

ForenXAI: An Intelligent Deep Learning Framework for Forensic Document Verification and Forgery Detection for Police Evidence

S. Nandhini Devi¹, and Dr.N. Sabiyath Fatima^{2*}

¹Research Scholar, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, India.
nandhini_cse_phd_18@crescent.education, <https://orcid.org/0000-0002-0459-9853>

^{2*}Professor, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, India. sabiyathfathima@crescent.education, <https://orcid.org/0000-0002-8918-4306>

Received: September 12, 2025; Revised: October 21, 2025; Accepted: December 15, 2025; Published: February 27, 2026

Abstract

Forensic document authentication is used to identify fakes and verify police evidence and other legal documents, making detection and authentication part of forensic science. Existing approaches face issues about low generalizability and low interpretability of results, and inability to detect subtle amid manipulations or cross-modal inconsistencies. ForenXAI addresses this gap with a smart deep learning (DL) system that differentiates visual and textual forgeries through fused ResNet50-CBAM and LSTM with Attention. It cross-verifies using dual-stream cross-modal methods and performs risk assessment, SHAP-based interpretability, and XAI-derived probabilistic risk scoring. It structures the process within multi-stage pre-processing, image-text alignment, anomaly detection, and decision support to achieve legal accuracy. ForenXAI is optimized for system security and trust through real-time monitoring and evidence security, including auditable logs, encryption, and access control to forensic evidence and other sensitive data. Evaluation over multiple documents and signatures found the framework attains an accuracy of 0.9788 with MCC of 0.9576 and G-mean of 0.9788 at 70% training. This further improved to an accuracy of 0.9894 and MCC of 0.9788 at 80% training. Along with this, the framework attains an optimal F1-score of 0.9894. Comparative analysis across processing time, data precision, time taken to encrypt, delays in real time monitoring, and SHAP feature importance with Cycle-GAN, Ta-RNN, and NSVNN emphasizes ForenXAI's efficiency and interpretability. These findings affirm that ForenXAI is principled, highly interpretable, secure, and extremely practical for forensic applications, thereby endorsing the use of AI systems in the policing and judiciary frameworks.

Keywords: Forensic Document Verification, Forgery Detection, Cross-Modal Deep Learning, SHAP Explainability, Resnet50-CBAM, LSTM Attention, Dual-Stream Transformer, Risk Scoring.

1 Introduction

The modification of police reports, identification documents, and case files, among other forensic documents, is a growing concern due to digital changes, affecting the authenticity and credibility of law

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February - 2026), pp. 181-207.
DOI: 10.58346/JISIS.2026.II.011

*Corresponding author: Professor, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, India.

enforcement and court proceedings. Document authentication and forgery detection processes underpin evidence-based value and belief. There is growing interest and success in deep learning for image-based forgery detection and text anomaly detection, particularly with CNNs and transformer models for diagram neural networks in recent years. (Pham & Park, 2023).

Additionally, methods for combining image processing with explainable AI (XAI) and risk scoring have gained ground in legal and forensic applications (Yang et al., 2023; Anomah et al., 2021). While advances in forgery detection have been made in bridging the gap between visual and textual representation, some challenges remain unsolved. The introduction of digital technologies and the challenges that come with it have made the authenticity and safety of even the simplest legal documents extremely complicated. Indeed, there are legal documents, and there are legal documents. The importance of these documents in activities conducted by any law enforcement body is cardinal. Such documents, in case of loss or theft, are left vulnerable to forgeries, unauthorized strippings of security features, and cursory or rampant document tinkering. The growing and sophisticated nature of cyber-attacks adds to the complication of evidence and makes digitization of documents more vital. Current protocols aimed at evidence-image focused loss of forgery access to the system and security control of the transmitter domain and the evidence as primary or secondary issues (Ishihara et al., 2024). This research attempts to solve these problems by applying ForenXAI and more advanced protocols than the image of the forgery. Through the framework, these documents are systematically and controlledly monitored to be ceased from service and protected against digital forensics by unauthorized users (Fakiha, 2024). This will also ensure that the documents verified as ForenXAI remain unaltered and protected from the moment of ingestion to the endpoint decision-making phases, thus maintaining their authenticity and security (Balakrishnan & Leema, 2025).

First, most forgery detection models likely focus exclusively on visual or textual domains (very seldom are both cross-modally incorporated), and therefore, analyses will facilitate siloed reviews that may not lead to cross-modality inconsistencies (Jabeen et al., 2021; Jung et al., 2022). Second, most models with high accuracy and reliability are black boxes, lacking explainability for forensic examiners and court officers (Silva et al., 2022). Third, it is commonly recognized that model generalization is weak across datasets that differ in document quality, scripting style, and language (Khosroshahi et al., 2022). Fourth, although implemented modestly, few systems articulated probability risk scores that were related to the legal threshold or confidence (Longjohn & Smyth, 2024). Fifth, signature morphing or pixel-level tampering is difficult to detect when forgers are moving without artefacts and attempting subtle changes to existing signatures (Zeng et al., 2022; Fahad et al., 2023).

These gaps provide the impetus for us to develop a holistic forensic intelligence framework, ForenXAI, which is purposefully designed for police and legal quantum validation of digital records. The proposed system's combination of image processing that detects tampering; text anomaly detection that identifies semantic conflicts, two-stream intermodality comparison, and XAI-guided risk scoring, substantially reduces the siloed, non-transparent, and non-generalizable nature of current tools, while also providing police agencies and forensic laboratories what they require to develop accurate, interpretable, and scalable tools to discover deep forgeries of evidence despite the restrictions of real-world situations (Geistová Čakovská et al., 2021). In this paper, ForenXAI is presented, a hybrid deep forensic intelligence framework designed to enhance the reliability of digital forensic results. The architecture is based on a multi-phase pipeline that uses visual forgery detection, textual anomaly detection, and a dual-stream cross-modal study to test for inconsistencies in visual and textual modalities (Prabu & Sudhakar, 2022). A ResNet50-CBAM hybrid CNN is used to detect pixel-level tampering and forged signature morphing in scanned documents (Wu et al., 2025). An attention LSTM system is used

to find potential forensics inconsistencies and fictions within forensics texts. Text-image streams consistencies are performed by a dual-stream transformer model which encodes and scores handwritten records and their corresponding text summaries. The system is equipped with a shapley additive explanation (SHAP)-based explainability mechanism and probabilistic risk assessment support which improves their utility for legal and forensics practitioners. During 2021 to 2024, ForenXAI has been evaluated against numerous open-source datasets, proving to possess cross-domain generalizability, with significant advancements over state-of-the-art unimodal systems in accuracy, robustness, and interpretability. This research has the following contributions:

- Development of ForenXAI, a comprehensive DL pipeline that combines visual forgery detection, textual anomaly detection, and dual-stream cross-modal verification to increase accuracy, robustness, and interpretability in forensic signature verification and document forgery detection.
- Integration of SHAP-based interpretability for both visual and textual modalities, and a probabilistic risk scoring system for evidential evaluation, providing legally defensible and scientifically sound forensic results.
- Showcase of robust cross-domain performance, and performance superior to unimodal baselines when using sophisticated architectures (e.g., ResNet50-CBAM, LSTM with attention, dual-stream transformers) on a variety of real-world and open-source forensic datasets.

In Section 2, an overview of the researched literature on forensic signature verification and document forgery detection will be covered. In Section 3, the proposed methodology of ForenXAI will be covered. In section 4, the results and discussion will be presented. In section 5, the research will be concluded with final observations and future possibilities.

2 Literature Survey

Yapıcı et al., 2021 addressed the data shortage affecting offline handwritten signature verification tasks by introducing a novel data augmentation tool based on Cycle-GANs. The research combined efficiency with training via the introduction of a new Caps-Net signature verification system. This new system was shown to augment performance across all the CNN architectures, with a clear improvement in performance for the DenseNet121 architecture. The two datasets used for testing, GPDS and MCYT, both showed state-of-the-art performance on the latter for offline handwritten signature verification. An inherent limitation considered in the study is the problem of data scarcity, specifically the lack of real-world data available to practitioners.

One of the foremost challenges associated with the expansion of new digital technologies pertains to the preservation of the authenticity and the security of legal documents. Legal documents can serve as key evidence during law enforcement legal proceedings. These documents can be easily susceptible to security breaches such as forgeries, tampering, and unauthorized modifications (Pragadeswaran et al., 2024). With the rise in complexity and frequency of cyberattacks, digital evidence in Afghanistan has become a target. Current attempts that disregard the securement of documents in transit or towards the end of a process predominantly focus on detecting image forgeries. Automated attempts at secure document transmission are largely absent. The present research which has enabled an embedded automated secure document transmission attempt to address those gaps in the forenXAI system. The integration of forenXAI with secure encrypted border control and real-time monitoring guarantees a first-of-its-kind automated system that secures evidence within the realm of digital forensics in

Afghanistan (Arora & Naik, 2025). It augments the integrity of the system which relies upon document verification at the initial or final steps in a complex system.

Tolosana et al., 2021 presented DeepSignDB, the largest database of online signatures to date (over 70K signatures from 1,526 users in a variety of contexts with multiple devices). The proposal involved Time-Aligned Recurrent Neural Networks (TA-RNNs), which integrated Dynamic Time Warping into RNNs as a means of dealing with sophisticated forgeries. In some datasets, the system attained an EER of less than 2.0% and was more accurate than previous systems. The system was highly generalizable, but further research was needed on the challenges of finger input and the integration of other behavioral biometrics.

Hasan et al., 2024 reported a solid user identification system that has analysed time-series data of handwriting taken from pen-tablet sensors. The system extracted 91 features, 36 of which were novel. Additionally, four feature selection techniques were used to improve performance. Using machine learning and deep learning techniques, the system achieved accuracy rates of up to 100% for a few tasks. Its contribution was mainly in classification efficacy with minimal resources, whereas scalability across many more behavioural traits remains an open problem for future research.

Bae et al., 2025 introduced an edge-enhancement technique for document forgery detection, using EAs and ECs to enhance edge features extracted by Sobel. The technique resulted in improved detection accuracies for DenseNet121, ResNet50, ViT, and CAE-SVM. The authors argued that edge sensitivity improved the detection of structural forensic inconsistencies, thus providing evidence of its effectiveness in forensics. As such, the slow inference latencies and the ineffectiveness of non-edge altering forgery remained.

