ISSN 2355-3286

Penelitian Mengenai Metode Steganografi Least Significant Bit

Ivan Jonathan[1], Albert Yeusiawan Haryono, Kevin Leonardi
Program Studi Teknik Informatika, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara, Tangerang, Indonesia

Diterima 14 Maret 2017
Disetujui 5 Juni 2017

Abstract - In today's technological era, the concealment of sensitive information is the concern of many people. Because the information is often shared and discussed through a very commonly used communication medium. Steganography is one technique to hide a secret message into a file that has a larger size. In this paper, we will discuss the methods that can be used in steganography, especially the method of Least Significant Bit.

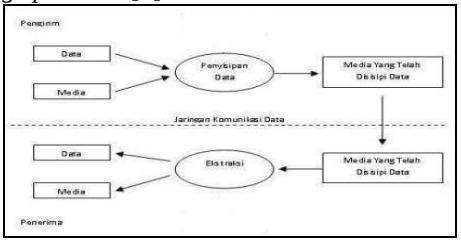
Keywords: Steganography, Data Hiding, Steganography Algorithm, Least Significant Bit.

I. PENDAHULUAN

Pada era sekarang ini, hampir semua hal dikomunikasikan menggunakan teknologi. Mulai dari percakapan sehari-hari, sampai dengan informasi yang sensitif. Maka dari itu, masalah keamanan dalam transfer data menjadi perhatian banyak orang. Sampai saat ini teknik pengamanan informasi yang dipakai adalah enkripsi dan steganografi.

Steganografi adalah seni penyembunyian informasi atau pesan rahasia pada suatu media sehingga tidak terdeteksi oleh pihak lain. Kata steganografi berasal dari bahasa Yunani yaitu *steganos* yang berarti "tersembunyi" dan *graphein* yang berarti "menulis".

Markus Kahn mendefinisikan steganografi sebagai berikut, "*Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present*".[1]



Gambar 1: Proses Steganografi [2]

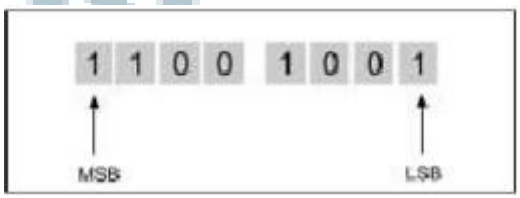
"Steganografi mempunyai dua proses utama yaitu embed/penyisipan dan ekstrak/pengungkapan seperti pada gambar 1. Proses penyisipan merupakan proses menyisipkan hidden object atau informasi/pesan yang akan disisipkan, ke dalam sebuah cover object atau media penampung, sehingga menghasilkan file baru yang telah tersisipi pesan didalamnya yang disebut dengan stego file. Sedangkan proses ekstrak merupakan proses pengembalian hidden object secara utuh setelah disisipkan ke dalam cover object." [2]

II. METODE *LEAST SIGNIFICANT BIT* (LSB)

LSB adalah algoritma sederhana yang menukar bit terkecil ke dalam beberapa byte media penyembunyiannya secara berurutan. [3]

Digital image pada komputer merupakan kumpulan dari angka-angka yang merepresentasikan *grid* dan titik-titik yang disebut *pixel.* Karena itu, digital image dapat dipakai menjadi media dalam penyembunyian pesan dengan metode LSB.

Berikut ini adalah contoh sebuah deretan angka biner dari angka decimal 201:



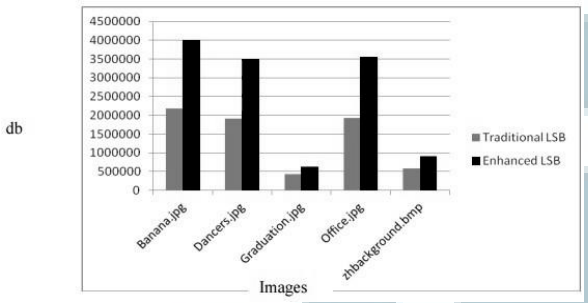
Gambar 2: Deretan Angka Biner dengan Digit LSB(https://www.academia.edu/11764630/Steganografi_ Metode_LSB)

Bit paling kanan dari sebuah deretan angka biner merupakan bit yang disebut Least Significant Bit (LSB). Apabila kita mengganti nilai bit LSB pada deret tersebut, maka akan dihasilkan deret "11001000". Deret tersebut bila dikonversikan ke dalam decimal bernilai 200. Perbedaan yang sangat kecil ini menyebabkan file media yang disisipi pesan di dalamnya tidak akan kelihatan jelas perbedaannya.

