DETEKSI POSISI DAN VOLUME PADA CITRA TERSTEGANOGRAFI MENGGUNAKAN METODE LSB, DCT DAN PEMBAGIAN BLOK

DETECTION OF POSITION AND VOLUME ON IMAGE STEGANOGRAPHY USING LSB, DCT, AND BLOCKING METHOD

Wijayaning Bawono[1],Iwan Iwut Tritoasmoro[2],Nur Andini[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom, Bandung
[1]wijayaningbawono@gmail.com, [2]iwaniwuttritoasmoro@telkomuniversity.ac.id,
[3]nurandini@telkomuniversity.ac.id

Abstrak

Berbagai jenis cara untuk berkomunikasi dapat dilakukan, salah satnya dengan menyembunyikan pesan ke dalam suatu objek lain. Hal itu dapat disebut sebagai dengan steganografi. Steganografi merupakan seni atau ilmu yang mempelajari proses dalam menyembunyikan suatu informasi ke dalam *cover* data yang berupa video, audio, citra. Steganografi dapat dikelompokan menjadi 2 jenis yaitu: *blind* steganografi dan *non blind* steganografi, penyalahgunaan steganografi sering terjadi, salah satunya digunakan untuk menyisipkan suatu pesan tertentu atas dasar tindak kriminal. Maka dari itu, diperlukan adanya steganalisis untuk mengontrol akan adanya penyalahgunaan steganografi. Steganalisis adalah teknik yang digunakan untuk mendeteksi dan menganalisa kemungkinan adanya data tersembunyi ke dalam cover data. Penelitian ini merancang sebuah arsitektur dari metode DCT (*Discrete Cosine Transform*) dan pembagian blok sebagai metode ekstraksi ciri , menggunakan PCA (*Principal Component Analysis*) sebagai pereduksi citra digital, K-NN (*K-Nearest Neighbor*) untuk proses klaisfikasi, dan metode *Windowing* untuk menentukan letak posisi dan volume pada citra tersteganografi, dan didapatkan akurasi sebesar 75% pada sistem steganalisis dan akurasi sebesar 72% pada deteksi posisi dan volume citra tersteganografi.

Kata Kunci: Steganografi, Steganalisis, DCT, PCA, K-NN, *Windowing*

Abstract

Various types of ways to communicate can be done, one of them is by hiding the message into another object. That can be referred to as steganography. Steganography is an art or science that studies the process of hiding information into cover data in the form of video, audio, image. Steganography can be grouped into 2 types, namely: blind steganography and non-blind steganography, abuse of steganography often occurs, one of which is used to insert a particular message on the basis of a crime. Therefore, steganalysis is needed to control the existence of misuse of steganography. Steganalysis is a technique used to detect and analyze the possibility of hidden data in the data cover. This study designed an architecture from the DCT (Discrete Cosine Transform) method and blocking method as a feature extraction method, using PCA (Principal Component Analysis) as a digital image reduction, K-NN (K-Nearest Neighbor) for classification process, and Windowing method for determine the position and volume position of the echographic image, and obtained an accuracy of 75% on the steganalysis system and an accuracy of 60% on the detection of position and volume of images steganography.

