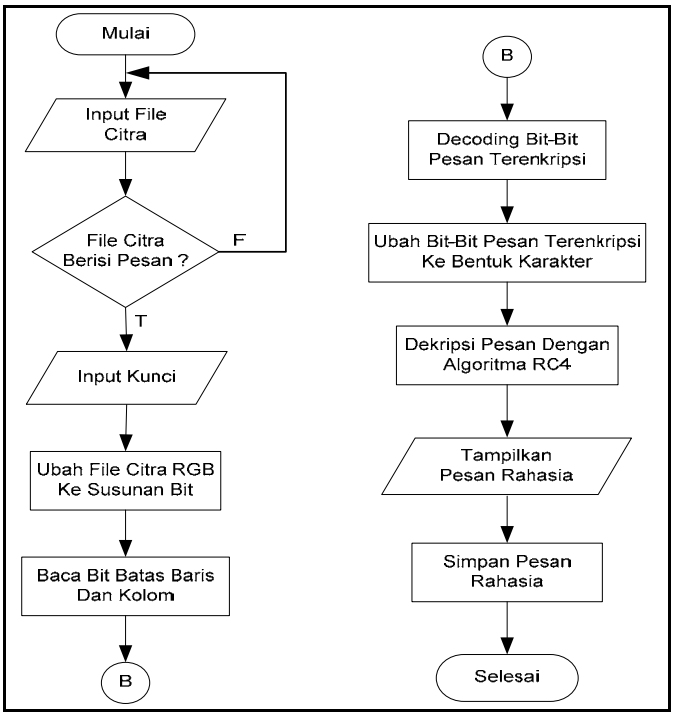


Gambar 2. Diagram Alir Proses Penyisipan Pesan Rahasia

Proses pengungkapan pesan rahasia (Gambar 3) dari citra digital dimulai dengan memasukkan *file* citra digital tersisipi dan memasukkan kunci. Kemudian *file* citra digital tersisipi diubah ke susunan bit. Langkah selanjutnya adalah membaca bit-bit batas baris dan kolom untuk memperoleh lokasi bit-bit penyisipan pesan rahasia terenkripsi yang ada dalam citra digital tersisipi.

Setelah diperoleh lokasi bit-bit penyisipan pesan rahasia ter-enkripsi maka proses *decoding* akan berjalan sehingga bit-bit pesan rahasia ter-enkripsi akan diperoleh. Bit-bit pesan rahasia ter-enkripsi ini diubah kembali ke bentuk karakter.

Karakter pesan rahasia terenkripsi tersebut lalu didekripsi menggunakan algoritma RC4 untuk menghasilkan pesan rahasia yang diinginkan.



Gambar 3. Diagram Alir Proses Pengungkapan Pesan Rahasia

4. Hasil Uji dan Pembahasan

Pengujian bertujuan untuk memastikan bahwa perangkat lunak yang dibuat memenuhi tujuan yang diinginkan. Pengujian dilakukan terhadap empat aspek, yakni aspek *imperceptibility*, aspek *fidelity*, aspek *recovery* dan aspek *security*.

Aspek *imperceptibility* yang dimaksud adalah keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi (Munir, 2006). Untuk dapat menguji aspek ini pada perangkat lunak yang telah dibuat, maka akan dilakukan dengan menyebarkan kuesioner secara acak. Sebanyak lima puluh responden diminta untuk membandingkan sepuluh pasangan citra digital yang belum tersisipi pesan dan yang sudah tersisipi pesan. Responden hanya memilih satu di antara 5 skala pilihan yang telah disediakan. Skala pilihan yang digunakan adalah skala Likert. Pesan rahasia yang disisipkan ke dalam citra digital ini merupakan pesan rahasia dengan kapasitas terbesar yang dapat ditampung oleh masing-masing citra digital uji. Pemilihan pesan rahasia ini disebabkan karena semakin besar ukuran pesan rahasia yang digunakan, maka semakin kecil kualitas citra digital yang dihasilkan. Hal ini akan cukup mewakili penilaian keberhasilan penelitian ini. Hasil pengujian aspek *imperceptibility* dapat dilihat pada Tabel 1.

