

Perancangan Sistem Anti Deepfake Berbasis Steganografi Qr Code Dan Algoritma DCT

Qadri Tasri^{1*}, Ahmad², Ahyuna²

¹Teknik Informatika, Universitas Dipa Makassar, Makassar, Indonesia

²Universitas Dipa Makassar, Makassar, Indonesia

e-mail: ^{*1}qadricoy22@gmail.com, ²ahmadjabbareng@gmail.com, ³Ahyuna@undipa.ac.id

Abstrak

Perkembangan teknologi kecerdasan buatan, khususnya deepfake, memungkinkan manipulasi gambar dan video yang sangat realistis sehingga menyulitkan verifikasi keaslian media digital. Metode steganografi konvensional sering gagal mempertahankan jejak penyisipan, sehingga diperlukan sistem yang mampu meninggalkan penanda keaslian secara tersembunyi. Penelitian ini merancang sistem anti-deepfake berbasis QR Code dengan algoritma Discrete Cosine Transform (DCT) dan Quantization Index Modulation (QIM). QR Code disisipkan pada citra wajah 512×512 piksel melalui koefisien frekuensi rendah hingga menengah (koordinat 2,2; 2,3; 3,2) dengan Delta = 50 untuk memperkuat jejak steganografi. Hasil embedding dievaluasi menggunakan PSNR untuk menjaga kualitas visual, dan ekstraksi QR Code digunakan untuk menilai keberhasilan deteksi pada citra maupun video deepfake. Hasil menunjukkan bahwa sistem berhasil mengekstraksi QR Code pada 90% gambar dan 80% video deepfake. Pada video dengan manipulasi ringan, watermark tak terlihat berhasil diekstraksi pada frame awal; pada video manipulasi kompleks, ekstraksi menurun tetapi jejak visual tetap dapat terdeteksi. PSNR rata-rata >30 dB menunjukkan kualitas citra tetap terjaga. Temuan ini menegaskan bahwa QR Code-DCT-QIM lebih robust dibanding steganografi konvensional, mampu mempertahankan artefak visual yang dapat diekstraksi meskipun citra/video dimanipulasi oleh GAN. Sistem ini efektif dalam mendeteksi manipulasi deepfake sambil menjaga kualitas visual, sehingga memberikan solusi yang adaptif dan kuat untuk verifikasi keaslian media digital.

Kata kunci— Deepfake, Steganografi, QR Code, DCT, QIM.

Abstract

The rapid development of artificial intelligence, particularly deepfake technology, enables highly realistic manipulation of images and videos, complicating the verification of digital media authenticity. Conventional steganography often fails to preserve embedding traces, creating the need for systems capable of leaving hidden authenticity markers. This study proposes an anti-deepfake system based on QR Code steganography using Discrete Cosine Transform (DCT) and Quantization Index Modulation (QIM). QR Codes are embedded in 512×512 facial images through low- to mid-frequency DCT coefficients (coordinates 2,2; 2,3; 3,2) with Delta = 50 to strengthen the embedding trace. The embedding quality is evaluated via PSNR, and QR Code extraction is used to assess detection success in both images and AI-generated deepfake videos. Results indicate that the system successfully extracts QR Codes from 90% of images and 80% of deepfake videos. For videos with minor manipulations, the hidden watermark is reliably detected in the first frames. In videos with complex manipulations, extraction success decreases, yet visual traces remain detectable. Average PSNR above 30 dB confirms that visual quality is preserved. These findings demonstrate that QR Code-DCT-QIM steganography is more robust than conventional methods, retaining extractable visual artifacts even after deepfake manipulations. The system effectively detects deepfake alterations while maintaining image quality, providing an adaptive and reliable solution for verifying digital media authenticity.

Keywords— *Deepfake, Steganography, QR Code, DCT, QIM.*

1. PENDAHULUAN

Perkembangan pesat teknologi Artificial Intelligence (AI) membuka peluang besar di berbagai sektor, namun juga menghadirkan risiko serius, salah satunya adalah teknologi deepfake. Deepfake memungkinkan manipulasi gambar, video, dan audio menggunakan algoritma deep learning untuk menciptakan konten palsu yang sangat realistis. Fenomena ini mengancam kepercayaan publik terhadap informasi digital dan dapat menyebabkan penyebaran disinformasi, khususnya di media sosial dan dunia politik [1]. Keakuratan deepfake dalam mengganti wajah atau suara seseorang berpotensi merusak reputasi individu serta integritas informasi yang beredar di masyarakat [2].

Penyalahgunaan teknologi ini semakin meluas, khususnya dalam manipulasi video publik yang bertujuan merusak reputasi individu, yang berpotensi menurunkan tingkat kepercayaan publik. Di Indonesia, dengan tingginya tingkat penggunaan media sosial, fenomena ini semakin memperburuk risiko terhadap keamanan siber dan stabilitas sosial [3], [4]. Penyalahgunaan teknologi serupa juga terjadi dalam manipulasi gambar atau video publik yang dapat merusak kepercayaan publik terhadap pemberitaan yang ada pada sosial media, memperburuk komunikasi publik, serta menambah ketidakpastian dan kebingungan di masyarakat.

