KOMPARASI *IMPERCEPTIBILITY* STEGANOGRAFI CITRA PADA METODE LSB DAN MSB

Cahaya Jatmoko[1], Lekso Budi Handoko[2], De Rosal Ignatius Moses Setiadi[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: [1]cahayajatmoko@dsn.dinus.ac.id, [2]handoko@dsn.dinus.ac.id, [3]moses@dsn.dinus.ac.id

ABSTRAK

Steganografi sangat penting dilakukan untuk mengamankan komunikasi data. Teknik steganografi biasanya digunakan pada jenis algoritma operasi bit tunggal misalnya Least Significant Bit (LSB) dan Most Significant Bit (MSB). Kedua metode tersebut merupakan metode dengan jenis operasi setipe sehingga dapat dikomparasi. Keunggulan LSB yaitu mudah diterapkan dan memiliki komputasi cepat sedangkan MSB dapat digunakan sebagai algoritma optimisasi perolehan payload yang lebih besar dibanding hanya menggunakan LSB saja. Dalam makalah ini, media citra digital dipilih sebagai media penelitian, dalam hal ini cover object berukuran 256x256 piksel dan kunci berupa teks sederhana. Pengujian eksperimen untuk mengetahui perolehan imperceptibility dengan menghitung nilai Structural Similarity Index Measurement (SSIM) dan Peak Signal to Noise Ratio (PSNR). Dengan menggunakan Matlab, komparasi metode di analisa dan telah menghasilkan nilai SSIM mendekati 1, sedangkan perubahan intensitas piksel yang terjadi diilustrasikan melalui perbandingan histogram citra asli dan citra hasil steganografi. berdasarkan hasil yang didapat, diperoleh kesimpulan bahwa LSB lebih impercept dibanding MSB.

Kata Kunci: steganografi, citra, SSIM, PSNR, LSB-MSB

1. PENDAHULUAN

Beberapa teknik kamuflase digunakan untuk proteksi data khususnya gambar digital. Kamuflase gambar dengan menggunakan *tool* seperti photoshop tidak dapat digunakan untuk menyisipkan data rahasia lain misalnya teks atau gambar lain ke dalam media awal. Steganografi adalah studi tentang penyisipan dan penyembunyian pesan dalam medium yang disebut covertext (Ge, Huang, & Wang, 2011). Steganografi berhubungan dengan kriptografi (Sari & Rachmawanto, 2016) dan hampir sama tuanya. Metode ini digunakan oleh orang-orang Yunani Kuno dalam berperang dan menyembunyikan rahasia (Negrat, Smko, & Almarimi, 2010). Perbedaan utama antara steganografi dan kriptografi dengan proses 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 (Baker, 2011). Contoh umum steganografi sering dikaitkan dengan file media digital, karena hal ini merupakan terbaik untuk menyimpan pesan karena ukurannya yang besar dan bersifat umum yang tidak mencolok. Misalnya, seseorang bisa mengubah setiap piksel ke-100 dalam file gambar menjadi warna yang sesuai dengan huruf alphabet (Al-Afandy, Faragallah, Elmhalawy, El-Rabaie, & El-Banby, 2016). Sementara gambar itu sendiri tidak akan tampak terlalu terdistorsi sehingga orang lain dapat dengan mudah mengambil gambar dan menemukan pesannya.

Penggunaan steganografi beragam seperti penggunaan komunikasi itu sendiri. Tentunya ini dapat digunakan untuk mengirim pesan rahasia (Rachmawanto, Amin, Setiadi, & Sari, 2017) ke teman, kolega, atau co-konspirator, atau untuk mengubah data sensitif dari titik A ke titik B sehingga transfer data tidak diketahui. Seperti yang ditunjukkan oleh situs web ini, bisa juga digunakan di topologi jaringan. Ini sangat berguna untuk komunikasi terselubung botnet dan sistem lainnya di bawah kendali peretas. Ini juga bisa digunakan untuk lebih jauh mengaburkan originasi dan endpoint data karena beberapa paket prosedural hanya sangat umum, dan sering diabaikan. Ini bisa memakan waktu berjam-jam analis malware yang terlatih sampai berminggu-minggu untuk menemukan kapan dan bagaimana sebuah sistem dikompromikan dari sebuah paket dump. Program steganografi jaringan yang dirancang dengan baik mungkin dapat bertahan dalam ujian waktu yang lebih lama.

