TEKNIK MENYEMBUNYIKAN PESAN RAHASIA MENGGUNAKAN *STEGANOGRAPHY* DAN *CRYPTOGRAPHY*

M. Miftakul Amin

Jurusan Teknik Komputer, Politeknik Negeri Sriwijaya Palembang
Jalan Srijaya Negara, Palembang 30139
Telp. 0711 – 353414 Fax. 0711 – 355918
e-mail : miftakul_a@polsri.ac.id

ABSTRACT

Development of Internet technology has demonstrated the communication that occurs does not require face to face directly. Safety factor becomes an important issue in the communication using the Internet network. Various attempts were made to keep the information security and confidentiality can be maintained. Steganography and cryptography techniques present as a technique to achieve data security. This research attempts to develop an application that can be used for communication by using two techniques. In this study steganography method used is the Least Significant Bit (LSB) whereas cryptography method used is the Caesar cipher. From the research that has been done can be generated an application that has been able to perform encryption and decryption of secret messages that can be hidden in a digital image color (24 bit).

Key words : steganography, cryptography, LSB

ABSTRAK

Perkembangan teknologi internet telah memperlihatkan komunikasi yang terjadi tidak mengharuskan bertatap muka secara langsung. Faktor keamanan menjadi isu penting dalam komunikasi menggunakan jaringan internet. Berbagai upaya dilakukan untuk menjaga supaya informasi dapat terjaga keamanan dan kerahasiaannya. Teknik *steganography* dan *cryptography* hadir sebagai teknik untuk mewujudkan keamanan data. Penelitian ini mencoba mengembangkan sebuah aplikasi yang dapat digunakan untuk melakukan komunikasi dengan menggunakan kedua teknik tersebut. Dalam penelitian ini metode *steganography* yang digunakan adalah *Least Significant Bit* (LSB) sedangkan metode *cryptography* yang digunakan adalah Caesar cipher. Dari penelitian yang telah dilakukan dapat dihasilkan sebuah aplikasi yang telah mampu melakukan proses enkripsi dan dekripsi pesan rahasia yang dapat disembunyikan dalam citra digital berwarna (24 bit).

Kata kunci : ***steganography, cryptography, LSB***

1. PENDAHULUAN

Teknologi informasi dan komunikasi mengarah kepada teknologi yang bersifat heterogen dan berjalan menggunakan jaringan internet. Hal ini membawa konsekuensi kepada dibutuhkannya komunikasi yang bersifat rahasia. Terdapat 2 teknik yang digunakan dalam komunikasi rahasia, yaitu teknik *cryptography* dan *seganography* [1]. Teknik *cryptography* digunakan untuk melakukan *encoding* atau enkripsi terhadap pesan rahasia. Pesan dilindungi sedemikian rupa sehingga tidak dapat terbaca oleh pihak yang tidak berwenang. Pesan hanya dapat dibaca oleh pihak yang memiliki otoritas. Sedangkan teknik yang ke-2 merupakan teknik *steganography* yang memiliki fungsi untuk menyembunyikan pesan rahasia. Dari sisi visibilitas teknik *steganography* disebut sebagai *invisible communication* sedangkan teknik *cryptography* disebut dengan *visible communication* [2].

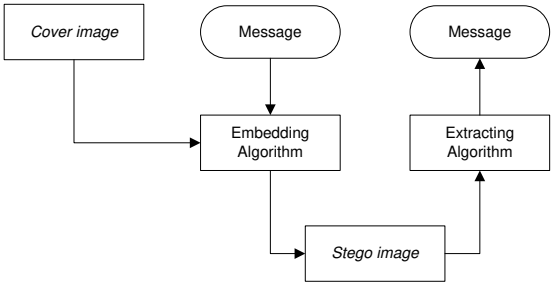
Masalah keamanan (security) pada komputer menjadi isu penting pada era teknologi informasi. Banyak kejahatan cyber yang pernah kita dengar dari media massa terutama berita dari internet, pelaku kejahatan memanfaatkan celah keamanan yang ada untuk dimasuki dan melakukan manipulasi. *Cryptography* merupakan ilmu dan seni untuk menjaga keamanan pesan. Cryptography berasal dari bahasa Yunani terdiri dari *cryptos* yang berarti rahasia, sedangkan *graphein* yang berarti tulisan [3].

