

Digital Forgery Detection for Certificates and Documents Using Image Processing and AI

A. Mariam Aysath Minha

*PG Scholar, Department of Computer Science and Engineering
Mohamed Sathak Engineering College, Kilakarai, Tamil Nadu, India*

N. Balasubramanian

*Professor, Department of Computer Science and Engineering
Mohamed Sathak Engineering College, Kilakarai, Tamil Nadu, India*

K. Seeni Pulavar Pitchai

*Assistant Professor, Department of Computer Science and Engineering
Mohamed Sathak Engineering College, Kilakarai, Tamil Nadu, India*

Abstract

In the digital age certificate forgery and other official documents are a major menace to academic, corporate and legal organizations. Some of the traditional manual forms of verification can be inefficient, time consuming and subject to human error. The paper presents a Digital Forgery Detection System that combines Image Processing and Artificial Intelligence (AI) to classify elements that might be manipulated in digitized documents with high accuracy and is automated. The multi-staged framework used in the system has Optical Character Recognition (OCR) to analyze text and extract patch-level features as a way of identifying structural inconsistencies. The model can detect tampered signatures, logos, and seals specifically by employing Convolutional Neural Networks (CNNs) and feature-matching algorithms. The result is a forensic report that points to the existence of manipulated areas and a conclusive authenticity rating.

The architecture takes advantage of a hybrid architecture in the detection of minute pixel-level anomaly, including copy-move or splicing attacks, which are not always noticeable by the naked eye. Image inpainting can also be combined to enable the system to rebuild original backgrounds which can serve as a base to detect disturbed text or foreign objects. This two-layered verification provides that even advanced forgeries that imitate original fonts or textures are correctly identified as such.

Comparison of the algorithm with a wide range of real and fake certificates shows that the CNN-based classification is more accurate in comparison with traditional threshold-based algorithms. The system can be scaled and be depended upon by institutions to provide an objective, quantified authenticity score which can be used in institutional security. This study fills the void between forensic image and real-life document authentication and provides a strong defense against digital fraud.

OPEN ACCESS

Volume: 1

Issue: 2

January 2026 to June 2026

E-ISSN: 3108-3420



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Introduction

The digital age has greatly enhanced efficiency and accessibility in the academic, corporate and governmental realms through the proliferation of electronic certificates and documents. Nonetheless, this change has also prompted a fast rise in digital forgery, wherein bad actors can alter documents with the help of sophisticated editing programs.

These forgeries comprise inscriptions on text, signature, logos, and pixel-based structures and it is becoming harder to detect.

The conventional methods of checking in documents, such as manual checking and database checking are very inefficient and time consuming procedures which are likely to be affected by human error. Further, they cannot be effectively

used in identifying advanced manipulations like copy-move forgery, splicing, and recompression artifacts [6], [26], [35]. The initial studies of digital image forensics provided the basis on finding such manipulations through passive methods of detection.

The latest developments in Artificial Intelligence (AI) and deep learning have greatly enhanced the ability of forgery detection systems. Neural network-based methods and convolutional neural networks (CNNs) have been extensively used in identifying forged areas in images and documents [2], [4], [10]. Also, with the help of Optical Character Recognition (OCR) method it is possible to extract and verify textual data and identify inconsistencies in the content of the documents [8], [11]. OCR systems that are hybridized with deep learning models have been shown to be more accurate as they combine both text and visual processing [19], [22].

Moreover, the recent methods like edge-based neural patterns feature extraction, multi-modal neural network, and transformer-based models have improved the detection of subtle and sophisticated forgeries in documents [10], [21], [22]. These innovations underscore the need to come up with smart, computerized applicants that can perform real life document verification tasks.

Problem Statement

The swift development of the use of digital documents has prompted a tremendous rise in forging of certificates and documents, which is threatening to academic, corporate, and legal systems. The current verification techniques can be quite ineffective, as they cannot reveal small manipulations, including textual ones, signature forgeries, and pixel manipulations [6], [29]. Most of the existing methods concentrate on either the textual or visual analysis but do not have a single framework that is used to detect all the information together [8], [11].

Moreover, the majority of systems offer poor results with no in-depth forensic evidence and cannot be used to process a great number of documents [9], [25]. The lack of built-in and scalable solutions decreases the trustworthiness of the document authentication procedure. Consequently, it is necessary to have an automated and integrated system capable of properly identifying various forms

of forgeries and offer credible authenticity analysis [2], [4].