Penelitian ini mempunyai tujuan utama untuk mengembangkan algoritma dalam topik steganografi untuk komunikasi rahasia yang diterapkan dengan menggunakan algoritma *Least Significant Bit* (LSB) dan *Most Significant Bit* (MSB), sehingga orang lain tidak mengetahui bahwa data yang digunakan telah dimanipulasi. Komparasi hasil LSB dan MSB akan dievaluasi menggunakan alat ukur seperti *Peak Signal to Noise Ratio* (PSNR), *Structural Similarity Index Measurement* (SSIM), dan histogram citra.

2. METODE PENELITIAN

2.1 Least Significant Bit (LSB)

LSB merupakan pemrosesan stream cipher yang sangat cepat dan mudah untuk diterapkan (Irawan, Setiadi, Sari, & Rachmawanto, 2017). LSB juga fleksibel sehingga dapat dikombinasi dengan teknik proteksi data lainnya seperti kriptografi dan *watermarking* (Bhattt, Ray, Ghoshttt, & Raytttt, 2015) khususnya pada media citra. Dalam makalah ini, telah diterapkan model *embedding* dengan LSB sebagai berikut:

```
i,j,k]=size(C);
```

```
W=C;
m=imread('c.bmp');
mm=size(m,1);
nm=size(m,2);
message=reshape(m,mm*nm,1);
bim = de2bi(m,8);
l=1;x=1;
for(z=1:8192)
    bimr(l:l+7)=bim(x,1:8);
    l=l+8;x=x+1;
end
x=1;y=1;l=1;
for(z=1:65536)
    bi=de2bi(C(x,y),8);
    if(bimr(l)~=bi(1))
        bi(1)=bimr(l);
    end
    W(x,y)=bi2de(bi);
    l=l+1;
    if x >= 256
        x=1;
        y=y+1;
    else
        x=x+1;
    end
end
```

Sedangkan proses ekstraksi dengan LSB yaitu:

```
mm=size(m,1);
nm=size(m,2);
x=1;y=1;l=1;
for(z=1:65536)
    bi=de2bi(W(x,y),8);
    bimr(l)=bi(1);
    l=l+1;
    if x >= 256
        x=1;
        y=y+1;
    else
        x=x+1;
    end
end
l=1;x=1;
for(z=1:8192)
    bim(x,1:8)=bimr(l:l+7);
    l=l+8;x=x+1;
end
message=bi2de(bim);
rm=reshape(message(1:mm*nm),mm,nm);
```

2.2 Most Significant Bit (MSB)

MSB merupakan pengolahan stream cipher sama seperti LSB namun pesan disembunyikan di bagian awal bit (Sharma, Poriye, & Kumar, 2017)(Garg & Gulati, 2012) sehingga kemungkinan perubahan intensitas piksel menjadi lebih besar. *Pseudocode* MSB dalam proses *embedding* dapat dilihat sebagai berikut:

```
bim = de2bi(m,8);
l=1;x=1;
for(z=1:8192)
    bimr(l:l+7)=bim(x,1:8);
    l=l+8;x=x+1;
end
x=1;y=1;l=1;
for(z=1:65536)
    bi=de2bi(C(x,y),8);
    if(bimr(l)~=bi(8))
        bi(8)=bimr(l);
    end
    W(x,y)=bi2de(bi);
```

```
    l=l+1;
    if x >= 256
        x=1;
        y=y+1;
    else
        x=x+1;
    end
end
```

Sedangkan proses ekstraksi diilustrasikan pada *pseudocode* berikut:

```
mm=size(m,1);
nm=size(m,2);
x=1;y=1;l=1;
for(z=1:65536)
    bi=de2bi(W(x,y),8);
    bimr(l)=bi(8);
    l=l+1;
    if x >= 256
        x=1;
        y=y+1;
    else
        x=x+1;
    end
end
l=1;x=1;
for(z=1:8192)
    bim(x,1:8)=bimr(l:l+7);
    l=l+8;x=x+1;
end
message=bi2de(bim);
rm=reshape(message(1:mm*nm),mm,nm);
```

3. HASIL DAN PEMBAHASAN

Dalam makalah ini, metode LSB dan MSB telah diketahui performa pada proses *embedding* dan ekstraksi dengan bantuan pemrograman Matlab. Beberapa citra yang digunakan dapat dilihat pada Gambar 1, dengan format *grayscale* pada ukuran 256x256 piksel sedangkan citra pesan seperti tampak pada Gambar 2 pada ukuran 128x64 piksel.

