DINAMIKA REKAYASA
http://dinarek.unsoed.ac.id

Vol. 14 No. 1 (2018) Hal. 47-55
p-ISSN1858-3075 | e-ISSN 2527-6131

UJI PERFORMA PENYISIPAN PESAN DENGAN METODE LSB DAN MSB PADA CITRA DIGITAL UNTUK KEAMANAN KOMUNIKASI

PERFORMANCE EVALUATION MESSAGE USING LSB AND MSB METHOD ON DIGITAL IMAGE FOR COMMUNICATION SECURITY

Cahaya Jatmoko*, L. Budi Handoko, Christy Atika Sari, De Rosal Ignatius Moses Setiadi

*Email: jatmoko74@gmail.com

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang

Abstrak— Salah satu teknik penyembunyian data yang populer adalah steganografi. Teknik ini dapat mengecoh pihak penyadap data sehingga informasi rahasia tetap aman. Steganografi dapat digunakan dengan menerapkan sejumlah algoritma dengan bantuan pemrosesan komputer. Algoritma steganografi yang sering diteliti antara lain *least significant bit* (LSB) dan *most significant bit* (MSB). LSB merupakan salah satu algoritma steganografi yang melakukan proses perhitungan bit dengan nilai paling kecil, sedangkan MSB melakukan proses yang sama namun dengan pilihan angka yang besar. LSB merupakan algoritma sederhana namun dapat digunakan pada proses steganografi, begitu pula dengan MSB. Penelitian ini membahas tentang uji performa algoritma LSB dan MSB dalam steganografi, baik dari segi kulitas hasil steganografi, dan ketahanan terhadap serangan. Alat ukur yang digunakan dalam penelitian adalah *Mean Square Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), dan *Coefficient Correlation* (CC). Berdasarkan hasil penelitian metode LSB terbukti lebih baik dari segi kulitas, sedangkan ketahanan terhadap serangan MSB lebih unggul pada jenis serangan *salt and pepper*.

Kata kunci— Steganografi, penyembunyian pesan, LSB, MSB, uji komparasi.

Abstract— One of the most popular data hiding techniques is steganography. This technique can outwit the data tapper so that the secret information remains safe. Steganography can be used by applying a number of algorithms with the help of computer processing. Steganography algorithms that are often studied include Least Significant Bit (LSB) and Most Significant Bit (MSB). LSB is one of the steganography algorithms that perform the bit calculation process with the smallest value, while the MSB perform the same process but with a large number of choices. LSB is a simple algorithm but can be used in steganography process, as well as MSB. This study discusses the performance test of LSB and MSB algorithm in steganography, both in terms of quality of steganography, and resistance to attack. The measuring instruments used in this research are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Coefficient Correlation (CC). Based on the results of research LSB method proved better in terms of quality, whereas resistance to MSB attacks superior to the type of attack salt and pepper.

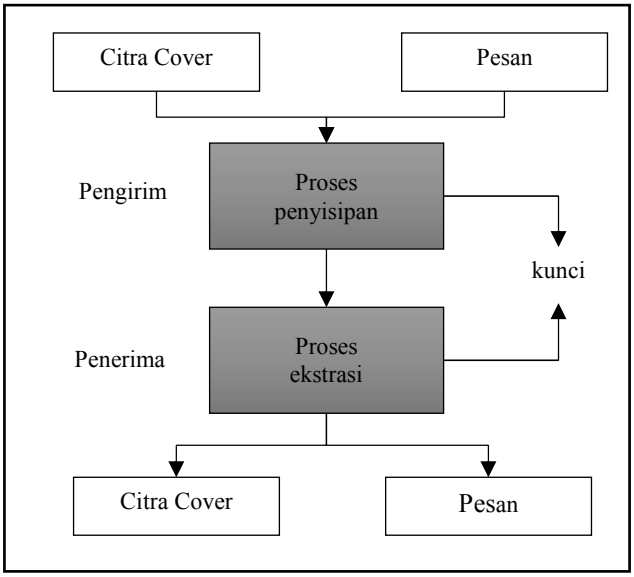
Keywords— Steganography, data hiding, LSB, MSB, comparative test.

I. PENDAHULUAN

Komunikasi rahasia dalam era komputerisasi menyebabkan berbagai masalah, misalnya penyadapan data dan perusakan data. Model komunikasi rahasia telah ada sejak zaman Yunani kuno menggunakan teknik penyandian data [1]. Menyandikan data berarti mengubah data ke dalam bentuk lain. Dengan demikian data yang diproses akan mengalami perubahan. tentu saja hal ini akan membuat penyadap data menjadi tahu bahwa data tersebut telah terproteksi.

Terdapat pula teknik lain yang dapat menghasilkan data akhir dengan tampilan yang sama dengan data asli. Teknik ini akan mengecoh pihak penyadap data sehingga informasi rahasia tetap aman. Teknik ini dikenal dengan nama steganografi [1]. Steganografi dapat digunakan dengan menerapkan sejumlah algoritma dengan bantuan

pemrosesan komputer. Algoritma steganografi yang sering diteliti antara lain *least significant bit* (LSB) dan *most significant bit* (MSB). LSB merupakan salah satu algoritma steganografi yang melakukan proses perhitungan bit dengan nilai paling kecil, sedangkan MSB melakukan proses yang sama namun dengan pilihan angka yang besar. LSB berada pada barisan bit paling kanan. LSB merupakan algoritma sederhana namun dapat digunakan pada proses steganografi [3], begitu pula dengan MSB.



Gambar-1. Perbedaan Proses LSB dan MSB.