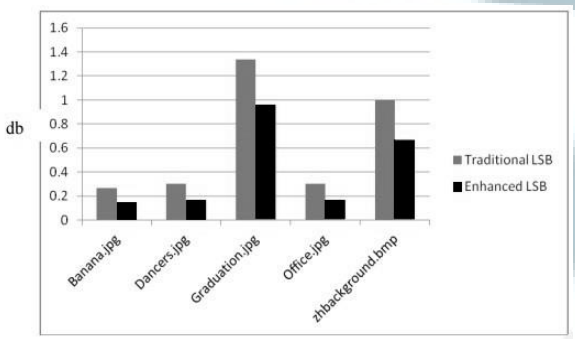
Dengan cara ini, LSB memanfaatkan fakta bahwa tingkat presisi dalam digital image jauh lebih tinggi daripada yang bisa dilihat oleh mata manusia.

III. TINJAUAN PUSTAKA

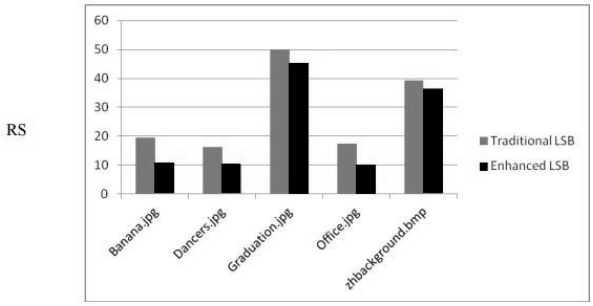
Gabriel dkk [3] mengajukan sebuah metode yang meningkatkan kualitas dari LSB. Metode tersebut menggunakan *linear congluential pseudo random number generator (LCG)* dengan sebuah *stego key* yang di-*hash* untuk memilih secara acak bit dari *cover image* yang akan ditukar dengan bit dari informasi rahasia. Hasil dari percobaan menunjukkan bahwa metode ini menghasilkan PSNR yang lebih tinggi, MSE yang lebih rendah, serta RS yang lebih rendah daripada metode LSB tradisional. Hal ini menunjukkan bahwa metode ini menghasilkan kualitas *stego image* yang lebih baik dengan penyimpangan dan noise yang lebih sedikit.



Gambar 3: Hasil PNSR (Db) Dari Percobaan Menggunakan Metode LSB Tradisional Dan *Enhanced LSB*



Gambar 4: Hasil MSE Dari Percobaan Menggunakan Metode LSB Tradisional Dan *Enhanced LSB*



Gambar 5: Hasil RS Dari Percobaan Menggunakan Metode LSB Tradisional Dan *Enhanced LSB*

Shahim dan Kattamanchi [4] mengajukan sebuah metode yang menggabungkan kriptografi dan steganografi untuk menyelesaikan masalah akses data yang tidak terotorisasi. Metode menggabungkan kriptografi dan steganografi ini diajukan karena penyembunyian data yang hanya menggunakan metode LSB masih tidak terlalu aman. Jadi, untuk menambah keamanan data digunakan kriptografi. Mula-mula pesan dienkripsi dengan menggunakan metode *transposition cipher*, kemudian pesan yang telah terenkripsi tersebut ditanamkan ke dalam sebuah digital image menggunakan metode LSB. Dengan metode ini, apabila seorang *attacker* berhasil mengekstrak data dari *stego image*, ia masih membutuhkan *decoding key* untuk mendekripsi data tersebut.