Sebuah pesan rahasia dapat disisipkan ke dalam beragam file digital, seperti file teks, file audio, file video, maupun file image atau citra digital, dan protokol jaringan [4]. Beragam media yang digunakan sebagai tempat disisipi pesan dikenal sebagai media (carrier). Dalam teknik *image stegnography* dengan menggunakan citra digital sebagai file pembawa pesan, terdapat beberapa komponen yang terlibat, yaitu:

- ***Cover image***, sebagai citra digital asli yang digunakan untuk menyembunyikan pesan.
- ***Message***, pesan yang akan disisipkan ke dalam *cover image*. Pesan dapat berupa file teks ataupun file citra digital.
- ***Stego-image***, *cover image* yang telah disisipi *message* di dalamnya.
- ***Stego-key***, sebuah kunci yang digunakan untuk melakukan proses penyisipan pesan ke dalam *cover image* dan pembacaan pesan dari *stego image*.

Secara umum *image steganography* merupakan sebuah metode yang digunakan untuk menyembunyikan pesan rahasia ke dalam *cover image* dengan menggunakan

sebuah *stego image*. Selanjutnya *stego image* dikirimkan ke pihak yang berhak menerima pesan melalui sebuah saluran komunikasi. Pihak yang tidak berhak atas isi pesan tidak menyangka bahwa gambar atau image tersebut berisi sebuah pesan rahasia. setelah pesan image sampai kepada penerima selanjutnya pesan dapat dibaca. Gambar 1 memperlihatkan bagaimana cara kerja dari *image steganography*.

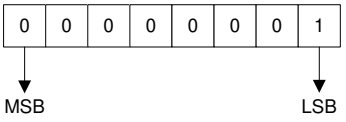


Gambar 1. *Image Steganography*

Beberapa aspek penting dalam *image steganography* diharapkan memenuhi beberapa criteria sehingga diperoleh teknik steganography yang handal [5], diantaranya:

- ***High Capacity***, merupakan seberapa besar informasi yang dapat disisipkan dalam sebuah citra digital.
- ***Perceptual Transparency***, setelah sebuah pesan disisipkan dalam *cover image*, maka kualitas dari sebuah *stego image* tidak jauh berbeda dengan *cover image*. Artinya kualitas dari file image yang asli dengan yang telah disisipi pesan tidak jauh berbeda.
- ***Robustness*****,** pesan yang telah disisipkan dalam citra digital (*image*) tidak akan rusak atau hilang akibat terjadinya proses modifikasi terhadap citra digital seperti proses pemotongan (*cropping*), perbesaran/pengecilan (*scaling*), putaran (*rotation*), maupun penambahan noise.
- ***Temper Resistence***, pesan yang telah disisipkan dalam *stego image* dilindungi dari terjadinya proses modifikasi oleh pihak yang tidak berwenang.
- ***Computation Complexity***, seberapa besar kompleksitas komputasi maupun algoritma yang digunakan dalam proses penyisipan dan ekstraksi pesan yang telah ditanamkan dalam *stego image*.

Dalam *Image Steganography* dengan menggunakan teknik *Least Significant Bit* (LSB) yang digunakan untuk menyembunyikan pesan, dilakukan dengan cara mengganti bit-bit data di dalam segmen citra dengan bit-bit data pesan rahasia yang akan disisipkan [6]. Gambar 2 meperlihatkan bagaimana posisi LSB dalam byte data.



Gambar 2. Posisi LSB dan MSB

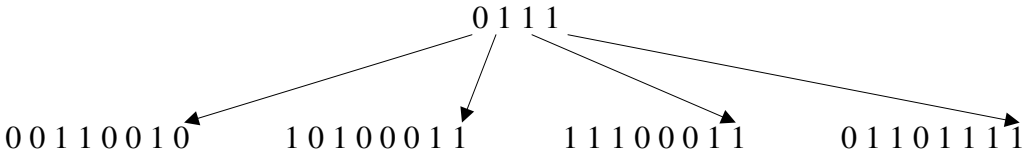
Seperti diperlihatkan pada Gambar 2 posisi bit LSB adalah posisi bit yang memiliki nilai pangkat 0, sedangkan Most

Significant Bit (MSB) merupakan posisi bit dengan nilai pangkat paling tinggi. Penggunaan LSB untuk menyembunyikan pesan rahasia karena posisi bit dengan pangkat 0 akan bernilai 1 atau 0, artinya perubahan yang dilakukan pada LSB hanya akan menaikkan atau menurunkan nilai sebagnyak 1. Sehingga kualitas dari image asli dan image setelah disisipi pesan tidak akan berbeda jauh.