Gambar 1. Citra cover

Gambar 2. Citra pesan

Dengan menggunakan pengukuran *Peak Signal to Noise Ratio* (PSNR) dan *Structural Similarity Index Measurement* (SSIM) sesuai Tabel 1, dapat disimpulkan bahwa secara visual LSB terbukti memperoleh nilai

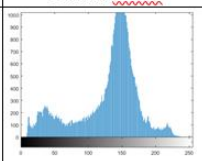
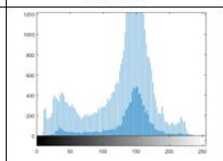
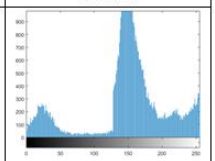
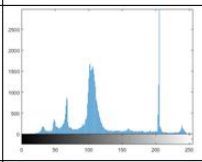
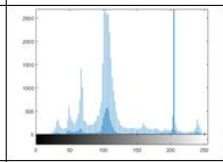
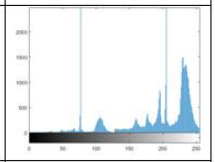
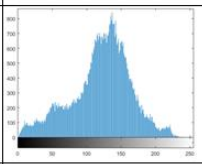
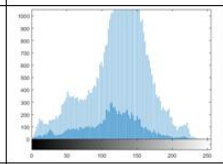
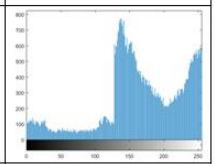
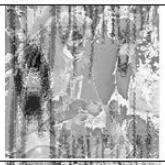
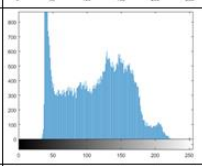
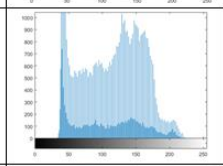
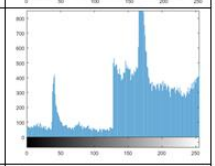
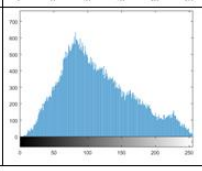
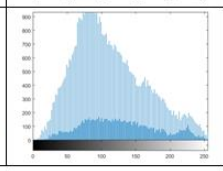
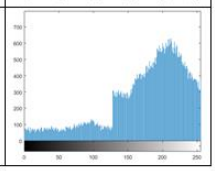
tinggi baik di PSNR maupun SSIM. Meskipun selisih nilai yang diperoleh tidak terlalu signifikan, LSB telah memenuhi aspek *imperceptibility* yang ditandai dengan perolehan nilai PSNR lebih dari 40 dB.

Tabel 1. Perbadingan LSB dan MSB pada nilai PSNR dan SSIM

Nama Citra	PSNR (dB)		SSIM	
	LSB	MSB	LSB	MSB
fishingboat	51.8916	29.6278	0.9982	0.1064
house	53.1281	27.0600	0.9978	0.2331
livingroom	51.9061	27.8816	0.9985	0.1079
pirate	51.8928	27.3258	0.9984	0.1279
walkbridge	51.9076	26.6250	0.9993	0.1640

Dalam perkembangannya PSNR dianalisa kembali dan menghasilkan nilai SSIM. Menurut Hore (Hore & Ziou, 2010), nilai SSIM mendekati 1 dapat diartikan bahwa citra hasil pemrosesan tidak dapat dibedakan dengan mata manusia. Untuk lebih jelas, pada Tabel 2 telah disajikan perbedaan hasil embedding menggunakan LSB dan MSB secara visual baik dengan citra asli maupun penegasan perubahan piksel dengan histogram.