Some areas of the Forensic Computing discipline that deal with the protection of the evidential value of documents and signatures require knowledge on verification and authentication of documents. Within Forensic Computing, the tasks of Network Forensics and Forensic Document Examiners that monitor and examine the digital avenue for illegal access and illicit data manipulations are closely related. Within digital forensics the authentication of a document is only one step, other evidence must also be proved to be static and unchanged during preservation or transit. The ForenXAI framework incorporates visual forgery detection with the bifunctional textual anomaly's detection. The incorporation of advanced deep learning models such as ResNet50-CBAM and attention LSTM greatly enhances evidence tampering detection at the pixel or word level while providing a more integrated approach to forensic investigators.

Boonkrong, 2024 investigated the possibility of forgery detection using hash functions as certifying methods to compute a distinctive signature of an academic document, thus demonstrating originality and encryption preservation for the document.

The goal of the approach was to protect documents originality with high fidelity and processing speed. The method was able to detect manipulations when the originals were available. However, its reliance on original hash values, secured key management for obtaining hashes, and exposure to collision and birthday attacks limit its applicability compared to machine learning-based methods.

Hosny et al., 2022 developed a deep neural learning-based Copy-Move Forgery detection method to classify an image as either forged or original. It extracted feature vectors from images and classified them with a fully connected layer to identify the dependencies of the image features. The final model exhibited 100% accuracy for all three datasets, MICC-F2000, MICC-F600, and MICC-F220. Completion times also demonstrated that testing the model took less time than other reported study

methods. While the model provided outstanding results, it required pre-training, and the authors did not discuss whether the methods described generalize to different forgery types or real-life scenarios.

Hall et al., 2022 analyzed the benefits of XAI to DF in assisting with the investigation, case management, and case prioritization. The researched maintained the case with XAI's greatest contribution being the boosting of 'transparency' in digital forensics, but the question of legal admissibility remained murkier. The work also addressed the use of AI in digital forensics in the context of adversarial learning and deepfakes, as well as proposing a novel methodology for testing the empirical performance of XAI outputs and a baseline for how durable XAI systems need to be to counter adversarial XAI. All in all, the optimism for the advancement of XAI in digital forensics remained well-founded, but the XAI outputs for DF and the legal validation of the outputs were critical boundaries to the optimism.

Islam et al., 2023 proposed the Novel Support Vector Neural Network (NSVNN) for anomaly detection, focusing on digital forensics data to detect unusual patterns that indicate possible criminal activities (Xiao & Ding, 2022). The NSVNN, evaluated on real datasets, produces better performance measures (accuracy, precision, recall, and F1-score) than standard support vector machines (SVM) and neural networks, and it also provides interpretability through feature importance analyses. There were limitations concerning the scalability of NSVNN as well as the reliance on quality labelled data for performance to be maximized.

Momeni & BabaAli, 2024 examined offline Arabic handwriting recognition through the application of new Transformer (i.e., Transformer Transducer and sequence-to-sequence Transformer) network architectures in place of CNN-RNN models. The goal was to leverage the Transformer attention mechanism's ability to parallelize the model, modulate its linguistic model, and employ a pre-trained Transformer. The method was evaluated using the KHATT (Qur'anic) dataset, achieving superior accuracy and speed compared to state-of-the-art models. Limitations included computational cost and the potential need for domain-specific fine-tuning for practical use across the OCR community.

Xi et al., 2023 proposed a cross-attention-based dual-stream architecture for test-to-image (T2I) generation and AI-generated content (PG) detection. To improve forgery detection in images, the proposed method was validated on custom DALL·E2 and DreamStudio datasets, along with DsTok and SPL2018. The proposed dual-stream drove improved T2I image generation and consistently outperformed CG detection methods in each of the resolutions outside of modes focused on the initial 3 stages of T2I. Although effective, the project's caveats include the potential for deployed pre-trained models to be used in mid-range fine-tuning and the need for larger cohort-level validations on various types of forgery.

Table 1 presents a systematic overview of recent research in forensic signature verification and document forgery detection. It emphasizes the main techniques, achievements, and continuing weaknesses of each method, serving as a comparative basis for anchoring the proposed ForenXAI to current developments.

Table 1: Summary of recent techniques in forensic document verification and forgery detection

Author(s)	Technique Used	Achievements	Limitations
Yapıcı et al., 2021	Cycle-GAN	Improved DenseNet121 performance; state-of-the-art results on GPDS and MCYT datasets	Limited by the scarcity of real-world data
Tolosana et al., 2021	TA-RNN	Achieved <2% EER; highly generalizable on DeepSignDB	Challenges with finger input and integration of behavioural biometrics
Hasan et al., 2024	ML/DL classification	Up to 100% accuracy in tasks with efficient feature selection	Scalability to broader behavioural traits remains a challenge
Bae et al., 2025	Edge-Attention (EA) and Edge-Concatenation (EC) in CNNs	Enhanced detection accuracy	Limited to non-edge-altering forgeries
Boonkrong, 2024	Hash-based forgery detection	Detects manipulation when original hashes exist	Susceptible to hash collision
Hosny et al., 2022	DNN-based Copy-Move Forgery Detection	Fast execution	Needs pre-training
Hall et al., 2022	XAI evaluation in digital forensics	Improved transparency and prioritization of cases	Trust and legal admissibility of XAI outputs are not fully established
Islam et al., 2023	NSVNN	Interpretable via feature analysis	Scalability issues
Momeni & BabaAli, 2024	Transformer and Transformer-Transducer	Faster due to parallelism	High computational cost
Xi et al., 2023	Cross-attention dual-stream model	Superior to baseline CG detection methods.	Limited mid-range fine-tuning

Problem Statement

Although there are significant strides in signature verification and document forgery detection using DL methods, challenges remain, including data insufficiency, deficiencies in generalizability, computational costs, lack of recognition for cross-modal analytic tasks, and the possibility of explanation. These challenges made for reliable deployment in authentic investigations impractical, signifying the need for a framework that is integrated, interpretable, and scalable to provide robust forgery detection and verification.

Cyber threats against digital forensic documents include visual manipulations-altered signatures, fraudulent additions, and undocumented changes to police and witness statements-and textual alterations. Such security threats make document verification uniquely challenging, as systems must identify subtle manipulations and anomalies, including pixel-level forgery and text anomalies. Furthermore, unimodal isolated systems forensic document verification continues to rely on traditional methods, which are ineffective for threats involving both the visual and textual components. ForenXAI takes a comprehensive route for the first time by combining visual forgery detection and textual anomaly detection systems to the first cross-modal verification system. This system's ability to handle intricate multi-level security threats is greatly enhanced by using cross-modal techniques. These techniques

provide a comprehensive solution to digital forgery and manipulation, proving highly effective against complex and multi-dimensional security threats.

3 Proposed Methodology

This research presents ForenXAI, a DL-based intelligent framework designed to verify signatures and detect forgery in forensic applications, addressing the significant problem of document forgery and handwriting manipulation. The primary goal is to develop a scalable, interpretable, and multi-modal framework that overcomes challenges in prior studies (e.g., limited generalizability, lack of explainability, non-availability of data, and the inability to appropriately detect cross-modal content). By leveraging visual and textual content analysis with explainable AI and probabilistic risk scoring, the credibility of digital forensic evidence is enhanced, enabling real-time, legally defensible decisions in police investigations. Figure 1 shows the proposed architecture of the ForenXAI model.

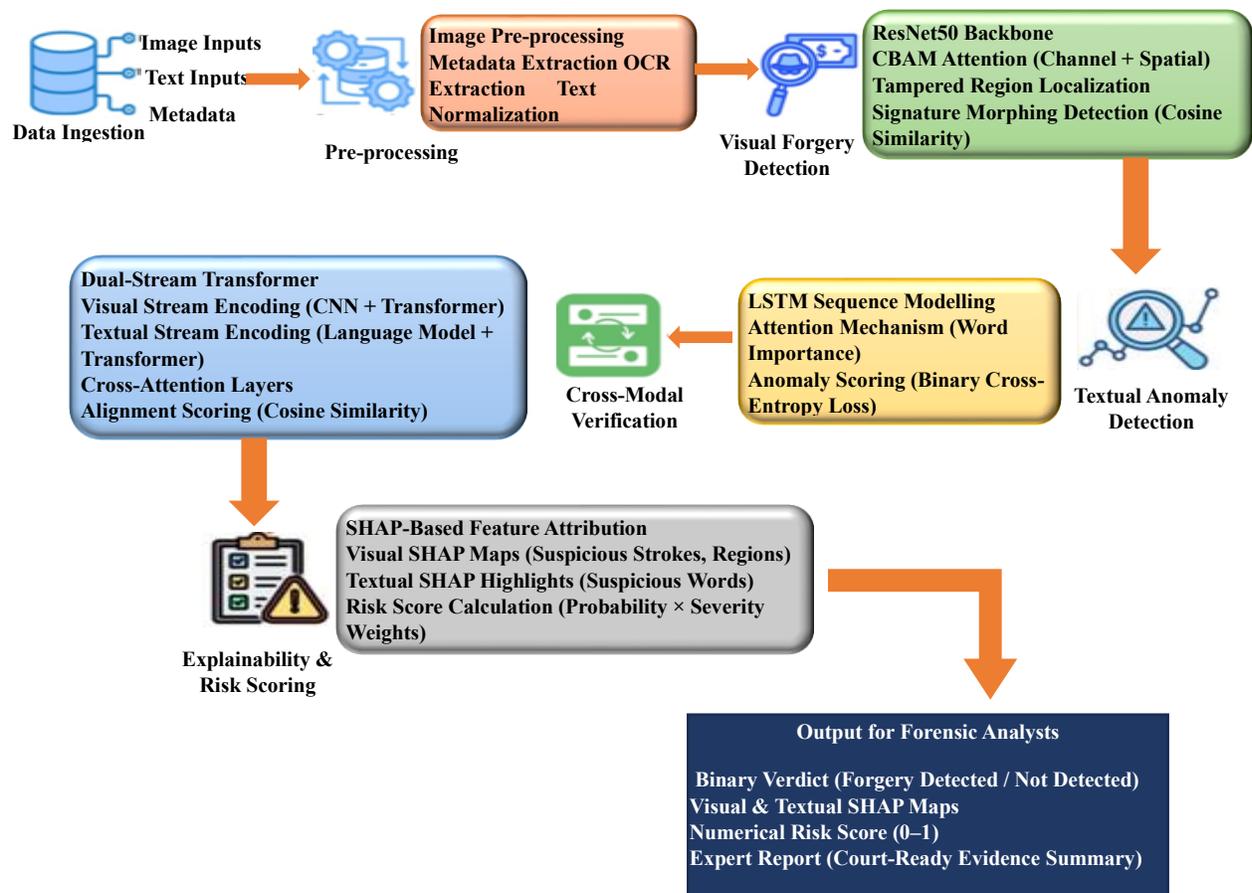


Figure 1: Architecture of the forenXAI model

Data Ingestion

- **Image Inputs:** Scanned forensic documents, including handwritten signatures, police reports, identity forms, and questioned document samples.
- **Textual Inputs:** Ground truth or extracted summaries, witness statements, and transcribed police reports.