Sebagai contoh terdapat segmen data citra (pixel) sebelum disisipi pesan rahasia seperti pada deretan berikut.

0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0
1 1 1 0 0 0 1 0 0 1 1 0 1 1 1 1

Kemudian terdapat pesan yang akan disisipkan ke dalam citra digital dengan bit 0 1 1 1, maka pixel citra sekarang menjadi:



Selanjutnya untuk memperkuat teknik penyembunyian pesan, bit-bit data rahasia tidak digunakan mengganti bit-bit pixel penyusun citra secara berurutan, melainkan dipilih susunan penyisipan secara acak. Sebagai contoh jika terdapat 50 posisi *byte* dan terdapat 6 bit data yang akan disembunyikan, maka posisi *byte* yang akan diganti bit LSB-nya dipilih secara acak, sebagai contoh bit nomor 36, 5, 21, 10, 18, dan 49. Bilangan acak tersebut dapat dibangkitkan dengan menggunakan algoritma kriptografi *metode pseudo-random-number-generator* (PRNG). Pada dasarnya algoritma PRNG digunakan untuk melakukan enkripsi.

Sharma [7] melakukan penelitian dengan melakukan proses penyembunyian file image ke dalam file image (sebagai *cover image*). Metode yang digunakan adalah Least Significant Bit (LSB). Jenis file image yang digunakan adalah *grayscale* (8 bit) dan *true colour* (24 bit). Teknik yang digunakan adalah dengan cara file image yang akan disisipkan adalah nilai MSB yang selanjutnya dimasukkan ke dalam LSB *cover image*. Penelitian ini membuktikan bahwa kualitas dari cover image tetap terjaga dan kompleksitas algoritma yang digunakan juga tidak terlalu rumit.

Dewi [8] yang mengembangkan perangkat lunak steganografi pada file AVI yang diberi nama AVISteg. Metode yang dikembangkan dalam penelitian ini adalah *LSB Modification*. AVISteg

diimplementasikan dalam bahasa pemrograman pascal dengan kompilator Borland Delphi 7 dan beroperasi pada lingkungan sistem operasi *windows*. AVISteg ini berhasil menyisipkan data ke dalam kumpulan file BMP, tetapi tidak berhasil mengubah kembali kumpulan file BMP tersebut ke dalam file AVI. Penelitian yang dilakukan oleh Amin [9] telah mengembangkan aplikasi steganography menggunakan metode LSB pada file citra digital berwarna (24 bit). Penyisipan bit dilakukan pada setiap komponen warna RGB.

Penelitian ini mencoba mengembangkan penelitian yang telah dilakukan oleh Amin [9] yang telah berhasil membuat aplikasi *steganography* menggunakan metode LSB, dengan menambahkan fungsiolitas berupa enkripsi dan dekripsi menggunakan *cryptography* klasik *Caesar Cipher*.

2. METODE PENELITIAN

Dalam penelitian ini dikembangkan aplikasi *steganography* untuk menyisipkan pesan rahasia berupa teks dan mengekstraknya kembali sesuai dengan pesan teks yang disisipkan ke dalam file gambar.

Kebutuhan Fungsional

Kebutuhan fungsional dari aplikasi yang akan dikembangkan dapat melakukan fungsi-fungsi diantaranya:

1. Dapat memberikan kemudahan kepada user untuk menggunakan aplikasi *steganography* citra digital (*image*).
2. Sebelum pesan rahasia disisipkan, pesan tersebut telah di-enkripsi terlebih dahulu, demikian juga pada saat ekstraksi pesan tersebut di-dekripsi untuk diperoleh pesan sesusungguhnya.

