JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Pemanfaatan Fingerprint Multi-Hash Ensemble dengan Mekanisme Veto untuk Mitigasi Fraud AI Berbasis Blockchain

Nawirah Athqiyah, Ali Ibrahim*, Fathoni, Mgs Afriyan Firdaus

Fakultas Ilmu Komputer, Sistem Informasi,Universitas Sriwijaya, Palembang, Indonesia
Email: [1]nawirahathqiyah67@gmail.com, [2]aliibrahim@unsri.ac.id, [3]fathoni@unsri.ac.id, [4]afriyanfirdaus@gmail.com
Email Penulis Korespondensi: aliibrahim@unsri.ac.id*
Submitted **27-04-2026**; Accepted **21-05-2026**; Published **31-10-2026**

Abstrak

Proliferasi gambar hasil generasi AI seperti DALL-E, Midjourney, dan Stable Diffusion telah menciptakan ancaman serius terhadap autentikasi visual di berbagai platform digital. Kemampuan AI generatif dalam menghasilkan gambar fotorealistik membutuhkan pendekatan verifikasi yang robust dan efisien untuk memitigasi penyalahgunaan konten visual. Penelitian ini mengusulkan framework Multi-Hash Ensemble yang mengintegrasikan dua pendekatan fingerprinting, yaitu Full Image Hash Ensemble dan Hybrid Fingerprint dengan ROI Extraction, yang diperkuat oleh Veto Mechanism berbasis gradient signature, Local Binary Pattern (LBP), distribusi warna, dan shape descriptor, serta arsitektur blockchain on-chain/off-chain untuk menjamin keimutabelan data. Evaluasi dilakukan pada dataset 200 citra dari kategori face dan nature dengan 22.847 perbandingan melalui tiga skenario pengujian. Metode 1 (Full Image Hash Ensemble) menghasilkan True Acceptance Rate (TAR) 94,15%, True Rejection Rate (TRR) 98,97%, akurasi 98,43%, F1-Score 93,03%, dan Equal Error Rate (EER) 3,44%. Metode 2 (Hybrid Fingerprint) mencapai akurasi 96,71%, FAR terendah 0,68%, dan FAR nol pada mode HYBRID_ENSEMBLE untuk seluruh 3.486 pasangan imposter. Analisis sensitivitas threshold pada Metode 2 menunjukkan titik optimal pada 0,22 dengan F1-Score 85,18% dan akurasi 96,92%. Kedua metode menunjukkan ketahanan sempurna terhadap kompresi JPEG dan resize, namun memiliki kelemahan pada serangan Crop 10%. Dari aspek efisiensi blockchain, arsitektur hibrida on-chain/off-chain berhasil mereduksi data penyimpanan dari citra 2–5 MB menjadi hanya 64 byte per registrasi (rasio kompresi >99,99%), dengan estimasi biaya Gas Fee < $0,01 USD per citra pada jaringan Layer-2 (Polygon dan Arbitrum). Keimutabelan data off-chain dijamin melalui Content Hash SHA-256 yang dikunci pada blockchain, sehingga manipulasi data dapat dideteksi secara otomatis. Temuan ini menunjukkan bahwa framework yang diusulkan memberikan keseimbangan optimal antara akurasi deteksi, efisiensi penyimpanan, dan biaya operasional untuk verifikasi integritas citra digital skala besar.

Kata Kunci: AI-generated image; multi-hash ensemble; perceptual hashing; blockchain; veto mechanism; image integrity verification; IPFS.

Abstract

The proliferation of AI-generated images, such as those produced by DALL-E, Midjourney, and Stable Diffusion, has created a serious threat to visual authentication across various digital platforms. The capability of generative AI to produce photorealistic images necessitates a robust and efficient verification approach to mitigate the misuse of visual content. This study proposes a Multi-Hash Ensemble framework integrating two fingerprinting approaches, namely Full Image Hash Ensemble and Hybrid Fingerprint with ROI Extraction, reinforced by a Veto Mechanism based on gradient signature, Local Binary Pattern (LBP), color distribution, and shape descriptor, along with an on-chain/off-chain blockchain architecture to ensure data immutability. Evaluation was conducted on a dataset of 200 images from face and nature categories with 22,847 comparisons across three testing scenarios. Method 1 (Full Image Hash Ensemble) achieved a True Acceptance Rate (TAR) of 94.15%, True Rejection Rate (TRR) of 98.97%, accuracy of 98.43%, F1-Score of 93.03%, and Equal Error Rate (EER) of 3.44%. Method 2 (Hybrid Fingerprint) attained an accuracy of 96.71%, the lowest FAR of 0.68%, and zero FAR on HYBRID_ENSEMBLE mode for all 3,486 imposter pairs. Threshold sensitivity analysis on Method 2 revealed an optimal point at 0.22 with F1-Score of 85.18% and accuracy of 96.92%. Both methods demonstrated perfect resilience against JPEG compression and resizing, yet exhibited vulnerability to Crop 10% attacks. Regarding blockchain efficiency, the hybrid on-chain/off-chain architecture successfully reduced storage data from 2–5 MB images to merely 64 bytes per registration (compression ratio >99.99%), with estimated Gas Fee costs of < $0.01 USD per image on Layer-2 networks (Polygon and Arbitrum). Off-chain data immutability is guaranteed through SHA-256 Content Hash locked on the blockchain, enabling automatic detection of data manipulation. These findings demonstrate that the proposed framework provides an optimal balance between detection accuracy, storage efficiency, and operational cost for large-scale digital image integrity verification.

Keywords: AI-generated image; multi-hash ensemble; perceptual hashing; blockchain; veto mechanism; image integrity verification; IPFS.

1. PENDAHULUAN

Kepercayaan manusia terhadap representasi visual telah menjadi fondasi komunikasi dan transaksi sejak zaman pra-sejarah. Dari lukisan gua di Lascaux hingga fotografi digital pada platform media sosial, gambar selalu berfungsi sebagai bukti yang dianggap meyakinkan atas realitas yang ditangkapnya [1]. Sistem hukum mengandalkan rekaman foto dan video sebagai alat bukti[2], dan transaksi komersial memanfaatkan identifikasi visual untuk verifikasi produk dan pengguna. Dari setiap konteks tersebut, asumsi dasar yang dapat dikatakan adalah sebuah gambar merupakan representasi yang jujur dari realitas yang diabadikannya.

Asumsi tersebut kini menghadapi krisis epistemologis yang belum pernah terjadi sebelumnya. Generasi model AI yang mampu menghasilkan gambar fotorealistik [3], seperti DALL-E 3, Midjourney v6, dan Stable Diffusion XL, telah mendemokratisasi kemampuan untuk menciptakan visualisasi yang nyaris tidak dapat dibedakan dari foto asli oleh pengamatan manusia biasa [4]. Teknologi ini tidak hanya menghasilkan gambar wajah manusia yang tidak pernah ada,

Copyright © 2026 The **Nawirah Athqiyah**, Page 1246
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

tetapi juga mampu memproduksi gaya fotografi tertentu, meniru kondisi pencahayaan dunia nyata, dan bahkan ke detail tekstur yang mirip dengan pengetahuan fisik dunia nyata [4]. Implikasi dari kemampuan ini sangat luas, mulai dari potensi penyalahgunaan pada platform verifikasi identitas, manipulasi bukti hukum, penipuan komersial dengan produk palsu, hingga disinformasi berskala masif yang dapat mengancam integritas proses demokratis [5].

Blockchain sebagai teknologi ledger terdistribusi menawarkan solusi potensial untuk masalah provenance digital [6]. Sifatnya yang *immutable* dan transparan dapat digunakan untuk pencatatan *fingerprint* atau sidik jari digital dari gambar hasil citra / modifikasi AI, sehingga verifikasi selanjutnya dapat merujuk pada rekaman yang tidak dapat dimanipulasi [7]. Namun, efektivitas pendekatan ini sangat bergantung pada kualitas dan *robustness* dari *fingerprint* gambar yang disimpan. Jika *fingerprint* yang direkam tidak mampu mengidentifikasi gambar secara unik, atau terlalu rentan terhadap perubahan manipulasi yang wajar, maka seluruh sistem verifikasi akan runtuh dari dasar.

Perceptual hashing telah menjadi teknik utama dalam *fingerprinting* gambar karena kemampuannya menghasilkan representasi ringkas yang tetap konsisten meskipun gambar mengalami transformasi tertentu [8]. Berbeda dari cryptographic hashing seperti MD5 atau SHA-256 yang menghasilkan hash berbeda secara total meskipun hanya terjadi perubahan satu bit, perceptual hash dirancang untuk menghasilkan output yang serupa untuk gambar-gambar yang secara visual memiliki kemiripan [8], [9]. Teknik ini sangat berguna untuk deteksi duplikasi gambar, verifikasi integritas konten visual, dan identifikasi gambar yang telah dimanipulasi [9].

Namun demikian, penggunaan perceptual hashing secara tunggal menghadapi trade-off fundamental yang sulit diatasi [10]. Full image hash, yang dihitung dari keseluruhan piksel dalam gambar, menunjukkan *robustness* yang baik terhadap berbagai transformasi seperti kompresi JPEG, perubahan kecerahan, dan rotasi kecil [11]. Pendekatan ini unggul dalam mendeteksi pasangan gambar yang merupakan gambar yang sama yang telah mengalami manipulasi (actual same pair) [13]. Namun, kelemahannya terletak pada diskriminasi, yaitu kemampuan untuk membedakan gambar yang benar-benar berbeda (actual different pair). Dua gambar yang secara visual berbeda secara signifikan dapat memiliki full image hash yang cukup mirip dan menyebabkan false positive, terutama jika memiliki distribusi intensitas piksel yang serupa [13].

