International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Artificial Intelligence in Detecting Fake Academic Certificates

Sahil Gole1, Abhishek Bhosale 2, Dr. Swati Joshi3

1,2 Department of Computer Science, PVG's College of Science and Commerce
3 Research Guide, Department of Computer Science, PVG's College of Science and Commerce

Abstract

The selling of fake academic diplomas has become a major international business that endangers the usual legitimacy of academic institutions and the security of the labor force. With billions of dollars in illegal revenues through the operation of the so-called diploma mills and the digital methods of forgery actually moving beyond the reach of the naked eye, the old methods of manual verification, usually marked by bureaucratic latency and human error, have become obsolete. The proposed research report is a thorough study exploring how Artificial Intelligence (AI) can be radically applied to the field of document forensics and credential validation. We discuss a multilayered technological model based on Deep Learning (DL) networks, i.e., Convolutional Neural Networks (CNNs) and Graph Convolutional networks (GCNs) and forensic tools such as Error Level Analysis (ELA) and Optical Character Recognition (OCR). We go even further to the application of blockchain technology as an unchangeable register to support the authenticity of the digital credentials. This report reveals the promise of using AI in automating the detection of micro-anomalies that can be used to identify forgery by conducting a stringent analysis of methodologies, such as the mathematical foundations of the Structural Similarity Index Measure (SSIM) and the cryptographic logic of smart contracts. We offer comprehensive performance measures of the modern literature where accuracy rates are above 97 percent in the controlled settings, yet we approach the so-called innovative threat to the adversarial attacks with seriousness and the ethical discussions on transparency of algorithms are also stated. This paper seeks to offer a conclusive technical architecture of the implementation of AI-based verification systems.

Keywords:
The AI, artificial intelligence, Fake Certificate Detection, Deep learning, Computer vision, Pentium blockchain, Convolutional neural network, error level analysis, Optical Character Recognition, academic integrity, Graph convolutional networks.

Introduction

Academic certification is sacrosanct to contemporary labor markets and higher learning. Academic degree is not just a sheet of paper, it is the indication of proven abilities, knowledge, and moral training. But this trust is growing more and more endangered. The barrier to forgery has been brought down to virtually nothing by high-fidelity digital editing tools and vigorous promotions by scams commonly known as diploma mills of false credentials.
So far checking of academic certificates has been a physical process in a digital world.
A manual inquiry (thru email, telephone, or post) of a verifier (such as an employer or other university) with the issuing institution makes up the gold standard. This is an active process

invoked by a certain suspicion and slower in nature since it usually takes weeks to complete because of registrar overload. The resulting verification gap gives some period through which fraudsters can get employment or be admitted before they are caught. Manual validation is also finding it hard to keep up with the sheer numbers of credentials within the mobile workforce of the globe, as cross-border checks introduce a linguistic and bureaucratic dimension.
Artificial Intelligence - more specifically Computer Vision and Machine Learning - is a radical solution, which is expected to shift toward practice in sensitive areas such as education and fraud detection in 2023. The AI systems do not merely read documents; their sensitivity can read every pixel, which is far much better than their human counterparts. Deep-learning algorithms are capable of detecting minor statistical anomalies that come about as a result of digital manipulation: anomalies of mismatched compression artifacts in a spliced signature, microscopic aliasing of substituted font, or the invisible break in structural symmetry in a synthetic template.

Advantages of Artificial Intelligence in Certificate Verification

AI also improves the verification of academic credentials through increased speed, cost and quality. Machine learning models have the capability to handle high amounts of data in a consistent manner, which deals with the "Iron Triangle" of administrative processing.

- **Dealing with Large Scalable Datasets.**

The tertiary industry generates millions of higher education qualifications annually. In old systems, documents are checked separately.
They are capable of operating peak loads in case of graduation or recruitment without being affected in terms of performance. This is essential to national repositories and multinational companies which receive tens of thousands of applications. This is made possible by AI where there is widespread verification, rather than isolated screening of suspicious candidates.

- **Improved Pattern Detection and Pattern Recognition.**

The human readers depend on the visual clues such as signatures or seals. Artificial intelligence and most prominently deep-learning networks like Convolutional Neural Networks (CNNs) learn minor patterns of features that are imperceptible by humans. Figuratively speaking, a CNN can notice that in a particular university the true certificate must have an effective metric between the logo and the background, always having a certain level of pixel-intensity. AI detects deviations of templates font sizes or any other imperceptible anomalies that indicate a scan-and-print process.

