STEGANALISIS PADA STEGANOGRAFI CITRA DIGITAL MENGGUNAKAN METODE BINARY SIMILARITY MEASURES DAN HIDDEN MARKOV

STEGANALYSIS ON DIGITAL IMAGES STEGANOGRAPHY USING BINARY SIMILARITY MASURES METHOD AND HIDDEN MARKOV MODEL

Faizhal Rifky Alfaris[1] , Rita Magdalena, Ir., MT.[2] , I Nyoman Apraz Ramatryana, ST., MT [3]
Prodi S1 Teknik Telekomunikasi, Fakultas Elektro, Universitas Telkom

[1]faizhal.alfaris@gmail.com, [2]ritamagdalena@telkomuniversity.ac.id , [3]ramatryana@telkomuniversity.ac.id ,

ABSTRAK

Steganografi adalah teknik penyisipan pesan/informasi ke dalam media lain (gambar, audio, video, dll) sehingga informasi tersebut aman dan tidak mudah disalahgunakan oleh orang lain. Penggunaan steganografi juga dapat mempermudah pengirim informasi untuk menyembunyikan pesan dalam bentuk lain. Untuk mendeteksi keberadaan pesan yang tersembunyi perlu adanya teknik tersendiri yang disebut Steganalisis. Bisa diartikan bahwa steganalisis adalah suatu ilmu untuk mengetahui/mendeteksi adanya pesan tersembunyi dalam sebuah media yang telah disisipkan menggunakan steganografi.

Dalam proses pembuatan Proposal Tugas Akhir ini, analisis deteksi stego (stegano object) akan menggunakan metode Binary Similarity Measures (BSM). Metode BSM digunakan untuk mengetahui perubahan pada bit-bit dengan perhitungan kemiripan pada level biner. Untuk metode klasifikasi akan digunakan HMM (Hidden Markov Model), dengan cara memprediksi hasil yang dicari menggunakan perhitungan probabilitas (kemungkinan). Pada penelitian sebelumnya penggunaan HMM sangat efektif untuk proses klasifikasi dalam sistem pengenalan (recognition). Maka pada penelitian kali ini HMM akan digunakan untuk membantu proses klasifikasi ciri terutama untuk mencari informasi yang tersembunyi.

Pada Tugas Akhir ini diimplementasikan metode steganalisis Binary Similarity Measures (BSM) dan Hidden Markov Models (HMM) untuk mendeteksi beberapa citra digital dengan format JPG yang telah disisipi steganografi LSB. Berdasarkan pengujian yang telah dilakukan, program tersebut dapat mendeteksi steganografi LSB dengan akurasi mencapai 74,80%. Hal tersebut juga dapat menghindarkan dari penyalahgunaan informasi dengan cara penyusupan pesan lain kedalam objek tersebut.

Kata kunci Steganografi, Steganalisis, Citra Digital, Teks, Hidden Markov Model (HMM), Binary Similarity Measures (BSM)..

ABSTRACT

Steganography is the technique of inserting a message / information into other media (images, audio, video, etc.) so that the information is secure and not easily be abused by others. The use of steganography can also facilitate the information's sender to hide the message in another form. To detect the presence of hidden messages need a certain technique called Steganalisis. Could mean that steganalisis is a science to determine / detect the presence of hidden messages in a media that has been inserted using steganography.

In the process of making this Final Assigment Proposal, stego detection analysis (stegano object) will use Binary Similarity Measures (BSM) methods. BSM method is used to determine changes in the bits with the similarity calculation at the binary level. For the classification method will be used HMM (Hidden Markov Model), by way of predicting the outcome use the calculation of probability (likelihood). In the previous study the use of HMM is very effective for the classification process in the recognition system. So in this study HMM will be used to assist in the classification of the characteristics, especially to find the hidden information.

In this Final Assigment will be implemented the steganalisis Binary Similarity Measures (BSM) method and Hidden Markov Models (HMM) for detection of multiple digital images in JPG format that has been inserted LSB steganography. Based on the testing, the program can detect LSB steganography with accuracy of 74,80%. It can also avoid the misuse of information by means of infiltration another message into the object..

1. Pendahuluan

Steganografi merupakan sebuah teknik untuk menyisipkan pesan/informasi ke dalam suatu media lain (gambar, audio, video, dll) sehingga keamanan informasi penting tersebut dapat terjamin. Namun terdapat beberapa kasus penyalahgunaan teknik ini, salah satunya penyelundupan data rahasia sebuah perusahaan oleh oknum-oknum tertentu. Maka dari itu perlu adanya cara atau strategi pengawasan untuk data yang penting bagi pribadi maupun organisasi.

