Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.2, April 2026, pp. 1614~1621
e-ISSN: 2548-6861

Comparative Analysis Chi-Square and Histogram Methods for Video Steganography Detection

Alfira Yuniar Rusman Putri [1]*, Senie Destya [2]*, Miko Kastomo Putro [3]*
*Teknik Komputer, Universitas Amikom Yogyakarta
alfirayuniar@students.amikom.ac.id [1], seniedestya@amikom.ac.id [2], miko.putro@amikom.ac.id [3]

Article Info

Article history:

Received 2025-12-26
Revised 2026-02-16
Accepted 2026-02-27

Keyword:

Video Steganography,
DCT – QIM,
Chi – Square Attack,
Histogram Analisys.

ABSTRACT

The quick increase in using videos to share data makes it easier for secret messages to be hidden using steganography. Even though many methods have been made to find these hidden messages, they aren't well tested when it comes to hiding messages in videos using the frequency domain. This study compares two methods, Chi-Square Attack and Histogram Analysis, to detect hidden messages in videos that use Discrete Cosine Transform (DCT) and Quantization Index Modulation (QIM). MP4 videos are broken into PNG frames, and secret messages are hidden in the mid-frequency DCT parts of the video. The amount of hidden data varies at 0.5%, 2.0%, and 5.0%. The quality of the video after hiding messages is checked using PSNR, SSIM, and Bit Error Rate (BER). The ability of the detection methods to find hidden messages is measured by how accurate they are and how long they take to process. The tests are done on five frames taken from one video without re-compressing it. The research results show that the DCT-QIM method produces very good stego quality with PSNR values consistently above 52 dB and SSIM values ranging from 0.9989 to 0.9999. However, the steganalysis results show that the Chi-Square method only achieved a detection accuracy of 30%, while the Histogram method reached an accuracy of 50%. Paired tests show there's a big difference between the two methods ($p < 0.05$), even though the overall detection performance is still not very good. These results show that the DCT-QIM-based insertion is fairly resistant to traditional statistical detection methods in controlled testing scenarios.

I. PENDAHULUAN

Pada perkembangan teknologi yang sangat pesat membawa dampak positif terhadap penyimpanan dan pertukaran data digital yang dimana menimbulkan banyak ancaman terhadap keamanan informasi. Steganografi dan kriptografi merupakan pendekatan utama dalam pengamanan informasi digital [1]. Salah satu teknik yang digunakan untuk menjaga kerahasiaan data tersebut dengan menggunakan teknik steganografi, yang merupakan sebuah teknik penyembunyian pesan rahasia pada media digital seperti video, gambar maupun audio tanpa mengubah tampilan aslinya [2]. Media video menjadi pilihan karena banyaknya jumlah frame yang besar sehingga bisa memungkinkan untuk melakukan penyisipan pesan tanpa mengurangi kualitas visualnya [3]. Dimana karakteristik spasial dan temporal pada video bisa memberikan kapasitas penyisipan yang lebih tinggi dibandingkan dengan citra statis [4].

Menggunakan teknik *Discrete Cosine Transform (DCT)* untuk melakukan penyisipan pesan rahasia pada domain frekuensi sehingga perubahan yang terjadi dapat diminimalisir [5]. Pada saat penyisipan dilakukan pada koefisien *mid – frequency DCT* dianggap optimal karena proses tersebut mampu menjaga kualitas visual nya dengan sekaligus bisa mempertahankan kestabilan pesan yang disisipkan [6], [6]. Dimana dengan pemilihan koefisien frekuensi yang tepat berpengaruh ke dalam signifikan pemilihan keseimbangan antara kapasitas dan imperceptibility [6]. Dengan menggunakan skema *Quantization Index Modulation (QIM)* yang bisa

memberikan keunggulan dalam mempertahankan ekstraksi pesan pada kondisi yang masih bisa dikontrol [7].

Ada berbagai penelitian yang telah mengembangkan teknik steganografi video berbasis DCT yang bisa digunakan untuk meningkatkan kapasitas dan ketahanan terhadap manipulasi [8]. Dimana pendekatan berbasis domain frekuensi bisa juga terbukti mampu untuk meningkatkan keamanan dibandingkan dengan menggunakan domain spasial yang sederhana [9]. Kemudian mendeteksi keberadaan pesan tersembunyi menggunakan metode *Chi - Square Attack* dan Histogram Analisis. Metode *Chi – Square Attack* digunakan untuk mendeteksi ketidaksesuaian distribusi antar bit [10]. Sedangkan Histogram Analisis digunakan untuk mendeteksi intensitas piksel pada setiap frame untuk mengidentifikasi anomali [11]. Kedua metode tersebut memiliki tantangan sendiri – sendiri terhadap format video yang digunakan dan tingkat kompresinya pada format MP4 [11].

Dimana penelitian ini membandingkan cara kerja metode *Chi-Square Attack* dan Histogram Analisis dalam mendeteksi pesan tersembunyi yang dimasukkan menggunakan teknik DCT pada frame video MP4 [12]. Penelitian dilakukan dengan variasi tingkat *payload* dan tingkat kompresi agar bisa melihat seberapa baik kedua metode tersebut mendeteksi pesan dalam kondisi yang berbeda [13]. Parameter yang dilihat meliputi tingkat akurasi dan waktu proses yang dibutuhkan untuk memproses, sehingga hasilnya memberikan gambaran yang lengkap tentang kinerja kedua metode.

