Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 1) : 25 - 30. Th. 2018
ISSN: 2620-620X

PERANCANGAN STEGANOGRAFI *HIDDEN MESSAGE* DENGAN METODE *LEAST SIGNIFICANT BIT INSERTION* (LSB) BERBASIS MATLAB

Hidden Message Steganography Design with Matlab-based Least Significant Bit Insertion (LSB)

Nizirwan Anwar, nizirwan.anwar@esaunggul.ac.id[1)]
[1)] Teknik Informatika / Fakultas Ilmu Komputer Universitas Esa Unggul Jakarta

ABSTRACT

Steganography (steganography) is the science or technique of art to hide secret messages in other messages so that the existence of such secret messages can not be accessed by others who have no authority. In terms of data security (, text or audio) should follow the appropriate 5 (five) main rules is the factor of confidentiality, integrity, availability, authenticity, and non-repudiation. LSB algorithm method is a method used steganography where the process of combining messages containing text stored in a particular in this format made this research JPG and BMP with a certain pixel size. This research resulted after the process of testing and analyzing using matrix based application (M-File, Matlab) there is no significant change in quality (cover and stego) and text.
Keywords: *Steganography, Cover-Image, Stego-Image, LSB Method*

ABSTRAK

Steganografi (*steganography*) adalah ilmu teknik atau seni untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat di-akses oleh orang lain yang tidak mempunyai kewenangan. Dalam hal keamanan data (teks atau audio) sebaiknya mengikuti sesuai 5 (lima) kaidah utama adalah faktor *confidentiality, integrity, availability, authenticity*, dan *non-repudiation*. Metode algoritma LSB merupakan metode yang digunakan steganografi dimana proses penggabungan pesan yang berisi teks disimpan dalam tertentu dalam hal ini format yang dilakukan penelitian ini JPG dan BMP dengan ukuran piksel tertentu. Penelitian ini menghasilkan setelah proses pengujian dan penganalisaan dengan menggunakan aplikasi berbasis matriks (M-File, Matlab) tidak terdapat perubahan yang siginifikan baik kualitas (*cover* maupun stego) dan teks..
Kata Kunci: Steganografi, *Cover-Image, Stego-Image*, Metode LSB

PENDAHULUAN

Dalam dunia globalisasi teknologi informasi yang dipengaruhi oleh beberapa proses faktor antara lain oleh bisnis dan tata kerja, ekonomi, sosial, sumber daya sosial-budaya, dan lingkungan alam. Dampak berkembang teknologi informasi 'digital' dengan adanya fenomena bagaimana proses sharing data hanya dapat dilihat, dibaca dan di-akses hanya orang yang tepat dan terpercaya. Dalam mengatasi dan melindungi data (teks, dan suara)dari orang yang tidak punya 'kewenangan' atau 'pencuri' atau 'pembajak' data (*data pricacy*), untuk mengatasi hal ini agar tidak terjadi pada orang tertentu.

Tabel 1 Komparasi teknik pengamanan data [4]

	Confidentiality	*Integrity*	*Unremovability*
Encryption	√	×	√
Digital Signatures	×	√	×
Steganography	√	√/	√

Maka dibutuhkan suatu terobosan teknik kriptografi dan atau steganografi, teknik secara umum prinsip nya adalah melindungi keamanan data[4] dengan 5 (lima) kaidah utama adalah faktor

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 1) : 25 - 30. Th. 2018
ISSN: 2620-620X

confidentiality, integrity, availability, authenticity, dan *non-repudiation*.

