Steganalisis LSB Matching pada Citra Berwarna

Dindin Dhino Alamsyah[1], Rimba Whidiana Ciptasari[2], Febryanti Sthevanie[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]dindhino@student.telkomuniversity.ac.id, [2]rimbawh@telkomuniversity.ac.id,
[3]sthevanie@telkomuniversity.ac.id

Abstrak

***Least Significant Bit* (LSB) *matching* steganografi merupakan teknik untuk menyembunyikan informasi pada citra digital dengan menyisipkan bit-bit pesan pada bit-bit terakhir data piksel. Dengan kehadiran steganografi yang berkembang cepat, diperlukan teknik steganalisis untuk mengawasi pertukaran data yang terjadi pada jaringan komunikasi karena adanya pelaku kriminal yang menggunakan steganografi untuk merencanakan kejahatan.**

Terdapat sebuah referensi teknik steganalisis *Least Significant Bit* (LSB) *matching* yang memiliki kekurangan sehingga menyebabkan penurunan tingkat deteksi. Teknik steganalisis tersebut menggunakan daerah *plain* pada citra keabuan dengan pengambilan daerah plain menggunakan *DCT-based block classification* dan normalisasi histogram yang mengakibatkan hilangnya beberapa informasi. Dalam Tugas Akhir ini, diusulkan teknik steganalisis LSB *matching* pada citra berwarna dengan mempertimbangkan daerah *non-plain* untuk memperbaiki tingkat deteksi menggunakan *fuzzy logic*.

Hasil evaluasi menunjukkan bahwa sistem yang dibangun pada penelitian ini mampu mendeteksi LSB *matching* steganografi dengan ukuran *payload* mulai dari 15% berdasarkan distorsi *incidental attack* dengan jenis *salt & pepper* dengan *noise density* sebesar 0.05 yang akurasinya mencapai 94.75%.

Kata kunci : steganalisis, citra berwarna digital, LSB matching, fuzzy logic.

Abstract

Least Significant Bit (LSB) matching steganography is an information hiding technique on digital image by inserting message bits in the last bits of pixel data. With the presence of rapidly evolving steganography, steganalysis technique requires to keep an eye on data exchange that occurs in communication network because of criminals who use steganography to plan crime.

The existing research on LSB matching steganalysis has disadvantages that lead to decrease in detection rate. That steganalysis technique uses plain areas on grayscale image by taking plain areas using DCT-based block classification and normalize the histogram resulting in loss of some information. This research proposes a steganalysis technique on color image by considering non-plain areas to fix the detection rate using fuzzy logic.

Evaluation result shows that the proposed system is able to detect LSB matching steganography with payload size start from 15% on salt and pepper noise incidental attack with noise density 0.05. The accuracy on incidental attack distortion achieve 94.75%.

Keywords: steganalysis, digital color image, LSB matching, fuzzy logic.

1. Pendahuluan

Latar Belakang

Steganalisis adalah ilmu yang mempelajari karakteristik penyembunyian informasi dalam suatu objek dan mempelajari bagaimana cara untuk mendeteksi adanya informasi tersebut [1]. Terdapat dua jenis steganalisis, yaitu *blind steganalysis* dan *targeted steganalysis*. Dalam Tugas Akhir ini, jenis steganalisis yang dibahas adalah *targeted steganalysis* dimana teknik penyembunyian informasi diasumsikan diketahui menggunakan *Least Significant Bit* (LSB) *matching* steganografi.

LSB *matching* steganografi menggunakan kelemahan mata manusia dalam mendeteksi perbedaan warna. Cara kerja dari metode tersebut adalah menyisipkan bit-bit pesan pada bit-bit terakhir data piksel pada citra digital [2].

Dengan kehadiran steganografi yang berkembang cepat, diperlukan suatu cara untuk mengawasi pertukaran data yang terjadi pada jaringan komunikasi dengan tujuan untuk mengetahui ada tidaknya informasi tersembunyi.

Hal ini dilatarbelakangi oleh adanya pelaku kriminal yang menggunakan steganografi untuk merencanakan kejahatan.

Perumusan Masalah

Berdasarkan studi literatur terhadap literatur [2], dirumuskan beberapa permasalahan, yaitu pendeteksian LSB *matching* steganografi dilakukan menggunakan daerah *plain* pada citra keabuan. Pengambilan daerah *plain* dilakukan menggunakan *DCT-based block classification* dan normalisasi histogram yang menyebabkan hilangnya beberapa informasi sehingga dapat terjadinya penurunan tingkat deteksi.

Berdasarkan kondisi tersebut, hal yang penting untuk diselesaikan dalam Tugas Akhir ini adalah pendeteksian LSB *matching* steganografi pada citra berwarna digital dengan mempertimbangkan daerah non-*plain*.

