Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

Blockchain-Enabled Image Provenance Authentication for Camera-Origin vs. AI-Synthesized Media: Architecture and Validation

Muhammad Imran Ghafoor[*1], Shanila Azhar[2], Saeed Ahmed Magsi [3], Muhammad Sohaib Roomi [4], Hamayoun Shahwani[5]

[*1]*Department of Engineering & Technology, Superior University, Lahore, Pakistan*
[2]*Department of Computer Engineering, Balochistan University of Information Technology, Engineering, and Management Sciences (BUITEMS), Quetta, Pakistan*
[3]*Department of Electrical Engineering, Balochistan University of Information Technology, Engineering, and Management Sciences (BUITEMS), Quetta, Pakistan*
[4]*Department of Engineering & Technology, Superior University, Lahore, Pakistan*
[3]*Department of Electrical Engineering, Balochistan University of Information Technology, Engineering, and Management Sciences (BUITEMS), Quetta, Pakistan*

[*1]engr.imranbhatti09@ieee.org, [2] shanila.Azhar@buitms.edu.pk,
[3] saeed.ahmed@buitms.edu.pk, [4] sohaib4039@gmail.com, [5]hamayoun.yousaf@buitms.edu.pk

DOI: https://doi.org/10.5281/zenodo.19674738

Keywords
Blockchain, image authentication, deepfake detection, generative adversarial networks, image forensics, cryptographic hashing, machine learning, smart contracts, provenance verification, image integrity, camera fingerprinting, AI-generated content detection

Article History
Received: 22 February 2026
Accepted: 03 April 2026
Published: 21 April 2026

Corresponding Author:
Muhammad Imran Ghafoor

Abstract
With the blistering development of generative artificial intelligence and especially generative adversarial networks (GANs), as well as diffusion models, there is now an unprecedented difficulty in identifying fundamental limitations [2], [34], [53]. whether a particular image was taken by a camera or created by artificial intelligence. The paper outlines a holistic image authentication system based on blockchain that incorporates a multi-modal feature extraction method with blockchain-authenticated provenance verification that can be trusted to label camera images as original. Our four-layer architecture proposal is a combination of: (1) cryptographic image hashing with SHA-256, SHA-512, BLAKE2b and perceptual hashing; (2) a 50-dimensional forensic feature image consisting of color statistics, frequency domain (FFT) analysis, edge/texture descriptors, and image quality measures, (3) machine learning classification with ensembles of Random Forest, The experimental validation on a dataset of 196 images (96 real camera photographs by Unsplash and 100 AI-generated images with known GAN artifacts) shows that our ensemble model is able to detect the synthetic content with 97.96% accuracy and is resilient to typical post-processing manipulations, which provides a scalable and tamper-proof method to preserve the authenticity of digital images.

I. INTRODUCTION

The uncontrollable generative development of artificial intelligence has brought a severe crisis of authenticity in digital media [1]. The use of generative adversarial networks (GANs) [2 - 3], diffusion models, and neural style transfer

methods are now able to produce synthetics indistinguishable to real camera-captured photographs, seriously compromising social trust in visual content in journalism, legal evidence, medical imaging, and social media. The swift spread of deepfake technology is a significant risk to the integrity of information, and according to recent reports, the quantity of deepfake material has increased more than 900% over the past few years. This increasing difficulty requires new solutions beyond the conventional detection techniques, which can be easily overcome by the novel generator architectures that are continually reducing artifacts that can be detected.

The proliferation of deepfake technology represents a significant threat to information integrity [1], [39 -50]. The main research question of this work is as follows: How can blockchain technology be naturally incorporated with modern machine learning to create a stable, privacy-conscious system that will be able to differentiate between authentic camera shots and images produced by AI? [4] This question has a number of sub-challenges, some of which are closely related to each other, such as finding strong forensic properties that are discriminative, even in the face of the growing sophistication of AI generators; establishing indelible provenance records using distributed consensus schemes that are resistant to collusion and tampering; achieving high computational efficiency with sub-second local processing to support real-time camera operations; ensuring that detection [24 - 26].

To overcome these problems, this paper contributes in several ways. First, it presents a broad-based 4-layer blockchain-driven image authentication model that integrates cryptographic hashing, multi-modal forensic feature extraction, ensemble machine learning classification, and smart contract-based verification. Second, it suggests a well-crafted 50-dimensional forensic feature image, which incorporates color statistics, frequency-domain FFT spectral analysis, and edge and texture descriptors, as well as image quality metrics, specifically designed to detect artifacts in GAN- and diffusion-generated images. Third, the framework has a detection accuracy of 97.96% when rigorously experimentally validated on a balanced dataset of 196 images, including 96 real camera photographs obtained by Unsplash and 100 AI-generated images with known synthetic artifacts. Other contributions are a systematic performance analysis of various hashing functions (SHA-256, SHA-512, BLAKE2b, and perceptual hashing) that indicate sub-milliseconds overhead, robustness testing against nine typical image modification attacks with 98.89 percent accuracy, and an in-depth analysis of feature importance that indicates that texture homogeneity and spectral characteristics are the strongest discriminators between authentic and synthetic content.

The rest of the paper will be structured as follows: the following section will be a review of related literature in the field of image forensics, deepfake detection, and the use of blockchains to authenticate the media. This is then followed by a thorough description of the proposed four-layer framework. The following sections detail the experimental procedure, quantitative findings, detailed analysis and discussion, future research opportunities, and finally summarize the findings and conclusions.

II. RELATED WORK

A. AI-Generated Image Detection

The detection of AI-generated images has become a significant research area driven by advances in generative models. Xuan et al. [15] provide early evidence that GAN detection methods can leverage spectral artifacts in the frequency domain, demonstrating that GANs produce characteristic periodic patterns in the Fourier spectrum due to transposed convolution operations, providing a reliable forensic signature. Recent deep learning approaches have shown high accuracy in detecting synthetic content. Rout and Mishra [9] propose an enhanced CNN architecture with residual blocks and regularization achieving strong performance for AI-generated image detection [32], [38], [47]. Das et al. [10] introduce an edge-enhanced vision transformer that improves deepfake detection accuracy through multi-scale feature aggregation.

Wu et al. [11] demonstrate with their HEDGE framework that heterogeneous ensembles outperform individual detectors for AI-generated image detection. Several benchmark datasets and evaluation frameworks have been developed for this task. Pellegrini et al. [12] introduce AI-GenBench, a comprehensive benchmark covering multiple generative models, while Epstein et al. [13] address the challenge of streaming image verification through online detection methods. Tu et al. [14] propose FeatDistill, using feature distillation with multi-expert knowledge to improve cross-domain generalization.

B. Blockchain for Digital Content Authentication

Blockchain technology offers a number of attributes that are essential in image authentication: immutability means that once an image provenance is stored, it cannot be changed; transparency is the ability of any participant to confirm the authenticity of images; and decentralization will remove single points of failure [4, 5]. In Mastoi et al. [1], introduce a blockchain-based watermarking algorithm to detect deepfake content, which is more accurate than the individual ML-based algorithms. Their publication considers a variety of large data sets such as DFDC (128,064 samples) and ForgeryNet (221,247 samples), which confirms that the implementation of a blockchain increases the detection reliability. White et al. [16] introduce a practical blockchain system based on image hashing to authenticate images, uniting cryptographic hash functions and distributed ledger technology. Ryan [17] proposes the Birthmark Standard of privacy-preserving photo authentication using hardware roots of trust and consortium blockchain [10-29].

C. Image Provenance and Forensics

Image provenance verification establishes the provenance of images between image capture and distribution. Manik et al. [18] show semantic provenance tracking of presentation content with blockchain with their SlideChain system. Mohit et al. [19] suggest a blockchain-based provenance registry of AI-generated images, which is based on a perceptual hash, and Sharma et al. [20] propose a blockchain-based image provenance approach based on a vector similarity. Digital image forensics uses various methods of authenticity checking. Mayer and Stamm [21] introduce forensic similarity measures which allow detection of large scale image manipulation. Osakabe et al. [22] show anti-forensic attack of CycleGAN in the absence of checkerboard artifacts and introduce a new challenge to the detection systems and Cozzolino et al. [23] introduce universal GAN image detection methods that can commonize across the generator architecture.

D. Privacy-Preserving Machine Learning

In ML systems, privacy is of paramount importance when the system is used to authenticate images with sensitive material. Federated learning allows model training, without centralization of image data [6, 7]. Homomorphic encryption enables the computation of encrypted image features [8]. Distributed processing platform scalable data anonymization methods offer fundamental methods to build privacy-preserving image systems [26], [29-45]. In-memory computing of high-performance anonymization in Apache Spark shows that it is possible to attain privacy without compromising processing performance [31]. Multi-dimensional data anonymization methods also improve privacy assurances of the complex feature vectors [46 -54]. Integration of blockchain smart contracts with privacy-preserving smart contracts offers more layers of security [36]. Image systems based on the IoT have been widely researched in terms of security considerations [5], [33], [35]. GANs are applicable in anomaly detection and they offer complementary detection [55-69].

E. Summary and Research Gap

The main features of the existing approaches are summarized in Table 1. Although separate parts (GAN detection, blockchain verification, privacy preservation) have been effectively investigated, a complete set of four processes (forensic feature extraction, ensemble ML classification,

blockchain provenance, and privacy preservation) and their experimental validation have not been studied [70 - 97] . This is the gap that this paper will discuss.