Hasil dari penelitian ini diharapkan bisa memberikan manfaat dalam bidang keamanan multimedia, terutama dalam pembuatan sistem deteksi steganografi video yang lebih baik. Selain itu, penelitian ini juga diharapkan bisa menjadi pedoman bagi para peneliti dalam memilih metode deteksi yang sesuai dengan karakteristik data dan kebutuhan yang ada, serta membantu dalam meningkatkan perlindungan informasi di tengah perkembangan pertukaran data digital yang semakin cepat.

Meskipun dari teknik deteksi klasik tersebut sudah banyak diterapkan pada citra digital, kajian empiris terhadap efektivitasnya pada steganografi video berbasis DCT – QIM dengan menggunakan payload rendah masih terbatas. Dimana sebagian besar penelitian hanya berfokuskan pada peningkatan kualitas visual dan kapasitas penyisipan dibandingkan dengan analisis komparatif performa deteksi secara statistik signifikan.

Berdasarkan dari permasalahan yang sudah ada, penelitian ini bertujuan untuk melakukan analisis komparatif antara Chi – Square Attack dan Histogram Analysis untuk mendeteksi pesan tersembunyi pada frame video berformat MP4 dengan menggunakan DCT – QIM. Evaluasi ini dilakukan dengan menggunakan variasi payload 0,5%, 0,2% dan 5% dengan analisis menggunakan parameter kualitas visual (PSNR dan SSIM), tingkat kesalahan bit (BER), confusion matrix dan uji t berpasangan untuk mengetahui lebih signifikan perbedaan performa antara kedua deteksi tersebut.

II. METODE

A. Pengujian dan Dataset

Dalam pengujian penelitian ini dilakukan pada lingkungan komputasi dengan berbasis Python pada spesifikasi perangkat keras berupa processor kelas Intel, RAM 8GB dan menggunakan sistem operasi Windows. Video yang diujikan berformat MP4 lalu dilakukan ekstraksi menjadi frame PNG tanpa melakukan kompresi ulang sehingga bisa menjaga nilai statistik piksel dari video tersebut. Dimana pemilihan format PNG dilakukan karena bersifat lossless sehingga tidak terjadi degrdasi akibat kompresi [9].

Dataset yang digunakan terbatas hanya pada satu sumber video dengan pemilihan lima frame secara deterministik. Dimana kondisi ini bertujuan untuk memastikan reprodusibilitas eksperimen dan sekaligus menjadi batasan penelitian karena belum mencerminkan variasi konten video, resolusi dan kompleksitas visual yang beragam.

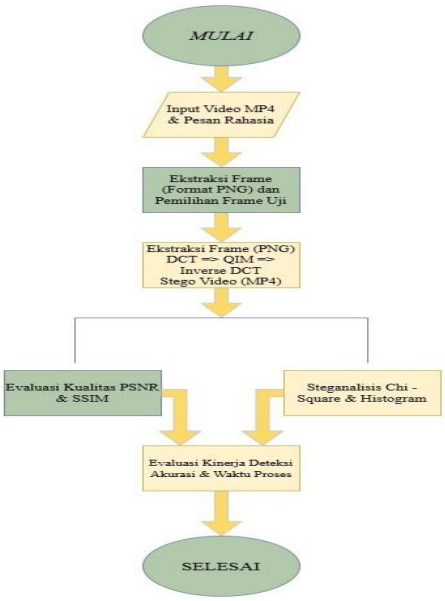
TABEL I
DATA PENELITIAN

Data	**Keterangan**
Jenis data	Video digital
Format video	MP4
Jumlah frame uji	5 frame
Format frame	PNG (lossless)
Pesan	Rahasia1
Variasi payload	0,5%, 2%, dan 5%
Resolusi	1080 x 1920
Frame Rate	29 fps
Durasi Video	12 detik
Jumlah Frame	364 frame
Ruang Warna	YcrCb (Channel Y)

Dimana tabel 1 menjelaskan lebih spesifikasi mengani dataset yang digunakan untuk penelitian ini.

B. Kerangka Penelitian

Untuk penelitian ini menggunakan pendekatan eksperimental dan komparatif yang digunakan untuk mengevaluasi kinerja dua metode steganalisis yaitu Histogram Analisis dan *Chi – Square Attack* dalam mendeteksi steganografi video berbasis DCT QIM. Tahapan penelitian berupa penyisipan pesan, ekstraksi pesan lalu analisis kualitas visual dan melakukan pendeteksian steganografi lalu setelahnya frame yang sudah dilakukan penyisipan akan digabungkan kembali dengan frame asli sehingga menjadi format MP4 seperti pada format awal.