Tujuan

Tujuan dari Tugas Akhir ini adalah membangun model steganalisis LSB *matching* pada citra berwarna digital dengan mempertimbangkan daerah non-*plain* yang dapat digunakan untuk mendeteksi ada tidaknya informasi tersembunyi menggunakan *fuzzy logic* karena *fuzzy logic* dapat menangani data yang kurang presisi dan data yang memiliki kebenaran parsial dengan membangun *membership function* dan aturan *fuzzy* berdasarkan pengamatan data.

Organisasi Tulisan

Tugas Akhir ini disusun dengan struktur sebagai berikut. Setelah dijelaskan pendahuluan pada bagian pertama, dijelaskan pemodelan sistem pada bagian kedua. Selanjutnya, dijelaskan evaluasi performansi sistem terhadap sistem yang dibangun pada bagian ketiga. Setelah itu, dijelaskan kesimpulan dan saran untuk penelitian selanjutnya pada bagian keempat.

2. Pemodelan Sistem: Steganalisis LSB Matching Citra Berwarna

Secara umum, sistem yang dibangun terdiri dari pembangunan model LSB *matching* dan pendeteksian LSB *matching*. Dalam pembangunan model, gambar tes yang dapat berupa *stego-object* atau *cover-object* dilakukan proses per *channel* (*channel red*, *channel green*, dan *channel blue*) sehingga pendeteksian dilakukan dengan dua kali *fuzzy logic*, yaitu untuk penggabungan model tiap *channel* dan penggabungan *channel*.

2.1 Pembangunan Model LSB Matching

2.1.1 LSB Matching Steganografi

Dalam literatur [2], dijelaskan bahwa LSB matching steganografi atau ± 1 *embedding* adalah teknik penyembunyian informasi dengan membandingkan antara bit pesan yang akan disembunyikan dengan bit terakhir pada piksel dari *cover-object*. Jika kedua bit tersebut berbeda, nilai piksel pada *cover-object* ditambah satu atau dikurang satu sesuai dengan bit pesan yang akan disembunyikan. Dalam literatur [3], dijelaskan bahwa distorsi akibat *non-adaptive* $\pm k$ *embedding* dimodelkan sebagai *additive noise* η dengan *Probability Density Function* (PDF) $p \in [0,1]$ sehingga $P(\eta = 0) = 1 - \frac{p}{2}$ dan $P(\eta = k) = P(\eta = -k) = \frac{p}{4}$.

2.1.2 Model Steganalisis LSB Matching

2.1.2.1 Analisis Tekstur dengan *Gray-level Co-occurrence Matrix* (GLCM)

Tingkat keabuan dalam piksel yang bertetangga dalam sebuah gambar sangat berkorelasi dan GLCM dari sebuah gambar cenderung terdistribusi secara diagonal. Setelah penyisipan data, konsentrasi tinggi di sepanjang matriks diagonal utama dari GLCM menyebar karena korelasi tinggi antara piksel pada gambar asli telah berkurang. Dalam literatur [4], dijelaskan bahwa GLCM merupakan salah satu metode untuk melakukan identifikasi suatu citra dengan menghitung kemunculan hubungan ketetanggan antara dua intensitas piksel pada orientasi sudut dan jarak atau *range* tertentu.

Dalam Tugas Akhir ini, digunakan nilai θ sebesar 0° dalam satu piksel dengan ukuran GLCM sebesar 8x8. Setelah terbentuknya matriks GLCM, dilakukan perhitungan *contrast*, *correlation*, *energy*, dan *homogeneity* [4] untuk mengekstrak beberapa fitur dari gambar tersebut.

2.1.2.2 *Center of Mass* dari *Histogram Characteristic Function* (HCF-COM)

Berdasarkan pengamatan data, *cover-object* memiliki komponen frekuensi tinggi yang lebih banyak dibandingkan dengan histogram *stego-object*-nya. Oleh karena itu, nilai *Center of Mass* dari *cover-object* akan bernilai lebih

besar daripada *Center of Mass* dari *stego-object*. Dalam literatur [5], dibuktikan bahwa dalam LSB *Matching*, histogram dari *stego-object* sama dengan konvolusi antara histogram *cover-object* dan *Probability Mass Function* (PMF) dari *stego-noise* yang disebabkan oleh data yang disembunyikan. Pembuktian tersebut diberikan oleh persamaan (1).

$$h_s[n] = h_c[n] * f_\Delta[n], \qquad n = [1,255] \tag{1}$$

Dimana $h_s[n]$ adalah histogram *stego-object*, $h_c[n]$ adalah histogram *cover-object*, $f_\Delta[n]$ adalah PMF dari *stego-noise*, dan * melambangkan konvolusi. Dengan menerapkan *Discrete Fourier Transform* (DFT) pada persamaan (1), diperoleh persamaan (2).