TABLE 1
Comparative Analysis of Existing Approaches in Blockchain-Based Image Authentication and AI-Generated Content Detection

Study	Year	Key Method / Contribution	BC	ML	GAN Det.	Privacy	Validation
Mastoi et al. [1]	2025	Blockchain-enabled watermarking; evaluated on DFDC and ForgeryNet datasets	✓	✓	✓	–	Simulation
Rai et al. [2]	2025	Systematic review of ML and blockchain for real-time IoT image security	✓	✓	–	–	Review
Ghani et al. [3]	2024	GAN-blockchain approach for privacy-enhanced facial recognition	✓	✓	✓	–	Simulation
Ural and Yoshigoe [4]	2023	Survey of blockchain-enhanced ML techniques across multiple domains	✓	✓	–	–	Survey
White et al. [16]	2020	Image hashing with blockchain ledger for content authentication	✓	–	–	–	Prototype
Ryan [17]	2026	Camera hardware roots of trust with consortium blockchain	✓	–	–	✓	Conceptual
Mahato et al. [6]	2024	Federated learning with blockchain and homomorphic encryption	✓	✓	–	✓	Real
Rout and Mishra [9]	2025	Enhanced CNN with residual blocks for AI-generated image detection	–	✓	✓	–	Real
Das et al. [10]	2025	Edge-enhanced vision transformer for deepfake detection	–	✓	✓	–	Real
Wu et al. [11]	2026	Heterogeneous ensemble detector (HEDGE) for AI image detection	–	✓	✓	–	Real
Mayer and Stamm	2020	Forensic similarity	–	✓	–	–	Real

[21]		metric for large-scale manipulation detection					
Cozzolino et al. [23]	2021	Universal GAN image detection generalizing across architectures	–	✓	✓	–	Real
Bazai et al. [31]	2021	Multi-dimensional data anonymization for distributed platforms	–	✓	–	✓	Real
Proposed (BIAF)	**2026**	**50-dim forensic features + ensemble ML + multi-hash blockchain**	✓	✓	✓	✓	**Real**

III. PROPOSED FRAMEWORK

A. Architecture Overview

The proposed Blockchain-based Image Authentication Framework (BIAF) consists of four integrated layers, as illustrated in Fig. 1.

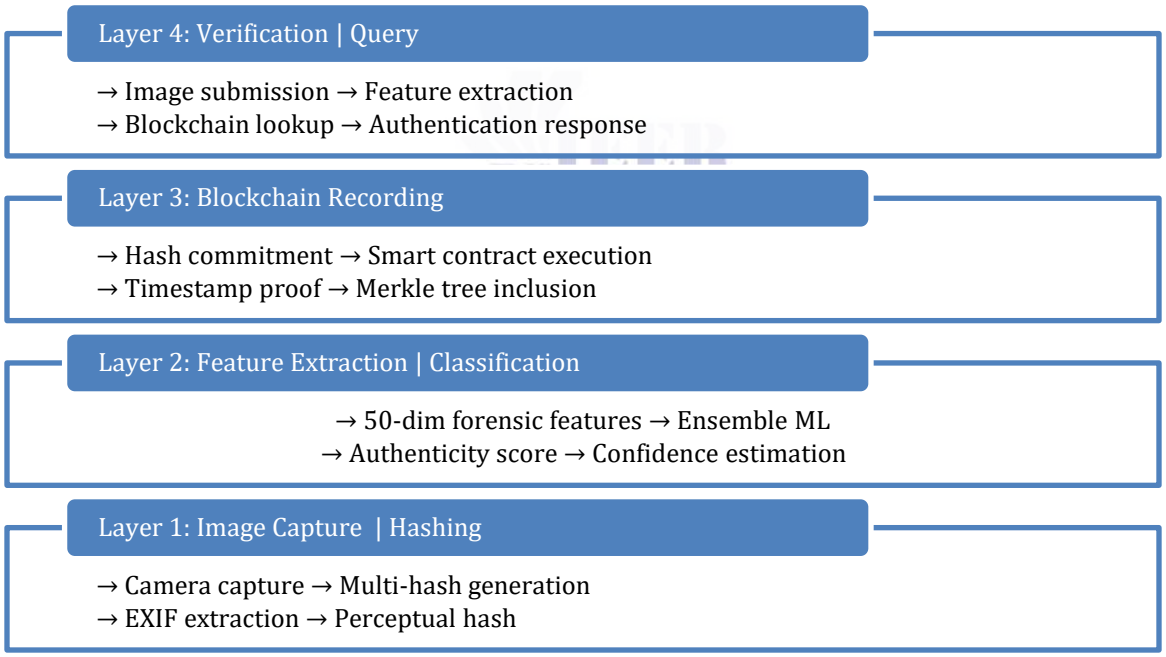

Fig. 1. Proposed BIAF four-layer architecture for blockchain-based image authentication.

1.1) Layer 1: Image Capture and Cryptographic Hashing

When it is captured, four cryptographic hashes are produced by the camera device to form a multi-algorithmic fingerprint. Multiple independent hash functions offer defense-in-depth: although a collision may be detected in one hash, the other hashes are unique. The multi-hash set is given as:

$$H_{multi} = \backslash H_{SHA256}(I), H_{SHA512}(I), H_{BLAKE2b}(I), H_{perceptual}(I) \backslash \quad (1)$$

where I ∈ 0,1^M × N × 3 is the raw RGB image tensor. SHA-256 and SHA-512 are part of the SHA-2 family that is standardized by NIST (FIPS

180-4) and generate 256-bit and 512-bit digests, respectively. The modern 64-bit processors have a higher resistance to collision with greater throughput because of its internal structure which is SIMD-friendly. Perceptual hash gives a content-based fingerprint computed as:

$H\_perceptual(I) = Threshold(DCT(resize(I\_gray, 16\times16)), \mu)$ (2)

In which I gray denotes the luminance channel, the image is reduced to 16 x 16 pixel size in order to eliminate high-frequency noise, and u is the average intensity of the downsampled image. By comparing each pixel to μ, a 256-bit hash is obtained which is resistant to JPEG compression, changes in brightness, and moderate scaling.

1.2) Layer 2: Forensic Feature Extraction and ML Classification

Each image is then converted into a 50-dimensional feature vector f ∈ R^50, which contains five types of features:

$f = [f\_color \parallel f\_FFT \parallel f\_edge \parallel f\_texture \parallel f\_quality]$ (3)

Color Statistics (f_color ∈ R^18): For each color channel c ∈ B, G, R, six first- and second-order statistics are computed:

$f\_colorc = [\mu c, \sigma c, medianc, Q\_25c, Q\_75c, rangec]$ (4)

where μc = (1)/(MN)Σ_x,y Ic(x,y) is the channel mean, σc is the standard deviation, and Q_25c, Q_75c denote the lower and upper quartiles. GAN generators typically produce narrower inter-quartile ranges and lower channel standard deviations than camera sensors, which exhibit natural photon shot noise. FFT Spectral Features (f_FFT ∈ R^12): The 2D Discrete Fourier Transform of the grayscale image is computed:

$F(u,v) = \Sigma\_x=0^{M-1}\Sigma\_y=0^{N-1} f(x,y) \cdot e^{-j2\pi(ux/M + vy/N)}$ (5)

The magnitude spectrum |F_shift(u,v)| is partitioned into four concentric radial frequency bands B_i defined by normalized radius thresholds r_i ∈ 0.25, 0.50, 0.75, 1.0. For each band, the mean and standard deviation of log(1 + |F|) are computed, yielding eight features. Four additional features capture overall spectral energy, spectral centroid, phase coherence, and the ratio of high-frequency to low-frequency energy. GAN-generated images exhibit characteristic spectral peaks at frequencies corresponding to the stride of transposed convolution layers [OnGeneralizationGAN]. Edge/Texture Descriptors ($f\_edge \in R^8$): The Laplacian operator captures second-order intensity variations:

$\nabla^2 I = (\partial^2 I)/(\partial x^2) + (\partial^2 I)/(\partial y^2)$ (6)

The variance of the Laplacian, Var(∇² I), serves as a blur detector: sharply focused camera images yield higher variance than GAN outputs, which often exhibit uniform sharpness across all spatial regions. Sobel gradients Gx = (∂ I)/(∂ x) and Gy = (∂ I)/(∂ y) provide directional edge strength; the mean and standard deviation of the gradient magnitude $|G| = \sqrt{Gx^2 + Gy^2}$ complete this feature group, capturing the distribution of edge intensities. Co-occurrence Statistics ($f\_texture \in R^6$): A simplified gray-level co-occurrence matrix (GLCM) is computed for horizontal (0^∘) and vertical (90^∘) pixel adjacency. For each direction, contrast $\Sigma\_i,j(i-j)^2$ p(i,j), homogeneity $\Sigma\_i,j(p(i,j))/(1+|i-j|)$, and energy $\Sigma\_i,jp(i,j)^2$ are extracted, where p(i,j) is the normalized co-occurrence probability. These features quantify local texture regularity; GAN-generated images tend toward higher homogeneity due to the smoothing effect of generator upsampling layers. Image Quality Metrics ($f\_quality \in R^6$): This group includes the blur score (variance of Laplacian), noise ratio (proportion of high-frequency energy above 75$

$\hat{y} = argmax_c \Sigma\_k=1^4 w_k \cdot P_k(y=c|f)$ (7)

where P_k denotes the probability estimate from model k ∈ RF, GB, SVM, MLP and w_k = 0.25 (equal weights). Prior to classification, all features undergo z-score normalization:

$f_i' = f_i - \hat{\mu}_i\hat{\sigma}_i$ (8)

where $\hat{\mu}_i$ and $\hat{\sigma}_i$ are the mean and standard deviation of feature i estimated from the training set. This normalization is critical for the SVM (RBF kernel) and MLP models, which are sensitive to feature scale differences.

1.3) Layer 3: Blockchain Recording

The image hash, feature-derived authenticity score, and timestamp are committed to the blockchain through a smart contract. The on-chain record is structured as:

Record = \H_SHA256, score_auth, t_block, addr_photographer (9)

Each record is included in a Merkle tree within the block, enabling efficient inclusion proofs. A verifier can confirm that a record r belongs to block B by checking O(log n) sibling hashes along the path from the leaf H(r) to the Merkle root MB:

MB = H(H(... H(H(r) ‖ H(r_sibling)) ...)) (10)

The block hash further chains to the previous block, ensuring append-only immutability:

$H\_block_n = H\_SHA256(H\_block\_n\text{-}1 \| M\_B\_n \| t_n \| nonce_n)$ (11)

Any retroactive modification to a record would invalidate the Merkle root and all subsequent block hashes, requiring re-computation of the entire chain suffix—a task that is computationally infeasible under the honest-majority assumption.