Keywords: Steganography, Steganalysis, DCT, PCA, K-NN, Windowing

1. Pendahuluan

Dengan adanya kemajuan teknologi yang sangat pesat kususnya dalam bidang komunikasi, komunikasi bukanlah suatu hal yang perlu dipermasalahkan lagi karena berkomunikasi tidak harus bertatap muka, pada jaman sekarang berkomunikasi dapar dilakukan dimana saha dan kapan saja. Berbagai jenis cara untuk berkomunikasi dapat dilakukan, salah satunya dengan menyembunyikan pesan ke dalam suatu objek lain disebut sebagai steganografi, bertujuan agar orang yang tidak diinginkan tidak dapat mengetahui apa informasi yang telah disisipkan [1]. Steganografi dikelompokan menjadi 2 jenis berdasarkan informasi yang dibutuhkan untuk proses pengekstraksian yaitu : *blind* steganografi dan *non blind* steganografi, metode dimana *image cover* tidak dibutuhkan untuk mengambil atau mengekstrak pesan rahasia terebut disebut *blind* steganografi, sedangkan metode dimana membutuhkan *image cover* untuk mengekstrak pesan rahasia disebut *non blind* steganografi, dalam proses steganografi lebih bagus menggunakan *blind* steganografi karena lebih kuat (*robust*) dan aman daripada *non blind* steganografi [2]. Dengan cara seperti ini dapat memudahkan kita untuk saling bertukar pesan, baik yang menguntungkan maupun yang merugikan. Penyalahgunaan steganografi sering terjadi, salah satunya digunakan untuk menyisipkan suatu pesan tertentu atas dasar tindak kriminal. Maka dari itu, diperlukan adanya

steganalisis untuk mengontrol akan adanya penyalahgunaan steganografi. Steganalisis merupakan teknik yang digunakan untuk mendeteksi dan menganalisa kemungkinan adanya data tersembunyi ke dalam citra digital yang menggunakan steganografi, steganalisis terbagi menjadi 3 tingkatan yaitu: deteksi, ekstraksi, dan menonaktifkan atau menghancurkan data yang disembunyikan atau melakukan tindakan lain untuk mencegah data tersebut tersebar luas [3]. Penelitian tentang steganalisis sudah banyak dilakukan seperti "Image Steganalysis with Binary Similarity Measures" yaitu penelitian steganalisis menggunakan metode BSM, SVM mendapatkan akurasi sebesar 85.61% , "A Blind Steganalysis on JPEG Gray Level Image Based on Statistical Features and its Performance Analysis" tentang proses *blind* steganalisis menggunakan metode DWT, SVM menggunakan variasi penyisipan dan mendapatkan akurasi terbaik sebesar 69.5%, "Digital image steganalysis based on local texturalfeatures and double dimensionality reduction" tentang proses steganalisis menggunakan metode PCA dan *Ensemble* meghasilkan akurasi sebesar 88.6%.

2. Tinjuan Pustaka

A. Citra Digital

Citra adalah gambar dua dimensi matriks yang dihasilkan dari gambar analog dua dimensi yang kontinu menjadi gambar diskrit melaluai proses sampling. Dimana elemen matriks tersebut berupa nilai intensitasi cahaya.

B. Steganografi

Steganografi merupakan suatu ilmu dalam menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain atau data lain. Dengan demikian keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi dalam steganografi pesan disembunyikan sedemikian rupa sehingga pihak lain tidak dapat mengetahui pesan rahasia. Pesan rahasia tidak akan berubah seperti kriptografi. Pesan tersebut hanya disembunyikan ke dalam suatu media berupa citra, teks, audio maupun video [7].

C. LSB (*Least Significant Bit*)

LSB merupakan teknik penyembunyian data yang bekerja pada domain spasial, dengan cara penyisipan pada bit terakhir, metode ini sangat efektif digunakan untuk penyisipan karena hanya merubah nilai bit terakhir menjadi 1 atau 0 dari nilai sebelumnya. Namun metode LSB tidak aman sebab jika citra yang telah tersteganografi menggunakan LSB mengalami *preprocessing* seperti *resize,* kompresi, dan sebagainya, maka semua bit LSB dari pesan yang telah tersteganografi atau *stegotext* di dalam citra menjadi rusak sehingga pesan tidak dapat diungkapkan kembali, dan lokasi penyisipan selalu pada bit terakhir, mengakibatkan pihak lawan yang curiga dapat menghapus pesan dengan mengganti semua bit LSB pada *stegotext* [7].

