

Robust DCT-Domain Watermarking against Screen-Shooting using Improved SIFT and Adaptive Embedding with CRC+BCH Error Protection

1st Ilham Adyansyah
School of Electrical Engineering
Telkom University
Bandung, Indonesia

ilhamadyansyah@student.telkomuniversity.ac.id

2nd Rangga Aditia Permana
School of Electrical Engineering
Telkom University
Bandung, Indonesia

arangga@student.telkomuniversity.ac.id

3rd Ledy Novamizanti
School of Electrical Engineering
The Center of Excellence of AILO
Telkom University
Bandung, Indonesia

ledyaldn@telkomuniversity.ac.id

4th Gelar Budiman
School of Electrical Engineering
The Center of Excellence AICOMS
Telkom University
Bandung, Indonesia

gelarbudiman@telkomuniversity.ac.id

Abstrak—Penelitian ini mengusulkan sistem watermarking citra digital yang tangguh terhadap serangan screen-shooting dengan menggabungkan lokalisasi titik kunci berbasis Improved Scale-Invariant Feature Transform (I-SIFT), penyematan Discrete Cosine Transform (DCT) adaptif pada domain frekuensi menengah, serta pengkodean ganda CRC-8 dan BCH (63,36) untuk integritas dan koreksi kesalahan. Penyematan dilakukan pada blok 64×64 yang dipusatkan pada titik kunci I-SIFT dengan skor respons tertinggi, dengan fallback ke wilayah pusat jika jumlah titik kunci terbatas. Hasil uji pada citra standar (Zelda, Baboon, Peppers, Airplane) menunjukkan imperceptibility tinggi (PSNR rata-rata 42,39 dB) dan ketahanan penuh terhadap distorsi screen-shooting dari jarak 45–105 cm, termasuk distorsi perspektif dan noise sensor, dengan BER = 0,00 pada beberapa kondisi. Pendekatan ini mengungguli metode benchmark Fang et al. dalam hal kualitas visual dan keberhasilan pemulihan watermark, membuktikan efektivitas kombinasi I-SIFT, embedding adaptif, dan proteksi error ganda dalam menghadapi distorsi fisik dunia nyata.

Index Terms—Robust watermarking, screen-shooting attack, SIFT, discrete cosine transform.

I. PENDAHULUAN

Di era penyebaran konten digital yang meluas, penandaan air (watermarking) citra digital memainkan peran penting dalam menegaskan kepemilikan konten, mengautentikasi integritas visual, dan melacak distribusi yang tidak sah [10]. Tujuan utamanya adalah untuk menanamkan data tambahan secara diam-diam ke dalam citra tanpa menurunkan kualitas visualnya secara signifikan. Skema penandaan air yang tangguh harus menyeimbangkan tiga atribut yang saling bersaing: ketidaksadaran, ketahanan, dan kapasitas muatan [11]. Di antara ketiganya, ketahanan menjadi sangat menantang dalam kondisi nyata yang merugikan seperti pengambilan gambar layar.

Serangan pengambilan gambar layar, diilustrasikan pada Gambar 5, terjadi ketika citra digital ditampilkan di layar dan kemudian ditangkap ulang menggunakan kamera digital. Serangan ini menimbulkan serangkaian degradasi: distorsi perspektif, pola moiré akibat interferensi antara piksel tampilan dan susunan sensor [1], distorsi fotometrik seperti pencahayaan yang tidak merata, dan defokus optik. Distorsi nonlinier ini secara signifikan merusak integritas tanda air yang tertanam, terutama yang menggunakan pendekatan spasial atau transformasi domain tradisional. Contoh skenario ini ditunjukkan pada Gambar 1, di mana gambar bertanda air ditangkap ulang menggunakan kamera eksternal dalam kondisi praktis.



Gambar 1. Ilustrasi skenario serangan penyadapan layar. Konten yang ditampilkan (misalnya, berita rahasia) ditangkap menggunakan kamera eksternal, melewati lapisan perlindungan digital.

