STEGANOGRAFI BERDASARKAN METODE *LEAST SIGNIFICANT BIT* (LSB) PADA CITRA DIGITAL DENGA TEKNIK KOMPRESI *LOSSLESS*

[1)]I Gede Wiryawan,[2)] Sariyasa, [3)]I Gede Aris Gunadi

[1,2,3)]Program Studi Ilmu Komputer, Program Pascasarjana
Universitas Pendidikan Ganesha, Singaraja, Indonesia

e-mail: igdw@windowslive.com, sariyasa@undiksha.ac.id, igagunadi@gmail.com

Abstrak

Banyak media digital yang dapat digunakan sebagai *cover-object* dalam steganografi. Contohnya citra digital yang dapat dibedakan berdasarkan teknik kompresinya, yaitu *lossy* dan *lossless*. Teknik kompresi *lossless* terdapat beberapa algoritma di dalamnya, antara lain algoritma *Run Length Encoding* pada format file *Bitmap Picture*, algoritma *Lempel-Ziv-Welch* pada *Graphic Interchange Format*, dan algoritma LZW yang dikombinasikan dengan algoritma *Huffman Encoding* dalam format file *Portable Network Graphics*. Teknik kompresi *lossless* ini lebih cocok diimplementasikan pada metode steganografi dalam domain spasial, dengan keunggulan pada kapasitas penampungan. Dalam penelitian ini citra digital dengan tiga format file tersebut digunakan pada metode steganografi dalam domain spasial, yaitu *Least Significant Bit*. Dengan tujuan untuk mengetahui perbandingan diantara ketiganya, dengan melakukan pengujian perubahan kualitas dan karakteristik yang terjadi. Hasil yang diperoleh, citra digital dengan format file BMP dan PNG memiliki nilai yang identik setelah dilakukannya pengujian perubahan kualitas (*Image Quality Assessment*) dan perubahan karakteristik. Hasil dari pengujian tersebut nilai MSE sebesar $2{,}686 \times 10^{-6}$ dan nilai PSNR sebesar $103{,}89$ dB. Kemudian perubahan nilai-nilai karakteristik yang diperoleh dari pengujian karakteristik sangat kecil, yaitu perubahan nilai *Mean*, *Standard Deviation* dan *Entropy* hanya sebesar $4{,}5798 \times 10^{-5}$, $1{,}3304 \times 10^{-5}$, dan $7{,}1328 \times 10^{-4}$. Untuk ke depannya, dapat dikombinasikan antara metode-metode steganografi dengan dua domain yang berbeda dan untuk mendapatkan tingkat keamanan yang lebih baik dapat dikombinasikan steganografi dengan kriptografi.

Kata kunci: steganografi, *bitmap picture, portable network graphics*

Abstract

A lot of digital media could be used as a cover-object in steganography. For example digital images that could be subdivided based on compression techniques, lossy and lossless. Lossless compression techniques contain several algorithms, such as the Run Length Encoding algorithm in Bitmap Picture file format, Lempel-Ziv-Welch algorithm in Graphic Interchange Format, and algorithms LZW combined with Huffman Encoding algorithm in Portable Network Graphics file format. Lossless compression technique is more suitable to be implemented in steganographic methods in spatial domains, with an advantage on payload capacity. In this study, three file format of digital image applied to steganography method in spatial domain, Least Significant Bit. The goal is to know the comparison between them, by testing the quality and characteristics changes that occur. The results obtained, digital images with BMP and PNG file formats have identical values after the testing of quality changes with Image Quality Assessment and changes in digital image characteristics. The results of these tests include the MSE value is $2{,}686 \times 10^{-6}$ *and the value of PSNR is* $103{,}89$ *dB. Then the change of characteristic values obtained from the testing of characteristics is very small, i.e. changes in Mean, Std. Deviation and Entropy values are* $4{,}5798 \times 10^{-5}$, $1{,}3304 \times 10^{-5}$, *and* $7{,}1328 \times 10^{-4}$. *For the future, it is expected to be combined between steganographic methods with two different domains and to obtain a better level of security can be combined with cryptographic steganography.*

