STEGANOGRAFI PESAN TEKS KE DALAM CITRA DENGAN METODE LSB PADA RUANG WARNA YCOCG TERDEKOMPOSISI IWT

Sony Herwindyo[*1)], Helmie Arif Wibawa[*2)]

**Jurusan Ilmu Komputer/Informatika, Fakultas Sains dan Matematika,
Universitas Diponegoro
[1)]sonyherwindyo@rocketmail.com, [2)]helmie.arif@gmail.com

Abstrak

Keamanan adalah hal yang sangat penting dalam proses komunikasi. Integritas data dan kerahasiaan menjadi hal mutlak yang harus dipenuhi. Salah satu cara mengamankan komunikasi adalah dengan Steganografi. Penelitian ini membahas tentang implementasi Steganografi pesan teks menggunakan LSB (Least Significant Bit) dengan menyisipkanya ke dalam ruang warna YCoCg yang sudah terdekomposisi dengan IWT (Integer Wavelet Transform). Berdasarkan hasil analisis didapat nilai rata-rata PSNR sebesar 57,51 DB yang berarti memiliki nilai kerusakan yang rendah atau secara kasat mata sangat sulit untuk membedakan citra kover dengan citra stego. Dalam hal ketahanan citra stego terhadap serangan sangat lemah dikarenakan penggunaan pesan teks yang tidak dapat mentoleransi perubahan sedikitpun. Namun kesamaan pesan hasil ekstraksi terhadap pesan yang disisipkan selalu identik bila tidak terjadi perubahan pada citra stego yang dapat merubah nilai dan posisi piksel.

***Kata kunci** : Steganografi, pesan teks, LSB, ruang warna YCoCg, IWT*

Abstract

Security is the most important issue in communication. Data integrity and confidentiality are absolutely have to be fulfilled. The example of securing communication is by using Steganography. This study discussed about implementation of Steganography that securing text message using LSB (Least Significant Bit) into YCoCg color space which has been decomposed using Integer Wavelet Transform. From the result of analysis, the average value of PSNR was at 57.51 DB, and if it was seen in plain sight it would be hard to distinguish the cover image and the stego image. In terms of resilience against attacks stego image was fragile due to the text message could not tolerate any slightest change. However, the extracted message was always identical compared to the text message as long as stego image was not getting any attacks that could change the pixels value and position.

***Keywords:** Steganography, text message, LSB, YCoCg color space, IWT.*

1 PENDAHULUAN

Media komunikasi yang paling mudah, murah, dan cepat pada saat ini adalah internet, dimana segala jenis data dapat dikirimkan melalui media komunikasi global ini. Faktor keamanan tentunya menjadi sangat penting dalam proses komunikasi melalui media ini. Pengguna internet perlu untuk mengirim dan

menerima pesan yang bersifat *private* hingga tidak boleh seorangpun yang mengetahui, cara yang paling baik untuk berkomunikasi aman adalah dengan mengubah data menjadi bentuk lain, sehingga data hasil perubahan hanya dapat dimengerti oleh penerima yang mengetahui cara mengembalikanya ke bentuk semula[1].

Salah satu metode untuk mengamankan data adalah dengan membuatnya menjadi tidak terlihat yang dinamakan dengan Steganografi. Steganografi merupakan seni penyembunyian pesan ke dalam media lainnya sedemikian rupa sehingga orang lain tidak menyadari keberadaan pesan di dalam media tersebut[2]. Keberadaan pesan yang tersembunyi diharapkan dapat mengelabuhi pihak yang ingin mencuri informasi yang dikirimkan.

Ada dua properti utama yang dibutuhkan untuk melakukan Steganografi, yaitu wadah penampung (media) dan pesan atau data rahasia yang akan disembunyikan. Menyembunyikan pesan rahasia dalam citra digital adalah yang paling banyak digunakan dari semua metode dalam dunia digital saat ini. Hal ini karena dengan media citra digital maka dapat diambil keuntungan dari daya terbatas dari sistem visual manusia (HVS). Hampir semua teks biasa, sandi teks, gambar, dan lainnya dapat dikodekan menjadi aliran bit sehingga dapat disembunyikan dalam citra digital[3].

Penelitian ini menggunakan file citra RGB berformat JPEG , PNG dan BMP sebagai media penyisipan dan karakter ASCII sebagai pesan yang akan disisipkan dalam citra kover menggunakan metode LSB yang dikombinasikan dengan transformasi YCoCg dan IWT. Adapun keluaranya berupa citra stego atau file citra yang telah disisipi pesan teks.

