Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 14 Issue 03s, 2025

Blockchain-based Academic Certificate Fraud Detection: A Comparative Review and Combined Framework

[1]Priti Golar, [2]Tanushri Kalaskar, [3]Jennifer Joseph, [4]Mayuri Atkar, [5]Sakshi Bute

[1,2,3,4,5] Information Technology St. Vincent Pallotti College of Engineering and Technology, Nagpur, India

Email: [1]pgolar@stvincentngp.edu.in, [2]tanushrikalaskar.24@stvincentngp.edu.in, [3]jennifergjoseph.24@stvincentngp.edu.in, [4]mayuriatkar.24@stvincentngp.edu.in, [5]sakshibute.24@stvincentngp.edu.in

Peer Review Information

Submission: 05 Nov 2025

Revision: 25 Nov 2025

Acceptance: 17 Dec 2025

Keywords

Blockchain, Certificate Verification, Image Forensics, Machine Learning, Deep Learning, IPFS, QR Code, Forgery Detection

Abstract

The rapid rise in forged academic and professional certificates has become a major challenge across higher education and employment sectors. Manual verification is slow, inconsistent, and vulnerable to manipulation, especially with modern digital editing tools. Over the past decade, researchers have proposed automated approaches combining image forensic techniques, machine learning, and blockchain to enhance accuracy, transparency, and tamper-proof validation. This review summarizes recent advancements in feature extraction methods such as GLCM, LBP, SIFT, and copy-move detection, as well as deep learning models including CNN, VGG-16, and ResNet for forgery identification. It also examines blockchain-based frameworks leveraging IPFS, QR codes, and decentralized ledger architecture for immutable credential verification. Strengths, limitations, datasets, and implementation challenges are critically evaluated. The review concludes by proposing an integrated framework that combines machine learning-based forgery detection with blockchain-supported authentication to achieve secure, scalable, and trustworthy certificate verification.

Introduction

Forgery of academic and professional credentials has evolved from isolated incidents into a widespread challenge affecting universities, recruitment systems, international admissions, and regulated professions.

With advanced image-editing software, attackers can modify certificate templates, logos, signatures, grades, and dates with high precision, making manual inspection increasingly unreliable. Traditional a verification—contacting institutions or visually cross- checking documents—is slow, subjective, and impractical for large-scale or cross-border verification. Recent technological advancements present two major directions for solving this problem. First, image forensics and machine learning techniques detect visual anomalies by analyzing texture patterns, font inconsistencies, seal displacement, and cloned regions. Second, blockchain-based credential verification stores cryptographic hashes or metadata of certificates on a tamper-proof distributed ledger. This allows institutions and employers to verify authenticity using QR codes or on-chain lookups without relying on intermediaries.

This review examines recent developments in both domains, summarizes contributions from existing studies, highlights limitations, and proposes an integrated framework that combines ML-based forgery detection with blockchain-enabled authenticity verification for higher reliability.

Literature Review

A wide range of research has focused on developing automated certificate verification systems that minimize manual effort, reduce fraud, and ensure secure authentication. Traditional verification methods —such as physical letters sent to universities, email- based confirmation, and manual cross-checking—have proven slow, inconsistent, and prone to human error. As global student mobility increases, institutions require faster and more secure verification mechanisms. Consequently, researchers have shifted toward blockchain technology, image forensics, and hybrid verification models.

A. Blockchain-Based Verification Approaches Blockchain has become a leading solution for addressing certificate forgery due to its immutability, decentralization, and transparent auditing capabilities. Kishore T. Patil and his team proposed a decentralized blockchain architecture that ensures tamper-proof certificate issuance and verification. Their work, "Detection of Fake Physical Certificates Using a Blockchain-Based Certificate Verification and Issuer Validation System" (ICBDS, 2024) ([1]), demonstrates how cryptographic hashing and distributed ledgers prevent unauthorized modifications while enabling scalable verification across institutions.

