DETEKSI POSISI PESAN RAHASIA PADA CITRA STEGANOGRAFI BERBASIS LSB MENGGUNAKAN DISCRETE WAVELET TRANSFORM DAN KLASIFIKASI *SVM*

POSITION DETECTION OF SECRET MESSAGES FROM LSB-BASED IMAGE STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM AND SVM CLASSIFICATION

Anindita Fitriani[1],Iwan Iwut Tritoasmoro[2],Nur Ibrahim[3]

[1,2,3] Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

[1]aninditaf94@gmail.com, [2]iwaniwuttritoasmoro@telkomuniversity.ac.id, [3]nuribrahim@telkomuniversity.ac.id

Abstrak

Pada zaman di era globalisasi ini, perkembangan teknologi dan informasi sudah semakin meningkat. Seiring perkembangan teknologi yang semakin meningkat ini, kondisi privasi setiap orang semakin berkurang, sedangkan kebutuhan privasi setiap orang harus tetap dipertahankan. Oleh karena itu, dibutuhkan sebuah teknik untuk menyembunyikan suatu pesan rahasia ke dalam sebuah media. Teknik tersebut dinamakan *steganography*. *steganography* mempunyai efek negatif dimana seseorang memanfaatkan teknik *Steganography* tersebut untuk disalahgunakan dan tidak bertanggung jawab**.** Oleh karena itu, terciptalah sebuah teknik untuk menyerang teknik *steganography* itu sendiri yang dinamakan *steganalysis.* Tujuan dari *steganalysis* itu sendiri adalah untuk mengetahui ada atau tidaknya pesan yang tersisipi pada suatu media. Pada penelitian kali meancang system steganalisis untuk dengan menggunakan metode DWT dan klasifikasi SVM untuk mendeteksi ada tidaknya pesan tersisipi serta letak posisi sisipan dan volume pesan rahasia dengan metode windowing.

Kata Kunci: Steganografi, Steganalisis, DWT, SVM, *Windowing*

Abstract

In this era of globalization, the development of technology and information has increased. As the development of technology is increasing, the condition of each person's privacy is diminishing, while the privacy needs of each person must be maintained. Therefore, a technique is needed to hide a secret message into a media. This technique is called steganography. steganography has a negative effect where one uses the Steganography technique to be misused and irresponsible. Therefore, a technique for attacking the steganography technique itself is called steganalysis. The purpose of steganalysis itself is to find out whether or not the message is inserted in a media. In this research, I designed the steganalysis system to use the DWT method and SVM classification to detect the presence or absence of messages inserted in and the position of the insertion and volume of the secret message with windowing method.

Keywords: Steganography, Steganalysis, DWT,SVM, Windowing

1. Pendahuluan

Seiring dengan perkembangan teknologi di era globalisasi ini, kebutuhan dalam teknologi dan informasi juga semakin meningkat. Seiring meningkatnya permintaan akan teknologi dan informasi ini, kebutuhan dalam *privacy* seseorang pula semakin menipis. Oleh karena itu, terciptalah sebuah metode untuk menyisipkan suatu pesan rahasia ke dalam suatu media penampung untuk menyembunyikan suatu pesan rahasia. Media penampung tersebut bisa berupa teks, video, audio, maupun gambar. Teknik penyisipan pesan rahasia tersebut dinamakan *Steganography*. Banyak penelitian yang dilakukan untuk menemukan cara agar pesan rahasia tersebut dapat dideteksi keberadaannya sekaligus mengekstrak atau minimal menghancurkan pesan rahasia tersebut dari media penampungnya. Teknik mendeteksi, mengekstrak, dan menghancurkan pesan rahasia tersebut dinamakan *steganalysis* [1]. *Steganalysis* merupakan anti-steganografi, dimana algoritma *steganalysis* yang saat ini terus berkembang untuk mendeteksi keberadaan pesan rahasia yang disembunyikan dengan algoritma-algoritma steganografi [1].

Sudah banyak penelitian yang merancang system steganalisis salah satunya " Simulasi dan Analysis Steganalisis Citra Domain DMWT Menggunakan Klasifikasi KNN" Dari hasil pengujian berdadarkan penggunaan level DMWT didapatkan akurasi tertinggi 58.75% pada level 1. Setelah itu pada ukuran gambar didapatkan akurasi tertinggi pada ukuran gambar 256x256 sebesar 60.41%, dan pada pengaruh jumlah sisipan didapatkan 70% pada sisipan ukuran 5KB [15].