2 TINJAUAN PUSTAKA

2.1 STEGANOGRAFI

Steganography (berasal dari bahasa Yunani) yaitu *Steganos,* yang berarti tersembunyi, dan *Graphein,* yang berarti menulis, sehingga memiliki arti seni untuk berkomunikasi dengan cara menyembunyikan keberadaan dari komunikasi itu sendiri. Tujuan utama dari Steganografi adalah untuk menyembunyikan pesan sehingga diharapkan orang yang tidak berkepentingan tidak menyadari adanya data yang disembunyikan di dalamnya. Steganografi dan Kriptografi memiliki suatu kesamaan yaitu untuk menjaga kerahasiaan suatu data, namun perbedaanya adalah steganografi menyembunyikan keberadaan pesan seingga tidak ada yang menyadari adanya komunikasi rahasia antara pengirim dan penerima, hal inilah yang menyebabkan Steganografi menjadi lebih populer pada beberapa kasus seperti permasalahan tentang hak cipta [4].

2.2 CITRA DIGITAL

Agar dapat diolah dengan komputer digital, maka suatu citra harus direpresentasikan secara numerik dengan nilai-nilai diskrit. Representasi citra dari fungsi kontinu menjadi nilai-nilai diskrit disebut digitalisasi. Citra yang dihasilkan inilah yang disebut citra digital [5]. Pada umumnya citra digital berbentuk persegipanjang, dan dimensi ukurannya dinyatakan sebagai tinggi x lebar atau lebar x panjang.

2.3 RUANG WARNA YCOCG

Kemampuan penglihatan manusia akan lebih sensitif terhadap *spatial detail Luminance,* daripada *Chrominance*. Oleh

karena itu sistem pengkodean gambar dapat dioptimalkan dengan komponen *Chrominance* dari suatu gambar dengan detail yang lebih rendah[6].

Berikut adalah bentuk umum dari transformasi ruang warna RGB menjadi YCoCg [7].

$$\begin{aligned} Co &= R - B & \qquad t &= Y - \lfloor Cg / 2 \rfloor \\ t &= B + \lfloor CO / 2 \rfloor & \qquad G &= Cg + t \\ Cg &= G - t & \Leftrightarrow \qquad B &= t - \lfloor CO / 2 \rfloor \\ Y &= t + \lfloor Cg / 2 \rfloor & \qquad R &= B + Co \end{aligned}$$

Dimana :

R = *Red*

G = *Green*

B = *Blue*

Co = *Chrominance Orange*

t = *temporary variable*

Cg = *Chrominance Green*

Y = *Luminance*

2.4 *LEAST SIGNIFICANT BIT*

Berdasarkan kaitanya dengan steganografi bagi sebuah komputer citra digital adalah sekumpulan angka yang menunjukan tingkat intensitas sebuah warna. Tiap angka-angka tersebut secara individu disebut dengan piksel, dan steganografi pada citra digital adalah suatu cara untuk mengeksploitasi piksel-piksel tersebut yang merepresentasikan sebuah warna. Perubahan warna yang sangat sedikit akibat dari penyisipan pesan akan sangat sulit untuk diamati perbedaanya[8]

Algoritma penyisipan pada *Least Significant Bit* [9]:

1. Membaca citra digital sebagai kover dan pesan teks yang akan disisipkan.
2. Mengkonversi citra digital dan pesan teks menjadi bentuk biner.
3. Menghitung seluruh LSB yang dimiliki oleh citra digital
4. Menggantikan nilai LSB citra digital dengan bit pesan teks.

2.5 *INTEGER WAVELET TRANSFORM*

Integer Wavelet Transform memetakan data *integer* menjadi bentuk *integer* lainya. Transformasi ini secara sempurna dapat dikembalikan tepat seperti data aslinya yang bertujuan untuk menghindari permasalahan dari didapatkanya nilai pecahan akibat dari penggunaan *wavelet filter*.