Keywords : steganography, *bitmap picture, portable network graphics*

I. PENDAHULUAN

Keamanan informasi yang ingin disampaikan adalah merupakan hal penting dalam komunikasi di era digital saat ini. Pada awalnya kriptografi sebagai suatu teknik untuk menjaga keamanan informasi. Namun kekurangan kriptografi yang mengubah (*encrypt*) informasi yang disampaikan dapat menimbulkan kecurigaan dan kemudian membuat mereka yang mengetahui pentingnya informasi tersebut untuk melakukan serangan-serangan guna mengetahui isi dari informasi yang sebenarnya.

Guna mengatasi kekurangan kriptografi tersebut ialah dengan menggunakan steganografi. Kata steganografi berasal dari bahasa Yunani, terdiri atas dua kata yaitu stegos dan grafia yang apabila digabungkan berarti tulisan yang tertutup (*covered writting*). Secara umum steganografi adalah seni dan ilmu komunikasi yang tidak terlihat (Morkel, 2005). Sedangkan menurut Munir, R. (2004), steganografi adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui.

Seperti kriptografi yang terdiri atas *plain-text* dan *chipper-text*, steganografi juga terdiri dari beberapa objek, antara lain *secret-data*, *cover-object*, dan *stego-object*. Metode *Least Significant Bit* (LSB) merupakan salah satu metode steganografi yang paling umum dan sederhana dalam implementasinya. Hanya dengan memanfaatkan bit terakhir yang paling tidak berpengaruh dalam menyusun warna-warna di setiap *pixel*-nya untuk kemudian diganti dengan bit-bit dari *secret-data* yang akan disembunyikan. Sebenarnya *Least Significant Bit* adalah bit yang paling tidak berarti dari 8-bit yang ada, tetapi bit tersebut merupakan objek penting dalam metode steganografi ini.

Berdasarkan *cover-object* yang digunakan sebagai media penampung dari *secret-data*, citra digital merupakan media yang paling sering digunakan karena ukurannya yang relatif kecil dibandingkan media lainnya seperti audio dan video. Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek (Sutoyo, 2009). Menurut Munir, R. (2004), secara harafiah citra adalah gambar pada bidang dwimatra (dua dimensi). Kemudian ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dua dimensi. Citra digital berdasarkan teknik kompresinya dapat dibedakan menjadi 2 (dua) macam teknik kompresi, yaitu *lossless* dan *lossy compression*. Dari kedua teknik kompresi tersebut, teknik kompresi *lossless* adalah merupakan teknik kompresi yang cocok apabila diimplementasikan sebagai *cover-object* pada metode *Least Significant Bit* (Morkel, 2005).

Hal ini dikarenakan teknik kompresi memproses data asli menjadi bentuk yang lebih ringkas tanpa menghilangkan informasi penting di dalamnya, sedangkan teknik kompresi *lossy* adalah teknik memampatkan data yang lebih ringkas dengan melalui proses aproksimasi dari data asli dengan tingkat kesalahan (*error*) yang masih dapat diterima (Hernawati, 2013). Teknik kompresi *lossy* juga dapat menghasilkan ukuran yang lebih kecil, namun ada kemungkinan informasi yang tersebunyi di dalamnya hilang karena banyak informasi dari citra yang akan dihapus (Dunbar, 2002). Sedangkan teknik kompresi *lossless*, menghasilkan citra digital asli tetap apa adanya tanpa adanya kemungkinan hilangnya informasi, meskipun tidak menghasilkan citra digital dengan ukuran yang kecil (Johnson, 1998)

