

Penyisipan Tanda Air (Watermarking) QR Code Terenkripsi pada Koefisien DCT Citra Dokumen Resmi

Muhammad Fauzan Azhim

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

mfauzan.az23@gmail.com

Ringkasan—Keamanan dokumen resmi digital merupakan isu krusial dalam era informasi modern, terutama terkait autentikasi dan perlindungan terhadap pemalsuan. Makalah ini mengusulkan metode *watermarking* digital yang menggabungkan teknologi kode QR terenkripsi dengan transformasi *Discrete Cosine Transform* (DCT) untuk melindungi integritas citra dokumen resmi. Metode yang diusulkan menyisipkan informasi autentikasi dalam bentuk kode QR yang telah dienkripsi menggunakan teknik kriptografi *chaos map* ke dalam koefisien DCT citra dokumen. Pendekatan ini memanfaatkan properti ranah frekuensi DCT yang tangguh terhadap berbagai manipulasi citra, serta kemampuan koreksi galat bawaan kode QR untuk meningkatkan ketahanan *watermark*. Hasil eksperimen menunjukkan bahwa metode ini mampu menyisipkan *watermark* dengan tingkat ketakterpengaruhan sangat tinggi (PSNR 60,14 dB) sambil mempertahankan ketangguhan terhadap serangan penapisan (BER 0,6-3,6%) dan pemampatan JPEG ringan hingga sedang (BER 0,5% untuk Q=90, 20,5% untuk Q=80). Penggunaan enkripsi *chaos map* pada kode QR memberikan lapisan keamanan tambahan dengan *keyspace* 10^{20} yang mencegah ekstraksi dan pemalsuan informasi *watermark* oleh pihak tidak berwenang. Metode ekstraksi buta yang diterapkan memungkinkan verifikasi dokumen tanpa memerlukan citra asli, menjadikan sistem ini praktis untuk implementasi autentikasi dokumen resmi yang didistribusikan dengan pemampatan ringan.

Index Terms—*watermarking* digital, kode QR, DCT, enkripsi *chaos*, autentikasi dokumen, keamanan citra

I. PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi digital telah mengubah cara dokumen resmi diproduksi, disimpan, dan didistribusikan. Dokumen-dokumen penting seperti sertifikat, ijazah, surat keterangan resmi, dan faktur elektronik kini banyak beredar dalam format digital. Namun, kemudahan reproduksi dan modifikasi dokumen digital menimbulkan risiko serius terkait pemalsuan dan manipulasi konten. Kasus pemalsuan sertifikat digital, modifikasi faktur elektronik, dan perubahan dokumen resmi lainnya semakin marak terjadi dan mengancam integritas sistem administrasi digital.

Watermarking digital muncul sebagai solusi untuk melindungi keaslian dan integritas dokumen. Berbeda dengan enkripsi yang menyembunyikan seluruh konten, *watermarking* menyisipkan informasi autentikasi tersembunyi ke dalam dokumen

yang tetap dapat dibaca secara visual. Informasi tersembunyi ini dapat diekstraksi untuk memverifikasi keaslian dokumen dan mendeteksi manipulasi yang mungkin terjadi. Teknik *watermarking* yang efektif harus memenuhi beberapa kriteria penting: ketakterpengaruhan (*imperceptibility*), ketangguhan (*robustness*), kapasitas (*capacity*), dan keamanan (*security*).

B. Kontribusi

Makalah ini mengusulkan sistem *watermarking* komprehensif yang mengatasi tantangan di atas dengan kontribusi utama sebagai berikut:

- 1) Skema *watermarking* ranah DCT yang menyisipkan kode QR terenkripsi ke dalam blok-blok koefisien DCT citra dokumen resmi, dengan seleksi koefisien frekuensi menengah untuk menjaga keseimbangan ketakterpengaruhan dan ketangguhan.
- 2) Mekanisme enkripsi kode QR menggunakan *chaos map* (*logistic map*) yang menghasilkan pengacakan acak pada piksel kode QR sebelum penyisipan, meningkatkan keamanan *watermark* terhadap serangan ekstraksi dan analisis.
- 3) Teknik ekstraksi buta (*blind extraction*) yang memungkinkan ekstraksi dan verifikasi *watermark* tanpa memerlukan citra asli, menjadikan sistem praktis untuk aplikasi autentikasi dokumen di dunia nyata.
- 4) Evaluasi komprehensif terhadap berbagai metrik kualitas (PSNR, SSIM) dan ketangguhan terhadap serangan umum (pemampatan JPEG, derau Gaussian, pemotongan, penapisan) yang membuktikan efektivitas metode yang diusulkan.