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. DCT (*Discrete Cosine Transform*)

DCT adalah metode transformasi yang mempresentasikan suatu sinyal ke dalam deret batas suatu point data, dimana sinyal tersebut adalah hasil penjumlahan komponen-komponen yang merupakan fungsi *cosinus* yang berisolasi di frekuensi berbeda. Metode ini akan menggunakan pembagian blok dengan ukuran blok 8×8 *pixel* pada proses DCT 2-D dimana DCT-2D digunkan untuk mengolah sinyal berdimensi dua, seperti citra[9].

F. PCA *(Principal Component Analysis).*

PCA adalah metode analisis statistik multivariat yang memilih variabel penting dengan transformasi linier dari beberapa variabel, metode ini dapat menjadi komponen utama dalam orthogonal transformasi yang dapat mereduksi atau menghilangkan korelasi antara fase multi temporal, yang dapat meningkatkan akurasi klasifikasi [10].

G. K-NN (*K-Nearest Neigbor*)

K-NN adalah metode klasifikasi terhadap objek berdasarkan data latih yang nilainya paling mendekati objek. Metode ini membutuhkan data latih yang nilainya paling mendekati objek, dan membutuhkan data latih

sebagai acuan terhadap data uji, sehingga jumlah K-tetangganya yang mayoritas diambil akan menentukan banyak data dari kelas yang masuk ke dalam region tersebut**.** Perhitungan jarak dapat menggunakan berbagai macam teori, diantaranya *Euclidan Distance, City Block, Cosine, Correlation*.

a. *Euclidan distance* merupakan teori perhitungan yang paling umum digunakan, menggunakan rumus[11]:

$$J(v_1, v_2) = \sqrt{\sum_{k=1}^{N} (v_1(k) - v_2(k))^2} \quad (1)$$

b. *City Block* adalah matriks yang digunakan untuk menghitung nilai perbedaan absolut antara dua vektor[11].

$$J(v_1, v_2) = \sum_{k=1}^{N} |v_1(k) - v_2(k)| \quad (2)$$

c. *Cosine Distance* merupakan pengukuran terhadap sudut antara dua vektor[11].

$$cos(N_i, N_j) = \frac{\sum_k a_{i,k}.a_{j,k}}{\sqrt{\sum_k a_{i,k}^2}\sqrt{\sum_k a_{j,k}^2}} \quad (3)$$

d. *Correlation Distance* merupakan titik-titik dimana dianggap sebagai barisan nilai[11].

$$S_{i,j} = \frac{\sum_{k=1}^{n}(x_{i,k} - \acute{x}_i)(x_{j,k} - \acute{x}_j)}{\sqrt{\sum_{k=1}^{n}(x_{i,k} - \acute{x}_i)^2 \sum_{k=1}^{n}(x_{j,k} - \acute{x}_j)^2}} \quad (4)$$

Dimana:
$v_1\ dan\ v_2 = Data\ latih\ dan\ Data\ uji$
$J(v_1, v_2) = jarak\ (J)\ dari\ \ v_1\ ke\ v_2$
$N = Dimensi\ data$
$k = Jumlah\ data\ dari\ tetangga\ terdekat$

