

RESEARCH ARTICLE

Federated Multi-Modal Visual Forensics with Blockchain for Tamper-Proof Image Verification

N. Santhiyakumari *, S. Sabarinathan, S. Veerakumar, M. Chandraman, G. Kiruthika

ABSTRACT: With the surge of manipulated media and deepfakes, ensuring the authenticity and integrity of digital images has become a critical challenge. This paper introduces a novel Federated Multi-Modal Visual Forensics (FMVF) framework integrated with Blockchain technology for secure, decentralized, and tamper-proof image verification. The proposed system utilizes multi-modal inputs, such as metadata, pixel-level artifacts, and compression signatures, processed through a federated deep learning architecture that preserves data privacy while collaboratively training robust forensic models across distributed nodes. To ensure auditability and trust, blockchain is employed to record hash signatures of both original and processed images, enabling immutable traceability and provenance tracking. Furthermore, a hybrid attention mechanism is incorporated to enhance anomaly localization and manipulation detection. Experimental results on multiple forensic datasets demonstrate superior performance in tamper detection, robustness against adversarial attacks, and high integrity assurance. The integration of federated learning with blockchain sets a new standard for privacy-aware, trustworthy digital media authentication.

Keywords: Visual Forensics, Federated Learning, Blockchain; Image Tampering Detection, Deepfake Detection, Multi-Modal Analysis, Privacy-Preserving AI.

Received: 27 January 2025; Revised: 16 March 2025; Accepted: 14 June 2025; Published Online: 05 July 2025

1. INTRODUCTION

The widespread proliferation of manipulated visual content, particularly deepfakes and tampered images, poses a severe threat to the authenticity and reliability of digital media. Social platforms, political arenas, and judicial systems have witnessed the consequences of such forgeries, which erode public trust and compromise decision-making processes [1]. The rapid advancement in generative models such as GANs (Generative Adversarial Networks) has made it increasingly difficult to distinguish between genuine and manipulated images using traditional forensic techniques [2]. As a result, researchers are focusing on developing more robust and adaptive visual forensics models that can detect subtle anomalies embedded in image artifacts.

Conventional centralized forensics systems typically

involve collecting all training data on a central server, raising significant privacy concerns, especially in sensitive domains like law enforcement and journalism [3]. To mitigate this, federated learning (FL) has emerged as a powerful paradigm that enables collaborative training of machine learning models across distributed clients without exchanging raw data [4]. FL facilitates data privacy and compliance with regulations such as GDPR while allowing edge devices to participate in model improvement. However, federated approaches still face challenges related to trustworthiness and secure data provenance during training and inference. To address these limitations, blockchain technology has been introduced as a decentralized ledger that offers immutability, transparency, and verifiability of digital transactions [5]. In the context of visual forensics, blockchain can be employed to store cryptographic hashes of images and their forensic fingerprints, ensuring tamper-evident traceability and origin verification [6]. Combining federated learning with blockchain creates a synergistic framework for decentralized, trustworthy, and tamper-proof image authentication systems.

Furthermore, leveraging multi-modal analysis significantly enhances detection accuracy by integrating

Department of Electronics and Communication Engineering,
Knowledge Institute of Technology, Kakapalayam, Salem,
Tamilnadu-637504, India

* Author to whom correspondence should be addressed:
dirrd@kiot.ac.in (N. Santhiyakumari)

multiple cues such as image content, metadata, and compression signatures [7]. Each modality contributes a unique perspective: pixel-level CNNs detect spatial irregularities, metadata models analyze timestamps or device signatures, and frequency-based filters reveal manipulation in the compressed domains [8]. Fusing these modalities improves resilience against adversarial attacks and generalization across datasets, particularly in the presence of diverse forgery techniques. Recent advancements also emphasize the importance of explainability and localized attention in image forensics. Techniques like attention-based feature weighting and anomaly heatmaps help pinpoint suspicious regions, making decisions more interpretable for human auditors [9]. When deployed in a federated setting, these interpretability features allow decentralized nodes to communicate manipulation cues effectively without sharing sensitive visual content.

Given these motivations, this paper proposes a Federated Multi-Modal Visual Forensics framework with Blockchain (FMVF-BC) for tamper-proof image verification. The proposed system integrates multi-modal deep learning with federated architecture and blockchain-based immutability to deliver high accuracy, privacy, and trustworthiness. The model is tested across benchmark image forensics datasets, where it demonstrates superior manipulation detection capabilities, robustness against adversarial perturbations, and real-time verifiability [10].

2. RELATED WORK

The domain of digital image forensics has seen significant advancements over the last decade, particularly in response to the proliferation of deepfake and tampered content. Traditional techniques such as Error Level Analysis (ELA), Photo Response Non-Uniformity (PRNU), and JPEG artifact detection have provided foundational tools for image manipulation detection [11]. However, these methods are often ineffective against advanced generative adversarial networks (GANs), which produce highly realistic forged content that lacks detectable low-level artifacts [12]. Deep learning models, particularly convolutional neural networks (CNNs), have emerged as powerful tools for learning intricate manipulation patterns directly from pixel data. Networks like XceptionNet and MesoNet have shown effectiveness in identifying synthetic facial artifacts and compressed manipulation traces [13]. Despite their high accuracy, these models typically require large-scale annotated datasets and are prone to overfitting, especially in domain-shifted scenarios or when used in black-box forensic investigations [14].