Objectives of the Study

- Key Performance Indicators: The project aims to create an automated framework of AI-based detection of digital forgery in certificates and documents through image processing.
- In order to use Optical Character Recognition (OCR) to extract and verify textual information in documents [8].
- And close To apply deep learning models, like Convolutional Neural Networks (CNNs), to analyze signatures, logos, and visual features [2].
- To perform textual and visual analysis to detect multi-mode forgery correctly [4].
- To produce forensic reports containing authenticity scores to verify documents with authenticity [9].

Literature Review

The Digital forgery detection is no longer a traditional image processing method like edge detection, noise analysis, and copy-move detection, but rather an advanced AI-based processing method. Early detection approaches worked on detecting pixel-level anomalies in images, but failed to detect more complicated and high-quality forgeries [26], [35].

The development of deep learning has enabled the use of Convolutional Neural Networks (CNNs) and similar models to enhance detecting forged areas by acquiring intricate visual patterns [2], [4], [10]. In addition, Optical Character Recognition (OCR)-based methods are widely used for detecting textual inconsistencies in documents [8], [11], [19].

Recent studies focus on hybrid methods which unite textual and visual analysis such as signature check and multi-modal models to provide higher quality forgery detection [14], [15], [22]. Nevertheless, several issues like expensive computational cost and the absence of integrated systems remain, which indicates the necessity of an overall solution.

Related Work

The problem of digital forgery detection has been a subject of considerable research because the number of forged documents is rapidly expanding in academic, professional, and legal spheres. The current studies are primarily concerned with the analysis of either text or the analysis of images, but little work is done on the multi-modal systems. The text based techniques mainly utilize Optical Character Recognition (OCR) to extract and analyze the content of documents. Text comparison, semantic analysis, and similarity measures are among the techniques that are used to identify anomalies such as font changes, spacing problems, and altered text. Such techniques are successful in finding content-based manipulations but cannot recognize visual forgeries, like signatures and logos, [8], [11], [19].

Image processing and deep learning-based systems are visual analysis-based systems, which are used to identify forgery of signatures, logos, and pixel-level localities. Convolutional Neural Networks (CNNs), Siamese networks, and Error Level Analysis (ELA) are among the popular methods to detect graphical manipulations and image inconsistencies [2], [12], [14]. Although these methods are very effective in identifying visual tampering, they have drawbacks in the analysis of textual content within documents.

In order to eliminate these constraints, recent research suggests hybrid methods that will integrate textual and visual analysis. Two-stream systems that combine OCR and CNN models are also known as multi-modal systems, and they are more accurate since they can identify textual and visual forgeries at the same time [16], [22]. Nevertheless, such systems can be costly in terms of computational requirements and both size and size of labeled datasets, which underscores the necessity of a scalable and efficient integrated system.

Proposed System

The Objective of the Proposed System is to Identify Digital Forgeries in Certificates And Documents With The Help of a Complex Ai + Image Processing Pipeline. the Architecture Combines Several Modules, Such As, Ocr, Image Inpainting, Patch Extraction, Web Entity Detection, and Classification Networks.

System Architecture



Figure 1 Overall System Architecture

Optical Character Recognition (OCR)

OCR is an important component of document forgery detection as it allows one to extract and analyze textual information on scanned certificates. It helps to detect the abnormalities like typographical errors, font changes, inconsistent spacing, and text omissions or alterations, which are typical signs of fraud. This is because OCR-based methodologies are extensively used in AI-based document verification systems because they can identify textual manipulations [8], [11].

The methodology starts with the preprocessing in which the input document is first turned into grayscale to make further processing simpler. The use of tools like OpenCV to enhance visibility of text is achieved by image enhancement techniques like thresholding and noise removal. Also, skew correction can be carried out to put the document in the right position, so that the text can be extracted accurately.



Figure 2 OCR Pipeline

After preprocessing, OCR engines like Tesseract are used to extract the text which transforms the image of the document to a machine-readable one. In addition to the extracted content, there is an analysis of textual features like font type, font size, and spacing that aid in detecting anomalies.