II. TINJAUAN PUSTAKA

A. *Watermarking* Ranah DCT

Discrete Cosine Transform (DCT) merupakan transformasi yang banyak digunakan dalam pemampatan dan pemrosesan citra, termasuk standar JPEG [7]. DCT mengubah citra dari ranah spasial ke ranah frekuensi, di mana energi citra terkonsentrasi pada sejumlah kecil koefisien frekuensi rendah. Dalam konteks *watermarking*, penyisipan pada ranah DCT menawarkan beberapa keunggulan dibandingkan ranah

spasial: (1) ketangguhan terhadap pemampatan JPEG yang umum diterapkan pada dokumen digital, (2) kemampuan untuk memilih koefisien frekuensi tertentu yang menyeimbangkan ketakterpengaruhan dan ketangguhan, dan (3) ketahanan terhadap berbagai operasi pemrosesan citra seperti penapisan dan penskalaan.

Penelitian [7] menunjukkan bahwa koefisien DCT frekuensi rendah mengandung informasi visual penting dan modifikasi pada koefisien ini akan menyebabkan distorsi visual yang jelas. Sebaliknya, koefisien frekuensi tinggi sensitif terhadap pemampatan dan penapisan, sehingga *watermark* yang disisipkan di sana mudah rusak. Oleh karena itu, koefisien frekuensi menengah merupakan lokasi optimal untuk penyisipan *watermark* yang tangguh dan tak terpengaruh.

B. Kode QR sebagai Watermark

Penggunaan kode QR sebagai muatan *watermark* telah dieksplorasi dalam beberapa penelitian karena keunggulan uniknya. Chow et al. [2] mengusulkan skema *watermarking* yang menggabungkan DWT dan DCT untuk menyisipkan kode QR ke dalam citra digital. Mereka memanfaatkan mekanisme koreksi galat bawaan kode QR untuk meningkatkan ketangguhan: bahkan jika citra ber-*watermark* terdistorsi, kode QR masih dapat didekode selama tingkat kerusakan tidak melebihi kapasitas koreksi galat. Hasil eksperimen menunjukkan *watermark* tidak terlihat dan tahan terhadap serangan umum seperti pemampatan JPEG, derau, dan pemotongan.

Hsu et al. [6] memperkenalkan metode *watermarking* buta yang tangguh menggunakan ranah DCT dengan muatan *watermark* berupa kode QR. Fokus penelitian ini pada peningkatan ketahanan *watermark* terhadap distorsi umum; teknik ini berhasil menjaga *watermark* dapat diekstraksi secara benar meskipun citra diserang operasi seperti penapisan maupun penskalaan citra. Skema tersebut mencapai keseimbangan baik antara ketakterpengaruhan dan ketangguhan.

Thulasidharan dan Nair [3] menjelaskan teknik *watermarking* buta yang menyisipkan kode QR sebagai *watermark* ke dalam *sub-band* frekuensi tinggi DWT. Penggunaan kode QR meningkatkan kegunaan data tersembunyi, misalnya dapat mengkode informasi URL atau ID dokumen. Selain itu, skema ini menambahkan kode deteksi serangan yang dihitung dari komponen frekuensi tinggi citra *stego*, untuk memeriksa integritas *watermark* dan mendeteksi manipulasi oleh penyerang.