Kedua algoritma tersebut mempunyai kelemahan dan kelebihan masing-masing sehingga dalam penelitian ini mengkaji ulang mengenai performa dari masing-masing algoritma. LSB dan MSB telah digunakan dalam teknik steganografi namun belum diketahui secara detail bagaimana performanya jika dikomparasi melalui teknik steganografi. Penelitian yang dilakukan oleh Garg pada tahun 2012 telah menggunakan LSB dan MSB dalam steganografi gambar namun hasil eksperimen dalam penelitian ini mempunyai nilai PSNR yang masih perlu dikaji ulang [2]. Sedangkan penelitian yang dilakukan oleh Khurana lebih jelas dan lebih terukur namun hasil gambar proses steganografi dalam keadaan yang rusak, hal ini ditandai dengan perubahan gambar yang sangat signifikan [3]. Penelitian lain dengan inputan pesan berupa teks telah dilakukan oleh Anand pada tahun 2014 dengan LSB dan MSB, dalam penelitian ini dijelaskan bahwa LSB mempunyai nilai PSNR yang lebih baik [4]. Penelitian lain dalam steganografi pada tahun 2017 telah dilakukan oleh Sharma dengan menggunakan MSB saja dan didapatkan nilai MSB yang baik [5]. Berdasarkan latar belakang penelitian terkait di atas maka dapat ditarik kesimpulan bahwa kedua algoritma di atas mempunyai celah untuk dianalisa khususnya dalam teknik steganografi. Maka perlu dilakukan komparasi terhadap algoritma LSB dan MSB dalam mencapai komunikasi rahasia pada media gambar.

II. TINJAUAN PUSTAKA

A. Steganografi

Steganografi adalah studi tentang penyisipan dan penyembunyian pesan dalam medium yang disebut *covertext*. Steganografi berhubungan dengan kriptografi dan hampir sama tuanya. Ini digunakan oleh orang-orang Yunani Kuno untuk menyembunyikan informasi tentang gerakan pasukan dengan menato informasi di kepala seseorang dan kemudian membiarkan orang tersebut menumbuhkan rambut mereka. Sederhananya, steganografi setua kotoran [6]. Ide dasar dibalik kriptografi adalah Anda bisa menyimpan pesan rahasia dengan mengkodekannya sehingga tidak ada yang bisa membacanya. Jika *cipher* kriptografi yang baik digunakan, kemungkinan tidak ada satu, bahkan entitas pemerintah pun, yang bisa membacanya.

Ada sejumlah besar metode steganografi yang kebanyakan dikenal, mulai dari tinta tak terlihat dan microdots hingga mengeluarkan pesan tersembunyi dalam huruf kedua dari setiap kata dari sebuah tubuh besar. komunikasi radio teks dan spektrum penyebaran. Dengan komputer dan jaringan, ada banyak cara lain untuk menyembunyikan informasi [7], seperti di bawah ini.

1. Saluran terselubung, sebagai saluran komunikasi antara "orang jahat" dan sistem yang disusupi.
2. Teks tersembunyi di dalam halaman Web.
3. Menyembunyikan file di "pemandangan biasa" (misal tempat yang lebih baik untuk "menyembunyikan" file daripada dengan nama yang terdengar penting di direktori c:\winnt\ system32?).
4. *Null ciphers* (misalnya, menggunakan huruf pertama setiap kata untuk membentuk pesan tersembunyi dalam teks yang tidak berbahaya).

Steganografi adalah seni dan praktik berkomunikasi menggunakan pesan tersembunyi, sering kali disamarkan dalam hal lain yang tidak diharapkan adanya pesan [8]. Umumnya pesan

steganografi akan terlihat biasa pada pandangan pertama: gambar seekor kucing, daftar belanjaan, sebuah artikel atau puisi, dll. Tersembunyi dalam tulisan atau objek biasa ini (dalam istilah steganografi, ** rahasia rahasia) adalah pesan tersembunyi [9]. Perbedaan utama antara steganografi dan kriptografi dan enkripsi adalah bahwa pesan tersebut tidak menarik perhatian pada diri mereka sendiri. Komunikasi steganografi sering disembunyikan di depan mata, sedangkan komunikasi terenkripsi, meski tidak terbaca, sangat jelas fakta bahwa mereka mengirim rahasia [10].

Contoh umum steganografi sering dikaitkan dengan file media digital, karena ini adalah cara terbaik untuk menyimpan pesan karena ukurannya yang besar dan sifat umum yang tidak mencolok. Misalnya, seseorang bisa mengubah setiap piksel ke-100 dalam file gambar menjadi warna yang sesuai dengan huruf alphabet [11]. Sementara gambar itu sendiri tidak akan tampak terlalu terdistorsi orang bisa dengan mudah mengambil gambar dan menemukan pesannya [12]. Steganografi bergantung pada tidak terlihat atau diperiksa bila terdeteksi ada sedikit perlindungan terhadapnya sendiri. Dengan mengkombinasikan steganografi dan kriptografi, didapat metode komunikasi yang sangat aman, pesan tersembunyi dan terenkripsi.

Penggabungan dua metode kriptografi dan steganografi dapat meningkatkan keamanan sebuah pesan, karena pesan yang akan disisipkan kedalam sebuah media gambar akan dilakukan proses enkripsi terlebih dahulu sehingga pesan yang sudah tersembunyi sudah berupa pesan acak [12]. Pada Penelitian tersebut digunakan 90 dataset yakni 30 file citra dengan format *bmp, 30 file citra dengan format *jpg, dan 30 file citra dengan format *png. Dengan masing masing format citra mempunyai resolusi 512 x 512 piksel, 256 x256 piksel, dan 128 x 128 piksel. Semua data set akan dilakukan proses enkripsi dan dekripsi menggunakan metode *one-time pad* proses *embedded* dan *Extract* menggunakan teknik least significant bit (LSB). Namun citra yang tersisipi data akan pengalami penurunan kualitas citra akan menurun sehingga perlu adanya evaluasi kualitas citra yang telah disisipi secara obyektif yakni menghitung nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) [14].

