Penerapan Steganografi Metode Least Significant Bit (LSB) dengan Invers Matriks Pada Citra Digital

Eza Budi Perkasa[1], Lukas Tommy[2], Dwi Yuny Sylfania[3] , Lianny Wydiastuty Kusuma[4]

Abstrak— **Pada proses pertukaran informasi, biasanya informasi yang ditransimsikan akan disembunyikan dengan teknik tertentu. Sayangnya, beberapa teknik tersebut dapat mengundang kecurigaan bagi pihak yang tidak berwenang. Oleh karena itu, penelitian ini menawarkan teknik steganografi. Steganografi adalah suatu ilmu dan seni menyembunyikan data pada suatu media. Steganografi tercipta sebagai salah satu cara yang digunakan untuk mengamankan data dengan cara menyembunyikannya dalam media lain agar "tidak terlihat". Terdapat berbagai metode dalam penyisipan pesan pada steganografi. Salah satu metode yang digunakan adalah metode *Least Significant Bit*. Pada penelitian kali ini, akan dibahas mengenai metode tersebut yang digabungkan dengan pencarian invers matriks pada citra digital. Hasil akhir yang telah diperoleh adalah metode ini memiliki kelebihan dan kekurangan tertentu dibandingkan metode steganografi konvensional.**

Kata kunci-steganografi, Least Significant Bit, invers matriks, citra digital

I. PENDAHULUAN

Manusia merupakan makhluk sosial yang saling membutuhkan satu sama lain. Dalam hal berkomunikasi misalnya, tiap manusia pasti membutuhkan komunikasi dengan manusia lainnya. Seiring berkembangnya teknologi informasi saat ini manusia dapat berkomunikasi melalui berbagai media informasi digital. Contoh dengan adanya internet sebagai sistem jaringan terluas yang menghubungkan hampir seluruh komputer di dunia, membuat semua komputer dapat dengan mudah untuk saling bertukar data.

Pertukaran informasi melalui internet memiliki banyak kelebihan dibandingkan dengan media komunikasi lainnya, terutama dari segi kecepatannya. Namun informasi yang dikirimkan melalui internet tidak dapat dijamin keamanannya. Penyadapan terhadap informasi rahasia sering terjadi pada media komunikasi ini. Walaupun sebenarnya ada saluran yang aman telah tersedia, tetapi kecepatan koneksi menggunakan saluran yang aman ini biasanya cenderung lambat.

Terdapat beberapa usaha untuk menangani masalah keamanan data rahasia yang dikirimkan melalui internet. Diantaranya adalah menggunakan teknik kriptografi. Dengan teknik kriptografi, pesan asli (*plain text*) yang ingin dikirimkan diubah atau dienkripsi dengan suatu kunci (*key*) menjadi suatu informasi acak (*cipher text*) yang tidak bermakna. Kunci hanya diketahui oleh pengirim dan penerima. Kunci ini dapat digunakan untuk mengembalikan *cipher text* ke *plain text* oleh penerima sehingga orang lain yang tidak memiliki hak akses terhadap pesan tersebut tidak dapat mengetahui isi pesan sebenarnya, tetapi hanya mengetahui pesan acaknya saja. Akan tetapi, karena sifatnya yang acak, timbul suatu kecurigaan terhadap pesan yang dikirim. Untuk mengatasi hal tersebut, digunakanlah teknik lainnya yaitu teknik steganografi.

Steganografi merupakan suatu teknik yang mengizinkan para pengguna untuk menyembunyikan (*embedding*) suatu berkas atau pesan ke dalam pesan lain. Misalkan dalam suatu citra disisipkan suatu berkas atau pesan rahasia, tetapi dalam citra tersebut, berkas atau pesan rahasia tidak terlihat secara kasat mata. Sedangkan apabila diekstrak dengan suatu software khusus, maka akan terlihat bahwa terdapat berkas atau pesan rahasia dalam citra tersebut. Dibantu oleh kemajuan teknologi yang semakin canggih, hal ini dapat dengan mudah diaplikasikan. Contohnya dengan bantuan *software* seperti steghide, mp3stego, HideInsidePicture, dan lainnya. Teknik tersebut dapat digunakan juga untuk menyembunyikan informasi hak cipta seperti identitas seorang pengarang, tanggal ciptaan, dan lain-lain dengan cara menyisipkan atau menyembunyikan informasi tersebut ke dalam berbagai macam variasi jenis dokumen besar seperti teks ataupun citra.