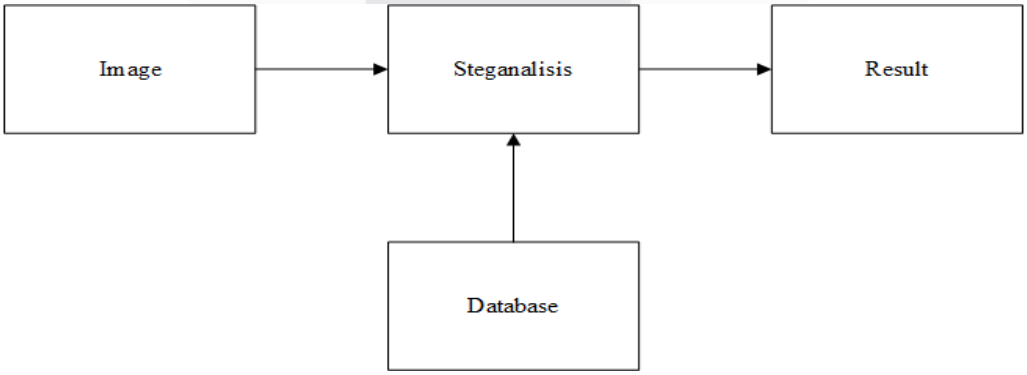
H. *Windowing*

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

Sistem Steganalisis yang dirancang akan mengolah *image* agar mendapatkan hasil keluaran apakah *image* tersebut termasuk kelas asli atau kelas tersisipi. Sebuah *image* diproses dalam steganalisis berdasarkan *database training* dari K-NN yang akan menghasilkan analisis apakah *image* tersebut disisipi pesan rahasia atau tidak.



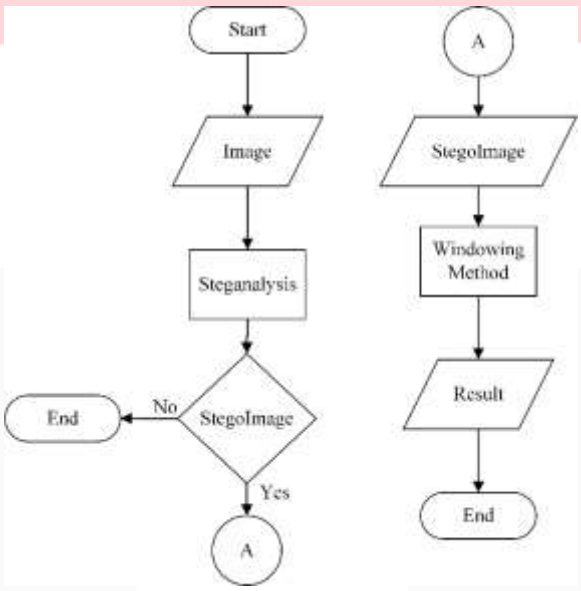
Gambar 1 Blok diagram steganalisis

Setelah proses steganalisis, stegoimage yang terdeteksi memiliki pesan rahasia akan dilakukan proses *windowing*, dimana pada proses ini dirancang mengolah stegoimage agar mendapatkan hasil keluaran berdasarkan letak posisi dan volume pesan rahasia pada stegoimage.

Gambar 2 Blok diagram deteksi posisi dan volume pesan tersteganografi

B. Perancangan Sistem Utama

Sistem steganalisis yang dirancang terdiri dari dua bagian yaitu proses ekstraksi dan klasifikasi. Proses ekstraksi ciri adalah proses dimana mengabil fitur ciri yang menjadi acuan dari K-NN untuk menentukan kelas pada proses klasifikasi. Ekstraksi ciri akan terbagi menjadi dua kelas yaitu kelas asli dan kelas tersisipi dari citra acuan.



Gambar 3 Desain system utama

Proses pada sistem utama ini adalah :