- **Metadata:** Includes timestamp, origin, capture method (e.g., scanner or digital pad), and author identification.

Pre-processing

At the beginning of ForenXAI, the different forensic data is organized and preprocessed to prepare for the next modules in the process. This step provides clean data as input to the respective modules. So, this preprocessing step incorporates both image-based and text-based data, ensuring they relate to each other for cross-modal verification.

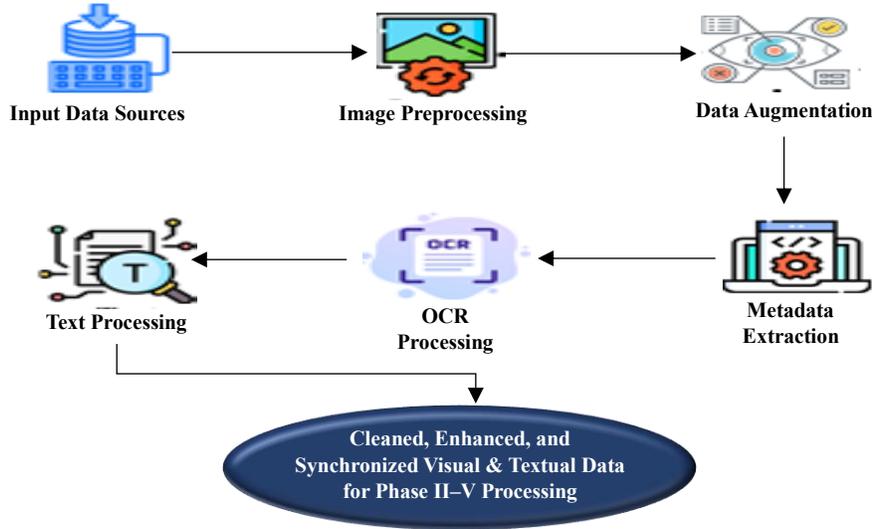


Figure 2: Structure of the pre-processing phase

The structure of the pre-processing phase is shown in Figure 2. To reduce high-frequency noise while maintaining important edges, a Gaussian filter is applied, as described in equation (1):

$$I_{smooth}(x, y) = \sum_{i=-k}^k \sum_{j=-k}^k G(i, j) \cdot I(x - i, y - j) \quad (1)$$

Where $G(i, j) = \frac{1}{2\pi\sigma^2} e^{-\frac{i^2+j^2}{2\sigma^2}}$ with σ referring to the standard deviation, which controls the amount of smoothing. Otsu's Thresholding is applied to eliminate the primary foreground writing from background noise, as seen in equation (2):

$$T = \arg \max_{\theta} \left[\omega_0(\theta)\omega_1(\theta)(\mu_0(\theta) - \mu_1(\theta))^2 \right] \quad (2)$$

Where ω_0 and ω_1 are the class probabilities, μ_0 and μ_1 are the class means for the pixel intensities below and above the threshold θ . Histogram equalization is used to recover the visibility of faint strokes, as seen in equation (3):

$$P'(i) = \left\lfloor \frac{L-1}{MN} \sum_{j=0}^i H(j) \right\rfloor \quad (3)$$

Where $P'(i)$ is the new pixel intensity, $H(j)$ is the histogram number of counts, L is the number of levels of intensity, and $M \times N$ is the number of pixels in the image. To aid in generalization and alleviate the issue of class imbalance, data had to be augmented for Rotation, Scaling, and Translation, as seen in equations (4, 5 and 6):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} s_x & 0 \\ 0 & s_y \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (5)$$

$$x' = x + t_x, y' = y + t_y \quad (6)$$

Where θ is the angle of rotation, s_x and s_y are the scale factors, t_x and t_y are the translation adjustments. By utilizing regular expressions and parsing libraries, the metadata from the headers of the image files is extracted as seen in equation (7):

$$Metadata = \{Date, ScannerID, Resolution, ColorDepth, AuthorID\} \quad (7)$$

These features contribute to contextual filtering and forensic source authentication. OCR was performed using Tesseract, and a custom CNN-LSTM OCR pipeline as seen in equation (8):

$$T = OCR(I_{binarized}) \quad (8)$$

Where T is the extracted text sequence, while $I_{binarized}$ is the input image processed. The extracted text is tokenized, normalized, and stored for semantic alignment with the images of signatures in Phase III. This complete pre-processing ensures all modalities (visual and textual) are properly aligned, cleaned, and enhanced to better facilitate the downstream DL models at the forensic signature verification level. Figure 3 shows the sample images of pre-processing.

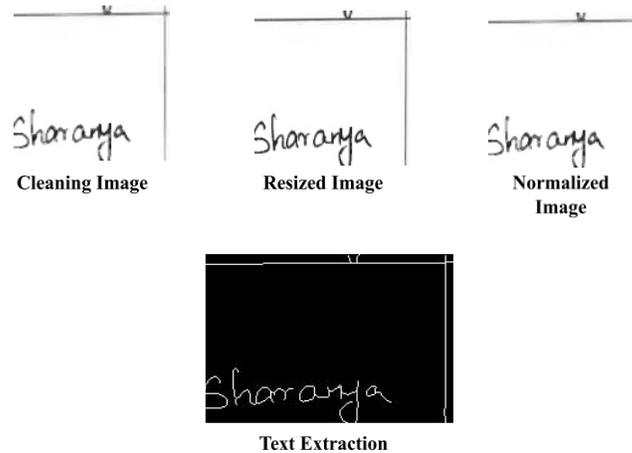


Figure 3: Sample images of pre-processing

ForenXAI incorporates advanced key management and authentication strategies to safeguard forensic documents while verifying them. At the start of the processing for any document and signature that enters the system, an authentication procedure is completed, and the digital signature or hash is verified. Documents and forensic data access controls via role-based authentication are aligned with organizational policies, ensuring data access only for designated personnel. Documents and forensic data are overseen via a role-based authentication access policy. Documents and their metadata are stored in a secure database, and accessibility is aligned to organizational policies. Each document is traceably supported to control and record unauthorized access and/or modifications to closures. The secure management of documents is especially critical in forensic science environments where the evidence's integrity is of utmost importance. All these practices are aligned to the expected industry protocols evidencing the trust and reliability of the ForenXAI framework when used in legal matters.

Visual Forgery Detection

After completing the pre-processing, the next process is visual forgery detection. During this phase, forensic imaging inputs are thoroughly analyzed using a deep convolutional architecture to detect tampering and forged aspects. The visual forgery detection pipeline combines a ResNet50 backbone with a Convolutional Block Attention Module (CBAM) to enhance sensitivity to spatial and channel-wise features, enabling the detection of document forgeries at a fine-grained level.

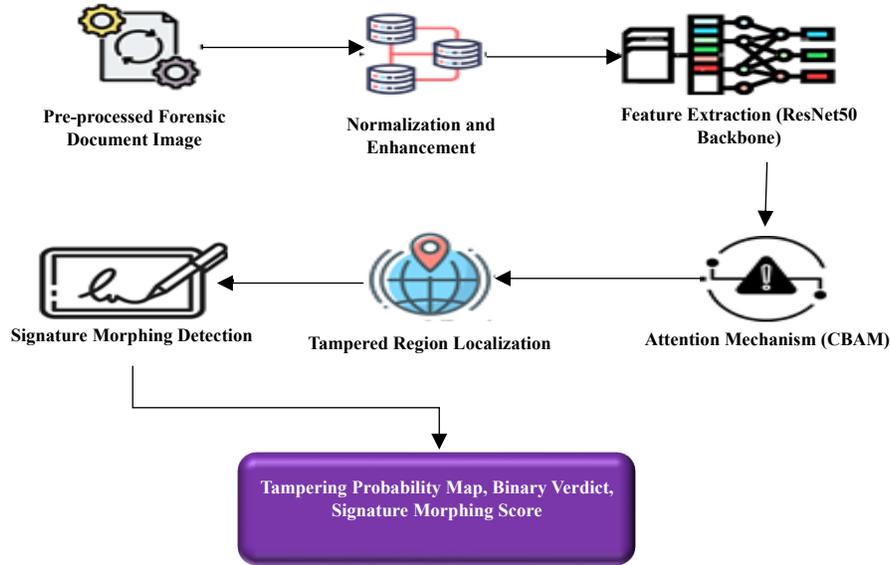


Figure 4: Architecture of the process of visual forgery detection

Figure 4 displays the process of visual forgery detection. The scanned document image is individually normalized with image sizing to a specific input size (e.g., 224×224 pixels) and histogram equalization to improve image contrast and normalize lighting conditions per equation (9):

$$I_{eq}(x, y) = \frac{L-1}{MN} \sum_{i=0}^{L-1} h(i) \quad (9)$$

Where $I_{eq}(x, y)$ is the equalized intensity, L is the number of gray levels, MN is the total number of pixels, and $h(i)$ is the histogram count of intensity i . Edge-preserving filtering (for example, bilateral filtering) is used to reduce noise while preserving edges according to the equation (10):

$$I_{filtered}(x) = \frac{1}{W_p} \sum_{x_i \in \Omega} I(x_i) \cdot f_s(\|x_i - x\|) \cdot f_r(|I(x_i) - I(x)|) \quad (10)$$

Where f_s is the spatial Gaussian kernel, f_r is the range (or intensity difference) kernel, and W_p is the normalization factor. The pre-processed image is passed to ResNet50, which is a deep residual network with 50 layers deep and applies hierarchical feature-extraction through residual blocks, according to equation (11):

$$y = F(x, \{W_i\}) + x \quad (11)$$

Where x is the input feature map, $F(\cdot)$ is the residual function (which consists of convolution, batch normalization, and ReLU), and $\{W_i\}$ are the learnable weights. The advantage of using residual mapping lies in learning how to model complex tampering patterns, such as smudges, copy-move forgeries, and localized erasures in handwritten forms and signatures. To further improve tampered region localization,

CBAM is used on the output of ResNet50. CBAM has the following equations (12) and (13) to infer attention maps in channel and spatial dimensions from the feature maps:

$$M_c(F) = \sigma \left(MLP(AvgPool(F)) + MLP(MaxPool(F)) \right) \quad (12)$$

$$M_s(F) = \sigma(f^{7 \times 7}([AvgPool(F); MaxPool(F)])) \quad (13)$$

Where σ is the sigmoid activation, $f^{7 \times 7}$ is a convolution using a 7×7 kernel, F is the feature map input, M_c is the attention mask in the channel dimension, M_s is the attention mask in the spatial dimension and M_i is the intermediate feature map, the final feature map is shown in equation (14):

$$F' = M_s(F \cdot M_c) \cdot (F \cdot M_c) \quad (14)$$

This adaptive attention guarantees that the network is encouraged to pay attention to the suspicious regions, such as distorted strokes, unnatural pixel clusters, and blurry document edges. The result of this module is a binary mask or probability map according to equation (15):

$$T(x, y) = \begin{cases} 1 & \text{if tampered region detected at pixel } (x, y) \\ 0 & \text{otherwise} \end{cases} \quad (15)$$

Additionally, signature morphing detection is done by comparing embeddings of multiple signatures of the same author with cosine similarity according to equation (16):

$$Similarity(A, B) = \frac{A \cdot B}{\|A\| \|B\|} \quad (16)$$

If there is low similarity across samples with similar metadata, it is possible that morphing or impersonation occurred intentionally.

