2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)

Otentikasi Gambar menggunakan QR Code Pendekatan Watermarking berdasarkan Gambar Segmentasi

Xiaomei Liu
School of Information Science and Technology
University of International Relations
Beijing,China
liuxiaomei@uir.edu.cn

Xin Tang*
Sekolah Ilmu Informasi dan Teknologi
Universitas Hubungan Internasional
Beijing,China xtang@uir.edu.cn

***Abstrak*— Perkembangan teknologi multimedia yang pesat telah membawa tantangan besar terkait keamanan konten multimedia. Tanda air digital adalah bentuk perlindungan yang banyak digunakan, tetapi terbukti sulit untuk meningkatkan ketahanan tanda air digital dan menemukan cara untuk mencegah serangan berbasis penyalinan. Makalah ini mengusulkan metode otentikasi citra baru yang menggabungkan tanda tangan digital dan watermarking digital dalam bentuk kode QR. Beranjak dari teknik yang ada, metode yang diusulkan menggunakan segmentasi gambar untuk mengeksploitasi kemampuan koreksi kesalahan kode QR dengan mengubah tanda tangan digital dari setiap sub-blok menjadi kode QR sebelum menyematkannya ke dalam gambar. Tanda tangan digital kemudian disimpan sebagai tanda air, yang mengimbangi kelemahan penyimpanan tanda tangan dan sulit untuk disalin. Eksperimen menunjukkan bahwa metode ini efektif dalam hal derau gambar dan tanda air kuat dan aman terhadap serangan berbasis salinan.**

Kata kunci—Tanda air digital; Tanda tangan digital; Kode QR; Transformasi Kosinus Diskrit (DCT); Otentikasi gambar; perlindungan hak cipta; serangan salinan

I. PENDAHULUAN

Dengan pesatnya perkembangan teknologi multimedia, keamanan gambar digital semakin menarik perhatian karena dapat diperoleh, disimpan, dan dimodifikasi dengan mudah. Pada saat yang sama, keamanan layanan cloud juga memprihatinkan [1-2]. Watermarking digital adalah teknik yang banyak digunakan dan efektif untuk melindungi konten gambar digital.
Menawarkan perlindungan hak cipta, gangguan otentikasi dan pelacakan distribusi. Namun, copy attack [3] adalah masalah umum yang dihadapi watermarking digital. Ini bekerja dengan menyalin tanda air dari satu gambar legal ke gambar ilegal lainnya untuk melegalkan gambar ilegal. Tanda tangan digital [4] adalah salah satu cara untuk mengatasi serangan semacam ini dengan menggabungkan tanda air digital [5-10]. Tanda tangan gambar dapat secara unik mendeskripsikan konten gambar asli. Namun, pendekatan ini tidak tahan terhadap banyak transformasi, yang dapat menghancurkan tanda air hingga tidak dapat diekstraksi. Oleh karena itu, bagaimana meningkatkan ketangguhan watermarking merupakan masalah mendesak lainnya yang perlu dipecahkan.

Cara potensial untuk mengatasi masalah di atas adalah dengan menggunakan kode Quick Response (QR). Ini dikenal karena kemampuannya untuk mengatasi kesalahan [11] dan ketahanannya terhadap kerusakan lokal. Dengan memasukkan kode QR ke dalam tanda air digital, ketahanannya dapat ditingkatkan secara signifikan. Algoritma watermarking berbasis kode QR dimulai dengan mengubah watermark menjadi kode QR (lihat Gambar 1) sebelum disematkan ke dalam gambar sampul. Eksperimen sebelumnya telah menunjukkan bahwa pendekatan ini kuat terhadap rotasi umum, penskalaan, dan serangan kompresi JPEG [12-15].

*Penulis yang sesuai

Meski efektif, konten watermark tidak terkait dengan gambar sampul itu sendiri, artinya masih rentan terhadap serangan penyalinan.

Oleh karena itu, dalam makalah ini, kami fokus pada pembuatan sarana untuk mengkorelasikan tanda air berbasis kode QR dan konten gambar sampul. Pertama-tama, gambar dibagi menjadi sub blok untuk mengaktifkan lokasi tampering area. Kemudian, konten utama dari setiap sub-blok dikodekan menjadi kode QR yang dapat diproses sebagai watermark. Ini menyediakan sarana pendeteksian serangan penyalinan karena tanda air terkait dengan konten gambar. Ini juga meningkatkan kekokohan tanda air dengan memanfaatkan karakteristik kode QR yang lebih kuat secara umum.