Gambar 1 Alur Penelitian

Dalam melakukan penelitian ini diawali dengan mengekstraksi frame dari video MP4 yang akan digunakan untuk media cover [14]. Lalu menyisipkan pesan rahasi yang sudah dibuat ke dalan frame secara acak, disini mengambil 5 frame dengan menggunakan teknik steganografi berbasis DCT. Frame stego yang sudah dihasilkan lalu dilakukan analisis dengan menggunakan dua metode steganalisis yaitu *Chi – Square Attack* dan Histogram Analisis untuk mendeteksi adanya pesan yang tersembunyi. Dilakukan evaluasi terhadap performa deteksi menggunakan confusion matrix dan uji t berpasangan. Lalu video beberapa frame tersebut akan dijadikan satu kembali sehingga menjadikan format MP4 kembali dimana di dalam beberap frame yang sudah digabungkan terdapat frame yang sudah disisipkan pesan tersebut.

C. Proses Embedding DCT – QIM

Untuk setiap frame cover yang dikonversi ke dalam ruang warna YcrCb dan *kanal luminance* (Y) itu akan dibagi menjadi blok dengan ukuran 8x8 piksel dimana untuk setiap blok tersebut akan digunakan untuk memindahkan representasi citra ke domain frekuensi dalam steganografi *Discrete Cosine Transform (DCT)* [5]. Lalu untuk penyisipian pesan yang dilakukan pada koefisien *mid-freuqency DCT* dengan menggunakan skema *Quantization Index Modulation (QIM)* yang dimana digunakan untuk menjaga keseimbangan antara kualitas video stego frame dengan ketahanan pesan terhadapa deteksi yang dilakukan [15]. Disini menggunakan *payload* penyisipan yang divariasikan menjadi 0,5% ,2,0%, dan 5,0% dari total blok DCT yang sudah tersedia[16]. Untuk pesan yang disisipkan dengan panjang pesan tetap yaitu “rahasia1” dimana semua pengujian menggunakan pesan yang sama. Seteah semua pesan berhasil di sisipkan maka akan dilakukan *inverse DCT* untuk dilakukan konstruksi stego frame yang ada.

D. Proses Ektraksi dan Berhitungan BER

Pada saat dilakukan ekstraksi pesan dengan menggunakan pola blok dan parameter yang sama dengan proses embedding. Dengan koefisien DCT yang diesktraksi kembali sehingga bisa memperoleh bit pesan berdasarkan aturan dari *Quantization Index Modulation (QIM)* [17]. Lalu pesan hasil ekstraksi tersebut dibandingkan dengan pesan yang asli untuk bisa menghitung *Bit Error Rate (BER)* digunakan sebagai indikator keberhasilan pemulihan pesan. Perhitungan BER digunakan dengan rumus:

$$\mathrm{BER} = \frac{1}{n} \sum_{i-1}^{n} (\mathrm{bit}_i \neq \mathrm{bit}_i^1)$$

n = jumlah total bit
bit_i = bit asli ke-i
bit^1_i = bit hasil ekstraksi ke-i

Dimana BER menunjukkan bahwa proporsi kesalahan pada saat proses ekstraksi pesan, jika semakin kecil BER yang dihasilkan maka akan semakin tinggi keandalan steganografi dalam menjaga integritas datanya [14].

E. Evaluasi Kualitas Visual

Kualitas visual dievaluasi dengan menggunakan Peak Signal – to – Noise Ratio (PSNR).

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{MAX}\,\frac{2}{1}}{\mathrm{MSE}}\right)$$

Semakin kecil nilai dari MSE maka akan semakin besar nilai yang diperoleh dari PSNR nya yang dimana menunjukkan bahwa distorsi akibat penyipan semakin rendah. Nilai PSNR diatas 40 dB menunjukkan perbedaan visual antara frame cover dn frame stego tidak bisa dibedakan secara signifikan [13].

Dan juga menggunakan Structural Similarity Index (SSIM)

$$\mathrm{SSIM}\,(x,y) = \frac{(2_{\mu_x \mu_y} + C_1) + (2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

μ_x, μ_y = rata – rata intensitas pixel gambar asli dan stego
σ_x^2, σ_x^2 = varian pixel
σ_{xy} = kovarians gambar asli dan stego
C_1, C_2 = konstanta kecil untuk stabilisasi pembagian

Dimana SSIM mendekati 1 menunjukkan bahwa kesamaan struktural yang tinggi antara dua citra [15].

F. Metode Steganalisis

Metode teganalisis yang digunakan untuk mendeteksi adanya penyisipan pesan dengan menggunakan analisis ketidakseimbangan distribusi antara statistik nilai piksel atau keofisien DCT yaitu menggunakan metode *Ch – Square Attack* [9]. Nilai *Chi – Square Attack* bisa diperoleh engan menggunakan persamaan sebagai berikut:

$$X^2 = \sum_{i-1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

Yang dimana O_i adalah frekuensi observasi dan E_i adalah frekuensi harapan. Nilai sattistik dari *Chi – Square* yang tinggi dapat mengindikasikan adanya perubahan distribusi karena adanya proses penyisipan pesan, sehingga bisa digunakan untuk indikator melakukan deteksi pesan dalam steganografi.