- **Identification of Invisibility Forgeries (Digital Forensics)**

Digital fingerprints are created by photo-editing software. When a part of an image is modified, such as copying a pass grade into a failed one, the manipulated shape on the image has a differing compression history to the rest. These differences are emphasized by Error Level Analysis (ELA) that shows the modified area bright and the original one normal.

- **Real-time Data Analysis and Integration**

FinTech detects fraud transactions in real-time with the help of AI. The same real time has been extended to document verification. A certificate is uploaded and would give an instant probability score through an AI-based system. Should the score pass a specified threshold (say, 60 percent

risk of forgery), the system may demand further evidence or may prompt a manual check-up 19 builds hiring or admission faster. AI is also combined with OCR and blockchain or university databases in which it checks the data within a certificate, not its image.

Disadvantages of Artificial Intelligence

Although powerful, AI has serious challenges that should be comprehended to develop strong Systems

.

- **Bias and Generalization Failures In Data.**

AI learns through the data which it is trained on. Models that are primarily trained on Western certificates (typically in English with Latin scripts and standard layout) can perform poorly on certificates in the Global South which can be written in different scripts, on different paper or artistically designed

- **Adversarial Attack Vulnerability.**

Fraudsters change tactics as AI detection grows to be a standard. Adversarial attacks manipulate a fake image by introducing some noisy data that usually cannot be seen but which reveals itself as arealimage to the model.

- **There are high computational demands and cost of infrastructure**

Forensic analysis models based on deep-learning, including ResNet-50 or VGG-16, require large memory and strong GPUs to train. The hardware or cloud compute prices might be prohibitive to small schools or agencies operating in developing economies. This builds a digital divide, which only deep-pocket institutions can afford the best defense against forgery..

- **Lack of Explainability (The "Black Box" Problem)**

Deep-learning models do not provide a clear explanation as to why a document was flagged as they provide a many-to-many probability score. In law or other fields, this would make it harder to justify the comments of fraud, as well as to appeal against individuals who have been flagged down on technical issues.

Literature Reviews on Artificial Intelligence in Certificate Verification

The field of detecting fake certificates in academia has shifted to complex hybrid AI-blockchain technology rather than the simple image processing technology. The following is a discussion of the major research contributions, which informed the present-day methodology.

Misbah Shaikh, Dr. Dipak Patil (2022):

This study discusses scalability of image forgery detection in cloud-based architecture. The authors note that local implementation of deep learning models can be done, but it is not scalable to institutional scale scales. They indicate that cloud-based solutions are more scalable, have better real-time processing as they can engage in the analysis of large amounts of images.

Yoosuf, Mohamed Sirajudeen (2020):

Yoosuf, in a groundbreaking article on the verification of documents, introduces an automatic verification framework based on Convolutional Neural Networks (CNN) and trained on the MIDV 500 (256 Azerbaijani passport images) dataset. It has a unique methodology by using sliding window operations which provide the assessment of authenticity region-by-region. The research

is also based on the combination of Optical Character Recognition (OCR) and Linear Binary Pattern (LBP) texture analysis.

Nnamdi Azikiwe University Research (2021):
An empirical implementation project based on the Nigerian context where certificate forgery is a major problem. The researchers elaborated an intelligent verification system based on the Artificial Neural Networks (ANN). They gathered a set of 1,180 authorized certificates of the university in the period of 2016-2020. The model attained a Regression value of R = 0.99373 and a Mean square error (MSE) = 0.000100. The high value of regression shows that the predicted validity and the actual validity of the certificates in the test set is almost the same.

Yuan et al. (2022) - Graph Convolutional Networks:
Leaving the traditional CNNs, Yuan et al. have suggested a new strategy which operates with the help of Graph Convolutional Networks (GCNs) to recognize the malicious digital certificates. Although their area of focus largely matches that of cybersecurity (SSL certificates), the methodology is very relevant. With this the model is able to learn the structural semantics of a valid certificate. Their GCN model reached the accuracy level of 97.41, which is more than traditional machine learning algorithms. This implies that to consider a certificate a network of connected information (e.g. the association between the date and the signatory) is an effective detection vector.

Sari & Fahmi (2021) - ELA and Deep Learning:
The given research deals with the forensic examination of the image manipulation directly. The authors tested the application of Error Level Analysis (ELA) to the preprocessing of a CNN. The following paper essentially gives the empirical rationale to the use of ELA as a standard preprocessing step in our proposed methodology.

Isizoh et al. (2021) - Neural Networks and Clustering:
This group considered unsupervised methods of learning, namely clustering, to do the issue of fraud detection. In contrast to the supervised learning, where it is necessary to provide labeled fake examples, clustering can detect so-called outliers that are not represented by the statistical distribution of the true certificates. This can be very handy in the detection of new forgeries that have not been encountered before. Their study is comparable with FinTech where fraudulent transactions based on an anomaly detection are applied that do not fit with a normal spending pattern of a user.