Gambar 1. Kode QR “Hello World”

Metode otentikasi gambar yang diusulkan memiliki keuntungan sebagai berikut: (1) dapat secara efektif menahan serangan penyalinan; (2) secara signifikan meningkatkan ketahanan watermark; (3) itu memungkinkan keberhasilan lokasi area yang dirusak. Kontribusi utama dari makalah ini meliputi: (1) deskripsi cara penerapan tanda tangan konten gambar digital sebagai tanda air untuk melindungi gambar dari serangan salinan; (2) detail cara menyandikan tanda tangan gambar dengan menggunakan kode QR, untuk meningkatkan kekokohan tanda air; (3) pembentukan metode segmentasi citra yang dapat mengidentifikasi lokasi area yang dirusak.

II. PEKERJAAN TERKAIT

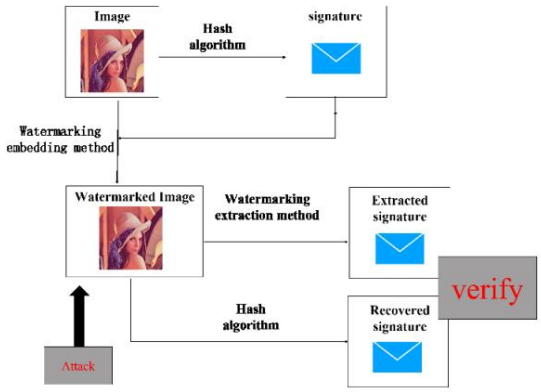
A. Algoritma tanda tangan digital untuk serangan anti-salinan

Teknologi tanda tangan digital tradisional menggunakan algoritme hash untuk menghitung intisari gambar, kemudian menggunakan enkripsi kunci privat untuk menghasilkan tanda tangan. Tanda tangan dilampirkan pada gambar dan ditransmisikan dengan gambar sebagai hal yang biasa. Saat gambar diterima, penerima menggunakan kunci publik untuk mendekripsi tanda tangan dan mendapatkan intisari, yang secara bersamaan menggunakan algoritme hash untuk menghasilkan intisari baru untuk perbandingan. Algoritma tanda tangan digital tradisional terutama didasarkan pada algoritma kriptografi. Oleh karena itu mereka sangat sensitif terhadap konten gambar dan proses transmisi. Jadi, kompresi, gangguan derau, dll. Dapat membuat autentikasi akhir gagal. Oleh karena itu, metode tanda tangan yang lebih kuat telah dikembangkan yang didasarkan pada

978-1-6654-0392-4/20/$31,00 ©2020 IEEE
DOI 10.1109/TrustCom50675.2020.00217

karakteristik gambar [15]. Serangkaian metode transformasi digunakan untuk mengekstrak fitur utama dari citra sebagai intisari, sehingga meningkatkan kekokohan tanda tangan [17-19].

Untuk menghadapi serangan penyalinan, algoritma telah diusulkan yang menggabungkan kekokohan tanda tangan digital dengan tanda air digital. Tanda tangan disematkan pada gambar sebagai tanda air. Ketika serangan salinan terjadi, konten tanda air diekstraksi dan kesamaan antara tanda tangan yang dihitung ulang dan tanda tangan yang diekstraksi dihitung. Jika kesamaan lebih rendah dari ambang batas yang telah ditetapkan, tanda air ditentukan bukan milik gambar. Gambar 2 menunjukkan kerangka umum algoritma watermarking digital berdasarkan tanda tangan digital untuk perlindungan terhadap serangan salinan.



Gambar 2. Framework dari algoritma copy attack protection

B. Pendekatan watermarking kode QR

Kode QR memiliki keuntungan karena mampu menyimpan informasi dalam jumlah besar, sangat andal, sangat aman dan mampu menolak pemalsuan, semuanya dalam kode satu dimensi [20]. Bergantung pada bagaimana kode QR dikodekan, ini dapat memberikan empat tingkat koreksi kesalahan, yang mencakup hingga 30% dari kata kode data yang ada.