Selain menggunakan teknik steganalisis *Chi – Square Attack* adapun dilakukan analisis menggunakan teknik Histogram Analisis yaitu dengan melakukanperbandingan distribusi histogram antara frame cover dan juga frame stego [11]. Perbedaan histogram dihitung dengan menggunakan *norma L2* sebagai indikator perubahan statistiknya yang dimana semakin besar nilai selisih histogramnya maka akan semakin besar juga kemungkinan keberadaan pesan dari steganografi yang sudah dilakukan.

$$\| H_1 - H_2 \|_2 = \sqrt{\sum_{i-1}^{n} (H_1(i) - H_2(i))^2}$$

Teknik Histogram Analisis ini bersifat sederhana namun efektif dalam melakukan deteksi adanya perubahan statistik kecil akibat adanya penyisipan pesan yang dilaukan terutama pada payload menengah hingga payload yang tinggi.

G. Penentuan Threshold Adaptif

Dimana penelitian ini, threshold digunakan untuk metode Chi – Square dan Histogram tidak ditentukan secara arbitrer namun dihitung dengan berdasarkan distribusi statistik frame cover. Dimana bertujuan untuk meningkatkan sensitivitas deteksi terhadap pesan perubahan distribusi yang diakibatkan oleh proses penyisipan pesan.

$$\text{Threshold} = \mu_{cover} + k \cdot \sigma_{cover}$$

Dimana pendekatan ini memungkinkan sistem melakukan deteksi distribusi terhadap karakteristik frame cover secara lebih objektif [16].

H. Evaluasi Performa Deteksi

Setelah semuanya selesai maka akan dilakukan evaluasi terkit kinerja deteksi dari metode *Chi – Square Attack* dan Histogram Analisis dengan berdasarkan parameter akurasi deteksi dan waktu prosesnya, yang dimana digunakan untuk melakukan penilaian terhadap efektivitas dan efisiensi dari masing – masing metode untuk mendeteksi adanya keberadaan pesan yang tersembunyi pada frame video.

Akurasi deteksi dilakukan perhitungan dengan berdasarkan jumlah frame yang terdeteksi dengan benar terhadap total frame yang sudah diuji, untuk frame cover dan juga frame stego yang sudah tersedia [12]. Perhitungan tersebut dilakukan dengan menggunakan persamaan rumus sebagai berikut:

$$\text{Akurasi} = \frac{\text{Nbenar}}{\text{Ntotal}} \text{ x } 100\%$$

Parameter akurasi ini digunakan untuk memberikan gambara secara umum terkait kemampuan metode steganalisis untuk melakukan identifikasi adanya steganografi atau penyisipan pesan secara tepat dan tanpa melakukan pemisahan secara rinci terkait kesalahan deteksinya [18].

Untuk parameter yang lain dengan menggunakan waktu proses yang dimana parameter tersebut digunakan untuk melakukan pengukuran efisiensi komputasi dari masing – masing metode steganalisis yang digunakan. Waktu proses dapat dihitung dengan berdasarkan durasi yang dibutuhkan untuk setiap metode dalam uji analisis terhadap frame stego dengan mencakup proses pembacaan frame sampai diperolehnya hasil deteksi akhirnya [19]. Waktu proses juga dihitung sebagai selisih anatara waktu akhir dan waktu awal dari proses analisis tersebut. Dilakukan perhitungan dengan menggunakan persamaan sebagai berikut:

$$T_{proses} = T_{akhir} - T_{awal}$$

Dan untuk melakukan perhitungan rata – rata nilai yang lebih efisien menggunakan persamaan sebagai berikut:

$$T = \frac{1}{n} \sum_{i=1}^{n} T_i$$

T_{awal} = waktu mulai proses steganalisis
T_{akhir} = waktu selesai proses steganalisis
T_i = waktu proses pada pengujian ke-1
N = jumlah pengujian

Penggabungan frame menjadi video stego ini adalah tahap terakhir untuk melakukan penelitian yaitu dilakukan penggabungan seluruh frame kembali, baik frame stego maupun frame yang tidak disisipi pesan menjadi sebuah video stego dengan format MP4 sesuai dengan format awal sebelum dilakukan ekstraksi frame. Proses ini dilakukan untuk memertahankan resolusi dan *frame rate* agar tetap sama dengan video yang aslinya sehingga untuk durasi dan karakteristik video tersebut tidak berubah [19].

III. HASIL DAN PEMBAHASAN

Setelah melakukan analisis terhadap metode DCT dan melakukan anaslisis steganalisis teknik *Chi – Square Attack* dan Histogram Analisis terdapat beberapa hasil sebagai berikut ini:

A. Pengujian Kualitas Stego Video

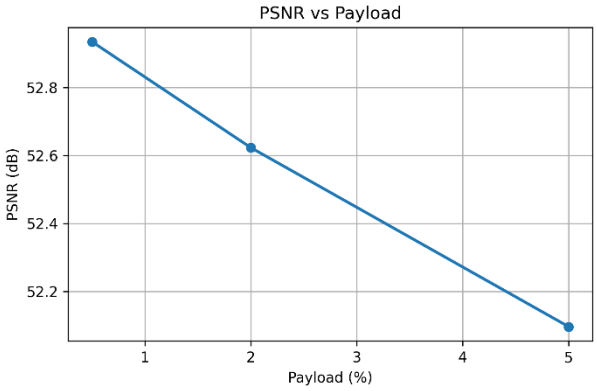
Pengujian ini dilakukan untuk melakukan evaluasi tingkat imperceptibility dan keberhasilan ekstraksi pesan dari metode steganografi berbasis DCT – Qim. Dengan menggunakan parameter PSNR dan SSIM. Serta untuk mengevaluasi tingkat error bit dengan menggunakan BER.