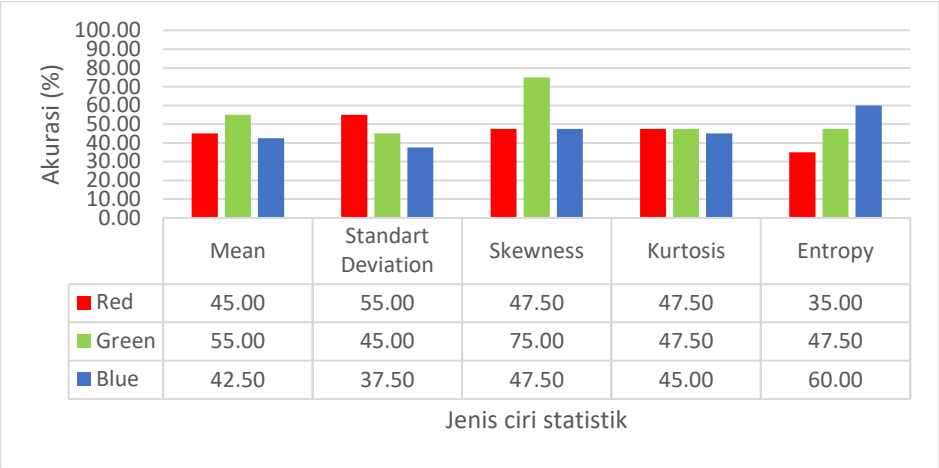
a. Memilih *image* yang akan dianalisis.
b. Tahap ini melakukan proses steganalisis menggunakan metode DCT, PCA, KNN, lalu apakah image yang akan diproses termasuk dalam kelas tersisipi atau tidak.
c. *Image* yang termasuk kelas tersisipi akan diproses lanjut menggunakan metode *windowing* dimana pada 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, entropy*. Ukuran citra yang digunakan yaitu 256 × 256 *pixel*, menggunakan jenis jarak K-NN *euclidean, cosine, city block, correlation*, menggunakan nilai K = 1-9, dan menggunakan *layer* di *R, G, B* untuk normalisasi. Hasil dari pengujian akurasi terbaik pada ciri statistik, digunakan sebagai parameter pengujian berikutnya.



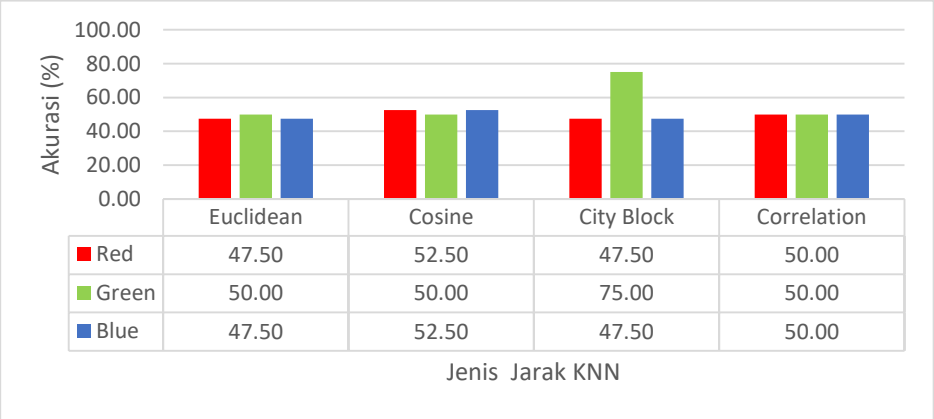
	Mean	Standart Deviation	Skewness	Kurtosis	Entropy
Red	45.00	55.00	47.50	47.50	35.00
Green	55.00	45.00	75.00	47.50	47.50
Blue	42.50	37.50	47.50	45.00	60.00

Gambar 4 *Bar Char* hasil pengujian ciri statistic PCA

Berdasarkan hasil pengujian tersebut, diambil akurasi terbesar dan didapatkan ciri statistik *skewness* yang menghasilkan akurasi terbesar pada *layer green* sebesar 75%, sedangkan ciri statistik *entropy* menghasilkan akurasi terbesarnya pada *layer blue* sebesar 60%, dan pada ciri statistik *standard deviation* menghasilkan akurasi terbesar pada *layer red* sebesar 55%.

b. Pengujian jenis pencarian jarak K-NN.

Pada proses pengujian ini akan menganalisis perbedaan pengunaan metode dalam mencari jarak pada K-NN.