Cover image	Stego Image	Amount of data embedded	MSE %	PSNR (dB)	Amount of data extracted
clover (35 KB)	stegclover (35 KB)	4267 bytes	0.48	51.28	4267 bytes
flower (43 KB)	stegflower (43 KB)	4513 bytes	0.41	51.93	4513 bytes
bud (47 KB)	stegbud (47 KB)	5075 bytes	0.43	51.69	5075 bytes

Gambar 6: Tabel Nilai MSE Dan PSNR Dari Cover Image Dan Stego Image.

Champakamala dkk [5] mengajukan sebuah teknik baru dalam steganografi LSB yang merupakan improvisasi dari teknik *one bit LSB*. Pada teknik LSB Tradisional, kita membutuhkan 8 byte pixel untuk menyimpan 1 byte data, sedangkan pada teknik ini hanya membutuhkan 4 bytes pixel untuk menyimpan 1 byte data. Dalam teknik ini, data disisipkan pada 2 bit terakhir dari setiap pixel. Simulasi dari teknik ini dilakukan menggunakan MATLAB dengan empat langkah utama:

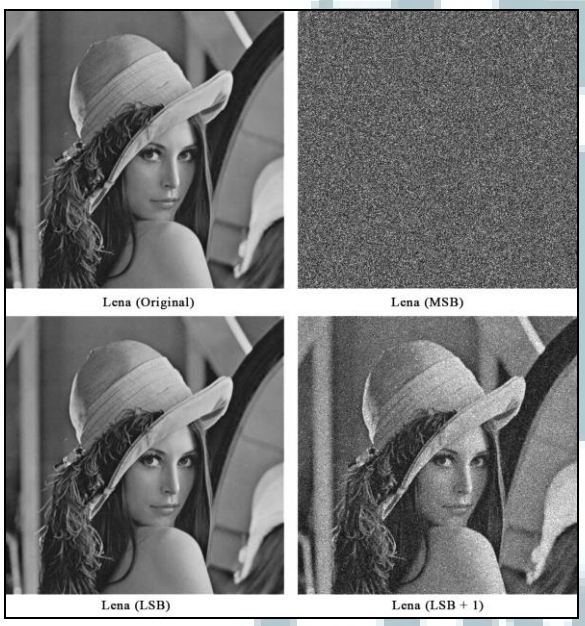
- Konversi gambar ke matrix
- Proses penyisipan data
- Konversi matrix kembalik ke gambar
- Proses ekstraksi data

Setelah melakukan beberapa percobaan, dapat dikatakan bahwa teknik ini membantu dalam menyembunyikan data rahasia ke dalam *cover image* tanpa adanya distorsi.

Gies Masita dan Tri Ismardiko [6] mengajukan penggunaan metode LSB dalam pemrograman berbasis web menggunakan bahasa pemrograman PHP. Pemanfaatan metode LSB pada PHP dapat dilakukan dengan menggunakan *Stegger*, sebuah *class library open source* berlisensi. *Stegger* menukar bit terakhir dari setiap warna primer pada pixel. Jadi dengan stegger dapat dlakukan penyimpanan 3 bit

data di setiap pixelnya. Gies dan Tri juga menambahkan enkripsi pada data rahasia sebelum data tersebut disisipkan ke dalam *cover image* agar tercipta keamanan data yang lebih baik. Untuk melakukan enkripsi pada data, digunakan fungsi secrypt pada *stegger* yaitu dengan cara mengkombinasikan antar informasi rahasia dengan sebuah key.

Yudhi Andrian [3] memaparkan perbandingan antara metode LSB, LSB+1, dan MSB. Perbedaan terdasar dari ketiga metode ini adalah letak bit yang ditukar dengan bit dari pesan rahasia. Pada LSB bit yang disisipi data adalah bit terakhir (bit ke-8), pada LSB+1 bit yang disisipi data adalah bit ke-7, sedangkan pada MSB bit yang disisipi data adalah bit ke-1. Selain memaparkan perbedaan ketiga metode ini secara teori, Yudhi juga menambahkan perbedaan ketiganya dilihat dari hasil stego image dan nilai dari PSNR-nya.



Gambar 7: Citra Lena Original Dan Setelah Disisipkan Data.