B. *Least Significant Bit* (LSB)

LSB adalah salah satu metode steganografi pada domain spasial yang melakukan penyisipan pesan dengan cara mengubah nilai bit terkecil [13]. Bit terkecil terletak pada paling katan barisan bit data. Berikut adalag sebuah contoh sebuah byte data 01011001, maka nilai bit terkecilnya (LSB) adalah bit “1”, yaitu bit yang terletak di paling kanan. Bilangan yang terdiri dari bit-bit biasanya diatandi dengan huruf "b" diakhir bilangan menjadi 01011001b. Huruf huruf b yang terletak diakhir bilangan memiliki arti biner atau bit. Nilai biner juga dapat dikonversi menjadi nilai desimal, untuk lebih jelasnya dapat melihat cara dibawah ini.

$$0*2^7+1*2^6+0*2^5+1*2^4+1*2^3+0*2^2+0*2^1+1*2^0$$

$$0+64+0+16+8+0+0+1= 89$$

Teknik Steganografi dengan memodifikasi LSB dilakukan dengan memodifikasi bit-bit LSB pada setiap *byte* piksel citra [14]. LSB piksel tersebut digantikan dengan bit informasi pesan yang ingin disembunyikan. Setelah bit-bit informasi telah tersemat semua dalam piksel citra, maka pesan rahasia berhasil disembunyikan. Untuk mengambil kembali pesan rahasia tersebut, maka bit-bit LSB dibaca kembali satu per satu kemudian disusun menjadi *byte-byte* pesan dan kembali menjadi asli yang disembunyikan [15]. Penyisipan tersebut biasanya dilakukan secara berurutan mulai dari piksel awal sampai terakhir, menyesuaikan panjang pesan yang disematkan. Pesan tersebut seharusnya tidak boleh lebih besar dari citra awal wadah penampungnya. Karena pengubahan nilai piksel hanya mengubah satu nilai lebih tinggi atau lebih rendah, maka biasanya hasil penyisipan tidak dapat dideteksi secara visual manusia. Berikut adalah contoh penggunaan metode LSB, jika terdapat pesan sebesar 5 bit = 10010, maka jumlah *byte* yang disipi juga 5, yaitu:

10110110 11001011101110011010100010101011 (*byte* yang digunakan sebagai wadah penyisipan pesan), dengan pesan **10010,** sehingga hasil penyisipan menjadi **10110111 11001010101110001010100110101010,** jadi metode LSB ini hanya menggantikan bit pertama. Yang paling utama, LSB tidak mencurigakan dimata manusia, mudah untuk diimplementasikan, dan mempunyai *high perceptual transparency*.

C. *Most Significant Bit* (MSB)

MSB merupakan kebalikan dari LSB, MSB juga disebut sebagai urutan terbesar bit (*High-Order Bit*)

[3] yang merupakan bit terbesar dalam bilangan biner. Letak bit MSB biasanya terletak dipaling kiri, akan tetapi dalam bahasa pemrograman seperti MATLAB letak ini juga dapat diatur. Misalnya pada sebuah byte 11011000, maka bit terbesarnya (MSB) adalah bit yang terletak di paling kiri yaitu "1". Hal ini sangat umum untuk menetapkan setiap posisi bit mulai dari 0 hingga N-1, dimana "N" adalah jumlah bit yang digunakan dalam biner [18]. Biasanya, ini hanya untuk pangkat bit yang sesuai.

Binary (Decimal: 149)	1	0	0	1	0	1	0	**1**
Bit weight for given bit position n (2^n)	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Bit position label	MSB	___	___	___	___	___	___	**LSB**

Gambar-2. Perbedaan Posisi Bit LSB dan MSB.

III. METODE

Metode yang digunakan dalam penelitian ini adalah menguji performa dua metode LSB dan MSB dalam steganografi citra. Penelitian ini akan mengukur kualitas citra hasil steganografi dengan LSB, dan ketahanan citra stego. Terdapat empat tahap dalam metode penelitian yang dilakukan disini, yaitu pengumpulan data, analisis dan perancangan, uji komparasi. Gambar-3 menunjukkan tahapan metode yang digunakan pada penelitian ini.

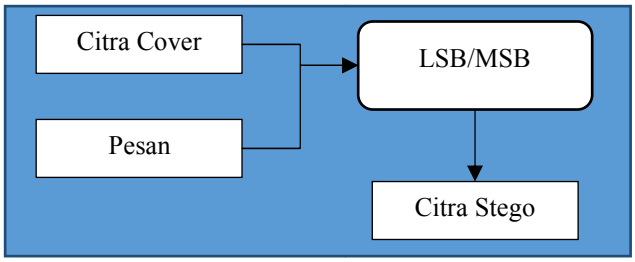
Gambar-3. Metode yang digunakan.

A. Pengumpulan Data

Terdapat dua macam sumber data yang digunakan pada penelitian ini. Yang pertama yaitu sumber data primer yang terdiri data citra standar yang digunakan dalam penelitian pengolahan citra. Jenis citra yang digunakan adalah citra keabuan dengan format *bitmap*. Untuk melakukan konversi warna citra digunakan metode rgb2gray pada MATLAB untuk mengubah citra berwarna menjadi keabuan. Berikutnya adalah data sekunder yang juga berupa citra yang diambil dari literatur dan penelitian terkait tentang metode LSB dan MSB dalam teknik steganografi.

