PERBAIKAN ALGORITMA STEGANOGRAFI TEKNIK LEAST SIGNIFICANT BITS UNTUK APLIKASI KEAMANAN DATA

Tika Erna Putri[1*], Muhammad Rifqi Al Fauzan[2], Prima Asmara Sejati[1]

[1] *Electronics Instrumentation / Electrical Engineering and Informatics / Vocational Collage, Universitas Gadjah Mada, Indonesia*

[2] *Metrology and Instrumentation / Electrical Engineering and Informatics / Vocational Collage, Universitas Gadjah Mada, Indonesia*

[*] *E-mail: tika.erna.p@mail.ugm.ac.id*

Abstrak

Masalah keamanan telah menjadi masalah besar di bidang komunikasi data, khususnya dalam transmisi data melalui internet. Salah satu solusinya adalah menyembunyikan pesan melalui media digital sehingga perhatian penyerang atau pihak ketiga dapat dihindari. Metode keamanan ini biasanya dikenal sebagai steganografi. Dalam penelitian ini, kami menggunakan gambar sebagai media digital. Kami memodifikasi Least Significant Bit (LSB) yang merupakan teknik yang paling umum digunakan dalam steganografi. Sayangnya LSB memiliki tingkat keamanan yang buruk karena teknik ini sudah dikenal luas. Oleh karena itu, penting untuk memodifikasi algoritma LSB untuk memastikan aspek keamanannya. Perbaikan teknik LSB disarankan dengan memilih hanya piksel ganjil dan mengabaikan piksel genap dalam implementasi steganografi. Kami berhasil menerapkan algoritma LSB yang dimodifikasi dengan menggunakan gambar RBG dan citra grayscale sebagai media steganografi. Mean Squared Error (MSE) dan Peak Signal-to-noise Ratio (PSNR) digunakan untuk mengevaluasi kualitas stego-image. Perhitungan kami menunjukkan bahwa algoritma LSB yang dimodifikasi memberikan hasil yang lebih baik daripada LSB konvensional. Algoritma LSB konvensional memberikan 1.98 10-5 untuk MSE dan 95.20893 dB untuk perhitungan PSNR, sedangkan LSB yang dimodifikasi memberikan nilai masing-masing 1. 80 10-5 dan 95.6101 dB untuk MSE dan PSNR.

Kata Kunci: keamanan data, LSB, modifikasi, steganografi.

Abstract

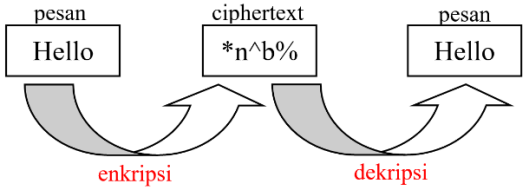
[Title: Improving The Steganography Algorithm Of Least Significant Bits Engineering For Data Security Applications] *Security issues have become major problem in the field of data communications, specifically in the data transmission through the internet. One of the solutions is to hide the messages through a digital media so the attention of the attacker or third party can be avoided, this method is known as steganography. In this research, we use images as digital media. We modify the Least Significant Bit (LSB) which is the most commonly used technique in steganography. Unfortunately LSB has poor security level since it is already widely known technique. Therefore, it is important to modify the algorithm of LSB to ensure its security aspect. An improvement to LSB technique is suggested by selecting only odd pixels and ignoring even pixels in the implementation of steganography. We successfully implement the modified LSB algorithm by using RBG image and grayscale image as steganography media. Mean Squared Error (MSE) and Peak Signal-to-noise Ratio (PSNR) are employed to evaluate the stego-image quality. Our calculations show that the modified LSB algorithm provides better results than the conventional LSB. The conventional LSB algorithm gives 1.98 10-5 for MSE and 95.20893 dB for PSNR calculations, while the modified LSB gives 1. 80 10-5 and 95.6101 dB for MSE and PSNR, respectively.*

Keywords: data security, steganography, LSB, modified.