Penelitian ini bertujuan merancang sistem yang mampu mengenali perubahan pada citra akibat konversi menjadi video deepfake oleh AI image generator. Sistem melakukan analisis dengan mengekstraksi QR Code dari lima frame awal video sebagai sampel. Setiap frame dihitung jumlah piksel putih hasil ekstraksi, dan frame tersebut dikategorikan berhasil mengidentifikasi data yang tertanam apabila jumlah piksel putih mencapai 20% untuk citra tunggal dan 10% untuk video. Penetapan ambang ini didasari uji coba awal: pada citra tunggal, pixel hasil ekstraksi terkadang hanya muncul di bawah 20% area, sehingga tidak cukup representatif; sedangkan pada video, detail pixel QR Code menurun drastis akibat proses deepfake, sehingga ambang 10% lebih realistis untuk mendeteksi keberhasilan ekstraksi. Sementara itu, nilai Peak Signal-to-Noise Ratio (PSNR) digunakan sebagai metrik untuk memastikan bahwa embedding QR Code tetap mempertahankan kualitas visual citra, sehingga sistem mampu meninggalkan jejak autentik tanpa merusak tampilan asli, menunjukkan keunggulan dibanding steganografi konvensional yang sering hilang ketika citra dimanipulasi.

Kebutuhan akan sistem ini muncul karena metode steganografi konvensional sering hilang saat menghadapi deepfake canggih berbasis Generative Adversarial Networks (GANs) [5]. Penelitian ini menawarkan pendekatan baru dengan menyisipkan QR Code sebagai payload khusus menggunakan DCT dan QIM, sehingga jejak autentik tetap terdeteksi meskipun citra dikonversi menjadi video. Berbeda dengan metode steganografi berbasis GAN atau watermarking frekuensi tinggi sebelumnya, sistem ini mempertahankan artefak visual yang jelas, mudah diekstraksi, dan menjaga kualitas citra (PSNR > 30 dB), sekaligus memberikan solusi sederhana dan adaptif untuk mendeteksi manipulasi deepfake.

Untuk meningkatkan efektivitas sistem, penelitian ini mengusulkan penggunaan model QIM-DCT, yang menyisipkan informasi ke dalam area frekuensi rendah hingga sedang (LFC-MFC) pada citra. Model ini menggunakan teknik untuk meningkatkan ketahanan terhadap gangguan dan manipulasi, dengan faktor pengulangan yang memperkuat sinyal dan meninggalkan jejak visual. QR Code yang disisipkan dalam citra diproses menggunakan DCT dan QIM, memungkinkan deteksi manipulasi dengan deepfake. Tujuan utama dari penelitian ini adalah merancang sistem yang menghasilkan gambar dengan visual yang mudah dikenali ketika menghadapi manipulasi deepfake dan memberikan solusi untuk memverifikasi keaslian media digital.

Kontribusi utama dari penelitian ini adalah pengembangan pendekatan forensik dalam

steganalisis serta verifikasi keaslian citra yang dimanipulasi menggunakan teknologi deepfake. Pendekatan ini tidak hanya memberikan manfaat signifikan dalam konteks media sosial, tetapi juga dapat meningkatkan keamanan bagi pemilik citra saat berinteraksi di platform media sosial, dengan menyediakan solusi yang lebih adaptif terhadap perkembangan teknologi kecerdasan buatan yang terus berkembang [6].

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen kuantitatif untuk merancang dan menguji sistem anti-deepfake berbasis steganografi QR Code yang menggunakan algoritma Discrete Cosine Transform (DCT) dan Quantization Index Modulation (QIM). Sistem ini dirancang untuk menyisipkan penanda keaslian berupa QR Code secara tersembunyi pada citra wajah dan untuk mengevaluasi apakah jejak penyisipan tersebut tetap dapat dikenali meskipun citra telah dimanipulasi menjadi video deepfake oleh teknologi kecerdasan buatan (AI). Proses evaluasi kualitas citra hasil penyisipan dilakukan menggunakan Peak Signal-to-Noise Ratio (PSNR), yang digunakan untuk menilai kualitas visual citra, serta analisis jejak visual pada hasil ekstraksi QR Code yang tertanam dalam citra. Penelitian ini juga memperhatikan metode deteksi dan analisis yang memungkinkan sistem mendeteksi perubahan akibat manipulasi deepfake yang dilakukan menggunakan model AI seperti Generative Adversarial Networks (GANs).