Metode penandaan air berbasis transformasi konvensional, seperti Transformasi Kosinus Diskrit (DCT) atau Transformasi Wavelet Diskrit (DWT), dirancang untuk ketahanan terhadap kompresi dan derau, tetapi seringkali gagal ketika terdapat

distorsi geometrik. Sebagai respons, para peneliti telah memperkenalkan teknik penyematan berbasis fitur seperti Transformasi Fitur Invarian Skala atau ORB untuk melokalisasi wilayah penyematan yang robust.

Fang et al. mengusulkan sistem penandaan air yang tahan terhadap pengambilan gambar layar (screen shooting) yang menggunakan pengodean BCH (63,39) dan menyematkan bit tanda air ke dalam koefisien DCT frekuensi menengah pada titik kunci SIFT. Namun, metode mereka bergantung pada kekuatan penyematan yang tetap, yang mungkin tidak beradaptasi dengan baik terhadap konten gambar lokal, dan tidak memiliki mekanisme validasi selama ekstraksi.

Untuk mengatasi keterbatasan metode sebelumnya, jurnal ini memperkenalkan beberapa inovasi utama. Pertama, kami meningkatkan lokalisasi fitur menggunakan transformasi fitur invarian skala berbasis intensitas (I-SIFT) yang secara akurat mengidentifikasi wilayah penyisipan tanpa memerlukan pengetahuan sebelumnya tentang citra asli. Kedua, kami menerapkan strategi penyisipan ringkas yang menyisipkan tanda air secara redundan ke dalam beberapa wilayah. Redundansi ini memastikan bahwa setidaknya satu wilayah kaya informasi dapat bertahan di bawah distorsi yang disebabkan oleh lengkungan perspektif dan artefak moiré. Ketiga, kami merancang kerangka kerja ekstraksi buta yang tangguh yang memanfaatkan validasi silang berbasis BER pada beberapa kandidat, yang secara signifikan meningkatkan keandalan dekode. Terakhir, kami memperkenalkan pendekatan penyempurnaan fitur untuk meningkatkan ketahanan dan pengurangan titik kunci, yang pada akhirnya meningkatkan tingkat keberhasilan penyisipan dan akurasi ekstraksi.

Sisa jurnal ini disusun sebagai berikut. Bagian II menugulaskan pekerjaan terkait dan karakteristik distorsi yang disebabkan oleh serangan screen-shooting. Bagian III menjelaskan konstruksi tanda air, penyisipan, dan proses ekstraksi yang diusulkan. Bagian IV menyajikan pengaturan eksperimental dan mengevaluasi sistem di bawah berbagai serangan fisik dan simulasi. Bagian V membahas hasil, ketahanan, dan keterbatasan metode yang diusulkan. Akhirnya, Bagian VI menyimpulkan jurnal dan menguraikan arah kerja masa depan.

II. KAJIAN TEORI

Serangan screen-shooting menimbulkan distorsi kompleks seperti lengkungan perspektif, artefak moiré, dan derau sensor yang secara signifikan menurunkan keandalan tanda air yang disematkan. Berbagai metode telah diusulkan untuk mengatasi tantangan ini, terutama dalam domain transformasi dan berbasis fitur.

Fang et al. [1] memperkenalkan metode penandaan air berbasis SIFT menggunakan BCH (63,39) untuk pengodean muatan dan penyematan DCT pada titik kunci SIFT. Metode mereka menunjukkan ketahanan terhadap distorsi screen-shooting dengan memanfaatkan lokalisasi spasial dan redundansi di berbagai wilayah. Namun, kekuatan penyematan tetap di semua blok dan tidak memiliki validasi intra-kandidat, sehingga membatasi ketahanan terhadap distorsi berat.

