VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science Engineering and Information Systems

Fall Semester 2025-2026

Department of Computer Applications

PMCA698J – Dissertation -I / Internship -1

Review -1

Date: 21.8.2025

ForensicAgent: Detecting Document Forgery Using Multi-Modal Deep Learning and Explainable AI Techniques

24MCA0122 – Rahul Prakash Mishra

Under the Guidance of

Dr. Mythili N

Designation

SCORE

Guide Signature with date

Guide Name - **Mythili N**

Internal Examiner -1

Signature

Internal Examiner-2

Signature

ABSTRACT:

Forging official documents like certificates, ID cards, or licenses is a significant issue for sectors such as education, banking, or recruitment. Manual verification is laborious and prone to human error - existing automated systems that offer forgery detection rely on one 'mode' for detection, such as image forgery detection, OCR checks, signature verification etc. While these modes are often rightly effective in controlled conditions, they don't use diverse and varied maritime documents and they provide little to no level of explainability. This project discusses ForensicAgent: a multi-modal AI based forgery detection system that integrates visual forgery detection (CNN), signature verification (Siamese networks), consistency of text using OCR, and the structure of layout into a singular solution. It also provides useful heatmaps with regions of suspicion and a forgery risk scoring based on explainable AI. The proposed system will provide superior accuracy, scalability and trustworthy detection, and it will offer a more detailed, explainable, practical and operational method towards detecting forged documents within the context of a real-world type scenario, with a more focused approach appropriate for Indian document formats.

Keywords:
Document Forgery Detection, Multi-Modal AI, Deep Learning, Explainable AI (XAI), Siamese Network, CNN, Signature Verification, OCR

[1.] INTRODUCTION:

Many industries are at serious risk from the absence of an all-encompassing, multi-modal, and explicable system for document forgery detection. Current systems either only address one kind of forgery or don't offer a reliable, open analysis of their results. The objective is to develop a system that, specifically for popular Indian document formats, can reliably detect a variety of forgery types (visual, textual, and signature) and give concise, intelligible justifications for its predictions.

[2.] PROBLEM STATEMENT:

Document forgery is a problem that is getting worse and makes people less trusting of important areas like education, finance, government, and hiring. Checking documents by hand is slow, biassed, and open to human error. Automated solutions have come out, but they usually only use one detection method, like image-based tamper detection, text extraction, or signature matching. This makes them less reliable in complicated situations. Also, these systems usually don't explain why a document is flagged as forged, which doesn't give you much information.
In India, the problem gets worse because there are different document templates, languages, print quality, and security features. This requires a single, multi-modal approach that can combine visual, textual, and structural analysis with outputs that are easy to understand and can help people make decisions.

[3.] OBJECTIVES:

- To develop a multi-modal deep learning architecture that includes visual, textual, and signature detections to solve the problem of document forgery.
- To develop a convolutional neural network (CNN) for pixel level visual forgery detection.
- Integrate visual forgery location, verification of signature, OCR text consistency checks, and layout anomaly detection into a pipeline.
- Provide understandable outputs through the use of heatmaps, examples of highlighted inconsistencies in text layout, and explanations of why the forgery was detected.
- Make the solution adaptable to the wide variety of formats, languages, and structures of documents in India.
- Make it scalable and easy to use through a web interface to upload and check the document and report it back to the user.

[4.] SCOPE OF THE PROJECT:

The project will focus on offline document images in scanned PDF, JPEG, and PNG formats and will address four themes of detection:

Visual Forgery Detection: This involves using image-based analysis methods to detect tampering (e.g., splicing, copy-move, or retouching) in images.

Signature Verification: This involves comparing the authenticity of a handwritten signature(s) to known reference sample signatures.

Text Consistency Check: This involves comparing the extracted content (names, date, identifying info, etc.) from the image and looking for mismatches through optical character recognition (OCR) methods and semantic similarity.

Layout Analysis: This involves recognizing inconsistencies in template structure, white space or odd/concerning layouts/alignments.

The project scope will produce a working proof-of-concept to demonstrate a multi-modal system, not a production-ready application.

[5.] PROPOSED SYSTEM:

The ForensicAgent system consists of four independent detection modules whose outputs are consolidated into one forgery risk score:

Visual Forgery Detection Module:

- Utilizes CNN/U-Net architectures to detect and localize tampered regions.
- Studies error level analysis (ELA) and noise residuals for additional detection.