Lutfiani et al. (2022) & Thakare et al. (2024) - Blockchain Integration:
The authentication process turns into a cryptographic look up instead of a picture scanning. But in their presence, they admit that it is difficult to be scalable and incur gas charges. According to this literature, the future will be hybrid: AI will authenticate the physical/legacy document, and blockchain will authenticate the digital hash.

1. Problem Definition
The core problem addressed in this research is the Automated Binary Classification of Academic Credentials into two distinct classes: "Authentic" and "Forged." This is a complex classification problem due to the heterogeneous nature of the input data. Certificates vary wildly in layout, font,

language, and paper type across different institutions and eras. Furthermore, the class of "Forged" documents is adversarial; it is not a fixed class but an evolving one, designed specifically to minimize the distance between itself and the "Authentic" class in feature space.

Methodology:

Objective Identification: The primary objective is to develop a robust AI pipeline that accepts a digital image of a certificate (scanned or photographed) and outputs a confidence score regarding its authenticity. Secondary objectives include:

o Localization: Identifying the specific region of the document that has been altered (e.g., changing the name or the grade).

o Content Verification: Extracting semantic data (text) to cross-reference with external truth sources (databases or blockchains).

Data Requirements: The system requires a multi-modal dataset:

o Visual Data: High-resolution RGB images of certificates.

o Forensic Data: ELA maps and edge-detected versions of the visual data.

o Structural Data: JSON or XML templates defining the expected layout (bounding boxes of logos, text fields) for specific document types.

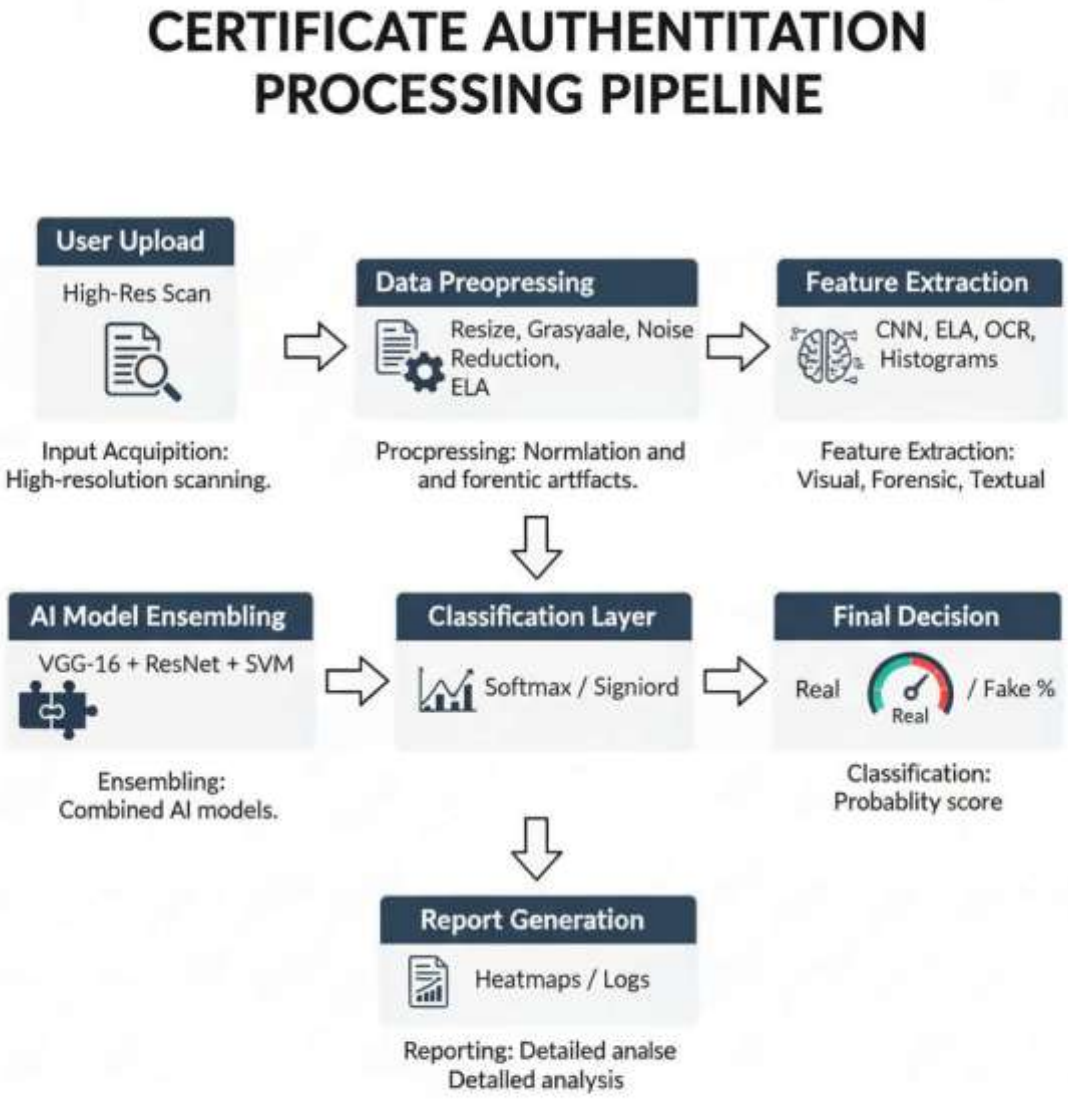
o Textual Data: Ground truth strings for the expected content.