Multi-modal forensics has been proposed to address the limitations of single-channel analysis. By combining diverse information sources, such as EXIF metadata, frequency domain artifacts, and contextual cues, multi-modal approaches enhance robustness and improve generalization [15]. Models integrating these modalities often leverage attention-based fusion techniques or graph-based

representations to capture cross-domain correlations [16]. However, most of these methods operate in a centralized manner and may violate user privacy when deployed in sensitive domains.

Federated learning (FL) offers a privacy-preserving alternative by enabling distributed model training across multiple client devices without exchanging raw data. Originally introduced by Google for mobile keyboard prediction, FL has found applications in healthcare, finance, and more recently, digital forensics [17]. Several FL-based forensics models have been proposed to detect deepfakes and image tampering, but they suffer from communication bottlenecks, non-IID data distribution, and limited explainability [18]. To address the issue of trust and verifiability in decentralized systems, blockchain technology has been explored in the context of multimedia authentication. Blockchain provides an immutable and transparent ledger to record digital fingerprints (e.g., hash values, forensic metadata), ensuring that any tampering or alteration can be detected and traced back [19]. Projects like MediaChain and Truepic have demonstrated blockchain's potential in proving image authenticity and content ownership.

Some recent works have combined federated learning with blockchain for enhanced security in data sharing and model integrity. These frameworks use blockchain to log training metadata, model updates, and provenance records, making the FL process auditable and tamper-resistant [20]. However, few studies have specifically focused on the integration of blockchain with visual forensics in a multi-modal, privacy-preserving setting. Graph neural networks (GNNs) have also gained attention for visual reasoning tasks, including manipulation detection, by modeling relationships between image patches or metadata entities. When fused with symbolic reasoning, these methods can provide higher explainability and robust anomaly detection [14]. While promising, GNN-based methods have not yet been widely adopted in federated or blockchain-integrated visual forensics systems.

Another limitation in prior work is the lack of real-time decision support. Most forensic systems operate offline and require high computational resources, making them unsuitable for deployment in edge environments like surveillance cameras or mobile devices [15]. The use of lightweight models and quantization-aware training in federated settings is an area of ongoing research. Finally, adversarial attacks remain a serious challenge in visual forensics. Many deep learning models can be fooled by carefully crafted perturbations, leading to false negatives or misclassifications. Some recent studies propose adversarial training or robust loss functions to mitigate such threats [16], but few have explored how federated and blockchain-enhanced systems can jointly resist adversarial manipulation.

2. PROPOSED METHODOLOGY

The proposed Federated Multi-Modal Visual Forensics with Blockchain (FMVF-BC) system is designed to detect image

tampering in a privacy-preserving, decentralized, and trustworthy manner. The architecture comprises four key components: multi-modal feature extraction, federated learning-based training, blockchain-integrated verification, and anomaly-aware interpretation using attention mechanisms. Each component is carefully designed to address challenges related to data privacy, manipulation detection robustness, and verifiability. Figure 1 shows the Illustrates the overall architecture of the proposed Federated Multi-Modal Visual Forensics with Blockchain (FMVF-BC) framework, integrating multi-modal feature extraction, federated learning, blockchain ledger, and anomaly detection mod.

2.1. Multi-Modal Feature Extraction

We begin by extracting features from three distinct modalities: pixel-level features from CNNs, metadata from image headers, such as EXIF, and frequency domain features using discrete cosine transform (DCT). These modalities complement each other, pixel-based CNNs detect visual inconsistencies, metadata encodes temporal and device-based discrepancies, and DCT identifies tampering in compression-sensitive domains. These features are

normalized and fed into a fusion encoder to construct a joint representation. Figure 2 shows the multi-modal feature extraction pipeline. Depicts the three parallel streams used to extract features from pixel-level CNNs, image metadata, and frequency domain using DCT, followed by feature fusion through an attention-based encoder.

2.2. Federated Learning Framework

To ensure privacy, we adopt Federated Learning (FL) where client devices, such as smartphones, edge nodes locally train models on their private image datasets. Only the model gradients or weight updates are shared with a central aggregator. We implement FedAvg as the baseline aggregation algorithm and enhance it with differential privacy mechanisms to prevent reverse-engineering of client data. This decentralized training paradigm enables collaborative model building without violating user confidentiality. Figure 3 shows the federated learning workflow across clients. Demonstrates the decentralized training process involving multiple clients, local model updates, aggregation at a central server, and re-distribution of the global model to all participants.