Kode QR semakin banyak diterapkan pada gambar digital. Dalam sebagian besar penelitian saat ini, teks bertanda air, tautan situs web terkait, informasi pribadi, ikon, dll., Diubah menjadi kode QR dan disematkan dalam gambar, baik terlihat maupun tidak terlihat. Ini menciptakan hubungan sederhana antara gambar dan informasi terkait. [21], skema perlindungan privasi gambar diusulkan berdasarkan kode QR, yang dapat menyandikan informasi privasi mengenai gambar ke dalam kode QR yang kemudian disematkan ke dalam gambar. Metode ini memastikan bahwa kode QR tidak memengaruhi efek visual gambar, sekaligus menjaga agar kode QR dapat dikenali. Di [12], URL terkait gambar diubah menjadi kode QR dan disematkan di sudut gambar untuk mengaitkan gambar dengan informasi terkait, seperti tautan belanja online. Pada [22], ikon diubah menjadi kode QR sebagai tanda air yang dapat disematkan pada gambar. Eksperimen dengan ini menunjukkan bahwa kode QR dapat berfungsi dengan baik sebagai tanda air.

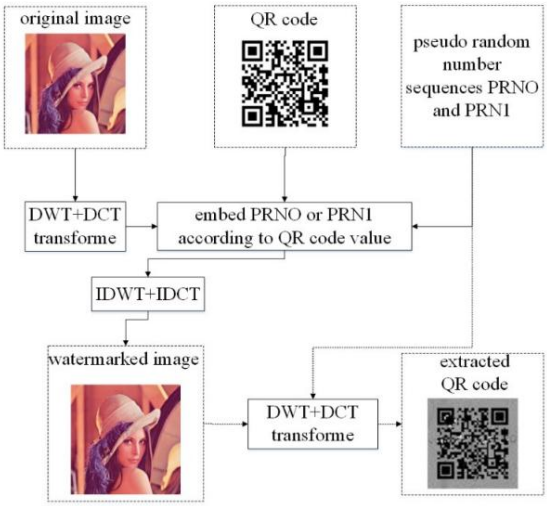
Namun, metode yang menyematkan informasi yang hanya memiliki hubungan yang lemah dengan konten gambar tidak efektif untuk melawan serangan penyalinan. Dalam beberapa tahun terakhir, beberapa penelitian telah mengeksplorasi cara mengonversi fitur konten gambar menjadi kode QR. Di [25], misalnya, fitur warna dalam dokumen elektronik berwarna disimpan sebagai kode QR. Perbatasan gambar, di sini, biasanya kosong sehingga kode QR dapat disematkan di sekelilingnya gambar. Posisi tersematnya kemudian disimpan dalam kode QR baru yang disematkan secara visual di salah satu sudut gambar. Metode ini tidak hanya mengaktifkan autentikasi gambar, tetapi juga lokasi dari setiap efek perusakan. Namun, penggunaannya sebagian besar terbatas pada dokumen warna digital. Pendekatan ini telah mengilhami makalah saat ini dan berfungsi sebagai dasar model sederhana dan lebih umum yang kami usulkan di sini.

Penyisipan watermark biasanya melibatkan penggunaan transformasi kosinus diskrit (DCT) dan transformasi wavelet diskrit (DWT) [23-24]. Pada Gambar 3, kami meringkas alur kerja algoritme untuk menyematkan dan mengekstraksi tanda air digital berdasarkan kode QR.

Pada [24], kode QR yang terdiri dari bit '0' dan '1' dimasukkan ke dalam koefisien DCT dengan menggunakan Persamaan. 1 (lihat di bawah), di mana, adalah koefisien DCT asli dalam blok DCT, ŷn adalah koefisien yang dimodifikasi; adalah faktor keuntungan; dan PRN0 dan PRN1 adalah urutan angka acak: 0, ÿ 1, ÿ

$$\hat{y} = \{ + \ddot{y} \quad + \ddot{y} \quad \begin{matrix} \ddot{y}0\ddot{y} \\ \ddot{y}1\ddot{y} \end{matrix} \qquad (1)$$