2. Data Collection & Preparation

The efficacy of any Deep Learning model is inextricably linked to the quality and quantity of its training data. In the domain of document forgery, data scarcity is a primary bottleneck—legitimate institutions do not publicize their security features, and fraudsters do not publish their failures.

System Architecture & Methodology

The proposed solution utilizes a hybrid pipeline that combines visual forensics (identifying image manipulation) with semantic verification (checking text validity). The architecture is designed to be modular, allowing institutions to plug in different models based on their computational Resources.



Data Preprocessing

Raw images must be standardized before ingestion by the neural network.

Normalization and Resizing: Images are resized to a fixed input dimension (e.g., 224×224 or 512×512 pixels) to ensure compatibility with CNN architectures like VGG-16. Pixel intensity values, originally ranging from 0-255, are normalized to a range of $$ or standardized to have zero mean and unit variance. This accelerates gradient descent convergence.

Augmentation: To prevent the model from memorizing specific examples (overfitting), we apply random transformations during training:

o Rotation: ± 5 degrees to simulate slightly skewed scans.

o Noise Injection: Adding Gaussian noise to simulate scan grain.

o Blurring: Applying slight Gaussian blur to simulate poor focus.

Forensic Transformation: A critical preprocessing step is the generation of Error Level

Analysis (ELA) maps. For every image in the dataset, a corresponding ELA image is generated. This transforms the input from "what the image looks like" to "how the image was compressed," making invisible tampering visible to the network.

3. Feature Engineering

Feature engineering bridges the gap between raw pixels and semantic understanding. We employ a hybrid approach, utilizing both "hand-crafted" features for interpretability and "learned" features for performance.

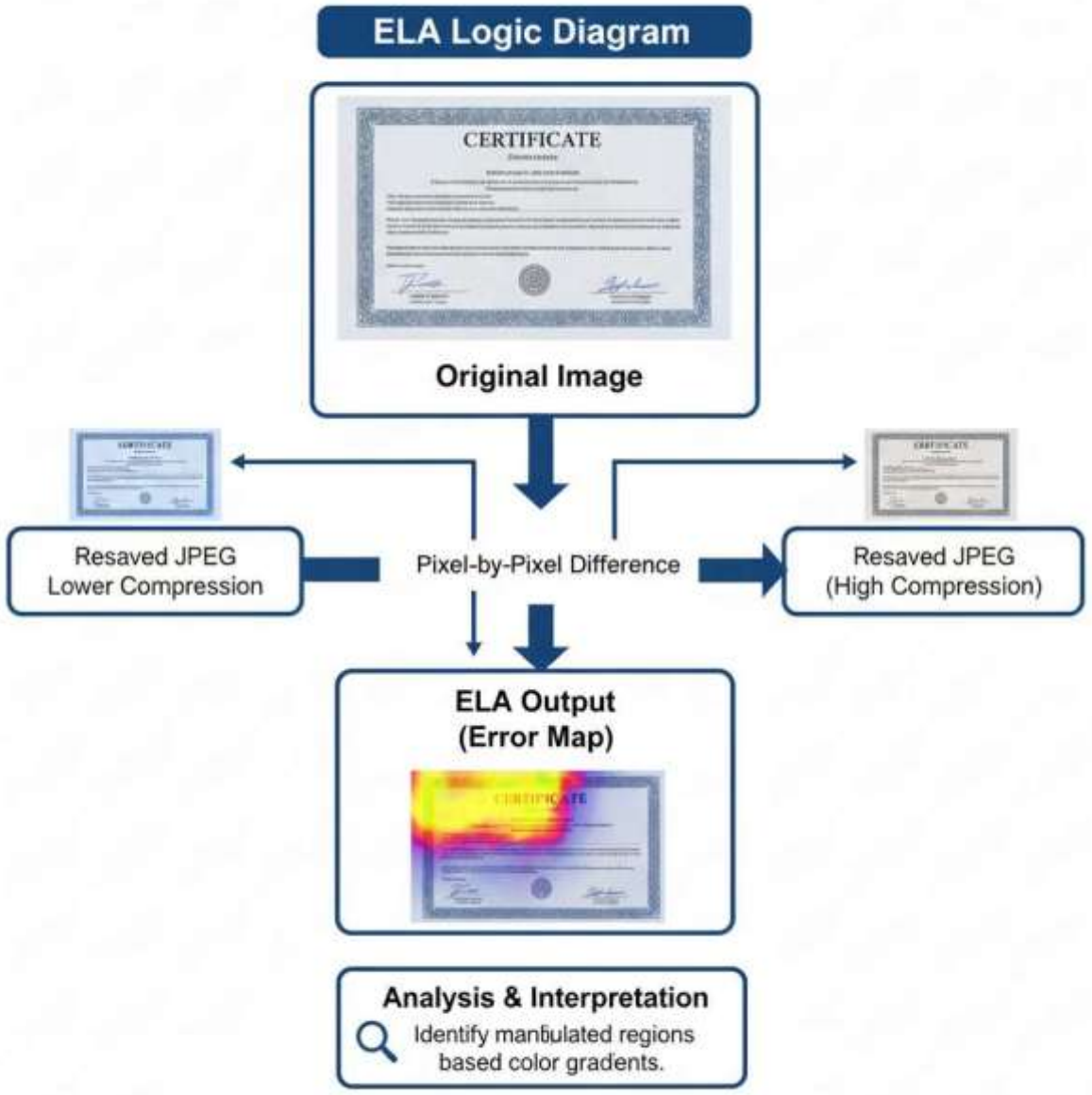
Manual Feature Extraction (Forensic & Structural)