2.1 Analisis Masalah

Permasalahan utama yang diangkat dalam penelitian ini adalah kerentanan steganografi konvensional saat menghadapi manipulasi citra oleh model deepfake berbasis AI. Sebagai contoh, penggunaan Generative Adversarial Networks (GANs) untuk menghasilkan video deepfake memungkinkan manipulasi gambar atau video dengan cara yang sangat realistis, sehingga menyebabkan jejak penyisipan steganografi konvensional sering kali hilang atau terganggu. Steganografi konvensional menggunakan teknik penyisipan data dalam domain spasial citra yang mudah terhapus atau berubah ketika proses manipulasi terjadi, seperti pada proses deepfake [5][6]. Oleh karena itu, penelitian ini menekankan pentingnya penguatan jejak steganografi dengan memanfaatkan teknik transformasi frekuensi (DCT) dan modulasi kuantisasi (QIM) untuk menghasilkan indikasi visual yang jelas dan tetap terdeteksi meskipun citra atau video dimanipulasi.

Dalam hal ini, penelitian ini berfokus pada pengembangan teknik steganografi QR Code yang dapat memberikan jejak visual yang tetap terlihat meskipun terjadi manipulasi dengan GAN. Pendekatan ini diharapkan dapat mempertahankan jejak steganografi yang cukup kuat untuk terdeteksi, meskipun citra telah diproses menjadi video deepfake yang dirender oleh algoritma AI [7], [8].

2.2 Arsitektur Sistem

Arsitektur sistem yang dikembangkan dalam penelitian ini terdiri dari tiga modul utama, yang secara terpisah menangani proses penyisipan QR Code, ekstraksi data, dan evaluasi kualitas citra. Ketiga modul ini bekerja bersama untuk memastikan bahwa jejak steganografi tetap terdeteksi meskipun terjadi manipulasi deepfake.

1. Modul Embedding (Encoder)

Pada modul ini, QR Code disisipkan ke dalam citra wajah berukuran 512×512 piksel melalui transformasi Discrete Cosine Transform (DCT). Dalam proses ini, citra dipecah menjadi blok 8×8 piksel, kemudian koefisien DCT frekuensi rendah hingga menengah dipilih untuk menyisipkan QR Code. Teknik Quantization Index Modulation (QIM) digunakan untuk memperkuat jejak penyisipan QR Code dengan pengaturan tingkat kuantisasi melalui parameter Delta (δ), yang ditetapkan sebesar 50 untuk meningkatkan ketahanan jejak terhadap gangguan manipulasi [6], [9].

2. Modul Decoding & Analisis (Decoder dan Steganalysis)

Modul ini bertanggung jawab untuk mengekstraksi QR Code yang disisipkan pada citra atau video yang telah dimanipulasi. Untuk video deepfake, sistem mengekstraksi lima frame awal sebagai sampel analisis. Dalam pengujian ekstraksi, sistem menghitung jumlah piksel putih yang dihasilkan dari ekstraksi QR Code, yang menunjukkan keberhasilan proses ekstraksi. Proses ini juga mengevaluasi indikator artefak (misalnya, dominasi piksel putih pada hasil ekstraksi) untuk menilai apakah perubahan akibat manipulasi telah terdeteksi [10][11].

3. Modul Evaluasi Kualitas

Pada modul ini, kualitas citra yang dihasilkan setelah penyisipan QR Code dievaluasi menggunakan PSNR (Peak Signal-to-Noise Ratio). PSNR digunakan untuk memastikan bahwa kualitas visual citra tetap terjaga setelah proses embedding, dengan target kualitas citra tetap berada di atas standar yang diterima, yaitu $\text{PSNR} > 30$ dB. Dengan menggunakan teknik DCT dan QIM, kualitas citra dapat dipertahankan meskipun QR Code disisipkan dalam citra [12][13].

2.3 Metode yang Digunakan

Metode inti penelitian ini meliputi:

1. Discrete Cosine Transform (DCT) : DCT digunakan untuk memindahkan representasi citra dari domain spasial ke domain frekuensi agar penyisipan dapat dilakukan pada area koefisien tertentu dengan dampak visual minimal. Citra dibagi menjadi blok 8×8 dan diproses pada kanal luminance (kanal Y) agar perubahan lebih stabil untuk dianalisis.
2. Quantization Index Modulation (QIM) : QIM digunakan untuk memperkuat sinyal penyisipan dengan pengaturan tingkat kuantisasi melalui parameter Delta (δ). Dalam penelitian ini, parameter Delta ditetapkan $\delta = 50$ untuk memperkuat jejak penyisipan namun tetap menjaga kualitas citra (ditunjukkan oleh capaian PSNR) [7].
3. Steganografi QR Code sebagai Penanda Keaslian : QR Code dikonversi menjadi bit payload, disusun bersama penanda (header/marker), lalu ditanamkan pada koefisien DCT yang dipilih. QR Code berfungsi sebagai “tanda autentik” tersembunyi, sehingga ketika terjadi manipulasi deepfake, struktur payload cenderung berubah dan memunculkan indikasi kerusakan/artefak pada hasil ekstraksi [8], [9].