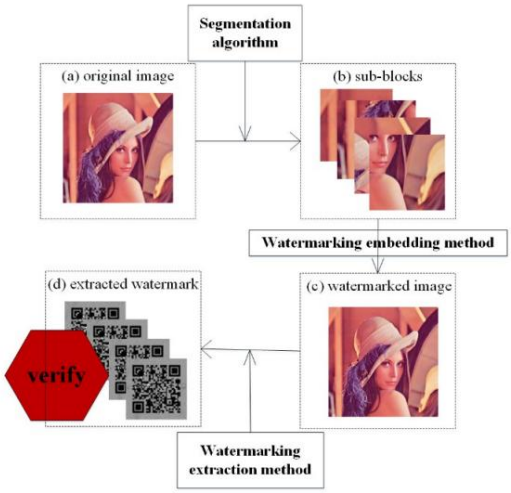
Saat ini, banyak teknologi baru yang mulai diterapkan untuk keamanan data multimedia. Misalnya, metode deep learning seperti CNN[26] dan GAN [27] digunakan untuk menentukan apakah gambar telah dirusak, dan teknologi blockchain digunakan untuk merekam jejak data dalam jaringan[28]. Kedepannya, pendekatan watermarking QR Code akan digabungkan dengan teknologi baru ini untuk memecahkan masalah baru, seperti mendeteksi deepfake [29].



Gambar 3. Metode penyematan dan ekstraksi kode QR

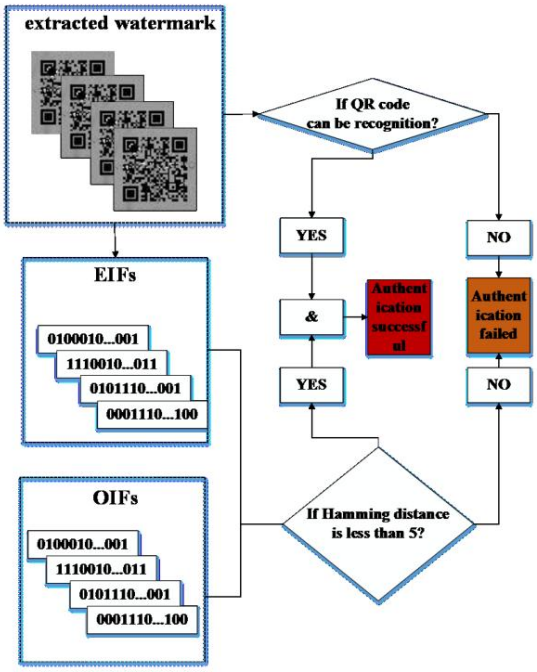
AKU AKU AKU. MODE OTENTIKASI GAMBAR

A. Kerangka



Gbr.4. Kerangka model otentikasi yang diusulkan

Model yang diusulkan menyediakan kerangka umum dan efisien untuk autentikasi gambar (lihat Gambar 4). Model pertama-tama menghitung tanda tangan dari gambar asli, kemudian memproses tanda tangan digital dan informasi teks untuk membentuk kode QR. Ini kemudian dimasukkan ke dalam gambar asli sebagai tanda air. Gambar watermark diperoleh dengan melakukan transformasi DCT+DWT. Untuk menemukan area yang diserang, model pertama-tama membagi citra menjadi sub-blok, kemudian melakukan operasi di atas pada sub-blok yang dipartisi.
Sub-blok kemudian disusun kembali menjadi gambar yang lengkap. Untuk autentikasi, citra yang diberi watermark dapat diekstraksi dan diverifikasi dengan menerapkan metode ekstraksi watermark.



Gambar 5. Proses otentikasi citra

B. Menyematkan Tanda Air

Proses penyisipan watermark terjadi setelah dilakukan segmentasi citra. Gambar asli tersegmentasi dengan membaginya menjadi sub-blok yang sama. Parameter segmentasi, d, ditambahkan untuk mewakili jumlah sub-blok. Proses watermarking untuk setiap sub-blok berisi tiga langkah utama: (1) menghitung tanda tangan digital; (2) menyandikan kode QR; (3) menyematkan tanda air (lihat di bawah).

- (1) *Menghitung tanda tangan digitalÿUntuk* memberikan perlindungan yang efektif terhadap serangan salinan, tanda tangan harus mewakili konten utama gambar.
  Namun, karena sensitivitas konten tanda tangan yang tinggi, setiap perubahan pada gambar dapat membuat autentikasi gagal. Jadi, untuk meningkatkan kekokohan metode, koefisien DCT dihitung terlebih dahulu, kemudian koefisien frekuensi rendah dipilih sebagai fitur citra. Kunci dari metode ini, yang disebut 'phash', adalah menggunakan rata-rata dari koefisien yang dipilih.
  Pada akhirnya, proses ini menghasilkan string “01” 64bit dengan membandingkan nilai koefisien dan rata-rata yang dihitung. String ini mewakili fitur gambar yang dipilih, yang diperlakukan sebagai tanda tangan.