A comprehensive global perspective is provided by Xiaoming Zheng, Shaoan Liu, Xiaocong Fan, and Dakai Zhu in their analysis "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" (IEEE BigData Congress, 2017) ([5]). Their study discusses how consensus algorithms maintain trust without intermediaries, improving reliability and decreasing verification delays.

Another significant blockchain-based educational framework is EDUCTX, proposed by Jayesh G. Dongre, Pratik Tiwari, and Sanjay Choudhary. Their work, "EDUCTX: Blockchain-Based Higher Education Credit Platform" (IJCA, 2019) ([6]), focuses on recording academic credits, grades, and certificates on a globally interoperable ledger. This enhances portability, credibility, and long-term preservation of academic documents.

A similar contribution is seen in the paper "Academic Certificate Fraud Detection System Framework Using Blockchain Technology" (Blockchain Frontier Technology, 2022) ([4]). This study outlines a blockchain-based validation system designed to verify issuing authorities and detect forged credentials, ensuring integrity across academic ecosystems.

A modern enhancement to blockchain verification is introduced by Nandini Chanekar et al. in "Fake Certificate Detection using Blockchain" (IRJET, 2023) ([3]). Their system integrates blockchain with IPFS (InterPlanetary File System), storing certificate data off-chain while maintaining cryptographic hashes on the blockchain. QR codes act as secure gateways, providing rapid verification while preserving privacy and scalability.

B. Image Forensics and Machine Learning Approaches Parallel to blockchain systems, researchers have explored image processing and machine learning techniques to detect manipulation within scanned or digitally created certificates.The study "Literature Review on Certificate Forgery Detection" (IJAEM, 2023) ([2]) categorizes image forensic methods into texture-based, transform-domain, keypoint-based, and deep learning–based approaches.

Texture-based methods such as Gray-Level Co-occurrence Matrix (GLCM) and Local Binary Patterns (LBP) examine patterns and textures to detect inconsistencies caused by editing. These techniques are particularly effective in identifying altered text segments, mismatched fonts, or replaced seals.

Keypoint-based techniques such as Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF) extract keypoints from document regions to detect copy-move forgery, duplicated elements, or spatial distortions.

Transform-domain methods, including Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), analyze frequency components to uncover compression artifacts and editing traces invisible to the human eye.

Recent research has increasingly adopted deep learning methods such as Convolutional Neural Networks (CNNs), VGG-16, ResNet, and transformer-based architectures. These models automatically learn hierarchical features and provide highly accurate detection of forged regions, even when the manipulation is subtle or visually sophisticated.

C. Combined Approaches (Hybrid Verification Models)

Multiple studies point toward hybrid systems—combining blockchain verification with image forensic techniques—as the most secure and comprehensive solution.

Papers such as "Detection of Fake Physical Certificates Using a Blockchain-Based Certificate Verification and Issuer Validation System" (ICBDS, 2024) ([1]) and "Literature Review on Certificate Forgery Detection" (IJAEM, 2023) ([2]) argue that blockchain alone cannot detect

visual tampering, while image forensics alone cannot prevent the circulation of entirely fabricated certificates.

Thus, integrating both technologies ensures that:

- Image forensics detect visual manipulation or digital editing.
- Blockchain confirms originality and issuer authenticity through immutable records.

This multi-layered approach significantly improves reliability, scalability, and resistance against sophisticated certificate fraud, making it suitable for universities, verification agencies, government bodies, and employers worldwide.

Problem Statement And Significance

Forgery of academic and professional certificates has escalated into a sophisticated cyber-enabled threat affecting global education and employment ecosystems. Fraudulent actors exploit modern image editing software, high-quality scanners, and desktop publishing tools to manipulate certificate elements such as institutional logos, official seals, signatures, typography, serial numbers, date formats, and holographic patterns. In several documented cases, counterfeiters replicate entire certificate templates and produce fabricated credentials indistinguishable to the human eye. These manipulations can be subtle— such as modifying a grade or replacing a candidate's name—or extensive, such as generating a complete degree document from scratch.