Textual Anomaly Detection

Upon completion of Visual Forgery Detection, the next stage is textual anomaly detection. This stage is devoted to detecting anomalies or distortions in the textual content extracted from forensic documents, such as police reports, incident narratives, statements of identity, and affidavits. The extracted text through the OCR preprocessing from Phase I is fed into an LSTM model-based sequential DL model, which uses an Attention Mechanism. Figure 5 illustrates the process of textual anomaly detection.

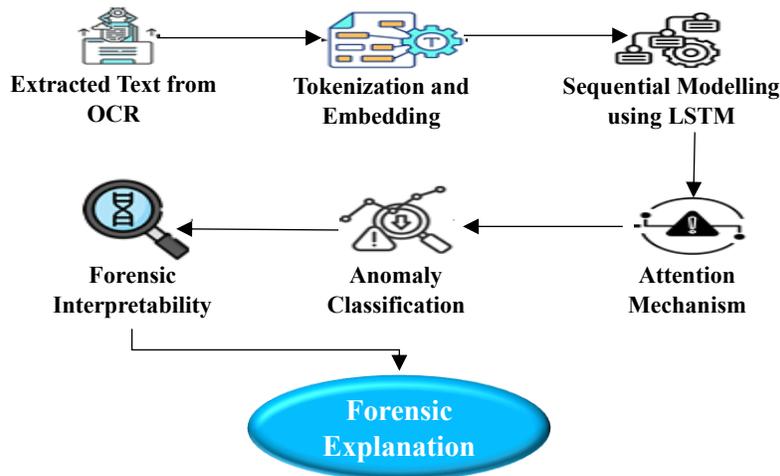


Figure 5: Architecture of the textual anomaly detection

Text Sequence Modeling with LSTM

LSTM networks with recurrent layers help capture temporal dependencies and semantic flow present within sequential data. When given a sequence of tokens $x = (x_1, x_2, \dots, x_T)$, LSTMs process the tokens in a manner where they remember past states to maintain context, meaning that the processing is more of a dilation instead of a simultaneous operation. The computation for the hidden state h_t at time step t is presented below in equation (17):

$$h_t = \alpha_t \cdot o_t \cdot \tanh(C_t) \quad (17)$$

Where h_t is the final hidden state at time step t , o_t is the output gate at time step t , C_t is the internal memory cell, $\tanh(C_t)$ is the activation function that is scaled between -1 and 1, and α_t is the attention weight at time t .

Incorporating Attention Mechanism

To enhance interpretability and sensitivity to anomalous or manipulative content, an attention layer is added on top of the LSTM output. This attention layer disambiguates the importance of words used to create suspicious deviations in textual style or narratives. Let h_t represent the hidden state at timestep t , the attention score α_t is defined in equations (18 and 19):

$$e_t = \tanh(W_a h_t + b_a) \quad (18)$$

$$\alpha_t = \frac{\exp(e_t)}{\sum_{k=1}^T \exp(e_k)} \quad (19)$$

The context vectors c , a weighted average of all previous hidden states, is defined using equation (20):

$$c = \sum_{t=1}^T \alpha_t h_t \quad (20)$$

This context vector c is finally passed as input through a dense classifier to produce an anomaly score $y \in [0,1]$, where values closer to 1 signal an increasing likelihood for forgery. The model is trained using binary cross-entropy loss as described in equation (21):

$$L = -[y \log(\hat{y}) + (1 - y) \log(1 - \hat{y})] \quad (21)$$

Where y refers to the ground truth label (0 for authentic and 1 for forged), and \hat{y} refers to the predicted probability of an anomaly. The attention mechanism provides interpretability by providing relevant tokens of text, i.e. consistencies or inconsistencies with the name, formatting of date, features that tell a narrative outside of an already known template (i.e. police complaint) and aberrant word choice (e.g. in use of forged identity descriptors). The highlighted tokens allow forensic practitioners to backtrack the anomaly and provide an explanation of the model's decision when assessing its validity in a court of law or legal review.

Verification Phase

During this stage, cross-modal verification is executed to identify discrepancies between visual signature images (visual modality) and text modality with extracted text content. The architecture is based on a Dual-Stream Transformer architecture, in which there are two individual encoders working with each modality before cross-modal interaction. The visual-stream encoder encodes the signature images using convolutional neural networks as a feature extractor before encoding in transformer layers. Denote the visual feature sequence as in equation (22):

$$V = \{v_1, v_2, \dots, v_m\}, v_i \in R^d \quad (22)$$

The textual-stream encoder encodes the OCR extracted text, embedding each token as an embedding using a pre-trained language model, and then encodes using transformers according to equation (23):

$$T = \{t_1, t_2, \dots, t_n\}, t_j \in R^d \quad (23)$$

Cross-attention layers blend these two modalities, allowing the network to associate the corresponding signature strokes with semantic textual references. Cross-modal attention can be computed according to equation (24):

$$Attn(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d}}\right)V \quad (24)$$

in which Q (queries) come from one modality (text, for example) and K, V come from the other (image, for example). This allows each text token to attend to the meaningful visual feature regions, and vice versa. The score S_{align} is calculated typically cosine similarity defined in equation (25):

$$S_{align} = \frac{F_v \cdot F_t}{\|F_v\| \|F_t\|} \quad (25)$$

as F_v and F_t denotes the vector representations of text and visual streams, post fusing Cross-Attention. An even S_{align} score is indicative of a forgery, for example, an adjustable set of signature stylizations or the signatures having mismatched signer identities. The system interfaces a sigmoid layer in equation (26):

$$P_{mismatch} = \sigma(W_s \cdot S_{align} + b_s) \quad (26)$$

which is forwarded to the explainability module so as to formulate an understandable mismatch report intended to assist forensic specialists in verifying the authenticity of the documents.

Explainability and Risk Scoring

In forensic document verification, model transparency is not only appreciated, but is also a legal requirement to substantiate the evidentiary reliability of the model's outcome. This phase of the process. Involves the integration of XAI along with risk quantification to render the initial predictions transitioned into optimal succinct, legally defensible conclusions.

The process of Explainability and Risk Scoring is displayed in Figure 6.

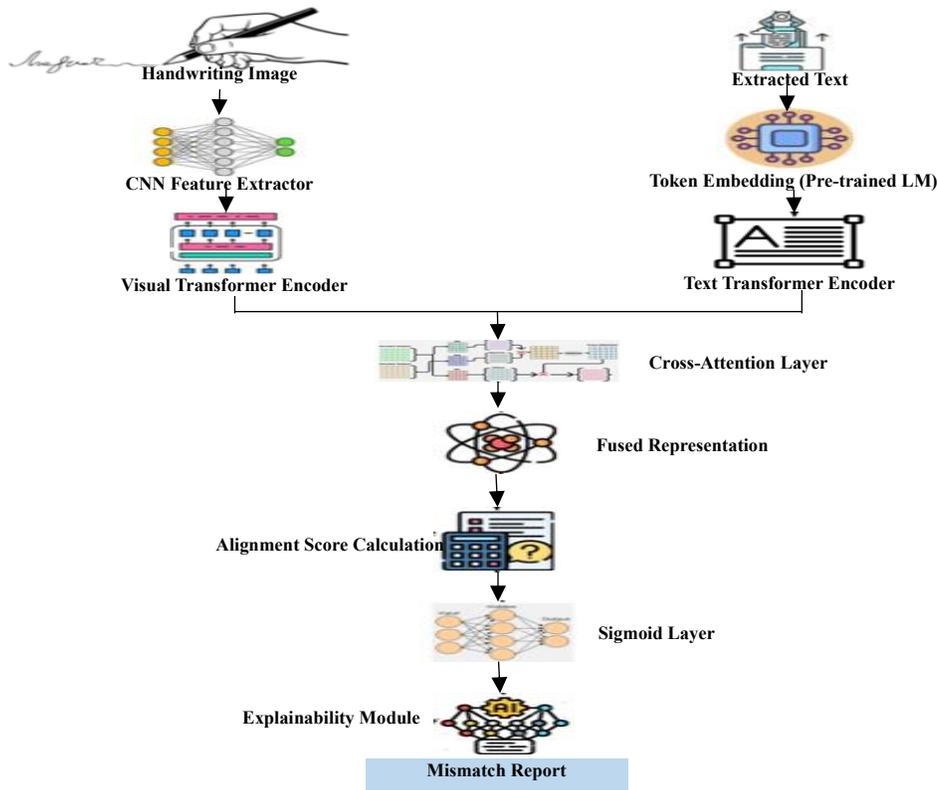


Figure 6: Architecture of the explainability and risk scoring

Explainability via SHAP

SHAP (SHapley Additive exPlanations) is a method that attributes the prediction result to individual input features, whether they are visual features (e.g., strokes, curves, spatial pressure patterns) or textual features (e.g., named entities, syntactic patterns). SHAP is based upon cooperative game theory, and the contribution of each feature, x_i , for the prediction, $f(x)$, is represented in the following equation (27):

$$\phi_i = \sum_{S \subseteq N \setminus \{i\}} \frac{(|S|! (|N| - |S| - 1)!)}{|N|!} [f(S \cup \{i\}) - f(S)] \quad (27)$$

Where ϕ_i is the Shapley value for the feature i . N is the set of all features. S is a subset of N not including i . $f(S)$ is the model output using just the features in S . In practice, the SHAP methodology is applied to both modalities separately. Visual SHAP map overlays capture document regions (e.g., suspect strokes, erased areas) that impacted the model's decision, and Textual SHAP importance plots highlight influential words or patterns (e.g., mismatched names, altered dates). This allows forensic experts to see where potential missing or forgery flags originated.