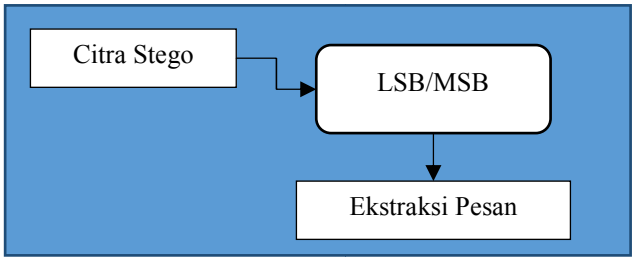
B. Analisis dan Perancangan

Berdasarkan analisis sumber data primer dan sekunder yang telah didapatkan maka dalam penelitian ini dirancang dua proses utama, yaitu proses penyisipan pesan dan proses ektraksi pesan. Gambar-4 adalah deskripsi metode LSB/MSB penyisipan pesan yang diusulkan.



Gambar-4. Metode penyisipan pesan yang diusulkan.

Gambar-5 mendeskripsikan metode ekstraksi pesan yang digunakan.



Gambar 5. Metode ekstraksi pesan yang digunakan.

Hasil perancangan metode akan diimplementasikan dengan *software* MATLAB menggunakan fungsi pengolahan citra digital.

C. Uji Komparasi

Agar komparasi dapat dilakukan secara *apple to apple*, maka pesan yang diinputkan harus sama besarnya. Pesan yang disisipkan pada penelitian ini terdiri dari beberapa ukuran dengan penyisipan yang dilakukan secara urut dari piksel pertama citra hingga piksel terakhir. Pesan berupa citra digital dengan ukuran yang lebih kecil dari citra cover. Pengujian dilakukan

D. Evaluasi Hasil dan Pengukuran

Pada penelitian ini dilakukan dua tahap pengukuran, yaitu pengukuran pada citra stego, dan pengukuran pada citra pesan hasil ekstraksi. Pada citra stego diukur dengan PSNR dan MSE. Nilai

MSE dan PSNR didapatkan dari hasil perbandingan citra cover dan citra stego. Persamaan (1) digunakan untuk menghitung MSE, sedangkan persamaan (2) untuk menghitung PSNR.

$$MSE = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \|c(m,n) - s(m,n)\|^2 \qquad (1)$$

$$PSNR_{dB} = 10\, log_{10} \left(\frac{255^2}{MSE} \right) \qquad (2)$$

Dimana:

m dan *n* merupakan ukuran citra

c adalah citra cover

s merupakan citra stego.

Sedangkan pengukuran pada hasil ekstraksi digunakan alat ukur *correlation coefficient* (CC). Nilai CC dihitung dengan membandingkan citra pesan asli dengan citra pesan hasil ekstraksi. Persamaan (3) digunakan untuk menghitung CC.

$$CC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} [p(i,j).e(i,j)]}{\sum_{i=1}^{m} \sum_{j=1}^{n} (p(i,j))^2} \qquad (3)$$

Dimana:

m dan n merupakan ukuran citra

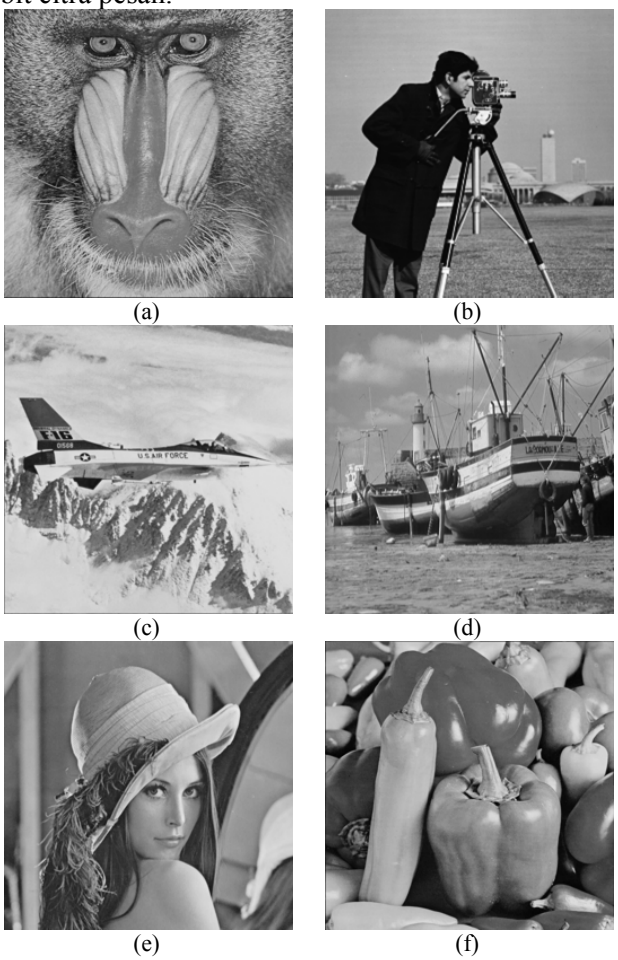
p adalah citra pesan asli

e merupakan citra pesan hasil ekstraksi.

IV. HASIL DAN PEMBAHASAN

A. Sumber Data yang Digunakan

Seperti yang telah dibahas pada bagian sebelumnya, terdapat data primer yang digunakan, yaitu citra digital standar. Citra digital terdiri dari dua macam, yaitu citra cover dan citra pesan. Citra cover menggunakan ukuran 256*256 dengan tipe *grayscale*. Sedangkan citra pesan juga menggunakan citra *grayscale* dengan ukuran 128*64. Ukuran citra pesan yang digunakan lebih kecil dari citra cover karena dalam teori steganografi pesan tidak lebih besar dari cover. Ukuran pesan ditentukan dengan ukuran tersebut karena pada penelitian ini menggunakan metode LSB dan MSB. Dimana satu piksel citra cover diisi dengan satu bit citra pesan. Jika citra cover berukuran 256*256 maka terdapat 65536 pixel citra. Dimana satu piksel citra *grayscale* mewakili satu *byte* data. Hal ini disebabkan karena rentang nilai piksel dalam citra *grayscale* dalam rentang 1 sampai 255. Sedangkan jika pesan dengan ukuran 128*64 akan memiliki 8192 *pixel/ byte*. Satu byte mewakili 8 bit, maka jika 8192 dikonversi menjadi bit akan mendapatkan nilai 65536 bit. Jika penyisipan dilakukan dengan metode LSB atau MSB maka seluruh piksel citra *cover* akan tersematkan 1 bit citra pesan.