- (2) *Pengkodean kode QR:* Untuk meningkatkan pengenalan tanda air, beberapa informasi teks ditambahkan, seperti pemilik atau stempel waktu. Informasi watermark kemudian menjadi informasi teks dan informasi tanda tangan. Nantinya, metode pengkodean kode QR digunakan untuk mengubah tanda air menjadi kode QR.

- (3) *Menyematkan tanda air:* untuk menyematkan tanda air, metode yang sama diadopsi seperti yang diusulkan dalam [24], yang diperkenalkan dalam karya terkait.

C. Mengekstraksi tanda air

Karena transformasi DCT dan DWT yang dapat dibalik, kode QR dapat dengan mudah diekstraksi dari gambar. Sebagai hasil dari kemampuan koreksi kesalahan kode QR yang kuat, setelah serangkaian transformasi, pengguna masih dapat memperoleh informasi watermark pada gambar dengan memindai. Ini dapat digunakan untuk mengonfirmasi hak cipta. Fitur gambar yang dibaca dari kode QR yang diekstraksi disebut *EIF.* Fitur gambar yang dihitung ulang dari gambar yang diberi watermark disebut *OIF.* Sehingga pada tahap verifikasi, *EIF* dapat dibandingkan dengan *OIF* dengan menggunakan jarak Hamming. Setelah banyak percobaan, kami menetapkan ambang jarak Hamming ke 5. Jika jarak Hamming kurang dari 5 dan kode QR yang diekstraksi telah dikenali, ini menandakan bahwa gambar tersebut belum diserang. Proses verifikasi citra ditunjukkan pada Gambar 5.

IV. EKSPERIMEN DAN ANALISIS

Kami mengevaluasi kinerja metode yang diusulkan dengan memilih gambar berukuran 1024*1024 piksel untuk pengujian. Eksperimen ini bertujuan untuk menunjukkan bahwa metode tersebut: (1) secara konsisten meningkatkan ketangguhan watermarking, terutama ketika mengalami noise, rotasi, dan membuat gambar menjadi lebih gelap atau lebih terang; (2) efektif untuk melindungi hak cipta dari gambar digital, terutama terhadap serangan salinan; dan (3) secara praktis mendukung lokasi area yang dirusak dengan menggunakan sub-blok. Implementasi Perpustakaan Python digunakan untuk mewujudkan pengkodean kode QR.

A. Metode Eksperimen

Parameter segmentasi ditetapkan dalam percobaan menjadi 4, 6, dan 9. Selama pemrosesan gambar, kami memperoleh gambar watermark dari setiap sub-blok, sebelum mengekstraksi gambar watermark dan watermark akhir. Mari kita periksa hasil eksperimen dalam kaitannya dengan segmentasi. Gambar. 6-9 menunjukkan hasil split, dengan pemrosesan yang sesuai. Misalnya, Gambar 6(a) adalah gambar aslinya, Gambar 6(b) menunjukkan QR kode dihitung dari setiap blok dalam 6 (a), yang dibagi menjadi empat blok. 6(c) menunjukkan seluruh gambar 6(a) setelah tanda air disematkan, 6(d) adalah kode QR yang diekstraksi dari 6(c), di mana setiap kode QR dikenali. Penjelasan serupa berlaku untuk Gambar 7, dimana terdapat 6 sub blok dan Gambar 8, dimana terdapat 9 sub blok. Semua gambar disimpan dalam format 'jpeg' dan, seperti dapat dilihat, dalam setiap kasus, tanda air berhasil diekstraksi dan dikenali.