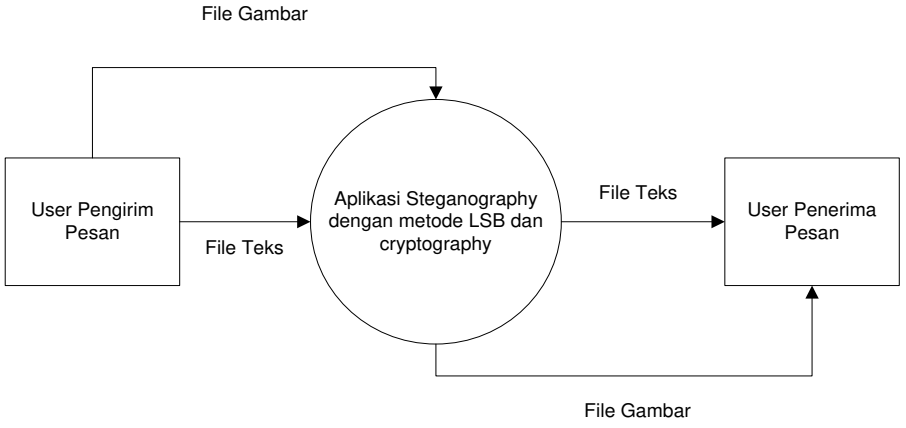
Kebutuhan Antar Muka

Kebutuhan *user interface* dikembangkan untuk berinteraksi dengan lingkungan eksternal perangkat lunak. Aplikasi dibangun supaya mudah digunakan oleh pengguna (*user friendly*). Kebutuhan ini diharapkan dapat disesuaikan dengan kebiasaan pengguna, sehingga meningkatkan produktifitas dalam bekerja.

Perancangan Sistem

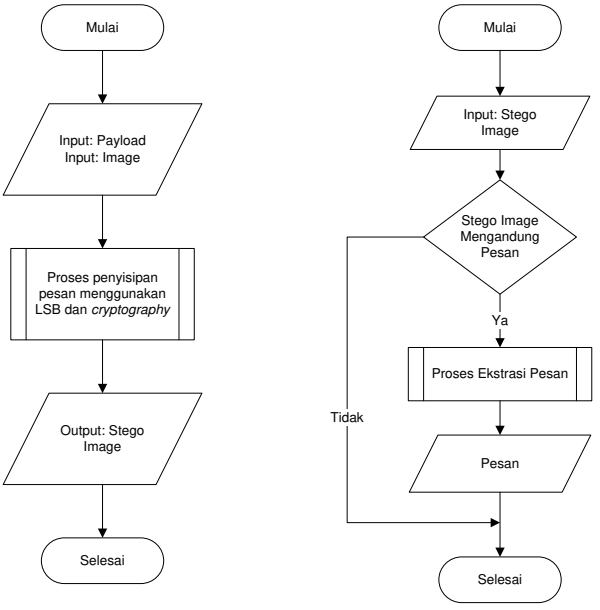
Untuk menggambarkan sistem secara utuh yang menggambarkan hubungan antara lingkungan internal dan eksternal dapat dituangkan menggunakan Data Flow Diagram (DFD). Gambar 3. menggambarkan Context Diagram dari sistem yang akan dikembangkan. Proses

yang terjadi adalah bahwa user pengirim melakukan proses penyisipan pesan rahasia dengan menggunakan file teks untuk disisipkan ke dalam file image. Dalam prosesnya pesan disisipkan menggunakan metode LSB dan *cyrptography* untuk melakukan enkripsi pesan. User penerima dapat melakukan ekstraksi pesan dengan menggunakan file image yang telah diterima.



Gambar 3. Context Diagram

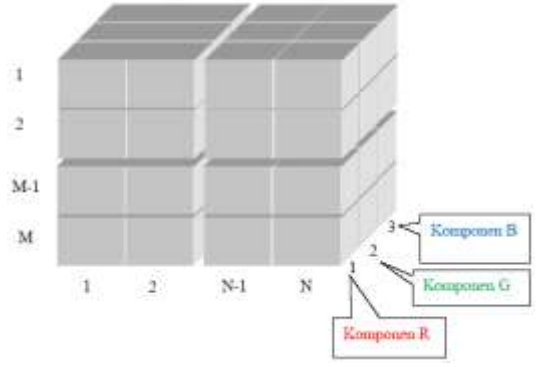
Logika program digambarkan menggunakan flowchart program seperti dapat dlihat pada Gambar 4.



(a)Proses Penyisipan Pesan (b) Proses Ekstraksi Pesan

Gambar 4. Flowchar Program Penyisipan dan Ekstraksi Pesan

Pada uji coba ini digunakan media citra digital *true colour* 24 bit dengan model warna RGB. Pada citra digital nantinya terdapat 3 bit yang dapat disisipi dalam 1 pixel. Hal ini dikarenakan dalam 1 pixel warna tersusun dari 3 komponen warna, yaitu Red, Green, dan Blue yang masing-masing disusun oleh 8 digit bilangan biner dari rentang nilai 0 sampai dengan 255 dalam desimal atau 00000000 sampai 11111111 dalam representasi biner. Representasi pixel citra digital 24 bit dengan model warna RGB dapat dilihat pada Gambar 5.