Nakamura et al. [2] mempelajari penandaan air yang robust dengan memperkenalkan modul kalibrasi geometrik sebelum deteksi tanda air. Pendekatan mereka mencakup pencocokan templat untuk menyelaraskan sudut gambar di bawah distorsi yang ditangkap kamera, sehingga meningkatkan tingkat deteksi tanda air pada gambar yang ditangkap ulang. Namun, metode ini membutuhkan penanda fiducial dan titik referensi eksternal, yang seringkali tidak praktis dalam aplikasi dunia nyata.

Wang et al. [3] mengatasi ketahanan tangkapan layar dengan mengadopsi strategi pemilihan fitur adaptif berdasarkan titik kunci SURF. Tanda air disematkan ke dalam wilayah dengan karakteristik tekstur yang stabil, meningkatkan ketahanan terhadap perubahan geometrik dan pencahayaan. Meskipun terdapat peningkatan, metode ini tidak mendukung deteksi buta, sehingga membatasi skalabilitasnya untuk aplikasi yang aman.

Chen et al. [4] mengusulkan kerangka kerja penandaan air yang menggabungkan penyematan DCT quaternion dengan fitur momen invarian rotasi. Penggunaan representasi quaternion memungkinkan stabilitas yang lebih tinggi di bawah variasi orientasi selama pengambilan ulang layar. Namun, kompleksitas sistem meningkat secara signifikan karena dekomposisi tensor dan pasca-pemrosesan titik kunci.

Lie et al. [6] memajukan domain penandaan air dengan mengimplementasikan model saraf berbasis atensi yang dilatih pada distorsi tangkapan layar. Metode mereka memanfaatkan fitur-fitur mendalam untuk mengidentifikasi wilayah invarian dan mencapai BER yang lebih baik pada sudut pandang yang bervariasi. Namun demikian, model mereka dibatasi oleh keragaman dataset dan generalisasi ke perangkat yang tak terlihat.

Baru-baru ini, Li dan Liao [5] mengembangkan pendekatan hibrida menggunakan CNN ringan untuk mensimulasikan dan membalikkan artefak moiré yang muncul selama tangkapan layar. Watermark yang tertanam diselaraskan menggunakan pelacakan titik kunci dan dipulihkan menggunakan dekoder neural yang dilatih dengan data tangkapan ulang nyata. Meskipun menjanjikan, sistem ini sangat bergantung pada pelatihan model dan membutuhkan dataset beranotasi yang besar untuk ketahanan.

Dibandingkan dengan metode-metode ini, skema yang kami usulkan menggabungkan CRC-8 dan BCH (63,36) untuk integritas dan koreksi kesalahan, tertanam secara adaptif pada titik kunci I-SIFT, dan menggunakan pemungutan suara wilayah berbasis BER untuk ketahanan yang lebih baik. Tidak seperti pendekatan pembelajaran mendalam, metode kami tetap ringan dan blind, sekaligus mengungguli sistem DCT dan SIFT konvensional dalam distorsi tangkapan layar.

III. METODE

Meskipun terdapat kemajuan signifikan dalam penandaan air tangguh untuk pengambilan gambar layar, sebagian besar metode yang ada masih memiliki keterbatasan yang mengurangi efektivitasnya dalam kondisi dunia nyata. Strategi penyematan dengan kekuatan tetap gagal beradaptasi dengan

variasi tekstur lokal, sehingga menghasilkan trade-off yang kurang optimal antara ketidakepekaan dan ketahanan. Pendekatan domain frekuensi saja seringkali mengalami kesulitan sinkronisasi di bawah distorsi perspektif dan artefak moire' yang ditimbulkan oleh sensor kamera. Demikian pula, sistem berbasis keypoint meskipun lebih tangguh terhadap transformasi geometris cenderung menyematkan muatan tanpa modulasi adaptif atau validasi tingkat bit yang presisi, sehingga rentan terhadap kesalahan dekode di bawah degradasi yang parah. Selain itu, metode berbasis pembelajaran mendalam, meskipun canggih, seringkali membutuhkan kumpulan data beranotasi yang besar dan beroperasi dalam pengaturan non-blind, sehingga membatasi kepraktisannya dalam penerapan di dunia nyata di mana gambar asli mungkin tidak tersedia.