Risk Scoring Framework

After interpretability, there is then a forgery risk score to determine the likelihood and level of severity of documented anomalies. Let $P_{mismatch}$ is the probability of a mismatch (from Phase IV), and W_s is a severity weight vector specific to the domain, based on evidence and legal requirements. The risk score R is shown in equation (28):

$$R = \lambda \cdot P_{mismatch} + (1 - \lambda) \cdot Severity(x) \quad (28)$$

Where $\lambda \in [0,1]$ adjusts the tradeoff between statistical probability and qualitative severity. The $Severity(x) = \sum_{i=1}^n W_{s,i} \cdot |\phi_i|$, or the absolute value of SHAP values weighted by the worth of each feature under forensic inquiry. That is to say, a minor inconsistent visual change and a significant name change should not be given an identical weight when assessing legal risk.

The final product presented to forensic analysts involves several decision-support elements to provide both technical reliability and legal defensibility. First, the system creates a forensics decision statement which classifies the evidence of a forgery in the documents as a yes/no and captures the reasoning behind the pessimistic outcome with a system of SHAP derived graphic and textual maps of the forgery decision's critical regions and most important words. Secondly, a risk score for a forgery is generated between 0 and 1. This score indicates how extensive a forgery might be, and how extensive damage might be done because of it. Third, and a lot more fundamental, the expert report synthesizes all the outputs into a single coherent and comprehensive document which aids the forensic practitioner in consolidating the findings in a form which is easily digestible for an appellate review. The findings concerning DL analysis and evidence within the report are crafted in a reporting format that is meant to exemplify forensic rigor and analysis. ForenXAI, in this case, is able to leverage the synergistic effect of this multi-phase pipeline to address shortcomings of prior forensic AI systems by offering an aligned, comprehensible, and multi-format solution to reliable signature verification and forgery detection.

The core issue of the legal admissibility of forensic document verification systems still rests upon the concepts of privacy and trust. Forensic experts are required to trust that document verification systems provide reliable, as well as consistent, and interpretable results. In ForenXAI, privacy is one of the numerous considerations where forensic data is protected during analysis. For example, avoidance and anonymization of personally identifiable information (PII) during processing is one of the mechanisms of compliance with privacy laws such as the GDPR (General Data Protection Regulation). In addition, the SHAP explainability framework enhances privacy by depicting the modes of each prediction, thereby assisting experts in forensic analysis to monitor the flow of the analysis. Such flows promote system transparency and trust in the results, facilitating the presentation of results in court without fear of objection for opacity or inaccuracy. Furthermore, the risk scoring system accounts for privacy in assessing the impact a forgery may have, and the consequences that false positives/negatives may have in a decision and vice versa. The performance evaluation of the proposed model is explained in the next section.

4 Results and Discussion

The performance of the proposed ForenXAI framework in forensic signature verification and forgery detection is noted in the results and discussion section. The model has been shown to be highly accurate, precise, sensitive, and specific at various percentages of training. The results confirm the strength of combining ResNet50-CBAM, LSTM with attention, and dual-stream transformers, with explainability and risk scoring to support reliable forensic use. The proposed model is compared with techniques like Cycle-GAN [16], Ta-RNN (Tolosana et al., 2021), NSVNN (Islam et al., 2023) and Transformer Momeni & BabaAli, 2024.

Experimental Setup

ForenXAI was experimentally evaluated in Python and combined with DL libraries, including TensorFlow and PyTorch. Different document and forensic signature datasets were pre-processed and run through the multi-phase pipeline of the model. Accuracy, F1-score, MCC, NPV, precision,

sensitivity and specificity were calculated as performance metrics to confirm the effectiveness of the system.

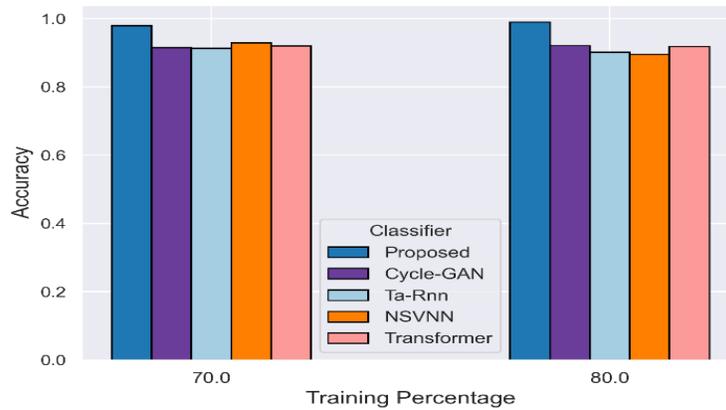


Figure 7: Accuracy of the forenXAI model

The accuracy of the proposed ForenXAI framework is illustrated in Figure 7. With a training percentage of 70, this model had an accuracy of 0.9788, which increased to 0.9894 at 80 training percentage. These values show that the proposed model always outperforms competing baselines, which proves the strength of the proposed model to distinguish between genuine and forged signature samples. The great accuracy demonstrates the efficiency of the integrated ResNet50-CBAM visual forgery detection, the LSTM-based textual anomaly detection, and the dual-stream transformer verification in cross-modal learning.

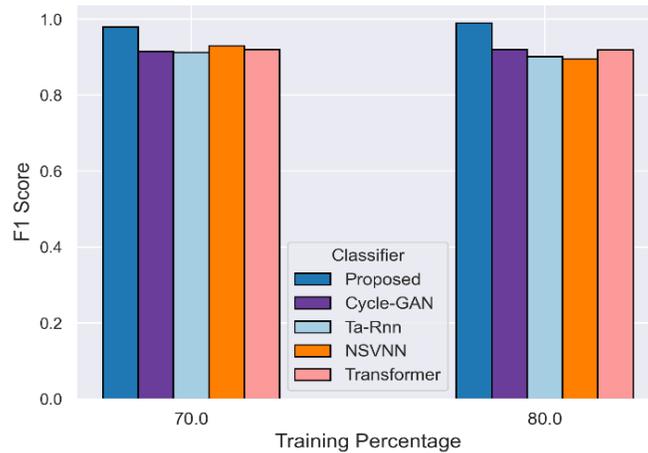


Figure 8: F1-Score of the forenXAI model

Figure 8 indicates the performance of the F1 score. The ForenXAI model achieved 0.9787 in 70 per cent training and 0.9894 in 80 per cent training. The F1 score is a trade-off between precision and sensitivity, whereby both the forged and authentic cases are treated equally. The F1 score is consistently high at various training percentages, which demonstrates the strength of ForenXAI that builds on the complementary capabilities of CNNs, RNNs, and transformers. This keeps the misdetections and false alarms to a minimum.

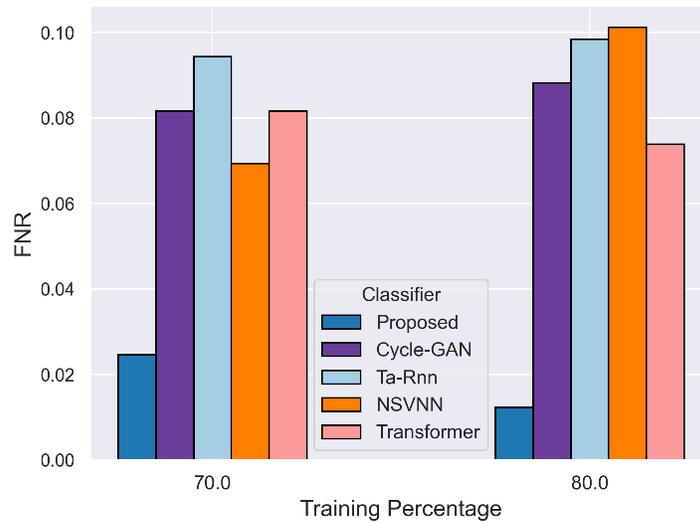


Figure 9: FNR of the forenXAI model

The false negative rate is shown in Figure 9. The ForenXAI method had 0.0246 at 70% training, and 0.0123 at 80% training. A small FNR means that the system prevents the detection of forged samples. In forensics, the failure to notice forged signatures can result in critical mistakes in court. ForenXAI reduces the risk of undetected forgeries by jointly applying edge-preserving visual detection and attention-based textual anomaly detection.

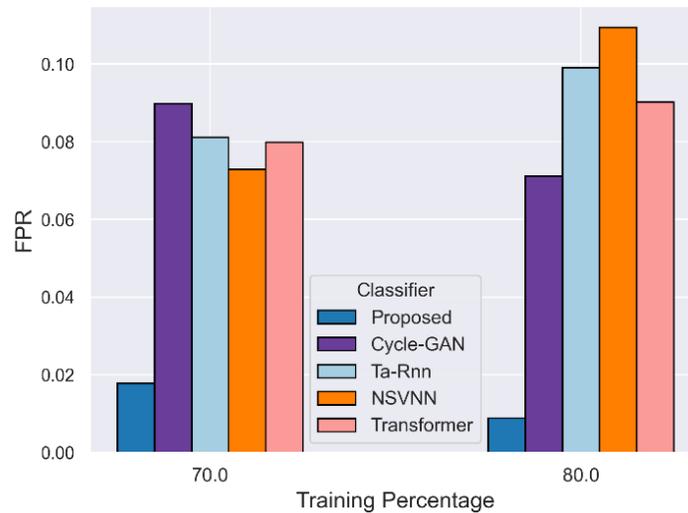


Figure 10: FPR of the forenXAI model

The false positive rate is shown in Figure 10. FPR was 0.0178 at 70 per cent training and 0.0089 at 80 per cent training. The reduced FPR is critical towards the ability to store original documents without falsely identifying them as forged. This enhancement demonstrates that the ForenXAI framework is very efficient in suppressing irrelevant alarms, which is backed by the addition of cross-modal transformers that match handwriting strokes with textual evidence.