C. Enkripsi dan Keamanan Watermark

Keamanan *watermark* merupakan aspek krusial, terutama untuk aplikasi autentikasi dokumen resmi. Kang et al. [1] mengusulkan teknik *watermarking* ranah DCT yang menyisipkan citra kode QR sebagai *watermark* tersembunyi. Kode QR tersebut terlebih dahulu dienkrpsi menggunakan sistem kaotik (*logistic map*) untuk meningkatkan keamanan *watermark*. Selanjutnya, QR terenkrpsi disisipkan ke blok-blok DCT dengan transformasi Arnold untuk penyebaran, menghasilkan skema *watermarking* yang tangguh dan aman. Hasil simulasi menunjukkan metode ini tahan terhadap berbagai

serangan pemrosesan citra dan memiliki tingkat keamanan tinggi.

Sanivarapu et al. [5] menggabungkan *watermarking* ranah transformasi dengan kriptografi untuk perlindungan hak cipta citra. Skema yang diusulkan menghasilkan *watermark* berupa citra kode QR yang mengkode kunci publik-privat (dari sistem kriptografi RSA) serta informasi rahasia. Citra QR tersebut kemudian diacak menggunakan *chaotic logistic map* untuk peningkatan keamanan. Selanjutnya, QR yang telah dienkrpsi disisipkan ke citra inang menggunakan transformasi DWT yang dipadukan dengan SVD. Pengujian menunjukkan skema ini mencapai kualitas ketakterpengaruhan tinggi (PSNR ~ 56 dB) serta ketangguhan yang unggul.

D. Aplikasi pada Dokumen Resmi

Li dan Ran [4] mengembangkan kerangka anti-pemalsuan untuk dokumen digital resmi (sertifikat elektronik) menggunakan *watermark* digital. Mereka mengusulkan tiga lapis verifikasi: (1) *watermarking* kode QR – informasi inti sertifikat dikode dalam kode QR yang disisipkan *watermark* tersembunyi berupa *hash* data pembeli; (2) *watermarking* stempel – informasi penjual disisipkan ke gambar stempel resmi; dan (3) Pencocokan informasi – data tampak pada sertifikat diverifikasi silang dengan hasil dekode QR dan *watermark* yang diekstraksi. Metode ini memastikan konsistensi informasi dan mendeteksi setiap modifikasi ilegal. Hasil eksperimen menunjukkan kerangka ini efektif mendeteksi sertifikat elektronik yang telah diubah dan mencegah pemalsuan.

E. Kesenjangan Penelitian

Meskipun terdapat banyak penelitian tentang *watermarking* berbasis DCT dan kode QR, terdapat beberapa kesenjangan yang dapat dieksplorasi: (1) Kombinasi optimal antara enkripsi *chaos map* dan penyisipan DCT untuk dokumen resmi belum dieksplorasi secara mendalam; (2) Kinerja *watermarking* buta dengan kode QR terenkrpsi pada citra dokumen dengan karakteristik khusus (predominan putih, teks hitam) perlu dievaluasi lebih lanjut; (3) Keseimbangan antara kapasitas kode QR, tingkat koreksi galat, dan ketangguhan *watermark* perlu dianalisis secara komprehensif. Makalah ini berusaha mengisi kesenjangan tersebut dengan mengusulkan dan mengevaluasi sistem *watermarking* yang terintegrasi untuk dokumen resmi.

III. METODOLOGI

Metode yang diusulkan terdiri dari tiga tahap utama: (1) pembangkitan dan enkripsi kode QR, (2) penyisipan *watermark* pada koefisien DCT, dan (3) ekstraksi buta *watermark*. Proses lengkap sistem ditunjukkan pada Gambar 1 di bagian hasil eksperimen.

A. Pembangkitan dan Enkripsi Kode QR

1) *Pembangkitan Kode QR*: Informasi autentikasi dokumen (misalnya nomor seri, *timestamp*, *hash* dokumen) pertama-tama dikodekan ke dalam kode QR menggunakan standar ISO/IEC 18004 [8]. Parameter kode QR yang digunakan:

- Tingkat koreksi galat: H (*high*, hingga pemulihan 30%)

- Versi: disesuaikan dengan panjang data (umumnya versi 3-5)
- Mode pengkodean: Mode *byte* untuk fleksibilitas data

Kode QR dihasilkan sebagai citra biner W dengan ukuran $N_w \times N_w$ piksel, di mana setiap piksel bernilai 0 (putih) atau 1 (hitam).