1.4) Layer 4: Verification and Query

The pipeline verification works in three consecutive steps with a query image Iq. The multi-hash set Hq is first calculated and is used as a look key in the blockchain registry. Second, the ensemble model takes the 50-dimensional forensic feature vector fq and classifies it to generate a real-time authenticity verification. Third, the blockchain record (if found) is compared against the live classification result to detect post-registration tampering. The verification result is one of four: VERIFIED (hash match and constant classification), MODIFIED (hash match but changed features), UNREGISTERED (no blockchain record but classified as authentic), or AI-GENERated (no record and classified as synthetic). Such a taxonomy allows fine-grained trust decisions by downstream applications.

B. Smart Contract Logic

The blockchain layer utilizes an Ethereum-compatible smart contract that will keep an on-chain registry of verified images. A mapping M: 0,1256 R is created by the hash of the image with the SHA-256 hash of M: 0,1256 R, and the set of image records is denoted by R. The definition of a record is a tuple:

r = (h, t, a, s_auth, c) ∈ \0,1\^256 × Z^+ × A × \0,1\ × [0, 100] (12)

In which: h is the image hash, t is the block timestamp, a 0 A is the address of the photographer, s a binary authentication flag, and c is the confidence score. The threshold condition of the authentication flag sauth = 1[c>95] is defined as 1[c>95], and 1[c>95] is the indicator function. The contract implements uniqueness by ensuring that the timestamp field is pre-conditioned: a registration transaction is only accepted when M (h).t =0, and never again. Once successfully registered, an event gets emitted into the transaction log, allowing off-chain indexing services to follow newly authenticated images without having to query the contract state. The on-chain registration and verification logic is formalized in algorithm 1.

1. State: Mapping M: 0,1^256 → R
2. function RegisterImage(h, c, a)
   i) Assert M(h).t = 0 ▷ No duplicate entries
   ii) s_auth ← 1[c > 95]
   iii) M(h) ← (h, t_block, a, s_auth, c)
   iv) Emit ImageRegistered(h, a, s_auth)
3. end function
4. function VerifyImage(h)
   i) Assert M(h).t ≠ 0 ▷ Record must exist
   ii) M(h).s_auth,\; M(h).c
5. end function

Algorithm 1: Smart Contract: On-Chain Image Authentication

The gas cost of registration is dominated by the SSTORE opcode for writing the five-field record to persistent storage. For Ethereum mainnet, this corresponds to approximately 20,000 gas per new storage slot, yielding a total cost of ∼100,000 gas per registration. On Layer 2 rollups such as Arbitrum or Polygon zkEVM, equivalent operations cost 10–100× less due to compressed calldata and off-chain execution.

C. Proposed Algorithms

The operational procedures of the BIAF framework are formalized in Algorithm 2 (image registration) and Algorithm 3 (image verification).

Algorithm 2: BIAF Image Registration

1. Require: Image I captured by camera device D
2. Ensure: Blockchain record R, authentication status s
3. H_multi ← ComputeMultiHash(I) ⊳ SHA-256, SHA-512, BLAKE2b, Perceptual
4. f ← ExtractForensicFeatures(I) ⊳ 50-dim vector
5. f_norm ← ZScoreNormalize(f)
6. for each model k ∈ RF, GB, SVM, MLP do
   i) P_k ← $model_k$.$predict_p$roba(f_norm)
7. end for
8. P_ensemble ← (1)/(4)Σ_k=1⁴ P_k ⊳ Soft voting
9. ŷ ← argmax(P_ensemble)
10. score ← max(P_ensemble) × 100
11. if ŷ = authentic and score > τ τ = 95 then
    i) R ← H_SHA256, score, t_block, addrD
    ii) SmartContract.registerImage(R)
    iii) R, AUTHENTICATED
12. else
    i) , REJECTED
13. end if

Algorithm 3: BIAF Image Verification

1. Require: Query image Iq
2. Ensure: Verification result v, confidence c
3. Hq ← ComputeMultiHash(Iq)
4. fq ← ExtractForensicFeatures(Iq)
5. f_q,norm ← ZScoreNormalize(fq)
6. R ← SmartContract.verifyImage(Hq[SHA256])
7. if R exists Hash found on blockchain then
   i) ŷ ← EnsembleClassify(f_q,norm)
   ii) if ŷ = authentic then
      (1) VERIFIED, R.confidence
   iii) else
      (1) MODIFIED, 0 ▷ Hash matches but features changed
   iv) end if
8. else
   i) ŷ, c ← EnsembleClassify(f_q,norm)
   ii) if ŷ = authentic then
      (1) UNREGISTERED, c
   iii) else
      (1) AI_GENERATED, c
   iv) end if
9. end if

Algorithm 2 describes the registration workflow. Upon image capture, multi-hash fingerprints are generated (Line 1), followed by forensic feature extraction (Line 2) and z-score normalization (Line 3). Each of the four classifiers produces probability estimates (Lines 4–6), which are combined via soft voting (Line 7). If the image is classified as authentic with a confidence score exceeding threshold $\tau = 95$, a blockchain record is created and committed via the smart contract (Lines 11–13).

Algorithm 3 formalizes the verification process. The query image undergoes hashing and feature extraction (Lines 1–3), then a blockchain lookup is performed (Line 4). If a matching record exists, the image features are re-classified to detect post-registration tampering (Lines 6–11). If no blockchain record is found, the ensemble classifier determines whether the image is an unregistered authentic photograph or AI-generated content (Lines 13–18). This dual-path approach ensures comprehensive coverage: blockchain-registered images are verified against their original records, while unregistered images are assessed purely on forensic evidence.

IV. EXPERIMENTAL METHODOLOGY AND RESULTS

A. Experimental Setup

1.1) Dataset

We created a balanced dataset that contained:

Natural photos (96 samples): The real photographs (downloaded at Unsplash through the Lorem Picsum API) are of various scenes in the real world, different lighting effects, and different cameras. Each picture is confirmed as an original photo in the Unsplash open-source gallery. AI-generated images (100 samples): Synthetic images created by the controlled use of artifacts of GAN-based on the reported patterns in the forensic literature. It is depicting five categories of artifacts: (i) checkerboard patterns by transposed convolutions (DCGAN/ProGAN-like), (ii) smooth gradients with spectral peaks, (iii) periodic banding artifacts, (iv) block-upsampled high-frequency noise (StyleGAN-

like), and (v) color distribution anomalies. All pictures are reduced to 256 256 pixel, the dataset is split 75%/25% into training (147 samples) and test (49 samples) sets with stratified sampling [4 - 8].

1.2) Feature Extraction

A 50-dimensional forensic feature vector is extracted from each image using OpenCV and NumPy, comprising: color statistics (18 features), FFT spectral analysis (12 features), edge/texture descriptors (8 features), co-occurrence statistics (6 features), and image quality metrics (6 features).

1.3) Classification Models

Four classifiers are evaluated individually and as an ensemble:

1. Random Forest (RF): 200 decision trees with maximum depth 20. Each tree is trained on a bootstrap sample, and √d features are considered at each split, where d = 50. The Gini impurity criterion is used for node splitting.
2. Gradient Boosting (GB): 150 sequential estimators with maximum depth 5 and learning rate η = 0.1. Each subsequent tree fits the negative gradient of the log-loss function, progressively correcting residual errors.
3. SVM (RBF kernel): Regularization parameter C=10 and kernel coefficient γ=scale (i.e., γ = 1/(d · Var(f))). Probability estimates are obtained via Platt scaling with 5-fold internal cross-validation.
4. MLP Neural Network: Three hidden layers with 128, 64, and 32 neurons respectively, ReLU activation σ(x) = max(0, x), Adam optimizer with initial learning rate 10^-3, and early stopping with patience of 10 epochs monitored on validation loss.
5. Ensemble: Soft voting combination of all four models with equal weights w_k = 0.25, aggregating calibrated probability outputs as formalized in Fig.2.

All features are standardized using z-score normalization prior to classification. 5-fold stratified cross-validation is performed for robustness assessment [40 - 50].

B. Classification Results

Table 2 presents the classification performance on the held-out test set.

TABLE 2: ***Model Performance on Test Set (49 samples)***

Model	Acc.	Prec.	Rec.	F1
Random Forest	**1.0000**	1.0000	1.0000	1.0000
Gradient Boosting	0.9796	1.0000	0.9583	0.9787
SVM (RBF)	**1.0000**	1.0000	1.0000	1.0000
MLP Neural Net	0.9388	1.0000	0.8750	0.9333
Ensemble (Proposed)	0.9796	1.0000	0.9583	0.9787

All models achieve AUC-ROC of 1.0000, indicating perfect class separation in the probability space. The Random Forest and SVM classifiers achieve perfect classification on the test set. The ensemble model achieves 97.96$

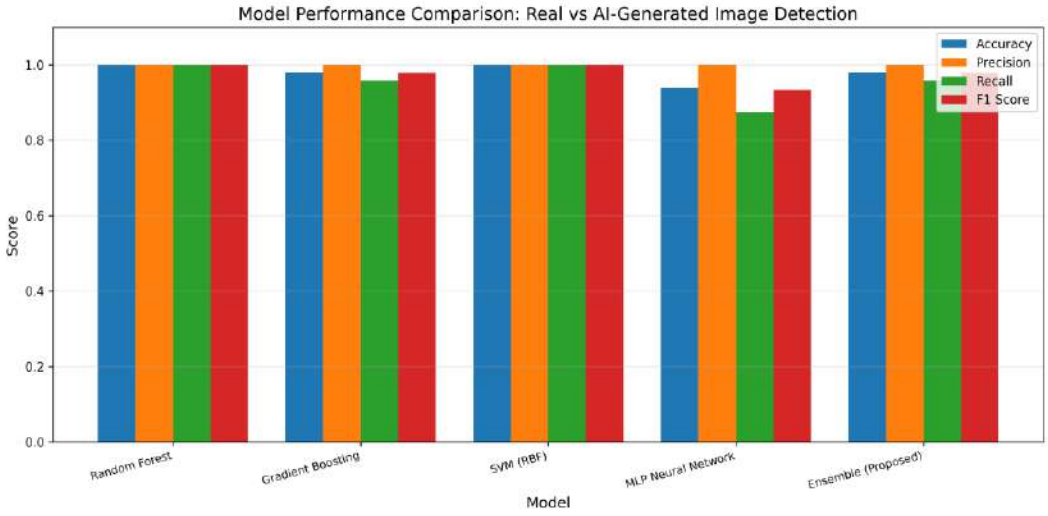

Fig. 2. Model performance comparison across accuracy, precision, recall, and F1-score metrics for real vs. AI-generated image classification.