Dalam teknik kompresi *lossless* terdapat beberapa algoritma, diantaranya algoritma *Run Length Encoding* (RLE), *Adaptive Dictionary Based* (*Lempel-Ziv-Welch* disingkat LZW), dan Entropy Encoding (*Huffman Encoding* dan *Arithmetic Encoding*). Jika algoritma *Run Length Encoding* (RLE) yang diimplementasikan maka akan dihasilkan citra digital dengan format file *Bitmap Picture* (BMP), kemudian algoritma *Adaptive Dictionary Based* (*Lempel-Ziv-Welch* disingkat LZW) akan menghasilkan citra digital dengan format file *Graphic Interchange Format* (GIF), dan yang terbaru algoritma *Adaptive Dictionary Based* (*Lempel-Ziv-Welch* disingkat LZW) dikombinasikan dengan algoritma *Huffman Encoding* akan dihasilkan citra digital dengan format file *Portable Network Graphics* (PNG).

Berdasarkan uraian sebelumnya, dalam penelitian ini akan diimplementasikan steganografi dengan metode *Least Significant*

Bit (LSB) pada ketiga format file citra digital tersebut. Dengan tujuan untuk mengetahui perubahan kualitas dan karakteristik dari citra digital sebagai *cover-object* dan *stego-object*. Kemudian dapat diketahui keunggulan dan kelemahan dari ketiga citra digital tersebut.

II. TINJAUAN PUSTAKA

Penelitian oleh T. Morkel, J.H.P. Eloff dan M.S. Oliver (2005) dilakukan evaluasi berbagai macam metode dalam steganografi dengan kriteria-kriteria, yaitu *Invisibility*, *Payload Capacity*, *Robustness*, *Independent of file format*, dan *Unsuspicious*. Hasil penelitian ini menunjukkan masing-masing metode steganografi memiliki keunggulan dan kelemahannya masing-masing, tidak ada metode steganografi yang ideal atau sempurna. Contohnya saja metode *Least Significant Bit* (LSB) pada format file BMP memiliki keunggulan pada *payload capacity* dibandingkan dengan metode steganografi lainnya, tetapi untuk kriteria lainnya sangat rendah.

Penelitian berikutnya dilakukan oleh Reddy, V. Lokeswara (2011). Penelitian ini membandingkan metode *Least Significant Bit* (LSB) dengan berbagai format file, yaitu format file BMP, GIF, dan PNG. Evaluasi dalam penelitian ini adalah *Evaluation of Image Quality*, yaitu *Mean-Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). Hasil evaluasi yang ditunjukan hanyalah hasil evaluasi dari metode *Least Significant Bit* (LSB) pada format file BMP, selain itu dalam hasil penelitian ini menunjukan format file yang digunakan adalah format file 8-bit. Hasil dari pembandingan dalam penelitian ini menunjukan metode *Least Significant Bit* (LSB) dengan format file BMP memiliki keunggulan pada *payload capacity* namun kelemahannya terdapat pada *Independent of file format*.

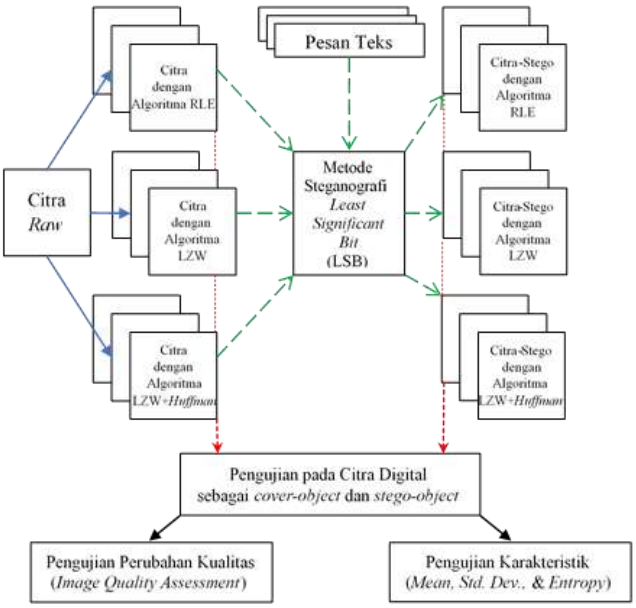
Kemudian penelitian oleh Bharat Sinha (2015) yang melakukan komparasi antara dua format file citra digital dengan teknik kompresi yang berbeda, yaitu format file PNG dengan teknik kompresi *lossless* dan format file JPG dengan teknik kompresi *lossy*. Namun metode steganografi yang digunakan tetap sama, yaitu *Least Significant Bit* (LSB). Hasilnya format file PNG hanya kalah pada kriteria *robustness against statistical attack*. Kesimpulan yang didapat dari penelitian ini adalah metode *Least Significant Bit* (LSB) tidak efektif jika diimplementasikan pada format file JPG. Sedangkan untuk format file PNG dapat diaplikasikan pada metode steganografi tersebut dengan simpel tanpa adanya kehilangan data dalam kompresinya.