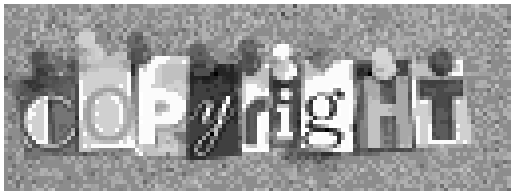


(a) (b) (c) (d) (e) (f)

Gambar-6. Citra *cover* yang digunakan dari www.petitcolas.net.

Keterangan Gambar:

(a) baboon
(b) cameraman
(c) F16
(d) fishingboat
(e) lena
(f) peppers.



Gambar-7. Citra pesan yang digunakan.

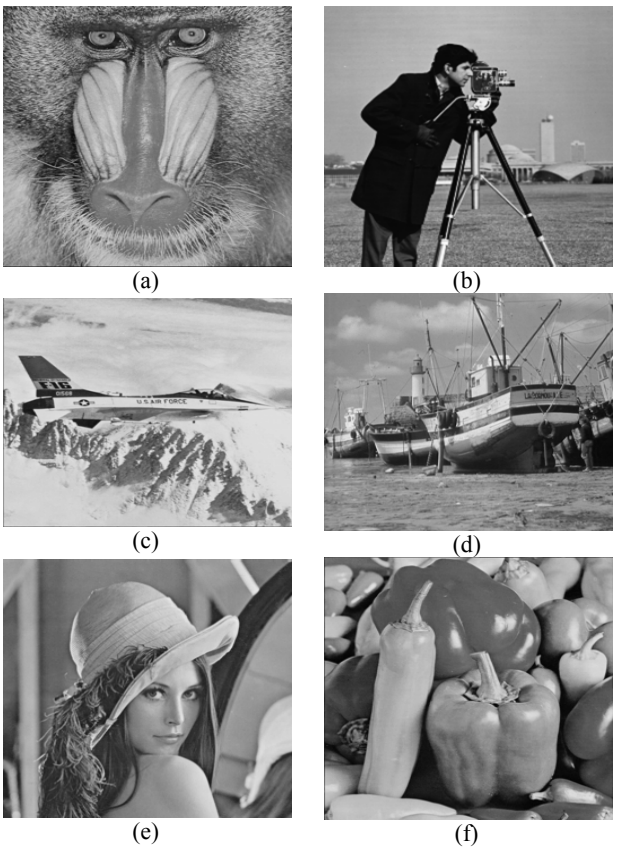
Gambar-6 menunjukan citra cover yang digunakan, sedangkan Gambar-7 menunjukkan citra pesan yang digunakan. Citra yang terdapat pada Gambar-6 merupakan citra standar yang dapat diperoleh dari *website* petitcolas [17]. Sedangkan citra pesan dibuat secara *custom*.

B. Penyisipan Pesan

Penyisipan pesan merupakan salah satu dari proses utama steganografi. Sesuai dengan judul penelitian ini, metode penyisipan digunakan metode LSB dan MSB. Selanjutnya hasil penyisipan akan diukur kualitasnya dengan MSE dan PSNR. Selain itu diuji performa komputasi yang dibutuhkan dengan fungsi tic toc pada MATLAB. Tabel-1 akan menunjukkan nilai MSE dan PSNR pada metode LSB.

Tabel-1. Nilai MSE dan PSNR penyisipan pesan dengan metode LSB.

Citra *Cover*	MSE	PSNR
Baboon	0,2520	54,1173
Cameraman	0,2492	54,1649
F16	0,2510	54,1342
Fishingboat	0,2509	54,1366
Lena	0,2518	54,1200
Peppers	0,2510	54,1342

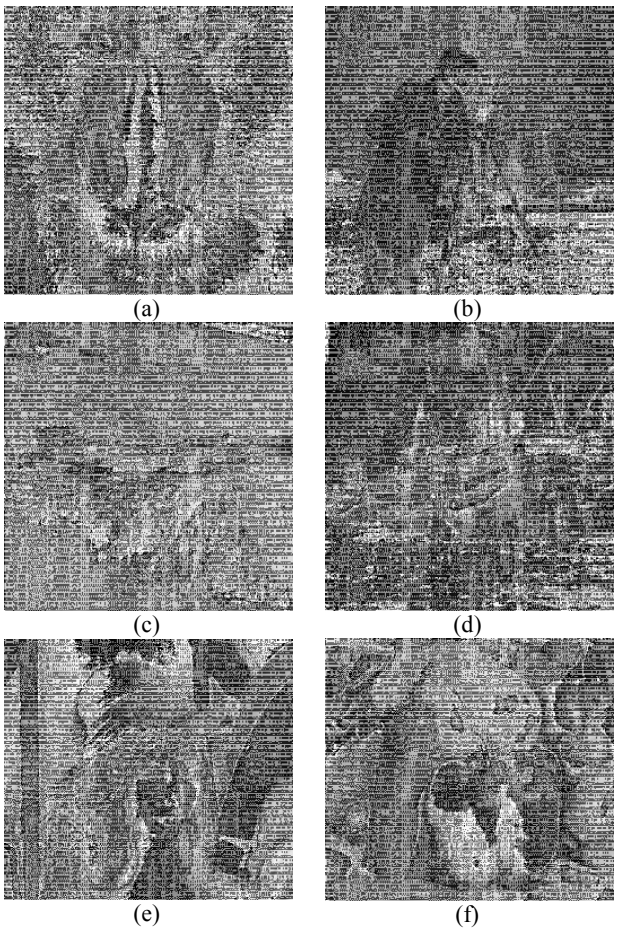


(a) (b) (c) (d) (e) (f)