2.4 Implementasi Sistem

Implementasi sistem dilakukan dengan menggunakan Python sebagai bahasa pemrograman utama untuk pemrosesan citra dan analisis. Beberapa library Python yang digunakan dalam penelitian ini antara lain OpenCV (cv2) untuk memproses citra, NumPy untuk perhitungan numerik, dan qrcode serta pyzbar untuk pembuatan dan pembacaan QR Code yang disisipkan pada citra. Untuk menyediakan layanan pemrosesan dan endpoint pengujian, digunakan framework Flask yang memungkinkan sistem untuk menerima input citra atau video melalui antarmuka berbasis web. Di sisi antarmuka (front-end), digunakan Laravel, yang mempermudah pengguna dalam mengunggah citra dan video serta memperoleh hasil analisis yang telah dilakukan oleh sistem. Penggunaan Laravel juga memudahkan integrasi antara backend dan frontend dalam mengelola interaksi pengguna dengan aplikasi web. Sistem ini memastikan bahwa setiap langkah dalam proses embedding dan ekstraksi QR Code dapat dilakukan dengan efisien dan dapat diakses dengan mudah melalui tampilan web [14], [15].

2.5 Dataset dan Desain Eksperimen

Objek dan Format Data uji berupa citra wajah dari dataset publik yang diproses menjadi citra stego (JPG/PNG/JPEG), lalu dikonversi menjadi video deepfake (MP4) menggunakan layanan AI image-to-video. Resolusi citra embedding dibatasi pada 512×512 , sedangkan video ditetapkan pada resolusi standar 720p. Jumlah Data Uji menggunakan 60 citra wajah dan 20 video deepfake. Untuk evaluasi video, tiap video diambil 5 frame sebagai sampel analisis.

2.6 Kriteria Keberhasilan dan Teknik Pengujian

1. Uji Kualitas Citra (PSNR)

PSNR digunakan untuk menilai apakah citra hasil embedding masih mempertahankan kualitas visual yang baik. Target kualitas ditunjukkan oleh PSNR rata-rata di atas 30 dB.

2. Uji Keberhasilan Ekstraksi & Indikator Artefak

Sistem menetapkan ambang indikator piksel putih hasil ekstraksi sebagai sinyal keberhasilan identifikasi payload, Dimana Pada gambar, ekstraksi dianggap teridentifikasi bila piksel putih mencapai sekitar 20% dari total piksel, dan pada video, ambang yang digunakan sekitar 10% dari total piksel pada frame yang dianalisis.

3. Uji Fungsional (Black Box)

Pengujian black box dilakukan untuk memverifikasi fungsi utama sistem (embedding, decoding, dan analisis) berjalan sesuai rancangan tanpa menilai struktur internal kode, sehingga validasi berfokus pada input–proses–output yang dihasilkan.

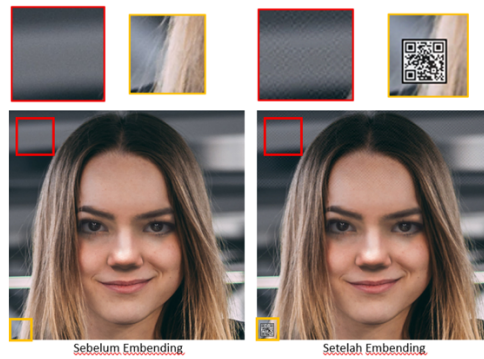
3. HASIL DAN PEMBAHASAN

Pada bagian ini, akan dibahas mengenai hasil implementasi sistem yang telah dirancang, pengujian yang dilakukan, serta analisis yang diperoleh berdasarkan eksperimen yang dilakukan. Hasil penelitian ini mencakup kinerja sistem dalam menyisipkan QR Code menggunakan algoritma DCT dan QIM pada citra wajah, serta evaluasi efektivitas sistem dalam mendeteksi manipulasi deepfake. Pembahasan akan difokuskan pada tiga aspek utama: kualitas citra hasil embedding, kemampuan ekstraksi QR Code dari citra yang telah dimanipulasi, dan deteksi jejak visual pada video deepfake.

3.1 Perancangan dan Implementasi Sistem

Sistem yang dirancang bertujuan untuk menyisipkan QR Code ke dalam citra wajah dengan menggunakan algoritma DCT untuk konversi citra ke domain frekuensi dan QIM untuk penguatan jejak steganografi. Citra wajah berukuran 512×512 piksel digunakan sebagai input utama. Penyisipan QR Code dilakukan pada koefisien frekuensi rendah hingga menengah pada koordinat (2,2), (2,3), dan (3,2) dalam blok 8×8 yang dihasilkan oleh DCT. Pemilihan koordinat ini didasari oleh pertimbangan ilmiah: koefisien frekuensi rendah memengaruhi sebagian besar informasi visual, sedangkan frekuensi menengah relatif tahan terhadap kompresi dan manipulasi oleh algoritma deepfake. Dengan menanam payload pada koordinat ini, sistem dapat menjaga kualitas visual citra (PSNR > 30 dB) sekaligus meninggalkan jejak visual yang dapat diekstraksi.