Structural Similarity Index Measure (SSIM): We utilize SSIM as a primary feature. SSIM measures the perceived quality of a digital image by analyzing three components: Luminance (l), Contrast (c), and Structure (s). For a certificate verification system, we compare the input image (x) against a known template (y).

Histogram Analysis: We extract color histograms to detect "splicing." If a patch from a different image is pasted into the certificate, the local color histogram of that patch often diverges from the global histogram of the document.

Forensic Preprocessing: Error Level Analysis (ELA)

A critical step is ELA, which makes invisible manipulation visible. When an image is modified and resaved, the compression levels of the modified area differ from the background.



Automated Feature Learning (Deep Learning)

Convolutional Features: In the CNN approach, the initial layers act as feature extractors. The first layers might learn to detect the sharp edges of the border or the specific curves of the font. Deeper layers learn complex abstractions, such as the geometry of the university's holographic seal or the specific texture of the paper grain.

Attention Maps (MFAN): As described in recent research , we can utilize Multi-Level Features Attention Networks. These mechanisms allow the network to "pay attention" to specific discriminative regions—such as the signature block or the date field—while ignoring irrelevant background noise. This mimics the human forensic expert's focus on high-risk areas.

4. Model Selection

Given the complexity of the task, a single model is often insufficient. We propose an ensemble

architecture.

Convolutional Neural Networks (CNNs) - VGG-16 / ResNet-50

For the primary image classification task, we select proven architectures like VGG-16 or ResNet-50. These models are pre-trained on massive datasets (ImageNet), giving them a robust understanding of general visual features. Through Transfer Learning, we replace the final fully connected layers with new layers dimensioned for our binary classification task.

Graph Convolutional Networks (GCNs)

Drawing from Yuan et al. we incorporate GCNs for structural verification. We represent the certificate as a graph where text blocks, logos, and signatures are nodes, and their spatial distances are edges. The GCN learns the topology of a valid certificate. If a fraudster moves the "Date" field slightly to the left to fit a longer name, the graph topology changes, and the GCN detects this anomaly with high accuracy (reported at 97.41% in similar domains).

Support Vector Machines (SVM) & Logistic Regression

For simpler, resource-constrained environments (or for the final classification layer of an ensemble), we consider classical ML algorithms. Recent studies have shown that Logistic Regression, when fed with high-quality vector features (like those from a Count Vectorizer or extracted CNN features), can achieve accuracies up to 94.28%.

5. Training the Model

The training phase involves the iterative optimization of the model parameters to minimize classification error.

Supervised Learning Strategy

Loss Function: We employ Binary Cross-Entropy Loss for the classification task (Fake vs. Real). This penalizes the model heavily for confident but wrong predictions.