Table 2 Jenis Image dan ukuran bitnya

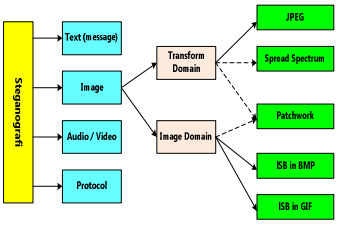
Jumlah Bit	Keterangan
1	Binary-value (0 – 1)
8	Gray level (0 – 255)
16	High colour (216)
24	True Colour (224)
32	True Colour (232)

Steganografi berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan «graphein», yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung" **(Sellars, 1996),** sedangkan kriptografi adalah merupakan teknik menyamarkan dari suatu pesan teks proses *plaintext* menjadi *ciphertext* dan sebaliknya (enkripsi dan deskrpisi) dengan pendekatan dikenal 2 (dua) algoritma simetrik dan a-simetrik[3]. Penelitian ini akan lebih difokuskan pada teknik steganografi dengan metode LSB menggunakan *platform* aplikasi yang berbasis Matlab dengan tujuan ;

(a) Untuk melakukan pengamanan data dan kinerja (*performance)* dengan metode LSB agar data tersrbut tidak dapat di-akses orang lain dan dapat disembunyikan, dapat pula terjaga kerahasiaannya dari pihak yang tidak berwenang (pihak ketiga)
(b) Menguji dan menganalisa ukuran (*size*) proses *file* sebelum (*cover*) dan setelah (*stego*) steganografi dengan metode LSB.
(c) Menguji perubahan yang dialami oleh *file* master dan *file* pesan program dengan menggunakan aplikasi *multi-purposes* M-File (Matlab), baik ukuran dan kualitas data (*compressing*) – JPG dan BMP.

Steganografi

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran *(incognito techniques)* menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas oleh pihak ketiga. Dalam perang Dunia II, teknik steganografi umum digunakan oleh tentara Jerman dalam mengirimkan pesan rahasia dari atau menuju Jerman[6]**.** Misalkan asumsikan terdapat gambar dengan piksel 100 x 100 dan *colourencoding (embedded)* 24 bits (R, G, dan B @ 8 bits) per piksel, maka *colourencoding (embedded)* akan mampu mewakili 0 .. 16.777.215 (mewakili 16 juta warna), dan ruang disk yang dibutuhkan = 100*100* 3 *byte* (karena RGB) = 30.000 bytes = 30 Kbyte atau 100*100* 24 bits = 240.000 bits.



Gambar 1 Kategori Steganografi

Kriteria Steganografi

Kriteria steganografi yang harus diperhatikan dalam penyembunyian data, *image*, teks dan suara[5] antara lain ;

(a) *Fidelity*. Mutu penampung tidak jauh berubah. Setelah penambahan data rahasia, hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam tersebut terdapat data rahasia.
(b) *Robustness*. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya). Bila pada dilakukan

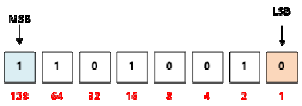
Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 1) : 25 - 30. Th. 2018
ISSN: 2620-620X

operasi pengolahan, maka data yang disembunyikan tidak rusak.

(c) *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*), dimana tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Algoritma Metode LSB

Metode ini bekerja dengan cara mengganti *bit* terakhir dari masing-masing piksel dengan pesan yang akan disisipkan[1][8]. LSB mempunyai kelebihan yakni ukuran gambar tidak akan berubah. Sedangkan kekurangannya adalah pesan/data yang akan disisipkan terbatas, sesuai dengan ukuran. Salah satu *cover* yang dapat digunakan untuk menyembunyikan pesan adalah digital warna 24 *bit*. Setiap piksel l pada warna 24 *bit* memiliki warna yang merupakan kombinasi dari tiga warna dasar *Red, Green, Blue* (RGB). Sedangkan satu piksel l warna 24 bit diwakili oleh 3 (tiga) *byte*, dimana masing-masing 1 *byte* merepresentasikan warna *Red, Green, Blue*. Penyisipan pesan ke dalam *cover* dinamakan *encoding (embedded)*, sedangkan ekstraksi pesan dari *stego* dinamakan *decoding (extraction)*.