III. METODE PENELITIAN

Sebelum dilakukannya penelitian ini, terlebih dahulu dilakukan studi literatur dan dapat diketahui bahwa steganografi di dalam *spatial domain*, khususnya metode *Least Significant Bit* (LSB), lebih cocok digunakan untuk citra digital dengan teknik kompresi *lossless*. Hal ini dikarenakan setelah melakukan teknik kompresi tersebut, hanya sedikit informasi dari citra asli yang hilang.

Kemudian data yang perlukan dalam penelitian ini adalah berupa citra digital yang tidak tekompresi (*uncompressed*), atau yang lebih dikenal dengan format *raw* (mentah). Lebih spesifiknya, format *raw* (mentah) adalah format file *Canon Raw version 2*, dapat disingkat CR2. Format file tersebut bersumber dari www.image-resource.com diambil dengan kamera Canon EOS-1D X. Untuk *secret-data* yang digunakan adalah berupa file teks.

Rancangan penelitian ini dapat diilustrasikan seperti Gambar 1. Awalnya penelitian ini dimulai dari data citra digital dengan format *raw*, untuk kemudian dikompresi dengan tiga teknik kompresi *lossless* sehingga dihasilkan tiga format file yang berbeda yaitu *Bitmap Picture* (BMP), *Graphic Interchange Format* (GIF), dan *Portable Network Graphics* (PNG). Guna menambah variasi dari citra digital yang digunakan, ketiga format file tersebut akan dibagi lagi menjadi lima ukuran resolusi yang berbeda.



Gambar 1. Ilustrasi Rancangan Penelitian

Setelah didapatkan tiga puluh citra digital, langkah selanjutnya adalah mengimplementasikan metode *Least Significant Bit* (LSB). Dengan pesan teks sebagai secret-data dan ukurannya disesuaikan dengan *payload capacity* dari setiap citra digital yang dapat dihitung secara matematis dengan Persamaan 1.

$$Cap = \frac{N \times M}{n} \times 3 \quad (1)$$

Dalam implementasinya akan dihasilkan *stego-object* dengan format file yang sama seperti format file citra digital sebagai *cover-object*.

Pengujian yang dilakukan antara lain pengujian karakteristik citra digital sebagai *cover-object* serta *stego-object* dan pengujian perubahan kualitas yang terjadi pada citra digital. Karakteristik tersebut dalam pengolahan citra digital dapat dianalisis berdasarkan bentuk, ukuran, geometri, tekstur, dan warna. Untuk metode steganografi dalam *spatial domain* seperti metode Least Significant Bit (LSB), karakteristik citra digital dianalisis berdasarkan teksturnya yang didalamnya terdapat beberapa parameter yang harus dihitung nilainya. Umumnya parameter-parameter tersebut adalah *entropy*, *mean*, dan *standard deviation*.