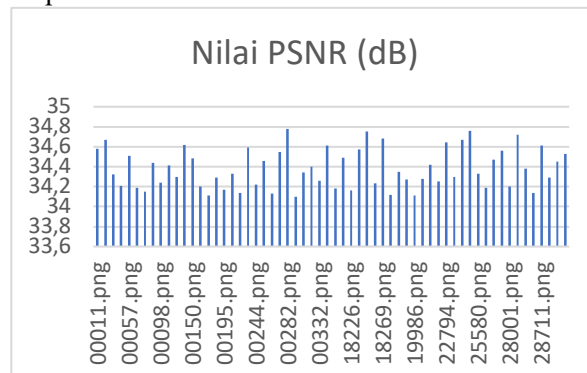
Parameter Delta (δ) = 50 digunakan untuk memperkuat jejak penyisipan QR Code. Nilai ini dipilih berdasarkan uji coba eksperimen awal, karena memberikan keseimbangan optimal antara ketahanan terhadap gangguan/manipulasi dan minimnya degradasi visual. Selain itu, penggunaan Delta 50 membuat pola data QR Code lebih kentara; ketika citra diperbesar, pola hitam-putih QR Code menjadi semakin jelas, memudahkan proses ekstraksi dan verifikasi. Hal ini menjadi penting karena AI deepfake berbasis GAN sangat sensitif terhadap pixel, sehingga terkadang hasil video menghasilkan artefak seperti gambar bergelombang, muncul salju, atau efek seperti pasir. Hasil embedding QR Code kemudian dievaluasi menggunakan metrik PSNR untuk memastikan kualitas visual tetap terjaga, sementara keberhasilan deteksi QR Code dan artefak visual dianalisis melalui metode ekstraksi dan perhitungan rasio piksel putih pada citra maupun video deepfake.



Gambar 1 Gambar Sebelum Dan Sesudah Embedding

3.2 Pengujian Kualitas Citra (PSNR)

Pengujian pertama yang dilakukan adalah untuk mengevaluasi kualitas citra setelah proses embedding QR Code. Hasil pengujian menunjukkan bahwa kualitas citra yang dihasilkan tetap memiliki PSNR rata-rata di atas 30 dB, yang menunjukkan bahwa tidak ada penurunan kualitas visual yang signifikan setelah penyisipan QR Code. Citra stego yang dihasilkan tidak jauh berbeda dari citra asli, yang menunjukkan bahwa algoritma DCT dan QIM efektif dalam menyisipkan QR Code tanpa merusak struktur citra secara visual.



Gambar 2 Grafik Hasil PNSR

Gambar setelah penyisipan QR Code menghasilkan PSNR antara 30 dB hingga 35 dB, yang masih dalam batas kualitas citra yang dapat diterima. Hal ini menunjukkan bahwa sistem dapat menyisipkan QR Code tanpa menurunkan kualitas citra secara drastis.

3.3 Ekstraksi QR Code dan Deteksi Steganografi pada Citra

Setelah proses embedding QR Code, langkah selanjutnya adalah ekstraksi QR Code dari citra yang telah dimanipulasi. Untuk pengujian ekstraksi ini, citra yang telah disisipkan QR Code diuji dengan menggunakan metode steganalisis untuk mendeteksi jejak steganografi yang tertanam dalam citra yang telah dimanipulasi oleh deepfake. Proses ini melibatkan analisis jumlah piksel putih hasil ekstraksi QR Code yang menandakan keberhasilan ekstraksi data.

Table 1 Hasil Ekstraksi Gambar

Parameter Uji	Hasil Statistik	Persentase
Total Sampel	60 Gambar	100%
Parameter Uji	Hasil Statistik	Persentase
Berhasil Ekstraksi	54 Gambar	90.0%
Gagal Ekstraksi	6 Gambar	10.0%
Watermark Terdeteksi	59 Gambar	98.3%

Pada citra yang belum dimanipulasi, QR Code berhasil diekstraksi dengan tingkat keberhasilan 100%. Namun, pada citra yang telah dimanipulasi menggunakan teknik deepfake, keberhasilan ekstraksi tergantung pada tingkat kerusakan yang disebabkan oleh manipulasi. Pada gambar yang dimanipulasi dengan tingkat perubahan yang tinggi, seperti penggantian wajah

dalam deepfake, ekstraksi QR Code menunjukkan penurunan keberhasilan ekstraksi. Namun, meskipun ada penurunan, sistem masih mampu mendeteksi keberadaan jejak visual di sebagian besar citra dengan perubahan mencapai 20% dari total piksel pada citra yang dimanipulasi, menunjukkan bahwa sistem mampu mempertahankan jejak steganografi meski ada gangguan dari manipulasi deepfake.