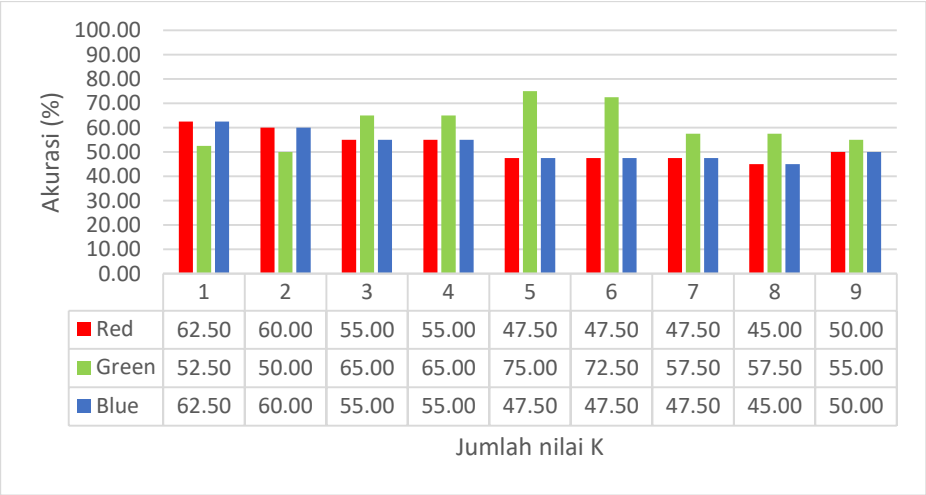
	Euclidean	Cosine	City Block	Correlation
Red	47.50	52.50	47.50	50.00
Green	50.00	50.00	75.00	50.00
Blue	47.50	52.50	47.50	50.00

Gambar 5 *Bar Chart* hasil pengujian jenis pencarian jarak K-NN

Berdasarkan hasil pengujian tersebut, jenis metode yang digunakan untuk mencari jarak pada K-NN yaitu *city block* yang menghasilkan akurasi terbesar pada *layer green* sebesar 75%.

c. Pengujian jumlah *K* pada K-NN.

Pada proses pengujian ini akan menganalisis nilai jumlah *K* pada K-NN, dimanakah nilai jumlah *K* yang menghasilkan akurasi terbaik pada sistem steganalisis ini.

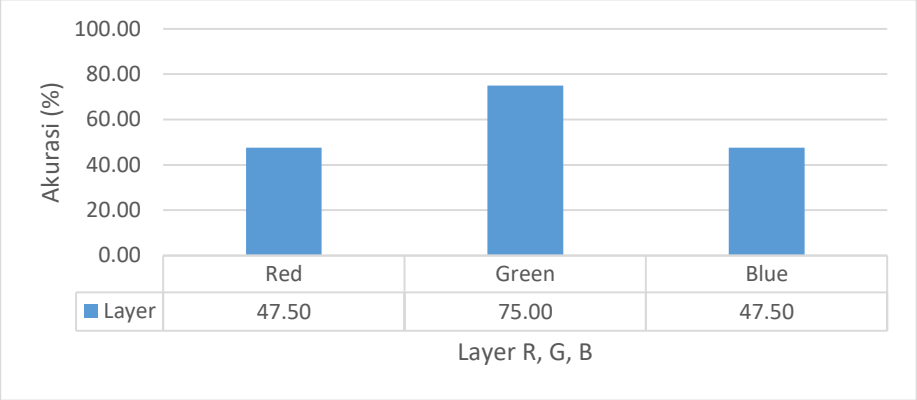


Gambar 6 *Bar Chart* hasil pengujian jumlah *K* pada K-NN

Berdasarkan hasil pengujian tersebut, nilai jumlah *K* yang digunakan di K-NN yaitu saat *K* = 5 menghasilkan akurasi terbesar pada *layer green* sebesar 75%

d. Pengujian layer pada akurasi sistem steganalisis.

Pada proses pengujian ini akan menganalisis *layer red*, *green* dan *blue* yang digunakan untuk menentukan dimanakah letak *layer* yang dapat menghasilkan nilai akurasi terbaik pada sistem steganalisis ini.