Tabel 2. Evaluasi Embedding pada LSB dan MSB

Citra asli	Perbandingan Visual Citra		Histogram Citra Asli	Perbandingan Histogram	
	LSB	MSB		LSB	MSB
					
					
					
					
					

Berdasarkan Tabel 2, dapat dilihat bahwa citra *cover* asli dan citra hasil steganografi LSB secara kasat mata tidak ditemukan perubahan. Di sisi lain, hasil proses steganografi MSB terlihat rusak dan lebih *noise* dimana citra pesan tampak seperti berada di atas permukaan. Hal ini disebabkan oleh perubahan bit yang sangat besar pada saat proses *embedding* dengan MSB. Bit awal akan berubah sehingga hampir seluruh nilai piksel akan berubah. Pengujian lain yang dilakukan yaitu membandingkan histogram citra asli dengan hasil pemrosesan steganografi. histogram MSB terindikasi bahwa telah terjadi perubahan piksel yang sangat signifikan sehingga bentuk histogram sangat berbeda dengan citra asli. Lain halnya dengan LSB yang mempunyai bentuk histogram mirip dengan histogram pada citra asli.

5. KESIMPULAN

Dari eksperimen yang dikakukan, LSB terbutki lebih *impercept* dibanding MSB. Pembuktian ditandai dengan hasil perhitungan PSNR pada semua citra LSB lebih dari standard yang ditetapkan yaitu 40 dB. Seluruh citra bahkan memperoleh PSNR lebih dari 50 dB. Pengukuran lain yang dilakukan dengan SSIM juga menunjukkan bahwa LSB jauh lebih unggul. Pada citra fishingboat didapat nilai SSIM LSB yaitu 9.9982 sedangkan pada SSIM MSB yatiu 0.1064. Nilai tersebut seperti terbalik satu sama lain, dimana standar nilai SSIM

antara 0 sampai 1. Komparasi juga dilakukan pada model histogram yang hasilkan, dan terbukti bahwa histogram LSB lebih mirip dengan histogram citra asli dibanding MSB.

DAFTAR PUSTAKA

[1] Al-Afandy, K. A., Faragallah, O. S., Elmhalawy, A., El-Rabaie, E.-S. M., & El-Banby, G. M. (2016). High security data hiding using image cropping and LSB least significant bit steganography. In *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)* (pp. 400–404). IEEE. https://doi.org/10.1109/CIST.2016.7805079

[2] Baker, E. J. (2011). Steganograhy in Images by Using Intersecting Planes. *Eng. & Tech. Journal*, *29*(7).

[3] Bhattt, S., Ray, A., Ghoshttt, A., & Raytttt, A. (2015). Image Steganography and Visible Watermarking using LSB Extraction Technique. In *9th International Conference on Intelligent Systems and Control (ISCO)2015*.

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

[5] Ge, H., Huang, M., & Wang, Q. (2011). Steganography and steganalysis based on digital image. In *2011 4th International Congress on Image and Signal Processing* (pp. 252–255). Ieee. https://doi.org/10.1109/CISP.2011.6099953

[6] Hore, A., & Ziou, D. (2010). Image Quality Metrics: PSNR vs. SSIM. In *2010 20th International Conference on Pattern Recognition* (pp. 2366–2369). Ieee. https://doi.org/10.1109/ICPR.2010.579

[7] Irawan, C., Setiadi, D. R. I. M., Sari, C. A., & Rachmawanto, E. H. (2017). Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption. In *International Conference on Informatics and Computational Sciences (ICICoS)*.

[8] Negrat, K., Smko, R., & Almarimi, A. (2010). Variable length encoding in multiple frequency domain steganography. In *2010 2nd International Conference on Software Technology and Engineering (ICSTE)* (pp. 305–309). IEEE. https://doi.org/10.1109/ICSTE.2010.5608853

[9] Rachmawanto, E. H., Amin, R. S., Setiadi, D. R. I. M., & Sari, C. A. (2017). A performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size. In *International Seminar on Application for Technology of Information and Communication*. https://doi.org/10.1109/ISEMANTIC.2017.8251836

[10] Sari, C. A., & Rachmawanto, E. H. (2016). Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting. *Journal of Applied Intelligent System (JAIS)*, *1*(3), 179–190. Retrieved from https://scholar.google.co.id/citations?view_op=view_citation&hl=id&user=RG2Im6cAAAAJ&citation_for_view=RG2Im6cAAAAJ:5nxA0vEk-isC

[11] Sharma, A., Poriye, M., & Kumar, V. (2017). A Secure Steganography Technique Using MSB. *International Journal of Emerging Research in Management &Technology*, *9359*(6), 208–214.