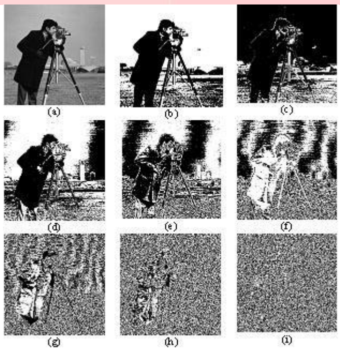
Steganalisis merupakan teknik untuk mendeteksi pesan tersembunyi dalam suatu objek steganografi. Karena pada dasarnya sebuah objek steganografi memiliki pola-pola tertentu untuk di deteksi. Metode steganalisis yang digunakan pada Tugas Akhir ini adalah metode Binary Similarity Measures (BSM) yang digunakan untuk mengetahui perubahan pada bit-bit dengan menghitung kemiripan pada level biner. Sedangkan untuk klasifikasi ciri menggunakan bantuan dari metode Hidden Markov Model (HMM), yang memungkinkan menganalisis data masukan dengan memprediksi hasil dari perhitungan probabilitas. Pada penelitian sebelumnya[1]&[3] sudah digunakan metode klasifikasi dengan metode SVM, namun pada penelitian ini dipilih metode klasifikasi HMM dikarenakan pada referensi Lawrence R. Rabiner[5], HMM memiliki kehandalan yang cukup memadai dalam pengenalan pola.

Dalam Tugas Akhir ini penulis mencoba menerapkan serta menganalisis metode steganalisis Binary Similarity Measures (BSM) dengan bantuan Hidden Markov Models (HMM) yang berperan sebagai *classifier*. Kedua algoritma tersebut akan digunakan untuk mendeteksi citra digital yang telah disisipi steganografi LSB (Least Significant Bit) yang merupakan steganografi paling sederhana dan umum digunakan.

2. Dasar Teori dan Metodologi

2.1 Binary Similarity Measures (BSM)

Binary Similarity Measures (BSM) merupakan metode perhitungan ukuran kedekatan antara bit satu dengan bit lainnya. Konsep ini memanfaatkan perhitungan kemiripan pada binary image, dalam hal ini yang akan diteliti adalah bitplane pada citra digital. Pemanfaatan konsep ini penting pada analisis pengelompokan data berdasarkan nilai kedekatan bit.



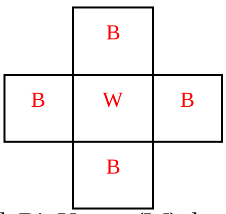
Gambar 2.1 : Contoh bitplane pada citra digital 8-bit[10]

Bitplane yang digunakan adalah bit-bit LSB yang kemudian akan diproses menggunakan BSM. Contohnya citra digital 8-bit berarti ada 8 bitplane pada setiap pixelnya. Pada bitplane ini yang akan terlihat jelas oleh mata adalah most significant bit (MSB) dan yang tidak terlihat adalah least significant bit (LSB). Dalam penelitian yang telah ada, perubahan satu bit saja pada LSB akan merubah bit-bit lain yang berada disebelahnya sehingga membentuk sebuah pola. Pola inilah yang akan dianalisa oleh BSM.

Representasi BSM digumakan untuk menghitung tiap perubahan pada pola-pola bit dari LSB. Perhitungan pada BSM juga berguna untuk menghitung perubahan bit-bit tetangga yang bersebelahan dengan bit utama.

$$\chi_{r,s} = \begin{cases} 1 & x_r = 0 \ \& \ x_s = 0 \\ 2 & x_r = 0 \ \& \ x_s = 1 \\ 3 & x_r = 1 \ \& \ x_s = 0 \\ 4 & x_r = 1 \ \& \ x_s = 1 \end{cases}$$

Dari perhitungan tersebut maka akan diberikan nilai-nilai pada perbandingan bit utama dengan bit tetangganya.



Gambar 2.2 : Contoh Bit Utama (W) dan Bit Tetangga (B) [3]

Selanjutnya nilai dari perhitungan tersebut akan dipakai untuk menghitung nilai α menggunakan persamaan berikut :

$$\alpha_i^n = \sum_{k=1}^{K} \delta(\chi_{r,s}^{k} = i) \qquad i = 1,2,\ldots.4 \ , \quad K = 4$$

$$\alpha(x_i, x_k) = \begin{cases} 1, & x_i = x_k \\ 0, & x_i \neq x_k \end{cases}$$

Nilai K merupakan representasi bit tetangga yang bersebelahan (atas, bawah, kanan, kiri), sedangkan index i melambangkan pixel keseluruhan pada citra. Setelah mendapatkan nilai α, langkah selanjutnya adalah memasukkan nilai α tersebut untuk menghitung nilai a,b,c,d dengan persamaan berikut :

$$a = \frac{1}{MN}\sum_i \alpha_i^1 , \qquad b = \frac{1}{MN}\sum_i \alpha_i^2 ,$$

$$c = \frac{1}{MN}\sum_i \alpha_i^3 , \qquad d = \frac{1}{MN}\sum_i \alpha_i^4 ,$$

Nilai MN merepresentasikan jumlah kolom dan baris atau bisa dikatakan nilai MN melambangkan besar ukuran gambar (MxN). Setelah mendapatkan nilai a,b,c,d selanjutnya nilai-nilai tersebut akan digunakan untuk mengukur dmx dengan persamaan-persamaan yang ada pada Binarry Similarity Measures seperti yang ada di tabel :

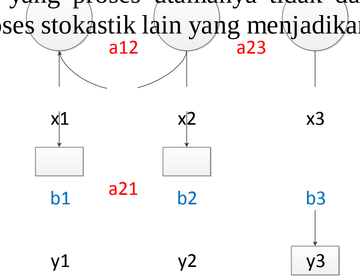
Tabel 2.1 : Tabel Perhtungan Binary Similarity Measures [1]