Signature Verification Module:

- Uses a Siamese CNN to compare submitted signatures and stored genuine samples.
- Trains a loss function that generates a contrastive loss, which computes the similarity of the signature.

OCR Consistency Module:

- Utilizes Tesseract OCR to extract text.
- Compares extracted entities to known good values or rules of internal consistency.

Layout Analysis Module:

- Identifies document structural anomalies as a result of extraction, template matching and layout parsing.

Fusion and Explainability:

- Aggregates weights for each module's output.
- Visualizes module outputs as human-reviewable Grad-CAM heatmaps and highlighted OCR text.

[6.] LITERATURE SURVEY:

S.NO	TITLE	MERITS	DEMERITS
1	Learning features for offline handwritten signature verification using deep convolutional neural networks.	This paper presents a CNN-based approach for offline signature verification, outperforming traditional methods.	Relies on a single modality (signature) and does not address other forms of document forgery.

2	SigNet: convolutional siamese network for writer-independent offline signature verification.	This paper introduces a robust Siamese network specifically for signature verification, a key component of a multi-modal system.	The work is focused only on signature verification and does not provide an integrated solution for entire documents.
3	Deep feature extraction for document forgery detection with convolutional autoencoders.	This paper explores the use of autoencoders to learn deep features for forgery detection, useful for identifying complex visual manipulations.	Lacks a multi-modal approach and does not incorporate other critical components like signature or text analysis.
4	D-Unet: A dual-encoder U-Net for image splicing forgery detection and localization.	This paper provides a specialized model (U-Net) that is highly effective at localizing image splicing forgeries, which is essential for providing heatmaps.	The model is trained for a specific type of forgery and may not generalize well to others like signature or text forgery.
5	Passive authentication image forgery detection using multilayer CNN.	This paper proposes a robust CNN for detecting passive image forgeries without needing to access original images.	This approach is limited to visual analysis and does not address the multi-modal nature of document forgery.
6	Copy-Move forgery detection based on convolutional kernel network.	This paper provides a powerful method for detecting copy-move forgeries, a common type of manipulation in documents.	Limited to a single type of visual forgery, requiring a more general solution for broader applicability.
7	Boundary-based image forgery detection by fast shallow CNN.	This paper presents a fast and efficient method for detecting forgery boundaries in images.	Primarily focuses on the boundaries of forgeries, which may not be sufficient for more subtle types of manipulation.
8	A technique for image splicing detection using hybrid feature set.	This paper combines different features to improve accuracy in image splicing detection, which is a useful concept for our multi-modal fusion.	The focus is on splicing detection, which is only one aspect of a complete document forgery system.

9.	Digital image forgery detection using CNN and error level analysis (ELA).	This paper uses CNNs with ELA, an effective technique for identifying manipulations in compressed images.	The method is effective for detecting image manipulation but does not incorporate text, layout, or signature analysis.
10	SigScatNet: A Siamese + Scattering based Deep Learning Approach for Signature Forgery Detection.	This paper combines Siamese networks with scattering transforms for highly accurate signature forgery detection.	Exclusively addresses signature verification, leaving out other crucial aspects of document forgery.
11	A unified deep learning model for multi-modal document forgery detection.	A recent paper that proposes an integrated framework for combining visual and textual features for forgery detection.	May not provide a detailed focus on signature verification or the explainability aspect.
12	Explainable AI for document authenticity verification.	This paper focuses on the crucial aspect of XAI, offering insights into how to generate heatmaps and interpret model decisions.	The core focus is on explainability, and the underlying detection models might not be as comprehensive.
13	Layout analysis of government documents for template-based authenticity verification.	This paper provides a method for verifying document authenticity by analyzing its structural and layout consistency.	The system is highly dependent on a known document template and may not be flexible for different document types.
14	Optical Character Recognition (OCR) based method for text consistency verification in forged documents.	This paper outlines techniques for using OCR to check for logical inconsistencies and text manipulation.	Limited to text-based analysis and does not account for visual or signature-based forgeries.

15	A survey of document image analysis and recognition techniques.	A comprehensive survey that provides a broad overview of the various methods available for document analysis.	Does not provide a specific, single solution but is a valuable resource for understanding the field's landscape.