Sebaliknya, pendekatan berbasis Region of Interest (ROI) yang mengekstrak dan meng-hash hanya area foreground dari gambar menawarkan diskriminasi yang lebih tinggi dibanding full image hash [10]. Dengan fokus pada bagian gambar yang mengandung informasi yang relevan dan mengabaikan latar belakang yang homogen, ROI hash mampu membedakan gambar yang berbeda dengan lebih akurat [14]. Namun, pendekatan ini lebih rentan terhadap false rejection, yaitu menolak gambar yang sebenarnya adalah sama tetapi telah mengalami transformasi yang mempengaruhi area ROI [15]. Trade-off ini menciptakan dilema dalam desain sistem fingerprinting: memilih *robustness* atau diskriminasi [16].

Beberapa penelitian terkait telah mengupayakan solusi verifikasi integritas citra. Xiong dkk. [9] mengembangkan perceptual hashing berbasis multitask neural network, Hassan [12] mengombinasikan visual attention model dengan DWT dan DCT, serta Zhang dkk. [14] mengusulkan robust hashing menggunakan NSCT untuk autentikasi citra. Di sisi blockchain, Qureshi dan Jimenez [6] mengidentifikasi tantangan skalabilitas perlindungan konten multimedia, sementara Shahzad dkk. [17] mengimplementasikan arsitektur zero-trust untuk berbagi citra medis. Meskipun demikian, terdapat GAP signifikan: studi sebelumnya menggunakan hashing tunggal tanpa ensemble sehingga tidak mengoptimalkan keseimbangan robustness-diskriminasi; tidak ada yang mengintegrasikan mekanisme veto sebagai hard constraint; dan arsitektur blockchain yang ada belum merancang penyimpanan hibrida on-chain/off-chain yang dioptimalkan. Perbedaan mendasar penelitian ini adalah pengintegrasian tiga komponen: (1) Multi-Hash Ensemble yang mengombinasikan full image hash dan ROI hash, (2) Veto Mechanism sebagai verifikasi sekunder, dan (3) arsitektur blockchain hibrida yang mereduksi data on-chain menjadi hanya 64 byte per registrasi.

Penelitian ini mengusulkan pendekatan Multi-Hash Ensemble yang bertujuan mengatasi trade-off tersebut dengan mengintegrasikan kekuatan dari kedua pendekatan. Kerangka kerja ini mengombinasikan beberapa algoritma perceptual hash secara simultan, baik dari full image maupun dari ROI, dengan bobot yang telah dioptimalkan untuk setiap skenario penggunaan. Meskipun pendekatan ensemble meningkatkan akurasi secara keseluruhan, sistem berbasis perceptual hashing murni tetap memiliki risiko inheren dalam menghadapi serangan collision yang disengaja atau artefak halus dari generatif AI yang menyerupai pola distribusi gambar asli.

Untuk mengatasi keterbatasan ini, penelitian ini mengusulkan *Veto Mechanism* (VM), sebuah lapisan verifikasi sekunder yang mengevaluasi integritas visual melalui empat deskriptor independen: gradient signature, Local Binary Pattern (LBP), distribusi warna, dan shape descriptor. Mekanisme ini beroperasi menggunakan sistem penalti tertimbang (weighted penalty), di mana setiap diskrepansi pada fitur tekstur mikro atau geometri objek akan memberikan nilai penalti terhadap skor kemiripan akhir. Jika akumulasi penalti tersebut mencapai ambang batas tertentu, VM akan berfungsi sebagai hard constraint yang secara otomatis membatalkan keputusan positif dari hash ensemble. Implementasi ini memastikan bahwa proses verifikasi tidak hanya bertumpu pada kemiripan matematis secara global, tetapi juga secara ketat mempertimbangkan konsistensi detail visual yang sering kali gagal direplikasi secara identik oleh model generatif AI saat ini

Dengan demikian, penelitian ini berupaya menjembatani celah antara *robustness* dan diskriminasi dalam fingerprinting gambar melalui pendekatan ensemble yang komprehensif, didukung oleh arsitektur blockchain untuk menjamin *immutability* data verifikasi. Kerangka kerja ini diharapkan dapat memberikan solusi yang lebih efektif dalam mitigasi fraud yang melibatkan gambar hasil generasi AI.

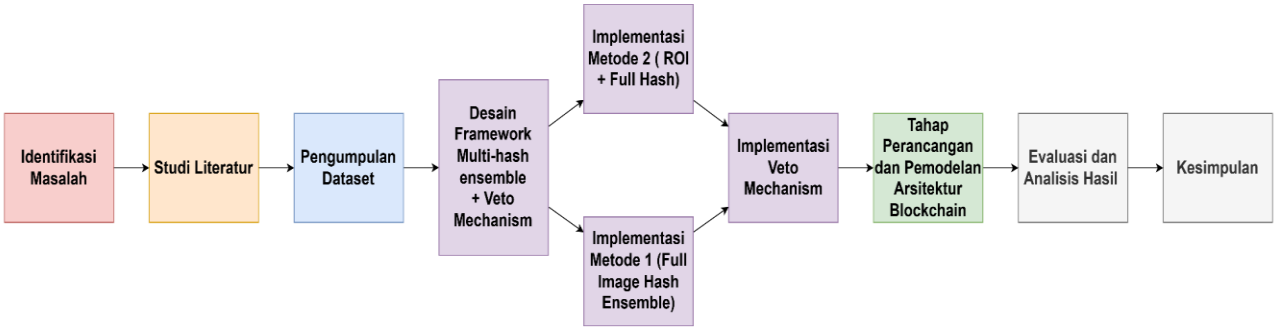
Copyright © 2026 The **Nawirah Athqiyah**, Page 1247
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

2. METODOLOGI PENELITIAN

2.1. Alur penelitian

Gambar 1 mengilustrasikan alur penelitian yang diawali dengan identifikasi masalah fraud citra AI-generated dan studi literatur. Tahap selanjutnya adalah pengumpulan 200 citra (real dan AI) dengan kategori face dan nature dari Roboflow Universe. Framework komputasi diimplementasikan melalui dua pendekatan paralel: Metode 1 (Full Image Hash Ensemble dengan threshold 0,20) dan Metode 2 (Hybrid Fingerprint berbasis latar belakang), yang keputusan akhirnya divalidasi secara ketat oleh Veto Mechanism. Sistem ini turut didukung oleh pemodelan arsitektur blockchain (on-chain/off-chain) untuk mengevaluasi efisiensi penyimpanannya. Terakhir, evaluasi kinerja dilakukan terhadap 22.847 perbandingan yang mencakup 13 jenis serangan on-the-fly pada tiga skenario pengujian (Skenario A, B, dan C), lalu diakhiri dengan analisis komparatif untuk menentukan metode yang paling optimal. Diagram alur penelitian secara keseluruhan ditampilkan pada Gambar 1.

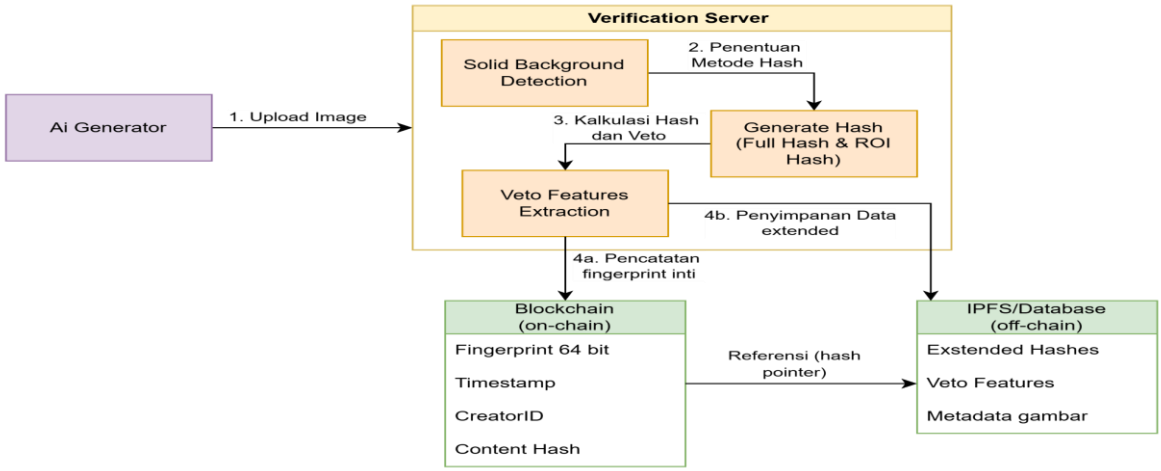


Gambar 1. Diagram Alur Penelitian Multi-Hash Ensemble.

2.2. Arsitektur Sistem

Arsitektur sistem yang diusulkan dirancang untuk menjembatani efisiensi komputasi dengan keamanan integritas data melalui pendekatan hibrida. Secara garis besar, arsitektur ini membagi proses menjadi dua fase krusial: fase pendaftaran (registry) dan fase pembuktian (verification), dengan memisahkan beban kerja antara penyimpanan blockchain (on-chain) dan penyimpanan terdistribusi (off-chain).

a. Arsitektur Registrasi Gambar. Secara fungsional, arsitektur sistem ini memadukan komputasi fitur citra dengan teknologi penyimpanan terdesentralisasi untuk menjamin provenance dan keimutabelan data. Alur kerja dimulai saat citra sintesis dari entitas AI Generator diproses oleh Verification Server melalui kalkulasi hybrid fingerprint (komputasi hash paralel pada citra utuh dan ROI), deteksi homogenitas latar belakang, serta ekstraksi veto features. Untuk mengoptimalkan skalabilitas dan efisiensi biaya, sistem menerapkan mekanisme penyimpanan dua lapis. Data kriptografis esensial—mencakup fingerprint 64-bit, timestamp, identitas kreator, dan content hash—dienkapsulasi secara on-chain pada jaringan blockchain guna menjamin integritas absolut. Sementara itu, beban data berdimensi tinggi seperti extended hashes dan fitur veto disimpan secara off-chain pada IPFS. Kedua lapisan ini dihubungkan secara permanen melalui hash pointer sebagai referensi silang di dalam blockchain. Pendekatan ini memastikan transparansi verifikasi tanpa membebani biaya transaksi jaringan. Arsitektur sistem pada fase registrasi ditampilkan pada Gambar 2.