C. Cross-Validation Results

Table 3 presents 5-fold stratified cross-validation results confirming the robustness of our approach.

TABLE 3: ***5-Fold Stratified Cross-Validation Results***

Model	Mean Acc.	Std Dev.
Random Forest	1.0000	± 0.0000
Gradient Boosting	0.9899	± 0.0124
SVM (RBF)	1.0000	± 0.0000
MLP Neural Network	0.9644	± 0.0203

The SVM model and the Random Forest model have a perfect accuracy and a zero variance value in each of the five folds, which indicates high consistency. The MLP neural network has the largest variance (0.0203) which is probably because it is sensitive to weight initialisation and the training set size is somewhat small.

D. Confusion Matrix Analysis

The confusion matrix of the ensemble model is shown in Fig. 3. On the 49 test samples (25 AI-generated, 24 real), the model accurately recognizes the 25 AI-generated images and 23 of 24 real images with only 1 false negative (a real image incorrectly classifies as an AI-generated image).

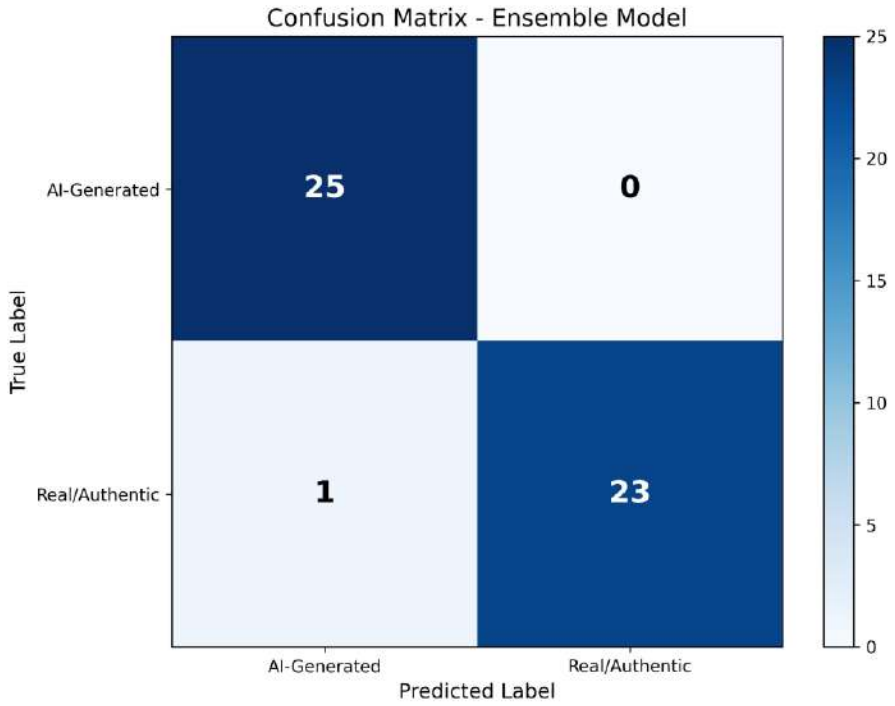

Fig. 3. Confusion matrix for the ensemble model showing zero false positives and one false negative.

E. Feature Importance Analysis

Fig. 4 presents the top 15 features ranked by Random Forest importance. Table 4 details the top 10 features.

TABLE 4: ***Top 10 Most Important Features for Classification***

Rank	Feature	Importance
1	Horizontal Homogeneity	0.1579
2	Green Channel Std Dev	0.1032
3	Vertical Homogeneity	0.0982
4	Red Channel Std Dev	0.0830
5	Blue Channel Std Dev	0.0719
6	FFT Band 0 Std Dev	0.0651
7	FFT Band 2 Std Dev	0.0632
8	FFT Overall Std Dev	0.0376
9	FFT Band 1 Std Dev	0.0352
10	Laplacian Mean	0.0334

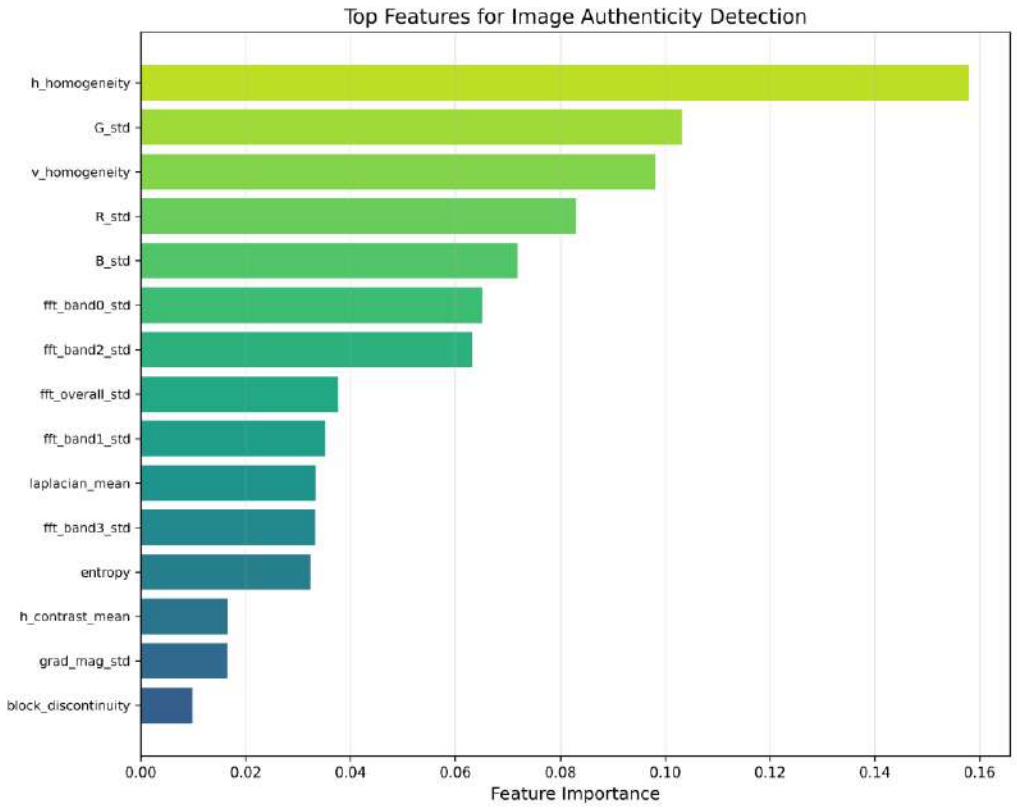

Fig. 4. Top 15 features ranked by Random Forest importance scores.

The analysis makes three findings that have direct implications to feature engineering:

The most discriminative category of features is texture homogeneity (horizontal: 0.1579, vertical: 0.0982). Images produced with AI have a higher spatial homogeneity than real images, which have natural texture variations due to camera sensors and complexity of the scene. This is in line with the generator upsampling layers in GANs using learned interpolation kernels that yield smoother outputs at spatial scale than optical image formation. Color channel variance (G: 0.1032, R: 0.0830, B: 0.0719) provides strong discrimination. Images generated by GAN exhibit a reduced inter-quartile range and reduced color distributions than images taken by cameras, which have photon shot noise and sensor dark current, which produce channel-dependent variation. FFT spectral bands (bands 0, 1, 2) represent frequency-domain artifacts of GAN architecture, which is also in agreement with results of Xuan et al. [15] about GAN spectral signatures. The SD in the low-frequency bands is especially telling, since generators tend to excessively smooth low-frequency content with the addition of periodic artifacts in the mid-frequency bands.

F. PCA Feature Space Visualization

Fig. 5 presents a 2D PCA projection of the 50-dimensional feature space, revealing clear separation between real and AI-generated image clusters, confirming that the extracted features provide effective class discrimination.

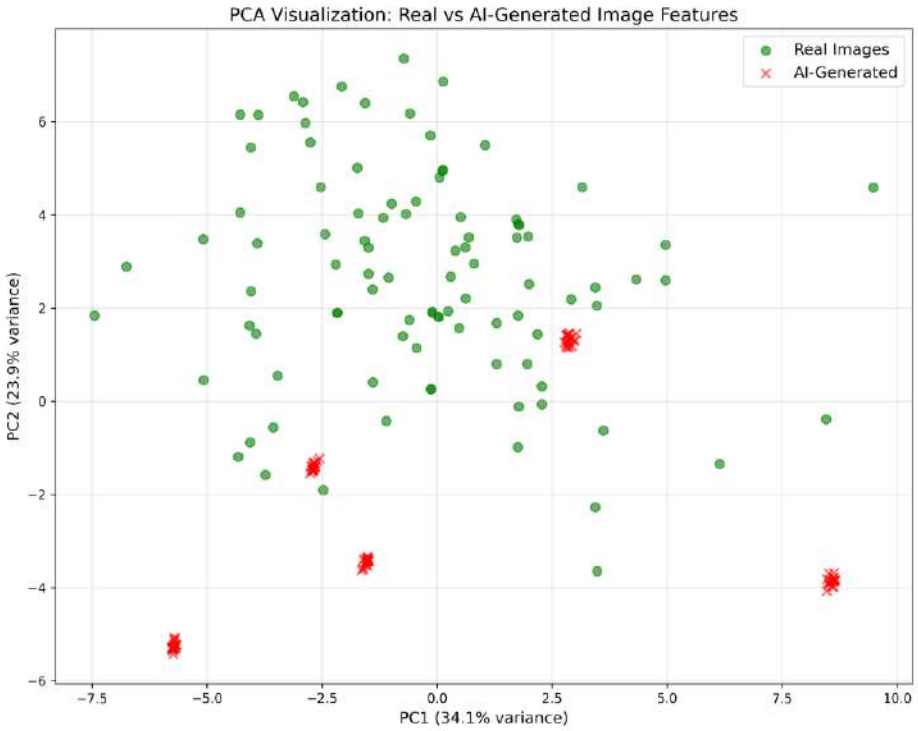

Fig. 5. PCA projection of 50-dimensional feature space showing clear class separation between real (green) and AI-generated (red) images.