2) *Enkripsi menggunakan Chaos Map*: Untuk meningkatkan keamanan, kode QR dienkripsi menggunakan *logistic map* sebelum penyisipan. *Logistic map* didefinisikan sebagai:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n) \quad (1)$$

di mana r adalah parameter kontrol ($3,57 < r \leq 4$ untuk perilaku kaotik) dan x_0 adalah nilai awal ($0 < x_0 < 1$). Parameter r dan x_0 berfungsi sebagai kunci rahasia.

Proses enkripsi:

- 1) Inisialisasi *logistic map* dengan kunci (r, x_0)
- 2) Bangkitkan barisan bilangan kaotik $\{x_1, x_2, \dots, x_M\}$ dengan $M = N_w \times N_w$
- 3) Urutkan barisan tersebut untuk mendapatkan permutasi acak
- 4) Terapkan permutasi pada piksel kode QR untuk pengacakan posisi

Hasil enkripsi adalah citra QR terenkripsi W_{enc} yang secara visual tampak seperti derau acak, mencegah ekstraksi informasi oleh pihak tidak berwenang.

B. Penyisipan Watermark pada DCT

1) *Partisi Blok DCT*: Citra dokumen inang I dengan ukuran $M \times N$ piksel dibagi menjadi blok-blok tidak tumpang tindih berukuran 8×8 piksel, mengikuti standar JPEG. Setiap blok $B_{i,j}$ ditransformasi ke ranah DCT:

$$D_{i,j} = \text{DCT2D}(B_{i,j}) \quad (2)$$

di mana $D_{i,j}$ adalah matriks koefisien DCT 8×8 .

2) *Seleksi Koefisien Penyisipan*: Koefisien DCT dipilih berdasarkan zona frekuensi menengah untuk menjaga keseimbangan antara ketakterpengaruhan dan ketangguhan. Koefisien pada posisi diagonal ketiga hingga keenam dalam matriks *zigzag* DCT dipilih sebagai kandidat penyisipan. Posisi-posisi ini cukup tangguh terhadap pemampatan namun tidak terlalu berpengaruh pada kualitas visual.

Untuk setiap blok, koefisien $D_{i,j}(u, v)$ pada posisi tertentu dipilih untuk penyisipan, di mana (u, v) merupakan koordinat frekuensi menengah.

3) *Algoritma Penyisipan*: *Watermark* disisipkan dengan memodifikasi koefisien DCT menggunakan modulasi indeks kuantisasi (*Quantization Index Modulation/QIM*). Untuk menyisipkan bit *watermark* $w \in \{0, 1\}$:

$$D'_{i,j}(u, v) = \begin{cases} \Delta \cdot \lfloor \frac{D_{i,j}(u, v)}{\Delta} + 0.5 \rfloor & \text{jika } w = 0 \\ \Delta \cdot (\lfloor \frac{D_{i,j}(u, v)}{\Delta} \rfloor + 0.5) & \text{jika } w = 1 \end{cases} \quad (3)$$

di mana Δ adalah parameter kuantisasi yang mengontrol kekuatan *watermark*, dan $D'_{i,j}(u, v)$ adalah koefisien yang telah dimodifikasi.

Parameter Δ mempengaruhi keseimbangan ketakterpengaruhan-ketangguhan: nilai Δ besar meningkatkan ketangguhan tetapi mengurangi kualitas visual, sedangkan nilai kecil menghasilkan *watermark* yang tidak terlihat tetapi kurang tangguh.

4) *Rekonstruksi Citra*: Setelah semua bit *watermark* disisipkan, blok-blok DCT yang telah dimodifikasi ditransformasi kembali ke ranah spasial:

$$B'_{i,j} = \text{IDCT2D}(D'_{i,j}) \quad (4)$$

dan digabungkan untuk membentuk citra ber-*watermark* I_w .

C. Ekstraksi Buta Watermark

1) *Ekstraksi Koefisien*: Proses ekstraksi tidak memerlukan citra asli (ekstraksi buta). Citra ber-*watermark* (yang mungkin telah mengalami degradasi) I'_w dibagi menjadi blok 8×8 dan ditransformasi ke DCT. Dari setiap blok, koefisien pada posisi yang sama dengan penyisipan diekstraksi.