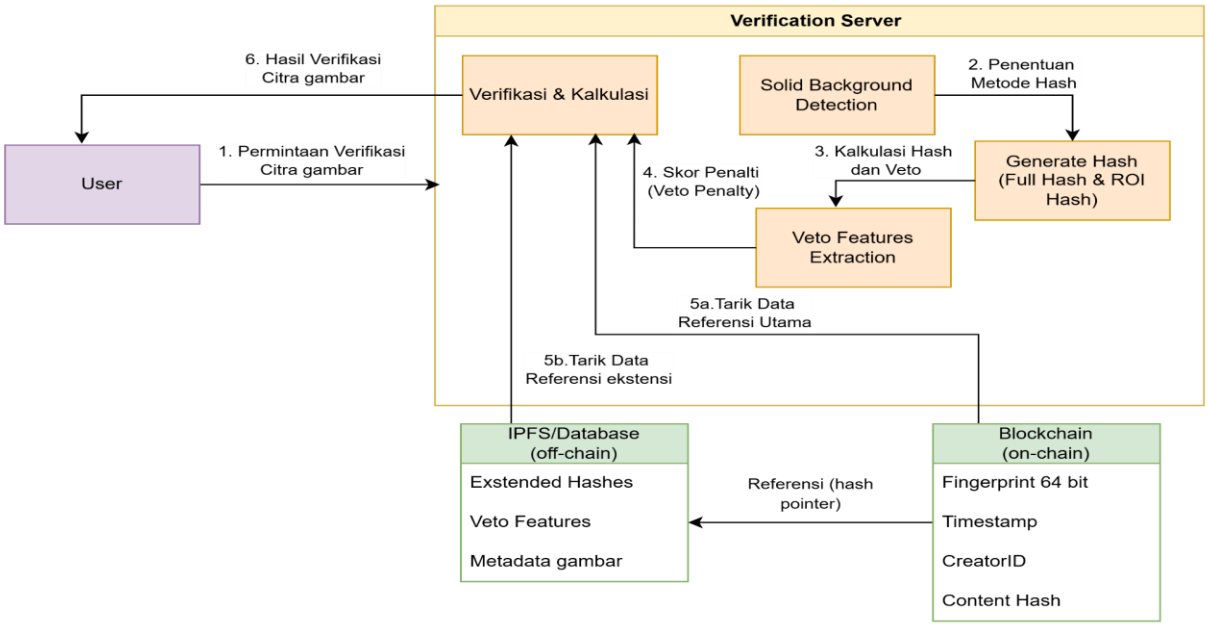
Gambar 2. Arsitektur Sistem Fase Registrasi

b. Arsitektur Verifikasi Autentikasi Gambar Untuk proses autentikasi, alur diinisiasi oleh pengguna (klien) yang mengirimkan permintaan verifikasi berupa citra uji ke Verification Server. Server kemudian mengalkulasi ulang

Copyright © 2026 The **Nawirah Athqiyah**, Page 1248
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

fingerprint dari gambar tersebut dan melakukan komparasi silang terhadap basis data referensi yang tersimpan baik secara on-chain maupun off-chain. Hasil komputasi ini kemudian dikembalikan kepada pengguna dalam bentuk metrik kesamaan (similarity score) beserta keputusan autentikasi akhir. Secara keseluruhan, arsitektur terintegrasi ini secara efektif memitigasi risiko manipulasi gambar manipulatif atau fraud dengan membangun rantai kepercayaan yang transparan, efisien secara komputasional, dan dapat diaudit secara kriptografis. Arsitektur sistem pada fase verifikasi diilustrasikan pada Gambar 3.



Gambar 3. Arsitektur Sistem Fase Verifikasi Autentikasi

2.3. Kajian Pustaka Algoritma

Kerangka kerja ini mengintegrasikan beberapa algoritma dengan landasan teori kuat. pHash memanfaatkan DCT pada frekuensi rendah untuk menghasilkan fingerprint yang robust terhadap skala dan rotasi [17]. wHash menggunakan Haar wavelet untuk menghasilkan hash yang tahan terhadap kompresi JPEG [12]. aHash membandingkan nilai piksel terhadap rata-rata intensitas untuk deteksi duplikasi [13]. dHash menghitung gradien horizontal untuk menangkap pola tepi [13]. LBP mengodekan hubungan piksel pusat dan tetangganya untuk ekstraksi tekstur mikro [9]. Operator Sobel menghasilkan informasi tepi dan kontur objek. K-Means Clustering diterapkan untuk klasifikasi latar belakang berdasarkan centroid cluster [8]. Integrasi algoritma-algoritma ini mengkompensasi kelemahan masing-masing sehingga menghasilkan sistem fingerprinting yang lebih robust dan diskriminatif.

2.4. Mekanisme Veto

Mekanisme veto berfungsi sebagai lapisan verifikasi sekunder (hard constraint) yang mengevaluasi integritas visual citra melalui empat fitur independen. Berbeda dengan mekanisme ensemble yang menggabungkan skor kemiripan secara global, mekanisme veto bekerja dengan cara memberikan penalti absolut jika terdeteksi diskrepansi yang signifikan pada tekstur mikro atau struktur geometri. Mekanisme ini memanfaatkan empat deskriptor visual dengan bobot yang telah ditentukan:

a. Gradient Signature (wgrad = 0.30): Menghitung distribusi magnitudo gradien citra menggunakan operator Sobel. Hasilnya dinormalisasi ke dalam histogram 64-bin dan dikodekan menjadi representasi heksadesimal 16-karakter.
b. LBP Signature (wlbp = 0.25): Menggunakan Local Binary Pattern untuk mengekstrak tekstur mikro citra. Histogram distribusi LBP diekstraksi dan dikonversi menjadi signature heksadesimal.
c. Color Distribution (wcolor = 0.20): Mengevaluasi konsistensi warna global melalui komputasi histogram RGB 16-bin pada setiap channel, yang direpresentasikan dalam signature 4-karakter heksadesimal per channel.
d. Shape Descriptor (wshape = 0.25): Mengekstrak fitur geometri dari Region of Interest (ROI) yang mencakup metrik Aspect Ratio (AR), Solidity (S), dan Extent (E).

2.4.1 Perhitungan Jarak Fitur (Feature Distance)

Untuk membandingkan fitur visual antara citra query dan citra referensi, sistem menghitung jarak atau diskrepansi (D) dari masing-masing deskriptor. Untuk fitur Gradient, LBP, dan Color, sistem menggunakan Normalized Hamming

Copyright © 2026 The **Nawirah Athqiyah**, Page 1249
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Distance terhadap signature heksadesimal.Sementara itu, untuk fitur Shape, jarak dihitung berdasarkan selisih absolut maksimum dari komponen geometrinya, yang diformulasikan sebagai:

$$\boldsymbol{D_{Shape}} = \boldsymbol{max}(|AR_1 - AR_2|, |S_1 - S_2|, |E_1 - E_2|) \quad (1)$$

2.4.2. Komputasi Veto Penalty

Total penalti dari mekanisme veto $(V_{penalty})$ dihitung berdasarkan akumulasi jarak berbobot (weighted sum) dari keempat fitur tersebut. Untuk menghindari penolakan yang terlalu agresif, nilai penalti dibatasi oleh ambang batas maksimum (cap) sebesar 0.60. Formulasi kalkulasi penalti didefinisikan pada persamaan berikut:

$$\boldsymbol{V_{penalty}} = \boldsymbol{min}(\textstyle\sum_{i\epsilon F} \quad w_i . D_i, C_{max}) \quad (2)$$