Persamaan IWT dua dimensi secara umum adalah sebagai berikut [10].

$$\begin{aligned} CA_{i,j} &= (\lfloor I_{2i,2j} + I_{2i+1,2j} / 2 \rfloor) & \qquad I_{2i,2j} &= CA_{i,j} - \lfloor CH_{i,j} / 2 \rfloor \\ CH_{i,j} &= I_{2i,2j+1} - I_{2i+1,2j} & \qquad I_{2i,2j+1} &= CA_{i,j} + \lfloor CH_{i,j} + 1 / 2 \rfloor \\ CV_{i,j} &= I_{2i+1,2j} - I_{2i+1,2j} & \Leftrightarrow \qquad I_{2i+1,2j} &= I_{2i,2j+1} + CV_{i,j} - CH_{i,j} \\ CD_{i,j} &= I_{2i+1,2j+1} - I_{2i+1,2j} & \qquad I_{2i+1,2j+1} &= I_{2i+1,2j} + CD_{i,j} + CV_{i,j} \end{aligned}$$

2.6 *PEAK SIGNAL TO NOISE RATIO*

Peak Signal to Noise Ratio (PSNR) digunakan untuk mengukur distorsi yang terjadi antara gambar yang telah mengalami manipulasi dengan gambar aslinya. Semakin besar nilai PSNR, semakin baik gambar tersebut karena gambar tersebut lebih sedikit mengalami distorsi dan sebaliknya. Satuan dari nilai PSNR adalah desibel (dB). Nilai PSNR dan MSE pada citra dapat dihitung dengan persamaan berikut [11].

$$PSNR = 10 \log_{10} \left(\frac{MAX_1^2}{MSE} \right)$$

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left[I_{i,j} - K_{i,j} \right]^2$$

3 PERANCANGAN

3.1 KEBUTUHAN FUNGSIONAL

Secara umum kebutuhan fungsional aplikasi ini adalah untuk pengamanan pesan, sehingga tidak membutuhkan banyak

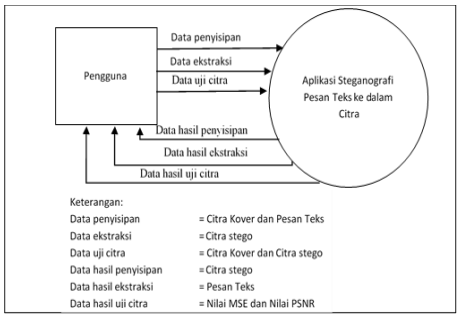
requirements melainkan hanya proses penyisipan dan ekstraksi pesan dalam citra. Secara lengkapnya kebutuhan fungsional dijelaskan pada tabel 3.1.

Tabel 3.1 Kebutuhan fungsional dan definisi

SRS ID	Definisi
SRS-F001	Membaca masukkan citra kover dan masukkan pesan teks dari pengguna.
SRS-F002	Menyisipkan pesan teks ke dalam citra kover yang telah diberikan transformasi ruang warna dan wavelet.
SRS-F003	Melakukan ekstraksi pesan teks dari dalam citra kover dan melakukan rekonstruksi kembali.
SRS-F004	Melakukan uji kualitas citra stego dengan menggunakan nilai MSE dan PSNR.

3.2 *DATA CONTEXT DIAGRAM*

Secara garis besar interaksi sistem dengan pengguna dapat digambarkan dengan DCD pada gambar 3.1.



Gambar 3.1 *Data Context Diagram*

3.3 ALGORITMA PENYISIPAN PESAN

Berikut adalah algoritma untuk menyisipkan pesan teks ke dalam sebuah citra kover :

1. Membaca / *Load* citra kover dan pesan teks yang dimasukkan oleh pengguna.
2. Mentransformasi ruang warna citra kover yang semua RGB menadi YCoCg, didapatkan kanal Y, Co, dan Cg.
3. Mentransformasi kanal Y dengan IWT *(Integer Wavelet Transform)* hingga didapatkan empat buah *subband* yaitu CA, CH, CV, CD.
4. Mengubah nilai piksel citra kover dan pesan teks menjadi format biner.
5. Menyisipkan bit pesan teks kedalam satu bit terahir citra kover.
6. Melakukan invers IWT kemudian invers YCoCg.
7. Didapatkan citra stego atau citra kover yang sudah tersisipi pesan.

3.4 ALGORITMA EKSTRAKSI PESAN

Proses ekstraksi pada dasarnya sama dengan proses penyisipan, perbdaanya terletak pada proses ini membaca nilai LSB citra kover. Berikut adalah algoritma ekstraksi pesan.