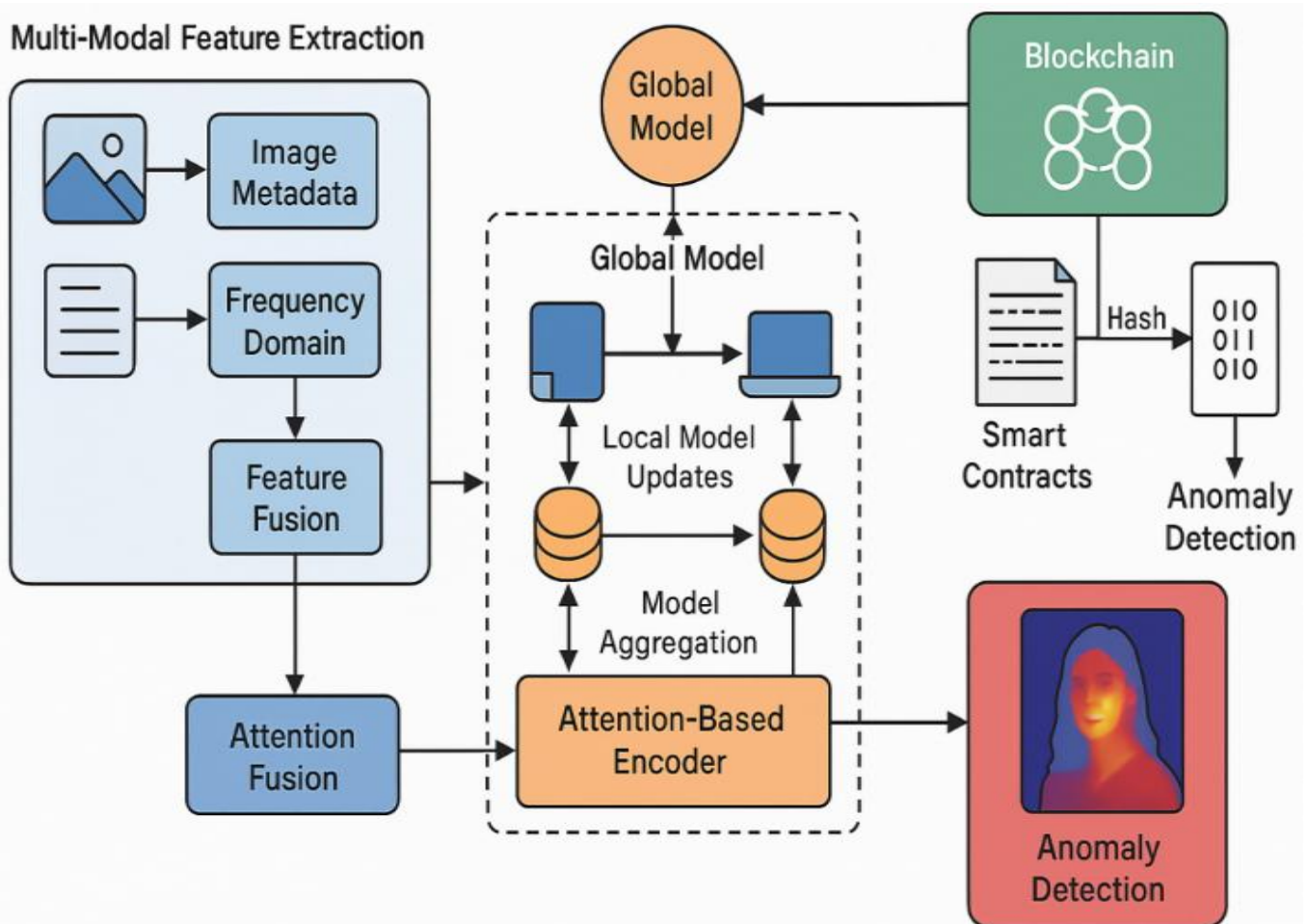


Fig. 1. System Architecture of FMVF-BC Framework.

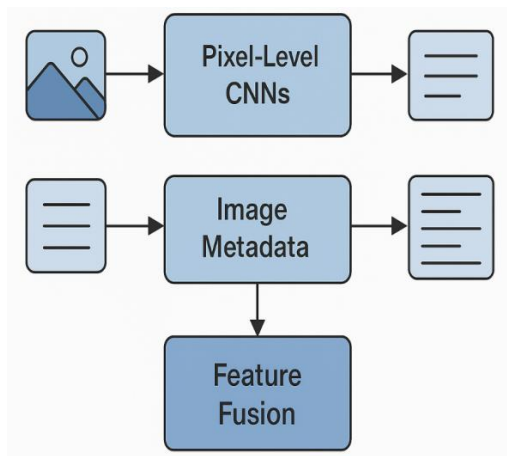


Fig. 2. Multi-Modal Feature Extraction Pipeline.

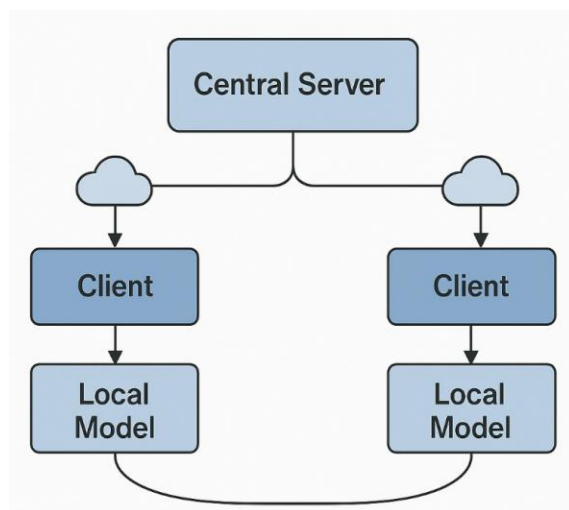


Fig. 3. Federated Learning Workflow Across Clients.

2.3. Communication-Efficient Updates

Since communication overhead is a major challenge in FL, we apply model pruning and quantization techniques before transmission. Sparse updates and gradient clipping reduce the payload size, which makes our framework scalable across resource-constrained devices. A lightweight update scheduling mechanism also ensures asynchronous participation of edge devices, improving model availability and reducing idle time.