Similarity Measures	Rumus	Similarity Measures	Rumus
Sokal & Sneath Similarity Measure 1	$dm_1 = \frac{2(a+d)}{2(a+d)+b+c}$	Variance Dissimilarity Measure	$dm_{10} = \frac{b+c}{4(a+b+c+d)}$
Sokal & Sneath Similarity Measure 2	$dm_2 = \frac{a}{a+2(b+c)}$	Binary Minimum Histogram Difference	$dm_{11} = \sum_{n=1}^{4} \min(p_n, q_n)$
Kulczynski Similarity Measure 1	$dm_3 = \frac{a}{b+c}$	Binary Absolute Histogram Difference	$dm_{12} = \sum_{n=1}^{4} \min\lvert p_n - q_n \rvert$
Sokal & Sneath Similarity Measure 3	$dm_4 = \frac{a+d}{b+c}$	Binary Mutual Entropy	$dm_{13} = -\sum_{n=1}^{4} p_n \log q_n$
Sokal & Sneath Similarity Measure 4	$dm_5 = \frac{\frac{a}{a+b}+\frac{a}{a+c}+\frac{d}{b+d}+\frac{d}{c+d}}{4}$	Binary Kullback-Leibler Distance	$dm_{14} = -\sum_{n=1}^{4} p_n \log \frac{p_n}{q_n}$
Sokal & Sneath Similarity Measure 5	$dm_6 = \frac{ad}{\sqrt{(a+b)(a+c)(b+d)(c+d)}}$	Ojala Minimum Histogram Difference	$dm_{15} = \sum_{n=1}^{4} \min(S_n^1, S_n^2)$
Ochiai Similarity Measure	$dm_7 = \sqrt{\left(\frac{a}{a+b}\right)\left(\frac{a}{a+c}\right)}$	Ojala Absolute Histogram Difference	$dm_{16} = \sum_{n=1}^{4} \lvert S_n^1 - S_n^2 \rvert$
Binary Lance & Williams Nonmetric Dissimilarity Measure	$dm_8 = \frac{b+c}{2a+b+c}$	Ojala Mutual Entrophy	$dm_{17} = -\sum_{n=1}^{N} S_n^1 \log S_n^2$
Pattern Difference	$dm_9 = \frac{bc}{(a+b+c+d)^2}$	Ojala Kullback-Leibler Distance	$dm_{18} = -\sum_{n=1}^{N} S_n^1 \log \frac{S_n^1}{S_n^2}$

Namun menurut Jing-Qu Lin [1], mengutarakan bahwa perhitungan BSM ke-15 sampai ke-18 mengacu pada perhitungan metode Local Binary Patterns (LBP) yang merupakan invarian untuk grayscale. Menurut hasil penelitian nilai dm15-dm18 untuk citra kosong dan citra stego tidak berada dalam skala yang stabil. Sehingga hasil perhitungan keempat rumus terakhir tersebut tidak membantu classifier untuk bekerja dengan baik. Jadi keempat perhitungan tersebut bisa diabaikan.

2.2 Hidden Markov Model

Hidden Markov Model (HMM) adalah model probabilitas yang menggambarkan hubungan stokastik antara urutan observasi dan state yang tidak teramati (hidden). HMM merupakan rantai Markov yang terdiri dari serangkaian proses stokastik rangkap yang proses utamanya tidak dapat diobservasi secara langsung namun hanya dapat diobservasi melalui set proses stokastik lain yang menjadikan suatu deretan observasi.



Gambar 2.3 : Contoh sederhana dari Hidden Markov Model

Dari gambar diatas dapat diasumsikan bahwa x merupakan *hidden state* dan y adalah *observable output*. Sedangkan a merupakan probabilitas transisi dan b menggambarkan probabilitas output. Keluaran dari suatu percobaan tidak bergantung pada kemungkinan keluaran selanjutnya, dan proses percobaan sebelumnya akan mempengaruhi keluaran selanjutnya.

Pada Hidden Markov Model state yang dimiliki tidak secara langsung dapat diamati. Masing-masing state dapat menimbulkan probabilitas observasi dan output.

Setiap HMM memiliki komponen-komponen sebagai berikut :

1. Jumlah state (N), HMM terdiri dari N-state yang dinotasikan dengan $S=(S_1,S_2,...S_N)$.
2. Jumlah simbol pengamatan yang berbeda tiap state (M), simbol pengamatan dinotasikan dengan $V=(V_1,V_2,...V_M)$.
3. Distribusi peluang transisi antar state (A), yaitu menyatakan distribusi peluang transisi dari state ke-i menuju state ke-j dimana :

$$\square = \square[\square_{+1} = \square|\square = \square], 1 \leq \square\square \leq \square$$

4. Distribusi peluang simbol observasi (B), yaitu menyatakan distribusi peluang simbol ke-k pada state ke-j yang dinyatakan dalam matriks BNxM, dimana :

$$\square(\square) = \square[\square_{\square\square\square\square\square}|\square = \square], 1 \leq \square \leq \square\square = 1,2,3, ... \square$$

5. Distribusi peluang inisialisasi (π), yaitu menyatakan distribusi peluang inisialisasi state ke-i dimana :

$$\pi_\square = \square[\square_1 = \square], 1 \leq \square \leq \square$$

3. Pengujian

Dalam pengujian ini akan dilakukan analisis pada program yang telah dibuat. Pada proses latih kali ini akan digunakan 300 buah citra biasa dan 300 buah citra stego dengan jenis file JPG. Semua citra latih tersebut akan dimasukan ke dalam proses latih sehingga terbentuk database dari semua inputan yang telah didapat dari citra latih.