Gambar 2 Ilustrasi MSB dan LSB

Sebuah merupakan kumpulan dari titik-titik yang disebut piksel l. Pada warna 24 *bit*, setiap piksel 1 berukuran 3 *byte* dimana setiap *byte* mewakili warna dari setiap komponen *Red, Green, Blue*. Misalkan terdapat 2 piksel l, dimana nilai intensitas setiap warna pada setiap piksel l setelah dikonversikan ke dalam biner memberikan nilai biner sebagai berikut

00100111 11101001 11001000
00100111 11001000 11101001

Untuk menyisipkan sebuah karakter "F" dengan bilangan biner 01000110 (kode ASCII 70) ke dalam 2 piksel 1 warna tersebut, setiap 2 *bit* dari pesan yang dimulai dari MSB disisipkan ke dalam 2 *bit* LSB dari setiap *byte* warna. Dan hasil penyisipannya memberikan nilai piksel l baru sebagai berikut:

00100101 11101000 11001001
001001110 11001000 11101001

Contoh lain penggunaan metode LSB; asumsikan pesan yang akan disisipkan 5 *bit* = 11010, maka jumlah *byte* yang digunakan = 5 *byte*

0010110 11001001 11111001 10001000 10100011

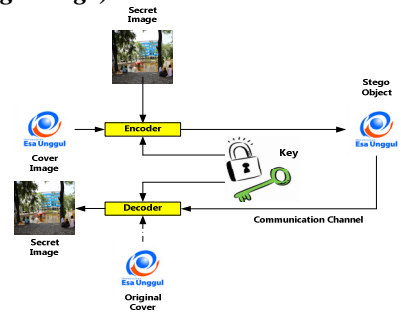
(*byte* yang digunakan untuk penyisipan pesan)

Proses penyisipan pesan **11010**

Hasil penyisipan menjadi ;

0010110<u>1</u> 1100100<u>1</u> 1111100<u>0</u> 1000100<u>1</u> 1010001<u>0</u>

Proses Steganografi (*Cover Image* dan *StegoImage*)



Gambar 3 Konsep Steganografi

Keterangan gambar 3 ;

Embedded-message : pesan yang disembunyikan dapat dalam format teks atau

CoverImage : pesan yang digunakan untuk

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 1) : 25 - 30. Th. 2018
ISSN: 2620-620X

menyembunyikan *embedded message*.

StegoImage : pesan yang sudah berisi pesan *embedded message*.

Stego-key : kunci digunakan berupa sebuah algoritma yang digunakan untuk melakukan penyisipan dan ekstraksi pesan rahasia dari stego

Gambar 4 Tahapan perancangan penelitian

METODE PENELITIAN

Tahapan Metode LSB (*Cover/Stego*)

Tahapan penelitian secara garis besar yang akan dan telah dilakukan adalah sebagai berikut:

(a) Studi literatur adalah studi pustaka yang membahas teknik penyembunyian (*embedding* dan *extraction*) dengan algoritma metode LSB.

(b) Tahapan operasional steganografi algoritma metode LSB, menuangkan tujuan, ruang lingkup dan batasan masalah yang akan diharapkan dalam penelitian.

(c) Perancangan program (model) dan *coding* yaitu membuat rancangan *interface* serta membuat diagram algoritma steganografi metode LSB. Pengkodean dilakukan untuk meng-implementasikan perancangan program ke dalam bahasa pemrograman Matlab (M-File).

(d) Pengujian dan Analisa Data terhadap program yang telah dibuat.

(e) Penyusunan dan pendokumentasian serta publikasi laporan hasil penelitian dan mendokumentasikan.

Tahapan Perancangan

Dalam penelitian steganografi dengan metode LSB pada media yang bersifat digital dengan format JPG dan BMP dengan ukuran piksel tertentu, diuraikan pada langkah-langkah sebagai berikut;

(a) Mempersiapkan digital dalam format JPG dan BMP (studi kasus sebagai sample logo Universitas Esa Unggul)

(b) Program aplikasi yang digunakan dalam metode pembuatan dan atau perancangan dengan aplikasi Matlab.