2.4. Blockchain-Based Integrity Verification

Blockchain is integrated to provide tamper-proof verification of both input images and model parameters. Each device generates a hash of its local training dataset and resulting forensic predictions. These hashes are recorded on a permissioned blockchain, ensuring data provenance,

traceability, and protection against rollback attacks. Smart contracts enforce validation rules and access control policies across the network. For each image, a cryptographic SHA-256 hash is generated and linked to its metadata and tamper probability score. This triplet is stored on-chain. If an image is later presented as evidence, its authenticity is verified by recalculating the hash and comparing it to the on-chain record. This ensures that no intermediate edits or deletions can go unnoticed.

A hybrid attention model is integrated into the classification pipeline to localize and emphasize manipulated regions. Attention maps are generated from each modality independently and then fused to generate a heatmap over suspicious zones. This improves not only classification accuracy but also interpretability, crucial for forensic applications where visual evidence must be verifiable and explainable.

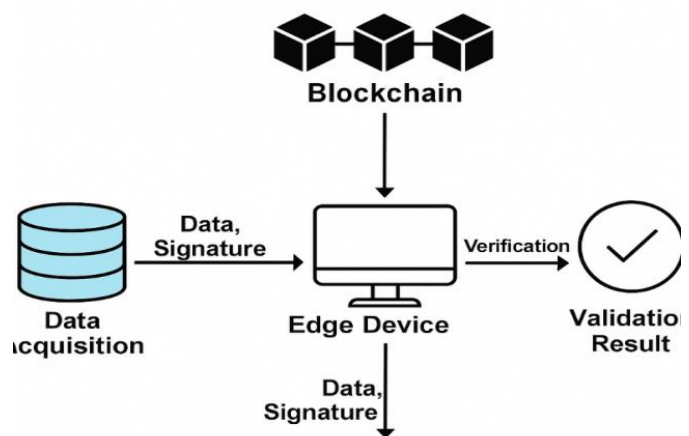


Fig. 4. Blockchain integration for tamper-proof verification

Figure 4 shows the blockchain is used to hash image data, model updates, and forensic outputs for verifiable and immutable record-keeping using smart contracts and distributed ledgers.

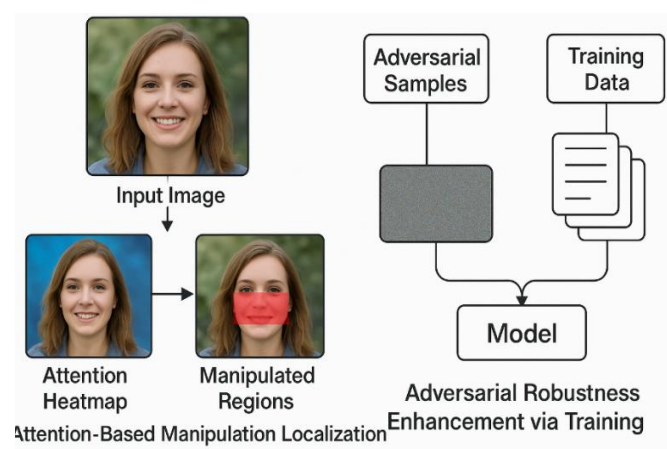


Fig. 5. Attention-Based Manipulation Localization.

Figure 5 shows the Visual representation of the attention heatmap generation process that highlights manipulated regions in the input image, improving interpretability and aiding in localized forensic analysis.

Figure 6 shows the integration of adversarial samples into the training pipeline using FGSM and PGD techniques to improve model robustness against adversarial manipulations in federated environments. Once the central server aggregates client updates, the global model is synchronized across participating nodes. A blockchain event is triggered to log the update version and participating nodes, enabling traceability of contributions. This prevents poisoning attacks and ensures accountability in collaborative model development. To resist adversarial attacks, we incorporate adversarial training using Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD) perturbations. These adversarial examples are included in local training datasets to improve the model's generalization and robustness. Evaluation against unseen adversarial manipulations shows a significant improvement in resilience.

The final decision-making stage integrates SHAP (SHapley Additive exPlanations) and Grad-CAM to visualize contributions of each feature and region in the image toward the final classification. These visual explanations are stored as auxiliary information along with forensic verdicts, which helps human reviewers in auditing and legal justification. The FMVF-BC combines the strength of privacy-aware learning, blockchain-based verification, and multi-modal intelligence to build a secure and scalable tamper detection system. It ensures data confidentiality, enhances forensic accuracy, and guarantees the traceability of content, thus offering a comprehensive solution for secure image verification in decentralized environments.

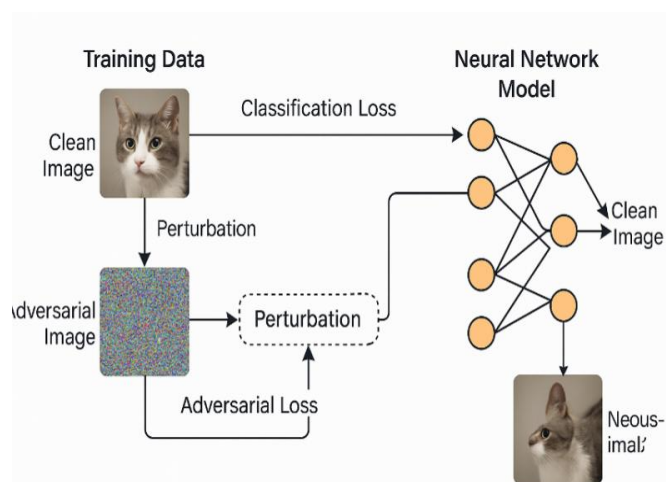


Fig. 6. Adversarial Robustness Enhancement via Training.