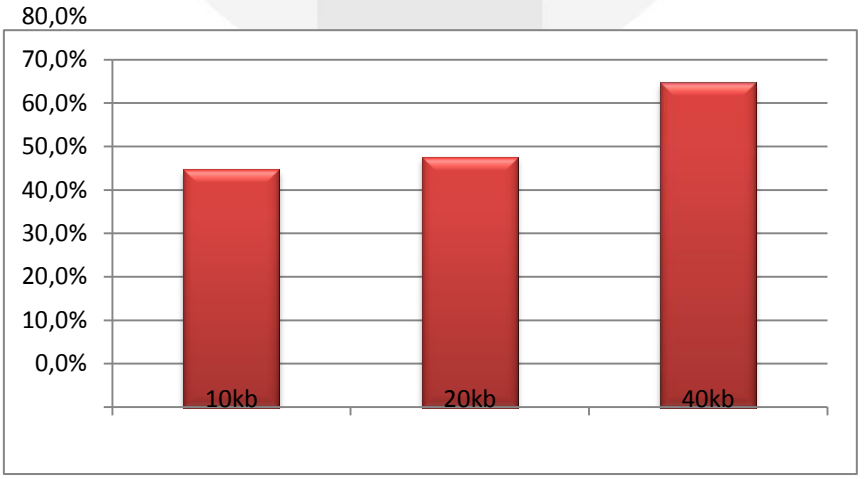
Dalam proses latih terdapat dua bagian proses yaitu proses ekstraksi ciri dan proses klasifikasi. Proses ekstraksi ciri dilakukan oleh BSM dimana pada proses tersebut nilai-nilai ketetanggaan dari suatu citra diambil dan dihitung menggunakan persamaan 18 fitur BSM untuk setiap citra.. Pada proses klasifikasi akan dibantu oleh HMM sebagai algoritma klasifikasi yang dianggap handal. Setelah itu akan dibuat kelas untuk citra yang terindikasi steganografi dan kelas untuk citra biasa (kosong).

Pada proses uji, citra yang akan dideteksi terlebih dahulu diambil cirinya oleh BSM kemudian masuk ke sistem klasifikasi HMM. Hasil yang dikeluarkan dari proses tersebut adalah text yang memberitahukan bahwa citra yang diuji tersebut tergolong kelas citra stego atau citra biasa.

3.1 Pengaruh Besar Ukuran Teks Sisipan

Pada analisis ini dilakukan analisis terhadap 3 data uji yang dibedakan berdasarkan ukuran teks yang disisipkan ke dalam citra digital. Besar teks yang disisipkan berukuran 10kb, 20kb, dan 40kb file dengan format txt.

Pada proses uji, akan diuji 300 set data uji yang akan dibagi 3 sesuai besar teks yang disisipkan. Dan data uji tersebut akan dibagi 2 yaitu citra kosong dan citra stego. Pada proses uji kali ini format citra digital yang digunakan memiliki format JPG, dengan metode steganografi LSB yang merupakan steganografi yang sangat sederhana. Dan BSM merupakan steganalisis yang cukup handal dalam mendeteksi steganografi terlebih untuk genre citra digital.



Gambar 4.1 :Grafik akurasi terhadap pengaruh besar file sisipan

Dapat dilihat pada grafik – yang terdapat diatas bahwa semakin besar ukuran file teks yang disisipkan, makin besar pula akurasi yang didapatkan. Untuk citra dengan sisipan teks sebesar 10kb memiliki akurasi 54,80%, untuk citra dengan sisipan teks sebesar 20kb memiliki akurasi 57,60%, dan untuk citra dengan besar sisipan 40kb memiliki akurasi 74,80%. Bisa dilihat melalui data ekstraksi HMM yang telah diperoleh seperti berikut :