Menghitung nilai *mean* dan *standard deviation* merupakan suatu cara dalam mengukur besaran kuantitatif dari ciri setiap *pixel* pada analisis karakteristik citra digital dengan menggunakan pendekatan statistik. *Mean* sendiri adalah ukuran rata-rata dari intensitas citra digital, sedangkan *standard deviation* adalah ukuran rata-rata kontras citra digital. Untuk menghitung nilai mean dan standard deviation dapat menggunakan persamaan 2 dan 3.

$$\mu = \frac{1}{N}\sum_{i=0}^{N-1} x_i \quad (2)$$

$$\sigma = \sqrt[2]{\frac{1}{N}\sum_{i=0}^{N-1}(x_i - \mu)^2} \quad (3)$$

Kemudian menghitung nilai *entropy* adalah merupakan suatu cara dalam mengukur keacakan. Nilai *entropy* menunjukan ketidakteraturan distribusi intensitas suatu citra digital. Dan untuk menghitung nilai *entropy* dari suatu citra digital dapat digunakan persamaan 4.

$$H = -\sum_i \sum_j p(i,j) \log(p(i,j)) \quad (4)$$

Pengujian berikutnya adalah pengujian perubahan kualias. Pengukuran perubahan atau degradasi dari sebuah citra digital dapat dilakukan dengan *Image Quality Assessment*. Dalam mengukur kualitas dari citra digital dapat didasarkan pada beberapa teknik pengukuran, antara lain *pixel difference* (perbedaan pixel), *correlation* (korelasi), *edge* (tepi), *spectral*, *context* dan *Human Visual System* (Avcibas, 2002). Metode steganografi pada *spatial domain* digunakan teknik pengukuran *pixel difference* yaitu dengan menghitung nilai *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR) dari citra digital sebagai *cover-object* dan *stego-object*. Nilai MSE dan PSNR dapat dihitung dengan menggunakan persamaan-persamaan 5 dan 6 (Yusra, 2012).

$$MSE = \frac{1}{NM}\sum_{m=0}^{M-1} \sum_{n=0}^{N-1} e(m,n)^2 \quad (5)$$

$$PSNR = 10 \log_{10} \frac{s^2}{MSE} \quad (6)$$

M dan N adalah ukuran resolusi (lebar dan tinggi) dari citra yang dinyatakan dalam satuan *pixel*. Sedangkan s adalah nilai maksimum yang memungkinkan dari citra

digital. Misalnya jika citra digital 8-bit, maka kemungkinan nilai s adalah 255.

IV . HASIL DAN PEMBAHASAN

4.1 Payload Capacity

Sebelum implementasi, terlebih dahulu dihitung *payload capacity* dari masing-masing citra digital menggunakan Persamaan 1. *Payload capacity* dari beberapa citra digital dapat dilihat pada Tabel 1.

Tabel 1. Payload Capacity dari Citra Digital

Format File	Resolusi	Cap. (*byte*)
BMP (*large*)	2609 x 1741	1.703.351
GIF (*real*)	5218 x 3482	2.271.135
PNG (*large*)	2609 x 1741	1.703.351

4.2 Pengujian

Image Quality Assessment dilakukan dengan tujuan untuk mengetahui perubahan kualitas yang terjadi pada citra digital sebagai *cover-object* dan *stego*-object. Adapun nilai *Mean Squared Error* (MSE dan *Peak Signal-to-Noise Ratio* (PSNR) yang diperoleh menggunakan persamaan 4 dan 5 untuk beberapa citra digital dapat dilihat pada Tabel 2.

Tabel 2. Hasil Pengujian Perubahan Kualitas (*Image Quality Assessment*)

Format	MSE	PSNR
BMP	0.0000025769	104.053870451
GIF	0.2745848496	53.778033596
PNG	0.0000025769	104.053870451

Selanjutnya pengujian perubahan karakteristik yang dilakukan terhadap semua citra digital baik sebagai *cover-object* dan *stego-object*. Dengan menggunakan persamaan 1, 2 dan 3 didapatkan nilai-nilai *Mean*, *Standard Deviation* dan *Entropy* seperti yang ditunjukan dalam Tabel 3.