A. Penyisipan Watermark

Algoritma 1 penyisipan watermark

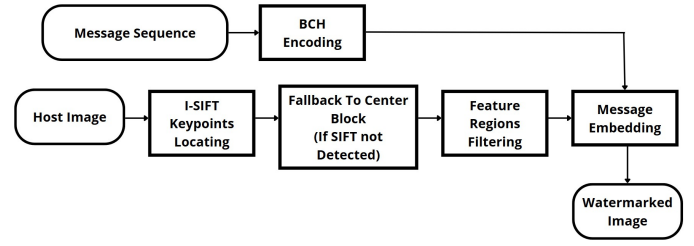
Require: Gambar asli I_{ori} , watermark matrix W , parameter kekuatan r

Ensure: Watermarked image I'

- 1: Convert I_{ori} ke grayscale Y channel
- 2: Deteksi I-SIFT keypoints p_i dengan margin > 32 px
- 3: **if** kurang dari 5 valid keypoints **then** gunakan fallback center block
- 4: **end if**
- 5: pilih top $k = 5$ high-response keypoints
- 6: **for** each 64×64 region $A(p_i)$ **do**
- 7: Divide into 8×8 sub-blocks
- 8: **for** each sub-block **do**
- 9: Terapkan DCT, extract $C_1 = D(4, 5), C_2 = D(5, 4)$
- 10: Hitung $\delta = 0.9 \cdot (|C_1| + |C_2|) + 20r$
- 11: Sisipkan w_{ij} by shifting C_1, C_2 polarity
- 12: Terapkan inverse DCT
- 13: **end for**
- 14: **end for**
- 15: Gabungkan modified blocks ke I_{ori}
- 16: **return** I'

Watermark adalah bilangan bulat 30-bit yang diberikan oleh pengguna, yang dikonversi ke biner dan ditambahkan dengan CRC-7 untuk deteksi kesalahan. Hasil 37-bit kemudian didekodekan dengan BCH (63,36), dan kata sandi 63-bit terakhir dibentuk ulang menjadi 8×8 matriks biner untuk penyisipan. Jika kurang dari 5 titik kunci valid ditemukan menggunakan I-SIFT, algoritma menanamkan watermark ke tengah gambar menggunakan 64×64 block.

Setiap wilayah yang dipilih dibagi menjadi 8×8 blocks, dan bit watermark disematkan dengan memodifikasi koefisien DCT frekuensi menengah (4, 5) and (5, 4). Nilai koefisien disesuaikan secara adaptif berdasarkan $\delta = 0.9 \cdot (|C_1| + |C_2|) + 20r$, dimana r adalah parameter kekuatan embedding. Proses ini memastikan keseimbangan antara imperceptibility dan robustness.



Gambar 2. Proses Penyisipan.