Tabel 1.
Hasil Kuesioner Pengujian Aspek *Imperceptibility*

Citra Digital Asli	Citra Digital Tersisipi Pesan	Nilai Rata-rata
About.bmp	Full-About.bmp	4,40
Bamboo.bmp	Full-Bamboo.bmp	4,46
Bitmap_001.bmp	Full-Bitmap_001.bmp	4,14
Flower.bmp	Full-Flower.bmp	3,64
Lena.bmp	Full-Lena.bmp	4,34
Loadscreen.bmp	Full-Loadscreen.bmp	4,14
Setup2.bmp	Full-Setup2.bmp	4,46
Setup3.bmp	Full-Setup3.bmp	4,20
Musi.bmp	Full-Musi.bmp	4,12
Worm.bmp	Full-Worm.bmp	4,40

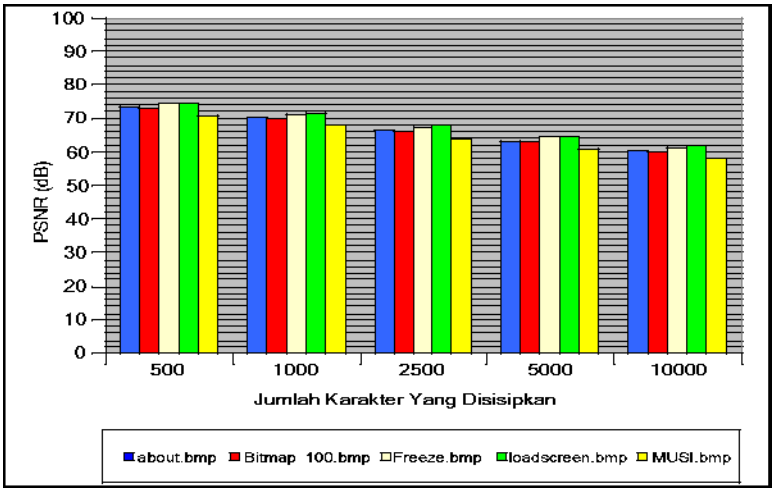
Berdasarkan Tabel 1 dapat dilihat bahwa rata-rata responden memilih skala keempat yaitu setuju dengan pernyataan jika citra digital yang dibandingkan tidak memiliki perbedaan.

Aspek *fidelity* yang dimaksud adalah bahwa mutu berkas citra digital hasil penyisipan pesan rahasia tidak jauh berubah jika dibandingkan dengan berkas citra digital asli (Munir, 2006). Pengujian terhadap aspek *fidelity* pada perangkat lunak ini dilakukan dengan menghitung nilai *Peak Signal to Noise Ratio* (PSNR) pada citra digital. PSNR merupakan nilai (rasio) yang menunjukan tingkat toleransi noise tertentu terhadap banyaknya noise pada suatu sinyal video/citra. PSNR menyatakan tingkat kemiripan antara citra terekonstruksi dengan citra digital asli (Sianipar dan Muliani, 2003). Nilai PSNR yang semakin tinggi akan menghasilkan kualitas kemiripan yang semakin baik. Nilai PSNR yang wajar mempunyai angka minimal 30 dB (decibel). Nilai PSNR ini akan dihitung dengan menggunakan software MSU Video Quality Measurement Tool Version 2.7.3.

Pengujian dilakukan terhadap 5 buah citra digital uji yang telah berisikan pesan rahasia tersisipi melalui perangkat lunak yang telah dibuat. Kelima citra digital uji ini akan disisipkan sejumlah karakter dengan jumlah yang bervariasi. Hal ini dimaksudkan untuk mengetahui seberapa besar perubahan yang terjadi pada citra digital uji yang diukur dengan besarnya perubahan nilai PSNR dari setiap citra digital uji tersebut. Citra digital pengujian memiliki ukuran bervariasi, yang diharapkan dapat menunjukkan kemampuan perangkat lunak yang dibuat terhadap berbagai macam ukuran citra digital uji.