Tabel 2.4 : Perbandingan nilai BSM antara citra kosong dengan citra stego

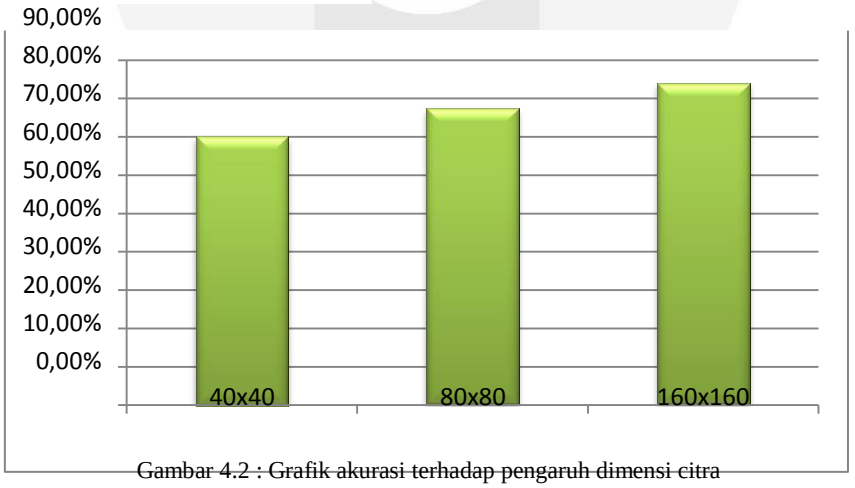
Fitur BSM	Citra kosong	10kb teks	20kb teks	40kb teks
Sokal & Sneath Similarity Measure 1	0,719305751	0,734521413	0,691687336	0,682700721
Sokal & Sneath Similarity Measure 2	0,274711691	0,267740766	0,20860146	0,203577164
Kulczynski Similarity Measure 1	0,757524111	0,731273169	0,527171708	0,511228848
Sokal & Sneath Similarity Measure 3	1,281297626	1,383391067	1,121730333	1,075799357
Sokal & Sneath Similarity Measure 4	2,228008078	2,319865815	2,112842668	2,071758208
Sokal & Sneath Similarity Measure 5	0,30819088	0,33616649	0,278781982	0,26810793
Ochiai Similarity Measure	0,602393309	0,593916271	0,513226468	0,505552081
Binary Lance & Williams Nonmetric Dissimilarity Measure	0,397606691	0,406083729	0,486773532	0,494447919
Pattern Difference	0,048037026	0,0440098	0,055534087	0,05801887
Variance Dissimilarity Measure	1,739442437	1,664932775	1,870259307	1,911642321
Binary Minimum Histogram Difference	0,976513755	0,966781153	0,91229694	0,909642594
Binary Absolute Histogram Difference	0,04697249	0,066437694	0,17540612	0,180714812
Binary Mutual Entropy	0,59228892	0,594742136	0,602198032	0,602559368
Binary Kullback-Leibler Distance	-4,95E-04	-1,57E-03	-8,53E-03	-8,93E-03

Dapat dilihat pada tabel hasil ekstraksi di atas bahwa semakin besar teks sisipan makin besar juga perubahan nilai ekstraksi BSM yang diperoleh. Hal tersebut juga mempengaruhi tingkat akurasi yang berbanding lurus dengan besar teks yang disisipkan

3.2 Pengaruh Besar Dimensi Citra Digital

Pada analisis kali ini dilakukan analisis terhadap 3 data uji yang dibedakan berdasarkan dimensi citra digital yang disisipi objek stego berupa teks sebesar 40kb. Dimensi citra yang akan diuji yaitu tidak lebih dari 40x40 pixel, 80x80 pixel, dan 160x160 pixel.

Pada proses ini, akan diuji 300 set data uji yang akan dibagi 3 sesuai dimensi citra yang diujikan. Dan data uji tersebut akan dibagi 2 yaitu citra kosong dan citra stego. Lalu akan diukur tingkat akurasi steganalisis jika citra cover-nya memiliki ukuran yang berbeda.



Gambar 4.2 : Grafik akurasi terhadap pengaruh dimensi citra

Dapat dilihat pada grafik – yang terdapat diatas bahwa semakin besar ukuran file teks yang disisipkan, makin besar pula akurasi yang didapatkan. Untuk citra dengan dimensi 40x40 pixel memiliki akurasi 70%, untuk citra dengan dengan dimensi 80x80 pixel memiliki akurasi 77,43%, dan untuk citra dengan dimensi 160x160 pixel memiliki akurasi 84%. Bisa dilihat melalui data ekstraksi HMM yang telah diperoleh seperti berikut :

Tabel 2.5 : Perbandingan nilai BSM pada citra berukuran 40x40 pixel

Fitur BSM	citra 1	citra 1 stego	citra 2	citra 2 stego
Sokal & Sneath Similarity Measure 1	0,66560	0,70922	0,66233	0,68379
Sokal & Sneath Similarity Measure 2	0,19913	0,22055	0,19757	0,18083
Kulczynski Similarity Measure 1	0,49730	0,56592	0,49243	0,44150
Sokal & Sneath Similarity Measure 3	0,99523	1,21951	0,98076	1,08121
Sokal & Sneath Similarity Measure 4	1,99522	2,19499	1,98056	2,06045
Sokal & Sneath Similarity Measure 5	0,24881	0,30081	0,24516	0,26321
Ochiai Similarity Measure	0,49865	0,53092	0,49619	0,46893
Binary Lance & Williams Nonmetric Dissimilarity Measure	0,50135	0,46908	0,50381	0,53107
Pattern Difference	0,06280	0,05075	0,06372	0,05772
Variance Dissimilarity Measure	1,88234	1,69213	1,89609	1,80458
Binary Minimum Histogram Difference	0,97627	0,95413	0,99459	0,93566
Binary Absolute Histogram Difference	0,04746	0,09173	0,01083	0,12868
Binary Mutual Entropy	0,60211	0,60429	0,60199	0,60658
Binary Kullback-Leibler Distance	-5,28E-04	-0,002255125	-3,44E-05	-4,65E-03