Gambar 6 Hasil Segmentasi dan Pengolahan Dimana d = 4

Gambar 7. Segmentasi dan hasil pengolahan dimana d = 6

Gambar 8. Segmentasi dan hasil pengolahan dimana d = 9

B. Pemrosesan Sinyal Konvensional

Untuk memverifikasi lebih lanjut kekokohan watermarking, kami menambahkan derau garam, menggelapkan dan mencerahkan gambar yang diberi tanda air. Di sini, kami menetapkan parameter segmentasi pada 4. Gambar. 9-11 menunjukkan hasil dari percobaan ini. Mengambil Gambar. 9 sebagai contoh, Gambar. 9 (a) adalah Gambar. 6 (a) di atas, dengan gangguan kebisingan. Gambar 9(b) adalah watermark hasil ekstraksi. Untuk membuat perbandingan lebih jelas, kami juga mencantumkan jarak Hamming *OIF* dan *EIF* pada Tabel 1. Dari hasil ini kita dapat melihat bahwa noise dan transformasi dapat dipindai dari tanda air yang diekstrak jika jarak Hamming kurang dari 5. Hal ini menegaskan bahwa metode pengkodean kode QR yang diusulkan dapat secara signifikan meningkatkan ketahanan watermark.

Gambar 9. Hasil untuk penambahan noise garam (dimana n=3000)

Gambar 10. Hasil peningkatan kecerahan (+10%)

Gambar 11. Hasil untuk peningkatan kegelapan (-10%)

TABEL I. HAMMING JARAK DAN HASIL PENGENALAN UNTUK GANGGUAN

Gangguan	Eksperimen				
	Hasil (berdasarkan sub-blok)	***1***	2	3	***4***
Kebisingan garam (n=3000)	Jarak hamming	2	2	0	0
	Hasil pengakuan	ÿ	ÿ	ÿ	ÿ
Lebih terang 10%	Jarak hamming	2	0	0	0
	Hasil pengakuan	ÿ	×	×	ÿ
Lebih terang 5%	Jarak hamming	2	2	0	0
	Hasil pengakuan	ÿ	ÿ	ÿ	ÿ
Lebih gelap sebesar 10%	Jarak hamming	2	2	0	0
	Hasil pengakuan	ÿ	ÿ	ÿ	ÿ

C. Hasil Deteksi Pengrusakan Tujuan

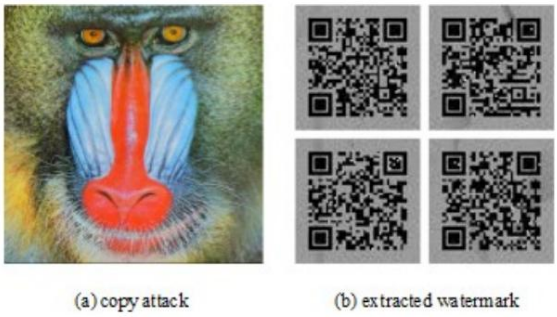
dari percobaan ini adalah untuk memverifikasi bahwa algoritma yang diusulkan dapat: (1) menemukan area yang dirusak; dan (2) secara efektif menahan serangan penyalinan.

Gambar. 12 dan 13 menunjukkan hasil sampul grafis. Format tampilannya sama seperti pada eksperimen B, dan sebuah tabel juga disediakan untuk referensi. Ketika serangan terjadi, tanda air yang disematkan di area yang sesuai tidak dapat dikenali dengan baik, atau jarak Hamming melebihi 5. Semakin kecil sub-blok, semakin akurat hasil pemosisian tamper.

Untuk menguji ketahanan pendekatan untuk menyalin serangan, tanda air untuk Gambar 6(a) disalin ke gambar baru. Hasil serangan ditunjukkan pada Gambar. 14 dan Tabel 2. Meskipun tanda air dapat dikenali, jarak Hamming jauh lebih besar dari 5.

Gambar 12. Hasil serangan penutup

Gambar 13. Hasil serangan randline



Gambar 14. Hasil copy attack

TABEL II. HAMMING JARAK DAN HASIL PENGENALAN UNTUK SERANGAN

Menyerang	Eksperimen				
	Hasil (berdasarkan sub-blok)	***1***	***2***	***3***	***4***
Serangan Randline	Jarak hamming	2	0	0	0
	Hasil pengakuan	×	ÿ ÿ ÿ		
Serangan penutup	Jarak hamming	6	0	0	0
	Hasil pengakuan	×	ÿ ÿ ÿ		
Salin serangan	Jarak hamming	28	34	36	30
	Hasil pengakuan	ÿ ÿ ÿ ÿ			

V. KESIMPULAN

Dalam makalah ini, kami telah mengusulkan pendekatan baru untuk melindungi gambar digital yang didasarkan pada kode QR yang menggabungkan tanda tangan digital dan tanda air. Tujuan utamanya adalah untuk meningkatkan ketahanan serangan gambar dan ketangguhan watermarkingnya dengan menggunakan karakteristik menguntungkan dari kode QR. Eksperimen telah membuktikan

efektivitas pendekatan terhadap serangan penyalinan dan untuk lokasi area yang dirusak. Karena ini adalah model yang relatif sederhana, pendekatan lain yang ada untuk watermarking digital juga dapat diintegrasikan ke dalam kerangka kerja yang sama untuk memperkuat kinerjanya.