Gambar 7 *Bar Chart* hasil pengujian *layer red*, *green* dan *blue*

Berdasarkan hasil pengujian tersebut, layer yang menghasilkan akurasi terbaik yaitu pada *layer green* sebesar 75% dengan komputasi sebesar 1.2012 *s*.

B. Pengujian Sistem Deteksi Posisi Pesan Sisipan

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.

Tabel 1 Hasil Pengujian deteksi posisi sisipan

Data Ke	Status	Posisi			Status Posisi	Data ke	Status	Posisi			Status Posisi
		R	G	B				R	G	B	
2	Salah	-	-	-	Benar	27	Benar	9-27	9-27	9-27	Benar
7	Salah	-	-	-	Benar	28	Benar	2-21	2-21	2-21	Salah
8	Salah	-	-	-	Benar	29	Benar	7-43	7-43	7-43	Benar

9	Salah	-	-	-	Benar	30	Benar	8-45	8-45	8-45	Benar
11	Salah	-	-	-	Benar	31	Benar	9-36	9-36	9-36	Benar
13	Salah	-	-	-	Benar	32	Benar	2-30	2-30	2-30	Salah
14	Salah	-	-	-	Benar	33	Benar	7-43	7-43	7-43	Benar
16	Salah	-	-	-	Benar	34	Benar	8-45	8-45	8-45	Salah
18	Salah	-	-	-	Benar	35	Benar	9-45	9-45	9-45	Benar
21	Benar	7-16	7-16	7-16	Benar	36	Benar	2-39	2-39	2-39	Salah
22	Benar	8-18	8-18	8-18	Salah	37	Benar	7-54	7-54	7-54	Salah
23	Benar	9-18	9-18	9-18	Benar	38	Benar	8-53	8-53	8-53	Benar
24	Benar	2-12	2-12	2-12	Salah	39	Benar	9-54	9-54	9-54	Benar
25	Benar	7-25	7-25	7-25	Benar	40	Benar	2-48	2-48	2-48	Salah
26	Benar	8-26	8-26	8-26	Benar						

Dari pengujian 29 data uji yang diidentifikasikan sebagai i*mage* yang tersisipi pesan, didapatkan data yang benar dalam mendeteksi posisi pesan sisipannya sebanyak 21 dari 29 data uji yang ada, maka akurasinya adalah 72%.

C. Pengujian Sistem Deteksi Volume Pesan Sisipan

Pada proses pengujian ini menganalisis bagaimana pengaruh banyak sedikitnya pesan yang disisipkan pada suatu citra.

Tabel 2 Hasil pengujian untuk deteksi volume sisipan

Data ke	Volume	Status Volume	Tambahan	Data ke	Volume	Status Volume	Tambahan
2	-	Benar	-	27	18	Benar	berkumpul di buba
7	-	Benar	-	28	19	Salah	gberkumpul di bubat
8	-	Benar	-	29	27	Benar	musuh menyerang kami tolong
9	-	Benar	-	30	27	Benar	musuh menyerang kami tolong
11	-	Benar	-	31	27	Benar	musuh menyerang kami tolong
13	-	Benar	-	32	28	Salah	gmusuh menyerang kami tolong
14	-	Benar	-	33	36	Benar	denisa sudah makeup tapi ga standart
16	-	Benar	-	34	37	Salah	denisa sudah makeup tapi ga standarts
18	-	Benar	-	35	36	Benar	denisa sudah makeup tapi ga standart
21	9	Benar	I love uu	36	37	Salah	gdenisa sudah makeup tapi ga standart
22	10	Salah	I love uug	37	47	Salah	ani cantik sekali pake banget banget bangetsstk
23	9	Benar	I love uu	38	45	Benar	ani cantik sekali pake banget banget bangetss

24	10	Salah	gi love uu	39	45	Benar	ani cantik sekali pake banget banget bangetss
25	18	Benar	berkumpul di bubat	40	46	Salah	gani cantik sekali pake banget banget bangetss
26	18	Benar	berkumpul di bubat				

Dapat dilihat pada tabel diatas, bahwa hasil akurasi pada deteksi volume sama seperti deteksi posisi pesan sisipan, karena pengujian volume pesan sisipan hasilnya berbanding lurus dengan pengujian pengaruh posisi pesan sisipan, dikarenakan untuk mendapatkan volume pesan sisipan yaitu dengan cara mengurangi posisi terakhir kali penyisipan dengan posisi awal penyisipan, apa bila dalam menentukan posisi didapatkan hasil yang salah, maka dalam menentukan volume juga akan mengalami kesalahan.