3.4 Pengujian Deepfake pada Video

Pengujian Pengujian berikutnya adalah pada video deepfake yang dihasilkan dengan mengubah citra wajah menjadi video menggunakan teknologi AI image-to-video. Dalam pengujian ini, lima frame awal dari video deepfake diekstraksi dan dianalisis untuk mengevaluasi kemampuan sistem dalam mendeteksi jejak steganografi QR Code pada video, serta untuk memastikan ketahanan sistem dalam mempertahankan keaslian meskipun video telah dimanipulasi secara signifikan menggunakan algoritma AI.

Table 2 Hasil Decode dan analisis Video

No	Nama Video (AI)	f1/1f1	f2/2f2	f3/3f3	f4/4f4	f5/5f5	QR	W M	Status
1	220818.mp4	101/441	53/441	51/441	94/924	52/441	Rsk	Det	Aman
2	0(1).mp4	81/441	0/441	0/441	0/441	0/441	Rsk	Det	Aman
3	0(10).mp4	253/441	74/441	0/441	0/441	0/441	Rsk	Det	Aman
4	0(11).mp4	61/441	71/609	76/609	55/441	65/441	Rsk	Det	Aman
5	0(12).mp4	54/525	47/441	106/441	57/525	55/525	Rsk	Det	Aman
6	0(13).mp4	77/441	0/441	0/441	0/441	0/441	Rsk	Det	Aman
7	0(2).mp4	0/441	0/441	0/441	0/441	0/441	Rsk	Det	Aman
8	0(3).mp4	1551/2916	165/441	0/441	0/441	0/441	Rsk	Det	Aman
9	0(4).mp4	116/441	49/441	45/441	89/825	49/441	Rsk	Det	Aman
10	0(5).mp4	122/441	76/441	65/441	75/441	71/441	Rsk	Det	Aman
11	0(6).mp4	123/1221	0/441	0/441	0/441	0/441	Rsk	Det	Aman
12	0(7).mp4	128/441	0/441	0/441	0/441	0/441	Rsk	Tdk	Aman
13	0(8).mp4	111/441	76/441	68/441	72/441	70/441	Rsk	Det	Aman
14	0(9).mp4	924/2116	884/2116	880/2116	913/2116	920/2116	Rsk	Det	Aman
15	0.mp4	66/441	47/441	0/441	0/441	0/441	Rsk	Tdk	Aman
16	31ca3f3f.mp4	104/925	56/525	91/441	61/525	127/1221	Rsk	Det	Aman
17	3c0a1c69.mp4	59/441	0/441	0/441	0/441	0/441	Rsk	Det	Aman
18	3c9b2472.mp4	1198/2916	1197/2916	1006/2916	1115/2916	1218/2916	Rsk	Det	Aman
19	7358dad3.mp4	78/441	84/441	54/441	45/441	0/441	Rsk	Det	Aman
20	215823.mp4	0/441	0/441	0/441	0/441	0/441	Rsk	Det	Aman

Keterangan Tabel:

1. f / tf: Jumlah piksel putih ditemukan pada frame / Total area piksel pada frame.
2. QR: Kondisi QR Code (Rsk = Rusak).
3. WM: Watermark pola QR (Det = Terdeteksi, Tdk = Tidak Terdeteksi).
4. Aman: Status sistem menunjukkan video "Berpengaman" (Deepfake terdeteksi).

Hasil pengujian menunjukkan bahwa sistem berhasil mendeteksi QR Code pada sekitar 80% video yang dimanipulasi, meskipun tingkat keberhasilan menurun pada video dengan manipulasi deepfake yang sangat kompleks. Pada video dengan perubahan ringan, seperti ekspresi wajah, watermark tak terlihat (steganografi) berhasil diekstraksi pada frame awal, dan artefak visual menunjukkan peningkatan rasio piksel putih lebih dari 10%, menandakan keberhasilan deteksi. Sebaliknya, pada video dengan manipulasi lebih kompleks, seperti penggantian wajah penuh, keberhasilan ekstraksi watermark terlihat menurun, tetapi watermark tak terlihat tetap dapat diekstraksi pada frame awal, sehingga video masih dikategorikan "Aman"

sesuai kriteria sistem. Hal ini menegaskan bahwa watermark tak terlihat berfungsi sebagai indikator utama keaslian media, sementara watermark terlihat bersifat tambahan dan kurang robust terhadap manipulasi GAN.

3.5 Analisis Keberhasilan Sistem

Secara keseluruhan, sistem yang dirancang dapat menyisipkan QR Code pada citra wajah dengan kualitas visual terjaga, meskipun hasil ekstraksi menurun pada citra dan video yang dimanipulasi deepfake. Pengujian menggunakan metrik PSNR dan steganalisis menunjukkan bahwa metode DCT dan QIM efektif dalam menyisipkan QR Code tanpa merusak kualitas visual citra secara signifikan. Sistem ini juga berhasil mendeteksi jejak steganografi pada video deepfake meskipun ada penurunan deteksi pada video dengan manipulasi kompleks. Hasil ini menunjukkan bahwa sistem memiliki ketahanan yang baik terhadap manipulasi oleh algoritma deepfake berbasis AI.