B. Ekstraksi Watermark

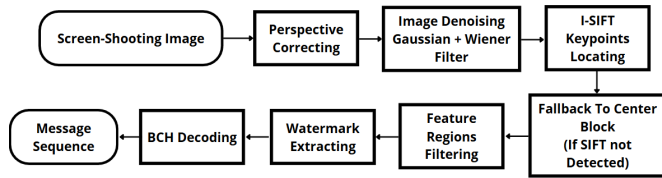
Algoritma 2 Ekstraksi Watermark

Require: Screen-shoot gambar I_0

Ensure: hasil ekstraksi 30-bit pesan watermark $\hat{w}$

- 1: Terapkan homography correction dan moire' filtering
- 2: Ubah ke grayscale dan terapkan I-SIFT
- 3: **if** kurang dari 5 valid keypoints **then** gunakan fallback center block
- 4: **end if**
- 5: Generate 3×3 shifted sub-blocks (up to 90 candidates)
- 6: **for** each 64×64 subregion **do**
- 7: Divide into 8×8 blocks
- 8: **for** each block **do**
- 9: Terapkan DCT, extract $C_1 = D(4, 5), C_2 = D(5, 4)$
- 10: Recover bit $w_{ij} = 1$ if $C_1 \leq C_2$, else 0
- 11: **end for**
- 12: **end for**
- 13: Bandingkan semua extracted codes via BER, pilih yang terbaik
- 14: Terapkan BCH(63,36) decoding
- 15: Gunakan CRC detector untuk validasi pesan
- 16: **return** 30-bit watermark jika CRC valid, else jika gagal

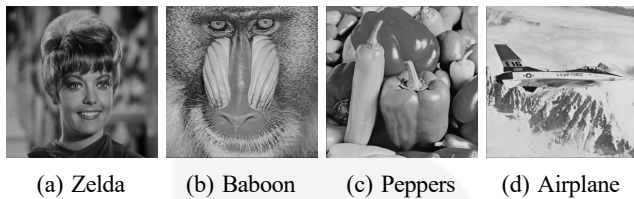
Seperti yang diilustrasikan pada Gambar. 3, Citra yang diterima pertama-tama dikoreksi untuk distorsi perspektif melalui homografi empat titik. Filter Gaussian dan Wiener diterapkan untuk mengurangi derau moire', meningkatkan deteksi titik kunci dan akurasi ekstraksi. Beberapa titik kunci I-SIFT dideteksi, dan di sekitar masing-masing titik kunci, sembilan subwilayah yang bergeser diekstraksi untuk memperhitungkan jitter geometrik lokal. Setiap subwilayah didekodekan menjadi matriks 64-bit dan diratakan menjadi kata sandi 63-bit. Dari semua kandidat, BER berpasangan dihitung, dan pasangan yang paling konsisten dipilih. Kata sandi akhir menjalani dekode BCH (63,36), dan validasi CRC-8 dilakukan pada pesan 30-bit yang telah didekodekan.



Gambar 3. Proses Ekstraksi.

IV. HASIL DAN PEMBAHASAN

Untuk memastikan evaluasi yang komprehensif, empat citra uji skala abu-abu standar Zelda, Baboon, Peppers, dan Airplane digunakan sebagai citra induk untuk penyisipan watermark, seperti yang diilustrasikan pada Gambar 4. Citra-citra ini dipilih karena karakteristik teksturnya yang beragam, mulai dari area halus (misalnya, Zelda) hingga detail frekuensi tinggi (misalnya, Baboon), yang memungkinkan penilaian yang kuat terhadap lokalisasi titik kunci dan fidelitas penyisipan. Nilai tanda air 30-bit sebesar 107374182 disisipkan ke dalam setiap citra dan uji tangkapan layar dilakukan menggunakan kamera ponsel pintar 48 megapiksel untuk mensimulasikan kondisi pengambilan ulang di dunia nyata.

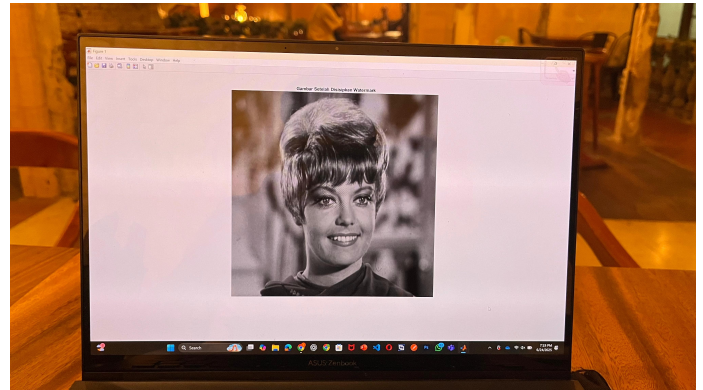


Gambar 4. Contoh gambar host yang digunakan untuk eksperimen penyisipan watermark.