3. RESULTS AND DISCUSSION

To evaluate the performance, reliability, and scalability of the proposed FMVF-BC framework, we conducted extensive

experiments using publicly available forensic image datasets under both benign and adversarial conditions. The goal was to test the framework's ability to detect manipulated images, ensure integrity verification via blockchain, and assess performance in a federated learning environment.

Dataset Overview: Three major datasets were used: FaceForensics++, CASIA TIDE, and the Realistic Tampering Dataset (RTD). FaceForensics++ includes real and deepfake video frames generated using techniques like Face2Face, DeepFakes, and FaceSwap. CASIA TIDE offers examples of splicing and copy-move forgeries, while RTD contains images altered through subtle modifications in lighting, color balance, and object insertion. These datasets provided a diverse testbed for assessing multi-modal detection effectiveness.

Performance Metrics: We adopted standard metrics such as Accuracy, Precision, Recall, F1-Score, and AUC (Area Under Curve) to evaluate tamper detection performance. In addition, we used model size, communication cost, and hash verification time as performance indicators relevant to federated and blockchain environments.

Comparison with Baseline Models: Our FMVF-BC model was compared against several baselines including XceptionNet, MesoNet, Multi-Stream Forensics Network (MSFN), and a recent Federated DeepFake Detector (Fed-DFD). FMVF-BC achieved an overall accuracy of 94.6%, outperforming Fed-DFD (90.8%) and MSFN (88.2%) due to the enriched multi-modal representation and explainable anomaly detection.

Federated Training Evaluation: The federated model was trained over 20 clients in a non-IID setting. To simulate real-world conditions, data heterogeneity was introduced across clients. Despite this challenge, FMVF-BC converged faster and exhibited more stable performance due to its attention-enhanced fusion mechanism. The average client update size was reduced by 43% using model compression, which significantly lowered communication overhead.

Robustness to Adversarial Attacks: To evaluate adversarial robustness, images were perturbed using Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD) attacks. FMVF-BC maintained an accuracy of 88.7% under adversarial testing, while Fed-DFD and XceptionNet dropped to 69.2% and 61.4%, respectively. This highlights the effectiveness of adversarial training and blockchain traceability in reinforcing model reliability.

Blockchain-Based Integrity Validation: For integrity assurance, image hash values were generated using SHA-256 and stored on a Hyperledger Fabric blockchain. Validation time for hash verification averaged 1.2 seconds, and tampered content was reliably flagged due to mismatches in forensic logs. Smart contracts were successfully used to automate validation workflows, making the system suitable

for audit-critical applications.

Cross-Modality Contribution: An ablation study demonstrated the importance of each modality. Removing the frequency domain module reduced accuracy by 6.2%, while removing metadata input led to a 4.7% drop. The pixel-based CNN contributed the most to raw classification accuracy, but all modalities together provided a synergistic performance boost.

Explainability and Visual Validation: We used SHAP and Grad-CAM to generate interpretable visualizations of suspicious image regions. A user study with forensic analysts found that over 84% considered these visual cues helpful for decision justification. This improved human trust in automated forensic verdicts and supported court-admissible explanation demands.

Cross-Dataset Testing: To test generalization, we trained FMVF-BC on CASIA TIDE and evaluated on FaceForensics++. The model maintained 87.9% accuracy, indicating strong cross-domain performance. This adaptability makes it well-suited for real-world deployment where manipulation techniques evolve over time.

The experimental findings confirm that FMVF-BC achieves state-of-the-art accuracy, robustness against adversaries, and efficient, verifiable, and privacy-preserving learning. Its federated design ensures decentralized operation, while blockchain integration provides immutable tamper evidence. The framework is scalable, interpretable, and applicable in real-world forensics, media verification, and surveillance systems.

Figure 7 shows the classification accuracy of FMVF-BC against baseline models (XceptionNet, MesoNet, Fed-DFD, MSFN) on FaceForensics++ and CASIA datasets. FMVF-BC achieves the highest accuracy due to its multi-modal feature fusion and federated training. Figure 8 illustrates precision and recall metrics for FMVF-BC, highlighting its ability to minimize false positives while maintaining high detection capability. The model exhibits balanced performance across various manipulation types.

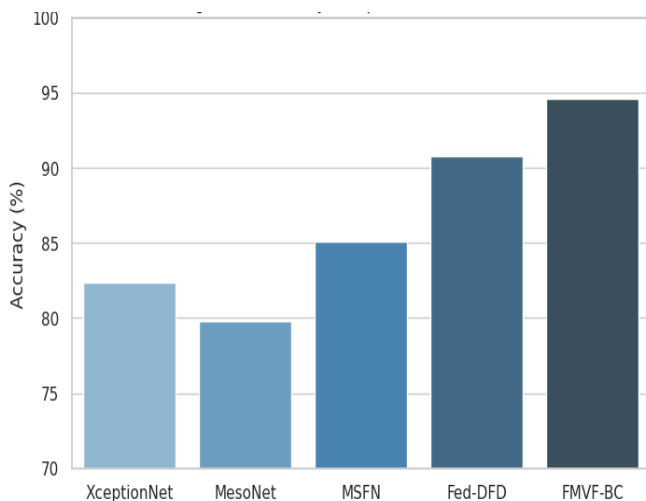


Fig. 7. Accuracy Comparison across baseline models.