Pada umumnya, ada tiga metode penyisipan pesan ke dalam citra yang dapat digunakan, yaitu *Least Significant Bit* (LSB) dan *Most Significant Bit* (MSB), *masking* dan *filtering*, serta *Discrete Cosine Transformation* (DCT) dan *Wavelet Compression*. Ketiga metode tersebut mempunyai kelebihan dan kekurangannya masing-masing. LSB merupakan metode yang dianggap sederhana, mudah dimengerti, dan masih digunakan sampai sekarang,

1,2,3,4Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur, Jakarta, Indonesia
1eza.pastro@gmail.com, 2lukastommy92@gmail.com, 3dysylfania@gmail.com, 4liannyw_k@yahoo.com

yaitu dengan mengganti bit rendah atau bit yang paling kanan pada data piksel yang menyusun berkas tersebut. Sebaliknya, MSB mengganti bit tinggi atau bit yang paling kiri pada data piksel tersebut. *Masking* atau *filtering* merupakan suatu metode yang mirip dengan *watermark*, yaitu suatu citra diberi tanda (*marking*) untuk menyembunyikan berkas atau pesan rahasia. Sedangkan DCT dan *wavelet compression* merupakan metode mentransformasi blok-blok piksel yang berurutan dari citra.

Pada penelitian ini, peneliti akan mengulas tentang steganografi menggunakan metode LSB yang digabungkan dengan invers matriks. Penelitian kali ini dibatasi hanya sampai pada tahap penyisipan pesan ke dalam citra, sehingga tidak terdapat teknik untuk mengekstrak pesan yang telah disisipkan. Penulis juga akan membandingkan metode LSB konvensional (selanjutnya disebut metode linear) dengan metode LSB yang digabungkan dengan invers matriks (selanjutnya disebut metode invers).

II. STEGANOGRAFI METODE *LEAST SIGNIFICANT BIT*

Steganografi berasal dari penggabungan dua kata dalam bahasa Yunani: *Steganos* yang berarti "tersembunyi" atau "terselubung" dan *graphein* yang berarti "menulis". Berdasarkan arti harfiah tersebut, maka steganografi dapat diartikan sebagai seni dan ilmu menulis atau menyembunyikan pesan rahasia dengan suatu cara. Steganografi berbeda dengan kriptografi. Kriptografi hanya menyamarkan arti dari suatu pesan tanpa menyembunyikan pesan itu sendiri.

Dalam era komputerisasi saat ini, istilah steganografi telah mencakup penyembunyian data digital dalam berkas komputer. Sebagai contoh, pengirim memulai dengan berkas gambar biasa. Langkah selanjutnya adalah mengatur warna pada setiap piksel ke-100 untuk menyesuaikan suatu huruf dalam abjad. Perubahan warna ini begitu halus sehingga tidak ada seorang pun yang mengetahui pesan tersebut jika tidak benar-benar diperhatikan.

Contoh penerapan dari steganografi metode LSB adalah penyembunyian pesan pada berkas gambar. Pesan dapat disembunyikan pada berkas tersebut dengan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada piksel yang menyusun berkas. Seperti diketahui, untuk berkas *bitmap* 24 *bit*, setiap piksel (titik) terdiri dari susunan warna merah, hijau, dan biru (RGB) yang masing-masing disusun oleh bilangan 8 *bit* (1 *byte*) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap piksel berkas *bitmap* 24 bit, dapat disisipkan 3 bit data [1].

III. INVERS MATRIKS

Invers matriks adalah sebuah matriks yang merupakan "kebalikan" dari matriks lainnya. Jika sebuah matriks dikalikan dengan inversnya, maka hasilnya adalah sebuah matriks identitas. Matriks identitas dapat dianalogikan sebagai nilai 1 pada perkalian bilangan skalar. Jika matriks yang dimaksud adalah A, maka inversnya adalah A^{-1}, dengan A^{-1} dapat dicari menggunakan persamaan:

$$A^{-1} = \frac{1}{\det(A)} \times \text{adj}(A), \quad (1)$$

dengan det(A) merupakan determinan A dan adj(A) adalah matriks adjoin dari A [2]. Sebuah matriks memiliki invers jika dan hanya jika determinannya tidak sama dengan 0.