Untuk mensimulasikan kondisi pengambilan gambar layar di dunia nyata, eksperimen pengambilan gambar ulang fisik dilakukan. Seperti yang diilustrasikan pada Gambar 5, pengaturan pengujian melibatkan tampilan gambar ber-watermark pada monitor LCD standar, yang kemudian diambil ulang menggunakan kamera digital yang dipasang pada tripod. Jarak antara layar dan kamera diukur dan diatur dengan cermat untuk memastikan konsistensi. Pencahayaan sekitar dijaga konstan, dan parameter kamera diatur secara manual untuk meminimalkan variasi pencahayaan otomatis. Pengaturan ini dirancang untuk mereplikasi kondisi pengambilan gambar layar praktis dan menghadirkan distorsi realistis seperti pergeseran perspektif, interferensi moire', dan noise sensor.

Pengujian dilakukan pada gambar standar yang diubah ukurannya menjadi 512×512. Watermark integer 39-bit dikodekan dan disematkan menggunakan alur kerja yang diusulkan. Ekstraksi diuji setelah kompresi JPEG, derau Gaussian, dan distorsi perspektif. BER dan PSNR diukur.

Untuk memastikan ketidakepekaan, parameter kekuatan penyisipan disetel sehingga citra ber-watermark yang dihasilkan mencapai Rasio Sinyal terhadap-Derau Puncak (PSNR) sekitar 42 dB dibandingkan dengan citra asli.



Gambar 5. Simulasi serangan screen-shooting. Gambar ber-watermark ditampilkan di layar laptop dan diambil ulang menggunakan kamera digital yang dipasang pada tripod pada jarak tertentu. Pengaturan ini menghasilkan distorsi praktis seperti lengkungan perspektif, interferensi moire', dan variasi iluminasi.

Tabel 1. Contoh Gambar Screenshot Dengan Jarak Pemotretan Yang Berbeda

Jarak	45cm	55cm	75cm	95cm	105cm
Recaptured					

Tabel 1 mengilustrasikan contoh representatif kondisi pengambilan gambar layar pada berbagai jarak, mulai dari 45 cm hingga 105 cm. Semakin jauh jarak pengambilan gambar, gambar yang ditangkap ulang menunjukkan tingkat distorsi geometrik dan degradasi visual yang lebih tinggi, termasuk lengkungan perspektif, interferensi moire', dan keburaman faktor-faktor yang sangat memengaruhi keberhasilan pemulihan watermark.

Tabel 2. Contoh Gambar Screenshot Dengan Sudut Perspektif Horizontal Berbeda

Sudut	Left 65°	Left 30°	0°	Right 30°	Right 65°
Recaptured					

Tabel 2 mengilustrasikan contoh visual citra yang ditangkap ulang dan dipulihkan pada berbagai sudut perspektif horizontal. Seiring bertambahnya sudut pandang (misalnya, ±65°), tanda air yang dipulihkan menunjukkan distorsi yang terlihat akibat lengkungan geometris dan artefak yang disebabkan oleh perspektif.

V. KESIMPULAN

Jurnal ini mempresentasikan metode watermarking citra digital yang menggabungkan DCT-domain embedding adaptif dengan lokalisasi titik kunci I-SIFT dan proteksi kesalahan CRC+BCH, yang dirancang untuk menyeimbangkan imperceptibility dan robustness terhadap serangan screen-shooting fisik. Eksperimen menunjukkan PSNR tinggi (42,39 dB) dan BER = 0,00 pada berbagai jarak dan sudut pengambilan ulang, melampaui performa metode benchmark Fang et al. (PSNR 31,65 dB). Integrasi jalur koreksi perspektif dan filtering moire' berperan penting dalam menjaga akurasi ekstraksi di bawah distorsi geometris dan fotometris. Untuk pengembangan selanjutnya, peningkatan invariansi rotasi dan eksplorasi transformasi yang lebih kuat seperti DWT direkomendasikan guna memperluas ketahanan terhadap variasi pengambilan ulang yang lebih ekstrem.