5. Kesimpulan

Metode DCT, PCA, K-NN dan *windowing* dapat diimplementasikan dalam sistem steganalisis dan sistem deteksi posisi, volume citra tersteganografi. Setiap sample data memilki ciri yang hampir mirip dan belum terujinya kulaitas dataset yang dipakai karena untuk mendapatkan dataset steganalisis yang teruji kualitasnya tidaklah mudah. Pada sistem deteksi posisi dan volume *image* tersteganografi ini memiliki kelemahan karena hanya dapat mendeteksi pesan yang selain huruf kapital dan simbol. Dari hasil analisis pada sistem steganalisis, didapatkan parameter - parameter yang dapat meningkatkan performasi sistem tersebut, yaitu dengan kondisi menggunakan ciri statistik PCA *kurtosis*, nilai *K* pada jenis pencarian jarak K-NN menggunakan *skewness* adalah 5 dan menggunakan l*ayer green* untuk pengambilan ciri fitur statistiknya yang menghasilkan akurasi sebesar 75% dengan nilai komputasi 1.2012 *s.* Akurasi terbaik yang didapatkan sistem deteksi posisi dan volume hanya sebesar 72%.

6. Daftar Pustaka

[1] K. C. Widadi, P. H. Ainianta, and C. C. W. C. C. Wah, "Blind Steganography using Direct Sequence/Frequency Hopping Spread Spectrum Technique," *2005 5th Int. Conf. Inf. Commun. Signal Process.*, pp. 6–10, 2005.

[2] B. G. Banik and S. K. Bandyopadhyay, "Blind Key based Attack Resistant Audio Steganography using Cocktail Party effect."

[3] T. Qian and S. Manoharan, "A comparative review of steganalysis techniques," *2015 IEEE 2nd Int. Conf. InformationScience Secur. ICISS 2015*, 2016.

[4] C. Paulin, S. A. Selouani, and E. Hervet, "A comparative study of audio/speech steganalysis techniques," *Can. Conf. Electr. Comput. Eng.*, pp. 1–4, 2017.

[5] N. Zarmehi and M. A. Akhaee, "Digital video steganalysis toward spread spectrum data hiding," *IET Image Process.*, vol. 10, no. 1, pp. 1–8, 2016.

[6] R. R. Chhikara, "GLCM Based Features for steganalysis," pp. 385–390, 2014.

[7] F. Monica and E. Insanudin, "Aplikasi Steganografi Citra Digital Menggunakan Metode LSB (Least Significant Bit) Visual Basic 6," no. May, 2016.

[8] N. F. Johnson and S. Jajodia, "Steganalysis: the investigation of hidden information," *Inf. Technol. Conf. 1998. IEEE.*, pp. 113–116, 1998.

[9] L. Mutmainnah, "Analisis Pengamanan Data dengan Steganografi Audio Berbasis Teknik Psychoacoustic," 2012.

[10] and C. Y. P. Wang, L,.Li, "Image Classification By Principal Component Analysis of Multi- Channel Deep Feature," pp. 696–700, 2017.

[11] S. AhmedMedjahed, T. Ait Saadi, and A. Benyettou, "Breast Cancer Diagnosis by using k-Nearest Neighbor with Different Distances and Classification Rules," *Int. J. Comput. Appl.*, vol. 62, no. 1, pp. 1–5, 2013.