(c) Metode yang digunakan dalam penggunaan steganography adalah penggunaan metode LSB dalam pengamanan data (file).

(d) Memproses *image* RGB menjadi *gray* dan *binary*, dengan menggunakan aplikasi Matlab serta mempersiapkan teks pada bit tertentu yang akan disisipkan dalam proses steganografi.

(e) Menampilkan hasil proses steganografi sebelum dan sesudahnya dalam satu tampilan (Gambar 5)

(f) Menghitung dan menganalisa membahas perubahan ukuran *file* sebelum dan setelah disisipkan pesan teks serta kualitas (faktor MSE dan PSNR)

$$MSE = \frac{1}{M*N}\sum_{x-1}^{M}\sum_{y-1}^{N}\left(S_{xy} - C_{xy}\right)^2 \cdots (1)$$

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 1) : 25 - 30. Th. 2018
ISSN: 2620-620X

$$PNSR = 10 \log_{10} \frac{C_{MSE}^{2}}{MSE} \quad \text{.....(2)}$$

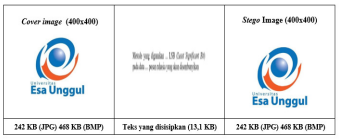
dimana ;

- C_{MSE} adalah nilai piksel terbesar.
- x dan y adalah koordinat suatu titik
- M dan N adalah dimensi dari *cover image*
- S adalah tersisipi *(stego image*)
- C adalah asli (*cover image*)

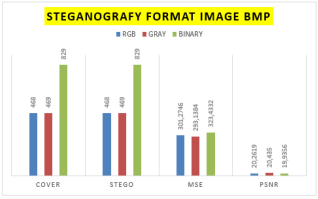
HASIL DAN PEMBAHASAN

Hasil dan luaran yang dilakukan meliputi aspek ukuran (size) - *cover* dan hasil (*stego*dan kualitas berdasarkan rumus empirik PSNR dan MSE hasil (*stego*) terhadap *cover*. Diperoleh hasil sebagai berikut ;

(a) Ukuran file tetap saat proses embedding (*cover*) dan ekstraksi (*stego*).
(b) Ukuran piksel tidak mengalami perubahan (tetap)
(c) Tidak mengalami perubahan kualitas (MSE dan PSNR)



Gambar 5 Steganografi dengan Metode Algoritma LSB



Gambar 6. Steganografi Format BMP (RGB, GRAY & BINARY)

Hasil proses steganografi dengan format BMP dan JPG dengan menggunakan Matlab ditunjukkan dalam tabel 3 & 4.

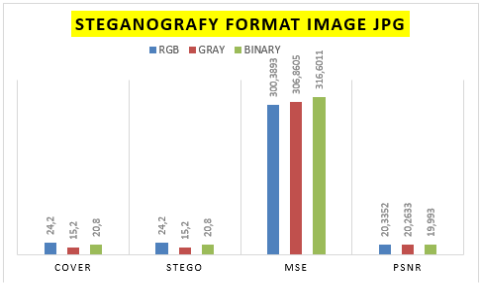
Tabel 3 Hasil Steganografi metode LSB file JPG

No.	Gambar (JPG)	Pesan (Text)	Size file (Kb)		Kualitas (dB)		Keterangan
			Cover	*Stego*	MSE	PSNR	
1	RGB Cover 400x400 (468 KB)	Metode yang digunakan ... LSB *(Least Significant Bit)* pada data .... pesan rahasia yang akan disembunyikan 13.1 KB 347 (ns) 407 (vs)	468	468	301,2746	20,2619	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
2	Gray Cover 572x 495 (469 KB)	kualitas image berdasarkan rumus empirik PSNR dan MSE steganografi 11.6 KB 46 (ns) 53 (vs)	469	469	293,1384	20,4350	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
3	Biner Cover 400x400 (829 KB)	perubahan ukuran file image sebelum dan setelah disisipkan pesan teks 11,5 KB 60 (ns) 69 (vs)	829	829	323,4332	19,9356	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)