Tabel 2.6 : Perbandingan nilai BSM pada citra berukuran 80x80 pixel

Fitur BSM	citra 1	citra 1 stego	citra 2	citra 2 stego
Sokal & Sneath Similarity Measure 1	0,672452	0,707742	0,665052	0,687019
Sokal & Sneath Similarity Measure 2	0,185025	0,206147	0,201634	0,197414
Kulczynski Similarity Measure 1	0,454064	0,519359	0,505117	0,491946
Sokal & Sneath Similarity Measure 3	1,026492	1,210819	0,992771	1,097539
Sokal & Sneath Similarity Measure 4	2,019389	2,179685	1,992590	2,087389
Sokal & Sneath Similarity Measure 5	0,254034	0,295684	0,248132	0,271653
Ochiai Similarity Measure	0,475926	0,509496	0,502545	0,495940
Binary Lance & Williams Nonmetric Dissimilarity Measure	0,524074	0,490504	0,497455	0,504060
Pattern Difference	0,060877	0,051149	0,062954	0,056822
Variance Dissimilarity Measure	1,903908	1,745170	1,938164	1,841356
Binary Minimum Histogram Difference	0,987470	0,969858	0,983039	0,962403
Binary Absolute Histogram Difference	0,025060	0,060283	0,033922	0,075194
Binary Mutual Entropy	0,600789	0,600579	0,602261	0,603590
Binary Kullback-Leibler Distance	-0,000164597	-8,02E-04	-4,48E-04	-1,54E-03

Tabel 2.7 : Perbandingan nilai BSM pada citra berukuran 160x160 pixel

Fitur BSM	citra 1	citra 1 stego	citra 2	citra 2 stego
Sokal & Sneath Similarity Measure 1	0,68452	0,68745	0,66697	0,69671
Sokal & Sneath Similarity Measure 2	0,23169	0,21221	0,19689	0,19916
Kulczynski Similarity Measure 1	0,60311	0,53876	0,49031	0,49739
Sokal & Sneath Similarity Measure 3	1,08487	1,09974	1,00137	1,14857
Sokal & Sneath Similarity Measure 4	2,07490	2,09479	2,00115	2,12871
Sokal & Sneath Similarity Measure 5	0,26829	0,27423	0,25026	0,28209
Ochiai Similarity Measure	0,54673	0,51865	0,49511	0,49869
Binary Lance & Williams Nonmetric Dissimilarity Measure	0,45327	0,48135	0,50489	0,50131
Pattern Difference	0,05752	0,05670	0,06241	0,05416
Variance Dissimilarity Measure	1,88861	1,87523	1,96960	1,83465

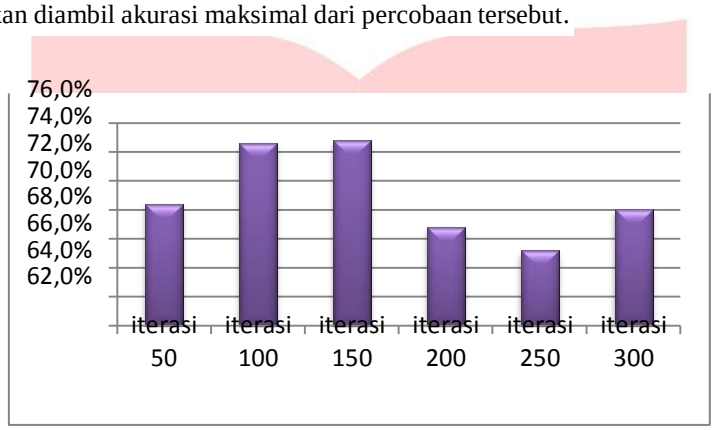
Binary Minimum Histogram Difference	0,99901	0,96480	0,99858	0,94976
Binary Absolute Histogram Difference	0,00198	0,07040	0,00283	0,10049
Binary Mutual Entropy	0,60022	0,60241	0,60204	0,60474
Binary Kullback-Leibler Distance	-1,24E-06	-1,68E-03	-2,85E-06	-2,69E-03

Dapat dilihat pada tabel hasil ekstraksi di atas bahwa semakin besar dimensi citra makin besar juga perubahan nilai ekstraksi BSM yang diperoleh. Dikarenakan semakin besar dimensi pada citra, semakin mudah untuk menghitung perbedaan LSB pada bitplane yang tersisipi.

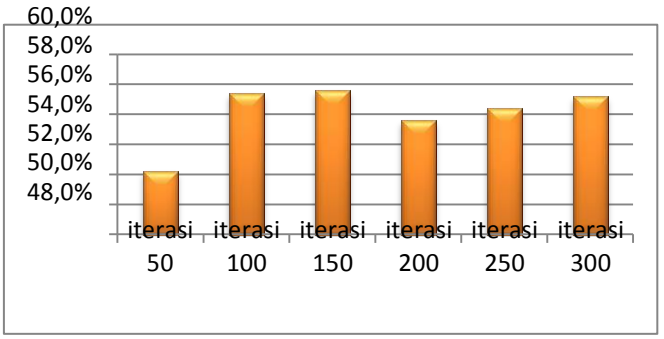
3.3 Pengaruh Parameter iterasi pada Klasifikasi

Pada analisis kali ini dilakukan analisis pengaruh perubahan parameter iterasi terhadap kehandalan klasifikasi HMM. Akan dianalisis dari iterasi 50 hingga 300 dengan kelipatan 50.