PENGAKUAN

Pekerjaan ini secara khusus didukung oleh Dana Riset untuk Konstruksi NSD, Universitas Hubungan Internasional (2019GA36), dan sebagian oleh Dana Riset Fundamental untuk Universitas Pusat, Universitas Hubungan Internasional (3262020T26).

REFERENSI

[1] Y. Xu, GJ Wang, dan JD Yang, *et* al., “Menuju Layanan Komputasi Jaringan Aman untuk Klien Ringan menggunakan Blockchain,” *Komunikasi Nirkabel dan Komputasi Seluler,* pp.1-12, 2018.

[2] Y. Xu, Q. Zeng, dan G. Wang, *et* al., “Mekanisme Kontrol Akses Berbasis Atribut yang Ditingkatkan Privasi yang Efisien,” *Praktik dan Pengalaman Konkurensi dan Komputasi,* vol. 32, tidak. 5, hlm. 1-10, 2020.

[3] P. Bas, and G. Doërr, “Evaluation of An Optimal Watermark Tampering Attack Against Dirty Paper Trellis Schemes,” in *Proceedings of the 10th ACM Workshop on Multimedia and Security,* 2008.

[4] X. Tang, YN Qi, dan YF Huang, “Bukti Pengambilan Kembali Berbasis Watermarking yang Rapuh untuk Data Cloud Arsip,” dalam *Prosiding Lokakarya Internasional ke-15 tentang Digital-forensik dan Watermarking,* hlm. 296-311, 2016.

[5] E. Maiorana, P. Campisi, dan A. Neri, “Signature-based Authentication System using Watermarking in The Ridgelet and Radon-DCT Domain,” dalam *Proceedings of the International Society for Optical Engineering,* 2007.

[6] T. Omar, MN Kabir, dan YM Alginahi, “A Hybrid Digital Signature and Zero-Watermarking Approach for Authentication and Protection of Sensitive Electronic Documents,” *The Scientific World Journal,* hlm. 1-14, 2014.

[7] HB Hu, Y. Huang, dan J. Liu, *et* al., “Skema Watermarking Berbasis ICA Tahan terhadap Serangan Salinan,” *Journal of Electronics and Information Technology,* vol. 07, hlm. 29-32, 2005.

[8] S. Katzenbeisser, dan H. Veith, “Securing Symmetric Watermarking Schemes Against Protocol Attacks,” dalam *Proceedings of the International Society for Optical Engineering,* hlm. 260-268, 2002.

[9] QY Zhang, LI Kai, dan ZT Yuan, “Algoritma Watermarking Gambar Digital yang Kuat berdasarkan Chaos dan SVD-DWT,” *Riset Aplikasi Komputer,* vol. 27, hlm. 718-720, 2010.

[10] X. Tang, YF Huang, dan CC Chang, *dkk .,* “Audit Integritas Real-Time yang Efisien dengan Arbitrase yang Menjaga Privasi untuk Gambar dalam Sistem Penyimpanan Cloud,” *IEEE Access,* vol. 7, hlm. 33009-33023, 2019.

[11] L. Li, J. Qiu, dan J. Lu, *dkk .,* “Solusi Kode QR Estetis berdasarkan Mekanisme Koreksi Kesalahan,” *Jurnal Sistem dan Perangkat Lunak,* hlm. 85-94, 2015.

[12] HC Huang, FC Chang, dan WC Fang, “Penyembunyikan Data yang Dapat Dibalik dengan Ekspansi Perbedaan Berbasis Histogram untuk Aplikasi Kode QR,” *Transaksi IEEE pada Elektronik Konsumen,* vol. 57, hlm.779-787, 2011.

[13] TT Bai, Z. Liu, dan LU Peng, "Watermarking Digital Tahan Serangan Geometris berdasarkan Kode QR," *Teknik pengemasan,* vol. 34, hlm. 121-124, 2013.