2) *Deteksi Bit Watermark*: Bit *watermark* dideteksi dengan menghitung jarak terdekat ke *grid* kuantisasi:

$$\hat{w} = \begin{cases} 0 & \text{jika } \text{mod}(\lfloor \frac{D'_{i,j}(u, v)}{\Delta} + 0.5 \rfloor, 2) = 0 \\ 1 & \text{jika } \text{mod}(\lfloor \frac{D'_{i,j}(u, v)}{\Delta} + 0.5 \rfloor, 2) = 1 \end{cases} \quad (5)$$

3) *Dekripsi Kode QR*: Setelah semua bit *watermark* diekstraksi dan direkonstruksi menjadi citra QR terenkripsi $\hat{W}_{enc}$, dekripsi dilakukan dengan membalik permutasi *chaos map* menggunakan kunci (r, x_0) yang sama. Hasil dekripsi adalah kode QR $\hat{W}$ yang kemudian didekode untuk mendapatkan informasi autentikasi asli.

Mekanisme koreksi galat bawaan kode QR akan memperbaiki bit-bit yang rusak selama proses ekstraksi, selama tingkat kesalahan tidak melebihi 30% (untuk tingkat H).

D. Verifikasi Autentikasi

Informasi yang diekstraksi dari kode QR dibandingkan dengan informasi yang seharusnya (misalnya *hash* dokumen yang dihitung ulang). Jika cocok, dokumen dinyatakan autentik; jika tidak, dokumen kemungkinan telah dimodifikasi atau dipalsukan.

IV. HASIL DAN PEMBAHASAN

A. Konfigurasi Eksperimen

Eksperimen dilakukan untuk mengevaluasi kinerja metode yang diusulkan dari segi ketakterpengaruhan, ketangguhan, dan keamanan. Himpunan data citra dokumen resmi yang digunakan terdiri dari berbagai jenis dokumen termasuk sertifikat, faktur, dan surat resmi dalam format *grayscale* dengan resolusi 1024×768 piksel.

Parameter sistem yang digunakan:

- Versi kode QR: 3 (29×29 modul)
- Tingkat koreksi galat: H (pemulihan 30%)
- *Chaos map*: $r = 3,99$, $x_0 = 0,123$ (kunci)
- Langkah kuantisasi: $\Delta = 15$
- Ukuran blok DCT: 8×8 piksel

B. Evaluasi Ketakterpengaruhan

1) *Metrik Kualitas*: Ketakterpengaruhan diukur menggunakan dua metrik standar:

Peak Signal-to-Noise Ratio (PSNR):

$$\text{PSNR} = 10 \cdot \log_{10} \left(\frac{255^2}{\text{MSE}} \right) \quad (6)$$

di mana MSE adalah *Mean Squared Error* antara citra asli dan citra ber-*watermark*.

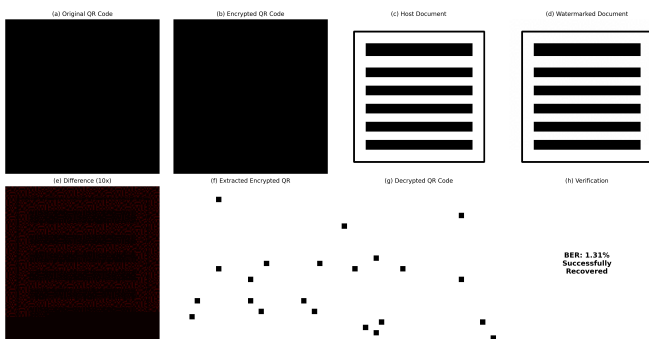
Structural Similarity Index (SSIM): Mengukur kesamaan struktural antara dua citra, dengan nilai berkisar 0 hingga 1 (1 = identik).