$$H_s[k] = F_\Delta[k]H_c[k] \tag{2}$$

Dimana H_s, H_c, dan F_Δ adalah *Histogram Characteristic Function* (HCF). Untuk mengukur distribusi energi pada HCF dari H_s dan H_c digunakan *Center of Mass* dari *Histogram Characteristic Function* (HCF-COM) yang diberikan oleh persamaan (3).

$$C(H[k]) = \frac{\sum_{k\in K} k|H[k]|}{\sum_{i\in K}|H[i]|} \tag{3}$$

2.2 Pendeteksian LSB Matching

Setelah dilakukan pembangunan model, langkah selanjutnya adalah pendeteksian dengan penggabungan model tiap *channel* dan penggabungan *channel* menggunakan metode *fuzzy logic* yang dijelaskan pada literatur [6]. Tiap-tiap fitur dilakukan proses fuzzifikasi menggunakan *membership function* sebagai berikut.

1. Struktur *membership function* untuk *contrast*

$$Tinggi(x) = \begin{cases} 0, & \text{if } x \le 0 \\ \dfrac{x-0}{0.6-0}, & \text{if } 0 < x < 0.6 \\ 1, & \text{otherwise} \end{cases} \qquad Rendah(x) = \begin{cases} 1, & \text{if } x \le 0 \\ \dfrac{0.6-x}{0.6-0}, & \text{if } 0 < x < 0.6 \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

2. Struktur *membership function* untuk *correlation*

$$Positif(x) = \begin{cases} 1, & \text{if } x \le 0.16 \\ \dfrac{0.89-x}{0.89-0.16}, & \text{if } 0.16 < x < 0.89 \\ 0, & \text{otherwise} \end{cases} \qquad Negatif(x) = \begin{cases} 0, & \text{if } x \le 0.16 \\ \dfrac{x-0.16}{0.89-0.16}, & \text{if } 0.16 < x < 0.89 \\ 1, & \text{otherwise} \end{cases} \tag{5}$$

3. Struktur *membership function* untuk *energy*

$$Tinggi(x) = \begin{cases} 0, & \text{if } x \le 0 \\ \dfrac{x-0}{1-0}, & \text{if } 0 < x < 1 \\ 1, & \text{otherwise} \end{cases} \qquad Rendah(x) = \begin{cases} 1, & \text{if } x \le 0 \\ \dfrac{1-x}{1-0}, & \text{if } 0 < x < 1 \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

4. Struktur *membership function* untuk *homogeneity*

$$Tinggi(x) = \begin{cases} 0, & \text{if } x \le 0.87 \\ \dfrac{x-0.87}{1-0.87}, & \text{if } 0.87 < x < 1 \\ 1, & \text{otherwise} \end{cases} \qquad Rendah(x) = \begin{cases} 1, & \text{if } x \le 0.87 \\ \dfrac{1-x}{1-0.87}, & \text{if } 0.87 < x < 1 \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

5. Struktur *membership function* untuk HCF-COM

$$Tinggi(x) = \begin{cases} 0, & \text{if } x \le 127.4 \\ \dfrac{x-127.4}{127.5-127.4}, & \text{if } 127.4 < x < 127.5 \\ 1, & \text{otherwise} \end{cases} \qquad Rendah(x) = \begin{cases} 1, & \text{if } x \le 127.4 \\ \dfrac{127.5-x}{127.5-127.4}, & \text{if } 127.4 < x < 127.5 \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

Hasil fuzzifikasi dari kelima fitur tersebut dilakukan proses *inference* dalam aturan yang terlampir pada Tabel 1 dengan operator *conjunction* dan *disjunction*. Hasil dari proses *inference* yang berupa label dan nilai dilakukan proses defuzzifikasi menggunakan *weighted average* untuk mendapatkan nilai *crisp*. Nilai dari hasil *inference* digunakan sebagai bobot (*weight*) sedangkan label dari hasil *inference* diberi nilai kelayakan sebesar 0 untuk label *cover* dan 100 untuk label *stego*.

Sampai tahap ini, diperoleh tiga nilai *crisp*, yaitu nilai *crisp* untuk *channel red*, nilai *crisp* untuk *channel green*, dan nilai *crisp* untuk *channel blue*. Selanjutnya, ketiga nilai tersebut dilakukan proses fuzzifikasi kembali menggunakan *membership function* pada Persamaan (9).

$$Rendah(x) = \begin{cases} 1, & \text{if } x \leq 45 \\ \dfrac{96-x}{96-45}, & \text{if } 45 < x < 96 \\ 0, & \text{otherwise} \end{cases} \qquad Tinggi(x) = \begin{cases} 0, & \text{if } x \leq 45 \\ \dfrac{x-45}{96-45}, & \text{if } 45 < x < 956 \\ 1, & \text{otherwise} \end{cases} \tag{9}$$

Hasil fuzzifikasi dari ketiga nilai tersebut dilakukan proses *inference* dalam aturan yang terlampir pada Tabel 2 dengan operator *conjunction* dan *disjunction*. Hasil dari proses *inference* yang berupa label dan nilai dilakukan proses defuzzifikasi menggunakan *weighted average* untuk mendapatkan nilai *crisp*. Nilai dari hasil *inference* digunakan sebagai bobot (*weight*) sedangkan label dari hasil *inference* diberi nilai kelayakan sebesar 0 untuk label *cover* dan 1 untuk label *stego*.