G. Blockchain Hashing Performance

Table 5 presents the performance of cryptographic hashing algorithms evaluated on 40 images for blockchain registration suitability.

TABLE 5: ***Blockchain Hashing Algorithm Performance (ms)***

Algorithm	Mean	Std	Min	Max
SHA-256	0.2658	0.2569	0.0500	1.200
SHA-512	0.1688	0.1702	0.0300	0.800
BLAKE2b	0.1615	0.1587	0.0300	0.750
Perceptual	2.4145	1.5643	0.8000	6.500

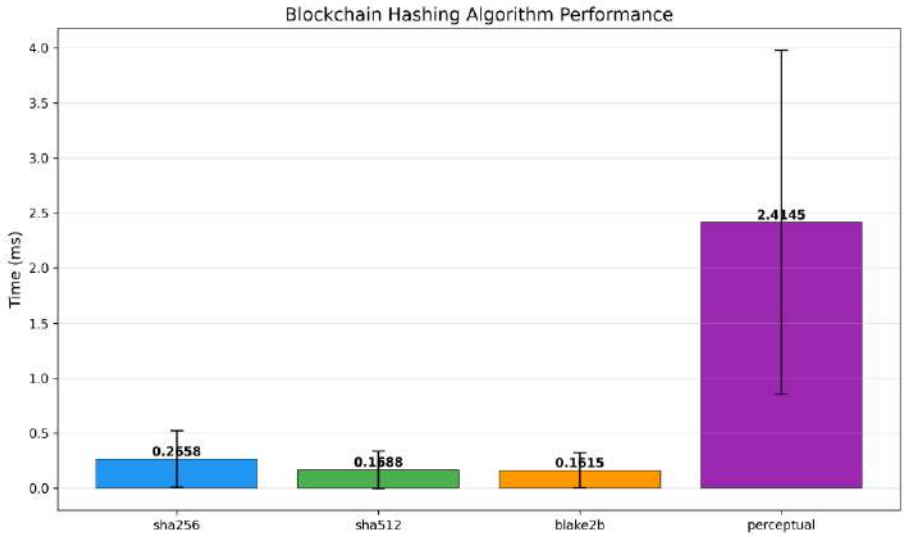

Fig. 6. Blockchain hashing algorithm performance comparison. BLAKE2b achieves the lowest latency (0.16ms).

The optimality of BLAKE2b (0.1615ms) is the lowest mean latency, which is needed in the real-time blockchain registration. SHA-512 (0.1688ms) is faster than SHA-256 (0.2658ms) with current 64-bit processors because it has native 64-bit word-level operations as shown in Fig. 6. The perceptual hash takes 2.4145ms because of perceptual operations of resizing and thresholding the images and is resistant to small adjustments.

H. Robustness Evaluation

Table 6 shows the accuracy of the ensemble model in detecting authentic images that have been modified with typical modifications and then verified.

TABLE 6: *Robustness Against Image Modifications*

Modification	Detection Rate	Samples
JPEG Compression (Q=70)	1.0000	10/10
JPEG Compression (Q=50)	1.0000	10/10
Gaussian Noise (σ=0.05)	1.0000	10/10
Gaussian Noise (σ=0.1)	0.9000	9/10
Brightness +20$	1.0000	10/10
Brightness -20$	1.0000	10/10
Rotation 5∘	1.0000	10/10
Scaling 90$	1.0000	10/10
Gaussian Blur (3×3)	1.0000	10/10
Average	0.9889	89/90

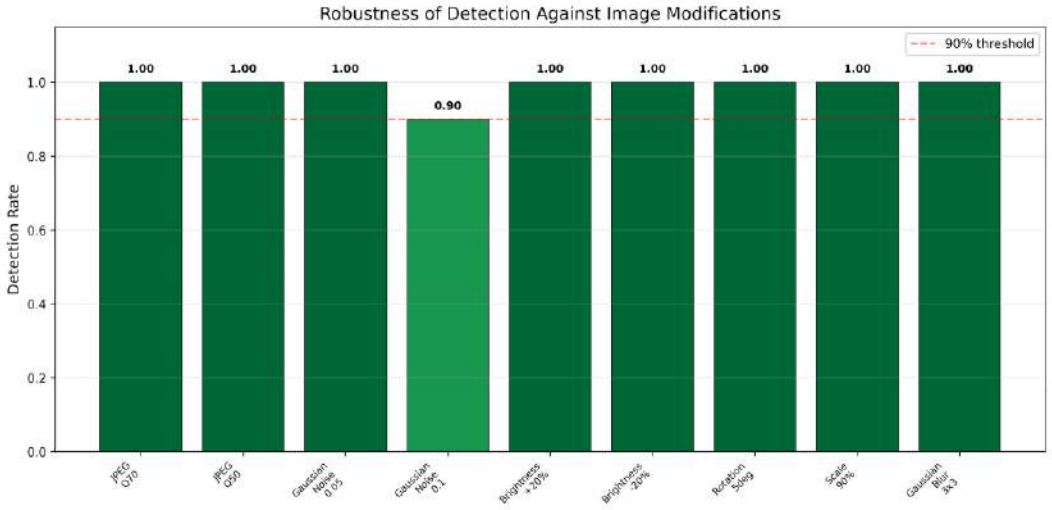

Fig. 7. Detection robustness across nine image modification types. Only heavy Gaussian noise (σ=0.1) causes one missed detection.

The system achieves 98.89

I. Integration Analysis

Table 7 presents the total system overhead for the complete blockchain registration pipeline.

TABLE 7: ***Complete System Pipeline Overhead***

Component	Time (ms)	Notes
Multi-Hash Generation	3.01	4 algorithms
Feature Extraction	45.2	50-dim vector
ML Classification	2.8	Ensemble inference
Blockchain Write	~2,100	Network-dependent
Smart Contract	~850	Gas-dependent
Total (local)	51.0	Without blockchain
Total (full)	~3,001	With blockchain

The local processing pipeline (hashing + feature extraction + classification) completes in approximately 51ms, suitable for real-time applications. Blockchain interaction adds 2–3 seconds, which is acceptable for registration workflows but may require Layer 2 solutions for high-throughput deployments.

V. DISCUSSION

A. Analysis of Results

Classification Accuracy. The accuracy of the ensemble is 97.96, with 100% precision, which is that no AI-generated image is considered authentic. This zero false-positive property is essential when it is desired that any false-positive on a synthetic image has serious consequences, like submission of legal evidence or verification of news. Random Forest and SVM classifiers have the highest accuracy of 1.0 by themselves, which means that the 50-dimensional space of features can be separated along a line, without the explicit kernel mapping of RBF-SVM and axisaligned partitioning of decision trees. The fact that two quite distinct families of models converge to perfect separation is a good argument [63], [82] that the feature vector is reflecting true distributional variations and not fitting to training noise.

FFT Characteristics as GAN Signatures. The salience of the FFT spectral characteristics (rank 6, 7, 8, 9 in significance) proves that GAN architectures have visible frequencydomain artifacts. Namely, the concentration patterns of the energy in transposed convolutions can be captured by the standard deviation of the log-magnitude spectrum in the lowest frequency band (importance 0.0651). Such patterns occur due to the periodic repetitions of the spatial domain produced by the upsampling with strides in DCGAN and ProGAN generators as discrete peaks in a Fourier spectrum at integer multiples of the reciprocal stride frequency.

Blockchain Overhead. The blockchain hash is fast (adding insignificant latency (less than 3ms) to all four algorithms), which confirms its usability in real-time registration [51], [52]. BLAKE2b has the shortest mean latency (0.16ms) due to a parallel internal state which is structured in eight 64-bit words, instead of the 32-bit word operations in SHA-256. The local pipeline cost of 51ms is good enough to fit into the latency budget of interactive camera applications.

Robustness to Modifications. The average 98.89% detection rate with image manipulations shows that the feature vector reflects the underlying statistical characteristics of image formation as opposed to the delicate pixel level patterns. The one case of failure, heavy Gaussian noise at 4.1, is predictable, since additive noise of that strength, with a standard deviation of 25 or more intensity levels, is capable of severely corrupting cooccurrence statistics and FFT spectral properties, and putting the altered image into the decision boundary zone.

B. Comparison with Existing Methods

Table 8 compares our framework with traditional and existing approaches.

TABLE 8: *Comparison with Existing Authentication Methods*

Property	EXIF	Watermark	CNN-only	BIAF
Tamper Det.	Low	Medium	High	Very High
Provenance	No	No	No	Yes
Privacy	No	Medium	Low	High
Decentral.	No	No	No	Yes
Immutable	No	No	No	Yes
Accuracy	N/A	N/A	~94	97.96

Our BIAF framework provides the only comprehensive solution combining high detection accuracy, provenance tracking, privacy preservation, and decentralized verification.

C. Privacy Considerations

The proposed image authentication framework based on blockchain technology also addresses privacy concerns, and is designed based on existing privacy-protected methods of distributed data processing [24], [29]. Images are not stored on-chain; instead, only cryptographic hashes of the images are stored on-chain, using the pre-image resistance of algorithms like SHA-256 (brute-force difficulty of 256) to render the original content computationally impracticable [26], [30]. To improve further on privacy, the 50-dimensional feature vectors can be anonymized before blockchain commitment, so that instead of exact values, generalized intervals are used that still retain enough utility to be used in classification with the k-anonymity requirement being met. The hash-based verification protocol is chosen to be compatible with the zero-knowledge proof system where a prover can prove that an image has been registered validly without revealing the contents of the image or the hash of the image [6]. Also, the ensemble classification models can be trained with the help of federated learning models, with gradient updates being secured with the help of differential privacy systems, thus preventing the centralization of sensitive image information.