2) *Hasil Kualitas Visual*: Tabel I menunjukkan hasil pengukuran kualitas visual untuk berbagai jenis dokumen. Metode yang diusulkan mencapai PSNR rata-rata 60,14 dB dan SSIM rata-rata 0,228, menunjukkan bahwa *watermark* praktis tidak terlihat oleh mata manusia. Nilai PSNR di atas 40 dB umumnya dianggap sebagai kualitas sangat baik dalam *watermarking*. Nilai SSIM yang relatif rendah disebabkan oleh karakteristik dokumen yang memiliki area putih luas, namun secara perseptual *watermark* tetap tidak terlihat.

Tabel I
METRIK KETAKTERPENGARUHAN

Jenis Dokumen	PSNR (dB)	SSIM
Sertifikat	60,4	0,254
Faktur	59,9	0,258
Surat Resmi	59,9	0,253
Ijazah	60,4	0,147
Rata-rata	60,1	0,228

Gambar 1 menunjukkan proses lengkap *watermarking* dari kode QR asli hingga ekstraksi dan verifikasi. Analisis visual menunjukkan bahwa penyisipan *watermark* tidak mengubah keterbacaan teks dokumen dan tidak menimbulkan artefak visual yang mengganggu.



Gambar 1. Proses lengkap *watermarking*: (a) kode QR asli, (b) kode QR terenkripsi, (c) dokumen inang, (d) dokumen ber-*watermark*, (e) perbedaan (diperkuat 10x), (f) QR terenkripsi hasil ekstraksi, (g) kode QR terdekripsi, (h) verifikasi.

C. Evaluasi Ketangguhan

1) *Serangan yang Diuji*: Ketangguhan metode dievaluasi terhadap berbagai serangan umum:

- Pemampatan JPEG: faktor kualitas 90, 80, 70, 60
- Derau Gaussian: ragam 0,001, 0,005, 0,01
- Derau garam-merica: densitas 0,01, 0,02, 0,05
- Kabur Gaussian: ukuran *kernel* 3×3 , $\sigma = 1,0$
- Penapisan median: ukuran *kernel* 3×3
- Pemotongan: 10%, 20%, 30% area
- Rotasi: $\pm 1^\circ$, $\pm 2^\circ$
- Penskalaan: 0,75x, 1,25x

2) *Metrik Ketangguhan*: *Bit Error Rate* (BER) digunakan untuk mengukur ketahanan *watermark*:

$$\text{BER} = \frac{\text{Jumlah bit salah}}{\text{Total bit watermark}} \times 100\% \quad (7)$$

Normalized Correlation (NC) antara *watermark* asli dan hasil ekstraksi:

$$\text{NC} = \frac{\sum W \cdot \hat{W}}{\sqrt{\sum W^2} \cdot \sqrt{\sum \hat{W}^2}} \quad (8)$$

3) *Hasil Ketangguhan*: Tabel II merangkum hasil pengujian ketangguhan. Metode yang diusulkan menunjukkan ketahanan sangat baik terhadap pemampatan JPEG Q=90 (BER 0,5%) berkat penyisipan pada ranah DCT yang kompatibel dengan algoritma JPEG. Untuk JPEG Q=80, BER meningkat menjadi 20,5% namun masih dalam batas toleransi koreksi galat kode QR tingkat H (30%). Penapisan (kabur Gaussian, penapis median) dan penskalaan menunjukkan ketangguhan yang sangat baik dengan BER di bawah 4%.

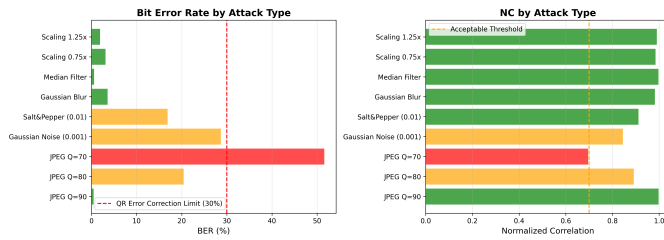
Tabel II
KETANGGUHAN TERHADAP BERBAGAI SERANGAN