Sampai tahap ini, diperoleh satu nilai *crisp* yang digunakan sebagai nilai prediksi. Nilai prediksi tersebut dilakukan *thresholding* untuk menentukan apakah gambar tes termasuk *stego-object* atau *cover-object*.

3. Evaluasi

3.1 Dataset

Dataset yang digunakan dalam Tugas Akhir ini menggunakan *dataset* yang diambil dari *Computer Vision Laboratory, ETH Zurich* [7] (dapat diakses pada `https://www.kaggle.com/kmader/food41/data`). Dalam *dataset* tersebut, terdapat 1000 citra berwarna yang disimpan di *Hierarchical Data Format* (HDF) dalam format .h5 dengan ukuran 384x384 piksel. Dari 1000 gambar tersebut, dipilih 200 gambar secara acak untuk membangun *dataset testing cover-object*, 800 gambar lainnya digunakan untuk pengamatan.

Pembangunan *dataset stego-object* dilakukan dengan menyembunyikan informasi (*ciphertext* dalam biner) pada *cover-object* menggunakan metode LSB *Matching* dengan ukuran *payload* 15%, 25%, 50%, 75%, dan 100%. *Dataset stego-object* juga dibangun berdasarkan jenis distorsi *incidental attack* dan *intentional attack*. *Incidental attack* dilakukan dengan menambahkan *noise* pada setiap gambar menggunakan jenis *salt & pepper* dengan *noise density* sebesar 0.05, *gaussian* dengan *variance* sebesar 0.01, dan *poisson*. *Intentional attack* dilakukan dengan *scaling* dengan ukuran 0.5, *rotate & crop* dengan sudut sebesar 45°, dan *compression* menggunakan *Discrete Cosine Transform* (DCT).

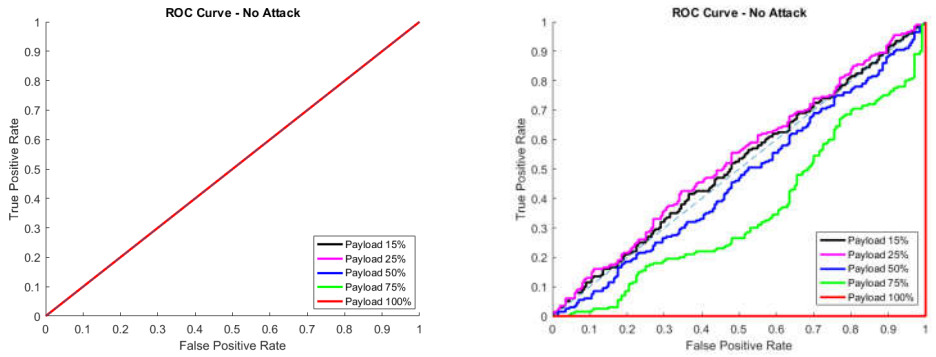
Total citra yang dibangun untuk *datates testing* berjumlah 14000 data yang terdiri atas 7000 data *cover-object* dan 7000 data *stego-object*. Sampel *dataset* yang dibangun terlampir pada Gambar 8.

3.2 Skenario Pengujian

Skenario pengujian dalam Tugas Akhir ini adalah mendeteksi ada tidaknya informasi tersembunyi pada citra berwarna digital dengan ukuran *payload* 15%, 25%, 50%, 75%, dan 100%. Selain *payload*, pendeteksian juga dilakukan berdasarkan jenis distorsi *incidental atack* dan *intentional attack*. Performansi sistem dievaluasi menggunakan *Receiver Operating Characteristic* (ROC) *Curve* yang dijelaskan dalam literatur [8] dan literatur [9]. Berdasarkan *Receiver Operating Characteristic* (ROC) *Curve* yang terbentuk, dapat dilakukan perhitungan *Area Under the Curve* (AUC) untuk mengukur performansi sistem yang perhitungannya dijelaskan pada literatur [10] dan literatur [11].

3.3 Pengujian dan Analisis Terhadap Payload

Setelah dilakukan pengujian terhadap *payload* menggunakan metode pada penelitian ini dan menggunakan metode pada penelitian sebelumnya dengan dataset yang telah disebutkan, perbandingan hasil performansi sistem dapat dilihat pada Gambar 1.