Sebuah citra tidak selalu berbentuk persegi. Untuk citra yang berbentuk persegi panjang, maka matriks pikselnya akan berbentuk persegi panjang juga. Selama ini, telah diketahui bahwa invers hanya berlaku untuk matriks persegi. Hal ini bukan berarti matriks yang berbentuk persegi panjang tidak memiliki invers. Matriks yang berbentuk persegi panjang juga memiliki invers. Hanya saja, untuk matriks tersebut, matriks inversnya tidak unik. Terdapat berbagai metode untuk mencari matriks invers dari matriks berbentuk persegi panjang. Salah satu dari metode tersebut adalah metode kuadrat terkecil (*least square*). Apapun metode yang digunakan, ukuran dari matriks invers selalu sama dengan penukaran ukuran dari matriks itu sendiri. Misalkan jika sebuah matriks berukuran 20 × 15, maka matriks inversnya berukuran 15 × 20.

Pada citra *true color*, terdapat dimensi ketiga yang menyatakan komposisi warna yang digunakan. Sebagai contoh, citra RGB berukuran 800 × 600 sama artinya dengan citra yang memiliki ukuran 800 × 600 × 3. Hal tersebut mengakibatkan matriks yang digunakan tidak lagi menggunakan matriks 2 dimensi seperti yang telah dikenal selama ini. Sebagai solusi, digunakanlah matriks 3 dimensi untuk memetakan pikselnya. Pada matriks ini, terdapat beberapa submatriks yang menjadi elemennya. Misalnya, sebuah matriks A berukuran 2 × 4 × 2, maka matriks tersebut dapat ditulis menjadi

$$A = \left[\begin{bmatrix} a_{111} & a_{121} & a_{131} & a_{141} \\ a_{211} & a_{221} & a_{231} & a_{241} \end{bmatrix} \begin{bmatrix} a_{112} & a_{122} & a_{132} & a_{142} \\ a_{212} & a_{222} & a_{232} & a_{242} \end{bmatrix}\right].$$

Seperti terlihat, matriks A terdiri dari 2 submatriks [3]. Nilai invers dari matriks 3 dimensi sama dengan nilai invers dari tiap-tiap submatriks [4].

IV. DESAIN PENELITIAN

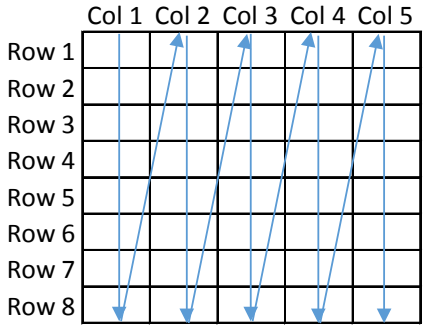
Pada steganografi metode invers, pertama-tama setiap piksel pada citra dipetakan pada sebuah matriks. Selanjutnya, matriks piksel tersebut dicari inversnya. Matriks tersebut dikalikan dengan bilangan skalar yang nilainya sama dengan jumlah elemen dari matriks invers dan dibulatkan. Hasil perkalian ini kemudian disaring agar tidak mengandung elemen bernilai kurang dari atau sama

dengan 0 dan juga elemen yang bernilai lebih dari bilangan skalar bersangkutan. Setiap elemen yang bernilai duplikat dihapus. Elemen-elemen hasil pemrosesan tersebut menunjukkan lokasi penyisipan bit dari pesan.

Penyisipan bit dilakukan dengan mengubah nilai elemen matriks semula ke dalam bentuk biner. Bit terkanan dari tiap-tiap bentuk biner yang sesuai dengan posisi yang ditunjukkan diganti dengan bit yang disisipkan. Penyisipan bit ini mengikuti aturan *column major order*. Sebagai contoh, posisi 5 pada matriks 2 × 3 berarti sama dengan baris pertama kolom ketiga. Penggantian bit ini tak akan mengubah warna citra secara signifikan. Hal tersebut dibuktikan pada Tabel I.