2. Tinjuan Pustaka

A. Citra Digital

Citra digital dapat di definisikan sebagai fungsi dua variable, f(x,y), dimana x dan y adalah koordinat spasial dan nilai f(x,y) adalah intensitas citra pada koordinat tersebut[7].

B. Steganografi

Steganography merupakan Teknik atau cara penyisipan suatu pesan rahasia ke dalam sebuah media [2]. Media yang digunakan dapat berupa gambar, video, atau audio. Pesan yang disisipkan pada media tersebut juga dapat berupa *text*, gambar, audio, maupun video.

C. LSB (*Least Significant Bit*)

LSB merupakan sebuah metode *steganography* dengan cara menyisipkan pesan ke dalam bit rendah pada data pixel yang menyusun citra digital. Cara kerja metode LSB ini sendiri yaitu, dengan mengubah bit redundan *cover image* yang tidak berpengaruh signifikan dengan bit dari pesan rahasia [7]. Dalam system ini, LSB digunakan sebagai metode penyisipannya agar mendapatkan ouputan *Stego Image.*

D. Steganalisis

Steganalisis merupakan teknik yang digunakan untuk mendeteksi dan menganalisa kemungkinan adanya data tersembunyi pada citra tersteganografi. Steganalisis dibagi menjadi tiga tingkatan yaitu : deteksi, ekstraksi, dan menonaktifkan atau melakukan tindakan lain untuk mencegah data tersebut tersebar luas [8]. Salah satu pengolahan steganalisis adalah transformasi data.

E. DWT (*Discrete Wavelet Transform*)

Discrete Wavelet Transform adalah dekomposisi suatu citra pada frekuensi *subband* citra tersebut. Pemfilteran pada DWT ini secara garis besar akan melewatkan sinyal yang akan dianalis pada filter dengan frekuensi dan skala yang berbeda [8].

F. SVM (*Support Vector Machine*)

Pada konsepnya SVM dapat dijelaskan secara sederhana sebagai usaha mencari *hyperplane* terbaik yang berfungsi sebagai pemisah dua buah kelas[10]. Kernel digunakan dalam model SVM, terdapat dua macam kernel yaitu : kernel linier dan non-linier. Kernel liner yang bertujuan agar data yang akan diklasifikasi dapat terpisah dengan sebuah garis / *hyperline*. Sedangkan kernel non-linier bertujuan agar ketika digunakan data hanya dapat dipisahkan dengan garis lengkung atau sebuah bidang dalam dimensi tinggi.

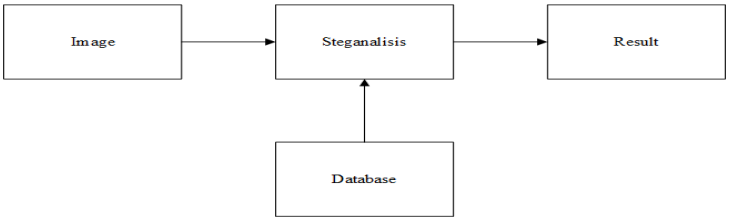
G. *Windowing*

Windowing adalah metode yang digunakan untuk mencari letak atau posisi pesan yang telah disisipkan dan volume citra yang telah tersteganografi dengan metode LSB, dengan cara melakukan pengelompokan mejadi 8 *pixel* pada tiap layer.

3. Perancangan Sistem

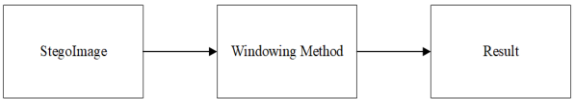
A. Desain Sistem

Desain sistem dimulai dengan memilih *image* yang akan di deteksi apakah tersisipi atau tidak. Sistem ini dirancang agar memiliki output apakah citra tersebut termasuk kedalam kelas asli *cover* atau kelas stego dengan menggunakan klasifikasi SVM..



Gambar 1 Blok diagram steganalisis

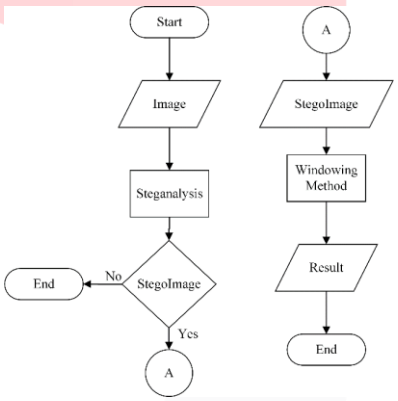
Setelah citra tersebut sudah terdeteksi apakah termasuk kedalam kelas tersisipi maka dilanjutkan dengan mencari posisi dan volume pesan rahasia yang disisipkan pada citra tersebut dengan menggunakan proses *windowing*.