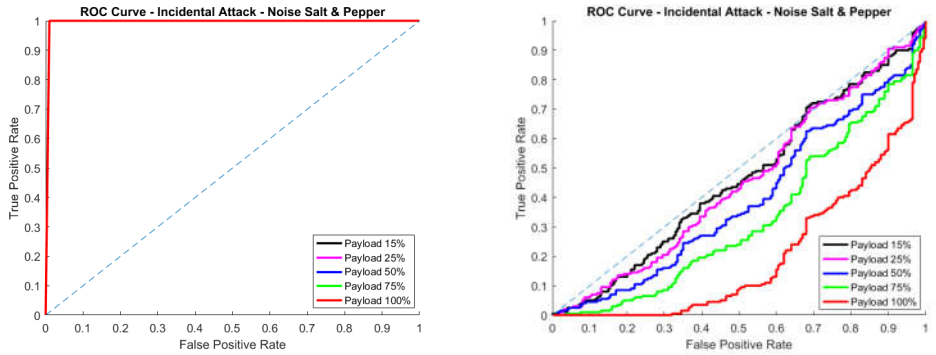
(a) Menggunakan metode pada penelitian saat ini. (b) Menggunakan metode pada penelitian sebelumnya.

Gambar 1. ROC *curve* yang dihasilkan terhadap *payload*.

Detail informasi terhadap ROC Curve pada Gambar 1 terlampir pada Tabel 3. Berdasarkan Tabel 3, performansi sistem yang dibangun pada penelitian ini kurang bagus untuk mendeteksi LSB *matching* steganografi dengan *payload* mulai dari 15% karena memiliki rata-rata akurasi sebesar 50%, data *stego* yang terklasifikasi dengan benar sebesar 10.5%, dan data *cover* yang salah terklasifikasi sebesar 10.5%. Hal ini terjadi karena adanya data yang *overlap* dalam beberapa fitur yang menyebabkan tidak terdeteksi adanya informasi tersembunyi.

3.4 Pengujian dan Analisis Terhadap Incidental Attack dengan jenis *Salt & Pepper*

Setelah dilakukan pengujian terdahap *incidental attack* dengan jenis *salt & pepper* menggunakan metode pada penelitian ini dan menggunakan metode pada penelitian sebelumnya dengan dataset yang telah disebutkan, perbandingan hasil performansi sistem dapat dilihat pada Gambar 2.



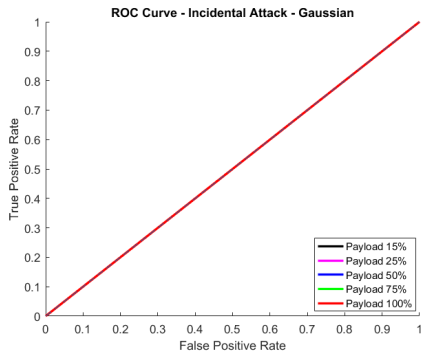
(a) Menggunakan metode pada penelitian saat ini. (b) Menggunakan metode pada penelitian sebelumnya.

Gambar 2. ROC *curve* yang dihasilkan terhadap *incidental attack* dengan jenis *salt & pepper*.

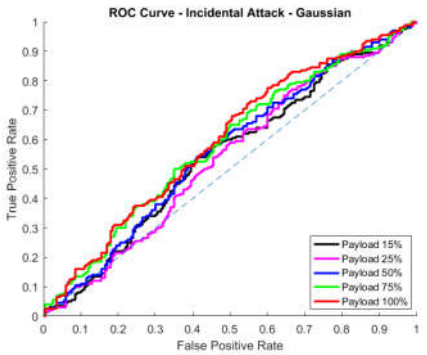
Detail informasi terhadap ROC Curve pada Gambar 2 terlampir pada Tabel 4. Berdasarkan Tabel 4, performansi sistem yang dibangun pada penelitian ini bagus untuk mendeteksi LSB *matching* steganografi berdasarkan *incidental attack* jenis *salt & pepper* dengan *payload* mulai dari 15% karena memiliki rata-rata akurasi sebesar 94.75%, data *stego* yang terklasifikasi dengan benar sebesar 100%, dan data *cover* yang salah terklasifikasi sebesar 10.5%. *Incidental attack* jenis *salt & pepper* mengubah nilai piksel menjadi 0 atau 255 sekitar 5% dari ukuran piksel. Dengan adanya transformasi *fourier* dalam perhitungan *center of mass*, transformasi *fourier* tersebut dapat digunakan sebagai *noise filtering* yang menyebabkan dapat terdeteksi adanya informasi tersembunyi.

3.5 Pengujian dan Analisis Terhadap Incidental Attack dengan jenis *Gaussian*

Setelah dilakukan pengujian terdahap *incidental attack* dengan jenis *gaussian* menggunakan metode pada penelitian ini dan menggunakan metode pada penelitian sebelumnya dengan dataset yang telah disebutkan, perbandingan hasil performansi sistem dapat dilihat pada Gambar 3.



(a) Menggunakan metode pada penelitian saat ini.