Tabel 2.
Hasil Pengujian Citra Digital Dalam Nilai PSNR (dB)

Jumlah Karakter Yang Disisipkan	Nilai PSNR (dB)				
	about.bmp	Bitmap_100.bmp	Freeze.bmp	loadscreen.bmp	MUSI.bmp
500	73,3930	72,9509	74,4629	74,6501	70,8098
1000	70,4235	70,0004	71,4549	71,6828	67,7907
2500	66,4413	66,0447	67,4608	67,7357	63,8621
5000	63,4282	63,0455	64,5035	64,7520	60,8920
10000	60,4193	60,0327	61,4841	61,7638	57,8924



Gambar 4. Grafik Perbandingan PSNR Terhadap Jumlah Karakter Yang Disisipkan

Dari hasil pengujian terhadap kelima buah *file* citra digital uji yang disisipkan karakter dengan jumlah karakter yang bervariasi diperoleh hasil nilai PSNR dari masing-masing *file* citra digital uji yang berbeda untuk setiap jumlah karakter yang disisipkan. Hasil pengujian nilai PSNR dari setiap *file* citra digital yang diuji dapat dilihat pada Tabel 2 dan grafik perbandingan nilai PSNR terhadap jumlah karakter yang disisipkan dapat pula dilihat pada Gambar 5. Dari tabel dan grafik tersebut terlihat sangat jelas bahwa jumlah karakter yang disisipkan pada setiap *file* citra digital uji berpengaruh terhadap nilai PSNR yang dihasilkan. *File* citra digital uji yang digunakan mengalami perubahan sesuai dengan jumlah karakter yang disisipkan ke dalam *file* citra digital sebelumnya.

Semakin banyak karakter yang disisipkan maka semakin berkurang pula kualitas citra digital yang dihasilkan. Hal ini ditandai dengan berkurangnya nilai PSNR yang dihasilkan oleh masing-masing *file* citra digital uji. Besarnya ukuran *file* citra digital juga mempengaruhi perolehan nilai PSNR. Nilai PSNR yang dihasilkan dari kelima *file* citra digital uji bervariasi sesuai dengan besarnya ukuran *file* citra digital yang digunakan. Hal ini membuktikan bahwa pada perangkat lunak yang dibuat ini menghasilkan hasil yang cukup baik untuk setiap penyembuyian pesan ke

dalam *file* citra digital uji.

Aspek *recovery* yang dimaksud adalah pesan rahasia rahasia harus dapat diungkapkan kembali (Munir, 2006). Pada tahap ini akan dilakukan pengujian beberapa kali untuk memastikan bahwa data rahasia yang disisipkan dalam citra digital dapat didapatkan kembali dalam keadaan utuh. Indikator keberhasilan pengujian ini adalah jika isi dan panjang teks pesan rahasia asli sama dengan isi dan panjang teks pesan rahasia hasil pengungkapan.

Tabel 3.
Pengujian Aspek *Recovery*

Pesan Asli	Panjang Pesan Asli (byte)	Citra Digital	Dimensi Citra Digital	Status Ekstraksi	Pesan Terungkap	Panjang Pesan Terungkap (byte)
readme.txt	991	about.bmp	579x351	Berhasil	2-about.txt	991
changelog.txt	5144	Bitmap_100.bmp	576x360	Berhasil	2-Bitmap_100. txt	5144
ABOUT_APACHE.txt	14605	Freeze.bmp	648x446	Berhasil	2- Freeze.txt	14605
LICENSE.txt	38204	loadscreen.bmp	640x480	Berhasil	2- loadscreen.txt	38204

Dari pengujian pada aspek *recovery* yang telah dilakukan, tingkat keberhasilannya adalah 100%. Hal ini dapat dilihat pada Tabel 3 di atas. Artinya, perangkat lunak ini mendukung aspek *recovery*.