Tabel 3. Hasil Pengujian Karakteristik

Format	Mean	Std. Dev.	Entropy
Cover-BMP	0.282309	0.169030	7.241651
Stego-BMP	0.282265	0.169032	7.242336
Cover-GIF	0.371107	0.249622	6.366160
Stego-GIF	0.370917	0.249619	6.952170
Cover-PNG	0.282309	0.169030	7.241651
Stego-PNG	0.282265	0.169032	7.242336

Pengujian terakhir adalah pengujian pada *secret-data*. *Secret-data* yang disembunyikan pada *cover-object* tentunya harus sama dengan *secret-data* yang diperoleh dari *stego-object*. Pengujian ini diperoleh dengan cara membandingkan ukuran dari kedua *secret-data* tersebut. Tabel 4 berikut ini menunjukan hasil dari dari pengujian pada *secret-data*.

Tabel 4. Hasil Pengujian pada Secret-data

Format	Ukuran *Secret-data* Awal (KB)	Ukuran *Secret-data* Akhir (KB)
BMP	1.664	1.664
GIF	2.218	2.218
PNG	1.664	1.664

Analisis

Secara keseluruhan berdasarkan hasil pengujian yang telah dilakukan, citra digital dengan format file BMP dan PNG ternyata memiliki hasil pengujian yang identik. Ini dikarenakan penyusun warna pada setiap *pixel* dari kedua format file tersebut juga sama, yaitu *Red Green Blue* (RGB), dengan kedalaman bit sebesar 24-bit. Untuk citra digital dengan format file GIF terjadi perubahan karakteristik yang paling tinggi. Tabel 5 menunjukan tingginya perubahan karakteristik pada citra digital dengan format file GIF.

Tabel 5. Perubahan Karakteristik

Format	Mean	Std. Dev.	Entropy
BMP	0.000044	0.000002	0.000685
GIF	0.000190	0.000003	0.586010
PNG	0.000044	0.000002	0.000685

Perubahan yang terjadi pada citra digital dengan format file GIF juga dapat terlihat secara langsung dengan penglihatan manusia biasa, seperti yang ditunjukan Gambar 2 dan 3.

Gambar 2. Citra Digital dengan Format File GIF sebagai *Cover-object*

Gambar 3. Citra Digital dengan Format File GIF sebagai *Stego-object*

Kotak di pojok kiri bawah pada kedua gambar di atas merupakan hasil pembesaran area di dalam citra digital yang terlihat sekali perbedaannya.

Pada pengujian Image Quality Assessment juga dihasilkan nilai MSE dan PSNR yang tidak berlawanan dengan hasil pengujian karakteristik dan penglihatan secara langsung. Nila MSE yang diperoleh pada citra digital dengan format file BMP dan PNG hanya sebesar $2{,}5769 \times 10^{-6}$ yang berarti kesalahan (*error*) sangat kecil sekali (mendekati nol), sedangkan citra digital dengan format file GIF memiliki nilai MSE yang lebih besar, yaitu $0{,}2746$. Begitu juga untuk nilai PSNR yang diperoleh, nilai PSNR pada citra digital dengan format file GIF hanya $53{,}778$ sedangkan nilai PSNR pada citra digital BMP dan PNG sebesar $104{,}054$.

4.3 Pembahasan

Identiknya hasil pengujian antara citra digital dengan format file BMP dan PNG dikarenakan miripnya kedalaman bit dan warna penyusun setiap pixel pada kedua citra digital tersebut, yaitu 24-bit dan *Red Green Blue* (RBG). Namun citra digital dengan format file PNG masih memiliki *ratio* kompresi yang jauh lebih baik dibandingkan dengan citra digital dengan format file BMP, lebih kecilnya ukuran citra digital dengan format file PNG ini dapat mempermudah proses pengiriman *cover-object*. Sedangkan citra digital dengan format file GIF masih jauh tertinggal dibandingkan kedua citra digital sebelumnya dan yang paling tidak dapat diterima adalah perubahan antara *cover-object* dan *stego-object* yang terjadi pada citra digital tersebut.