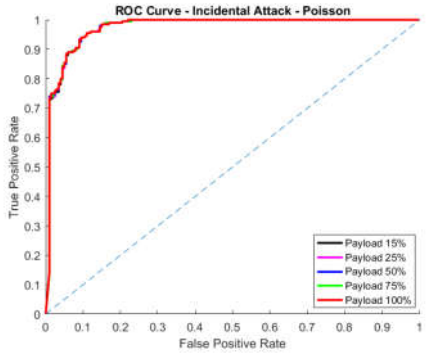
(b) Menggunakan metode pada penelitian sebelumnya.

Gambar 3. ROC *curve* yang dihasilkan terhadap *incidental attack* dengan jenis *gaussian*.

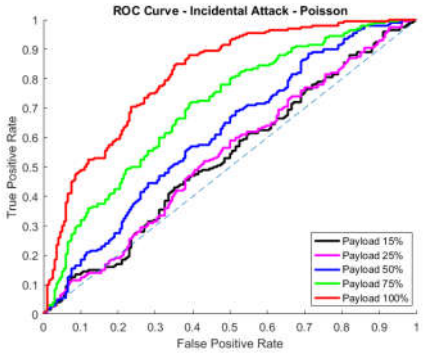
Detail informasi terhadap ROC Curve pada Gambar 3 terlampir pada Tabel 5. Berdasarkan Tabel 5, performansi sistem yang dibangun pada penelitian ini kurang bagus untuk mendeteksi LSB *matching* steganografi berdasarkan *incidental attack* jenis *gaussian* dengan *payload* mulai dari 15% karena memiliki rata-rata akurasi sebesar 50%, data *stego* yang terklasifikasi dengan benar sebesar 100%, dan data *cover* yang salah terklasifikasi sebesar 100%. Hal ini terjadi karena dalam domain frekuensi, *incidental attack* jenis *gaussian* merupakan sinyal acak yang memiliki intensitas yang sama pada frekuensi yang berbeda sehingga adanya data yang *overlap* antara *cover* dan *stego* yang menyebabkan tidak terdeteksi adanya informasi tersembunyi.

3.6 Pengujian dan Analisis Terhadap Incidental Attack dengan jenis *Poisson*

Setelah dilakukan pengujian terdahap *incidental attack* dengan jenis *poisson* menggunakan metode pada penelitian ini dan menggunakan metode pada penelitian sebelumnya dengan dataset yang telah disebutkan, perbandingan hasil performansi sistem dapat dilihat pada Gambar 4.



(a) Menggunakan metode pada penelitian saat ini.



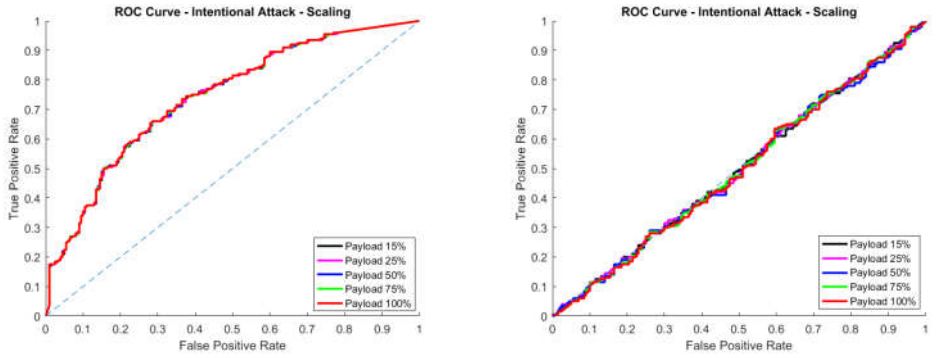
(b) Menggunakan metode pada penelitian sebelumnya.

Gambar 4. ROC *curve* yang dihasilkan terhadap *incidental attack* dengan jenis *poisson*.

Detail informasi terhadap ROC Curve pada Gambar 4 terlampir pada Tabel 6. Berdasarkan Tabel 6, performansi sistem yang dibangun pada penelitian ini bagus untuk mendeteksi LSB *matching* steganografi berdasarkan *incidental attack* jenis *poisson* dengan *payload* mulai dari 15% karena memiliki rata-rata akurasi sebesar 91.95%, data *stego* yang terklasifikasi dengan benar sebesar 100%, dan data *cover* yang salah terklasifikasi sebesar 10.5%. *Incidental attack* jenis *poisson* menghasilkan *noise* dari data (bukan menambahkan *noise* pada data) yang berarti bahwa *poisson noise* berkorelasi dengan intensitas setiap piksel. Perubahan intensitas tiap piksel dapat diamati dengan transformasi *fourier* saat perhitungan *center of mass*. Kondisi tersebut yang menyebabkan dapat terdeteksi adanya informasi tersembunyi.