1) *Analisis PSNR*

TABEL II
ANALISIS PSNR

Payload (%)	Min (dB)	Max (dB)	Mean (dB)
0,5	52,86	52,97	52,93
2,0	52,53	52,66	52,62
5,0	52,02	52,11	52,09

Terlihat dari nilai PSNR sedikit menurun dengan seiring peningkatan di payloadnya pada rata – rata frame stego. Hal ini bisa menunjukkan bahwa banyak koefisien DCT yang dimodifikasi, maka distori citra akan menjadi meningkat. Namun seluruh nilai masih tetap berada di atas 50dB. Dimana nilai PSNR diatas 40dB secara umum menunjukkan bahwa ada perbedaan visual yang tidak dapat dibedakan oleh pengamatan manuasia. Dengan demikian metode DCT – QIM ini mempu menjaga kualitas visual sangat baik meskipun payload ditingkatkan hingga menjadi 5%.



Gambar 2 Grafik PSNR vs Payload

Berdasarkan grafik pada gambar 2 terlihat bahwa seluruh nilai PSNR tetap berada di atas 53dB, yang menunjukkan bahwa distorsi yang dihasilkan dari proses penyisipan pesan menggunakan metode DCT – QIM masih berada di kategori sangat tinggi kualitasnya.

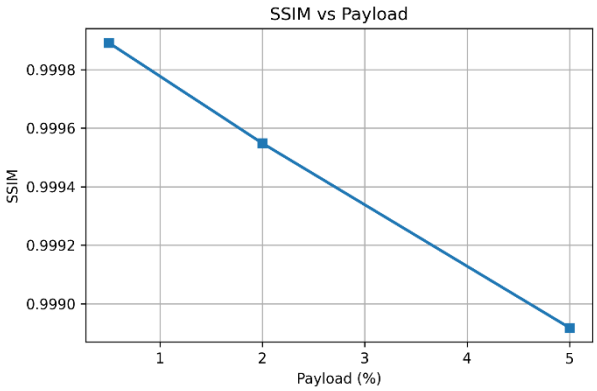
2) *Analisis SSIM*

Distribusi SSIM bisa ditunjukkan sebagai berikut:

TABEL III ANALISIS PSNR

Payload (%)	Min	Max	Mean
0,5	0,999884	0,999910	0,999892
2,0	0,999542	0,999555	0,999548
5,0	0,998895	0,998931	0,998918

Nilai SSIM mendekati 1 pada seluruh payload yang dimana menunjukkan bahwa struktur spasial antara frame cover dan frame stego yang hampir identik. Dan bisa dilihat dimana ada penurunan kecil pada payload 5% namun untuk nilainya tetap akan sangat tinggi. Hal ini ditunjukkan dengan penyisipan pesan pada koefisien mid – frequency DCT yang tidak merusak struktur citra secara signifikan.



Gambar 3 Grafik SSIM vs Payload

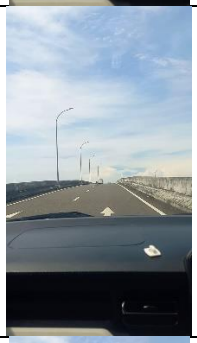
Grafik SSIM menunjukkan pola yang sama, nilai yang sangat mendekati 1 mengidentifikasi bahwa struktur spasial dan karakteristik visual frame stego hampir identik dengan frame asli. Dimana DCT – QIM mampu mempertahankan integritas visual secara konsisten pada seluruh payload.

3) *Analisis BER*

Untuk hasil ekstraksi menunjukkan nilai BER = 0,0000 pada seluruh pengujian. Pesan "rahasia1" berhasil diekstraksi secara sempurna pada seua frame yang digunakan untuk pengujian. Yang dimana skema QIM dapat bekerja dengan stabil, lalu untuk pemilihan blok DCT menggunakan seed deterministik menjaga konsistensi dan tidak adanya kompresi ulang atau gangguan eksternal mendukung kerberhasilan ekstraksi.

Dengan begitu, untuk metode DCT – QIM tidak hanya untuk menjaga kualitas visual tetapi juga bisa digunakan untuk mempertahankan intregitas pesan secara optimal. Untuk memastikan pada saat proses penyisipan pesan tidak terjadi perubahan visual yang dapat diamati secara langsung oleh manusia, maka diakukan perbandingan visual anatara frame stego dan frame asli yang sudah dipilih secara acak.

TABEL IV
PERBEDAAN FRAME STEGO DAN FRAME ASLI

Nama File	Frame Asli	Frame Stego
frame_0327.png		
frame_0057.png		
frame_0012.png		
frame_0140.png		
frame_0125.png		

Dengan demikian hasil visual frame stego dan frame asli yang dapat menyimpulkan bahwa visual nya tidak bisa dibedakan oleh manusia tanpa adanya bantuan analisis statistik ataupun komputer ketika sudah disisipi pesan rahasia. Dan juga dapat disimpulkan bahwa penyisipan berhasil dilakukan.