V. PENUTUP

Berdasarkan hasil analisis yang dilakukan dalam penelitian, dapat disimpulkan hal-hal sebagai berikut:

1. Citra digital dengan format file BMP dan PNG apabila diimplementasikan pada steganografi dengan metode *Least Significant Bit* (LSB) memiliki hasil pengujian yang sama, ini dikarenakan identiknya kedalaman bit dan warna penyusun setiap pixel pada kedua citra digital tersebut, yaitu 24-bit dan *Red Green Blue* (RBG). Sedangkan untuk citra digital dengan format file GIF, hasil pengujian yang didapatkan jauh lebih buruk dibandingkan dengan kedua citra digital lainnya.
2. Dalam pengujian karakteristik, perubahan karakteristik pada citra digital dengan format file GIF sebagai *cover-object* dan *stego-object* sangat besar, hal ini diperkuat dengan pembandingan dengan menggunakan peng-lihatan manusia biasa. Begitu pula nilai MSE dan PSNR dalam pengujian *Image Quality Assessment* pada citra digital dengan format file GIF jauh lebih buruk dibandingkan dengan dua citra digital lainnya.
3. Pada dasarnya steganografi dengan metode *Least Significant Bit* (LSB) memiliki keunggulan pada *payload*

capacity (kapasitas) namun lemah dalam hal ketahanan (*robustness*). Keunggulan ini diperlihatkan kembali dengan menggunakan *cover-object* berupa citra digital dengan format file BMP dan PNG. Untuk citra digital dengan format file GIF, karena hanya dapat menggunakan kedalaman bit sebesar 8-bit jadi *payload capacity* (kapasitas) dengan format file ini tidak setinggi dengan format file yang lain.

Berikut ini saran untuk penelitian ke depannya.

1. Menggabungkan steganografi dengan domain yang berbeda (*spatial* dan *frequency* atau *transform domain*) dapat diimplementasikan dengan tujuan saling menutupi kelemahan masing-masing domain.
2. Untuk lebih meningkatkan keamanan informasi dalam steganografi. Pada *secret-data* dapat diimplementasikan kriptografi terlebih dahulu. Sehingga walaupun steganografi berhasil dipatahkan, masih ada pengamanan lain berupa kriptografi.

DAFTAR PUSTAKA

Avcıbaş, İ., Sankur, B., & Sayood, K. 2002. Statistical Evaluation of Image Quality Measures. *Journal of Electronic Imaging*.

Dunbar, B. 2002. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment. *SANS Institute*.

Hermawati, F. A. 2013. *Pengolahan Citra Digital.* Yogyakarta: Penerbit Andi.

Johnson, N. F., & Jajodia, S. 1998. Exploring Steganography - Seeing the Unseen. *Computer Journal*.

Morkel, T., Eloff, J., & Olivier, M. 2005. An Overview of Image Steganography. *Proc. of the Fifth Annual Information Security South Africa Conference* .

Munir, R. 2004. *Pengolahan Citra Digital.* Bandung: Informatika.

Reddy, V. L., Subramanyam, A., & Reddy, P. C. 2011. Implementation of LSB Steganography and its Evaluation for Various File Formats. *International Journal Advanced Networking and Applications*.

Sinha, B. 2015. Comparison of PNG & JPEG Format for LSB Steganography . *International Journal of Science and Research*.

Sutoyo, T. 2009. *Teori Pengolahan Citra Digital.* Yogyakarta: Penerbit Andi.

Yusra, A. S. 2012. Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI . *International Journal of Scientific & Engineering Research*.