3.7 Pengujian dan Analisis Terhadap Intentional Attack dengan jenis *Scaling*

Setelah dilakukan pengujian terdahap *intentional attack* dengan jenis *scaling* menggunakan metode pada penelitian ini dan menggunakan metode pada penelitian sebelumnya dengan dataset yang telah disebutkan, perbandingan hasil performansi sistem dapat dilihat pada Gambar 5.



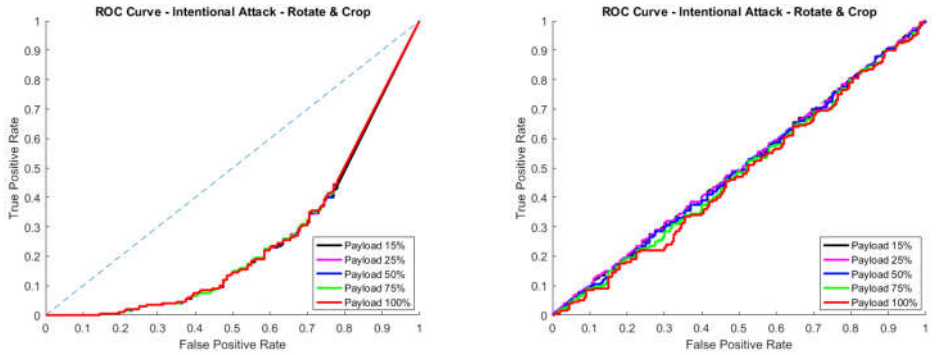
(a) Menggunakan metode pada penelitian saat ini. (b) Menggunakan metode pada penelitian sebelumnya.

Gambar 5. ROC *curve* yang dihasilkan terhadap *intentional attack* dengan jenis *scaling*.

Detail informasi terhadap ROC Curve pada Gambar 5 terlampir pada Tabel 7. Berdasarkan Tabel 7, performansi sistem yang dibangun pada penelitian ini bagus untuk mendeteksi LSB *matching* steganografi berdasarkan *intentional attack* jenis *scaling* dengan *payload* mulai dari 15% karena memiliki rata-rata akurasi sebesar 63.25%, data *stego* yang terklasifikasi dengan benar sebesar 37%, dan data *cover* yang salah terklasifikasi sebesar 10.5%. Adanya beberapa data yang tidak terdeteksi karena adanya pengaruh dari proses *scaling* dimana jika citra diubah skalanya menjadi dua kali lebih kecil, nilai dari empat piksel dijadikan nilai satu piksel dengan menghitung rata-ratanya. Jika citra diubah skalanya menjadi dua kali lebih besar, nilai dari satu piksel dijadikan nilai untuk empat piksel. Kondisi tersebut menyebabkan hilangnya beberapa informasi yang menyebabkan tidak terdeteksi adanya informasi tersembunyi.

3.8 Pengujian dan Analisis Terhadap Intentional Attack dengan jenis *Rotate & Crop*

Setelah dilakukan pengujian terdahap *intentional attack* dengan jenis *rotate & crop* menggunakan metode pada penelitian ini dan menggunakan metode pada penelitian sebelumnya dengan dataset yang telah disebutkan, perbandingan hasil performansi sistem dapat dilihat pada Gambar 6.



(a) Menggunakan metode pada penelitian saat ini. (b) Menggunakan metode pada penelitian sebelumnya.

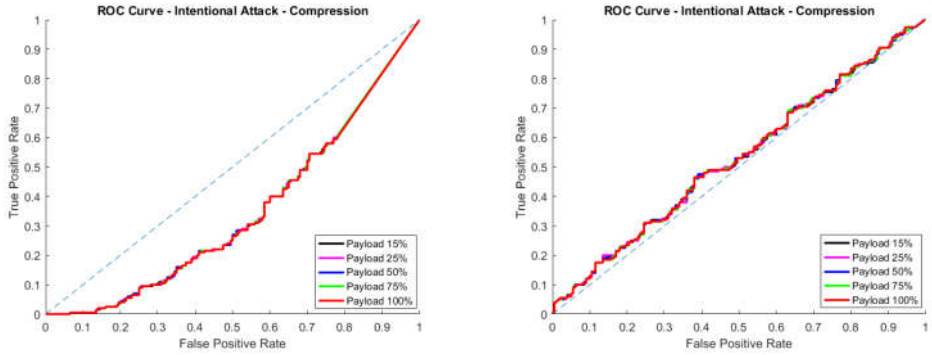
Gambar 6. ROC *curve* yang dihasilkan terhadap *intentional attack* dengan jenis *Rotate & Crop*.