Optimizer: The Adam optimizer (Adaptive Moment Estimation) is selected for its ability to handle sparse gradients and adapt learning rates for different parameters, ensuring faster convergence compared to standard Stochastic Gradient Descent (SGD).

Hyperparameters:

o Batch Size: 32 or 64 (depending on GPU memory).

o Learning Rate: Initialized at 10^{-4}, with a decay scheduler to reduce the rate as the loss plateaus.

o Epochs: 50-100, with Early Stopping implemented to halt training if validation loss.

To ensure the model generalizes to unseen certificates:

Dropout: We insert Dropout layers (e.g., rate of 0.5) in the fully connected layers. This randomly deactivates neurons during training, forcing the network to learn redundant representations and preventing reliance on any single feature.

Cross-Validation: We utilize k-fold cross-validation (e.g., $k=5$) to ensure that the model's performance is consistent across different subsets of the data.

6. Evaluation

Evaluation must go beyond simple accuracy, especially in a fraud detection context where "fake" samples are the minority class.

A critical evaluation step involves testing the model against Adversarial Examples. We generate adversarial images using the Fast Gradient Sign Method (FGSM).

7. Interpretation of Results

AI in high-stakes decision-making requires explainability. We cannot rely on a "black box."
Grad-CAM (Gradient-weighted Class Activation Mapping): We implement Grad-CAM to generate heatmaps overlaying the certificate image. These heatmaps visualize the regions of the image that were most influential in the AI's decision. If the AI flags a document as "Fake," Grad-CAM might highlight the signature area in red, indicating that the pixel artifacts in that specific region triggered the detection. This allows human operators to verify why the document was flagged.
SSIM Difference Maps: The system outputs a difference image where black pixels represent a perfect match to the template and white pixels represent deviations. This provides an immediate visual guide to structural forgeries.

Applications and Implementation Details
The theoretical framework described above translates into practical software modules. We detail four specific applications: Text Extraction (OCR), Structural Verification (SSIM), Forensic Analysis (ELA), and Blockchain Integration.

Application 1: Text Extraction and Validation using OCR
Context:
The textual content of a certificate—the name, degree, and date—is the primary target for forgery. Fraudsters may alter a "Second Class" degree to a "First Class" by changing just a few distinct characters.
Mechanism:
We utilize the Tesseract OCR engine (wrapped in Python via pytesseract). Tesseract uses a Long Short-Term Memory (LSTM) recurrent neural network to recognize character sequences. By preprocessing the image with adaptive thresholding (Otsu's method), we isolate the text from the background noise. We then use Regular Expressions (Regex) to validate the extracted text against expected patterns (e.g., detecting if a date follows DD-MM-YYYY format).
Python Implementation (OCR):
Python

```
# Python Code for Text Extraction using OpenCV and Pytesseract
import cv2
import pytesseract
import re
def extract_and_validate_text(image_path):
"""
Extracts text from a certificate image and validates specific patterns.
"""
# 1. Load Image
image = cv2.imread(image_path)
# 2. Preprocessing
# Convert to grayscale to remove color noise
gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
# Apply Otsu's Binarization to separate text from background
# This creates a high-contrast black/white image
thresh = cv2.threshold(gray, 0, 255, cv2.THRESH_BINARY | cv2.THRESH_OTSU)
# 3. Text Extraction via Tesseract
```

```
# Configuration: --oem 3 (Default LSTM engine), --psm 6 (Assume uniform text block)
config = r'--oem 3 --psm 6'
extracted_text = pytesseract.image_to_string(thresh, config=config)
print("--- Extracted Text ---")
print(extracted_text)
# 4. Validation Logic (Example: Checking for specific degree types)
valid_degrees =
flag = False
for degree in valid_degrees:
if degree.lower() in extracted_text.lower():
flag = True
print(f"\n Degree type detected: {degree}")
break
if not flag:
print("\n No standard degree type recognized. Possible OCR failure or forgery.")
# 5. Regex validation for Certificate ID (Example Pattern: 2 letters - 8 digits)
id_pattern = r'[A-Z]{2}-\d{8}'
match = re.search(id_pattern, extracted_text)
if match:
print(f" Certificate ID found: {match.group(0)}")
else:
print(" Certificate ID format mismatch.")
return extracted_text
```

Application 2: Structural Similarity Index Measure (SSIM)

Context:

Every university certificate follows a strict template. Forgeries often deviate structurally—elements are misaligned or resized.

Mechanism:

We use the SSIM metric to compare the submitted document against a stored "Master Template." The SSIM algorithm operates on sliding windows across the image, comparing the local luminance, contrast, and structure. A score of 1.0 indicates a perfect match. A score significantly below 1.0 (e.g., < 0.90) flags the document for review. We utilize the scikit-image library for this computation.