Gambar 5. Model Citra Warna RGB

Penelitian ini menghasilkan sebuah perangkat lunak untuk menyisipkan pesan teks ke dalam file citra digital (*image*). Perangkat lunak dikembangkan menggunakan bahasa pemrograman visual basic 6.0 yang memiliki beberapa kelebihan seperti berbasis objek, *event driven programming*, dan kemampuan membuat *user defined function*.

Dalam kriptografi klasik, secara umum dapat dikelompokkan dalam dua model yaitu menggunakan tekik substitusi dan transposisi [10]. Teknik substitusi dilakukan dengan mengganti salah satu karakter yang ada dalam sebuah teks menggunakan karakter yang lain. Teknik yang termasuk dalam kategori substitusi adalah kriptografi Caesar. Teknik yang digunakan adalah dengan memetakan karakter A-z ke dalam deretan index numeric seperti Gambar 6.

3. HASIL DAN PEMBAHASAN

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 6. Pemetaan Karakter

Algoritma Caesar chipper melakukan pergeseran karakter sebagai kunci (k)

dengan rentang nilai k sebesar 1 – 25, yang secara matematis dijabarkan dalam bentuk:

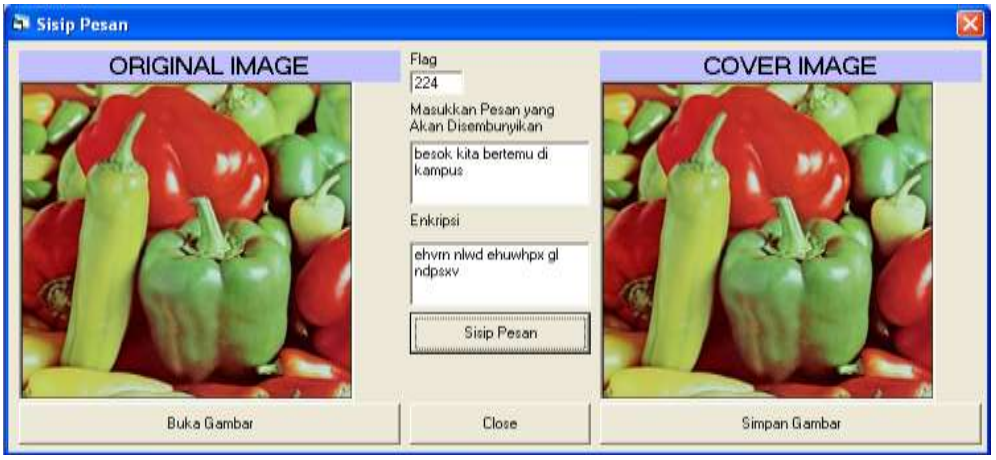
Untuk proses enkripsi :

C = E (k, p) = (p + k) mod 26 ... (1)

Sedangkan untuk melakukan proses dekripsi :

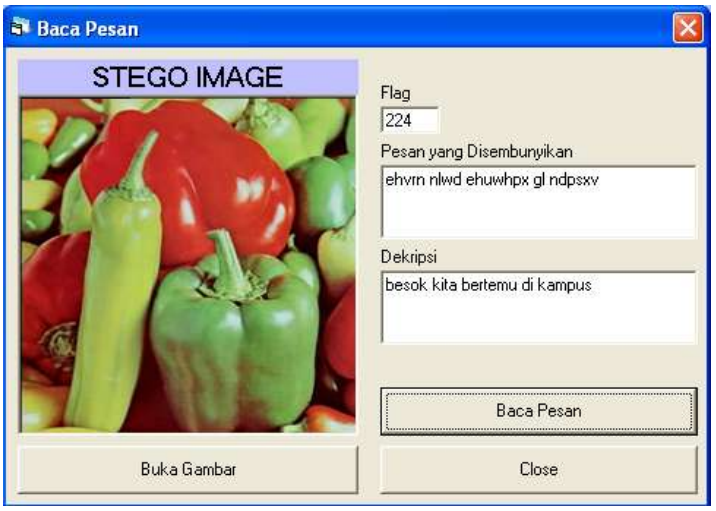
P = D (k, c) = (C – k) mod 26 ... (2)

Untuk menyisipkan pesan rahasia, terlebih dahulu dipilih file citra digital yang akan disisipi pesan. File image tersebut merupakan jenis citra berwarna 24 bit. Gambar 7 memperlihatkan proses penyisipan pesan ke dalam file citra digital. Pesan yang akan disisipkan terlebih dahulu dienkripsi sebelum proses penyisipan dengan metode LSB dilakukan. Selanjutnya setelah proses penyisipan selesai dilakukan maka gambar yang telah disisipi pesan tersebut perlu disimpan, dan dapat dikirimkan kepada pihak yang menerima pesan.



