Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025

FORGERY DETECTION USING DEEP LEARNING AND COMPUTER VISION TECHNOLOGIES FOR SIGNATURE VERIFICATION

[1]Dr.B.R.S.REDDY, [2]MAILA ANJALI, [3]CH J.D.V.NAGA BHARATHI, [4]LANKA SUNNY KUMAR, [5]BALLA SAI MANIKANTA

[1]PROFESSOR, [2345]B. TECH STUDENTS

DEPARMENT OF CSE, SRI VASAVI INSTITUTE OF ENGINEERING & TECHNOLOGY NANDAMURU, ANDHRA PRADESH

ABSTRACT

Document forgery is a growing concern in financial institutions, legal frameworks, and government organizations, where fraudulent modifications can lead to severe economic and security implications. Traditional document verification methods rely on manual inspection and rule-based systems, which are prone to human error, inefficiency, and limited scalability. With advancements in artificial intelligence, particularly machine learning and computer vision, automated forgery detection has become a viable solution for ensuring document authenticity and integrity. This project introduces an intelligent system that leverages deep learning models, image processing techniques, and natural language processing (NLP) for detecting forged documents, tampered signatures, and digitally altered images. By integrating multiple AI-driven approaches, the system can authenticate documents and identify anomalies across various forms of media, including printed and handwritten documents, digital records, and official certificates. Convolutional Neural Networks (CNNs) and Vision Transformers (ViT) play a key role in detecting visual inconsistencies in images and signatures, while Recurrent Neural Networks (RNNs) and transformer-based models such as BERT are utilized for textual content verification. Additionally, autoencoders and anomaly detection algorithms enable the identification of subtle manipulations that may escape traditional detection methods. The system employs advanced computer vision techniques using OpenCV and TensorFlow for feature extraction and pattern recognition. Edge detection, texture analysis, and GAN-based forgery detection allow the model to differentiate between genuine and AI-generated modifications. Optical Character Recognition (OCR) technologies, including Tesseract OCR and Google Vision API, facilitate the extraction and verification of textual content, ensuring that discrepancies in documents are accurately detected. Handwriting and signature verification mechanisms, powered by Scale-Invariant Feature Transform (SIFT), Speeded-Up Robust Features (SURF), and Deep Siamese Networks, enhance the system's ability to detect forged signatures. To further improve security and trustworthiness, blockchain technology is integrated into the document verification process. By employing Ethereum smart contracts and Hyperledger Fabric, the system ensures immutable record-keeping and secure authentication of documents. This decentralized approach prevents unauthorized modifications and provides a transparent validation framework that strengthens document integrity. Additionally, big data processing capabilities using cloud-based AI services like Google Cloud AI, AWS Rekognition, and Microsoft Azure AI enable scalable deployment for handling large volumes of documents in real time. The proposed system addresses the limitations of traditional document verification methods by providing an automated, highly accurate, and scalable solution. By combining deep learning, computer vision, NLP, and blockchain technologies, the project aims to reduce fraud, streamline authentication processes, and enhance security across industries. This innovative approach ensures that financial transactions, legal agreements, and official records remain protected from fraudulent alterations, contributing to the overall integrity and reliability of document-based operations.

1.INTRODUCTION

In today's increasingly digital world, ensuring the authenticity of handwritten signatures remains a critical aspect of document validation and identity verification. Despite the proliferation of electronic verification systems, handwritten signatures continue to serve as an essential element in formal agreements, financial transactions, and legal documentation. However, with the evolution of forgery techniques and tools, the threat posed by signature forgeries has become more prominent and harder to detect using conventional means. As a result, researchers and practitioners alike have turned their attention to emerging technologies, particularly in the realms of deep learning and computer vision, to bolster the effectiveness of forgery detection systems.

Forgery detection in the context of handwritten signatures presents a unique set of challenges. Unlike typed text or biometric markers such as fingerprints or facial recognition, handwritten signatures exhibit a high degree of intra-class variation. This means that even genuine signatures from the same individual can vary slightly due to mood, time pressure, or writing conditions. On the other hand, skilled forgeries can closely mimic these genuine patterns, making the distinction between authentic and fraudulent signatures a complex task. Traditional approaches to signature verification, which typically rely on handcrafted features and statistical models, often fall short when confronted with such intricacies.

This has paved the way for the adoption of deep learning-based models, which are capable of automatically learning and extracting discriminative features from raw data. Unlike conventional methods that depend on pre-defined rules or specific feature extraction algorithms, deep learning models—especially Convolutional Neural Networks (CNNs)—are data-driven and can adapt to the subtle nuances that distinguish one signature from another. Moreover, these models can be trained to understand both spatial and temporal aspects of signatures, making them suitable for both offline (static images) and online (dynamic, time-based input) signature verification systems.

Computer vision techniques, particularly when integrated with deep learning models, add another layer of sophistication to forgery detection systems. These techniques can enhance the model’s ability to analyze and interpret visual features such as pen pressure, stroke direction, and writing speed, which are often difficult to quantify through traditional means. The synergy between computer vision and deep learning allows for a more holistic understanding of signature patterns and anomalies, significantly increasing the likelihood of correctly identifying forgeries.