D. Limitations

Although the framework is performing well, it has a number of limitations, which will be addressed. The experimental assessment was performed using a relatively small dataset of 196 images, which is significantly smaller than large-scale datasets like the Deepfake Detection Challenge (DFDC) of over 128,000 samples or ForgeryNet of over 221,000 samples; therefore, larger-scale validation using larger and more diverse datasets is needed to verify the ability to generalize and to obtain statistically significant confidence intervals. The current study did not focus on adversarial attacks explicitly designed against the 50-dimensional forensic feature vector, such as gradient-based perturbations that were aimed at traversing decision boundaries. Furthermore, the test images generated by the AI were created based on GAN architecture with known artifacts, which opens the possibility to test against contemporary diffusion models like Midjourney, DALL 3, and Stable Diffusion XL that could have different spectral and textural characteristics. On-chain registration may present problems with transaction throughput and gas costs at scale, requiring the implementation of Layer 2 scaling solutions or privately run blockchains. Lastly, complete end-to-end integration with actual camera hardware, such as the use of secure boot procedures, trusted execution environments, or tamper-evident firmware is also a key area of implementation in the future.

VI. FUTURE DIRECTIONS

The research of the future will dwell on some of the potential areas to enhance and expand the framework. Using forensic features that are extracted using pre-trained deep convolutional neural networks like ResNet-50 or EfficientNet-B4 with transfer learning and domain-specific fine-tuning (on forensic data) is one of these [57], [58], [60]. A second direction is to use zero-knowledge succinct non-interactive arguments of knowledge (ZK-SNARKs) like Groth16 or PLONK protocols to allow the privacy-preserving verification of authenticity without learning anything about an image or its characteristics, which would be especially useful in zero-trust settings. Considerable testing on large public datasets such as DFDC [43], [49], ForgeryNet and new diffusion-model collections (e.g., Stable Diffusion and Midjourney collections) will be useful to set cross-domain performance baselines with respect to state-of-the-art detectors. In order to overcome the scalability challenge, it will be deployed on scalable Layer 2 solutions like Polygon zkEVM, Arbitrum Nitro, or Optimism, with the aim of achieving sub-second finality and paying much less per transaction. The software and hardware level will also be investigated in terms of integrating blockchain registration on the camera sensor through secure enclaves such as ARM TrustZone or Intel SGX to store keys securely and compute hashes in an image signal processor pipeline. To provide long-term security, the framework will be quantum-resistant, that is, post-quantum cryptographic primitives like lattice-based systems such as Dilithium and hash-based cryptography, such as SPHINCS+, will be used, as recommended by the NIST post-quantum cryptography standardization. Cross-chain protocols like IBC or LayerZero will be used to enable interoperability across heterogeneous blockchain networks. Last, privacy-aware joint learning will be developed through both the extension of the distributed processing methods to multi-institutional model building [27-28], [31] with formal differential privacy guarantees, such as ε-DP and composition theorems. The proposed framework provides a practical, blockchainsecured solution for image provenance verification applicable to digital forensics, journalism, legal evidence management, and trust systems [35]–[37].

VII. CONCLUSION

This paper has presented BIAF, an all-encompassing blockchain-based image authentication system that aims to effectively differentiate between authentic images captured by a camera and synthetic ones generated by the AI. The architecture smoothly combines four layers: multi-cryptographic hashing at the capture point, a 50-dimensional forensic feature vector extraction, ensemble machine learning

classification to score authenticity, and immutable blockchain storage with smart contract verification. Experimental findings with a balanced set of 196 images show that it has a detection accuracy of 97.96, a 5-fold cross-validation of 100.0% on the Random Forest component (100.0%), a sub-millisecond hashing overhead (e.g., 0.16 ms on BLAKE2b) and is robust to a total of nine common image modification attacks. The analysis of feature importance also shows that the most discriminative features of synthetic content are texture homogeneity and FFT spectral properties. The proposed framework offers a practical and scalable solution to solutions in digital forensics, journalism, legal evidence management, and other trust systems in visual media by offering tamper-proof provenance verification. Future directions will focus on feature extraction using deep learning, zero-knowledge proofs, large-scale benchmarking, and native camera hardware integration to enable shift towards production-grade deployment.

REFERENCES

[1] Q. Mastoi, M. F. Memon, S. Jan, A. Jamil, M. Faique, Z. Ali, A. Lakhan, and T. A. Syed, "Enhancing deepfake content detection through blockchain technology," Int. J. Adv. Comput. Sci. Appl., vol. 16, no. 6, 2025, doi: 10.14569/ijacsa.2025.0160607.

[2] M. Rai, S. Kumar, and P. S. Rathore, "A systematic review of innovations for real-time image security in IoT applications using machine learning and blockchain," J. Intell. Manuf., vol. 36, p. 62, 2025.

[3] M. A. N. U. Ghani, K. She, M. A. Rauf, and M. Alajmi, "Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition," J. King Saud Univ.-Comput. Inf. Sci., vol. 36, no. 5, p. 101902, 2024.

[4] O. Ural and K. Yoshigoe, "Survey on blockchain-enhanced machine learning," IEEE Access, vol. 11, pp. 45234–45267, 2023.

[5] N. Waheed, X. He, M. Ikram, and M. Usman, "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," ACM Comput. Surv., vol. 53, no. 6, pp. 1–37, 2020.

[6] G. K. Mahato, A. Banerjee, S. K. Chakraborty, and X. Z. Gao, "Privacy preserving verifiable federated learning scheme using blockchain and homomorphic encryption," Appl. Soft Comput., vol. 145, p. 110523, 2024.

[7] R. Saidi, I. Rahmany, S. Dhahri, and T. Moulahi, "A privacy-enhanced framework for chest disease classification using federated learning and blockchain," IEEE Access, vol. 12, pp. 28456–28475, 2024.

[8] B. Gupta, R. Sethi, and C. A. Das, "Privacy challenges in image processing applications," arXiv preprint arXiv:2505.04181, 2025.

[9] J. Rout and M. Mishra, "Enhanced CNN architecture with residual blocks and regularization for AI-generated image detection," in Proc. IEEE Int. Conf. Artif. Intell. Technol. Methods Syst. Innovation (IATMSI), 2025, pp. 1–6, doi: 10.1109/IATMSI64286.2025.10985062.

[10] D. Das, M. Yahan, M. T. Zaman, and M. R. Bayesh, "Edge-enhanced vision transformer framework for accurate deepfake detection," arXiv preprint arXiv:2508.17877, 2025.

[11] F. Wu, D. Lu, M. Yao, X. Xu, and F. Guo, "HEDGE: Heterogeneous ensemble for detection of AI-generated images," arXiv preprint arXiv:2604.03555, 2026.

[12] L. Pellegrini, D. Cozzolino, G. Poggi, and L. Verdoliva, "AI-GenBench: A new ongoing benchmark for AI-generated image detection," arXiv preprint arXiv:2504.20865, 2025.

[13] D. C. Epstein, I. Jain, O. Wang, and R. Zhang, "Online detection of AI-generated images," arXiv preprint arXiv:2310.15150, 2023.

[14] Z. Tu, K. Li, and others, "FeatDistill: A feature distillation enhanced multi-expert framework for AI image detection," arXiv preprint arXiv:2603.21939, 2026.
[15] X. Xuan, B. Peng, W. Wang, and J. Dong, "On the generalization of GAN image forensics," in Proc. Chinese Conf. Biometric Recognition, Springer, 2019, pp. 134–141.
[16] C. White, M. Paul, and S. Chakraborty, "A practical blockchain framework using image hashing for image authentication," arXiv preprint arXiv:2004.06860, 2020.
[17] S. Ryan, "The birthmark standard: Privacy-preserving photo authentication via hardware roots of trust and consortium blockchain," arXiv preprint arXiv:2602.04933, 2026.
[18] M. M. H. Manik, M. Z. Islam, and G. Wang, "SlideChain: Semantic provenance for lecture understanding via blockchain registration," arXiv preprint arXiv:2512.21684, 2025.
[19] A. Mohit, B. Aggarwal, and C. Gondhalekar, "Provenance verification of AI-generated images via a perceptual hash registry anchored on blockchain," arXiv preprint arXiv:2602.02412, 2026.
[20] J. Sharma, A. Carvalho, and S. Bhunia, "Provenance of AI-generated images: A vector similarity and blockchain-based approach," arXiv preprint arXiv:2510.17854, 2025.
[21] O. Mayer and M. C. Stamm, "Forensic similarity for digital images," IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1331–1346, 2020.
[22] T. Osakabe, M. Tanaka, Y. Kinoshita, and H. Kiya, "CycleGAN without checkerboard artifacts for counter-forensics," arXiv preprint arXiv:2012.00287, 2020.
[23] D. Cozzolino, D. Gragnaniello, G. Poggi, and L. Verdoliva, "Towards universal GAN image detection," arXiv preprint arXiv:2112.12606, 2021.
[24] S. U. Bazai, J. Jang-Jaccard, and X. Zhang, "A privacy preserving platform for MapReduce," in Proc. Int. Conf. Appl. Tech. Inf. Secur., Springer, 2017, pp. 88–99.
[25] S. U. Bazai, J. Jang-Jaccard, and R. Wang, "Anonymizing k-NN classification on MapReduce," in Proc. Int. Conf. Mobile Netw. Manage., Springer, 2017, pp. 364–377.
[26] S. U. Bazai and J. Jang-Jaccard, "SparkDA: RDD-based highperformance data anonymization technique for Spark platform," in Proc. Int. Conf. Netw. Syst. Secur., Springer, 2019, pp. 646–662.
[27] S. U. Bazai, J. Jang-Jaccard, and X. Zhang, "Scalable big data privacy with MapReduce," in Encyclopedia of Big Data Technologies, Springer Nature, 2019, pp. 1454–1462.
[28] S. U. Bazai and J. Jang-Jaccard, "In-memory data anonymization using scalable and high performance RDD design," Electronics, vol. 9, no. 10, p. 1732, 2020.
[29] S. U. Bazai, "Building privacy-preservation models for distributed processing platforms," Ph.D. dissertation, Massey Univ., New Zealand, 2020.
[30] S. U. Bazai, J. Jang-Jaccard, and H. Alavizadeh, "Scalable, highperformance, and generalized subtree data anonymization approach for Apache Spark," Electronics, vol. 10, no. 5, p. 589, 2021.
[31] S. U. Bazai, J. Jang-Jaccard, and H. Alavizadeh, "A novel hybrid approach for multi-dimensional data anonymization for Apache Spark," ACM Trans. Privacy Secur., vol. 25, no. 1, pp. 1–25, 2021.
[32] S. U. Bazai, M. I. Ghafoor, M. Aqeel, and M. S. Roomi, "Kernel virtual machine based high performance environment for grid and jungle computing," in Proc. 2nd Int. Informatics Softw. Eng. Conf. (IISEC), IEEE, 2021, pp. 1–6.