Table 1 Sample OCR Anomaly Detection Output

Field	Extracted Text	Reference Text	Status
Name	“John Doe”	“John Doe”	Genuine
Date of Issue	“15/01/2023”	“15/01/2022”	Tampered
Certificate ID	“CERT-00123”	“CERT-00123”	Genuine

Lastly, the extracted text is compared to the reference templates or existing data performed through textual analysis. The methods of identifying differences include Levenshtein distance, cosine similarity, or sophisticated language models such as BERT embeddings. These techniques are more effective in detecting the existence of subtle tampering of text and intensify the effectiveness of document authentication systems in general [19].

Image Inpainting

Image inpainting is a significant technology in digital forgery detection, which is applied to point out areas that have undergone cloning, removal or image splicing. It is also useful in re-creating missing or altered pixel areas, which can be further examined as possible tampering. The techniques based on inpainting are especially applicable to copy-move and splicing forgeries that frequently appear in the manipulated documents [6], [12].

The inpainting procedure includes the identification of suspicious areas and the re-creation of the areas with the help of computational methods. A common method is the openCV-based inpainting, and it involves the filling of the missing or distorted regions on an image using mask-based region filling. Comparing the original image to the inpainted one, it is possible to detect anomalies in the distribution of pixels, which can be used to detect areas of manipulation.

Generative Adversarial Networks (GANs) are another developed method of inpainting. GAN-based models are useful in identifying subtle and high-quality manipulations by creating realistic content to complete missing areas by learning complex image patterns. These methods improve the ability of forgery detection systems to detect tampered areas which are not readily visible to the naked eye [20], [26].



Figure 3 Image inpainting pipeline

Image Patch Extraction

Image patch extraction is one of the major methods in document forgery detection targeting the detection and analysis of Regions of Interest (ROIs) including signatures, logos, and stamps. Rather than the whole document, this method breaks the image down into smaller patches hence lowering the computational complexity and enhancing the detection efficiency. The system is able to conduct more detailed and accurate analysis on potential tampering by isolating critical regions [2], [33].

Using Faster C-RNN



Figure 4 Faster R-CNN Patch Extraction

Faster R-CNN is a popular deep learning-based object detector model to detect ROIs in document images. It identifies significant features like signatures, seals and logos through creation of bounding boxes around them. The identified regions are then cut to single patches to be analyzed further. Every extracted patch is then passed through a Convolutional Neural Network (CNN) classifier to classify the authenticity of the extracted patch depending on the trained visual features. This method improves the precision of the forgery detection method by concentrating on the most important document parts [4], [22].

Using Detectron

Detectron is a novel framework of object detectors that are applied to document images to localize objects with high precision, allowing the fine-grained features to be extracted with deep learning.

It is also useful in identifying slight differences like faint logos, small stamp alteration and slight signature differences and this makes it quite useful in identifying complex forgeries more precisely as compared to the traditional methods [10], [22].

Web Entity Detection

The veracity of the logos, seals and QR codes is checked by matching them with known online sources through web entity detection. It assists to determine the forged or modified visual components of documents.

It is carried out by extracting different entities like logos or QR code and comparing them with reference images using feature matching algorithms such as SIFT and ORB. Any discrepancy is notified as a possible tampering, enhancing the accuracy of forgery detection mechanisms [6], [22].

Single Stream Forgery Classification

Single-stream forgery classification is a classification method where the entire certificate is a single input to a deep learning model. The document is analyzed with a Convolutional Neural Network (CNN) or ResNet model and provides a score on how likely the document is forged. The procedure consists in downsizing the certificate image to a common size (e.g., 224 x 224 or 256 x 256), and inputting it into a transfer-learned CNN / ResNet model. The model then delivers a binary prediction (genuine or forged) or a probability score showing authenticity [2], [4].

Double Stream Forgery Classification

Two-stream forgery classification involves a combination of textual and visual analysis to be stronger in detection. The architecture comprises two parallel streams one text and the other image stream. The text stream uses NLP embeddings and fully connected layers to process features extracted with OCR, whereas the image stream uses CNN/ResNet models to process ROI patches. The results of the two streams are combined with a dense layer to produce the final authenticity score.

This method allows the detection of both textual and visual forgeries and detailed tampering analysis, module by module. It is also more accurate than single-stream techniques and can be applied to the complex task of verifying documents [16], [22].

Forensic Report Generation

The forensic report generation module gives a comprehensive report on forgeries that are detected. It produces visual heatmaps of areas that have been tampered in the document and has module-level text, logo, and signature scores of confidence. The end report is exportable in the form of PDF and thus suitable to be verified, audited as well as used in legal matters [9], [25].