Gambar-8. Citra *stego* hasil penyisipan dengan metode LSB

Keterangan Gambar:
(a) *baboon* (d) *fishingboat*
(b) *cameraman* (e) Lena
(c) F16 (f) *peppers*

Dari Tabel-1, nampak bahwa nilai MSE dan PSNR relatif sangat baik, dan seharusnya citra stego akan tampak sama dengan citra asli jika dilihat dengan mata telanjang. Jika Gambar-8 diamati memang citra stego (citra *cover* setelah disisipkan pesan) benar-benar terlihat sangat mirip dengan citra asli dan tidak nampak adanya perbedaan yang dapat dideteksi mata manusia.



(a) (b) (c) (d) (e) (f)

Gambar-9. Citra stego hasil penyisipan dengan metode MSB.

Keterangan Gambar:
(a) *baboon* (d) *fishingboat*
(b) *cameraman* (e) Lena
(c) F16 (f) *peppers*

Tabel-2. Nilai MSE dan PSNR penyisipan pesan dengan metode MSB.

Citra Cover	MSE	PSNR
Baboon	59.3921	30.3935
Cameraman	52.0420	30.9673
F16	23.1475	34.4858
Fishingboat	40.5169	32.0544
Lena	62.0963	30.2001
Peppers	66.9951	29.8704

Selanjutnya diterapkan pada metode MSB. Tabel-2 menunjukan hasil PSNR dan MSE hasil penyisipan dengan metode MSB, sedangkan Gambar-9 menampilkan citra hasil penyisipan pesan menggunakan metode MSB.

Berdasarkan Tabel-2 tampak bahwa nilai MSE sangat besar. Hal ini sangat kontras dengan metode LSB yang hanya memiliki nilai MSE tidak lebih dari 0.3. Sedangkan nilai MSE terkecil dari metode MSB sekitar 23 pada citra F16. PSNR terbaik yang didapatkan metode ini juga tidak lebih dari 35dB. Hal ini membuktikan bahwa kualitas *imperceptibility* LSB jauh lebih baik dibandingkan dengan MSB. Gambar-9 menunjukkan hasil citra stego metode MSB.

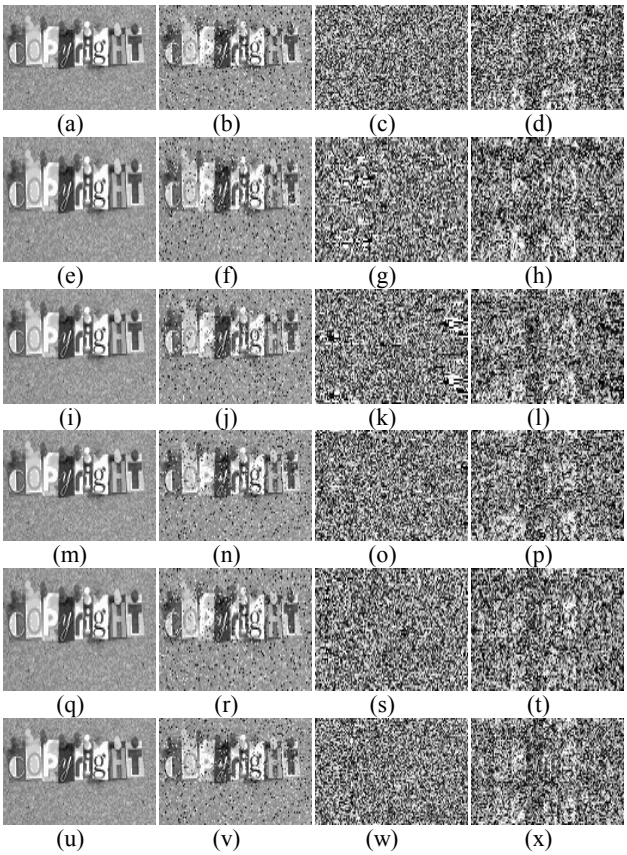
C. Ekstraksi Pesan

Metode steganografi yang baik, seharusnya dapat mengekstraksi pesan dengan sempurna. Karena jika pesan tidak dapat diekstraksi dengan sempurna maka pesan yang disampaikan dapat memiliki arti yang berbeda. Tabel-3 di bawah ini menunjukkan nilai CC yang dihasilkan metode LSB.