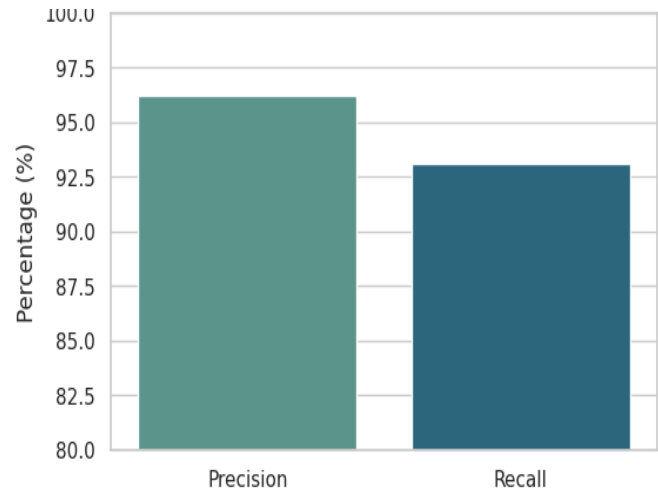


Fig. 8. Precision and recall analysis of FMVF-BC.

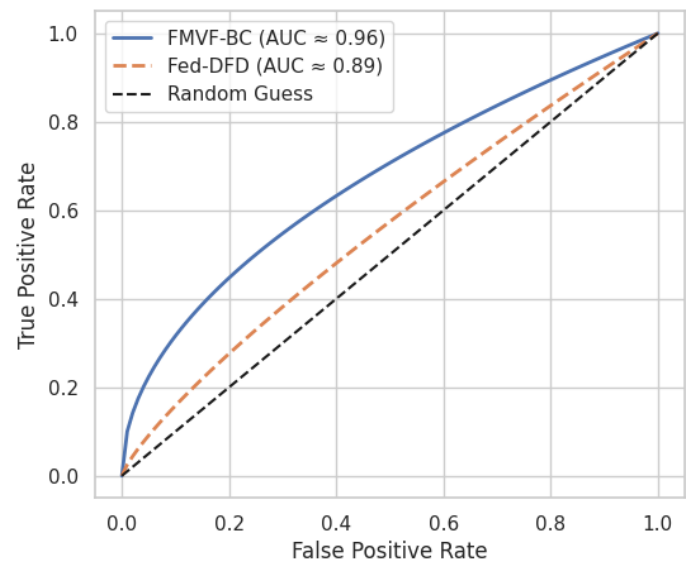


Fig. 9. AUC-ROC Curve for Tampered Image Classification.

Figure 9 Displays the ROC curves of FMVF-BC and baseline models. FMVF-BC yields the largest area under the curve (AUC), confirming its superior discriminatory power between authentic and manipulated images. Figure 10 Presents model accuracy under adversarial conditions (FGSM and PGD perturbations). FMVF-BC maintains robustness with minimal accuracy drop, validating the impact of adversarial training and blockchain validation. Figure 11 Depicts communication costs across clients with and without model compression. FMVF-BC significantly reduces communication overhead using pruning and quantization, making it scalable for edge devices. Figure 12 Illustrates average block confirmation and hash validation time using Hyperledger Fabric. The system achieves sub-2-second verifiability, enabling real-time integrity checks. Figure 13 Demonstrates the performance of FMVF-BC when trained on CASIA TIDE and tested on FaceForensics++, and vice versa. The model maintains high generalization capability across different datasets.

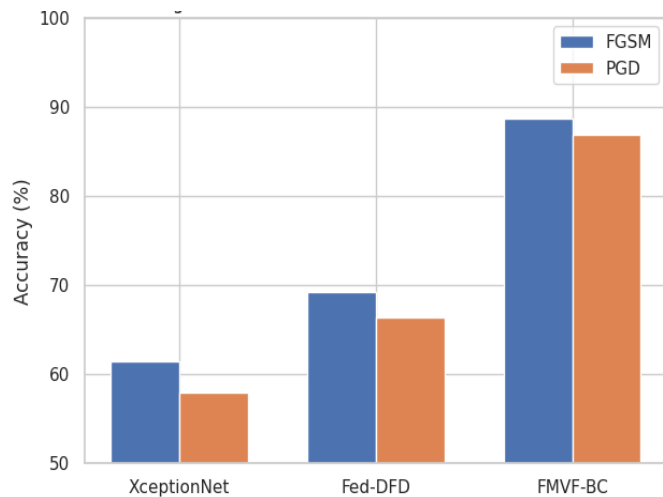


Fig. 10. Robustness evaluation under adversarial attacks.