TABEL I. CONTOH PENERAPAN LSB

Nilai Komposisi (Biner)			Sampel	Kode Warna
R	**G**	**B**		
1111111**1**	0000000**0**	0000000**0**		#ff0000
1111111**0**	0000000**0**	0000000**0**		#fe0000
1111111**1**	0000000**1**	0000000**0**		#ff0100
1111111**1**	0000000**0**	0000000**1**		#ff0001



1111111**0**	0000000**1**	0000000**0**		#fe0100
1111111**0**	0000000**0**	0000000**1**		#fe0001
1111111**1**	0000000**1**	0000000**1**		#ff0101
1111111**0**	0000000**1**	0000000**1**		#fe0101

Gambar 1. *Column Major Order*

V. PENGUJIAN

Pada penelitian kali ini, digunakan dua citra uji, yaitu satu citra uji *grayscale* (Lenna) dan satu citra uji *true color* (UBL). Pesan yang akan disisipkan berjumlah tiga buah untuk masing-masing gambar, yaitu `123`, `admin`, dan `Budi Luhur`.

TABEL II. WAKTU PENYISIPAN PESAN (METODE INVERS)

Pesan	Waktu Penyisipan (× 10^{-5} detik)
`123`	268,75
`admin`	134,74
`Budi Luhur`	129,53

	Lenna	UBL
`123`	268,75	5323,8
`admin`	134,74	118,57
`Budi Luhur`	129,53	125,82

TABEL III. WAKTU PENYISIPAN PESAN (METODE LINEAR)

Pesan	Waktu Penyisipan (× 10^{-5} detik)	
	Lenna	**UBL**
`123`	1357,3	885,69
`admin`	11,857	4,7554
`Budi Luhur`	12,582	6,5217

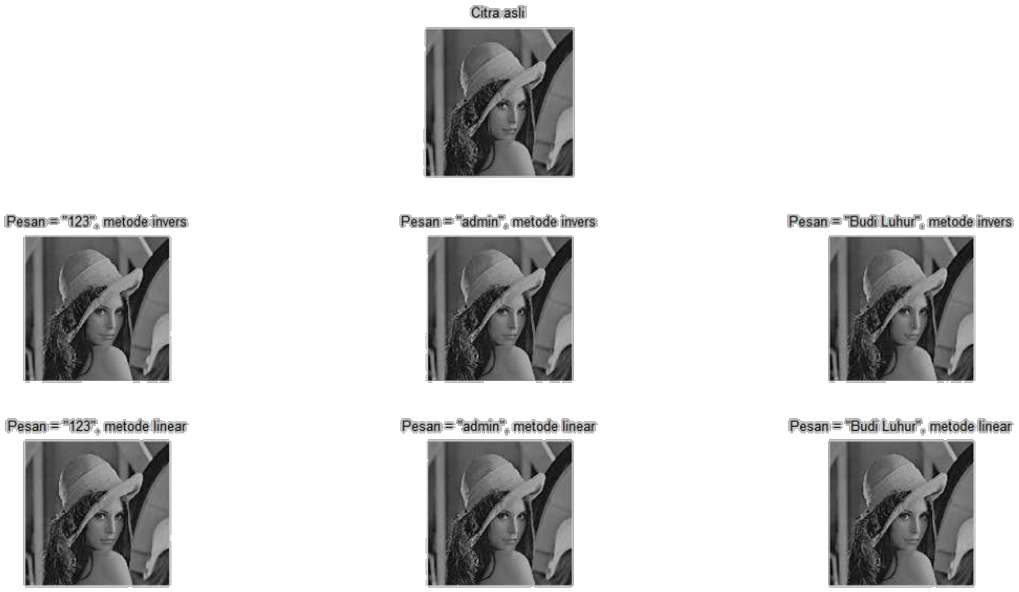
Pada kedua tabel di atas, terlihat bahwa waktu penyisipan metode linear lebih cepat dibandingkan metode invers. Hal ini disebabkan pada metode invers terdapat proses pencarian posisi penyisipan bit yang tidak ada pada metode linear.