Python Implementation (SSIM):

Python

```
# Python Code for Structural Similarity Analysis
import cv2
from skimage.metrics import structural_similarity as ssim
import imutils
def analyze_structure(template_path, suspect_path):
# Load images
template = cv2.imread(template_path)
suspect = cv2.imread(suspect_path)
# Convert to grayscale
```

```
template_gray = cv2.cvtColor(template, cv2.COLOR_BGR2GRAY)
suspect_gray = cv2.cvtColor(suspect, cv2.COLOR_BGR2GRAY)
# Resize suspect image to match template dimensions exactly
# (Note: In production, keypoint matching/homography would be used to align first)
(h, w) = template_gray.shape
suspect_gray = cv2.resize(suspect_gray, (w, h))
# Compute SSIM
# full=True returns the structural similarity image (diff map)
(score, diff) = ssim(template_gray, suspect_gray, full=True)
diff = (diff * 255).astype("uint8")
print(f"Structural Similarity Score: {score:.4f}")
# Threshold the difference image to find contours of mismatch
thresh = cv2.threshold(diff, 0, 255, cv2.THRESH_BINARY_INV | cv2.THRESH_OTSU)
cnts = cv2.findContours(thresh.copy(), cv2.RETR_EXTERNAL,
cv2.CHAIN_APPROX_SIMPLE)
cnts = imutils.grab_contours(cnts)
# Draw red boxes around structural mismatches
output = suspect.copy()
output = cv2.resize(output, (w, h))
for c in cnts:
(x, y, w_rect, h_rect) = cv2.boundingRect(c)
# Only highlight significant differences
if w_rect > 10 and h_rect > 10:
cv2.rectangle(output, (x, y), (x + w_rect, y + h_rect), (0, 0, 255), 2)
return output
```

Application 3: Forensic Analysis via Error Level Analysis (ELA)

When a digital image is modified and re-saved (e.g., pasting a signature), the compression level of the modified region becomes asynchronous with the rest of the image. This is the digital equivalent of seeing a patch on a pair of jeans.

Mechanism:

ELA works by intentionally re-compressing the image at a known error rate (e.g., 95%) and subtracting this from the original. Regions that have already been heavily compressed (or compressed differently) will yield different error residuals. We generate these ELA maps and feed them into a CNN, which learns to classify the distinct "noise patterns" of forgery.

Python Implementation (ELA):

Python

```
# Python Code for ELA Generation
from PIL import Image, ImageChops
import os
def convert_to_ela_image(path, quality):
filename = path
resaved_filename = 'temp_resaved.jpg'
# 1. Open original image
im = Image.open(filename).convert('RGB')
# 2. Save it again at specific quality (introducing known compression)
```

```
im.save(resaved_filename, 'JPEG', quality=quality)
resaved_im = Image.open(resaved_filename)
# 3. Compute absolute difference between original and resaved
ela_im = ImageChops.difference(im, resaved_im)
# 4. Enhance the ELA image brightness for visibility
extrema = ela_im.getextrema()
max_diff = max([ex for ex in extrema])
if max_diff == 0:
max_diff = 1
scale = 255.0 / max_diff
ela_im = ImageChops.multiply(ela_im, scale)
# Clean up temp file
os.remove(resaved_filename)
return ela_im
```

Conclusion

The issue of identifying criminal academic certificates is no longer merely an administrative undertaking. It has now turned out to be a complicated computational problem requiring a multidisciplinary
approach. In our study, we have demonstrated that Artificial Intelligence or more precisely, Deep Learning and Computer Vision and Forensic Analysis can exhibit a potent defense against the increasing onslaught of credential fraud.
In our analysis, the deep-learning models including CNN and GCN are able to identify fraud with an accuracy above 97 per cent due to ability to identify possible or even slight statistical and structural anomalies that can be overlooked by human beings.
In addition to that, the Python implementation provided here demonstrates that such sophisticated techniques are not only available but can also be implemented using open-source libraries. We will thus suggest continuous observation and enhancement.
AI will work as a scable, smart filter of legacy and physical paper, and Blockchain will provide the immutable platform of the new generation digital credentials.