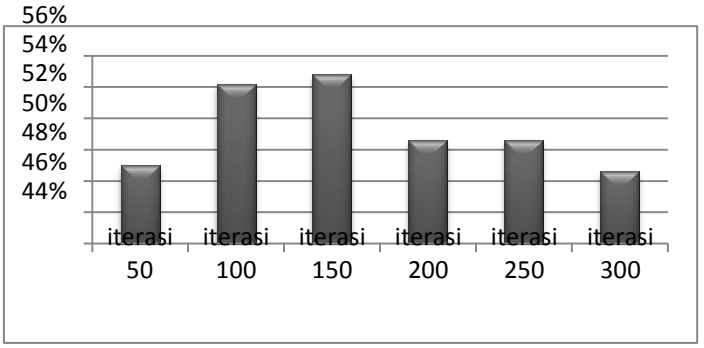
Pada proses ini, akan diuji 300 set data uji yang akan dilatih terlebih dahulu sehingga didapat model data menurut besar teks sisipan yaitu 10kb, 20kb, dan 40kb. Setelah diapat data ekstraksi akan diproses oleh HMM dengan mengubah-ubah parameter iterasi. Lalu akan diukur tingkat akurasi steganalisis jika parameter-parameter tersebut diubah, dan akan diambil akurasi maksimal dari percobaan tersebut.



Gambar 4.3 : Grafik akurasi perubahan iterasi terhadap citra dengan sisipan 40kb



Gambar 4.4 : Grafik akurasi perubahan iterasi terhadap citra dengan sisipan 20kb



Gambar 4.5 : Grafik akurasi perubahan iterasi terhadap citra dengan sisipan 10kb

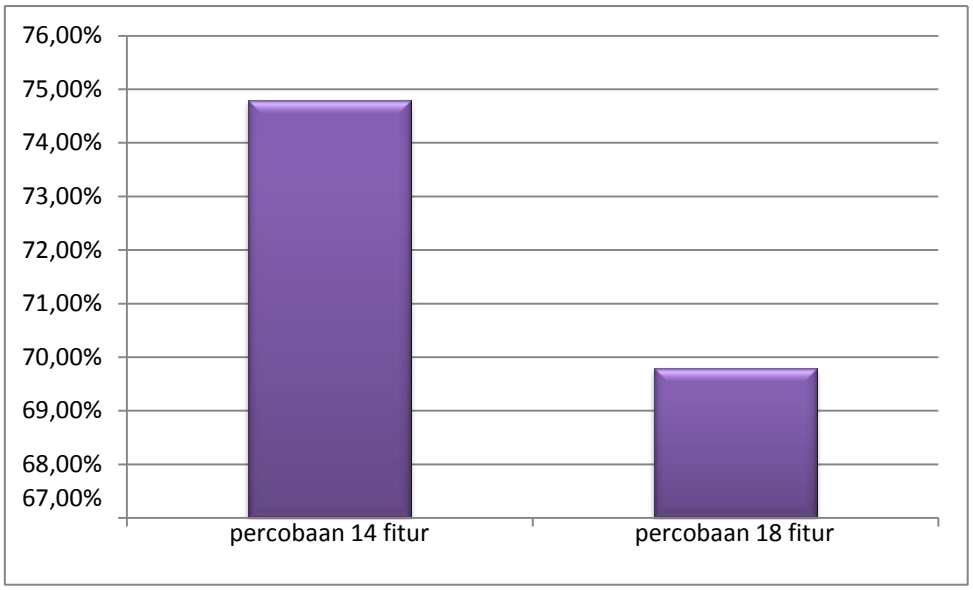
Pada ketiga grafik diatas dapat dilihat bahwa akurasi terbesar didapat saat di iterasi 150. Hal tersebut mengacu pada konvergensi HMM untuk menentukan model terbaik. Dari sekian banyak iterasi yang diujikan,

terbukti iterasi yang tepat digunakan dengan tingkat akurasi paling baik adalah 150. Maka iterasi yang akan digunakan untuk percobaan selanjutnya adalah sebesar 150.

3.4 Pengaruh Penggunaan 14 Fitur dan 18 Fitur BSM

Pada analisis kali ini dilakukan analisis perbandingan antara penggunaan 14 fitur BSM dan 18 fitur BSM. Pada referensi Jin-Qu Lin [1] penggunaan parameter BSM ke-15 sampai ke 18 tidak membantu classifier berjalan dengan baik. Hal tersebut dikarenakan nilai dari fitur ke-15 sampai 18 tidak stabil pada satu skala perhitungan. Sehingga membuat akurasi tidak maksimal.

Pada percobaan kali ini akan di tes perbandingan akurasi pengaruh penguunaan fitur BSM dengan teks sisipan 40kb menggunakan metode steganografi LSB serta iterasi sebesar 150.



Gambar 4.6 : Grafik akurasi perbandingan penggunaan fitur BSM

Pada grafik diatas dapat dilihat bahwa penggunaan 14 fitur BSM lebih dapat meningkatkan performa akurasi hingga sebesar 74,80%, sedangkan penggunaan 18 fitur BSM hanya mencapai akurasi 69,80%. Hal ini membuktikan bahwa perhitungan fitur BSM ke-15 sampai 18 tidak membantu classifier bekerja dengan maksimal sesuai percobaan Jing-Qu Lin [1]. Sehingga untuk memaksimalkan akurasi steganalisis cukup menggunakan 14 fitur BSM.