Gambar 2 Blok diagram deteksi posisi dan volume

B. Perancangan Sistem Utama

Sistem steganalisis yang dirancang terdiri dari dua bagian yaitu proses ekstraksi dan klasifikasi. Proses ekstraksi pada system ini menggunakan DWT untuk mendapatkan fitur ciri yang kemudian diklasifikasikan menggunakan metode SVM apakah termasuk kedalam kelas citra stego atau citra asli. Setelah itu dilanjutkan dengan *windowing method* untuk mengetahui letak posisi dan volume pesan rahasia tersebut



Gambar 3 Desain system utama

Proses pada sistem utama ini adalah :

a. Memilih *image* yang akan dianalisis.
b. Tahap ini melakukan proses steganalisis menggunakan metode DWT, dan SVM yang akan membagi kelas apakah image yang akan diproses termasuk dalam kelas tersisipi atau tidak.
c. *Image* yang termasuk kelas tersisipi akan diproses lanjut menggunakan metode *windowing* dimana pada proses ini akan mengeluarakan hasil letak posisi penyisipannya dan berapa jumlah volume pesan tersisipnya.

4. Hasil Analisis

A. Pengujian Sistem Steganalisis

a. Pengujian ciri statistik

Pada proses pengujian ini akan menganalisis perbedaan ciri statistik PCA antara *mean, standart deviation, skewness, kurtosis, Ratio*. Ukuran citra yang digunakan yaitu 128 × 128 *pixel*, menggunakan jenis kernel Quadratic dengan level DWT 1, jumlah karakter sisipan 9. Hasil dari pengujian akurasi terbaik pada ciri statistik, digunakan sebagai acuan pengujian selanjutnya. Berikut merupakan hasil yang didapatkan :

Tabel 1 Pengujian Ciri Statistik

Jumlah Ciri Statistik	Ciri Statistik	Akurasi (%)
1	Skewness	50.0
	Ratio	52.5
	Standar Deviasi	50.0
	Kurtosis	50.0
	Mean	50.0
2	Skewness, Ratio	52.5
	Skewness,Standar Deviasi	50.0
	Skewness, Kurtosis	50.0
	Skewness, Mean	50.0
3	Skewness, Ratio, Standar Deviasi	52.5
	Skewness,Kurtosis,Mean	50.0
	Ratio,Standar Deviasi,Kurtosis	57.5
	Ratio,Standar Deviasi,Mean	50.0
	Standar Deviasi,Kurtosis,Mean	50.0
	Skewness,Ratio,Kurtosis	**60.0**
	Skewness,Ratio,Mean	52.5
4	Skewness, Ratio, Standar Deviasi,Kurtosis	55
	Skewness,Ratio,Standar Deviasi,Mean	50.0
	Ratio,Standar Deviasi,Kurtosis,Mean	52.5
	Skewness,Standar Deviasi,Kurtosis, Mean	50.0
5	Skewness,Standar Deviasi,Kurtosis, Mean,Ratio	55.0

Berdasarkan hasil yang didapatkan bahwa didapatkan akurasi terbaik menggunakan kombinasi tiga ciri statistika Skewness, Ratio, dan kurtosis sebesar 60%.

b. Pengujian Pengaruh Jumlah Karakter Sisipan

Pada pengujian ini untuk membandingkan apakah jumlah karakter sisipan mempengaruhi akurasi. Jumlah karakter sisipan yang dipakai 6,9,12,15 karakter dengan ukuran citra 128x128 menggunakan jenis kernel *Quadratic* dan level DWT level 1. Berikut merupakan hasil yang didapatkan :

Tabel 2 Pengujian Pengaruh Jumlah Karakter

Jumlah Karakter	Akurasi (%)
6 Karakter	57.5
9 Karakter	60.0
12 Karakter	52.5
15 Karakter	50.0

Berdasarkan Tabel diatas, akurasi mengalami fluktuasi yang tidak terlalu signifikan. Hal ini disebabkan semakin banyak karakter sisipan ciri yang diperoleh lebih bervariasi yang memungkinkan ciri satu dengan yang lainnya sama. Pada pengujian ini didapatkan bahwa akurasi tertinggi berada pada pada jumlah sisipan sebanyak 9 karakter sebesar 60%.

c. Pengujian Pengaruh Level DWT

Pada pengujian ini digunakan ukuran citra 128x128 dengan jumlah karakter sisipan sebanyak 9 karakter. Berikut merupakan hasil yang diperoleh:

Tabel 3 Pengujian Pengaruh Level DWT

Level DWT	Akurasi(%)
Level 1	60
Level 2	55
Level 3	65

Berdasarkan table diatas, akurasi yang didapatkan mengalami fluktuasi. Akurasi tertinggi didapatkan pada DWT level 3 yaitu sebesar 65%. Pada level-3 citra akan didekomposisikan dalam frekuensi yang lebih banyak dengan menggunakan kombinasi tiga ciri statistik menyebabkan ukuran citra hasil dekomposisinya semakin kecil dan ciri yang dihasilkan lebih banyak. Sehingga, ciri yang didapatkan lebih spesifik dan meningkatkan kemungkinan bahwa sisipan tersebut berada pada *pixel-pixel* tertentu dan menyebabkan perbedaan antara citra *cover* dan citra stego semakin jauh. Dari hasil yang didapatkan pada pengujian ini, bahwa sistem bekerja lebih optimal pada level DWT-3.

d. Pengujian Pengaruh Jenis Kernel

Pada pengujian ini digunakan citra berukuran 128x128 dengan jumlah karakter sisipan sebanyak 9 karakter dengan mengunakan dekomposisi DWT level-3. Berikut merupakan hasil yang diperoleh:

Tabel 4 Pengujian Pengaruh Jenis Kernel

Jenis Kernel	Akurasi (%)
Quadratic	65
Polynomial	57.5
Linear	55

Berdasarkan data diatas hasil pegujian pengaruh jenis kernel,akurasi terendah pada jenis Kernel Linear sebesar 55% dikarenakan data citra menyebar sehingga diperlukan bantuan kernel untuk mengahasilkan *hyperplane* terbaik. Pada pengujian sistem ini jenis kernel *Quadratic* lebih cocok digunakan pada sistem ini. Karena, memiliki tingkat akurasi yag lebih tinggi yaitu sebesar 65% dan lebih baik untuk data inputan citra

e. Pengujian Pengaruh Ukuran Gambar

Tabel 5 Pengujian Pengaruh Ukuran Gambar

Ukuran Gambar	Akurasi (%)
128x128	65.0
256x256	55.0
512x512	52.5

Dari hasil Pengujian ditas menunjukan bahwa ukuran gambar mempengaruhi tingkat akurasi meskipun tidak terlalu signifikan. Akurasi mengalami penurunan dan tingkat akurasi terendah pada ukuran gambar 512x512 yaitu sebesar 52.5%. Hal ini disebabkan oleh semakin tinggi resolusi citra dipakai maka *volume* dari penyisipan juga semakin besar begitupun sebaliknya.

B. Pengujian Sistem Deteksi Posisi Pesan Sisipan dan Volume

Pada proses pengujian ini menganalisis bagaimana pengaruh perbedaan posisi penyisipan pesan rahasia. Data yang digunakan untuk analisis kali ini menggunakan hasil dari analisis steganalisis sebelumnya yang telah benar diidentifikasi memiliki

sisipan. Data uji yang digunakan sebanyak 20 dan yang teridentifikasi benar memiliki sisipan sebanyak 13. Berikut merupakan hasil dari deteksi posisi pesan :

Tabel 1 Hasil Pengujian deteksi posisi sisipan

Data Ke	Posisi Sisip	Status Posisi sisip
21	1-72	**Benar**
22	1-72	**Benar**
23	1-88	**Salah**
24	1-72	**Benar**
28	2-73	**Benar**
30	2-73	**Benar**
31	3-74	**Benar**
32	3-74	**Benar**
35	3-74	**Benar**
36	4-75	**Benar**
38	4-91	**Salah**
39	4-83	**Salah**
40	4-83	**Salah**

Dari 13 data uji yang dinyatakan benar memiliki pesan rahasia, 4 diantaranya salah dalam posisi sisipannya. Sehingga akurasi yang didapatkan sebesar 69%.

Tabel 2 Hasil Pengujian Volume Sisipan

Data Ke	Volume	Status Posisi sisip	Isi StegoText
21	72	**Benar**	01Maret97
22	72	**Benar**	01Maret97
23	88	**Salah**	**01Maret97HI**
24	72	**Benar**	01Maret97
28	72	**Benar**	01Maret97
30	72	**Benar**	01Maret97
31	72	**Benar**	01Maret97
32	72	**Benar**	01Maret97
35	72	**Benar**	01Maret97
36	72	**Benar**	01Maret97
38	88	**Salah**	**01Maret97n9**
39	80	**Salah**	**01Maret97D**

40	80	**Salah**	**01Maret97O**

Berdasarkan data diatas, dapat disimpulkan bahwa akurasi deteksi *volume* sama dengan deteksi posisi sisipan yaitu sebesar 69%. Hal ini dikarenakan untuk mendapatkan volume sisipan dengan cara mengurangi posisi awal sisipan. Volume disini menunjukan berapa banyak karakter yang disisipkan (dalam bit).