The core problem is twofold. First, determining whether the visual content of the certificate has been altered requires analyzing fine-grained patterns, textures, shadows, density variations, and pixel-level inconsistencies that cannot be reliably detected through manual inspection. Second, establishing whether the certificate was actually issued by the appropriate institution requires access to a trusted, tamper-proof record of certificate metadata, issuance history, and verification pathways.

Current verification practices face significant limitations. Different institutions follow varying formats, templates, fonts, and security features, making it challenging to create a universal verification process. In many countries, universities do not maintain centralized databases, resulting in fragmented and uncoordinated verification workflows. Additionally, certificates often exist only in printed form or as low- quality scanned copies, further complicating detection.The consequences of certificate forgery Eextend beyond academic dishonesty. Fraudulent credentials may allow unqualified individuals to enter regulated professions such as healthcare, engineering, aviation, and education, posing risks to public safety and institutional reputation. Employers also suffer financial losses and brand damage when falsified credentials go unnoticed during recruitment.

Therefore, there is a critical need for an automated system that can detect visual manipulation and verify the origin of the certificate. Integrating advanced image forensics and machine learning ensures precise visual forgery detection, while blockchain technology provides decentralized, immutable, and transparent verification. Such a combined framework would significantly improve trust, accuracy, scalability, and efficiency in credential authentication.

Methodology

A. Image Acquisition and Preprocessing

The methodology begins with acquiring the certificate image either through uploading, scanning, or capturing it using a digital device. To ensure the image is suitable for further analysis, several preprocessing operations are applied:

- Grayscale Conversion: Converts the image into a single-channel intensity format to simplify analysis and reduce computational load.
- Noise Reduction: Removes scanning artifacts, blur, and dust using filters such as Gaussian or median filtering.
- Resizing: Standardizes image dimensions, ensuring uniformity for machine learning model input.
- Contrast Enhancement: Improves the clarity of text, seals, and patterns, making fine-grained structural details more distinguishable.
- These preprocessing steps normalize the certificate image and preserve critical visual features required for accurate extraction and classification.

B. Feature Extraction

Following preprocessing, the system extracts distinctive visual and structural attributes that differentiate genuine certificates from forged ones. Several feature extraction techniques are employed:

- Gray-Level Co-occurrence Matrix (GLCM): Captures texture relationships and spatial intensity patterns.
- Local Binary Patterns (LBP): Extracts micro- texture attributes related to fonts, seals, and document backgrounds.
- Scale-Invariant Feature Transform (SIFT): Identifies robust keypoints related to logos, signatures, emblem alignment, and

structural elements.

These extracted features collectively represent the certificate's texture, layout, and design characteristics, forming the foundational input for machine learning classification.

C. Machine Learning Classification

The extracted features are then passed to machine learning models for authenticity prediction. Two primary classification approaches are used:

- Support Vector Machine (SVM): Effective in handling high-dimensional feature vectors derived from GLCM, LBP, and SIFT.
- Convolutional Neural Networks (CNNs): Automatically learn deep spatial representations, identifying subtle inconsistencies introduced during document tampering.

The classifier outputs a probability score indicating whether the certificate is genuine or forged, enabling reliable and accurate detection.

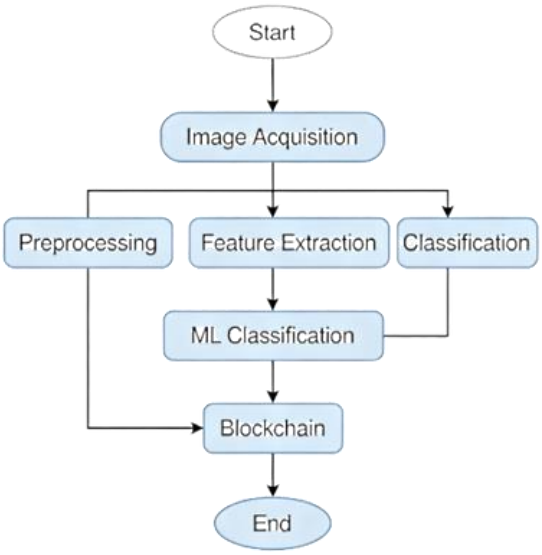

Figure 1: Machine Learning-Based Authentication Model

D. Blockchain-Based Verification

To ensure tamper-proof and decentralized verification, blockchain technology is integrated into the system. Once the classification stage is completed:

1. A cryptographic hash of the authenticated certificate is generated.
2. This hash is stored on a blockchain using the InterPlanetary File System (IPFS), ensuring immutability and secure distributed storage.
3. A QR code containing the hash or retrieval link is generated and printed or embedded on the certificate.

During verification, scanning the QR code retrieves the stored hash from the blockchain. A match between the stored hash and the hash of the presented certificate confirms authenticity; any mismatch indicates alteration, ensuring secure and transparent validation.

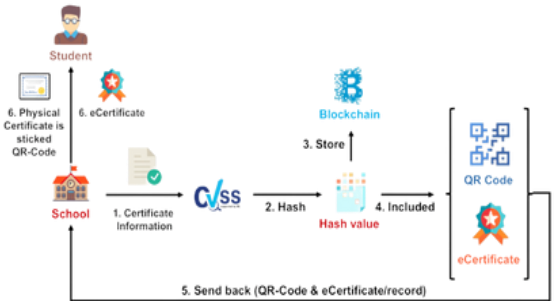

Figure 2: Blockchain Certificate Verification Process

Results And Discussion

The review of existing research demonstrates that integrating image processing, machine learning, and blockchain technology yields a robust and comprehensive approach to detecting and verifying academic certificates. Studies consistently report that image preprocessing techniques—such as noise reduction, contrast stretching, and grayscale normalization—significantly enhance feature visibility. These enhancements allow algorithms to better capture subtle anomalies introduced through forgery, ultimately improving classification accuracy. Feature extraction methods like the Gray-Level Co-occurrence Matrix, Local Binary Patterns, and Scale-Invariant Feature Transform perform well in isolating spatial irregularities, textural deformations, geometric distortions, and inconsistencies in logo placement or seal structures. Such techniques help identify copy–move forgery, region duplication, and manipulated segments of the certificate that may not be visible to the human eye.

Transform-domain methods, including the discrete cosine transform and discrete wavelet transform, further improve detection by capturing hidden frequency-domain artifacts created during editing or compression. Deep learning approaches demonstrate even higher accuracy. Convolutional Neural Networks automatically learn multi-level spatial features—edges, textures, gradients, and structural patterns—allowing them to detect even meticulously crafted manipulations. Studies evaluating architectures like VGG-16 and ResNet show that deep neural networks outperform traditional handcrafted feature-based models, especially when trained on sufficiently diverse datasets. However, their

performance depends heavily on the availability of high-quality training images, which remains a limitation.

Blockchain integration introduces a second validation . layer that ensures authenticity even when visual inspection is inconclusive. Systems that store certificate hashes on the blockchain, indexed through QR codes, enable rapid verification by comparing user- provided certificate hashes with on-chain records. This approach prevents tampering, eliminates dependency on manual verification, and preserves privacy by storing only cryptographic identifiers rather than the actual certificate contents. Experiments using blockchain frameworks confirm near-instantaneous verification times, high reliability, and strong resistance to tampering.

Despite promising results, several challenges remain. Many proposed systems rely on small or institution- specific datasets, limiting their generalizability across diverse certificate formats

Variation in scanning devices, lighting conditions, and compression settings can degrade image quality and reduce detection accuracy. Additionally, blockchain implementations must consider privacy regulations by ensuring that sensitive personal information is stored off-chain. Interoperability among institutions also remains a challenge, requiring standardized framworks to ensure seamless adoption across regions.