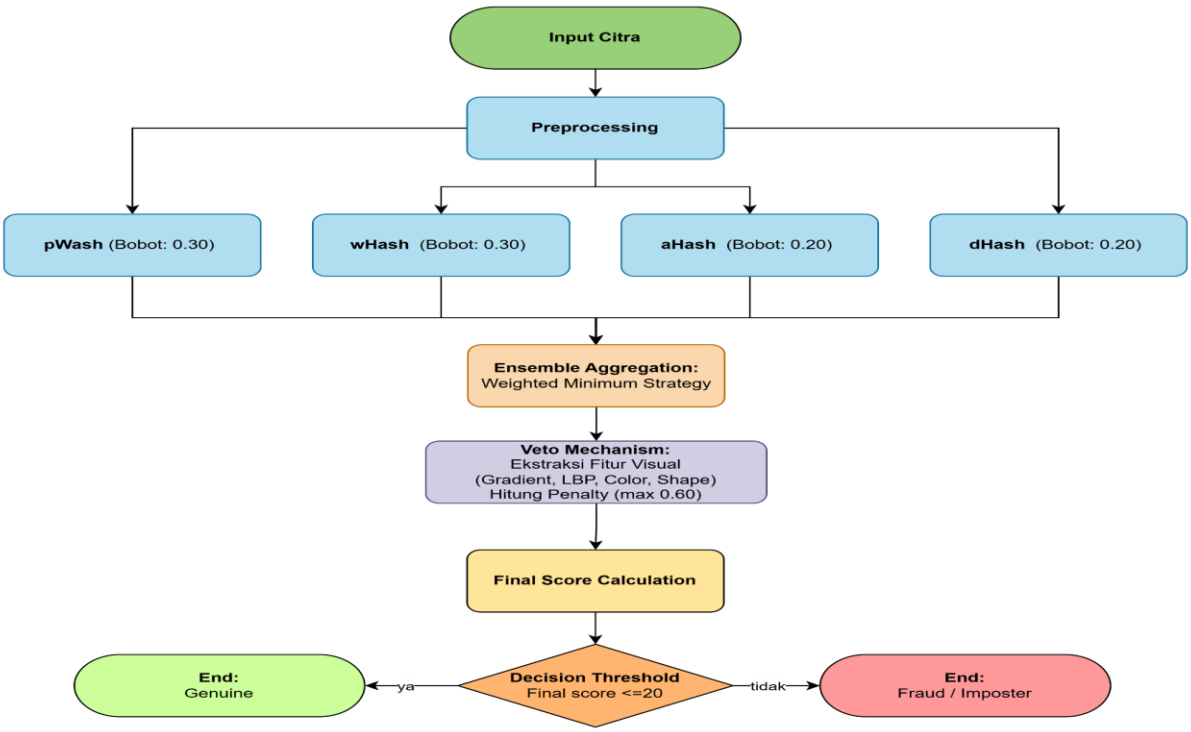
Dimana $F = \{grad, LBP, color, shape\}$,$w_i$merepresentasikan bobot masing-masing fitur, D_i adalah jarak hasil perbandingan fitur, dan $C_{max} = 0.60$ Nilai $V_{penalty}$ ini kemudian akan ditambahkan pada skor akhir hash ensemble. Jika akumulasi skor akhir melampaui threshold penerimaan, maka mekanisme veto secara efektif membatalkan keputusan positif awal dari sistem hashing.

2.5. Metode 1: Full Image Hash Ensemble

Metode 1 menggunakan full image hashing tanpa pemisahan foreground-background. Setiap citra diresize menjadi 8×8 piksel dan dihitung menggunakan empat algoritma secara paraleel: pHash (bobot 0.30) yang memanfaatkan DCT pada frekuensi rendah untuk robustness terhadap skala dan rotasi [18], wHash (bobot 0.30) yang menggunakan Haar wavelet transform untuk ketahanan terhadap kompresi JPEG, serta aHash (bobot 0.20) dan dHash (bobot 0.20) sebagai hash komplementer. Penggabungan skor dilakukan melalui weighted ensemble dengan strategi minimum, di mana skor akhir ditentukan oleh hash yang memberikan jarak Hamming terkecil, sebagaimana ditunjukkan pada Persamaan (1).

$$\boldsymbol{S_{ensemble}} = \boldsymbol{min}(\boldsymbol{w_{pHash}} \cdot \boldsymbol{d_{pHash}}, \boldsymbol{w_{wHash}} \cdot \boldsymbol{d_{wHash}}, \boldsymbol{w_{wHash}} \cdot \boldsymbol{d_{aHash}}, \boldsymbol{w_{dHash}} \cdot \boldsymbol{d_{dHash}}) \quad (3)$$

Pada Persamaan (3), w merepresentasikan bobot masing-masing algoritma dan d merepresentasikan normalized Hamming distance (0 = identik, 1 = berbeda penuh). Keputusan genuine diberikan jika S_ensemble ≤ 0.20. Strategi minimum dipilih karena dalam konteks keamanan, satu hash yang mendeteksi perbedaan sudah cukup untuk menandai citra sebagai fraud [19]. Flowchart Metode 1 ditunjukkan pada Gambar 4.



Gambar 4. Flowchart Metode 1 Full Image Hash Ensemble dengan strategi min dan Veto Mechanism

Gambar 4 memvisualisasikan arsitektur prosedural dari Metode 1 yang berfokus pada pendekatan Full Image Hash Ensemble terintegrasi dengan mekanisme veto. Alur komputasi diinisiasi melalui fase prapemrosesan (preprocessing), di mana citra masukan dinormalisasi dimensinya menjadi matriks 8×8 piksel. Selanjutnya, sistem melakukan ekstraksi fingerprint secara paralel menggunakan empat algoritma perceptual hashing dengan distribusi bobot

Copyright © 2026 The **Nawirah Athqiyah**, Page 1250
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

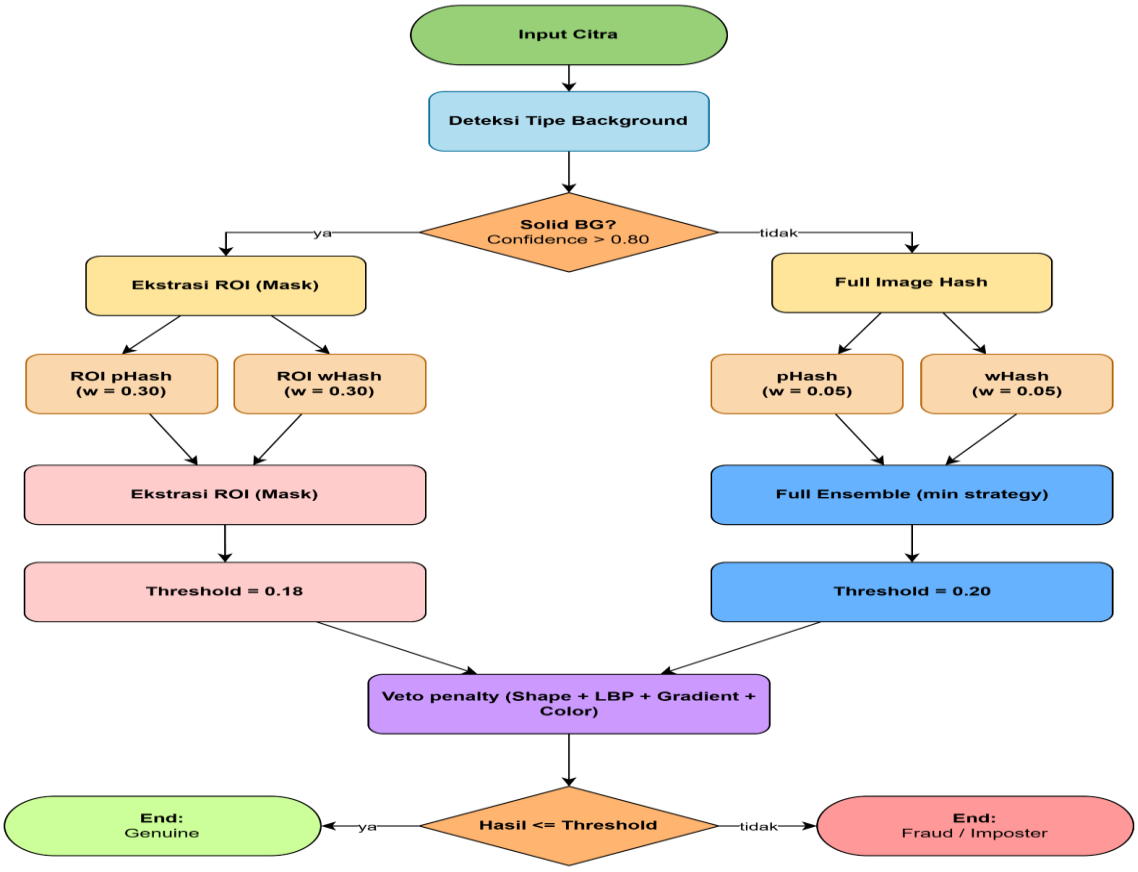
yang telah dikalibrasi: pHash (0,30) untuk menangkap frekuensi rendah berbasis Discrete Cosine Transform (DCT), wHash (0,30) berbasis transformasi Haar wavelet, serta aHash (0,20) dan dHash (0,20) sebagai hash komplementer.

2.5. Metode 2: Hybrid Fingerprint (ROI + Full Hash)

Metode 2 memperkenalkan pendekatan hybrid melalui ekstraksi Region of Interest (ROI) berdasarkan deteksi tipe background. Background diklasifikasikan sebagai solid jika memenuhi dua kriteria: confidence K-means clustering > 0.80 dan rasio foreground ≥ 0.03 [20]. Untuk citra dengan solid background, ROI diekstraksi dari foreground mask menggunakan bounding box dengan padding 15 piksel, kemudian di-hash secara terpisah menggunakan strategi maksimum (max strategy) dengan threshold 0.18. Untuk citra dengan background kompleks, sistem melakukan fallback ke full image hashing dengan strategi minimum dan threshold 0.20 . Skor ROI dikombinasikan dengan skor full hash menggunakan Persamaan (4).

$$S_{hybrid} = max(weighted\ ROI\ Score\ , ROI\ max\ \times\ 0.8) \quad (4)$$

Flowchart alur komputasi Metode 2 dapat dilihat pada Gambar 5.



Gambar 5. Flowchart Metode 2 Hybrid Fingerprint dengan branching ROI vs Full Hash.