PENDAHULUAN

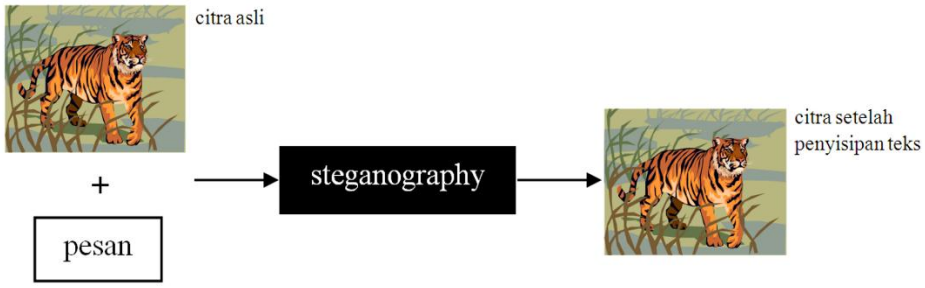
Data merupakan salah satu komoditas utama di era internet seperti sekarang. Proses komunikasi dengan bertukar data menjadi sangat mudah dilakukan dengan adanya internet melalui media online. Media tersebut dapat berupa surat elektronik, halaman blog, fasilitas chat, maupun media sosial. Di Indonesia sendiri jumlah pengguna internet bertambah secara signifikan dalam beberapa waktu terakhir. Berdasarkan data hasil polling pada tahun 2016 yang dirilis Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia mencapai 132,7 juta pengguna dengan nilai penetrasi internet 51,8 % (Asosiasi Penyelenggara Jasa Internet Indonesia, 2016). Jumlah ini merupakan yang terbesar ke-5 di seluruh dunia. Salah satu kendala paling serius dalam hal komunikasi data digital adalah faktor keamanan. Dari uraian permasalahan tersebut jelas dibutuhkan sebuah metode yang dapat menjamin keamanan dalam bertukar informasi digital.

Banyak hal yang dapat dilakukan untuk memperkuat faktor keamanan dalam komunikasi data digital. Salah satu metode yang paling populer adalah kriptografi, yaitu metode pengamanan pesan dengan mengenkripsi pesan tersebut menjadi ciphertext yang tidak dapat dibaca secara langsung. Untuk dapat membaca pesan tersebut maka pihak penerima pesan harus melakukan proses sebaliknya yaitu dekripsi terhadap pesan tersebut. Proses kriptografi diilustrasikan pada Gambar 1.



Gambar 1. Proses enkripsi dan dekripsi pada kriptografi

Hal yang menjadi kelemahan metode kriptografi adalah bahwa bentuk text hasil enkripsi pada kriptografi akan menimbulkan kecurigaan pihak ketiga bahwa informasi yang dikirimkan adalah rahasia atau penting. Kekurangan dari kriptografi tersebut tidak akan kita temui jika menggunakan metode steganografi sebagai faktor keamanan (proses steganografi diilustrasikan pada Gambar 2). Dalam implementasinya seringkali dilakukan kombinasi beberapa metode keamanan data untuk meningkatkan tingkat sekuritas suatu data (Gupta, 2012; Fadli, 2015; Pakereng, 2010; Suryani, 2008).



Gambar 2. Proses steganografi

Steganografi adalah seni menyembunyikan pesan menggunakan media tertentu seperti file citra atau file suara (Purba, 2012; David 2012). Output dari proses steganografi ini berupa media tersebut yang mirip dengan media asli sebelum disisipkan dengan sebuah pesan. Steganografi bekerja secara *bit wise*, bit pesan digunakan untuk mengubah bit terkecil (*least sinificant bits*) dari media sehingga nilai bit media akan bergeser (Frank, 2007; Fridrich, 2009). Pergeseran ini terjadi dalam rentang yang sangat sempit, sehingga perubahannya hampir tidak terasa oleh indra manusia. Media yang paling sering digunakan dalam steganografi adalah berupa citra atau gambar. Salah satu teknik steganografi yang paling banyak dipakai adalah teknik *least significant bits* (LSB) karena teknik ini sederhana untuk diimplementasikan (Gupta, 2012; Ahmed, 2011). Selain itu, teknik LSB juga unggul dalam masalah menjaga ukuran citra, karena ukuran citra sebelum dan sesudah

proses steganografi akan cenderung sama (Aditya, 2010).