5. Kesimpulan

Berdasarkan pengujian yang dilakukan citra dengan panjang karakater sisipan sebanyak 9 karakter dengan ukuran citra 128x128 memiliki akurasi yang tertinggi dan dengan menggunakan tiga ciri statistika yaitu *Skewness, Ratio, Kurtosis* akurasi yang didapatkan 60%. Pada pengujian mencari Level DWT dan jenis kernel terbaik didapatkan pada DWT Level-3 dan kernel *Quadratic* dengan akurasi sebesar 65%. Pada pengujian pengaruh ukuran citra hasil yang didapatkan tetap sama yaitu dengan ukuran citra 128x128 mendapatkan akurasi tertinggi sebesar 65%. Pada pengujian deteksi posisi dan *volume* memliki akurasi yang sama yaitu sebesar 69%.

6. Daftar Pustaka

[1] W. Hidayat, "Mendeteksi Keberadaan Pesan Tersembunyi dalam Citra Digital dengan Blind Steganalysis," *Seniati.,* Vol.3., no.2, pp. 77–81, 2011.

[2] D. Baby., J. Thomas.,G.Augustine.,E.George., and N. Rosi., "A Novel DWT based Image Securing Method using Steganography," *Int.Conf.inf.Tech.*, vol. 46, pp. 612 – 618, 2014

[3] A. A. Ali, "Image Steganography Technique By Using Braille Method of Blind People (LSBraille)," *Int. J. Image.Processing.*, Vol 7, pp. 81–89, 2013.

[4] R. Joshi, L. Gagnani, and S. Pandey, "Image Steganography," *Int. J. Latest Engineering. Mangement Reaserch.*,vol. 2, no. 1, pp. 224–227, 2013.

[5] M. Rodr, "Blind Steganalysis Method for Detection of Hidden Information in Images by Master in Computer Science Advisors :," 2013.

[6] Y. Kurniawan, "Studi Metode Steganalisis Pada Stegoimage," *Bandung Progr. Stud. Tek. Inform. Intitut Teknol. Bandung*, 2006.

[7] M. Marwa., A. Ali., and F. Omara., "A Modified Image Steganography Method based on LSB Technique," *Int. J. Comput. Appl.*, vol. 125, no. 5, pp. 12–17, 2015

[8] Nugraha, Anindito Setya. Tugas Akhir. Implementasi Steganalisis Dengan Menggunakan Metode BSM-SVM pada Steganografi Citra Digital. Bandung : Jurusan Teknik Informatika. Universitas Telkom.2013

[9] http://repository.petra.ac.id/16069/1/Publikasi1_01036_838.pdf

[10]mamcs.lecture.ub.ac.id/tag/support-vector-machine-svm

[11]http://sutikno.blog.undip.ac.id/files/2011/11/tutorial-svm-bahasa-indonesia-oleh-krisantus.pdf

[12] https://www.slideshare.net/farohalolya/*wavelet*-transform-and-dsp-applications

[13] D. Y. Apriliyana. 2015. Algoritma Discrete Wavelet Transform (Dwt) Dan Absolute Moment Block Truncation Coding (Ambtc) Pada Sistem Watermarking Untuk Deteksi Dan Recovery Citra Medis. Tugas Akhir. Jurusan Teknik Informatika. Universitas Telkom: Bandung.

[14] Putra, Fauzan Pradana Akinta. 2016. Steganalisis Citra Digital Domain Frekuensi Berbasisikan Descrete Wavelet Transform Dan Principal Component Analysis. Tugas Akhir. Jurusan Teknik Telekomunikasi. Universitas Telkom: Bandung.

[15] Levi, Diati Putri. 2016. Simulasi dan Analisis Steganalisis Citra Dengan Menggunakan Metode DMWT dan KNN. Tugas Akhir. Jurusan Teknik Telekomunikasi. Universitas Telkom: Bandung.

[16] Filzasavitra, Priyandanu. 2018. Penerapan Steganografi pada Citra PNG Menggunakan Metode *Least Significant Bit* (LSB). Tugas Akhir. Jurusan Sistem Komputer. Universitas Telkom: Bandung.