Overall, the reviewed findings strongly support the viability of a hybrid model where machine learning handles forgery detection and blockchain technology manages authenticity verification. This approach provides a scalable, secure, and trustworthy solution for combating the growing problem of academic certificate fraud.

Conclusion

This review highlights the growing sophistication of certificate forgery and the inadequacy of manual verification systems. Integrating machine learning and image forensics with blockchain technology presents a strong and reliable solution. Image processing techniques identify visual inconsistencies, while blockchain ensures tamper-proof, decentralized verification of certificate authenticity. Future work should focus on developing standardized datasets, optimizing deep learning models for real-time performance, and designing privacy-preserving blockchain frameworks for academic institutions worldwide.

References

"Detection of Fake Physical Certificates Using a Blockchain-Based Certificate Verification and Issuer Validation System," IEEE ICBDS, 2024.

"Literature Review on Certificate Forgery Detection," IJAEM, vol. 5, no. 3, pp. 660–666, 2023.

Nandini Chanekar, Divyani Gurnule, Aamir Giri, Ayaan Sayyad, Kushal Sawarkar, and Aditya Dandekar, "Fake Certificate Detection using Blockchain," IRJET, vol. 10, no. 7, 2023.

"Academic Certificate Fraud Detection System Framework Using Blockchain Technology," Blockchain Frontier Technology, vol. 1, no. 2, 2022.

Xiaoming Zheng, Shaoan Liu, Xiaocong Fan, and Dakai Zhu, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE BigData Congress, 2017.

Hazarika, I. (2022). Digital transformation of the silk industry of Assam. Archives of Business Research, 10(4), 110–119. https://doi.org/10.14738/abr.104.12261

Jumde, A., Hazarika, I., & Cho, B. Y. (2019). Block chain technology: A new enabler of financial services. In Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT) (pp. 259–263). IEEE. https://doi.org/10.1109/ITT48889.2019.9075091

Jayesh G. Dongre, Pratik Tiwari, and Sanjay Choudhary, "EDUCTX: Blockchain-Based Higher Education Credit Platform," IJCA, vol. 182, no. 47, 2019.

"E-Certificate Verification Using Blockchain," IJERT, 2024.

Sharma, B. (2025). Ethical and AI concerns in data privacy: A charismatic dilemma. International Journal of Multidisciplinary Research and Development, 12(7), 18–32.

Sharma, B. (2025). Liability and virtual spaces: Examining legal responsibilities in Metaverse. National Journal of Cyber Security Law, 8(2).

Hazarika, I., Khalfan, J., Ahmed, M., Yousif, A., & Hussain, J. (2024). Role of fintech as an enabler to fulfill HR requirements and attain sustainability. In A. Hamdan & A. Harraf (Eds.), Business development via AI and digitalization (Vol. 537, pp. 59–69). Springer. https://doi.org/10.1007/978-3-031-62106-2_5

"A. Gangwar, "Blockchain-Based Academic Certificate Verification System," IJCA, vol. 186, no. 26, 2024.

"Academic Certificate Authenticity Using Blockchain Technology: A Review," ResearchGate, 2024.

G. H. Kumar, J. Swapna, M. Sirisha, K. S. Gowthami, and B. S. Kumar, "Detection of Fake Certificate Using Blockchain Technology," IJMTST, vol. 10, no. 9, 2024.

IJIRCCE, "Certificate Verification Techniques," vol. 13, no. 9, 2025.

Patil, R. V., Gaidhani, V. A., Kashid, P. V., Hazarika, I., Mahadik, R. V., Poddar, G. M., & Patila, S. R. (2025). Decentralized autonomous organizations as emerging economic entities in accounting and governance frameworks. International Journal of Accounting and Economics Studies, 12(4), 166–177.

"Development of Blockchain-Based Academic Credential Verification," SCIRP, 2023.

"Blockchain Based Authentication and Verification System for Academic Certificate using QR Code and DApps," IJCA, 2024.

"Design and Analysis of Digital Certificate Verification using Blockchain Technology," ResearchGate, 2023.