METODE PENELITIAN

Dalam penelitian ini digunakan perubahan teknik LSB konvensional untuk melakukan proses steganografi. Modifikasi dilakukan dengan menambahkan aturan baru didalamnya. Penambahan aturan tersebut belum pernah dilakukan sebelumnya, maka teknik modifikasi LSB yang kami gunakan memiliki tingkat keamanan yang lebih baik dari teknik LSB konvensional. Secara umum skema proses modifikasi pada teknik LSB konvensional diilustrasikan pada Gambar 3.

karakter pesan	dec	bin							
h	104	0	1	1	0	1	0	0	0
i	105	0	1	1	0	1	0	0	1

(a)

piksel gambar	dec	bin								
1	69	0	1	0	0	0	1	0	1	← 0
2	127	0	1	1	1	1	1	1	1	
3	201	1	1	0	0	1	0	0	1	← 1
4	23	0	0	0	1	0	1	1	1	
5	92	0	1	0	1	1	1	0	0	← 1
6	9	0	0	0	0	1	0	0	1	
7	165	1	0	1	0	0	1	0	1	← 0
8	67	0	1	0	0	0	0	1	1	
...	...	...	...	...	...	...	...	...	...	
N										

(b)

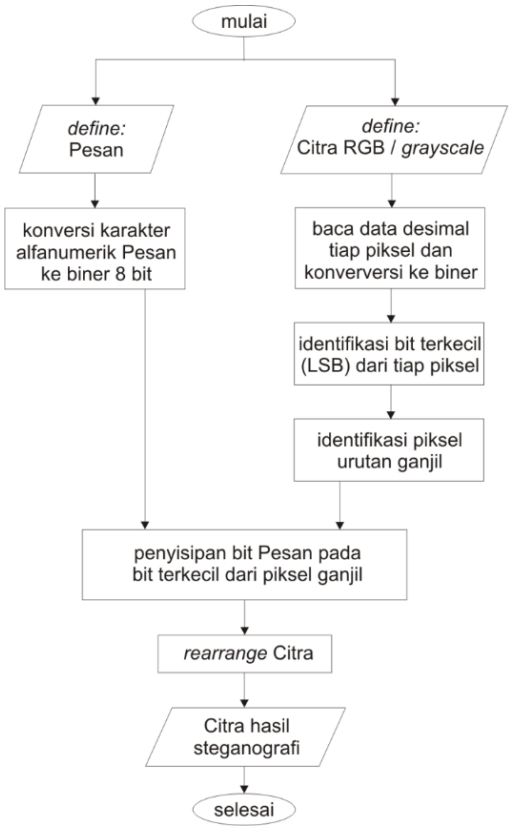
piksel gambar	dec	bin								
1	68	0	1	0	0	0	1	0	0	sisipkan
2	127	0	1	1	1	1	1	1	1	lewati
3	201	1	1	0	0	1	0	0	1	sisipkan
4	23	0	0	0	1	0	1	1	1	lewati
5	93	0	1	0	1	1	1	0	1	sisipkan
6	9	0	0	0	0	1	0	0	1	lewati
7	164	1	0	1	0	0	1	0	0	sisipkan
8	67	0	1	0	0	0	0	1	1	lewati
...	...	...	...	...	...	...	...	...	...	
N										

(c)

Gambar 3. (a) contoh data biner dari karakter pesan yang akan disisipkan (b) contoh data biner tiap piksel citra (c) cara penyisipan pada teknik LSB termodifikasi. Warna kuning, hijau, merah, dan biru digunakan untuk mempermudah pemahaman ilustrasi tersebut.

Pada teknik LSB konvensional bit pesan disisipkan ke bit terkecil tiap piksel citra secara langsung dan berurutan dari piksel pertama, kedua, ketiga, dan seterusnya. Sedangkan pada teknik LSB termodifikasi bit pesan disisipkan pada piksel dengan nomor ganjil saja, atau dengan kata lain ada satu piksel yang dilompati (*leaped*), lihat Gambar 3 (b) dan (c). Diagram alir proses penelitian steganografi dengan teknik LSB termodifikasi ini dirinci dalam Gambar 4.