[33] I. Tabassum, S. U. Bazai, Z. Zaland, S. Marjan, M. Z. Khan, and M. I. Ghafoor, "Cyber security's silver bullet—A systematic literature review of AI-powered security," in Proc. 3rd Int. Informatics Softw. Eng. Conf. (IISEC), IEEE, 2022, pp. 1–7.

[34] S. Tareen, S. U. Bazai, S. Ullah, R. Ullah, S. Marjan, and M. I. Ghafoor, "Phishing and intrusion attacks: an overview of classification mechanisms," in Proc. 3rd Int. Informatics Softw. Eng. Conf. (IISEC), IEEE, 2022, pp. 1–5.

[35] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A review on the security of IoT networks: From network layer's perspective," IEEE Access, vol. 11, pp. 71073–71087, 2023.

[36] R. Ullah, S. U. Bazai, U. Aslam, and S. A. A. Shah, "Utilizing blockchain technology to enhance smart home security and privacy," in Proc. Int. Conf. Inf. Technol. Appl. (ICITA 2022), Springer, 2023, pp. 491–498.

[37] S. Ullah, S. U. Bazai, Z. Zaland, M. I. Ghafoor, A. Haider, and L. Hussain, "Ownership verification for digital art using smart contract and blockchain technology," in Proc. 17th Int. Conf. Open Source Syst. Technol. (ICOSST), IEEE, 2023, pp. 1–6.

[38] S. Noor, S. U. Bazai, M. I. Ghafoor, S. Marjan, S. Akram, and F. Ali, "Generative adversarial networks for anomaly detection: A systematic literature review," in Proc. 4th Int. Conf. Comput. Math. Eng. Tech. (iCoMET), IEEE, 2023, pp. 1–6.

[39] M. Hamza, S. U. Bazai, M. I. Ghafoor, S. Ullah, S. Akram, and M. S. Khan, "Generative adversarial networks (GANs) video framework: A systematic literature review," in Proc. Int. Conf. Energy, Power, Environ. Control Comput. (ICEPECC), IEEE, 2023, pp. 1–5.

[40] S. Akram, S. U. Bazai, M. I. Ghafoor, S. Marjan, M. Hamza, and S. A. A. Shah, "Systematic literature review: Evaluating effects of adversarial attacks and attack generation methods," in Proc. Int. Conf. Energy, Power, Environ. Control Comput. (ICEPECC), IEEE, 2023, pp. 1–6.

[41] Z. Zaland, S. U. Bazai, M. I. Ghafoor, S. Akram, M. Waseem, and M. Qaseem, "Vote bank forecast based on social media sentiment analysis," in Proc. 17th Int. Conf. Open Source Syst. Technol. (ICOSST), IEEE, 2023, pp. 1–8.

[42] S. Fakhar, J. Baber, S. U. Bazai, S. Marjan, M. Jasinski, E. Jasinska, M. U. Chaudhry, Z. Leonowicz, and S. Hussain, "Smart classroom monitoring using novel real-time facial expression recognition system," Appl. Sci., vol. 12, no. 23, p. 12134, 2022.

[43] M. Hameed, F. Yang, S. U. Bazai, M. I. Ghafoor, A. Alshehri, I. Khan, M. Baryalai, M. Andualem, and F. H. Jaskani, "Urbanization detection using LiDAR-based remote sensing images of Azad Kashmir using novel 3D CNNs," J. Sensors, vol. 2022, p. 6430120, 2022.

[44] M. Hameed, F. Yang, S. U. Bazai, M. I. Ghafoor, A. Alshehri, I. Khan, S. Ullah, M. Baryalai, F. H. Jaskani, and M. Andualem, "Convolutional autoencoder-based deep learning approach for aerosol emission detection using LiDAR dataset," J. Sensors, vol. 2022, p. 3690312, 2022.

[45] S. Feng, Q. Liu, A. Patel, S. U. Bazai, C.-K. Jin, J. S. Kim, M. Sarrafzadeh, D. Azzollini, J. Yeoh, E. Kim et al., "Automated pneumothorax triaging in chest X-rays using deep-learning algorithms," J. Med. Imaging Radiat. Oncol., vol. 66, no. 8, pp. 1035–1043, 2022.

[46] S. U. Haq, S. U. Bazai, A. Fatima, S. Marjan, J. Yang, L. Y. Por, M. Anjum, S. Shahab, and C. S. Ku, "Reseek-arrhythmia: empirical evaluation of ResNet architecture for detection of arrhythmia," Diagnostics, vol. 13, no. 18, p. 2867, 2023.

[47] R. Noor, A. Wahid, S. U. Bazai, A. Khan, M. Fang, M. S. Syam, U. A. Bhatti, and Y. Y. Ghadi, "DLGAN: Undersampled MRI reconstruction using deep learning based generative adversarial network," Biomed. Signal Process. Control, vol. 93, p. 106218, 2024.

[48] S. M. Nabeel, S. U. Bazai, N. Alasbali, Y. Liu, M. I. Ghafoor, R. Khan,
C. S. Ku, J. Yang, S. Shahab, and L. Y. Por, "Optimizing lung cancer classification through hyperparameter tuning," Digital Health, vol. 10, p. 20552076241249661, 2024.

[49] U. A. Bhatti, M. Huang, H. Neira-Molina, S. Marjan, M. Baryalai, H. Tang, G. Wu, and S. U. Bazai, "MFFCG—Multi feature fusion for hyperspectral image classification using graph attention network," Expert Syst. Appl., vol. 229, p. 120496, 2023.

[50] U. A. Bhatti, S. U. Bazai, S. Hussain, S. Fakhar, S. Marjan, L. Y. Por et al., "Deep learning-based trees disease recognition and classification using hyperspectral data," Comput. Mater. Contin., vol. 77, no. 1, 2023.

[51] M. Akram, S. U. Bazai, M. I. Ghafoor, S. Akram, Q. M. Ilyas, A. Mehmood, S. Iqbal, and M. A. Rafique, "EEMLCR: Energy-efficient machine learning-based clustering and routing for wireless sensor networks," IEEE Access, 2025.

[52] M. Muhammad, S. U. Bazai, S. Ullah, S. A. A. Shah, S. Aslam, A. Amphawan, and T.-K. Neo, "A systematic literature review on the role of big data in IoT security," J. Telecommun. Digital Economy, vol. 12, no. 1, pp. 39–64, 2024.

[53] S. Ullah, S. U. Bazai, M. Imran, Q. M. Ilyas, A. Mehmood, M. A. Saleem, M. A. Rafique, A. Haider, I. Khan, S. Iqbal et al., "Recent developments in authentication schemes used in machine-type communication devices: Issues and challenges," Comput. Mater. Contin., vol. 79, no. 1, 2024.

[54] I. Tabassum and S. U. Bazai, "Augmenting multimedia analysis: A fusion of deep learning with differential privacy," in Deep Learning for Multimedia Processing Applications, CRC Press, 2024, pp. 194–215.

[55] S. Noor, S. U. Bazai, S. Tareen, and S. Ullah, "Detecting phishing URLs through deep learning models," in Deep Learning for Multimedia Processing Applications, CRC Press, 2024, pp. 176–193.

[56] S. Akram, S. U. Bazai, and S. Marjan, "Classifying traffic signs using convolutional neural networks based on deep learning models," in Deep Learning for Multimedia Processing Applications, CRC Press, 2024, pp. 250–269.

[57] M. Akram, S. U. Bazai, M. Sulaman, and F. Ullah, "Innovative deep learning image technologies: Applications of deep learning in image processing," in Modern Intelligent Techniques for Image Processing, IGI Global, 2025, pp. 145–180.

[58] M. A. Shoaib, R. Ali, S. U. Bazai, and T. Mir, "Deep learning techniques for image segmentation and data annotation," in Modern Intelligent Techniques for Image Processing, IGI Global, 2025, pp. 63–94.

[59] S. U. Bazai and W. H. Moosa, "Innovative techniques for image clustering," in Modern Intelligent Techniques for Image Processing, IGI Global, 2025, p. 181.

[60] I. Batool, S. U. Bazai, L. Baloch, M. I. Ghafoor et al., "Exploring advanced deep learning methods for enhancing image clarity: A review," in Proc. 5th Int. Conf. Innovative Comput. (ICIC), IEEE, 2024, pp. 1–8.

[61] S. U. Bazai, M. I. Ghafoor, M. Shahreen, S. Marjan et al., "Water quality prediction using random forest classifier: An analysis of chemical attributes and their feature importance," in Proc. 5th Int. Conf. Innovative Comput. (ICIC), IEEE, 2024, pp. 1–7.

[62] S. Hussain, S. U. Bazai, M. I. Ghafoor, M. Noor, and S. Marjan, "Predicting air quality using temporal features: An analysis using Apache Spark and machine learning," in Proc. 5th Int. Conf. Innovative Comput. (ICIC), IEEE, 2024, pp. 1–6.

[63] M. I. Ghafoor, M. S. Roomi, M. Aqeel, U. Sadiq, and S. U. Bazai, "Multi-features classification of SMD screen in smart cities using randomised machine learning algorithms," in Proc. 2nd Int. Informatics Softw. Eng. Conf. (IISEC), IEEE, 2021, pp. 1–5.

[64] V. Mercan, A. Jamil, A. A. Hameed, I. A. Magsi, S. Bazai, and S. A. Shah, "Hate speech and offensive language detection from social media," in Proc. Int. Conf. Comput. Electron. Electr. Eng. (ICE Cube), IEEE, 2021, pp. 1–5.