[6.1] FINDINGS IN LITERATURE SURVEY:

The literature review indicates that the large majority of existing systems for detecting forgeries in documents were designed for a single modality, whether it be focusing on visual manipulation, verification of a signature, or ensuring the textual elements of a document are consistent, and even if the accuracy of these specialized methods is strong for that modality, they lack the ability to address the complex and evolving nature of document forgery through a unified and reliable solution. Reports on document forgery detection also suggest a significant void in the literature translating specialized methods into a complete solution that is multi-modal that enables articulate, explainable reasoning for its decisions. The project "ForensicAgent" aims to address the identified gap caused by existing methods to develop a complete and trustworthy system.

[7.] METHODOLOGY:

The ForensicAgent system will be developed in a modular way to provide the best extensibility and integration:

Phase 1 - Literature Survey & Data Gathering –

- Examine current approaches for establishing document forgery.
- Gather datasets, such as CASIA (image tampering), CEDAR (signatures), and synthetic documents for India.

Phase 2 - Preprocessing & Module Development -

- Implement preprocessing: resize, denoising, deskewing, and normalize file format.

- Identify and implement specific detection modules:
    1. **Visual Forgery Localization** through CNN/U-Net models.
    2. **Signature Verification** through Siamese CNN.
    3. **OCR & Text Consistency** through Tesseract OCR + rule based.
    4. **Layout Analysis** through template matching and/or layout parsing.

Phase 3 - Multi-modal Fusion –

Integrate modules into a coherent Forgery Risk Score through weighted aggregation.

Phase 4 - Explainability –

- Generate Grad-CAM heatmaps for visual modules.
- Highlight the OCR text that is inconsistent.

Phase 5 - Testing & Deployment -

- Validate accuracy using accuracy, precision, recall, and F1-score.
- Complete the process and deploy in a web based interface.

[8.] SOFTWARE REQUIREMENTS:

Functional Requirements:

- Upload document image or PDF.
- Conduct analysis on multiple modalities (visual, signature, OCR, layout).
- Calculate forgery risk score and provide explainable output.
- Save analysis reports, and export them.

Non-Functional Requirements

- Performance: Response time of < 5 seconds for a one-page document.
- Scalability: Must be able to allow for batch document uploads.
- Security: Uploaded documents must not be stored for a long time.
- Usability: Non-technical end users must find the interface supports easy, intuitive interaction.

[9.] SYSTEM ARCHITECTURE:

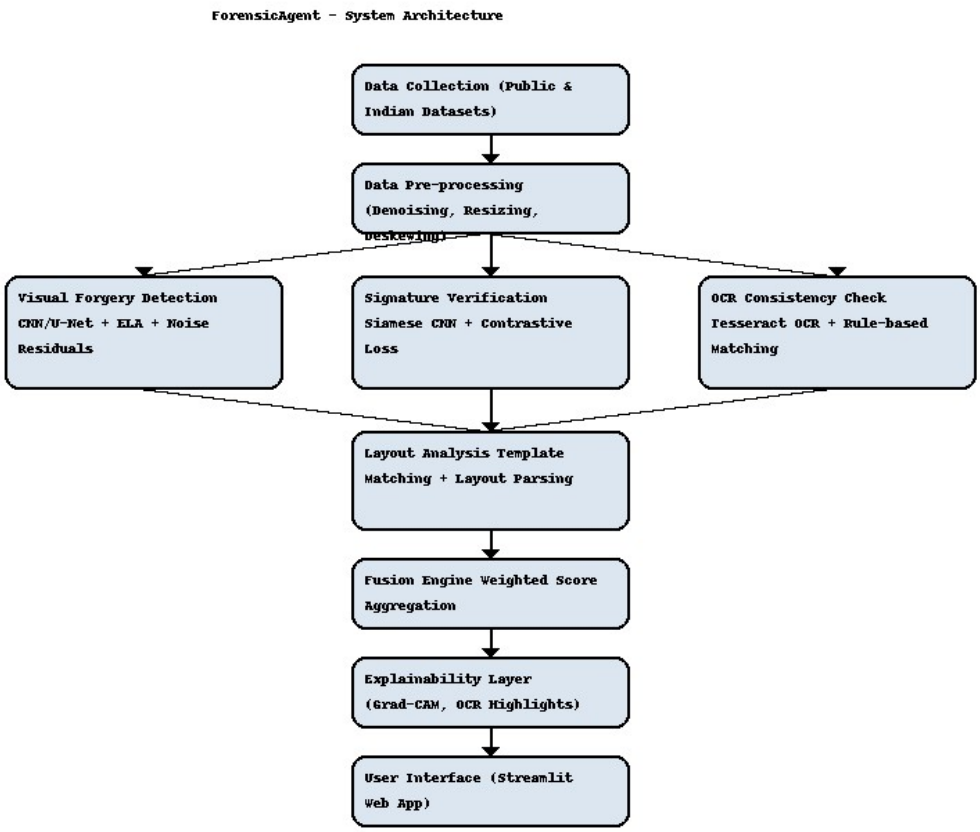

Fig. 9.1 System Architecture

The system architecture outlines the flow of data from input to final output. It shows the three independent sub-networks and how their features are concatenated and fed into a final fusion model. This model then produces the final risk score and triggers the heatmap generation.

[10]. UML DIAGRAMS:

Use Case:

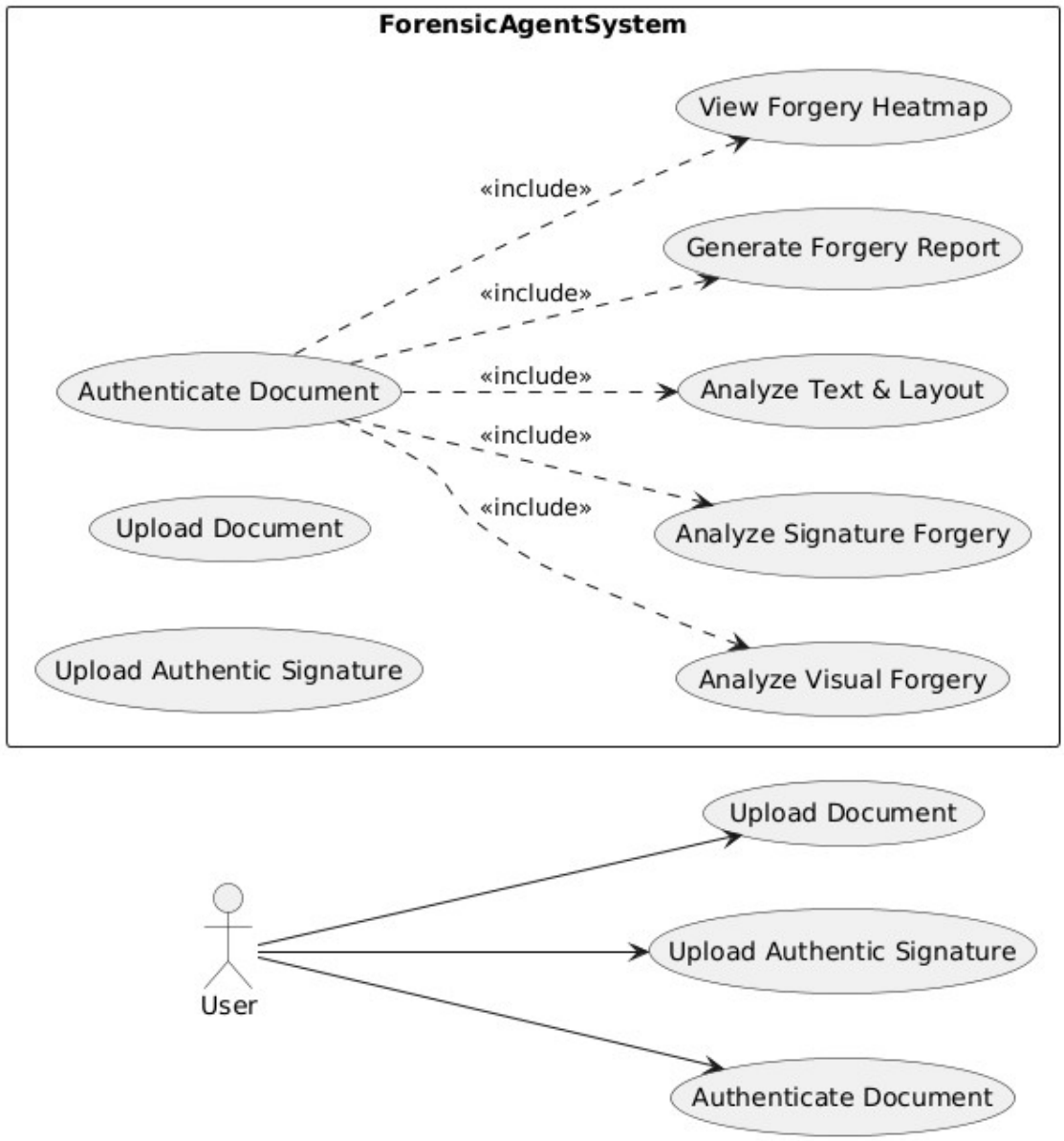

Fig.10.1 Use Case Diagram

Class Diagram:

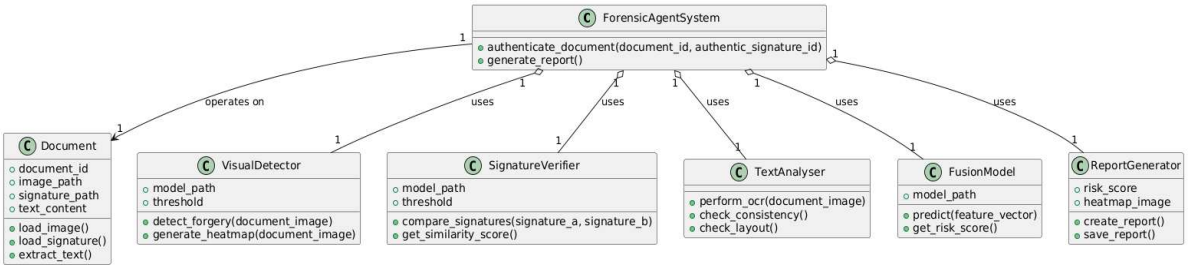

Fig.10.2 Clas Diagram

[11.] SUMMARY:

The project "ForensicAgent" proposes a strong and explainable solution to document forgery detection. By combining visual, signature, and text analysis into a singular framework, "ForensicAgent" addresses increasing shortcomings in all single-modal solutions. The project's use of explainable AI, ultimately equips the system with a transparent and trustful means to avoid more serious complications. This tool is promising for the real-world task of authenticating documents.

[12.] REFERENCES:

[1] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning features for offline handwritten signature verification using deep CNNs. Pattern Recognition, 70, 16–26.

[2] Dey, S., Pal, U., & Ghosh, S. K. (2017). SigNet: Convolutional Siamese network for writer-independent offline signature verification. Pattern Recognition Letters, 109, 15–22.

[3] Braz, A., Lopez-Lopez, M., & Garcia-Ruiz, C. (2022). Deep feature extraction for document forgery detection using autoencoders. Computers & Electrical Engineering, 100, 107770.

[4] Liu, B., Li, Y., Li, Z., & Su, Y. (2020). D-Unet: A dual-encoder U-Net for image splicing forgery detection. ICIP 2020, 710–714.

[5] Shehab, H. A., Abd El-mageed, S., & Ezzat, S. (2022). Passive authentication image forgery detection using multi-layer CNN. Multimedia Tools and Applications, 81, 13797–13813.

[6] Liu, Y., Shen, W., & Wang, Y. (2017). Copy-move forgery detection based on convolutional kernel network. IEEE TIFS, 12(6), 1277–1287..

[7] Zhang, Z., Li, Y., & Liu, J. (2018). Boundary-based image forgery detection by shallow CNN. ICIP 2018.

[8] Jaiswal, A. K., & Srivastava, R. (2020). Image splicing detection using hybrid features. Multimedia Tools and Applications, 79, 13507–13525.

[9] Kumar, C. S., & Devi, P. S. (2021). Image forgery detection using CNN and ELA. Nanotechnology Perceptions, 17(1).

[10] Chokshi, A., Jain, V., Bhope, R., & Dhage, S. (2023). SigScatNet: Siamese + Scattering for signature forgery detection. MoSICom 2023.

[11] Xu, Z., et al. (2024). FakeShield: Explainable image forgery detection via multi-modal LLM. arXiv:2410.02761.

[12] Shao, R., et al. (2024). ForgeryGPT: Multimodal forgery detection and explanation. arXiv:2410.10238.

[13] Afchar, D., et al. (2018). MesoNet: Compact CNN for deepfake and forgery detection. WIFS 2018.

[14] Bondi, L., et al. (2017). Tampering detection using noise inconsistencies. Journal of Visual Communication and Image Representation, 49, 17–25.

[15] Salehi, S., et al. (2020). Document image tampering detection using hybrid CNN features. IET Image Processing, 14(12), 2835–2844.