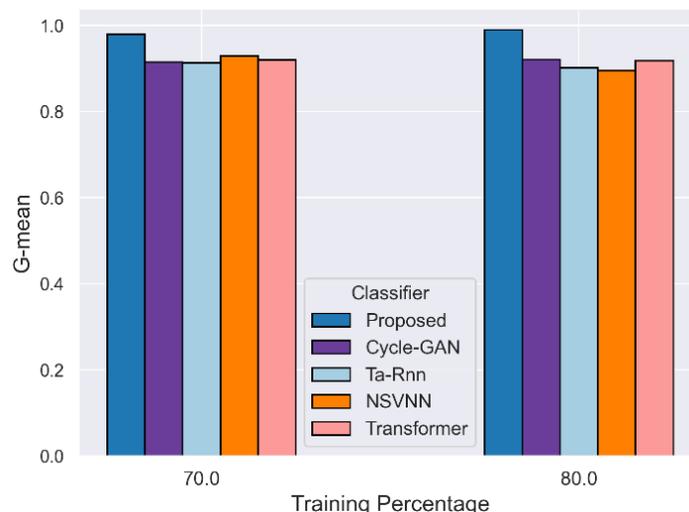


Figure 11: G-Mean of the forenXAI model

The G-mean scores of the ForenXAI method are represented in Figure 11. The value at 70% training was 0.9788, and at 80% training, the value was 0.9894. G-mean indicates the stability of the sensitivity and specificity, which implies that the model is effective on both forged and authentic samples. The large G-mean scores show the balanced effectiveness of the proposed framework in various classes. The multimodal design of ForenXAI guarantees high generalization during handwriting and textual verification tasks.

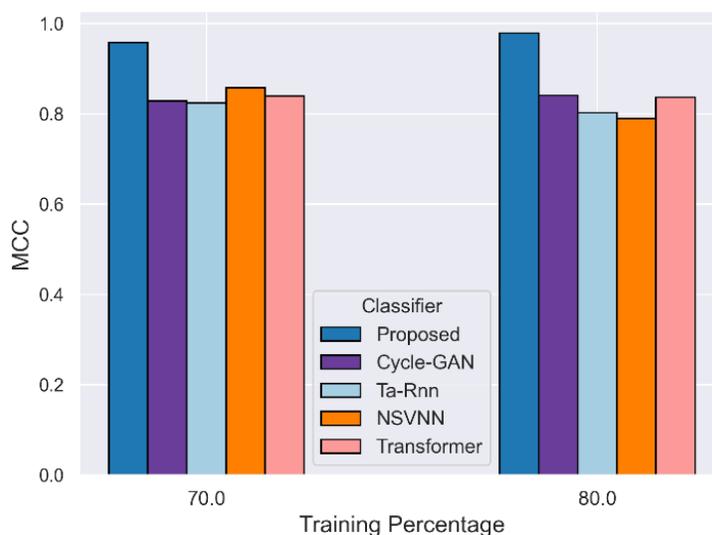


Figure 12: MCC of the ForenXAI model

Figure 12 shows the MCC results. At 70 per cent training, MCC was 0.9576 and at 80 per cent, it was 0.9788. MCC quantifies the total quality of binary classification in terms of true and false positives and negatives. The large MCC values near 1 ensure the proposed ForenXAI model is reliable in a variety of situations. Combining SHAP-based interpretability and forgery detection, the framework not only offers correct classifications but also balanced and impartial predictions.



Figure 13: Sample SHAP visualizations of feature contributions to model predictions for handwritten names

Figure 13 demonstrates SHAP plots of the contribution of features to the predictions of ForenXAI on handwritten names. The images are associated with a name sample, and colored overlays are used to demonstrate the areas that have the greatest effect on the classification of the model. The areas highlighted show the main characteristics employed by the model, which is a show of interpretability. The visualizations allow to evaluate the model behavior, detect possible biases, and enhance feature extraction. In general, they demonstrate that ForenXAI makes correct and balanced decisions in handwriting recognition.

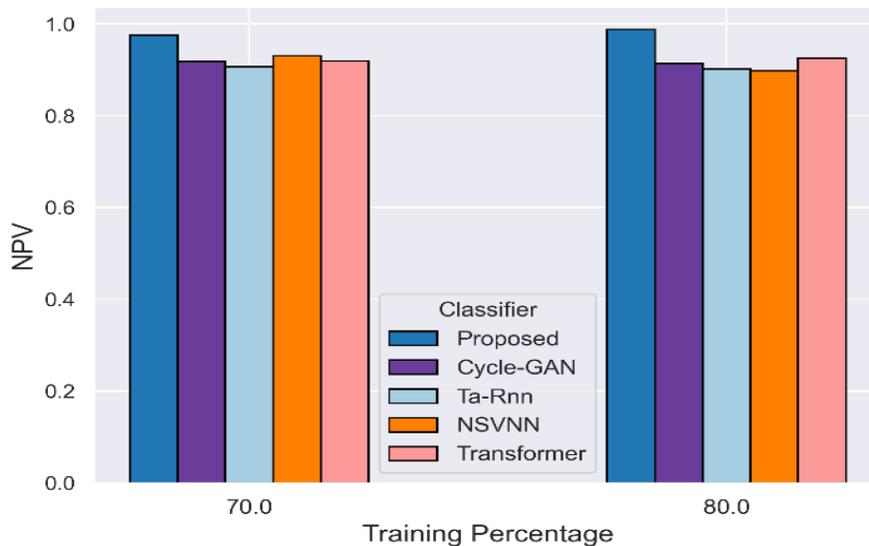


Figure 14: NPV of the forenXAI model

The NPV of the ForenXAI model is reported in Figure 14. NPV at 70 per cent training was 0.9756, and at 80 per cent training, it was 0.9877. High NPV indicates the accuracy of the model in validating the authenticity of the documents when it forecasts authenticity. To forensic examiners, this makes the documents that have been cleared by the system highly unlikely to be forged. The outcome is a combination of the two-fold effect of OCR-enhanced textual analysis and ResNet50-CBAM visual verification.

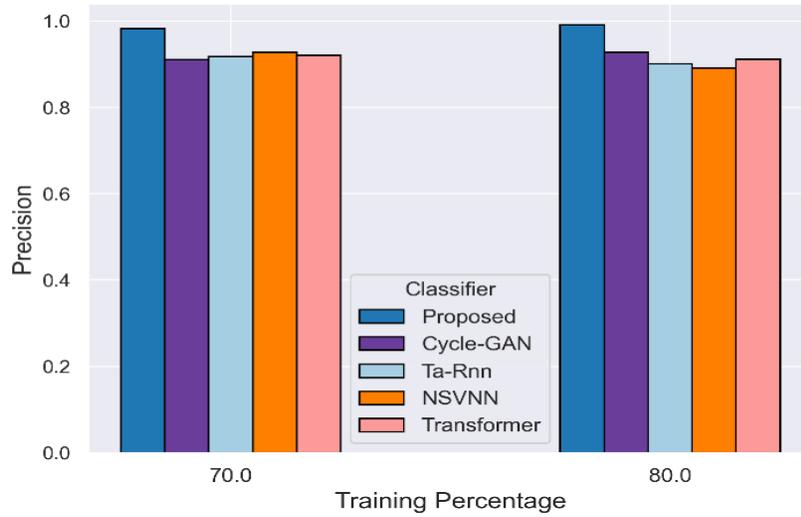


Figure 15: Precision of the forenXAI model

The accuracy of the ForenXAI system is shown in Figure 15. Precision at 70% training was 0.9821, and at 80% training it was 0.9911. Precision is the percentage of correctly identified forgeries out of all flagged samples, or the capacity of the model to reduce false positives. In cases of forensics, the precision must be very high to avoid wrongful classification of true signatures as a forgery. The localized tamper detection of ResNet50-CBAM and cross-modal transformer alignment guarantees that suspicious samples are the only ones that are highlighted, which increases the confidence of forensic analysts when they evaluate questioned documents.

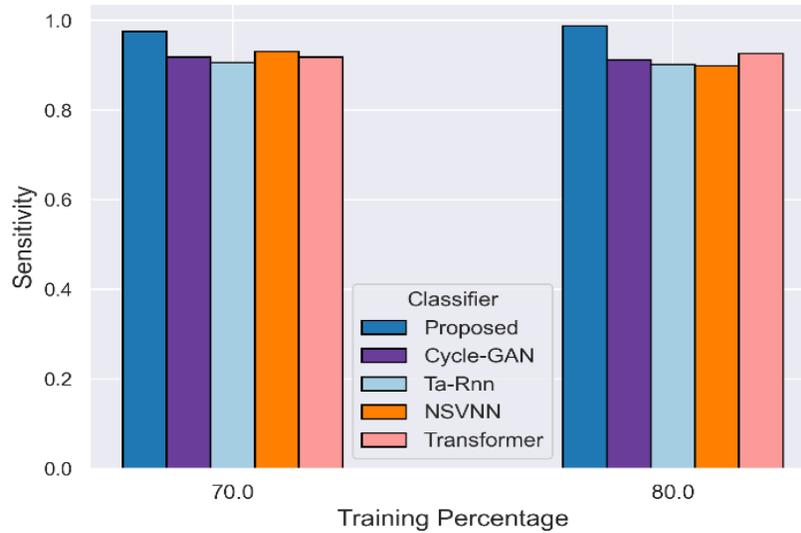


Figure 16: Sensitivity of the forenXAI model

The sensitivity results of the ForenXAI model are shown in Figure 16. The sensitivity with training of 70 per cent was 0.9754, and with 80 per cent training was 0.9877. High sensitivity: This means that false or altered examples of signatures are correctly identified, which is important to prevent fraudulent evidence from being introduced in the courts. ForenXAI uses the LSTM with an attention mechanism to enable subtle textual anomalies to be detected, and dual-stream transformers reinforce cross-modal verification.