Gambar 5 menggambarkan alur komputasi adaptif dari Metode 2 yang memperkenalkan pendekatan Hybrid Fingerprint. Berbeda dengan metode sebelumnya, arsitektur ini menerapkan percabangan (branching) dinamis berdasarkan hasil deteksi homogenitas latar belakang (background) dari citra masukan. Sistem secara otonom mengklasifikasikan latar belakang sebagai "Solid" apabila tingkat konfidensi K-means clustering melampaui 0,80 dan rasio foreground mencapai minimal 0.03Berdasarkan klasifikasi tersebut, alur sistem terbagi menjadi dua cabang utama:

a. Pendekatan Ekstraksi ROI (Latar Belakang Solid): Apabila kriteria latar belakang solid terpenuhi, sistem mengekstraksi Region of Interest (ROI) dari foreground mask (dilengkapi padding 15 piksel). Ekstraksi fingerprint kemudian difokuskan secara eksklusif pada area ROI ini menggunakan pHash (0,30) dan wHash (0,30) dengan ambang batas penerimaan yang lebih ketat, yakni 0,18. Pengetatan threshold ini dirancang untuk meningkatkan sensitivitas deteksi terhadap perubahan manipulatif pada objek utama.
b. Pendekatan Full Hash (Latar Belakang Kompleks): Sebagai mekanisme fallback untuk citra dengan latar belakang heterogen yang tidak memenuhi kriteria, sistem kembali mengimplementasikan Full Image Hash dengan strategi minimum dan ambang batas standar 0,20.

2.5. Integrasi Blockchain

Copyright © 2026 The **Nawirah Athqiyah**, Page 1251
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Data on-chain yang disimpan langsung pada blockchain mencakup fingerprint 64-bit, timestamp UNIX, creator ID, dan content hash SHA-256, dengan total ukuran hanya 20–30 byte per registrasi. Data off-chain yang disimpan pada IPFS mencakup extended hashes, veto features, background analysis, dan metadata citra. Pointer referensi ke data off-chain disimpan on-chain, memungkinkan pengambilan data lengkap saat verifikasi memerlukan analisis mendalam . Arsitektur ini memastikan integritas fingerprint sambil mengoptimalkan biaya penyimpanan [17].

2.6. Dataset dan Skenario Evaluasi

Dataset terdiri dari 200 gambar yang diperoleh dari beberapa dataset Roboflow, Dataset yang digunakan tidak diambil secara langsung dalam bentuk mentah, melainkan dilakukan proses kurasi dan restrukturisasi untuk menyesuaikan kebutuhan eksperimen pada sistem fingerprint berbasis hashing.
Secara khusus, citra dipilih dari dua kategori utama, yaitu wajah (face) [21] dan alam (nature) [22]. Pemilihan dua kategori ini didasarkan pada perbedaan karakteristik visual yang signifikan. Kategori wajah merepresentasikan citra dengan kemiripan struktural yang tinggi (fine-grained similarity), sehingga berpotensi menimbulkan collision pada metode hashing. Sebaliknya, kategori alam memiliki variasi visual yang lebih beragam, sehingga digunakan sebagai pembanding dalam kondisi dengan perbedaan yang lebih jelas (inter-class variability).

Setiap kategori selanjutnya dibagi menjadi dua sumber utama, yaitu skenario A (Genuine Pairs) menguji robustness dengan membandingkan citra yang sama setelah 13 jenis serangan on-the-fly (JPEG compression, blur, resize, rotasi, cropping, brightness). Skenario B (Intra-class Imposter) merupakan hard case yang membandingkan real vs ai dalam kategori sama (face/real vs face/ai, nature/real vs nature/ai), mensimulasikan deepfake berkualitas tinggi . Skenario C (Inter-class Imposter) membandingkan seluruh citra face terhadap nature sebagai baseline. Metrik evaluasi yang digunakan meliputi FAR, FRR, TAR, TRR, Accuracy, Precision, Recall, F1-Score, dan EER.

3. HASIL DAN PEMBAHASAN

Eksperimen dilaksanakan menggunakan dataset 200 citra yang dikurasi dari Roboflow Universe, terbagi ke dalam dua kategori utama (face dan nature) dengan masing-masing subfolder real dan ai. Total 22.847 perbandingan dievaluasi yang terdiri dari 2.546 pasangan genuine (original vs attacked) dan 20.301 pasangan imposter, mencakup 13 jenis serangan on-the-fly. Evaluasi dilakukan terhadap dua metode yang diusulkan, yaitu Metode 1 (Full Image Hash Ensemble) dan Metode 2 (Hybrid Fingerprint dengan ROI + Full Hash). Sub-bab berikut menyajikan hasil evaluasi masing-masing metode secara terpisah, diikuti analisis perbandingan komprehensif.

Penerapan Multi-Hash Ensemble dilaksanakan melalui tahapan sistematis. Tahap pertama: akuisisi dan kurasi 200 citra dari Roboflow Universe ke dalam kategori face dan nature. Tahap kedua: preprocessing berupa normalisasi ukuran citra menjadi 8x8 piksel dan deteksi latar belakang menggunakan K-Means Clustering. Tahap ketiga: ekstraksi fingerprint melalui dua jalur—Metode 1 menjalankan empat algoritma hash secara paralel terhadap citra utuh, sedangkan Metode 2 melakukan percabangan dinamis berdasarkan tipe latar belakang (ROI hash untuk solid, full hash untuk kompleks). Tahap keempat: validasi Veto Mechanism yang mengevaluasi integritas visual melalui sistem penalti tertimbang. Tahap kelima: penyimpanan blockchain hibrida on-chain/off-chain. Tahap terakhir: evaluasi komparatif 22.847 perbandingan melalui tiga skenario pengujian.

3.1 Evaluasi Metode 1: Full Image Hash Ensemble

Hasil evaluasi Metode 1 melalui confusion matrix dan metrik klasifikasi dirangkum dalam Tabel 1. Dari 2.546 pasangan genuine, sebanyak 2.397 pasangan berhasil diterima dengan benar (TP) dan 149 ditolak secara keliru (FN), menghasilkan True Acceptance Rate (TAR) sebesar 94,15%. Sementara itu, dari 20.301 pasangan imposter, sebanyak 20.091 ditolak dengan benar (TN) dan 210 diterima secara keliru (FP), menghasilkan False Acceptance Rate (FAR) sebesar 1,03%. Akurasi keseluruhan sistem mencapai 98,43% dengan F1-Score 93,03% dan EER 3,44%. Hasil ini menunjukkan bahwa Metode 1 memiliki keseimbangan yang baik antara keamanan (FAR rendah) dan kegunaan (FRR rendah), menjadikannya metode yang andal untuk skenario verifikasi citra yang memprioritaskan kemudahan pengguna tanpa mengorbankan keamanan.

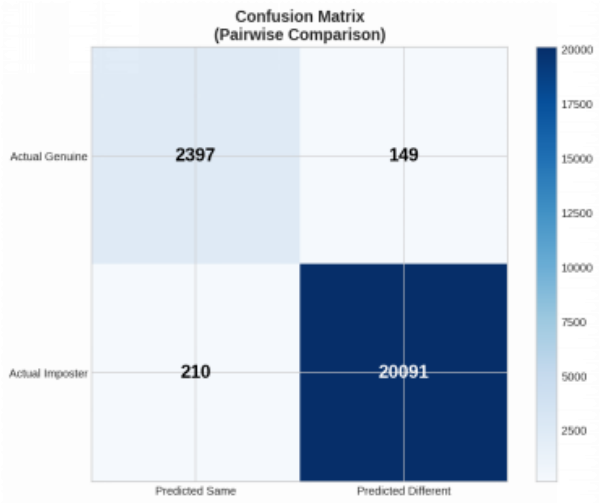
Tabel 1. Confusion matrix dan metrik klasifikasi Metode 1 (Full Image Hash Ensemble).

Metrik	Nilai	Presentase
True Positive (TP)	2.397	93,80%
False Negative (FN)	149	5,85%
True Negative (TN)	20.091	98,97%
False Positive (FP)	210	1,03%
Accuracy	-	98,43%
Precision / Recall / F1	-	91,94% / 94,15% / 93,03%
EER	-	3,44%

Copyright © 2026 The **Nawirah Athqiyah**, Page 1252
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Gambar 6 merepresentasikan visualisasi confusion matrix dari Metode 1 yang secara empiris merefleksikan kondisi ketidakseimbangan kelas (class imbalance) yang sangat wajar dijumpai pada sistem autentikasi riil. Dominasi absolut pada kuadran True Negative (20.091 pasangan) memvalidasi keandalan fungsionalitas ensemble dalam menolak pasangan citra imposter berskala masif. Di sisi lain, tingkat False Positive (FP) yang terkendali pada angka 210 mengindikasikan bahwa perpaduan pembobotan hash mampu mempertahankan batas diskriminasi struktural yang stabil.



Gambar 6. Confusion matrix Metode 1 (Full Image Hash Ensemble).

Detail detection rate untuk setiap jenis serangan on-the-fly pada Skenario A (Genuine Pairs) ditampilkan pada Tabel 2. Metode 1 menunjukkan robustness yang sangat tinggi terhadap serangan yang bersifat non-destruktif terhadap konten visual. Empat jenis serangan mencapai TAR sempurna 100%, yaitu JPEG Compression (Q=30 dan Q=50), Resize (75% dan 50%), serta Gaussian Blur (r=2). Hal ini menunjukkan bahwa keempat algoritma hash dalam ensemble mempertahankan representasi biner yang identik meskipun citra mengalami kompresi JPEG hingga kualitas sangat rendah, penskalaan dimensi hingga setengah ukuran, atau blur ringan. No Attack (Original) juga mencapai 100%, mengkonfirmasi bahwa sistem tidak menghasilkan false rejection pada citra yang tidak dimanipulasi.

Tabel 2. Detection rate per serangan on-the-fly pada Metode 1.