B. Hasil Deteksi Steganalisis Ch – Square dan Histogram

Uji steganalisis yang dilakukan menggunakan dua metode statistik yaitu dengan Chi – Square Attack dan Histogram Analisis terhadap frame stego. Threshold dihitung dengan cara adaptif berdasarkan pada distribusi statistik antar frame cover. Dimana nilai threshold itu diperoleh yaitu untuk Chi – Square Threshold diperoleh 62,7262 dan untuk Hitogram Threshold diperoleh nilai 77.897,4856. Dimana pendetekan ini memastikan bahwa ambang deteksi tidak bersifat tetap namun disesuaikan dengan menggunakan karakteristik data cover.

1) *Confusion Matrix dan Akurasi*

Metode Chi – Square untuk confusion matrix ini

9 6
15 0

Interpretasi:

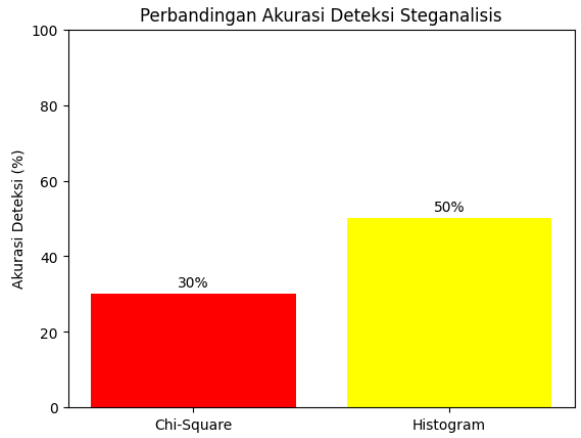
- True Negative (TN) = 9
- False Positive (FP) = 6
- False Negative (FN) = 15
- True Positive (TP) = 0

Dimana akurasi deteksinya mencapai 30%. Metode Chi – Square gagal mendeteksi seluruh frame stego (TP = 0). Namun terdapat perubahan distribusi statistik, dimana perubahan tersebut tidak cukup kuat untuk melewati threshold klasifikasi. Dengan ini ditunjukkan bahwa pendekatan Chi – Square kurang sensitif untuk digunakan pada pola modifikasi koefisien mid – frequency pada DCT – QIM dalam konfigurasi eksperimen ini.

Untuk metode Histogram Analysis dimana confusion matrix nya yaitu:

15 0
15 0

Nilai akurasi deteksi adalah 50% yang dimana metode Histogram mampu untuk mengenali seluruh frame cover dengan benar namun tetap gagal untuk melakukan pendeteksian frame stego. Dimana akurasi 50% ini menunjukkan bahwa performa setara dengan klasifikasi acak pada dua kelas tersebut.



Gambar 4 Akurasi Deteksi

Gambar 4 menunjukkan nilai kedua metode statistik konvensional tersebut belum mampu mendeteksi keberadaan pesan tersembunyi secara efektif pada stefo frame video yang dihasilkan. Dimana hal ini menunjukkan bahwa distribusi koefisien DCT hasil penyisipan QIM tidak megalami perubahan statistik yang cukup signifikan untuk dikenali oleh metode uji distribusi sederhana.

C. Hasil Uji t Berpasangan

Untuk memastikan apakah terdapat perbedaan yang signifikan antara distribusi statistik frame cover dan frame stego yaitu dengan menggunakan uji t berpasangan. Dimana hasil dari pengujian:

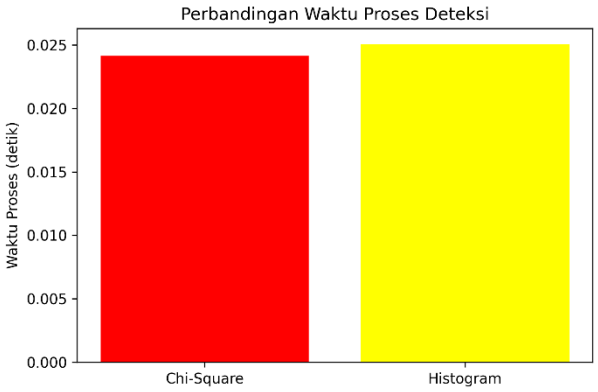
TABEL V
HASIL UJI T PERPASANGAN

Pengujian	Hasil
t-statistik	3,055
p-value	0,00856

Dikarenakan p-value < 0,05 maka akan terdapat perbedaan signifikan secara statistik antara distribusi cover dan distribusi stego. Namun, perbedaan signifikan secara global metode klasifikasi ini berbasis threshold sederhana yang dimana belum mampu untuk memanfaatkan perbedaan tersebut untuk melakukan deteksi individual secara efektif. Dan ditunjukkan bahwa secara statistik perubahan nyata akibat adanya embedding dan belum cukup kuat untuk dilakukan klasifikasi threshold konvensional.

D. Hasil Analisis Waktu Proses

Dimana waktu proses ini digunakan untuk melakukan evaluasi terhadap metode steganalisis yang sudah digunakan dengan mengukur efisiensi nya. Dalam pengukuran ini dilakukan perhitungan selisih waktu sebelum dan sesuah proses ekstraksi pesan pada setiap frame stego. Untuk penggunaan fungsi dari *time.time()* itu sendiri dapat memungkinkan pencatatan waktu dengan nilai resolusi yang tinggi sehingga dapat ditemukan perbedaan kinerja antara metode *Chi – Sqaure Attack* dan Histogram Analisis tersebut secara objektif.