Gambar 7. Proses Penyisipan Pesan Ke Citra Digital

File yang telah disisipi pesan dapat dibaca seperti dapat dilihat pada Gambar 8 yang memperlihatkan bahwa file image yang telah disisipi pesan rahasia dapat menampilkan pesan.



Gambar 8. Proses Pembacaan Pesan Dari Citra Digital

4. SIMPULAN

1. Aplikasi *steganography* ini dapat digunakan untuk melindungi pesan yang dikirimkan sehingga pesan sampai ke tempat tujuan dengan aman.
2. Teknik *cryptography* yang dikombinasikan ke dalam aplikasi dapat meningkatkan keamanan pesan yang tersembunyi.
3. Metode *cryptography* yang digunakan masih sangat sederhana yaitu menggunakan *Caesar cipher* yang hanya melakukan enkripsi dan dekripsi karakter dari A-Z.

PENELITIAN LANJUTAN

Aplikasi *steganography* ini sebaiknya dikembangkan menjadi sebuah aplikasi yang lebih kompleks dan menjadi lebih lengkap. Sebagai contoh berbagai jenis file dapat diproses sebagai media untuk menyisipkan pesan.

UCAPAN TERIMA KASIH

Ucapan terimakasih kepada seluruh teman sejawat di Jurusan Teknik Komputer Politeknik Negeri Sriwijaya Palembang, juga kepada seluruh civitas akademika IBI darmajaya Bandar Lampung terutama kepada lembaga penelitian yang telah memberikan kesempatan kepada penulis sehingga naskah ini dimuat dalam jurnal Informatika.

DAFTAR PUSTAKA

[1] Gayathri, C.; Kalpana, V. 2013. Study On Image Steganography Techniques, *International Journal of Engineering and Technology*

(IJECT) Vol 5 No 2 Apr-May 2013 ISSN: 0975-4024

[2]. Ramanpreet Kaur, Prof. Baljit Singh. 2012. Survey And Analysis Of Various Steganographic Techniques, *International Journal Of Engineering & Advanced Technology Volume-2, Issue-3, May-June 2012.*

[3]. Munir, Rinaldi. 2006. Kriptografi. Bandung: Penerbit Informatika Bandung.

[4]. Hussain, Mehdi; Hussain, Mureed. 2013. A Survey of Image Steganography Techniques, *International Journal of Advanced Science and Technology Vol 54 May 2013.*

[5]. E Lin, E Delp. 1999. A Review of Data Hiding in Digital Images. *Procedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, April 25-28, 1999.*

[6]. Saefullah, Asep; Himawan; Agani, Nazori. 2012. Aplikasi Steganografi Untuk Menyembunyikan Teks Dalam Media Image Dengan Menggunakan Metode LSB. *Seminar Nasional Teknologi Informasi dan Komunikasi Terapan Tahun 2012. ISBN: 979-26-0255-0, Semarang: 23 Juni 2012*

[7]. Sharma, Kumar, Vijay; Shrivastava, Vishal. 2012. A Steganography Algorithm for Hiding Image in Image By Improved LSB Substitution By Minimize Detection. *Journal of Theoretical and Applied Information Technology 15th February 2012 Vol 36 No 1.*

[8] Dewi, A.K. 2007. *Studi dan Implementasi Penyembunyian Data di Dalam File Video Digital dengan Metode Least Significant Bit Modification, Tugas Akhir Program Sarjana*. Bandung: Teknik Informatika ITB

[9] Amin, M.M. 2014. Image Steganography dengan Metode Least Significant Bit (LSB), *Computer Science Research and It's Development (CSRID) Journal, Vol 6 No 1 Februari 2014*. Medan: STMIK Potensi Utama

[10] Stalling, W. 2006. *Cryptography and Network Security Principles and Practice Fifth Edition*. New York: Prentice Hall