Experiment and Results

To test the proposed system, a database of scanned certificates and documents which included genuine and forged samples was used. In the experiments, the effectiveness of the multi-modal forgery detection methods including textual analysis, signature verification, logo/seal detection and pixel-level analysis were evaluated.

Analysis of Textual Data : Textual data analysis was conducted to identify anomalies like typographical mistakes, data omissions, font variances, and spacing anomalies. Using the Tesseract OCR engine, text was copied out of scanned certificates. The text obtained was then tested against predefined original document templates to detect the differences. The effectiveness of the process of the anomaly detection was evaluated with the help of such measures as accuracy, precision, recall, and F1-score.

Signature verification : The CNN based model was used to identify forged signatures with a set of 500 authentic and 200 forged signature samples. The images were first processed by making them 224x224 pixel images and turned them to grayscale. A Siamese network architecture was used to train the model by comparing input signatures with reference samples. Accuracy, precision, recall and F1-score were considered to measure the performance of the model. The experimental results reached the accuracy of 96.8, the precision of 97.2, the recall of 96.5, and the F1-score of 96.8 which is a positive indicator of the usefulness of the proposed method in signature forgery detection.



Figure 5 Example Detected Signature Forgery



Figure 7 Pixel-Level Forgery Detection Example

Logo/Seal Detection: Object detection was used to detect tampering in logos, stamps or seals on certificates. Logos and seals were recognized by means of Faster R-CNN and Detectron2 and the respective regions of interest (ROIs) were extracted. The identified elements were further matched with reference images that were sourced officially to detect inconsistencies. The findings revealed that 92% of the test images were localized successfully with tampered logos and seals. Besides, smaller manipulations, including minor adjustments of the logos and changes in colors, were successfully identified with the help of Detectron2.



Figure 6 Logo/Seal Detection Example

Pixel Level Detection: Advanced image forensics techniques were used to identify subtle manipulations that would have remained undetected by the human eye, such as copy-move, inpainting and splicing. The recompression artifact was determined by Error Level Analysis (ELA), and the inconsistency of noise and GAN-based anomaly detection were used to identify further irregularities. The regions that were manipulated in the images were visualized using heatmaps. The accuracy and precision of the results (97.5 and 98 respectively) and the recall (96.8) and F1-score (97.4) indicated the usefulness of the method in identifying fine-grained manipulations of images.

Multi-Modal Fusion and Overall System performance: The output of the textual, signature, logo/seal and pixel level analysis modules was integrated to give a holistic assessment. The final authenticity score of the document was then obtained by applying a two-stream classification approach.

Table 1 Overall Results, Module-wise Performance Metrics

Module	Accuracy	Precision	Recall	F1-score
OCR/Text Analysis	94.5%	93.0%	95.0%	94.0%
Signature Verification	96.8%	97.2%	96.5%	96.8%
Logo/Seal Detection	92.0%	91.5%	92.0%	91.7%
Pixel-level Detection	97.5%	98.0%	96.8%	97.4%
Overall System	98.2%	98.5%	96.5%	97.5%

The individual accuracy of pixel-level analysis was the highest of all modules. The use of signature verification was found to be essential in the detection of good quality forgeries. The classification approach which was based on two streams greatly enhanced the overall detection accuracy. Moreover, the created forensic reports were able to display successfully the areas of tampering such as textual information, signature, logos, and manipulations involving pixels.

Example Forensic Report : The certificate image was manipulated to draw attention to tampered areas, using textual anomalies in red, signature mismatches in yellow, logo mismatches in blue, and heatmap overlays were used to view pixel level manipulations. These identifications were then complemented by

computation of confidence scores, which were then applied to come up with the ultimate authenticity decision of the document.

Module Performance Summary				
OCR/Text Analysis	94.5%	93.0%	95.0%	97.8%
Signature Verification	96.8%	97.2%	96.5%	96.8%
Logo/Seal Detection	92.0%	91.5%	92.0%	92.7%

Figure 8 Sample Forensic Report

The system proves to be very effective in all modules. It is even more suitable to legal verification because of the visualization, heatmap, and module-based reports. The multi-modal two-stream fusion model is more efficient than the single-stream CNN models. Moreover, the system offers module-level in-depth insights, which are helpful to gain a full forensic reporting.