Hasil akhir yang diperoleh dari diagram alir pada Gambar 4 berupa citra yang sudah mengandung informasi berupa pesan yang tersisipkan, disebut citra stego. Selanjutnya, citra stego dapat dikirimkan memelaui internet atau media lain dan pihak penerima mengekstrak informasi pada citra stego dengan membalik proses pada diagram alir Gambar 3.2. Setelah proses ekstraksi selesai akan didapatkan kembali pesan yang tersisipkan dalam citra stego.



Gambar 4. Diagram alir proses modifikasi teknik LSB pada penelitian ini

Perlu dilakukan pengujian kuantitatif kualitas citra untuk menentukan seberapa jauh citra stego berubah dari citra asli. Untuk keperluan tersebut, kami menggunakan metode *Mean Squared Error* (*MSE*) dan *Peak Signal-to-noise Ratio* (*PSNR*) (Saffor, 2001). Dengan metode-metode ini pula kami melakukan perbandingan citra stego hasil proses steganografi teknik LSB konvensional dengan teknik LSB termodifikasi. Secara matematis *MSE* dan *PSNR* dapat dituliskan seperti yang tertulis pada Persamaan 1 dan Persamaan 2 (Saffor, 2001).

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

$$PSNR = 10\log_{10}\frac{255}{MSE} \quad (2)$$

Dimana x dan y adalah koordinat piksel citra, M dan N adalah ukuran resolusi citra, S_{xy} merupakan citra stego, dan C_{xy} merupakan citra asli sebelum dikenakan proses steganografi.

HASIL DAN PEMBAHASAN

Analisis kebutuhan sistem

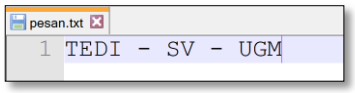
Perbaikan algoritma teknik LSB telah berhasil diimplementasikan berdasarkan skema yang sudah dijelaskan sebelumnya. Kebutuhan sistem steganografi yang dikembangkan dalam penelitian ini dapat dikelompokkan menjadi tiga jenis, yaitu kebutuhan masukan, kebutuhan proses, dan kebutuhan keluaran. Kebutuhan masukan sistem berupa sebuah file citra dan sebuah file pesan berekstensi **.txt*. Kebutuhan proses maksudnya bahwa dibutuhkan pengembangan atau perbaikan algoritma LSB konvensional dan pengimplementasiannya dalam sebuah perangkat lunak. Sedangkan kebutuhan keluaran adalah bahwa sistem harus dapat menghasilkan citra stego sesuai skema pemodifikasian algoritma teknik LSB konvensional.

Hasil pengujian

Dalam proses pengujian sistem, kebutuhan masukan yang kami gunakan berupa sebuah file citra berwarna (*RGB image*)berukuran 1855×1856 piksel sebagai media staganografi dan sebuah file pesan bertuliskan "TEDI - SV - UGM". Kedua file-file tersebut masing-masing berekstensi **bmp* dan **.txt* (lihat Gambar 5 dan Gambar 6). Kami juga melakukan perbandingan antara algoritma LSB konvensional dan algoritma LSB termodifikasi terutama dalam hal kualitas citra yang dihasilkan.

(a) (b) (c)

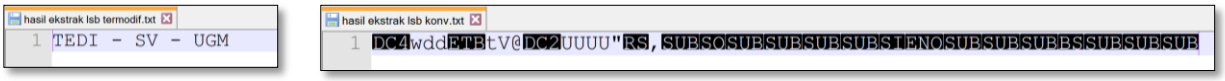
Gambar 5. File citra yang digunakan dalam pengujian (a) citra asli, (b) citra stego dari hasil proses steganografi LSB termodifikasi (c) citra stego dari hasil steganografi LSB konvensional



Gambar 6. File pesan yang digunakan dalam pengujian

Tidak tampak perbedaan yang signifikan pada Gambar 5 (a) - 5 (c), meskipun sesungguhnya ketiga citra tersebut berbeda. Citra pertama merupakan citra asli yang belum tersisipi pesan, sedangkan citra kedua dan ketiga merupakan citra yang sudah tersisipi pesan didalamnya namun dengan teknik yang berbeda. Hal ini terjadi karena algoritma LSB merubah nilai piksel hanya pada yang terkecil sehingga pergeseran skala warnanya sangat sempit, terlalu tidak signifikan bagi mata manusia untuk menyadari perbedaannya.