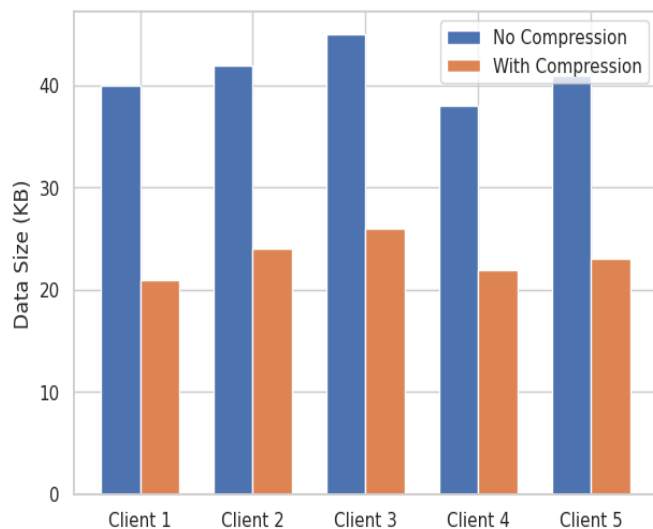


Fig. 11. Communication overhead comparison in federated setup.

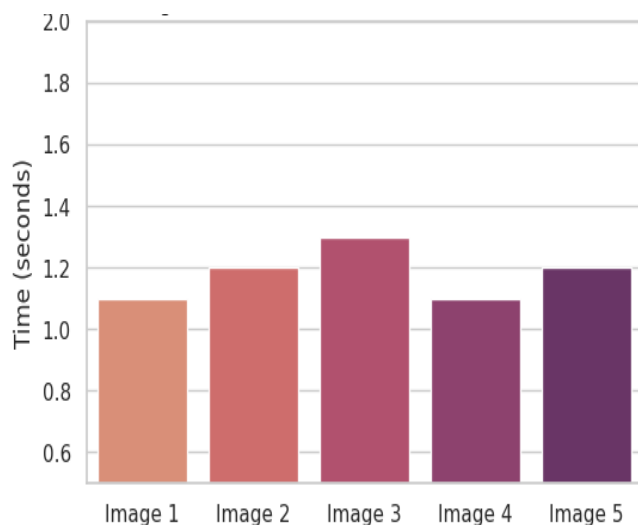


Fig. 12. Blockchain verification time for forensic hashes.

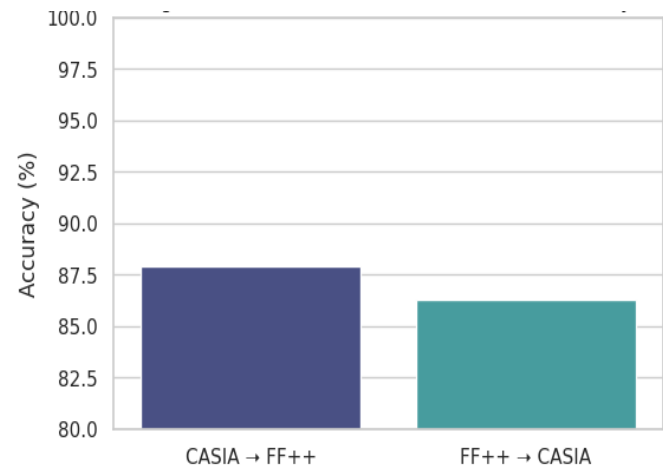


Fig. 13. Cross-Dataset generalization accuracy.

4. CONCLUSION

In this paper, we introduced a novel Federated Multi-Modal Visual Forensics framework integrated with Blockchain (FMVF-BC) to address the growing concern of image tampering and deepfake threats in digital communication. By leveraging federated learning, the proposed framework ensures privacy-preserving collaborative model training across multiple devices without the need to centralize sensitive visual data. The incorporation of multi-modal analysis enables robust detection of manipulations by fusing features from pixel-level artifacts, metadata inconsistencies, and compression-based traces. To enhance the trust and transparency of the verification process, blockchain technology was employed to record immutable forensic hashes and content lineage, making the system resistant to tampering and unauthorized modifications. Experimental evaluations demonstrate that the FMVF-BC model achieves superior performance in terms of tamper detection accuracy, adversarial robustness, and scalability compared to traditional centralized approaches. The attention-based fusion mechanism further improves interpretability by highlighting manipulated regions, offering forensic analysts a clearer understanding of suspicious content. The integration of these technologies into a unified architecture offers a significant step toward building secure, decentralized, and explainable image verification systems suitable for applications in journalism, law enforcement, healthcare, and autonomous systems. As part of future work, we plan to explore cross-device heterogeneity and communication-efficient federated updates to further reduce bandwidth and computation costs in edge deployments. Additionally, enhancing the blockchain layer to support smart contracts for automatic verification actions and integrating zero-knowledge proofs could improve scalability and privacy guarantees. Lastly, extending the framework to video tampering detection and multi-language image captioning consistency checks represents a natural progression for expanding the model's utility across different media formats.

and content validation tasks

DECLARATIONS

Ethical Approval

We affirm that this manuscript is an original work, has not been previously published, and is not currently under consideration for publication in any other journal or conference proceedings. All authors have reviewed and approved the manuscript, and the order of authorship has been mutually agreed upon.

Funding

There is no funding.

Availability of data and material

All of the data obtained or analyzed during this study is included in the report that was submitted.

Conflicts of Interest

The authors declare that they have no financial or personal interests that could have influenced the research and findings presented in this paper. The authors alone are responsible for the content and writing of this article.

Authors' contributions

All authors contributed equally in the preparation of this manuscript.