Gambar 5 Grafik Waktu Proses

Grafik waktu proses menunjukkan bahwa metode Chi – Square memiliki rata – rata waktu deteksi disekitar 0,024 detik di setiap pengujian, sedangkan untuk Histogram ada di sekitar 0,025 detik. Bisa menunjukkan bahwa kedua metode memiliki kompleksitas komputasi yang relatif ringan dan cocok untuk pengujian cepat, namun efisiensi waktu tidak diikuti dengan kemampuan deteksi yang memadai.

E. Penggabungan Frame menjadi Video Stego

Pada tahapan terakhir yang dilakukan adalah menggabungkan kembali seluruh frame yang ada baik untuk frame stego dan frame tidak disisipi pesan ke dalam format MP4 kembali seperti pada format awal. Dengan dilakukan proses ini digunakan untuk mempertahankan resolusi, frame rate dan durasi yang memiliki kemiripan dengan video yang asli sehingga karakteristik dari video tersebut tidak berubah.

```
out = cv2.VideoWriter(output_video, cv2.VideoWriter_fourcc(*'mp4v'), fps, (width, height))
for path in frame_paths:
    frame = cv2.imread(path)
    out.write(frame)
out.release()
```

Gambar 6 Sourcode Penggabungan Video

Untuk hasil terdapat perubahan pada ukuran file nya antara video asli dengan video stego dimana ukuran file video stego lebih besar dari pada file video yang aslinya.

TABEL V
HASIL UKURAN FILE VIDEO

Nama	Ukuran File
Video Asli	25,0 MB
Video Stego	11,1 MB

Namun untuk hasil penelitian ini ukuran stego lebih kecil dari pada ukuran aslinya. Jadi untuk konsistensinya berbeda – beda, pada beberapa video stego ada yang ukuran nya besar dan ada yang ukuran nya kecil dimana terjadi karena karakteristik konten video dan mekanisme kompresi *codec* MP4 tersebut bergantung pada redudansi dan kompleksitas visual antar frame nya. Maka dari itu untuk ukuran file video

tidak bisa dijadikan sebagai tolak ukur langsung keberadaan steganografi namun bisa dikatakan sebagai efek samping dari proses kompresi video dan karakteristik sebuah media video.

IV. KESIMPULAN

Setelah melakukan penelitian dan melakukan pembahasan dapat disimpulkan bahwa metode steganografi video berbasis *Discrete Cosine Transform (DCT)* dengan menggunakan skema *Quantization Index Modulation (QIM)* telah menghasilkan stego video dengan kualitas yang lebih baik. Dengan ditunjukkan bukti dari hasil nilai *Peak Signal-to-Noise Ratio (PSNR)* yang bernilai berada di atas 52dB dan untuk nilai *Structural Similarity Index Measure (SSIM)* yang menyatakan telah konsisten dengan hasil mendekati 1 pada seluruh variasi *payload* yang digunakan dalam pengujian penyisipan, sehingga untuk perubahan visual nya akibat dari penyisipan pesan tidak bisa dibedakan secara signifikan. Dan untuk nilai *Bit Error Rate* nya menunjukkan tingkat keberhasilan tinggi dengan niai 0. Untuk dari segi steganalisis nya kedua metode mampu mendeteksi keberadaan pesan yang tersembunyi pada seluruh frame stego. Ini menegaskan bahwa metode DCT – QIM yang digunakan memiliki tingkat robustness yang sangat baik terhadap proses penyisipan dan ekstraksi dalam kondisi eksperimen terkontrol.

Namun untuk hasil steganalisis nya menunjukkan bahwa kedua metode deteksi statistik yang diuji belum mampu mendeteksi keberadaan pesan secara optimal. Dimana metode Chi – Square hanya memperoleh akurasi deteksi sebesar 30% sedangkan untuk Histogramnya memperoleh akurasi deteksi sebesar 50%. Nilai precision, recall dan F1-score pada kedua metode menunjukkan performa yang rendah khususnya untuk mendeteksi kelas stego. Dan untuk hasil uji t berpasangan terhadap akurasi deteksi menunjukkan nilai p-value sebesar 0,0085 ($p<0,005$) yang bisa diartikan terdapat perbedaan signifikan secara statistik untuk kedua metode steganalisis.

Penelitian ini memiliki keterbatasan antara lain pada penggunaan dataset video, jumlah frame uji serta tidak mempertimbangkan skenario kompresi ulang, manipulasi ulang atau gangguan eskernal yang umum terjadi di dunia nyata. Untuk penelitian selanjutnya disarankan menggunakan dataset dengan variasi konten, resolusi dan codec yang lebih beragam serta melakukan kombinasi metode steganalisis dengan pendekatan berbasis pembelajaran mesin guna untuk meningkatkan kemampuan deteksi pada kondisi yang lebih kompleks dan realistis.

DAFTAR PUSTAKA

[1] Ms. Halima Abbas Ahmed, "Comprehensive Review of Cryptography and Steganography Algorithms," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 29s, pp. 211–228, Mar. 2025, doi: 10.52783/jisem.v10i29s.4471.