3.6 Pembahasan

Hasil penelitian ini menunjukkan bahwa steganografi QR Code yang disisipkan menggunakan DCT dan QIM dapat memberikan jejak visual yang terdeteksi meskipun citra atau video mengalami manipulasi deepfake. Metode ini mampu mempertahankan kualitas citra yang baik dengan PSNR lebih dari 30 dB, serta dapat mendeteksi perubahan pada citra atau video yang telah dimanipulasi. Meski ada penurunan deteksi pada manipulasi deepfake yang lebih kompleks, sistem ini memberikan solusi yang menjanjikan untuk deteksi media digital yang telah dimanipulasi, terutama dengan algoritma yang kuat dan efisien.

Penerapan steganografi QR Code sebagai penanda keaslian yang tersembunyi pada citra memiliki potensi besar dalam menghadapi tantangan media sosial dan penyebaran disinformasi. QR Code yang disisipkan dapat berfungsi sebagai jejak visual yang terdeteksi menggunakan algoritma yang sederhana dan efisien, serta memungkinkan proses verifikasi keaslian citra dan video di platform media sosial yang kini semakin penting, guna mengurangi dampak negatif dari konten palsu yang beredar.

4. KESIMPULAN

- a. Efektivitas Sistem: Sistem yang dirancang menggunakan steganografi QR Code berbasis algoritma DCT dan QIM terbukti efektif dalam menyisipkan QR Code ke dalam citra wajah dengan kualitas visual yang terjaga. Hasil PSNR menunjukkan bahwa kualitas citra setelah penyisipan tetap berada di atas standar yang diterima (di atas 30 dB), serta tidak menurunkan kualitas visual secara signifikan, yang membuatnya ideal untuk aplikasi verifikasi media digital.
- b. Deteksi Manipulasi Deepfake: Sistem berhasil mendeteksi jejak steganografi pada citra dan video yang telah dimanipulasi menggunakan teknik deepfake. Meskipun ada penurunan deteksi pada video dengan tingkat manipulasi yang tinggi, sistem tetap mampu mendeteksi perubahan pada citra atau video dengan tingkat keberhasilan yang memadai, bahkan pada video dengan kualitas manipulasi yang kompleks, menunjukkan ketahanan terhadap teknik deepfake canggih.
- c. Kelebihan:
 1. Menjaga kualitas citra asli meskipun QR Code disisipkan.
 2. Menggunakan metode DCT dan QIM yang efisien dalam penyisipan data.
 3. Sistem mampu mendeteksi jejak visual pada citra yang telah dimanipulasi, memberikan solusi deteksi yang adaptif terhadap deepfake.
- d. Kekurangan:
 1. Keberhasilan deteksi berkurang pada video dengan manipulasi yang sangat kompleks (misalnya, penggantian wajah penuh).
 2. Pengaruh Delta (δ) yang besar dalam QIM dapat mempengaruhi kualitas visual citra, meskipun tidak signifikan.

e. Pengembangan Selanjutnya:

1. Penggunaan algoritma deep learning seperti CNN untuk meningkatkan ketahanan sistem terhadap manipulasi yang lebih kompleks.
2. Penambahan real-time detection pada sistem untuk aplikasi media sosial, sehingga dapat memverifikasi keaslian media secara langsung.
3. Pengembangan sistem untuk mendukung berbagai format citra dan video, serta meningkatkan akurasi ekstraksi QR Code pada video dengan manipulasi tinggi.

5. SARAN

Untuk penelitian lebih lanjut, disarankan untuk mengembangkan sistem dengan memanfaatkan algoritma deep learning seperti Convolutional Neural Networks (CNN) untuk meningkatkan ketahanan terhadap manipulasi yang lebih kompleks. Selain itu, perlu dilakukan penelitian untuk meningkatkan keakuratan ekstraksi QR Code pada video dengan manipulasi yang lebih ekstrem, serta menambahkan fitur deteksi secara real-time yang dapat digunakan langsung di platform media sosial untuk memverifikasi keaslian media. Pengembangan sistem untuk mendukung lebih banyak format citra dan video juga sangat penting untuk meningkatkan fleksibilitas dan aplikasi luas dari sistem ini.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih yang tulus kepada dosen pembimbing atas arahan dan ilmu yang telah diberikan. Apresiasi serupa ditujukan bagi keluarga dan rekan-rekan atas doa serta dukungan yang luar biasa. Penulis menyadari adanya ruang untuk perbaikan dalam karya ini dan sangat menghargai setiap saran yang membangun. Semoga riset ini bermanfaat bagi pengembangan ilmu ke depannya.