Aspek *security* pada perangkat lunak ini diperoleh melalui kunci enkripsi. Untuk mendapatkan pesan rahasia yang telah disisipkan hanya dapat dilakukan dengan memberikan kata kunci yang tepat. Jika kata kunci yang dimasukkan tidak tepat, maka pesan rahasia yang ditampilkan tidak sesuai dengan pesan rahasia yang asli.

Untuk mengetahui aspek *security* pada perangkat lunak, dilakukan pengujian dengan proses penyisipan dan pengungkapan pesan pada citra digital. Pengujian ini akan menggunakan 2 buah kasus. Kasus yang pertama apabila kunci pengungkapan yang digunakan benar. Kasus kedua adalah apabila kunci pengungkapan yang digunakan salah. Dari pengujian kasus pertama dihasilkan pesan rahasia terungkap serupa dengan pesan rahasia yang asli. Sedangkan dari pengujian kasus kedua dihasilkan pesan rahasia terungkap berbeda jauh dengan pesan rahasia yang asli.

Dari pengujian pada aspek *security* yang telah dilakukan, tingkat keamanan pesan rahasia dirasakan cukup tinggi. Pesan rahasia yang disisipkan hanya dapat diungkap dengan menggunakan kunci yang benar.

Dari semua pengujian yang telah dilakukan, diketahui bahwa perangkat lunak memenuhi semua aspek pengujian yang dilakukan. Berdasarkan hasil pengujian, dapat dilihat bahwa dengan menggunakan perangkat lunak ini keamanan pesan rahasia yang disisipkan ke dalam citra digital akan semakin meningkat.

Daftar Pustaka

Angraini., Ema Utami. (2007). Analisis Penyisipan Data Pada Citra Bitmap Menggunakan Metode Bit Plane Complexcity Segmentation. *Seminar Nasional Teknologi 2007 (SNT 2007)*, Yogyakarta, 24 November 2007.

Anna, Theresia., M. A. Ineke Pakereng, Yos Richard Beeh. (2009). Implementasi Algoritma Chaos-Based Feedback Stream Cipher pada Enkripsi-Dekripsi Data Citra Digital. *Jurnal Informatika UKM*, Vol. 5, No. 2, pp: 151–169.

Bunyamin, Hendra., Andrian. (2009). Aplikasi Steganography pada File dengan Menggunakan Teknik Low Bit Encoding dan Least Significant Bit. *Jurnal Informatika UKM*, Vol. 5, No. 2, pp: 107–117.

Munir, Rinaldi. (2006). *Kriptografi*. Bandung: Informatika.

Narayana, Sujay., Gaurav Prasad. (2010). Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions. *Signal & Image Processing: An International Journal (SIPIJ)*, Vol. 1, No. 2, pp: 60-73.

Sarmah, Dipti Kapoor., Neha Bajpai. (2010). Proposed System for Data Hiding Using Cryptography and Steganography. *International Journal of Computer Applications*, Vol. 8, No. 9, pp: 7-10.

Schneier, Bruce. (1996). *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)*. John Wiley & Sons, Inc.

Shreelekshmi R., dan M. Wilscy. (2010). Preprocessing Cover Images for More Secure LSB Steganography. *International Journal of Computer Theory and Engineering*, Vol. 2, No. 4, pp: 546-551.

Sianipar, Rismon H., Sri Muliani WJ. (2003). *Kompresi Citra Digital Berbasis Wavelet*: *Tinjauan PSNR Dan Laju Bit*. Jurnal Informatika, Vol. 4, No. 2, pp: 81- 87.

Stallings, William. (2005). *Cryptography and Network Security Principles and Practices, Fourth Edition.* Prentice Hall.

Sukrisno., Ema Utami. (2007). Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher Dan Fungsi Hash MD5. *Seminar Nasional Teknologi 2007 (SNT 2007)*, Yogyakarta, 24 November 2007.

Swain, Gandharba., Dodda Ravi Kumar, Anita Pradhan, Saroj Kumar Lenka. (2010). A Technique for Secure Communication Using Message Dependent Steganography. *International Journal of Computer & Communication Technology*, Vol. 2, No. 2,3,4, pp: 177-1