Tabel 4 Hasil Steganografi metode LSB file BMP

No.	Gambar (JPG)	Pesan (Text)	Size file (Kb)		Kualitas (dB)		Keterangan
			Cover	*Stego*	MSE	PSNR	
1	RGB Cover 400x400 (24,2 KB)	Metode yang digunakan ... LSB *(Least Significant Bit)* pada data .... pesan rahasia yang akan disembunyikan 13.1 KB 347 (ns) 407 (vs)	24,2	24,2	300,3893	20,3352	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
2	Gray Cover 572x 495 (15.2 KB)	kualitas image berdasarkan rumus empirik PSNR dan MSE steganografi 11.6 KB 46 (ns) 53 (vs)	15.2	15.2	306,8605	20,2633	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
3	Biner Cover 400x400 (20.8 KB)	perubahan ukuran file image sebelum dan setelah disisipkan pesan teks 11,5 KB 60 (ns) 69 (vs)	20.8	20.8	316,6011	19,9930	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)

Dalam bentuk grafik, steganografi dalam format *image* BMP dan JPG dapat ditunjukkan dalam Gambar 7.



Gambar 7 Steganografi Format JPG (RGB, GRAY & BINARY)

SIMPULAN

Simpulan

Berdasarkan penelitian yang telah dilakukan, maka disimpulkan bahwa :

Jurnal Algoritma, Logika dan Komputasi
Vol.I (No. 1) : 25 - 30. Th. 2018
ISSN: 2620-620X

(a) Proses penyisipan metode LSB menggantikan hanya pada *bit* terakhir dari *cover*, dan setelah disisipkan pesan hanya mengalami sedikit penurunan kualitas yang tidak begitu berpengaruh secara signifikan bila dilihat oleh mata manusia, dan pada ukuran *size file* tidak mengalami perubahan (*cover* maupun *stego*)

(b) *Image* dengan ukuran 400x400 (RGB) dan 572x495 (Gray dan Biner) dapat menampung pesan sebanyak 480.000 (RGB) dan 566.280 (Gray dan Biner) karakter dengan metode algoritma LSB.

(c) Perubahan pada *compressing* pada format JPG mapun BMP yang dialami masih terlihat jelas, hal ini sangat berguna dalam menjaga kerahasiaan data sehingga tidak banyak orang yang menyadarinya

Saran

Untuk penelitian lebih lanjut bagi yang berminat ini dapat menggunakan format (yang lain, dengan menggunakan feature GUI Matlab agar dioperasikan dengan cara yang lebih optimal dan *automacillay* serta dibuat dalam bentuk yang ter-repository hasil proses *cover*, *stego* dan kualitas nya dalam database *back-end*.Dan saran yang lain teknik steganografi dapat pula menggunakan metode yang lain, misalnya *Algorithms and Transformation, End-Of-File, Redundant Pattern Encoding (embedded)* dan *Spread Spectrum*[2]**.**

DAFTAR PUSTAKA

[1] Champakamala .B.S, Padmini.K, Radhika .D.K, "Least Significant Bit algorithm for steganography", International Journal of Advance Computer Technology, volume 3, number 4, August 2014

[2] Katzenbeisser, Stefan and Fabien A.P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House Inc. computing library, 2000, ISBN 1-58053-035-4

[3] Stallings, William Cryptography and Network Security Principles and Practices, Fourth Editio, 2005, ISBN-10: 0-13-187316-4

[4] R. Popa, An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering,http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf, 1998

[5] Munir, Rinaldi. Diktat Kuliah IF5054 Kriptografi. Bandung: Penerbit ITB. 2006

[6] T. Morkel et.all, " An Overview Of Steganography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa

[7] Ravinder Reddy Ch and Roja Ramani, "The Process of *Encoding (embedded)* and *Decoding (extraction)* of Steganography using LSB Algorithm", IJCSET Volume 2, Issue 11, 1488-1492, November 2012.