Proses steganografi tidak berhenti sampai penyisipan bit pesan ke dalam bit terkecil dari piksel citra, namun juga mencakup proses ekstraksi atau mendapatkan kembali pesan dari citra stego. Proses yang dilakukan merupakan invers atau kebalikan dari proses penyisipan pesan. Gambar 7 (a) menunjukkan hasil ekstraksi pesan dari citra stego LSB termodifikasi menggunakan proses ekstraksi LSB termodifikasi juga, sedangkan Gambar 7 (b) hasil yang didapatkan jika menggunakan ekstraksi teknik LSB konvensional.



(a) (b)

Gambar 7. Hasil ekstraksi pesan dari citra stego teknik LSB termodifikasi (a) menggunakan teknik ekstraksi LSB termodifikasi dan (b) menggunakan teknik ektraksi LSB konvensional

Dari Gambar 7 dapat disimpulkan mengenai dua hal, pertama bahwa teknik LSB termodifikasi berhasil diimplementasikan baik dalam proses penyisipan maupun proses ekstraksi pesan. Kedua, citra stego hasil proses LSB termodifikasi hanya dapat diekstrak oleh invers dari teknik LSB termodifikasi itu sendiri, jika dipaksakan proses ekstraksi menggunakan teknik LSB konvensional hasilnya akan berupa teks tidak bermakna seperti ditunjukkan pada Gambat 7 (b). Hal ini berarti tingkat kemanan data dengan steganografi teknik LSB termodifikasi lebih baik dari pada menggunakan LSB konvensional, karena ekstraksi teknik LSB konvensional sudah diketahui banyak orang bahkan ada beberapa *website* yang dapat melakukan ekstraksi teknik tersebut secara gratis.

Kalkulasi *MSE* dan *PSNR* dilakukan untuk menguji kualitas citra hasil proses steganografi menggunakan referensi citra asli yang belum dikenakan proses steganografi. Dilakukan perbandingan antara citra stego teknik LSB konvensional dan teknik LSB termodifikasi, hasilnya ditampilkan pada Tabel 1.

Tabel 1. Perbandingan kualitas citra stego hasil steganografi teknik LSB termodifikasi dan teknik LSB konvensional.

Teknik	*MSE*	*PSNR* (dB)
LSB termodifikasi	$1{,}80\times10^{-5}$	95,61010
LSB konvensional	$1{,}98\times10^{-5}$	95,20893

Nilai MSE menyatakan error kuadrat rata-rata antara citra asli dengan citra stego, parameter ini tidak memiliki satuan. Semakin kecil nilai MSE semakin mirip citra stego dengan citra aslinya. Data pada Tabel 1 menunjukkan nilai MSE teknik LSB termodifikasi lebih kecil dari teknik LSB konvensional, sehingga citra stego teknik LSB termodifikasi memiliki kualitas yang lebih baik. Sedangkan nilai PSNR merupakan perbandingan nilai maksimal yang mungkin dimiliki oleh suatu piksel citra dengan derau yang berpengaruh pada citra tersebut. PSNR memiliki satuan *decibel* (dB), semakin tinggi nilai PSNR menandakan semakin mirip kedua citra yang diuji yang berarti semakin bagus teknik steganografi yang digunakan. Citra hasil proses steganografi diharapkan semirip mungkin dengan citra asli. Data pada Table 1 menunjukkan teknik LSB termodifikasi memiliki nilai PSNR 0.40117 dB lebih besar dari pada teknik LSB konvensional, sehingga citra stego hasil teknik LSB termodifikasi akan lebih mirip dengan citra asli.