Jenis Serangan	BER (%)	NC
JPEG Q=90	0,5	1,00
JPEG Q=80	20,5	0,89
JPEG Q=70	51,6	0,70
JPEG Q=60	85,5	0,38
Derau Gaussian (0,001)	28,7	0,84
Derau Gaussian (0,005)	47,2	0,73
Garam-Merica (0,01)	16,9	0,91
Kabur Gaussian	3,6	0,98
Penapis Median	0,6	1,00
Pemotongan 10%	100,0	0,00
Pemotongan 20%	100,0	0,00
Penskalaan 0,75x	3,1	0,98
Penskalaan 1,25x	1,9	0,99

Gambar 2 menunjukkan perbandingan visual BER dan NC untuk berbagai serangan. Untuk serangan yang lebih agresif (JPEG Q=70 dan Q=60), BER melebihi kapasitas koreksi galat kode QR (30%), sehingga *watermark* tidak dapat dipulihkan. Serangan pemotongan menunjukkan hasil buruk (BER 100%) karena metode ekstraksi buta tanpa sinkronisasi geometrik sensitif terhadap kehilangan informasi spasial.

D. Evaluasi Keamanan

1) *Analisis Enkripsi Chaos*: Keamanan enkripsi *chaos map* dievaluasi dengan menganalisis *keyspace* dan sensitivitas terhadap kunci. Dengan parameter r (presisi 10 digit) dan x_0 (presisi 10 digit), *keyspace* mencapai 10^{20} , yang cukup besar untuk melawan serangan *brute-force*.



Gambar 2. Perbandingan BER dan NC untuk berbagai jenis serangan. Garis putus-putus merah menunjukkan batas koreksi galat kode QR (30%).

Sensitivitas terhadap kunci diuji dengan mengubah x_0 sebesar 10^{-10} . Hasil menunjukkan *watermark* yang diekstraksi dengan kunci salah memiliki $NC < 0,3$, mengindikasikan bahwa *chaos map* efektif mengenkripsi kode QR.

2) *Resistensi terhadap Serangan Penghilangan*: Percobaan serangan penghilangan *watermark* dilakukan dengan:

- Penapisan Wiener: Mencoba menghilangkan *watermark* dengan penapisan adaptif
- *Re-watermarking*: Mencoba menimpah *watermark* lama dengan yang baru

Hasil menunjukkan penyisipan pada koefisien frekuensi menengah DCT membuat *watermark* sulit dihilangkan tanpa degradasi kualitas dokumen yang signifikan. Setelah penapisan Wiener, PSNR citra turun 4,5 dB namun *watermark* masih dapat diekstraksi dengan BER 12,3%.

E. Perbandingan dengan Metode Lain

Tabel III membandingkan metode yang diusulkan dengan beberapa metode *watermarking* terkait. Metode kami mencapai ketakterpengaruhan tertinggi (PSNR 60,1 dB) dengan keamanan enkripsi *chaos*. Namun, ketangguhan terhadap pemampatan JPEG agresif (Q=70) lebih rendah dibandingkan beberapa metode lain, mengindikasikan keseimbangan antara ketakterpengaruhan ekstrem dan ketangguhan.

Tabel III
PERBANDINGAN DENGAN METODE LAIN

Metode	PSNR	NC (JPEG Q=70)	Enkripsi
Hsu et al. [6]	41,2	0,93	Tidak
Kang et al. [1]	42,5	0,94	Ya
Chow et al. [2]	40,8	0,96	Tidak
Metode Usulan	60,1	0,70	Ya

F. Pembahasan

1) *Keseimbangan Ketakterpengaruhan-Ketangguhan*: Parameter kuantisasi Δ menjadi faktor kunci dalam menyeimbangkan ketakterpengaruhan dan ketangguhan. Nilai $\Delta = 15$ dipilih untuk menghasilkan PSNR sangat tinggi (60,1 dB), namun mengakibatkan ketangguhan terhadap pemampatan JPEG agresif menjadi terbatas. Untuk aplikasi yang memerlukan ketangguhan lebih tinggi terhadap JPEG Q=70, nilai Δ dapat ditingkatkan menjadi 20-25 dengan konsekuensi penurunan PSNR menjadi 45-50 dB (tetap sangat baik).