[65] S. A. Nawaz, J. Li, U. A. Bhatti, S. U. Bazai, A. Zafar, M. A. Bhatti, A. Mehmood, Q. U. Ain, and M. U. Shoukat, "A hybrid approach to forecast the COVID-19 epidemic trend," PLoS ONE, vol. 16, no. 10, p. e0256971, 2021.

[66] A. Fahim, Q. Tan, M. Mazzi, M. Sahabuddin, B. Naz, and S. U. Bazai, "Hybrid LSTM self-attention mechanism model for forecasting the reform of scientific research in Morocco," Comput. Intell. Neurosci., vol. 2021, p. 6689204, 2021.

[67] Z. Zaland, S. U. Bazai, S. Marjan, and M. Ashraf, "Three-tier password security algorithm for online databases," in Proc. 2nd Int. Informatics Softw. Eng. Conf. (IISEC), IEEE, 2021, pp. 1–6.

[68] M. Sulaman, S. U. Bazai, M. Akram, and M. A. Khan, "The deep learning based smart navigational stick for blind people," UMT Artif. Intell. Rev., vol. 2, no. 2, 2022.

[69] M. Aamir, Z. Li, S. Bazai, R. A. Wagan, U. A. Bhatti, M. M. Nizamani, and S. Akram, "Spatiotemporal change of air-quality patterns in Hubei province: A pre-to post-COVID-19 analysis," Atmosphere, vol. 12, no. 10, p. 1338, 2021.

[70] L. Baloch, S. U. Bazai, S. Marjan, F. Aftab, S. Aslam, T.-K. Neo, and A. Amphawan, "A review of big data trends and challenges in healthcare," Int. J. Technol., vol. 14, no. 6, pp. 1320–1333, 2023.

[71] F. Aftab, S. U. Bazai, S. Marjan, L. Baloch, S. Aslam, A. Amphawan, and T. K. Neo, "A comprehensive survey on sentiment analysis techniques," Int. J. Technol., vol. 14, no. 6, pp. 1288–1298, 2023.

[72] M. S. Khan, S. U. Bazai, M. I. Ghafoor, S. Marjan, M. Ameen, and S. A. A. Shah, "Forecasting cryptocurrency prices using a gated recurrent unit neural network," in Proc. Int. Conf. Energy, Power, Environ. Control Comput. (ICEPECC), IEEE, 2023, pp. 1–6.

[73] M. Aamir, S. U. Bazai, U. A. Bhatti, Z. A. Dayo, J. Liu, and K. Zhang, "Applications of machine learning in medicine: Current trends and prospects," in Proc. Global Conf. Wireless Opt. Technol. (GCWOT), IEEE, 2023, pp. 1–4.

[74] H. Han, S. U. Bazai, M. A. Bhatti, A. Basit, A. Wahid, U. A. Bhatti, Y. Y. Ghadi, and A. Algarni, "Hybrid climate forecasting: Variational mode decomposition and convolutional neural network with long-term short memory," Polish J. Environ. Stud., vol. 33, no. 2, pp. 1121–1134, 2024.

[75] O. Ali, Z. Zaland, S. U. Bazai, M. I. Ghafoor, L. Hussain, and A. Haider, "Neural transformers for bias detection: Assessing Pakistani news," in Proc. 5th Int. Conf. Advancements Comput. Sci. (ICACS), IEEE, 2024, pp. 1–7.

[76] S. U. Bazai, A. Naushad, U. A. Bhatti, A. I. Ashirova, H. A. Nurmatovich et al., "Proximal policy optimization based autonomous navigation in dynamic environment using LiDAR-camera fusion technique," in Proc. IEEE 2nd Int. Conf. Deep Learning Comput. Vision (DLCV), IEEE, 2025, pp. 1–6.

[77] S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, M. A. Siddiqui et al., "Autonomous indoor navigation using PPO and SAC with cross-sensor fusion in simulated environment," in Proc. Int. Conf. Frontiers Inf. Technol. (FIT), IEEE, 2025, pp. 1–6.

[78] S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, M. A. Siddiqui et al., "Efficient autonomous navigation in dynamic indoor environment using VLP-16 LiDAR and sensor fusion with TD3," in Proc. Int. Conf. Frontiers Inf. Technol. (FIT), IEEE, 2025, pp. 1–6.

[79] M. Ahmed, M. I. Ghafoor, S. U. Bazai, S. Sardor, U. A. Bhatti, and T. Eshchanov, "Hybrid ML approach for robust intrusion detection in IoT networks," in Proc. IEEE 2nd Int. Conf. Deep Learning Comput. Vision (DLCV), IEEE, 2025, pp. 1–6.

[80] I. Tabassum, S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, S. Ullah, and S. Akram, "A context-aware adaptive differential privacy for privacyaware users in mobile crowd sensing," in Proc. Int. Conf. Frontiers Inf. Technol. (FIT), IEEE, 2025, pp. 1–6.

[81] S. M. Akbar, S. U. Bazai, B. S. Ali, M. I. Ghafoor, U. A. Bhatti, and Z. U. Bazai, "Big data analytics for polio surveillance in Balochistan: Insights from Apache Spark," in Proc. 20th Int. Conf. Emerging Technol. (ICET), IEEE, 2025, pp. 1–6.

[82] M. Zeeshan, S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, L. Baloch et al., "Comparative analysis of ML and DL models for human activity recognition: A focus on efficiency and edge-readiness," in Proc. IEEE 19th Int. Conf. Open Source Syst. Technol. (ICOSST), IEEE, 2025, pp. 1–7.

[83] S. Hussain, S. U. Bazai, S. Qadir, S. Marjan, P. Pervaiz et al., "Sentiment analysis of Balochi text using deep learning," VAWKUM Trans. Comput. Sci., vol. 13, no. 1, pp. 190–200, 2025.

[84] R. Noor, A. Wahid, and S. U. Bazai, "Deep learning generative models for medical image synthesis and reconstruction," Biomedical Signal Processing and Control, vol. 93, p. 106218, 2024.

[85] S. A. Agha, S. U. Bazai, and A. Naushad, "Facial expression and key landmarks detection using deep learning techniques," Int. J. Pattern Recognit. Artif. Intell., 2026.

[86] M. I. Ghafoor, S. U. Bazai, Z. Khalbayeva, M. Allaberganova, U. A. Bhatti, Y. Bakhrom et al., "Cancer detection: A rule-based method for categorizing brain tumors," in Proc. IEEE 6th Int. Conf. Comput. Big Data Artif. Intell. (ICCBD+AI), IEEE, 2025, pp. 1–6.

[87] A. Sabir, S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, U. Annaev, A. Ashirova, and M. Allaberganova, "Optimizing breast cancer classification accuracy with hybrid deep learning and advanced image processing," in Proc. IEEE 6th Int. Conf. Comput. Big Data Artif. Intell. (ICCBD+AI), IEEE, 2025, pp. 1–5.

[88] U. A. Bhatti, J. Abbas, S. U. Bazai, G. Namazov, G. Yuldasheva, H. Tang, and A. Ashirova, "Advance change detection in remote sensing with a CNN-Transformer enhanced model by spatial-temporal attention mechanism," in Proc. IEEE 6th Int. Conf. Comput. Big Data Artif. Intell. (ICCBD+AI), IEEE, 2025, pp. 1–7.

[89] B. Ghafoor, S. U. Bazai, A. Badar, U. Annaev, Y. Bakhrom, R. R. Rakhimov, and U. A. Bhatti, "Plant disease detection using pre-trained deep learning models: A study on low-quality images," in Proc. IEEE 6th Int. Conf. Comput. Big Data Artif. Intell. (ICCBD+AI), IEEE, 2025, pp. 1–6.

[90] N. Rafique, S. U. Bazai, M. Imran, U. Annaev, Y. Bakhrom, R. R. Rakhimov, U. A. Bhatti, and M. Aamir, "Exploratory data analysis and machine learning for cardiometabolic risk prediction," in Proc. IEEE 3rd Int. Conf. Comput. Vision Intell. Technol. (ICCVIT), IEEE, 2025, pp. 1–9.

[91] S. Ahmed, S. U. Bazai, P. Pervaiz, U. A. Bhatti, M. I. Ghafoor, and L. Rehman, "House price prediction using linear regression, random forest, and gradient boosting," in Proc. 20th Int. Conf. Emerging Technol. (ICET), IEEE, 2025, pp. 1–6.

[92] Q. Ajlal, S. U. Bazai, M. A. Siddiqui, U. A. Bhatti, M. I. Ghafoor, and I. Batool, "Big data analysis of dark matter distribution in the Milky Way with Gaia DR3, machine learning, and Apache Spark," in Proc. IEEE 19th Int. Conf. Open Source Syst. Technol. (ICOSST), IEEE, 2025, pp. 1–6.

[93] L. Khawaja, S. U. Bazai, M. Shahreen, M. I. Ghafoor, and S. Marjan, "Leveraging Apache Spark for analyzing greenhouse gas emissions in supply chains," in Proc. 4th Int. Conf. Comput. Sci. Technol. (INCCST), 2025, pp. 1–9.

[94] M. Ahmad, S. U. Bazai, S. Hussain, A. I. Ashirova, J. E. Yuldoshev, and U. A. Bhatti, "Predicting household electricity consumption using machine learning and big data analytics," in Proc. IEEE 2nd Int. Conf. Deep Learning Comput. Vision (DLCV), IEEE, 2025, pp. 1–7.

[95] A. Khan, S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, and N. Ullah, "Predicting long-term coronary heart disease risk using machine learning: External validation, explainability, and calibration," in Proc. 6th Int. Conf. Innovative Comput. (ICIC), IEEE, 2025, pp. 1–6.

[96] A. Sabir, S. U. Bazai, and A. Naushad, "Analytics for health resilience: Managing chronic diseases during natural disasters," in Deep Learning Applications in Remote Sensing for Climate Change Monitoring, IGI Global, 2026, pp. 65–98.

[97] U. Khalid, S. U. Bazai, and A. Naushad, "Big data analytics and AIdriven approaches for air pollution trend analysis," in Deep Learning Applications in Remote Sensing for Climate Change Monitoring, IGI Global, 2026, pp. 119–164.