1. Membaca / *Load* citra stego dan pesan teks yang dimasukkan oleh pengguna.
2. Mentransformasi ruang warna citra stego yang semua RGB menadi YCoCg, didapatkan kanal Y, Co, dan Cg.
3. Mentransformasi kanal Y dengan IWT *(Integer Wavelet Transform)* hingga didapatkan empat buah *subband* yaitu CA, CH, CV, CD.
4. Membaca niai LSB *subband* CA sejumlah panjang pesan yang disisipkan.
5. Menyusun bit-bit yang didapatkan dari subband CA dan mengelompokkanya setiap delapan bit.
6. Konversi bit-bit pesan teks menjadi karakter, didapatkan pesan teks yang disisipkan.

4 HASIL DAN PEMBAHASAN

4.1 PENGUJIAN

Berdasarkan kebutuhan fungsional aplikasi, proses pengujian dibagi menjadi tiga kelas uji, yaitu pengujian penyisipan pesan teks ke dalam citra kover, pengujian ekstraksi pesan teks dari citra stego, ,pengujian perhitungan nilai PSNR citra kover dengan citra stego dan pengujian terhadap beberapa serangan pada citra stego.

Dari keempat kelas uji tersebut didapatkan hasil sebagai berikut.

1. Pengujian penyisipan pesan teks ke dalam citra telah berhasil dilakukan hingga didapatkan keluaran berupa citra stego yang sudah tersisipi pesan.
2. Pengujian ekstraksi pesan teks dari dalam citra stego telah berhasil dilakukan. Pesan teks yang disisipkan kedalam citra dapat diambil kembai secara utuh.
3. Pengujian kualitas citra stego dengan perhitungan PSNR didapatkan nilai rata-rata sebesar 57,51 DB.
4. Seluruh percobaan serangan terhadap citra stego menyebabkan kegagalan ekstraksi pesan teks, sedangkan serangan rotasi citra stego setelah dinormalkan kembali ke posisi semula maka pesan teks dapat diekstaksi dengan sempurna.

4.2 KESIMPULAN

Kesimpulan yang dapat diambil adalah telah dihasilkanya aplikasi steganografi yang mengamankan pesan teks kedalam sebuah citra yang sudah dilakukan transformasi ruang warna YCoCg dan IWT. Keluaran citra stego dari aplikasi ini memiliki tingkat kerusakan yang rendah dengan nilai PSNR rata-rata sebesar 57,51 yang termasuk dalam kategori sangat baik, namun citra stego sangat rentan terhadap serangan karena penggunaan pesan teks yang tidak dapat mentoleransi perubahan sedikitpun. Namun selama citra stego tidak mendapatkan serangan maka pesan teks hasil ekstraksi akan selalu sama dengan pesan teks yang disisipkan.

REFERENSI

[1]. Kumar, A. & Pooja, K., 2010. Steganography- A Data Hiding Technique. *International Journal of Computer Applications volume 9 No.7*, pp. 19-23.

[2]. Sellars, d., 1996. An Introduction to Steganography. *Jurnal ilmiah.*

[3]. Filipus, J., 2009. Perbandingan Digital Steganografi pada Media Image, Audio, Video, dan

[4]. Channalli, S. & Jadhav , A., 2009. Steganography Art Of Hiding Data. *International Journal on Computer Science and Engineering Vol.1(3).*

[5]. Munir, R., 2004. *Pengolahan Citra Digital dengan Pendekatan Algoritmik.* Bandung: Penerbit Informatika Bandung.

[6]. Malvar, H. & Sullivan, G., 2003. YCoCg-R: A Color Space with RGB Reversibility and Low Dynamic Range.

[7]. Starosolski, R., 2014. New simple and efficient color space transformations for lossless image compression. *Institute of Computer Science, Silesian University of Technology, Akademicka 16, 44-100.*

[8]. Laskar, S. A. & Hemachandran, K., 2012.High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Database Management Systems (IJDMS) Vol.4, No.6.*

[9]. Thangadurai, K. & Devi, G. S., 2014. An analysis of LSB Based Image Steganography Techniques. *2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA* .

[10]. Tolba, M. F., Gonemy, M. A. & Khalifa, A. S., 2004. Using Integer Wavelet Transforms In Colored Image-Steganography. *IJICIS Vol. 4 No. 2.*

[11]. Neyman, S. N., Lindayanti & Guritman, S., 2002. Teknik Penyembunyian Data Rahasia pada Berkas Gambar Digital Menggunakan Steganografi Least Significant Bit Variable-Size. *Jurnal Ilmu Komputer Agri-Informatika, Volume 1 Nomor 1 Halaman 30-36.*