Table 2 Sample Forensic Report Module Scores

Module	Confidence (%)	Tamper Status
OCR/Text Analysis	95	Genuine
Signature Verification	97	Forged
Logo/Seal Detection	92	Genuine
Pixel-level Detection	98	Forged
Overall Authenticity	96.5	Forged

Digital Forgery Detection Dataset

The quality and diversity of the dataset is a limiting factor to the effectiveness of any AI-based system of forgery detection. In this project, a large set of scanned certificates was created to train, validate and test the proposed model.

Dataset Composition: The dataset will be a combination of real and faked certificates and with different degrees of tampering to resemble real world conditions.

Table 3 Dataset Statistics

Category	Count	Description
Genuine	500	Original, unaltered certificates collected from universities, schools, and organizations
Forged	350	Digitally altered certificates with modifications in signatures, logos, and textual content
Total	850	Combined dataset for training, validation, and testing

Pie chart showing Genuine (59%) and Forged (41%) certificates.



Figure 9 Dataset Composition Pie Chart

Forgery Types Included

Textual Manipulations: Typographical errors, addition or removal of words, and changes of dates or certificate identification numbers are among the textual manipulations. It also entails the changes in font type and font size to create realistic forgeries.

Signature Forgeries: Signature forgeries are hand-edited or digitally pasted signatures, and can have differences in stroke patterns, orientation %

scale.

Logo/Seal Tampering: Logo or seal tampering is the manipulation of organizational logos or stamps e.g. changing color, size or placement.

Pixel-Level Tampering: The techniques of pixel-level tampering include copy-move and inpainting to remove or duplicate elements, or adding noise or compression artifacts to make something appear more authentic.



Figure 10 Sample Forgery Examples

Grid of 4-6 Image Certificate

- Row 1: Genuine certificates
- Row 2: Forged certificates with the areas of tampering highlighted (signatures/logos/text highlighted in red)

Data Preprocessing: The following preprocessing steps were used before feeding images into the AI pipeline:

1. Grayscale Conversion: Converts color certificates to grayscale to analyze them in OCR and pixel-by-pixel detail.
2. Noise Removal: Median and Gaussian filters to eliminate scanning artifacts.

3. Skew Correction: Text and logos alignment of rotated or scanned images.
4. Normalization & Resizing: Normalized all images to 224x224 or 256x256 image size in CNN input.

Data Augmentation: Data augmentation was used in order to enhance model robustness and generalization. This featured geometric (rotation, flipping, scaling, translation), color (brightness, contrast, saturation), noise (Gaussian and salt-and-pepper), and elastic transformations to produce effects of scanning distortions.

Table 4 Augmentation Summary

Technique	Purpose	Example Effect
Rotation	Simulate scanning misalignment	Certificate rotated $\pm 10^\circ$
Scaling	Test model invariance to size	Slight enlargement/reduction
Noise Injection	Simulate low-quality scans	Grainy texture added
Color Adjustment	Vary lighting conditions	Brightness/contrast altered
Elastic Transform	Simulate warp/fold	Minor text/line distortion

Dataset Splitting: To achieve proper evaluation of the model, the dataset was split into 70% (595 images) and 15% (128 images) and 15% (127 images) respectively.

Table 5 Train/Validation/Test Split

Dataset	Genuine	Forged	Total
Training	350	245	595
Validation	75	53	128
Testing	75	52	127
Total	500	350	850

The dataset is represented by various types of forgery to increase the robustness of the model. The methods of data augmentation enhance generalization of the AI models. OCR, CNN, and patch-based analysis requires standardized input, which is achieved by proper preprocessing. Also, dataset division allows fair and trustworthy testing within various modules, such as text, signature, logo, and pixel-level recognition.

Conclusion

The suggested forgery detection system based on digital signatures illustrates the power of multi-modal AI and image processing algorithms as

a means of automated certificate verification. Combining OCR-based textual analysis, visual feature detection (logos, stamps, and signatures), pixel-level tampering detection, and a two-stream classification architecture, the system offers a holistic solution to detecting forgery. According to experimental results, the accuracy is high across the modules, with 94.5% in text analysis, 96.8% in signature verification, 92.0% in logo/seal detection and 97.5% in pixel-level detection, with the overall system accuracy being 98.2%.