[2] F. Şahin, T. Çevik, and M. Takaoğlu, "Review of the Literature on the Steganography Concept," *Int. J. Comput. Appl.*, vol. 183, no. 2, pp. 38–46, May 2021, doi: 10.5120/ijca2021921298.

[3] J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, "Video steganography: recent advances and challenges," *Multimed. Tools Appl.*, vol. 82, no. 27, pp. 41943–41985, Nov. 2023, doi: 10.1007/s11042-023-14844-w.

[4] S. N. Alrekaby, M. A. A. Khodher, L. K. Adday, and R. Aljuaidi, "Secure Image Transmission Using Multilevel Chaotic Encryption and Video Steganography," *Algorithms*, vol. 18, no. 7, p. 406, Jul. 2025, doi: 10.3390/a18070406.

[5] Y. Yang, X. Xiang, J. Qin, Y. Tan, Z. Wang, and Y. Liu, "High-Embedded Low-Distortion Multihistogram Shift Video Reversible Data Hiding Based on DCT Coefficient," *Electronics*, vol. 12, no. 7, p. 1652, Mar. 2023, doi: 10.3390/electronics12071652.

[6] B. N. Babar, S. Javir, R. Harer, P. Nagwade, and A. Gade, "Video Steganography Using DCT Algorithm," vol. 11, no. 1, 2024.

[7] A. S. Pratama and I. M. Suartana, "Analisis Kualitas Stego Video dalam Penyisipan Data Memanfaatkan Metode DCT-DWT," *J. Inf. Eng. Educ. Technol.*, vol. 5, no. 1, pp. 13–18, Jun. 2021, doi: 10.26740/jieet.v5n1.p13-18.

[8] Y. Huang, Z. Liu, Q. Wu, and X. Liu, "Robust image steganography against JPEG compression based on DCT residual modulation," *Signal Process.*, vol. 219, p. 109431, Jun. 2024, doi: 10.1016/j.sigpro.2024.109431.

[9] R. Patel, K. Lad, and M. Patel, "Novel DCT and DST based video steganography algorithms over non-dynamic region in compressed domain: a comparative analysis," *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 1649–1657, May 2022, doi: 10.1007/s41870-021-00788-7.

[10] A. Mohamed AbdiRashiD, S. Solak, and A. K. Sahu, "Frekans Alanı Görüntü Steganografisine Dayalı Veri Gizleme," *Eur. J. Sci. Technol.*, Oct. 2022, doi: 10.31590/ejosat.1188597.

[11] D. Yanti, Y. B. Utomo, and H. Mukminna, "Implementation of Steganalysis Technique Using Chi Square Attack Method on Android-Based JPEG Stego Image Format," *JTECS J. Sist. Telekomun. Elektron. Sist. Kontrol Power Sist. Dan Komput.*, vol. 1, no. 1, p. 51, Jan. 2021, doi: 10.32503/jtecs.v1i1.661.

[12] M. Fuad, F. Ernawan, and L. J. Hui, "Video scene change detection based on histogram analysis for hiding message," *J. Phys. Conf. Ser.*, vol. 1918, no. 4, p. 042141, Jun. 2021, doi: 10.1088/1742-6596/1918/4/042141.

[13] E. Daraghmi and A. Hamoudi, "From Cryptography to Steganography: Detecting Hidden Data in the Digital World," *Int. J. Innov. Sci. Res. Technol. IJISRT*, pp. 1908–1914, Oct. 2024, doi: 10.38124/ijisrt/IJISRT24SEP937.

[14] S. Kapoor and S. Shivani, "Robust and high capacity image steganography technique using spiral-walk inter-block DCT coefficient differencing," *Multimed. Tools Appl.*, vol. 83, no. 39, pp. 86405–86424, Jun. 2024, doi: 10.1007/s11042-024-19520-1.

[15] T. Wang *et al.*, "Lossless image steganography: Regard steganography as super-resolution," *Inf. Process. Manag.*, vol. 61, no. 4, p. 103719, Jul. 2024, doi: 10.1016/j.ipm.2024.103719.

[16] F. Ernawan, "An improved hiding information by modifying selected DWT coefficients in video steganography," *Multimed. Tools Appl.*, vol. 83, no. 12, pp. 34629–34645, Sep. 2023, doi: 10.1007/s11042-023-17113-y.

[17] I. A. Saputro, F. S. Nugraha, L. Sugiarto, and I. A. Prabowo, "Evaluating Steganography Detection in JPEG Images Using Gaussian Mixture Model and Cryptographic Keys," *J. RESTI Rekayasa Sist. Dan Teknol. Inf.*, vol. 9, no. 6, pp. 1398–1404, Dec. 2025, doi: 10.29207/resti.v9i6.6084.

[18] S. Roy and J. Howlader, "Design and Analysis of a Novel Video Steganography Technique with Enhanced Resilience," *J. Inst. Eng. India Ser. B*, Aug. 2025, doi: 10.1007/s40031-025-01260-x.

[19] Y. B. Utomo and H. Mukminna, "Penerapan Teknik Steganalysis Menggunakan Metode Chi Square Attack Pada Stego Image Berformat Jpeg Berbasis Android," 2021.