Serangan	Total	TP	FN	TAR(%)
No Attack	202	202	0	100,00
JPEG Q=50	162	162	0	100,00
JPEG Q=30	162	162	0	100,00
Resize 75%	202	202	0	100,00
Resize 50%	202	202	0	100,00
Blur r=2	202	202	0	100,00
Brightness +30%	202	201	1	99,50
Rotation 2°	202	201	1	99,50
Crop 5%	202	197	5	97,52
Brightness +50%	202	195	7	96,53
Rotation 5°	202	191	11	94,55
Blur r=4	202	188	14	93,07
Crop 10%	202	92	110	45,55

Serangan yang paling menantang bagi Metode 1 adalah Cropping 10% dengan TAR hanya 45,55% (110 dari 202 pasangan ditolak). Hal ini konsisten dengan sifat fundamental perceptual hashing di mana penghapusan 10% area citra mengubah distribusi piksel secara signifikan, menyebabkan hash yang dihasilkan berbeda jauh dari citra asli. Blur r=4 juga menunjukkan penurunan yang cukup signifikan (93,07%) karena blur intensif mengaburkan detail frekuensi tinggi yang digunakan oleh pHash dan wHash. Rotation 5° menghasilkan TAR 94,55% yang masih cukup baik mengingat rotasi mengubah representasi piksel secara global.

3.2 Evaluasi Metode 2: Hybrid Fingerprint (ROI + Full Hash)

Confusion matrix dan metrik klasifikasi Metode 2 (Hybrid Fingerprint) dirangkum dalam Tabel 3. Dari 2.546 pasangan genuine, Metode 2 berhasil menerima 1.932 pasangan (TP) dan menolak 614 secara keliru (FN), menghasilkan TAR 75,88% dan FRR 24,12%. Namun, pada sisi keamanan, Metode 2 menunjukkan peningkatan signifikan dengan hanya

Copyright © 2026 The **Nawirah Athqiyah**, Page 1253
This Journal is licensed under a Creative Commons Attribution 4.0 International License

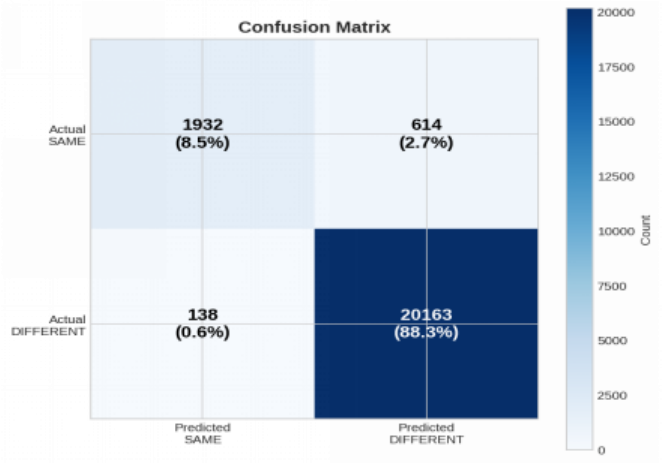
JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

138 false positive dari 20.301 pasangan imposter, menghasilkan FAR 0,68% yang lebih rendah dibanding Metode 1 (1,03%). Precision mencapai 93,33%, yang berarti dari setiap keputusan acceptance yang diberikan oleh Metode 2, 93,33% memang merupakan pasangan genuine. EER tercatat pada 4,62% dengan threshold optimal F1-Score berada pada 0,22.

Tabel 3. Confusion matrix dan metrik klasifikasi Metode 2 (Hybrid Fingerprint).

Metrik	Nilai	Presentase
True Positive (TP)	1.932	75,88%
False Negative (FN)	614	24,12%
True Negative (TN)	20.163	99,32%
False Positive (FP)	138	0,68%
Accuracy	-	96,71%
Precision / Recall / F1	-	93,33% / 75,88% / 83,71%
Specificity / Balanced Acc	-	99,32% / 87,60%
MCC / EER	-	0,824 / 4,62%

Penurunan TAR dari 94,15% (Metode 1) menjadi 75,88% (Metode 2) merupakan trade-off yang diakibatkan oleh threshold ROI yang lebih ketat (0,18 vs 0,20). Analisis per metode menunjukkan bahwa HYBRID_ENSEMBLE memiliki FRR 26,16% sementara FULL_HASH_COMPARISON (fallback) memiliki FRR 23,11%, mengindikasikan bahwa proses ROI extraction memperketat kriteria penerimaan. Namun, di sisi keamanan, HYBRID_ENSEMBLE mencapai FAR 0,00% (zero false positive) dari 3.486 pasangan imposter yang dievaluasi, sementara FULL_HASH_COMPARISON mencatat FAR 0,82% dari 16.815 pasangan. Keunggulan FAR nol pada mode HYBRID_ENSEMBLE ini membuktikan bahwa pendekatan ROI-based hashing memiliki daya pembeda yang lebih tinggi untuk mendeteksi citra berbeda pada background solid.Visualisasi confusion matrix Metode 2 ditampilkan pada Gambar 7.



Gambar 7. Confusion matrix Metode 2 (Hybrid Fingerprint).

Gambar 7 menunjukkan visualisasi confusion matrix dari Metode 2 (Hybrid Fingerprint) yang merefleksikan dampak threshold ROI yang lebih ketat terhadap distribusi keputusan klasifikasi. Dibandingkan dengan Metode 1, kuadran False Negative terlihat lebih dominan dengan 614 pasangan genuine yang ditolak secara keliru, mengonfirmasi peningkatan FRR menjadi 24,12%. Di sisi lain, kuadran True Negative tetap menunjukkan angka yang sangat tinggi, yang mengindikasikan bahwa pengetatan threshold berhasil mempertahankan kemampuan deteksi fraud dengan FAR yang sangat rendah.

Detection rate per jenis serangan pada Metode 2 diuraikan pada Tabel 4. Sama seperti Metode 1, No Attack mencapai 100% dan JPEG Compression memiliki TAR di atas 96%. Namun, threshold ROI yang lebih ketat (0,18) menyebabkan penurunan TAR yang lebih signifikan pada serangan geometris dan brightness dibanding Metode 1. Rotation 5° mengalami penurunan tajam menjadi 58,42% dan Cropping 10% hanya mencapai 22,77%. Hal ini menunjukkan bahwa ROI extraction sangat sensitif terhadap perubahan posisi objek akibat rotasi dan cropping, karena area foreground yang diekstraksi bergeser dari posisi aslinya sehingga ROI hash yang dihasilkan berbeda secara substansial.

Copyright © 2026 The **Nawirah Athqiyah**, Page 1254
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Tabel 4. Detection rate per serangan on-the-fly pada Metode 2.

Serangan	Total	TP	FN	TAR(%)
No Attack	202	202	0	100,00
JPEG Q=50	162	157	5	96,91
JPEG Q=30	162	156	6	96,30
Resize 75%	202	198	4	98,02
Resize 50%	202	195	7	96,53
Blur r=2	202	175	27	86,63
Brightness +30%	202	147	55	72,77
Rotation 2°	202	150	52	74,26
Crop 5%	202	130	72	64,36
Brightness +50%	202	126	76	62,38
Rotation 5°	202	118	84	58,42
Blur r=4	202	132	70	65,35
Crop 10%	202	46	156	22,77

3.3 Analisis Perbandingan Kedua Metode

Perbandingan komprehensif performa kedua metode dipaparkan pada Tabel 5. Metode 1 unggul secara keseluruhan pada metrik keseimbangan (Accuracy 98,43% vs 96,71%, F1-Score 93,03% vs 83,71%) dan memiliki FRR yang jauh lebih rendah (5,85% vs 24,12%), menjadikannya metode yang lebih sesuai untuk aplikasi verifikasi citra yang membutuhkan keseimbangan antara keamanan dan kegunaan. Namun, Metode 2 menunjukkan keunggulan signifikan pada aspek keamanan murni dengan FAR yang lebih rendah (0,68% vs 1,03%), Precision yang lebih tinggi (93,33% vs 91,94%), dan Specificity yang mendekati sempurna (99,32% vs 98,97%).

Tabel 5. Perbandingan metrik evaluasi antara Metode 1 dan Metode 2

Metrik	Metode 1	Metode 2	Selisih
TP	2.397	1.932	-465
FP	210	138	-72
FN	149	614	+465
TN	20.091	20.163	+72
FAR (%)	1,03	0,68	-0,35
FRR (%)	5,85	24,12	+18,27
Accuracy (%)	98,43	96,71	-1,72
Precision (%)	91,94	93,33	+1,39
Recall (%)	94,15	75,88	-18,27
F1-Score (%)	93,03	83,71	-9,32
EER (%)	3,44	4,62	+1,18

Perbedaan performa ini dapat dijelaskan melalui mekanisme operasional masing-masing metode. Metode 1 menggunakan threshold tunggal 0,20 dengan strategi minimum yang cenderung permisif terhadap perbedaan kecil, sehingga menghasilkan FRR rendah namun FAR sedikit lebih tinggi. Metode 2 menggunakan threshold adaptif (0,18 untuk ROI, lebih ketat) yang meningkatkan sensitivitas deteksi perbedaan pada citra dengan solid background, menghasilkan FAR lebih rendah namun FRR lebih tinggi. Keunggulan FAR nol pada mode HYBRID_ENSEMBLE (0 FP dari 3.486 pasangan) menunjukkan bahwa ROI-based hashing secara fundamental memiliki daya pembeda yang lebih kuat untuk citra yang secara visual berbeda namun berada dalam kategori sama.