Tabel-3. Nilai CC hasil ekstraksi pesan-pesan dengan metode LSB

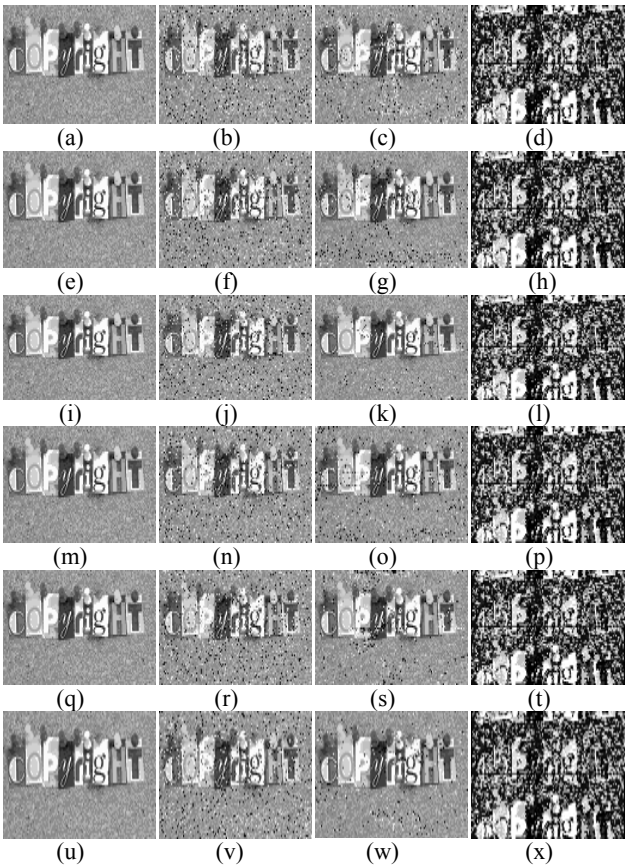
Citra *Cover*	Tanpa Serangan	*Salt and Pepper*	JPEG	Blur
Baboon	1	0,7688	0,0031	0,1610
Cameraman	1	0,7782	0,0128	0,1750
F16	1	0,7523	0,0158	0,1824
Fishingboat	1	0,7742	0,0129	0,1678
Lena	1	0,7688	0,0050	0,2115
Peppers	1	0,7742	0,0040	0,2269

Pada Tabel-3 nampak bahwa citra stego metode LSB dapat diekstraksi dengan sempurna jika citra stego tidak mengalami serangan atau manipulasi ataupun ganguan dalam proses pengiriman citra. Dalam penelitian ini juga diujikan tiga macam serangan yaitu *salt and pepper*, pengaburan atau *blur* dan kompresi JPEG. Berdasarkan Gambar-10 dan Tabel-3, tampak bahwa metode LSB sangat lemah terhadap berbagai serangan. Pesan hanya mampu bertahan pada serangan *salt and pepper*.



Gambar-10. Citra pesan hasil ekstraksi dengan metode LSB.

Keterangan Gambar:
(a) ekstraksi dari citra *baboon* tanpa serangan
(b) ekstraksi dari citra *baboon* dengan serangan salt and pepper
(c) ekstraksi dari citra *baboon* dengan serangan JPEG
(d) ekstraksi dari citra *baboon* dengan serangan blur
(e) ekstraksi dari citra *cameraman* tanpa serangan
(f) ekstraksi dari citra *cameraman* dengan serangan *salt and pepper*
(g) ekstraksi dari citra *cameraman* dengan serangan JPEG
(h) ekstraksi dari citra *cameraman* dengan serangan *blur*
(i) ekstraksi dari citra F16 tanpa serangan
(j) ekstraksi dari citra F16 dengan serangan *salt and pepper*
(k) ekstraksi dari citra F16 dengan serangan JPEG
(l) ekstraksi dari citra F16 dengan serangan *blur*
(m) ekstraksi dari citra *fishingboat* tanpa serangan
(n) ekstraksi dari citra *fishingboat* dengan serangan *salt and pepper*
(o) ekstraksi dari citra *fishingboat* dengan serangan JPEG
(p) ekstraksi dari citra *fishingboat* dengan serangan *blur*
(q) ekstraksi dari citra Lena tanpa serangan
(r) ekstraksi dari citra Lena dengan serangan *salt and pepper*
(s) ekstraksi dari citra Lena dengan serangan JPEG
(t) ekstraksi dari citra Lena dengan serangan blur
(u) ekstraksi dari citra *peppers* tanpa serangan
(v) ekstraksi dari citra *peppers* dengan serangan salt and pepper
(w) ekstraksi dari citra *peppers* dengan serangan JPEG
(x) ekstraksi dari citra *peppers* dengan serangan blur.



Gambar-11. Citra pesan hasil ekstraksi dengan metode LSB.

Keterangan Gambar:
(a) ekstraksi dari citra *baboon* tanpa serangan
(b) ekstraksi dari citra *baboon* dengan serangan salt and pepper
(c) ekstraksi dari citra *baboon* dengan serangan JPEG
(d) ekstraksi dari citra *baboon* dengan serangan blur
(e) ekstraksi dari citra *cameraman* tanpa serangan
(f) ekstraksi dari citra *cameraman* dengan serangan *salt and pepper*
(g) ekstraksi dari citra *cameraman* dengan serangan JPEG
(h) ekstraksi dari citra *cameraman* dengan serangan *blur*
(I) ekstraksi dari citra F16 tanpa serangan
(j) ekstraksi dari citra F16 dengan serangan *salt and pepper*
(k) ekstraksi dari citra F16 dengan serangan JPEG
(l) ekstraksi dari citra F16 dengan serangan blur
(m) ekstraksi dari citra *fishingboat* tanpa serangan
(n) ekstraksi dari citra *fishingboat* dengan serangan *salt and pepper*
(o) ekstraksi dari citra *fishingboat* dengan serangan JPEG
(p) ekstraksi dari citra *fishingboat* dengan serangan *blur*
(q) ekstraksi dari citra Lena tanpa serangan
(r) ekstraksi dari citra Lena dengan serangan *salt and pepper*
(s) ekstraksi dari citra Lena dengan serangan JPEG
(t) ekstraksi dari citra Lena dengan serangan *blur*
(u) ekstraksi dari citra *peppers* tanpa serangan
(v) ekstraksi dari citra *peppers* dengan serangan *salt and pepper*
(w) ekstraksi dari citra *peppers* dengan serangan JPEG
(x) ekstraksi dari citra *peppers* dengan serangan *blur*.

Tabel-4. Nilai CC hasil ektraksi pesan dengan metode MSB.