Selain diuji pada media citra berwarna, algoritma LSB termodifikasi juga kami uji pada citra skala abu-abu (*grayscale image*), citra hitam sepenuhnya (semua piksel gambar memiliki nilai RGB 0), dan citra putih sepenuhnya (semua piksel gambar memiliki nilai RGB 255). Hasil penelitian kami menunjukkan teknik LSB termodifikasi berhasil diimplementasikan pada semua jenis citra tersebut.

SIMPULAN DAN SARAN

Telah dilakukan perbaikan algoritma steganografi teknik LSB untuk meningkatkan tingkat kemanan dan kualitas citra hasil steganografi. Skema perbaikan dilakukan dengan hanya menggunakan piksel citra bernomor ganjil saja yang digunakan untuk menyimpan bit pesan. Skema ini berhasil diimplementasikan dan berhasil pula dilakukan ekstraksi pesan dari citra stego (citra hasil proses steganografi). Pengujian kuantitatif terhadap citra stego dilakukan menggunakan kalkulasi MSE dan PSNR untuk menentukan kualitas citra stego. Pengujian dilakukan menggunakan media berupa file citra berwarna dengan ukuran 1855×1856 piksel dan sebuah file pesan bertuliskan "TEDI - SV - UGM". Berdasarkan kalkulasi yang sudah dilakukan, teknik LSB termodifikasi memiliki nilai yang lebih baik untuk kedua parameter (MSE dan PSNR) dibandingkan teknik LSB konvensional. Teknik LSB termodifikasi menghasilkan nilai $1{,}80\times10^{-5}$ dan 95,61010 dB untuk parameter MSE dan PSNR, sedangkan teknik LSB konvensional menghasilkan nilai $1{,}98\times10^{-5}$ dan 95,20893 dB.

DAFTAR PUSTAKA

Aditya, Y., Pratama, A., dan Nurlifa, A. (2010). Studi pustaka untuk steganografi dengan beberapa metode. *Prosiding Seminar Nasional Aplikasi Teknologi Informasi 2010,* G-32 – G-35.

Ahmed, J.M. dan Ali, Z.M. (2011). Information hiding using LSB technique. *International Journal of Computer Science and Network Security*, 11, 18-25.

Asosiasi Penyelenggara Jasa Internet Indonesia. (2016) Infografis penetrasi & perilaku pengguna internet indonesia.

David, D., Murtado, A., dan Kasma, U. (2012). Steganografi pada citra bmp 24-bit menggunakan metode least significant bit. *Jurnal Sistem Informasi dan Teknik Informatika*, 2, 1.

Fadli, A., Fairuz, F., dan Dewi, N. (2015). Aplikasi kriptografi dan steganografi menggunakan algoritma caesar cipher dan least significant bit. *Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, 1

Frank, J., James, R., John, M., dan Ferguson, A. J. (2007). Unicode Steganographic Exploitsx. *IEEE Security and Privacy*, 5, 32-39.

Fridrich, J. (2009). *Steganography in digital media: principles, algorithms, and applications*. United Kingdom: Cambridge University Press, (Chapter 1).

Gupta, S., Goyal, A., dan Bhushan, B. (2012). Information hiding using least significant bit steganography and cryptography. *I. J. Modern Education and Computer Science*, 6, 27-34.

Pakereng, M.A.I., Beeh, Y.R., dan Endrawan, S. (2010). Perbandingan steganografi metode spread spectrum dan least significant bit (LSB) antara waktu proses dan ukuran file gambar. *Jurnal Informatika*, 6, 2.

Purba, J.V., Situmorang, M., dan Arisandi, D. (2012). Implementasi steganografi pesan text ke dalam file sound (.wav) dengan modifikasi jarak byte pada algoritma least significant bit (LSB). *Dunia Teknologi Informasi*, 1, 50.

Saffor, A., Ramli, A. R., Ng K.-H. (2001). A comparative study of image compression between jpeg and wavelet. *Malaysian Journal of Computer Science*, 14, 39-45.

Suryani, E. dan Martini, T.S. (2008). Kombinasi kriptografi dengan hillcipher dan steganografi dengan LSB untuk keamanan data teks. *Prosiding Seminar Nasional Teknoin 2008 Bidang Teknik Informatika*, D-47 – D-51.