4. Kesimpulan

Berdasarkan hasil pengujian dan analisis pada percobaan tugas akhir ini, diperoleh kesimpulan sebagai berikut :

1. Semakin besar ukuran file yang disisipkan ke citra digital, maka semakin mudah dideteksi, karena perbedaan nilai dari fitur BSM antara citra kosong dengan citra stego semakin besar. Hal ini terbukti oleh percobaan dengan akurasi sebesar 74,80% untuk citra dengan sisipan teks berukuran 40kb.
2. Semakin besar dimensi citra yang disisipi maka semakin mudah untuk mendeteksi pesan rahasiadi dalam citra. Hal tersebut dibuktikan dengan tingkat akurasi sebesar 84% dengan dimensi citra 160x160 pixel.
3. Iterasi yang konvergen untuk program steganalisis ini adalah 150, hal tersebut dibuktikan pada percobaan skenario 4.4.3 dengan tingkat akurasi tertinggi pada ketiga percobaan.
4. Penggunaan fitur-fitur ekstraksi pada BSM akan berjalan dengan baik dan memaksimalkan kinerja classifier jika perhitungan fitur ke-15 sampai 18 diabaikan. Hal tersebut dibuktikan dengan meningkatnya akurasi steganalisis hingga 74,80%.

5. Saran

Adapun saran yang dapat diberikan antara lain :

1. Dapat diteliti lebih lanjut untuk mendeteksi media lain misal audio, video ataupun dokumen.
2. Dapat menggunakan metode steganografi yang lain misal F5, Jsteg, SilentEye, dan OutGuess.
3. Dapat menggunakan citra dengan format lain misal GIF dan BMP.
4. Dapat mengunakan metode klasifikasi lain seperti FuzzyLogic dan JST.

DAFTAR REFERENSI

[1] Lin, Jing-Qu. Zhong, Shang-Ping. 2009. *JPEG Image Steganalysis Method Based On Binary Similarity Measures*. IEEE, Fuzhou University, China.

[2] Munir, Rinaldi.2006. *Diktat Kuliah Informatika Kriptografi : Steganografi dan Watermarking*. Informatika, Institut Teknologi Telkom, Bandung.

[3] Nugraha, Anindito Setya.2013.*Implementasi Steganalisis dengan Menggunakan Metode Binary Similarity Measures-Support Vector Machine pada Steganografi Citra Digital*. Tugas Akhir Program Sarjana Institut Teknologi Telkom, Bandung.

[4] Prarian, Cahyo. 2013. *Analisis Pengenalan Aksara Lampung Menggunakan Modified Direction Feature (MDF) dan Hidden Markov Model*. Tugas Akhir Program Sarjana Institut Teknologi Telkom, Bandung.

[5] Rabiner, Lawrence R. 1989. *A Tutorial on Hidden Markov Models and Selected Application in Speech Recognition*. IEEE, Vol.77, No.2, February 1989.

[6] Avcibas, Ismail. 2002. *Image Steganalysis with Binary Similarity Measures. IEEE, Uludag University, Turkey*.

[7] Yuwitaning, Eka Farda. 2014. *Implementasi Metode Hidden Markov Model Untuk Deteksi Tulisan Tangan*. Tugas Akhir Program Sarjana Universitas Telkom, Bandung.

[8] Prasetyo, Muhammad Eko Budi. 2010. *Teori Dasar Hidden Markov Model.Makalah II2092 Probabilitas dan Statistik*.Institut Teknologi Bandung, Bandung.

[9] Elfitri, Ikhwana. 2008. *Kuantisasi Vektor : Definisi dan Kinerja*.Jurnal TeknikA.Unand, Padang

[10] Zou, Dekun. et al. 2006. *Steganalysis Based on Markov Model of Thresholded Prediction-Error Image*. IEEE. New Jersey Institute of Technology, USA.

[11] Handoko, Ronny. 2014. *Steganalisis Citra Digital Menggunakan Metode Discrete Wavelet Transform dan K-Nearest Neighbor*. Tugas Akhir Program Sarjana. Universitas Telkom, Bandung.

[12] Hartono, Meilissa Pratiwi. 2014. *Simulasi Steganalisis Citra Digital Berbasis Domain Discrete Cosine Transform dan Domain Spasial*. Tugas Akhir Program Sarjana. Universitas Telkom, Bandung.

[13] Cha, Sung-Hyuk. et al. 2005. *On Binary Similarity Measures for Handwritten Character Recognition*. IEEE. Pace University, New York, USA.

[14] Broda, Martin. et al. 2014. *Universal Image Steganalytic Method Based on Binary Similarity Measures*. IEEE. Technical University of Kosice, Slovak Republic.

[15] Baryam, Sevnic. et al. *Image Manipulation Detection with Binary Similarity Measures*. Uludang University, Turkey.

[16] Battula, Bhanu Prakash. Prasad, R. Satya. *Essentials of Binary Similarity Measures*. JATIT. Vignan's Nirula Institute of Technology and Science, Acharya Nagarjuna University, Andhra Pradesh, India.

[17] Sujatha, P. Kolvankar, Shivranjan. *Performance Study of Image Steganalysis*. Vels University, Chennai, India

[18] Bertalya. 2005. *Representasi Citra*. Materi Perkuliahan. Universitas Gunadarma, Senen, DKI Jakarta.