Citra *Cover*	Tanpa Serangan	*Salt and Pepper*	JPEG	Blur
Baboon	1	0,7626	0,8262	0,3649
Cameraman	1	0,7505	0,8495	0,3649
F16	1	0,7689	0,9437	0,3649
Fishingboat	1	0,7747	0,8595	0,3649
Lena	1	0,7651	0,8655	0,3649
Peppers	1	0,7664	0,9109	0,3649

Tabel-4 merupakan nilai CC dari hasil ekstraksi pesan pada metode MSB. Berdasarkan Tabel-4 dan Gambar-11, tampak bahwa metode MSB memiliki keunggulan dalam ketahanan serangan, yaitu serangan *salt and peper* dan kompresi JPEG. Sedangkan pada serangan *blur* hasil ekstraksi metode MSB tampak rusak. Hanya saja, nilai CC mendapatkan nilai yang sama begitu juga hasil ekstraksi pada gambar 11 (d), (h), (l), (p), (t), (x), jika diamati hasil ekstraksi juga tampak sama.

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil uji komparasi dapat disimpulkan bahwa metode LSB memiliki keunggulan pada kualitas citra stego. Terbukti bahwa nilai PSNR yang mencapai lebih dari 54dB, nilai PSNR juga cukup stabil karena semua nilai PSNR pada metode LSB mendapatkan nilai dengan selisih yang sangat tipis atau tidak lebih dari 1 dB. Metode LSB juga cukup tahan terhadap serangan *salt and pepper*. Sedangkan metode MSB menghasilkan citra stego yang buruk bahkan nampak rusak, tetapi lebih tahan terhadap serangan *salt and pepper* dan kompresi JPEG. Kedua metode ini lemah terhadap serangan *blur* dibuktikan dengan nilai NC dan citra hasil ekstraksi yang rusak.

B. Saran

Metode LSB meruapakan metode yang dapat menghasilkan kualitas citra stego yang baik. Hanya saja metode ini cukup sederhana dan mudah ditebak. Maka metode ini perlu dikembangkan lagi atau digabungkan dengan metode lain untuk meningkatkan keamanan pesan.

DAFTAR PUSTAKA

[1] Setiadi DRIM, Rachmawanto EH, Sari CA. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. *Journal of Applied Intelligent System*. 2017; 2(1): 1-11.

[2] Garg R, Gulati T. Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images. *International Journal of Engineering Research & Technology*. 2012;.1(8),: 1-6.

[3] Khurana A, Mehta BM. Comparison of LSB and MSB based Image Steganography. *International Journal of Computer Science And Technology*. 2012; 3(3); 870-871.

[4] Anand K, Sharma R. Data Security using LSB & MSB Image Steganography. *International Journal of Electrical & Electronics Engineering*. 2014; 1(6): 10-13.

[5] Sharma PK, Rajni. Analysis of Image Watermarking using Least Significant Bit Aalgoritm. *International Journal of Information Sciences and Techniques*. 2012; 2(4): 95-101.

[6] Negrat K, Smko R, Almarimi A. *Variable Length Encoding in Multiple Frequency Domain Steganography*. International Conference on Software Technology and Engineering (ICSTE), San Juan, 2010.

[7] Skopin DE, El-Emary IMM, Rasras RJ, Diab RS. *Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal*. International Conference on Advanced Computer Control (ICACC), Shenyang, 2010.

[8] Binny A, Koilakuntla M. *Hiding Secret Information using LSB Based Audio Steganography*. International Conference on Soft Computing and Machine Intelligence (ISCMI), New Delhi, 2014.

[9] Watters P, Martin F, Stripf HS. Visual Detection of LSB-encoded Natural Image Steganography. *ACM Transactions on Applied Perception (TAP)*. 2008; 5(1).

[10] Baker EJ. Steganograhy in Images by Using Intersecting Planes. *Iraq Academic Scientific Journals*. 2011; 29(1): 1265-1275.

[11] Al-Afandy KA, Faragallah OS, Elmhalawy A, El-Rabaie ESM, El-Banby GM. *High Security Data Hiding using Image Cropping and LSB Least Significant Bit Steganography*. IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, 2016.

[12] Beguma M, Venkataramani Y. LSB Based Audio Steganography Based On Text Compression. *Procedia Engineering*. 2012 30: 703-710.

[13] Rakhmat B, Fairuzabadi M. Steganografi menggunakan Metodw Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4. *Dinamika Informatika*. 2010; V(2): 1-17.

[14] Male GM, Setijadi E, "Analisa KUalitas Citra pada Stegnografi untuk Aplikasi Egoverment," dalam Seminar Nasional Manajemen Teknologi XV, 2012, 2012.

[15] Verma R, Tiwari A. Copyright Protection for Watermark Image using LSB Algorithm in Colored Image. *Advance in Electronic and Electric Engineering*. 2014; 4 (5): 499-506.

[16] Wirayuda TAB, Adiwijaya dan Permana FP. *Medical Image Watermarking with Tamper Detection and Recovery using Reversible Watermarking with LSB Modification and Run Length Encoding (RLE) Compression*. IEEE International Conference on Communication, Networks and Satellite (ComNetSat), Bali, 2012.

[17] Kerek BE, Baba HE, Hassan ME, Hassan BE. *A New Technique to Multiplex Stereo Images: LSB Watermarking and Hamming Code*. International Conference on Artificial Intelligence, Modelling and Simulation (AIMS), Kinabalu, 2013.

[18] Akinola SO, Olatidoye AA. On the Image Quality and Encoding Times of LSB, MSB and Combined LSB-MSB Steganography Algorithms Using Digital. *International Journal of Computer Science & Information Technology (IJCSIT)*. 2015;. 7(4): 79-91.

[19] Petitcolas F. The Image Downgrading Problem. 2017. [Online]. Available: http://www.petitcolas.net/steganography/image_downgrading/. [Diakses 21 January 2018].