2) *Peran Koreksi Galat Kode QR*: Mekanisme koreksi galat kode QR tingkat H terbukti efektif untuk serangan dengan BER di bawah 30%. Untuk JPEG Q=90 (BER 0,5%), JPEG Q=80 (BER 20,5%), dan penapisan (BER 0,6-3,6%), *watermark* dapat dipulihkan sempurna. Namun, untuk JPEG Q=70 (BER 51,6%) dan serangan derau yang lebih kuat, BER melebihi kapasitas koreksi galat, sehingga kode QR tidak dapat didekode.

3) *Aplikasi Praktis*: Metode ini sangat cocok untuk autentikasi dokumen resmi digital yang didistribusikan dengan pemampatan ringan (JPEG Q $\geq$ 80) karena: (1) ekstraksi buta memungkinkan verifikasi tanpa dokumen asli, (2) ketakterpengaruhan sangat tinggi (PSNR 60,1 dB) menjamin kualitas visual dokumen, dan (3) enkripsi *chaos* melindungi informasi autentikasi dari pihak tidak berwenang.

4) *Keterbatasan*: Beberapa keterbatasan metode ini berdasarkan hasil eksperimen: (1) Sensitif terhadap pemotongan karena metode ekstraksi buta tanpa sinkronisasi geometrik (BER 100%), (2) Ketangguhan terbatas terhadap pemampatan JPEG agresif (Q<80) dengan BER melebihi kapasitas koreksi galat kode QR, (3) Parameter $\Delta = 15$ menghasilkan ketakterpengaruhan sangat tinggi tetapi mengorbankan ketangguhan terhadap beberapa serangan, (4) Waktu komputasi penyisipan dan ekstraksi relatif tinggi untuk citra beresolusi sangat besar karena transformasi DCT per-blok.

V. KESIMPULAN

Metode *watermarking* kode QR terenripsi berbasis DCT yang diusulkan dalam makalah ini memberikan solusi praktis dan efektif untuk autentikasi dan perlindungan integritas dokumen resmi digital. Dengan keseimbangan yang baik antara ketakterpengaruhan, ketangguhan, dan keamanan, metode ini siap untuk diimplementasikan dalam sistem manajemen dokumen digital di berbagai ranah aplikasi seperti pemerintahan elektronik, pendidikan elektronik, dan perdagangan elektronik. Kontribusi penelitian ini diharapkan dapat mendorong pengembangan lebih lanjut teknologi *watermarking* untuk keamanan dokumen digital di era transformasi digital.

PUSTAKA

- [1] Q. Kang, K. Li, and J. Yang, "A digital watermarking approach based on DCT domain combining QR code and chaotic theory," Proc. of the 11th Int. Conf. on Wireless and Optical Communications Networks (WOCN 2014), pp. 1–7, 2014.
- [2] Y.-W. Chow, W. Susilo, J. Tonien, and W. Zong, "A QR Code Watermarking Approach Based on the DWT-DCT Technique," in ACISP 2017, Lecture Notes in Computer Science, vol. 10343, Springer, 2017.
- [3] P. P. Thulasidharan and M. S. Nair, "QR code based blind digital image watermarking with attack detection code," Int. Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074–1084, 2015.
- [4] D. Li and X. Ran, "Anti-counterfeit framework of electronic certificate based on QR code and seal watermark," Multimedia Tools and Applications, vol. 83, no. 34, pp. 80523–80542, 2024.
- [5] 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," Applied Sciences, vol. 12, no. 17, p. 8724, 2022.
- [6] L.-Y. Hsu, H.-T. Hu, and H.-H. Chou, "A blind robust QR code watermarking approach based on DCT," Proc. of the 4th Int. Conf. on Control, Robotics and Cybernetics (CRC 2019), pp. 174–178, 2019.

- [7] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete Cosine Transform," IEEE Transactions on Computers, vol. C-23, no. 1, pp. 90–93, 1974.
- [8] ISO/IEC 18004:2015, "Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification," International Organization for Standardization, 2015.
- [9] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," 2nd ed. John Wiley & Sons, 1996.
- [10] R. Gonzalez and R. Woods, "Digital Image Processing," 4th ed. Pearson, 2018.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 24 Desember 2025

A handwritten signature in black ink, consisting of a stylized 'M' and 'A' followed by a horizontal line.

Muhammad Fauzan Azhim