Citra	MSE	PSNR
Lena	0,479	51,327

Gambar 8: Tabel MSE Dan PSNR Pada Metode LSB.

Citra	MSE	PSNR
Lena	1,905	45,332

Gambar 9: Tabel MSE Dan PSNR Pada Metode LSB+1.

Citra	MSE	PSNR
Lena	8185,701	9

Gambar 10: Tabel MSE Dan PSNR Pada Metode MSB.

Dari hasil stego image dan nilai PSNR-nya dapat dikatakan bahwa metode LSB lebih baik dari LSB+1 dan MSB. Tetapi, berdasarkan percobaan penghancuran pesan yang dilakukan oleh Yudhi dapat dikatakan bahwa metode LSB+1 dan MSB lebih tahan terhadap penghancuran pesan.

Metode	Pesan yang disisipkan	Hasil ekstraksi pesan
LSB	"Hancur"	ÿÿÿÿÿÿÿÿ
LSB+1	"Hancur"	"Hancur"
MSB	"Hancur"	"Hancur"

Gambar 11: Tabel Pengujian Tingkat Ketahanan Pesan Terhadap Penghancuran Pesan Menggunakan Metode LSB.

IV. SIMPULAN

Pada paper ini, dipaparkan hasil penelitian tentang metode steganografi LSB yang dilakukan dengan membandingkan beberapa paper yang telah dipublikasi. Masing-masing penulis memberikan metode mereka yang berbeda dengan yang lainnya. Beberapa mencoba meningkatkan keamanan data dan yang lainnya membandingkan beberapa metode.

Dari keseluruhan referensi, ditarik kesimpulan bahwa metode LSB pada steganografi menghasilkan *stego image* yang sangat mirip dengan *image original* yang digunakan sebagai *cover image*. Hal ini terjadi karena penyisipan data dengan metode LSB hanya mengganti bit terkecil dari pixel gambar, sehingga perbedaan *original image* dan *stego image* tidak dapat diketahui oleh mata manusia. Metode LSB juga memiliki kekurangan yaitu keamanan data masih kurang terjamin. Maka dari itu, sebaiknya dalam melakukan penyembunyian data rahasia kita sebaiknya steganografi dan kriptografi untuk meningkatkan keamanan data.

DAFTAR PUSTAKA

[1] Aditi dan Sujit, "A Survey on Spread Spectrum Image Steganography Hiding Text in Digital Data", International Journal for Scientific Research & Development, Vol 3, No.5, 2015.

[2] M. Maha Andar Pasaribu, "Perancangan Program Berbasis Mobile Dengan Menggunakan Metode Pixel Value Differencing dan Algoritma Rijndael", Binus University, 2014.

[3] Gabriel, Stephen, dan Waweru, "An enhanced Least Significant Bit Steganographic Method for Information Hiding", Journal of Information Engineering and Applications, Vol 2, No.9, 2012.

[4] Shahim dan Kattamanchi, "High Capacity data hiding using LSB Steganography and Encryption", Internationa Journal of Database Management Systems, Vol 4, No.6, 2012.

[5] Champakamala, Padmini, dan Radhika, "Least Significant Bit algorithm for image steganography", International

Journal of Advanced Computer Technology, Vol 3, No.4, 2013.

[6] Gies Masita dan Tri Ismardiko, "Pengamanan Pesan Steganografi dengan metode LSB Berlapis Enkripsi dalam PHP", Universitas Budi Luhur, https://www.academia.edu/5306496/Pengamanan_Pesan_Steganografi_dengan_Metode_LSB_Berlapis_Enkripsi_dalam_PHP

[7] Yudhi Andrian, "Perbandingan Metode LSB, LSB+1, dan MSB pada Steganografi Citra Digital", STMIK Potensi Utama, https://www.academia.edu/6024132/PERBANDINGAN_METODE_LSB_LSB_1_DAN_MSB_PADA_STEGANOGRAFI_CITRA_DIGITAL.

[8] Fahrijal, “Steganografi”,
Dilihat 12 April 2016
https://www.academia.edu/6977142/Steganografi.