References

1. Shaikh, M., & Patil, D. (2022). Image Forgery / Tampering Detection Using Deep Learning and Cloud. IEEE.
2. Dongre, J. G., Tikam, S. M., Gharat, V. B., & Patil, K. T. (2020). Education Degree Fraud Detection and Student Certificate Verification using Blockchain. IJERT.
3. Reddy, G. A., Reddy, G. S., Rama Raju, C. S., Padmaja, D., & Sreenivasulu, J. (2025). Forgery Detection in Digital Media using Neural Networks. International Journal of Computational Learning & Intelligence.
4. Nasreen, M. T., Sekhar, L. C., & Salim, I. (2023). Image Forgery Detection Using Deep Learning Techniques – A Review. IJSRST.
5. Pukale, D. D., Kulkarni, V. D., Jagadale, P., Bagwan, J., & Sarmokdam, R. (2024). Image Forgery Detection Using Deep Learning. IRJAEM.
6. Parkavi, C., Karthika, M., Dhanush, M., Saran, S. M., Srinivas, A. (2025). Digital Image Forgery Detection. International Journal of Innovative Science and Research Technology

(IJISRT).
7. Mandawgade, A., Alisha, N. A., Verma, D., Shivkumar, R. G. (2025). Automatic Detection of Fraudulent Image and Documents Using Deep Learning. International Journal of Science, Engineering and Technology.
8. Karmakar, M. (2023). Offline Signature Recognition and Its Forgery Detection using Machine Learning Technique. IJEBM.
9. Shaji, B., A, R., Harikrishnan, S. R. (2024). Autosignature Verification and Forgery Detection Using Deep Transfer Learning. IJARSCT.
10. Reddy, G. A., et al. (2025). Forgery Detection in Digital Media using Neural Networks. IJCLI.
11. Shaikh, M. A., Patil, D. (2022). Image Forgery / Tampering Detection Using Deep Learning and Cloud. IJARCCE.
12. Ravikumar, C., Radha, M., Mahendar, M., Manasa, P. (2024). A Comparative Analysis for Deep Learning-Based Approaches for Image Forgery Detection. IJOSI.
13. Gao, Y., Chang, D., Yu, B., Qin, H., Chen, L., Liang, K., Ma, Z. (2025). FakeReasoning: Towards Generalizable Forgery Detection and Reasoning. arXiv preprint.
14. Liu, D., Dang, Z., Peng, C., Zheng, Y., Li, S., Wang, N., Gao, X. (2022). FedForgery: Generalized Face Forgery Detection with Residual Federated Learning. arXiv preprint.
15. Wu, H., Chen, Y., Zhou, J. (2023). Rethinking Image Forgery Detection via Contrastive Learning and Unsupervised Clustering. arXiv preprint.
16. Guillaro, F., Cozzolino, D., Sud, A., Dufour, N., Verdoliva, L. (2022). TruFor: Leveraging All-Round Clues for Trustworthy Image Forgery Detection and Localization. arXiv preprint.
17. Mandawgade, A., et al. (2025). Automatic Detection of Fraudulent Image and Documents Using Deep Learning. IJSET.
18. Kuri, M., Bokare, P., Dhuri, S., Inamdar, A., Gavande, P., Gupta, A. (2025). Legal Document Authentication and Verification System Leveraging OCR, NLP, and CNN. IJRASET.
19. Meena, R. (2024). AI-Based Signature Identification Model for Forgery Detection. (News / Patent, related to AI signature forensics)
20. IJNRD authors. (2024). Applications of AI-Based Image Forgery Detection in Media and Forensic Analysis. IJNRD.
21. International Journal of Current Research. (2024). Advanced Deep Learning Strategies for Image Forgery Detection using CNN Architectures. IJCR.
22. IJARSCT. (2023). Fake Education Document Detection Using Image Processing and Deep Learning. (Praba, Jeevitha & Abitha)
23. Dongre, J. G., Tikam, S. M., & Patil, K. T. (2020). Education Degree Fraud Detection using Blockchain. IJERT.
24. Thakare, N., Narad, S., & Surysvanshi, Y. (2024). Fake Certificate Detection using Blockchain. AIP Conference Proceedings.
25. Lutfiani, N., et al. (2022). Academic Certificate Fraud Detection System Framework Using Blockchain Technology. Blockchain Frontier Technology.
26. Isizoh, A. N., et al. (2021). Certificate Fraud Detection Using Artificial Intelligence Technique. International Journal of Research Publication and Reviews.
27. Yuan, et al. (2022). Malicious Digital Certificate Detection based on Graph Convolutional Networks. MDPI Applied Sciences.

28. Sari, W. P., & Fahmi, H. (2021). The Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning. Kinetik.
29. Marra, F., et al. (2018). A Survey on Deep Learning-Based Image Forgery Detection. (preprint / research repository)
30. Arivanantham, T., Shirsath, P., Sayyed, Z., Potdar, K., Sagar, S. (2025). Survey Report on Forgery Signature Detection System. IJRASSET.