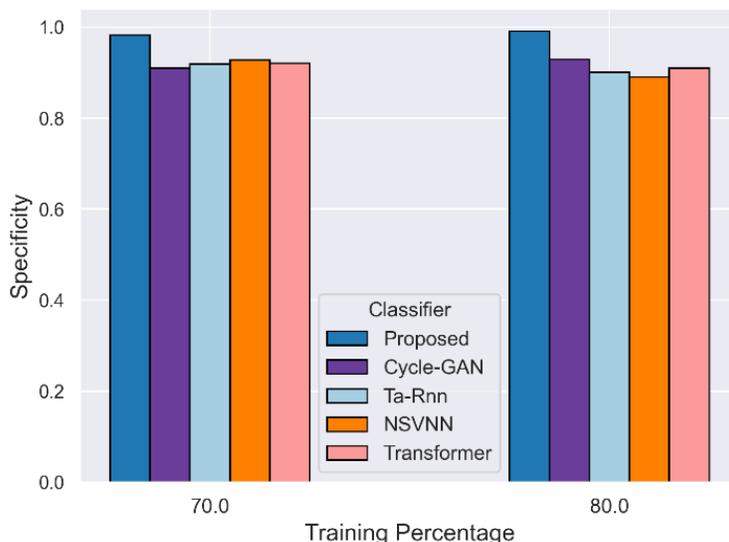


Figure 17: Specificity of the forenXAI model

The specificity scores of the ForenXAI model are emphasised in Figure 17. Specificity at 70% training was 0.9822, and at 80% it further rose to 0.9911. High specificity assures that ForenXAI is highly effective in properly classifying authentic documents without falsely classifying them as forgeries, which is a key element in forensic decision-making. This is possible due to the built-in pre-processing stage that adds value to handwriting strokes and reduces noise, combined with CBAM-attention in ResNet50 to accurately detect tampering.

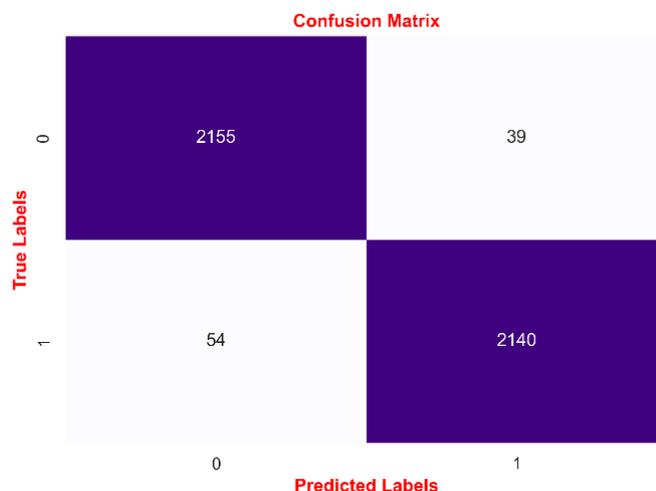


Figure 18: Confusion matrix of the forenXAI model for a 70-learning rate

Figure 18 shows the confusion matrix of the proposed ForenXAI with a training rate of 70 per cent. Among all the predictions, 2155 genuine samples and 2140 forged samples were correctly identified, and only 39 genuine and 54 forged samples were misidentified. These findings indicate that the model is very effective in reducing false positives and false negatives. The accuracy and balance of the classification metrics is a testament to the reliability of forensic handwriting verification, thus affirming that it can be used to validate police evidence.

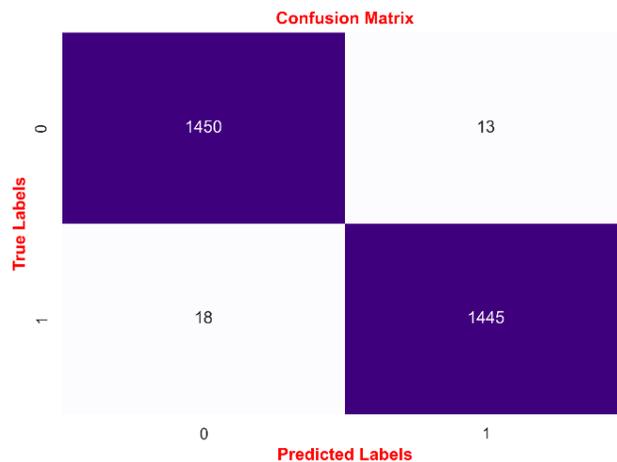


Figure 19: Confusion matrix of the forenXAI model for an 80-learning rate

The confusion matrix of the proposed ForenXAI at an 80 per cent training rate is depicted in Figure 19. The model classified 1450 documents as authentic, and 1445 as forged, with only 13 authentic samples, and 18 forged, being misclassified. These results are better balanced, and thus more accurate, as they reduce both false positives and false negatives. This high reliability indicates that the framework is reliable in forensic handwriting verification and provides reliable evidence validation in practical investigative and judicial contexts.

Malware detection systems have historically concentrated on software and network intrusion detection. The ForenXAI application functions on multiple AI paradigms to counter chargeable digital forgeries and manipulated police evidences. Advanced Digital ForensicsXAI contains counter forensic artificial intelligence and malware countering systems. At this level of development, it utilizes a number of different frameworks, for example, deep learning, Convolutional Neural Networks, and LSTM sequential systems, to capture deep-level digital communications. The system achieves certification and forgery detection at an unmatched level of precision and, thus, reduces document forgeries and greatly contributes to the fight against document forgeries and, thus, the system integrates SHAP-based explainability and risk scoring to deliver transparent automated decisions to the system, which is essential to those decisions in order to avoid the submission of false evidence to a court of law (Figure 20).

The results in Chapter 20 showcase a comparative assessment of four models: ForenXAI, CycleGAN, Ta-RNN, and NSVNN based on their processing time, data integration rate, encryption time, and real-time monitoring delay, as well as SHAP feature importance values. Each of these models along with multiple dependant parameters is illustrated with individual line graphs. These results highlight the differences in the overall performance of the models concerning the evaluation parameters. This will help in selecting the model which is both economical and appropriate.

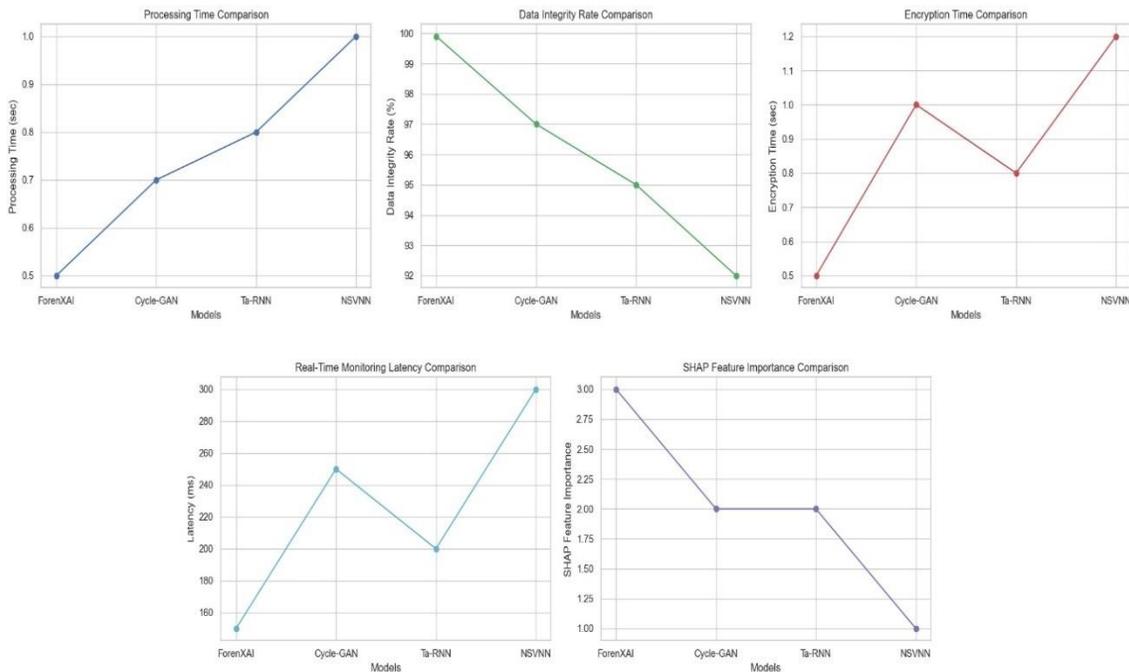


Figure 20: Performance comparison of models in multiple evaluation metrics

Discussion

The experimental results indicate ForenXAI’s proficiency in forensic signature verification and forgery detection. The framework’s accuracy reaches above 97% at 70% training, and continues to improve at 80% training, which through unimodal baseline methods, is easier to attain than at these baselines. Balanced positive predictive value and sensitivity underscored by high F1-score, at low false positive and false negative rates, is critical in forensic settings where the consequences and costs of false conclusions can be catastrophic. With a low false negative rate, the framework prevents forgeries from going undetected, while at a low false positive rate, it recognizes genuine documents. Furthermore, large values of MCC and G-mean demonstrate the model’s high precision and robustness across different samples.

The conducted experiments demonstrate exemplary performance of ForenXAI in forensic signature verification and forgery detection. The framework’s accuracy exceeds 97% and continues to improve with increased training to 85%, which is easier to attain than unimodal baselines. Along with unimodal baselines, the framework has balanced positive predictive value and sensitivity at low false positive and false negative rates, which is vital in forensic science with high Penalty and Cost of Wrong Classification. The framework with low false negative rate performs well in undetected forgery and low positive error rate in genuine document detection. The high values of MCC and G-Mean demonstrate the predictive power and robustness of the model across various samples.

Using SHAP explainability to score risk and the addition of explainability feature positively augments confidence in system reasoning which is important in the judicial system as well. The predicted outcomes are legally defensible and forensic specialists follow the system reasoning and model predictions. The combination of the ‘intelligent’ forgery detection and AI-based forgery detection

protective functions is similar to an intrusion detection system (IDS) in network security. This significantly extends the capacity of ForenXAI to mitigate digital forgeries and the tampering of diverse evidential materials. ForenXAI adds to the whole forensic process credibility by integrating Forensic Intelligence and multi-tiered security architecture which ensures the forensic evidence is safeguarded against tampering to the ForenXAI system. This enhanced forensic integrity and continuity which corroborates the evidential integrity. ForenXAI, in the context of Forensic Intelligence, remains the only integrated system of forensic systems in the market. Particularly, low interpretability and SHAP-based risk scoring are transparent, allowing model decisions to be traced and justified by forensic experts which increases their chances of being accepted in legal proceedings. As discussed, it is clear that the proposed framework is valid, clear, and extensible, and it is highly applicable to practical use in law enforcement and forensic labs.