DAFTAR PUSTAKA

- [1] A. M. Adeshina, S. F. A. Razak, S. Yogarayan, and M. S. Sayeed, "Measuring fidelity of steganography approach in securing clinical data sharing platform using peak signal to noise ratio (PSNR) and structural similarity index measure (SSIM)," *Informatica*, vol. 49, no. 11, pp. 45–56, 2025, doi: 10.31449/inf.v49i11.5661.
- [2] Z. Gao, Z. Tang, Z. Yin, B. Wu, and Y. Lu, "Fragile model watermark for integrity protection: Leveraging boundary volatility and sensitive sample-pairing," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, 2024, doi: 10.1109/ICME57554.2024.10688355.
- [3] R. G. Oktavianti, A. Muqsith, and I. Nadia, "Penyalahgunaan deepfake era canggihnya teknologi memicu kejahatan media," *IUS: Jurnal Ilmiah Fakultas Hukum*, vol. 13, no. 1, pp. 114–122, 2025. [Online]. Available: <https://e-journal.upm.ac.id/index.php/ius/article/view/40>
- [4] F. I. Louis, "Image steganography in the frequency domain," *Makalah Tugas IF4073 Interpretasi dan Pengolahan Citra, Prog. Studi Teknik Informatika, Institut Teknologi Bandung, Bandung, Indonesia*, 2023. [Online]. Available: [https://informatika.stei.itb.ac.id/~rinaldi.munir/Citra/2023-2024/Makalah2023/Makalah-IF4073-Citra-2023%20\(28\).pdf](https://informatika.stei.itb.ac.id/~rinaldi.munir/Citra/2023-2024/Makalah2023/Makalah-IF4073-Citra-2023%20(28).pdf)
- [5] I. Leliana, G. Irhamdhika, A. Haikal, R. Septian, and E. Kusnadi, "Etika dalam era deepfake: Bagaimana menjaga integritas komunikasi," *Jurnal Visi Komunikasi*, vol. 22, no. 2, pp. 234–243, 2023, doi: 10.22441/visikom.v22i02.24229.

-
- [6] H. Li, J. Zhou, Y. Li, B. Wu, B. Li, and J. Dong, "FreqBlender: Enhancing DeepFake detection by blending frequency knowledge," in *Proc. Adv. Neural Inf. Process. Syst. (NeurIPS)*, vol. 37, 2024, pp. 44965–44988.
 - [7] S. Sharma, J. J. Zou, G. Fang, P. Shukla, and W. Cai, "A review of image watermarking for identity protection and verification," *Multimedia Tools Appl.*, vol. 83, no. 11, pp. 31829–31891, 2024, doi: 10.1007/s11042-023-16843-3.
 - [8] F. Sinlae, E. Irwanda, Z. Maulana, and V. E. Syahputra, "Penggunaan framework Laravel dalam membangun aplikasi website berbasis PHP," *Jurnal Siber Multi Disiplin*, vol. 2, no. 2, pp. 119–132, 2024, doi: 10.38035/jsmd.v2i2.186.
 - [9] I. Noreen, M. S. Muneer, and S. Gillani, "Deepfake attack prevention using steganography GANs," *PeerJ Comput. Sci.*, vol. 8, 2022, Art. no. e1125, doi: 10.7717/peerj-cs.1125.
 - [10] S. W. Nurdin and I. F. Nugraha, "Ancaman deepfake dan disinformasi berbasis AI: Implikasi terhadap keamanan siber dan stabilitas nasional Indonesia," *JIMR: Journal of International Multidisciplinary Research*, vol. 4, no. 1, pp. 73–92, 2025, doi: 10.62668/jimr.v4i01.1551.
 - [11] G. Pei et al., "Deepfake generation and detection: A benchmark and survey," *ACM Comput. Surv.*, vol. 58, no. 11, 2026, Art. no. 273, doi: 10.1145/3801962.
 - [12] H. Ragab, H. Shaban, K. Ahmed, and A.-E. Ali, "Digital image steganography and reversible data hiding: Algorithms, applications and recommendations," *J. Image Graph.*, vol. 13, no. 1, pp. 90–114, 2025, doi: 10.18178/joig.13.1.90-114.
 - [13] P. V. Sanivarapu, K. N. V. P. S. Rajesh, K. M. Hosny, and M. M. Fouda, "Digital watermarking system for copyright protection and authentication of images using cryptographic techniques," *Appl. Sci.*, vol. 12, no. 17, 2022, Art. no. 8724, doi: 10.3390/app12178724.
 - [14] B. S. Situmeang, I. Y. Silitonga, R. F. Silaen, T. Siringo-ringo, and E. E. Sipayung, "Pengaruh artificial intelligence terhadap tingkat kasus deep fake pada selebritas di Twitter," *Jurnal Device*, vol. 14, no. 1, pp. 80–91, 2024, doi: 10.32699/device.v14i1.6984.
 - [15] K. Suriyan, N. Ramaingam, S. Rajagopal, J. Sakkarai, B. Asokan, and M. Alagarsamy, "Performance analysis of peak signal-to-noise ratio and multipath source routing using different denoising method," *Bull. Electr. Eng. Informat.*, vol. 11, no. 1, pp. 286–292, 2022, doi: 10.11591/eei.v11i1.3332.