[14] Q. Guo, GX Chen, dan QF Chen, "Algoritma Watermarking Kode QR Ganda berdasarkan DCT-SVD," *Teknik Pengemasan,* vol. 36, hlm.129-135, 2015.

[15] Q. Xue, W. Dan, dan D. Chen, *et* al., “Teknologi Watermarking Digital Tahan Serangan Geometris berdasarkan DWT-SVD dan Kode QR,” *Teknik Pengemasan,* vol. 11, hlm. 158-163, 2016.

[16] Y. Lin, JH Lu, dan J. Yao, “Struktur untuk Kode Batang Dua Dimensi dalam Laporan Uji Platform Anti-Palsu berdasarkan Tanda Tangan Digital RSA,” *Riset Pengawasan Kualitas dan Teknis,* hlm. 57-59, 2015 .

[17] C. Lin, dan S. Chang, "Tanda Tangan Digital Kuat untuk Otentikasi Multimedia: Ringkasan," *Majalah Sirkuit dan Sistem IEEE,* vol. 3, hlm. 23-26, 2003.

[18] M. Chen, “The Attack Methods of Digital Watermarking,” *Journal of Electronics and Information Technology,* pp.83-89, 2001.

[19] C. Liu, Z. Wang, dan Y. Dai, "Metode Penyerangan Saat Ini untuk Penandaan Air Gambar Digital dan Penanggulangan Dasar," *Kontrol dan Keputusan,* vol. 19, hlm. 601-606, 2004.

[20] S. Goyal, S. Yadav, and M. Mathuria, “Exploring Concept of QR Code and Its Benefits in Digital Education System,” in Proceedings of the International Conference on *Advances in Computing, Communications and Informatics,* hlm. 1141- 1147, 2016.

[21] YZ Yao, F. Wang, dan WB Yan, *et* al., “Skema Pelestarian Privasi Gambar berdasarkan Kode QR dan Tanda Air Terlihat yang Dapat Dibalik,” *Jurnal Komunikasi,* vol. 44, hlm. 65-75, 2019.

[22] XH Liu, dan RC Gong, “Algoritma Penandaan Air Digital Kode QR Berdasarkan Domain DCT,” *Teknologi Informasi Modern.* vol. 12, hlm. 21-26, 2018.

[23] W. Zhang, dan X. Meng, “Teknologi Watermarking Digital yang Disempurnakan berdasarkan Kode QR,” dalam *Prosiding Konferensi Internasional tentang Ilmu Komputer dan Teknologi Jaringan,* hlm. 1004-1007, 2015.

[24] YW Chow, W. Susilo, dan J. Tonien, *et* al., “Pendekatan Penandaan Air Kode QR berdasarkan Teknik DWT-DCT,” *Keamanan Informasi dan Privasi,* hlm. 314-331, 2017.

[25] ZM Arkah, L. Alzubaidi, dan AA Ali, *dkk .,* “Otentikasi Dokumen Warna Digital menggunakan Kode QR berdasarkan Penandaan Air Digital,” *Teori dan Aplikasi Tingkat Lanjut Termal Menekankan,* hlm. 1093-1101, 2020.

[26] J. Zhang, Y. Li, dan S. Niu, *et* al., "Jaringan Konvolusional Sepenuhnya yang Ditingkatkan untuk Deteksi Pemalsuan Wilayah Gambar Digital," *Material & Kontinu Komputer,* vol. 58, hlm. 287-303, 2019.

[27] XD Yan, BJ Cui, dan Y. Xu, *et* al., “Metode Perlindungan Informasi untuk Pembelajaran Mendalam Kolaboratif di bawah Serangan Model GAN,” *Transaksi IEEE/ACM pada Komputasi Biologi dan Bioinformatika,* 2019.

[28] Y. Xu, C. Zhang, dan QR Zeng, *dkk .,* “Mekanisme Akuntabilitas yang Diaktifkan Blockchain Terhadap Kebocoran Informasi dalam Layanan Industri Vertikal,” *Transaksi IEEE tentang Ilmu dan Teknik Jaringan,* DOI: 10.1109/TNSE.2020.2976697.

[29] X.Yang, YZ Li, dan S.Lyu. “Mengekspos Deep Fakes using Inconsistent Head Poses,” dalam *Proceedings of the 2019 IEEE International Conference on Acoustics, Speech and Signal Processing,* hlm. 8261-8265, 2019.