Analisis per skenario evaluasi memberikan insight tambahan. Pada Skenario B (Intra-class Imposter, hard case), kedua metode menunjukkan kemampuan yang baik dalam membedakan citra real dan AI-generated dalam kategori yang sama. Similarity rata-rata untuk pasangan imposter intra-class berada pada kisaran 0,25–0,50, yang menunjukkan bahwa meskipun citra real dan AI-generated memiliki konten visual yang mirip (keduanya menampilkan wajah atau pemandangan alam), perbedaan tekstur dan noise pattern yang ditangkap oleh ensemble hashing dan veto features cukup signifikan untuk membedakan keduanya. Pada Skenario C (Inter-class Imposter, easy case), kedua metode mencapai rejection rate mendekati 100% karena perbedaan visual antara kategori face dan nature sangat jelas, dengan similarity rata-rata di bawah 0,10.

Dari hasil kedua metode untuk implementasi mitigasi fraud di dunia nyata, karakteristik ini mengindikasikan bahwa Metode 1 lebih optimal untuk platform publik yang memprioritaskan kenyamanan pengguna (menghindari salah

Copyright © 2026 The **Nawirah Athqiyah**, Page 1255
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

blokir/FRR rendah), sementara Metode 2 wajib diterapkan pada sistem kritikal seperti verifikasi identitas (KYC) yang menuntut keamanan absolut dari celah manipulasi citra AI.

3.4 Analisis Efisiensi Penyimpanan dan Biaya Blockchain

Meskipun arsitektur yang diusulkan mengintegrasikan teknologi blockchain untuk menjamin keimutabelan (immutability) data, penyimpanan citra secara langsung pada ledger blockchain (on-chain) sangat tidak efisien dan memakan biaya Gas Fee yang eksponensial [23]. Pada jaringan Ethereum, setiap byte data yang disimpan dalam smart contract memerlukan biaya penyimpanan yang signifikan, yang secara langsung meningkat seiring dengan bertambahnya ukuran data. Studi empiris menunjukkan bahwa biaya penyimpanan on-chain bersifat non-linear terhadap volume data, sehingga menyimpan file citra secara langsung ke dalam blockchain menjadi tidak praktis dari segi ekonomis maupun teknis [24]. Oleh karena itu, penelitian ini mengadopsi arsitektur hibrida on-chain dan off-chain (IPFS) sebagai solusi untuk mengatasi kendala tersebut, sekaligus mempertahankan jaminan integritas data melalui mekanisme cryptographic binding.

3.4.1 Analisis Efisiensi Penyimpanan dan Biaya Blockchain

Sistem yang diusulkan mereduksi data yang masuk ke dalam smart contract secara drastis melalui teknik abstraksi fingerprint. Rata-rata ukuran citra dalam dataset pengujian berkisar antara 2 MB hingga 5 MB, tergantung pada resolusi dan tingkat kompresi. Jika menggunakan metode on-chain murni tanpa mekanisme kompresi data, beban penyimpanan akan menjadi sangat masif dan biayanya tidak terjangkau, terutama untuk platform dengan volume unggahan citra yang tinggi. Namun, dengan metode Multi-Hash Ensemble yang diusulkan, data on-chain hanya terdiri dari komponen-komponen ringkas yang merepresentasikan identitas unik citra tersebut.Komponen data on-chain yang disimpan dalam smart contract untuk setiap registrasi citra dirinci pada Tabel 6 berikut ini.

Tabel 6. Komponen Data On-Chain per Registrasi Citra.

Komponen Data	Ukuran	Satuan
Fingerprint citra (64-bit)	8	byte
Timestamp UNIX	4	byte
Creator ID (Alamat Wallet)	20	byte
Content Hash (SHA-256)	32	byte
Total	**~64**	byte
Total	~64	byte

Berdasarkan data pada Tabel 6, total ukuran data on-chain per registrasi citra adalah sekitar 64 byte. Angka ini merepresentasikan rasio kompresi penyimpanan spasial lebih dari 99,99% dibandingkan dengan penyimpanan citra mentah secara langsung pada blockchain. Sebagai gambaran perbandingan, sebuah citra berukuran 3 MB (setara dengan 3.145.728 byte) direduksi menjadi hanya 64 byte pada smart contract, yang merupakan faktor reduksi sebesar lebih dari 49.000 kali lipat. Hal ini menjadikan sistem yang diusulkan sangat ringan (lightweight) dan terukur (scalable) untuk platform dengan volume unggahan citra yang tinggi, seperti platform jurnalisme digital, repositori medis, atau sistem dokumentasi forensik [25].

Efisiensi penyimpanan ini dicapai melalui desain arsitektur yang memisahkan data berat (extended hashes, fitur Veto, metadata citra) ke penyimpanan off-chain berbasis IPFS, sementara hanya menyimpan komponen kritis berukuran minimal pada blockchain. Content Hash (SHA-256) berfungsi sebagai pengikat kriptografis (cryptographic anchor) yang menghubungkan data off-chain dengan catatan on-chain, sehingga memungkinkan verifikasi integritas tanpa perlu menyimpan data lengkap pada blockchain [26]. Pendekatan ini sejalan dengan prinsip desain sistem terdistribusi modern yang mengutamakan efisiensi penyimpanan tanpa mengorbankan keamanan dan keandalan verifikasi.

3.4.2 Estimasi Biaya Transaksi (Cost Analysis)

Berdasarkan literatur terkait biaya penyimpanan pada jaringan Ethereum Virtual Machine (EVM), setiap 1 Kilobyte (KB) data on-chain membutuhkan biaya Gas yang signifikan [27]. Pada Ethereum Yellow Paper, operasi penyimpanan non-zero byte (SSTORE) memerlukan 20.000 Gas, sedangkan zero byte memerlukan 4.000 Gas. Dengan beban data hanya ~64 byte per registrasi, estimasi Gas Fee untuk eksekusi fungsi pencatatan fingerprint berada pada rentang minimum, setara dengan transaksi transfer standar Ethereum yaitu sekitar 21.000 hingga 30.000 Gas. Estimasi biaya ini mencakup biaya operasi SLOAD untuk pembacaan state, SSTORE untuk penulisan data, dan biaya dasar transaksi (intrinsic gas) sebesar 21.000 Gas.Perbandingan estimasi biaya transaksi pada berbagai jaringan blockchain yang kompatibel dengan EVM disajikan pada Tabel 7.

Copyright © 2026 The **Nawirah Athqiyah**, Page 1256
This Journal is licensed under a Creative Commons Attribution 4.0 International License

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 5, Oktober 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v15i5.9732
Hal 1246-1258
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Tabel 7. Estimasi Biaya Transaksi per Jaringan Blockchain.

Jaringan	Gas Fee Estimasi (per transaksi)	Biaya per Citra
Ethereum Mainnet	21.000 – 30.000 Gas	$1,00 – $5,00
Polygon (Layer-2)	21.000 – 30.000 Gas	< $0,01
Arbitrum (Layer-2)	21.000 – 30.000 Gas	< $0,01

Berdasarkan estimasi pada Tabel 7, implementasi pada jaringan Ethereum Mainnet memiliki biaya tertinggi karena tingginya permintaan jaringan dan mekanisme konsensus Proof-of-Stake (PoS) yang tetap mempertahankan biaya Gas yang relatif tinggi untuk operasi penyimpanan. Namun, dengan migrasi ke jaringan Layer-2 seperti Polygon atau Arbitrum, biaya registrasi per citra secara teoretis dapat ditekan hingga di bawah $0,01 USD. Polygon menggunakan teknologi Plasma dan Validium yang memproses transaksi di luar rantai utama Ethereum, sementara Arbitrum memanfaatkan Optimistic Rollup yang mengagregasi beberapa transaksi menjadi satu bukti tunggal yang dikirimkan ke Ethereum Mainnet [28]. Kedua pendekatan ini secara signifikan mengurangi biaya operasional tanpa mengorbankan tingkat keamanan yang dijamin oleh jaringan utama (base layer) Ethereum.

Untuk aplikasi skala besar (enterprise-level deployment), efisiensi biaya ini memiliki implikasi praktis yang sangat signifikan. Sebagai ilustrasi, sebuah platform verifikasi citra forensik yang memproses 10.000 citra per hari akan mengeluarkan biaya on-chain sekitar $10–$50 pada jaringan Ethereum Mainnet, atau kurang dari $100 per hari pada Polygon. Bandingkan dengan pendekatan on-chain murni yang akan menghabiskan ratusan hingga ribuan dolar per hari untuk volume yang sama, menjadikan pendekatan hibrida yang diusulkan sebagai solusi yang jauh lebih ekonomis dan sustainable dalam jangka panjang [28].

3.4.3 Jaminan Integritas Data

Kelemahan fundamental penyimpanan off-chain berhasil dimitigasi melalui penguncian Content Hash (SHA-256) pada blockchain. Pada fase registrasi, sistem mengekstraksi hash dari seluruh payload data off-chain (termasuk fitur Veto dan metadata) untuk dicatat pada smart contract. Saat verifikasi, hash tersebut dihitung ulang dari IPFS dan dicocokkan dengan catatan on-chain [29].

Apabila terdapat manipulasi data oleh pihak tidak berwenang, diskrepansi nilai hash akan secara otomatis memicu penolakan sistematis oleh smart contract. Mekanisme ini memberikan jaminan integritas data yang esensial untuk pembuktian forensik digital, menghadirkan keamanan setara penyimpanan on-chain penuh namun dengan efisiensi biaya maksimal [30]. Lebih lanjut, sifat immutable blockchain memberikan trustless assurance—memastikan fingerprint tidak dapat dimodifikasi oleh entitas manapun—sehingga arsitektur hibrida ini sukses mencapai ekuilibrium antara efisiensi operasional dan keamanan data absolut [31].