5 Conclusion

ForenXAI represents a profound achievement in this area of research because it is a cross-modal deep learning model for verification document analysis and forgery detection. The interdisciplinary capabilities of visual forgery detection, textual anomaly detection, cross-modal dual stream verification, and explainable risk scoring capabilities of the system added much-needed specialization to the existing literature, which is lacking in generalization, black box predictions, and some degree of interference. ForenXAI's digitally carried out forensics are accompanied by the highest standards of safety, such as electronic system-generated logs proving the documents are secure throughout verification, archiving, and transmission. Forensic environments are safeguarded by proof of security exceeding fundamental forensic standards to advanced real-time elusive tracking. Even throughout transmission, forensic restriction with security logs is sustained. Within the ecosystem, the proof as well as the digital forensic proof of the forensic workflow is uncontestedly protected and preserved in original state. Individually, the components of the ecosystem exhibit digital protective elements, which cohesively fashion an interlocked proof mosaic to the evidence. The system's performance with training indicates an accuracy level of over 97%, which tends to 99% with added training. When training was done to 70%, the model achieved accuracy (0.9788), precision (0.9821), sensitivity (0.9754), specificity (0.9822), F1-score (0.9787), MCC (0.9576), NPV (0.9756), G-mean (0.9788), FNR (0.0246), and FPR (0.0178). The performance increased further at 80% training with accuracy (0.9894), precision (0.9911), sensitivity (0.9877), specificity (0.9911), F1-score (0.9894), MCC (0.9788), NPV (0.9877), G-mean (0.9894), FNR (0.0123) and FPR (0.0089).

These parallel capabilities confirmed the framework's ability to diminish the core forensics dependability false positives and false negatives. These capabilities aside, forensic practitioners must SHAP explainability and risk scoring model and rationalize decisions from the system's performance and transparency, as well as its legal admissibility. This renders the system appropriate in real policing and courtroom contexts. Its other domain attributes are further attested to by its range of datasets scalability and flexibility. In document forensics, the custody of digital evidence is essential (Hermosilla et al., 2025). ForenXAI preserves evidence workflows by remote monitoring and evidence tracking, reducing the risk of evidence tampering through encircled encryption and lockbox storage, which is inaccessible until properly recognized and subsequently vault-locked for long-term storage. This also minimizes control manipulation triage mistakes. The system further employs explainable AI risk scoring based on SHAP to assess risk across workflow segments, showcasing ForenXAI's sophisticated scalability for automated evidence triage and forgery detection. Work is underway to extend multilingual datasets, real-time forensic proofing system support, blockchain-based evidence tracking, and

adversarial robustness to deepfake handwriting. ForenXAI augmented the precision, explainability, and legal defensibility of AI-powered forensic intelligence systems which helps foster accountability in the system.

References

- [1] Anomah, S., Ayebofo, B., & Aduamoah, M. (2021). An audit risk model for it audits ecosystems and digital transformation (dx) decision making. *Edpacs*, 64(2), 1-33. <https://doi.org/10.1080/07366981.2021.1930643>
- [2] Arora, T., & Naik, A. (2025). Analysis of the Role of Algebraic Structures in Enhancing Cryptographic Security and Encryption Techniques. *International Academic Journal of Science and Engineering*, 12(2), 6-10. <https://doi.org/10.71086/IAJSE/V12I2/IAJSE1211>
- [3] Bae, Y. Y., Cho, D. J., & Jung, K. H. (2025). Enhancing document forgery detection with edge-focused deep learning. *Symmetry*, 17(8), 1208. <https://doi.org/10.3390/sym17081208>
- [4] Balakrishnan, P., & Leema, A. A. (2025). Vulnerabilities and defenses: A monograph on comprehensive analysis of security attacks on large language models. *Indian Journal of Information Sources and Services*, 15(2), 442–467. <https://doi.org/10.51983/ijiss-2025.IJISS.15.2.54>
- [5] Boonkrong, S. (2024). Design of an academic document forgery detection system. *International Journal of Information Technology*, 1-13.
- [6] Fahad, M., Airf, H., Kumar, A., & Hussain, H. K. (2023). Securing against apts: Advancements in detection and mitigation. *BIN: Bulletin of Informatics*, 1(2).
- [7] Fakiha, B. (2024). Investigating the Secrets, New Challenges, and Best Forensic Methods for Securing Critical Infrastructure Networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 15(1), 104-114. <https://doi.org/10.58346/JOWUA.2024.II.008>
- [8] Geistová Čakovská, B., Kalantzis, N., Dziedzic, T., Fernandes, C., Zimmer, J., Branco, M. J., ... & Kerkoff, A. (2021). Recommendations for capturing signatures digitally to optimize their suitability for forensic handwriting examination. *Journal of Forensic Sciences*, 66(2), 743-747. <https://doi.org/10.1111/1556-4029.14627>
- [9] Hall, S. W., Sakzad, A., & Choo, K. K. R. (2022). Explainable artificial intelligence for digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science*, 4(2), e1434. <https://doi.org/10.1002/wfs2.1434>
- [10] Hasan, T., Rahim, M. A., Shin, J., Nishimura, S., & Hossain, M. N. (2024). Dynamics of digital pen-tablet: handwriting analysis for person identification using machine and deep learning techniques. *IEEE Access*, 12, 8154-8177.
- [11] Hermosilla, P., Berríos, S., & Allende-Cid, H. (2025). Explainable AI for Forensic Analysis: A Comparative Study of SHAP and LIME in Intrusion Detection Models. *Applied Sciences*, 15(13), 7329. <https://doi.org/10.3390/app15137329>
- [12] Hosny, K. M., Mortda, A. M., Fouda, M. M., & Lashin, N. A. (2022). An efficient CNN model to detect copy-move image forgery. *IEEE Access*, 10, 48622-48632.
- [13] Ishihara, S., Kulkarni, S., Carne, M., Ehrhardt, S., & Nini, A. (2024). Validation in forensic text comparison: Issues and opportunities. *Languages*, 9(2), 47. <https://doi.org/10.3390/languages9020047>
- [14] Islam, U., Alwageed, H. S., Farooq, M. M. U., Khan, I., Awwad, F. A., Ali, I., & Abonazel, M. R. (2023). Investigating the effectiveness of novel support vector neural network for anomaly detection in digital forensics data. *Sensors*, 23(12), 5626. <https://doi.org/10.3390/s23125626>
- [15] Jabeen, S., Khan, U. G., Iqbal, R., Mukherjee, M., & Lloret, J. (2021). A deep multimodal system for provenance filtering with universal forgery detection and localization. *Multimedia Tools and Applications*, 80(11), 17025-17044.

- [16] Jung, D., Kim, M., & Cho, Y. S. (2022). Detecting documents with inconsistent context. *IEEE Access*, *10*, 98970-98980.
- [17] Khosroshahi, S. N. M., Razavi, S. N., Sangar, A. B., & Majidzadeh, K. (2022). Deep neural networks-based offline writer identification using heterogeneous handwriting data: an evaluation via a novel standard dataset. *Journal of Ambient Intelligence and Humanized Computing*, *13*(5), 2685-2704.
- [18] Longjohn, R., & Smyth, P. (2024). Likelihood ratios for changepoints in categorical event data with applications in digital forensics. *Journal of Forensic Sciences*, *69*(4), 1289-1303. <https://doi.org/10.1111/1556-4029.15512>
- [19] Momeni, S., & BabaAli, B. (2024). A transformer-based approach for Arabic offline handwritten text recognition. *Signal, Image and Video Processing*, *18*(4), 3053-3062.
- [20] Pham, N. T., & Park, C. S. (2023). Toward deep-learning-based methods in image forgery detection: a survey. *IEEE access*, *11*, 11224-11237.
- [21] Prabu, K., & Sudhakar, P. (2022, December). Design and Implementation of an Automated Control System for Anomaly Detection Using an Enhanced Intrusion Detection System. In *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 1-7). IEEE.
- [22] Pragadeswaran, S., Subha, N., Varunika, S., Mouliswar, P., Sanjay, R., Karthikeyan, P., ... & Vaasavathathai, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. *Archives for Technical Sciences*, *31*(2), 148-158. <https://doi.org/10.70102/afts.2024.1631.148>
- [23] Silva, S. H., Bethany, M., Votto, A. M., Scarff, I. H., Beebe, N., & Najafirad, P. (2022). Deepfake forensics analysis: An explainable hierarchical ensemble of weakly supervised models. *Forensic Science International: Synergy*, *4*, 100217. <https://doi.org/10.1016/j.fsisyn.2022.100217>
- [24] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2021). DeepSign: Deep on-line signature verification. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *3*(2), 229-239.
- [25] Wu, Y., Huang, H., Li, Z., & Zhang, S. (2025). CBAM-ResNet: A Lightweight ResNet Network Focusing on Time Domain Features for End-to-End Deepfake Speech Detection. *Electronics*, *14*(12), 2456. <https://doi.org/10.3390/electronics14122456>
- [26] Xi, Z., Huang, W., Wei, K., Luo, W., & Zheng, P. (2023, October). Ai-generated image detection using a cross-attention enhanced dual-stream network. In *2023 Asia Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* (pp. 1463-1470). IEEE.
- [27] Xiao, W., & Ding, Y. (2022). A two-stage siamese network model for offline handwritten signature verification. *symmetry*, *14*(6), 1216.
- [28] Yang, W., Wei, Y., Wei, H., Chen, Y., Huang, G., Li, X., ... & Kang, B. (2023). Survey on explainable AI: From approaches, limitations and applications aspects. *Human-Centric Intelligent Systems*, *3*(3), 161-188.
- [29] Yapıcı, M. M., Tekerek, A., & Topaloğlu, N. (2021). Deep learning-based data augmentation method and signature verification system for offline handwritten signature. *Pattern Analysis and Applications*, *24*(1), 165-179.
- [30] Zeng, P., Tong, L., Liang, Y., Zhou, N., & Wu, J. (2022). Multitask image splicing tampering detection based on attention mechanism. *Mathematics*, *10*(20), 3852. <https://doi.org/10.3390/math10203852>

Authors Biography



S. Nandhini Devi, Research Scholar, PhD Scholar, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai. She has professional experience of more than 12 years working in Teaching, completed Master of Technology in Computer Science Engineering. Acted as Coordinator in various industries and institutions as a part of training, seminars, workshops, international and national conferences. Her teaching and research expertise covers a wide range of subject area including Mobile Computing, Data mining, Deep Learning, Mobile Application Development and Machine learning.



Dr.N. Sabiyath Fatima, Professor, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai. She has professional experience of more than 20 years working in research and teaching. She has published book chapters and more than 40 papers in various National and International peer reviewed journals (IEEE and Springer) and conferences. Acted as resource person, panel member, chief guest, guest of honor and given plenary talk in various industries and institutions as a part of training, seminars, workshops, international and national conferences. She has been active reviewer in various International Journals and Conferences. Her teaching and research expertise covers a wide range of subject area including Mobile Ad Hoc Networks, Data mining, High Performance Computing, IoT, Big data, and Machine learning.