REFERENSI

- [1] H. Fang, S. Wang, Y. Zhao, and H. Leung, "Screen-shooting resilient watermarking," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1413–1426, Jun. 2018.
- [2] T. Nakamura, K. Kimura, and T. Yamasaki, "Digital watermarking robustness under camera recapture attacks," in *Proc. ACM Multimedia Asia*, 2018.
- [3] Z. Wang, Y. Xu, and L. Chen, "Robust watermarking against screen-cam attacks via feature-based DCT embedding," in *Proc. IEEE Int. Conf. on Multimedia and Expo*, 2019, pp. 1294–1299.
- [4] L. Chen, Y. Zhang, and J. Liu, "Screen content watermarking using region-based DCT embedding," *IEEE Access*, vol. 8, pp. 14256–14265, 2020.
- [5] Y. Li, M. Zhou, and H. Wang, "Deep feature learning for screen-capture resilient watermarking," *IEEE Transactions on Image Processing*, vol. 33, pp. 123–135, 2024.
- [6] X. Li, H. Zhang, and Y. He, "Robust Blind Watermarking Using Quaternion Tensor DCT and Keypoint Learning," *Sensors*, vol. 21, no. 19, pp. 6554, 2021.
- [7] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.
- [8] B. Bai, X. Chen, and Y. He, "ORB-based DWT-SVD blind watermarking for geometric attacks," in *IEEE ICME*, 2023.
- [9] M. Nasir, A. Mansoor, and M. Siddiqui, "A comparative study of robust digital image watermarking techniques," *International Journal of Computer Applications*, vol. 71, no. 5, pp. 1–6, 2013.
- [10] I. J. Cox, M. L. Miller, and J. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2002.
- [11] C.-S. Lu, S.-K. Huang, C.-J. Sze, and H.-Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Transactions on Multimedia*, vol. 2, no. 4, pp. 209–224, Dec. 2000.
- [12] M.-J. Tsai, H.-Y. Huang, and Y.-H. Chen, "Robust watermarking against screen-camcorder attack," in *Proc. Int. Conf. on Information Security and Assurance (ISA)*, 2009, pp. 161–164.
- [13] A. Panah, R. Safabakhsh, and M. Naderi, "Screen camcorder resilient watermarking using virtual watermarking and image registration," in *Proc. IEEE Int. Conf. on Multimedia and Expo (ICME)*, 2012, pp. 801–806.
- [14] H. Deng, L. Zhang, and S. Wang, "SVD-DCT Based Robust Watermarking in Feature Domain for Screen-Cam Resilience," *Multimedia Tools and Applications*, vol. 81, pp. 15345–15366, 2022.
- [15] A. Pramila, R. S. Kiran, and P. H. G. Kumar, "Perspective Resilient Watermarking with SIFT-Harris Localization for Printed-Cam and Screen-Cam Capture," *Signal, Image and Video Processing*, 2024.
- [16] T. Liang, Q. Jin, and Y. Luo, "ScreenMark: End-to-End Watermarking Framework Against Screen-Shot Attacks," *arXiv preprint*, arXiv:2409.03487, 2024.
- [17] A. Yakushev, E. Zakharov, and V. Lempitsky, "DocMarking: Document Screen-Capture Watermarking via Learned Visibility and Robustness," *arXiv preprint*, arXiv:2304.12682, 2023.
- [18] Y. Cao, B. Xie, and Z. Chen, "Lightweight Frequency-Domain Neural Watermarking under Screen-Cam Distortions," *Expert Systems with Applications*, vol. 239, pp. 123159, 2024.
- [19] E. T. Lin and E. J. Delp, "A review of fragile watermarking schemes for image authentication," in *Proc. SPIE Security and Watermarking of Multimedia Contents*, vol. 4675, 2001, pp. 25–36.