4. KESIMPULAN

Penelitian ini berhasil memvalidasi kerangka kerja *Multi-Hash Ensemble* dengan *Veto Mechanism* dan arsitektur *blockchain* hibrida untuk memitigasi *fraud* citra hasil *Artificial Intelligence* (AI) generatif, di mana Metode 1 (*Full Image Hash Ensemble*) terbukti memberikan keseimbangan optimal antara keamanan dan *usability* dengan tingkat akurasi 98,43%, *F1-Score* 93,03%, serta *Equal Error Rate* (EER) 3,44%. Sebagai komparasi untuk platform bersensitivitas keamanan tinggi, Metode 2 (*Hybrid Fingerprint*) menawarkan keunggulan keamanan absolut melalui strategi agregasi adaptif yang sukses menekan *False Acceptance Rate* (FAR) hingga 0% pada mode *HYBRID_ENSEMBLE*. Efisiensi arsitektur ini juga dibuktikan oleh integrasi *on-chain/off-chain* yang mencetak rasio kompresi spasial >99,99% (mereduksi data menjadi ~64 byte per registrasi) dengan estimasi beban transaksi Layer-2 di bawah $0,01 USD, sementara *Veto Mechanism* sukses bertindak sebagai *hard constraint* pembatal validasi saat terdeteksi inkonsistensi fitur struktural sekunder. Meskipun evaluasi terhadap 22.847 perbandingan menunjukkan hasil yang menjanjikan, penelitian ini masih memiliki beberapa keterbatasan, di antaranya kerentanan algoritma terhadap manipulasi pemotongan gambar (*cropping*), belum adanya kalibrasi *Gas Fee* dan latensi jaringan aktual secara *end-to-end* pada ekosistem *testnet blockchain*, serta keterbatasan evaluasi yang belum mencakup luaran dari model AI generatif mutakhir (seperti DALL-E 3 dan Midjourney v6), sehingga pengembangan pada aspek-aspek tersebut menjadi esensial untuk mengukur ketahanan sistem pada lingkungan operasional skala produksi.

REFERENCES

[1] A. R. S. Muhammad Bilal Fauzan, "Pengaruh Teknologi Visual Pengalaman Pengguna: Impilikasi Terhadap Budaya Konsumsi Dan Identitas Nasional," Nov. 2024, doi: 10.5281/ZENODO.14167733.
[2] D. A. Lestari and F. Lubis, "Pengaruh Bukti Fotografi Dan Videografi Dalam Proses Pembuktian Perdata".
[3] D. Maulana, N. S. Azzahrah, R. A. Syach, S. Syauri, M. Syafi'i, and C. Rozikin, "Identifikasi Konten Visual Buatan Ai Dengan Resnet Dan Fine-Grained Feature Extraction," *J. Inform. Dan Tek. Elektro Terap.*, vol. 13, no. 3S1, Oct. 2025, doi: 10.23960/jitet.v13i3S1.8056.

Copyright © 2026 The **Nawirah Athqiyah**, Page 1257
This Journal is licensed under a Creative Commons Attribution 4.0 International License

[4] J. C. Monge, "Dall-E 3 VS MidJourney 5.2 VS Stable XL — Same Prompt, Different Results," Medium. Accessed: Apr. 25, 2026. [Online]. Available: https://generativeai.pub/dall-e-3-vs-midjourney-5-2-vs-stable-xl-same-prompt-different-results-a68ae19b223e
[5] E. P. Boediman, "Exploring the Impact of Deepfake Technology on Public Trust and Media Manipulation: A Scoping Review," *J. Komun.*, vol. 19, no. 2, pp. 313–334, Apr. 2025, doi: 10.20885/komunikasi.vol19.iss2.art8.
[6] A. Qureshi and D. Megías Jiménez, "Blockchain-Based Multimedia Content Protection: Review and Open Challenges," *Appl. Sci.*, vol. 11, no. 1, p. 1, Jan. 2021, doi: 10.3390/app11010001.
[7] S. A. R and J. Katiravan, "BlockImage: A Secure Framework for Image Authentication and Provenance Using AI and Blockchain," *J. Innov. Image Process.*, vol. 7, no. 1, pp. 28–49, Mar. 2025, doi: 10.36548/jiip.2025.1.002.
[8] Q. Hao, L. Luo, S. T. K. Jan, and G. Wang, "It's Not What It Looks Like: Manipulating Perceptual Hashing Based Applications," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, Virtual Event Republic of Korea: ACM, Nov. 2021, pp. 69–85. doi: 10.1145/3460120.3484559.
[9] C. Xiong, E. Liu, X. Li, H. Yao, L. Zhang, and C. Qin, "Perceptual Image Hashing Based on Multitask Neural Network," *Secur. Commun. Netw.*, vol. 2021, no. 1, p. 8297244, 2021, doi: 10.1155/2021/8297244.
[10] M. Hamadouche, K. Zebbiche, M. Guerroumi, H. Tebbi, and Y. Zafoune, "A Comparative Study of Perceptual Hashing Algorithms: Application on Fingerprint Images".
[11] J. Madden, M. Bhavsar, L. Dorje, and X. Li, "Robustness of Practical Perceptual Hashing Algorithms to Hash-Evasion and Hash-Inversion Attacks," Dec. 05, 2024, *arXiv*: arXiv:2406.00918. doi: 10.48550/arXiv.2406.00918.
[12] A. Hassan, "Perceptual Image Hashing by Exploiting a Visual Attention Model Along with Discrete Wavelet Transform and Discrete Cosine Transform," *J. Electron. Imaging*, vol. 33, no. 6, p. 063057, Dec. 2024, doi: 10.1117/1.JEI.33.6.063057.
[13] C. Zauner, "Implementation and Benchmarking of Perceptual Image Hash Functions".
[14] Q.-Y. Zhang, Z. Yang, Q.-Y. Dou, and Y. Yan, "Robust Hashing for Color Image Authentication Using Non-Subsampled Contourlet Transform Features and Salient Features".
[15] V. Monga and B. L. Evans, "Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs," *IEEE Trans. Image Process.*, vol. 15, no. 11, pp. 3452–3465, Nov. 2006, doi: 10.1109/TIP.2006.881948.
[16] "(PDF) Robust Image Hashing Based on Structural and Perceptual Features for Authentication of Color Images," *ResearchGate*, doi: 10.3906/elk-2002-6.
[17] A. Shahzad, W. Chen, Y. Zhang, and R. Kumar, "Zero-Trust Medical Image Sharing: A Secure and Decentralized Approach Using Blockchain and the IPFS," *Symmetry*, vol. 17, no. 4, p. 551, Apr. 2025, doi: 10.3390/sym17040551.
[18] "Frontiers | Decentralizing video copyright protection: a novel blockchain-enabled framework with performance evaluation." Accessed: Apr. 12, 2026. [Online]. Available: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1655709/full
[19] Q. Hao, L. Luo, S. T. K. Jan, and G. Wang, "It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, Virtual Event Republic of Korea: ACM, Nov. 2021, pp. 69–85. doi: 10.1145/3460120.3484559.
[20] R. E. Arevalo-Ancona and M. Cedillo-Hernandez, "Zero-Watermarking for Medical Images Based on Regions of Interest Detection using K-Means Clustering and Discrete Fourier Transform," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, 2023, doi: 10.14569/IJACSA.2023.0140662.
[21] "Real vs AI faces Object Detection Dataset by Similarity," Roboflow. Accessed: Apr. 20, 2026. [Online]. Available: https://universe.roboflow.com/similarity-rgq5n/real-vs-ai-faces-2vvfg
[22] "Portfolio (AI vs Real Images) Dataset > Overview," Roboflow. Accessed: Apr. 20, 2026. [Online]. Available: https://universe.roboflow.com/similarity-rgq5n/portfolio-ai-vs-real-images-eitdu-nuqqb
[23] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".
[24] D. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger".
[25] T. S. Famuji, H. Herman, and S. Sunardi, "Smart Contract Penyimpanan Data Genetika Manusia Berbiaya Murah Pada Blockchain Ethereum," *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 11, no. 3, pp. 695–704, Jul. 2024, doi: 10.25126/jtiik.1137558.
[26] T. Bicara, "Peran IPFS (InterPlanetary File System) Dalam Web3," anakteknik.co.id. Accessed: Apr. 25, 2026. [Online]. Available: https://www.anakteknik.co.id/tatabicara12/articles/peran-ipfs-interplanetary-file-system-dalam-web3
[27] B. Chatwin, "Ethereum Gas Fees Explained." Accessed: Apr. 25, 2026. [Online]. Available: https://www.dwellir.com/blog/ethereum-gas-fees-explained
[28] Coinvestasi, "coinvestasi," Mengenal Arbitrum Proyek Layer-2 yang Curi Perhatian. Accessed: Apr. 25, 2026. [Online]. Available: https://coinvestasi.com/
[29] M. Kavitha, "Blockchain-Based Data Integrity Framework for Secure Cloud Storage Systems," 2024.
[30] S. Srivastava, G. Kaur, Himank, and S. Singla, "Implementation of Blockchain and IPFS to Safeguard Evidentiary Data," *2024 Int. Conf. Knowl. Eng. Commun. Syst. ICKECS*, pp. 1–6, Apr. 2024, doi: 10.1109/ICKECS61492.2024.10616708.
[31] G. Sinaga, "Analisa Metode Imagehash Untuk Mendeteksi Orisinalitas Citra Digital," vol. 1, no. 4, 2021.

Copyright © 2026 The **Nawirah Athqiyah**, Page 1258
This Journal is licensed under a Creative Commons Attribution 4.0 International License