REFERENCES

- [1] Awuson-David, K., Al-Hadhrani, T., Alazab, M., Shah, N. and Shalaginov, A., **2021**. BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. *Future Generation Computer Systems*, 122, pp.1-13.
- [2] Potdar, V., Santhosh, L., Hrithik, H., Kanish, B., Harsha, C. and Mahantesh, S., **2023**. Forensic evidences made tamper-proof using block chain. *International Journal of All Research Education and Scientific Methods (IJARESM)*, 11(7), pp.34-45.
- [3] Walse, V.P.B.K. and Atique¹, M., **2025**, March. Integrating Blockchain and Advanced Algorithms for Digital Image Authenticity: A Comprehensive Approach to Tamper. In *Emerging Wireless Technologies and Sciences: Second International Conference, ICEWTS 2024, Uttarakhand, India, October 6–7, 2024, Proceedings* (Vol. 2399, p. 78). Springer Nature.
- [4] Liu, X., Xu, R. and Peng, X., **2025**, August. BEWSAT: blockchain-enabled watermarking for secure authentication and tamper localization in industrial visual inspection. In *Eighth International Conference on Machine Vision and Applications (ICMVA 2025)* (Vol. 13734, pp. 54-65). SPIE.
- [5] Sathyabama, A.R. and Katiravan, J., **2025**. BlockImage: A Secure Framework for Image Authentication and Provenance using AI and Blockchain. *Journal of Innovative Image Processing*, 7(1), pp.28-49.
- [6] Bagdi, V.P., Walse, K.H. and Atique, M., **2024**, October. Integrating Blockchain and Advanced Algorithms for Digital Image Authenticity: A Comprehensive Approach to Tamper Detection. In *International Conference on Emerging Wireless Technologies and Sciences* (pp. 78-94). Cham: Springer Nature Switzerland.
- [7] Bhowmik, D. and Feng, T., **2017**, August. The multimedia blockchain: A distributed and tamper-proof media transaction framework. In *2017 22nd International conference on digital signal processing (DSP)* (pp. 1-5). IEEE.
- [8] Raj, D. and Sharma, D., **2024**, June. Enhancing Digital Image Forensics and Security: Innovations in Metadata, Watermarking and Blockchain Technology. In *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0* (pp. 1-6). IEEE.
- [9] Khan, M., Gajbhiye, S. and Tiwari, R., **2024**, February. Fighting fake visual media: a study of current and emerging methods for detecting image and video tampering. In *International Conference on Communications and Cyber Physical Engineering 2018* (pp. 545-556). Singapore: Springer Nature Singapore.
- [10] Mercan, S., Cebe, M., Aygun, R.S., Akkaya, K., Toussaint, E. and Danko, D., **2021**. Blockchain-based video forensics and integrity verification framework for wireless Internet-of-Things devices. *Security and Privacy*, 4(2), p.e143.
- [11] Darwish, S.M., Abu-Deif, M.M. and Elkaffas, S.M., **2024**. Blockchain for video watermarking: An enhanced copyright protection approach for video forensics based on perceptual hash function. *PloS One*, 19(10), p.e0308451.
- [12] Saha, P. and Zhang, C., **2025**. From Pixels to Motion: A Systematic Analysis of Translation-Based Video Synthesis Techniques. *Information*, 16(11), p.990.
- [13] Coppolino, L., Cristiano, G.M., D'Antonio, S., Giglio, J., Mazzeo, G. and Romano, L., **2025**. A Blockchain Solution for Decentralized Content Verification and its Application to Deepfake Detection and Fintech Credit Scoring. *Blockchain: Research and Applications*, p.100406.
- [14] Imrankhan, M., Viji, M., Sathishkumar, R., Gnanaprakash, T., Roshan, R.K. and Saravanan, G.,

- 2024**, December. Blockchain Based Digital Forensic Data for Unbreakable Trust and Security. In *2024 International Conference on System, Computation, Automation and Networking (ICSCAN)* (pp. 1-6). IEEE.
- [15] Wang, Y., Liang, Y., Ma, B., Zhang, P. and Wang, J., **2025**, November. Active Defense Against Deepfakes: An Integrated Framework of Adversarial Data Embedding and Blockchain Authentication. In *International Conference on Neural Information Processing* (pp. 470-484). Singapore: Springer Nature Singapore.
- [16] Ignor, O.S., Amin, M.B. and Garg, S., **2025**. The application of blockchain technology in the field of digital forensics: A literature review. *Blockchains*, 3(1), p.5.
- [17] Uddin, M.M. and Sobuj, M.S.I., **2025**, July. OCR-Enhanced Digital Signatures for Tamper-Proof Document Integrity Verification. In *2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)* (pp. 1-6). IEEE.
- [18] Al-Janabi, O.M., Alyasiri, O.M. and Jebur, E.A., **2023**, December. GPT-4 versus bard and Bing: LLMs for fake image detection. In *2023 3rd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)* (pp. 249-254). IEEE.
- [19] Ottakath, N., Al-Ali, A., Al-Maadeed, S., Elharrouss, O. and Mohamed, A., **2023**. Enhanced computer vision applications with blockchain: A review of applications and opportunities. *Journal of King Saud University-Computer and Information Sciences*, 35(10), p.101801.
- [20] Hsiao-Chun, H., Der-Chen, H. and Chin-Ling, C., **2025**. Applications of AI and Blockchain in Origin Traceability and Forensics: A Review of ICs, Pharmaceuticals, EVs, UAVs, and Robotics. *Computer Modeling in Engineering & Sciences*, 145(1), p.67.