Detail informasi terhadap ROC Curve pada Gambar 6 terlampir pada Tabel 8. Berdasarkan Tabel 8, performansi sistem yang dibangun pada penelitian ini kurang bagus untuk mendeteksi LSB *matching* steganografi berdasarkan *intentional attack* jenis *rotate & crop* dengan *payload* mulai dari 15% karena memiliki rata-rata akurasi sebesar 44.75%, data *stego* yang terklasifikasi dengan benar sebesar 0%, dan data *cover* yang salah terklasifikasi

sebesar 10.5%. Hal ini terjadi karena efek dari proses *crop* mengakibatkan beberapa area memiliki nilai yang sama (homogen) sehingga nilai untuk fitur *homogen* dari analisis teksur mendekati nilai 1 yang mengakibatkan data *stego* terdeteksi sebagai data *cover*.

3.9 Pengujian dan Analisis Terhadap Intentional Attack dengan jenis *Compression*

Setelah dilakukan pengujian terdahap *intentional attack* dengan jenis *compression* menggunakan metode pada penelitian ini dan menggunakan metode pada penelitian sebelumnya dengan dataset yang telah disebutkan, perbandingan hasil performansi sistem dapat dilihat pada Gambar 7.



(a) Menggunakan metode pada penelitian saat ini. (b) Menggunakan metode pada penelitian sebelumnya.

Gambar 7. ROC *curve* yang dihasilkan terhadap *intentional attack* dengan jenis *Compression*.

Detail informasi terhadap ROC Curve pada Gambar 7 terlampir pada Tabel 9. Berdasarkan Tabel 9, performansi sistem yang dibangun pada penelitian ini kurang bagus untuk mendeteksi LSB *matching* steganografi berdasarkan *intentional attack* jenis *compression* dengan *payload* mulai dari 15% karena memiliki rata-rata akurasi sebesar 45%, data *stego* yang terklasifikasi dengan benar sebesar 0.5%, dan data *cover* yang salah terklasifikasi sebesar 10.5%. Hal ini terjadi karena adanya informasi yang hilang yang disebabkan oleh adanya perkalian dengan matriks Discrete Cosine Transform (DCT) dan adanya kuantisasi citra sehingga nilai HCF-COM dari citra setelah dilakukan kompresi menjadi lebih besar daripada citra sebelum dilakukan kompresi sehingga tidak terdeteksi adanya informasi tersembunyi.

4. Kesimpulan

Pada Tugas Akhir ini, dibangun model steganalisis LSB *matching* dengan menerapkan konsep *fuzzy logic*. Model steganalisis yang dibangun mampu mendeteksi ada tidaknya informasi tersembunyi dengan ukuran *payload* yang bervariasi, yaitu 15%, 25%, 50%, 75%, dan 100% pada citra berwarna digital dengan mempertimbangkan daerah non-*plain*. Selain *payload*, model yang dibangun juga mampu mendeteksi ada tidaknya informasi tersembunyi pada citra berwarna digital berdasarkan distorsi *incidental attack* jenis *salt & pepper* dengan *noise density* sebesar 0.05 dan distorsi *incidental attack* jenis *poisson*.

Adapun kekurangan dari model steganalisis yang dibangun, yaitu performansi sistem yang dibangun kurang bagus untuk mendeteksi LSB *matching* steganografi berdasarkan distorsi *intentional attack*.

Daftar Pustaka

[1] J. Fridrich and M. Goljan, "Practical steganalysis of digital images - state of the art," in *Security and Watermarking of Multimedia Contents IV*, vol. 4675, 2002.

[2] O. Juarez-Sandoval, M. Cedillo-Hernandez, M. Nakano-Miyatake, H. Perez-Meana, and K. Toscano-Medina, "Image-adaptive steganalysis for lsb matching steganography," in *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*, 2016, pp. 478–483.

[3] T. Holotyak, J. Fridrich, and D. Soukal, "Stochastic approach to secret message length estimation in $\pm k$ embedding steganography," *Proc.SPIE*, vol. 5681, p. 12, 2005.

[4] R. M. Haralick, K. Shanmugam, and I. Dinstein, "Textural features for image classification," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. SMC-3, no. 6, pp. 610–621, 1973.

[5] J. J. Harmsen and W. A. Pearlman, "Steganalysis of additive-noise modelable information hiding," 2003.

[6] Suyanto, *Artificial Intelligence: Searching, Reasoning, Planning and Learning*. Informatika Bandung, 2014.

[7] L. Bossard, M. Guillaumin, and L. Van Gool, "Food-101 – mining discriminative components with random forests," in *European Conference on Computer Vision*, 2014.

[8] T. Fawcett, "An introduction to roc analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006.

[9] C. Sammut and G. I. Webb, *Encyclopedia of Machine Learning*. Springer US, 2010.

[10] J. A. Hanley and B. J. McNeil, "The meaning and use of the area under a receiver operating characteristic (roc) curve," *Radiology*, vol. 143, no. 1, pp. 29–36, 1982.

[11] S. J. Mason and N. E. Graham, "Areas beneath the relative operating characteristics (roc) and relative operating levels (rol) curves: Statistical significance and interpretation," *Quarterly Journal of the Royal Meteorological Society*, vol. 128, no. 584, pp. 2145–2166, 2002.