TABEL IV. PERBANDINGAN UKURAN BERKAS CITRA

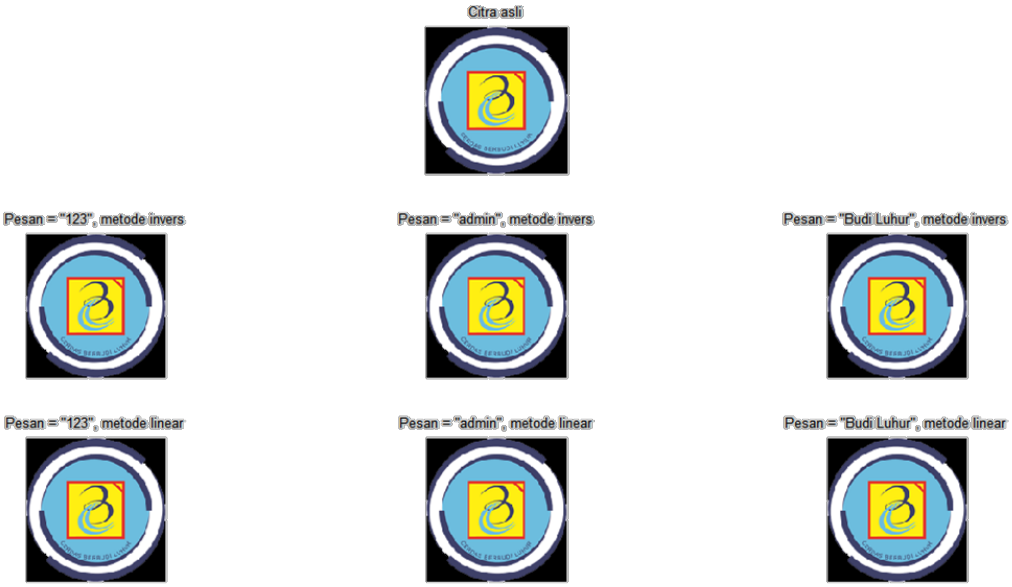
Citra	Ukuran Semula (Byte)	Pesan	Ukuran Setelah Penyisipan (Byte)	
			Invers	**Linear**
Lenna	247.548	`123`	247.552	247.554
		`admin`	247.548	247.552
		`Budi Luhur`	247.548	247.554
UBL	22.444	`123`	20.285	20.277
		`admin`	20.280	20.276
		`Budi Luhur`	20.282	20.276

Seperti terlihat pada Tabel IV, citra yang telah disisipkan pesan lebih menghemat ruang penyimpanan untuk citra *true color*. Selain itu, pesan yang disipkan dengan metode invers mengakibatkan ukuran citranya lebih kecil dibandingkan dengan metode linear.

Baik metode invers maupun linear, keduanya tidak akan mengubah piksel warna secara signifikan. Hal ini dibuktikan pada gambar-gambar berikut.



Gambar 2. Citra Lenna sebelum dan setelah penyisipan pesan



Gambar 3. Citra UBL sebelum dan setelah penyisipan pesan

VI. KESIMPULAN DAN PENELITIAN SELANJUTNYA

Dari hasil percobaan yang telah dilakukan sebelumnya, dapat disimpulkan bahwa baik metode invers dan metode linear memiliki kelebihan dan kekurangan masing-masing. Penyisipan pesan dengan metode invers membutuhkan waktu yang lebih lama dibandingkan metode linear. Selain itu, citra *grayscale* yang telah disisipkan pesan dengan metode invers memiliki ukuran yang lebih kecil dibandingkan dengan menggunakan metode linear. Sebaliknya, citra *true color* yang telah disisipkan pesan menggunakan metode linear memiliki ukuran yang lebih kecil dibandingkan metode invers. Ke depannya, akan dibahas mengenai teknik mengekstrak pesan yang telah disisipkan ke dalam citra dengan metode invers.

REFERENSI

[1] Presetya, D. A. *dkk.* 2014. "Pengertian, contoh, serta perbedaan dari Kriptografi dan Steganografi" *http://root-coder.blogspot.com/2014/09/pengertiancontohserta-perbedaan-dari.html*, diakses tanggal 23 April 2015.

[2] Supranto, J. 2001. *Statistik: Teori dan Aplikasinya (Jilid 1)*. Edisi 6. Jakarta: Erlangga.

[3] Solo, A. M. G. "Multidimensional Matrix Mathematics: Notation, Representation, and Simplification, Part 1 of 6," *Proceedings of the World Congress on Engineering 2010 Vol III* (2010), pp. 1824-1828.

[4] Solo, A. M. G. "Multidimensional Matrix Mathematics: Multidimensional Matrix Transpose, Symmetry, Antisymmetry, Determinant, and Inverse, Part 4 of 6," *Proceedings of the World Congress on Engineering 2010 Vol III* (2010), pp. 1838-1841.