The multi-modal model improves the detection performance of the system as it integrates both textual and visual features, allowing subtle manipulations to be identified, as well as detailed forensic reports regarding each individual module. The system considerably minimizes manual verification efforts since it automates the verification process and offers visual confirmation like heatmaps and highlighted anomalies. Moreover, its modular structure guarantees flexibility and scalability so that it can be easily integrated with new functionality and institutional processes. In general, the suggested hybrid solution is more reliable and effective than the traditional systems that rely on a single mode.

Limitations of the Current System

Despite the high accuracy of the proposed system, there are a number of limitations:

Computational Complexity

Multi-stream analysis and patch extraction is a computationally expensive task, especially when dealing with large amounts of certificates.

Limited Language Support

The present OCR and NLP modules only support English restricting the usefulness of the system to non-English certificates without further training.

Signature Reference Dependency

The signature verification will only be accurate when true reference signatures are available.

Dataset Size Constraints

The system is trained with a rather small dataset of 850 certificates; even better results can be achieved with larger and more varied datasets.

Future Work

To enhance the system scalability, accuracy, and applicability, a number of improvements can be done:

Ensemble CNN Models to be More Accurate: CNNs prediction can be enhanced by adding further CNNs like ResNet, DenseNet, and EfficientNet to perform better in tricky forgery instances and achieve higher accuracy.

Blockchain Integration: It can be used to store certificate authenticity data and tamper-proof logs on blockchain to allow safe and irreversible verification history to institutions and individuals.

Mobile Application Deployment: Android and iOS applications can be created to help verify certificates in real time with smartphone cameras, and thus be validated on the spot.

Multilingual Certificates Support: Multilingual OCR and Multilingual NLP modules should be supported to make it global.

Institutional Workflow API: API can be offered to achieve a seamless integration with university, banking, and government systems, automating verification processes.

Cloud and Edge Integration: Large-scale batch processing and centralized storage can be facilitated

by cloud-based deployment, and low-latency and offline verification can be supported by edge computing.

Synthetic Forgery Generation as a Training Method: GANs can be used to generate synthetic forgeries to generate more diverse datasets and enhance model generalization.

Explainable AI (XAI) in Forensic Reporting: The implementation of XAI methods can be used to gain insight into the characteristics that can be used to detect tampering to enhance transparency and trust when using AI in legal and institutional contexts.

References

- AI-driven document forgery detection using OCR and Levenshtein text comparison. (n.d.). *International Journal of Communication & Information Technology*.
- Birajdar, G. K., & Mankar, V. H. (n.d.). Image forgery detection using passive techniques: A survey.
- Copy detection pattern: *Authentication codes for printable documents*. (n.d.).
- Digital forgery in the age of misinformation: Reliable image manipulation detection*. (n.d.). Journal of Digital Security and Forensics.
- EdgeDoc: *Hybrid CNN-transformer model for accurate forgery detection in ID documents*. (n.d.). arXiv.
- Farid, H. (2009). Image forgery detection. *IEEE Signal Processing Magazine*.
- Hyperspectral document forgery detection using deep feature extraction (CAE-LR). (n.d.). ScienceDirect. *Image forgery detection: Digital investigation and passive techniques review*. (n.d.).
- Identity documents authentication based on forgery detection of guilloche pattern*. (n.d.). arXiv.
- Image forgery detection: A survey of recent deep learning approaches. (n.d.). *Multimedia Tools and Applications (Springer)*.
- Koul, M., et al. (n.d.). *Efficient copy-move image forgery detection using CNN*. Springer.
- Liao, X., et al. (n.d.). *CTP-Net: Character texture perception network for document forgery localization*. arXiv.
- Mankar, V. H., & Gurjar, A. (2015). *Image forgery types and detection review*.

- Murphy, et al. (n.d.). *Image generation and learning strategy for deep document forgery detection*. arXiv.
- Ni, R., et al. (n.d.). Evaluation of deep learning-based image forgery detection approaches. *IEEE Access / Journal of Imaging*.
- Questioned document examination (QDE): *Forensic methods for disputed documents*. (n.d.).
- Shivakumar, B. L., & Baboo, S. S. (2010). Detecting copy-move forgery in digital images. *Global Journal of Computer Science & Technology*.
- Wang, J., et al. (2009). Fast and robust forensics for image region-duplication forgery. *Acta Automatica Sinica*.
- Zheng, T., & Zhang, Z. (n.d.). Survey on image tampering and detection. *Journal of Visual Communication and Image Representation*.