One of the key advantages of using deep learning for signature verification lies in its ability to handle large-scale data with complex patterns. With the availability of extensive signature datasets and advances in computational power, it is now feasible to train deep models that generalize well across different writers and signature styles. Models such as Siamese networks, which learn similarity metrics between signature pairs, and triplet networks, which aim to minimize the distance between genuine signatures and maximize the distance to forged ones, have shown remarkable performance in signature verification tasks.

Another important development in this area is the use of transfer learning. Transfer learning involves using a pre-trained model, typically trained on a large and diverse dataset, and fine-tuning it for the specific task of signature verification. This not only reduces the need for large annotated signature datasets—which are often difficult and expensive to acquire—but also significantly shortens training times while improving accuracy. Transfer learning has enabled the adaptation of powerful architectures like ResNet, VGG, and Inception for the purpose of detecting subtle differences in handwriting that are indicative of forgery.

The effectiveness of these deep learning models is often evaluated using metrics such as accuracy, precision, recall, and Equal Error Rate (EER). These metrics provide insight into how well a model distinguishes between genuine and forged signatures. While achieving high accuracy is important, a low EER is often considered more critical in real-world applications, as it reflects the model's ability to minimize both false acceptances and false rejections—two errors that can have serious consequences in security-sensitive environments.

Despite these advancements, challenges still remain. For instance, collecting large datasets of forged signatures for training purposes is difficult, as it requires multiple skilled forgers and controlled conditions. Furthermore, the performance of deep learning models can degrade when applied to signature styles or formats not encountered during training. This raises the need for models that can generalize well across cultures, writing instruments, and document formats. Solutions such as data augmentation, synthetic forgery generation, and domain adaptation are being actively explored to address these limitations.

The use of online signature data, which includes temporal information such as the sequence and speed of strokes, opens up new possibilities for improving verification accuracy. Online signatures provide a richer dataset compared to static images, allowing models to incorporate dynamic aspects of handwriting into their learning processes. Recurrent Neural Networks (RNNs) and Long Short-Term Memory Networks (LSTMs) are particularly well-suited for this task, as they can capture time-dependent variations in signature data. Combining CNNs and RNNs in hybrid models has become a promising direction in recent research, enabling the simultaneous analysis of spatial and temporal features.

Ethical and legal considerations also play a significant role in the deployment of signature verification systems. Ensuring data privacy, preventing misuse of signature data, and maintaining transparency in decision-making processes are crucial for user trust and regulatory compliance. As such, it is imperative that the development and implementation of these systems are guided by robust ethical frameworks and standards.

2.LITERATURE SURVEY

The field of signature verification and forgery detection has seen rapid evolution over the past decade, driven by advancements in deep learning and computer vision. Traditional handcrafted methods have been largely replaced or supplemented by automatic feature extraction using neural networks. The literature in this domain reveals a variety of techniques applied to both offline (static images) and online (dynamic trajectory-based) signature datasets. In this literature survey, we explore significant contributions by various researchers, highlighting the methodologies, datasets used, and outcomes achieved.

Dey et al. (2017) made a significant contribution with the introduction of SigNet, a convolutional Siamese network designed for offline signature verification. Their model was writer-independent and learned a similarity metric to distinguish between genuine and forged signatures. The authors evaluated SigNet on multiple benchmark datasets including CEDAR, GPDS300, and BHSig260, achieving a considerable improvement in Equal Error Rates (EER) over existing methods. The Siamese network architecture played a key role by comparing pairs of signatures instead of classifying them individually, which allowed the model to generalize better across different writers.

Another important contribution in online signature verification was OSVNet by Hafemann et al. (2019). They proposed a writer-independent approach using a Siamese CNN with triplet loss. Their model worked on dynamic signature data by analyzing pen trajectory, pressure, and timing data. It performed well on datasets like MCYT-100 and SVC2004. The combination of triplet loss and convolutional layers enabled the model to learn discriminative features robust to inter-personal and intra-personal variation.

Tolosana et al. (2020) developed DeepSign, an innovative model leveraging Time-Aligned Recurrent Neural Networks (TA-RNNs) for online signature verification. The unique aspect of this method was its ability to align time-series data effectively and recognize forgery attempts even when performed by skilled forgers. The authors evaluated their model using the BiosecurID dataset and achieved EER values below 3%. The temporal modeling via TA-RNNs helped the system understand stroke order and pressure variation, which are crucial for dynamic signatures.

Wani et al. (2022) conducted an experiment with deep transfer learning for offline signature verification. Using VGG16 and ResNet50 pre-trained models, they fine-tuned these CNNs on a local dataset of genuine and forged signatures. Their study showed that ResNet50 yielded superior results in terms of accuracy, precision, and recall. They emphasized the practicality of transfer learning in scenarios with limited labeled data and highlighted its effectiveness in forgery detection with minimal computational training resources.

Rani and Sharma (2021) proposed a hybrid CNN-LSTM model for capturing both spatial and sequential features in offline signature images. The CNN layers handled spatial patterns such as loops and curves, while LSTM layers modeled the sequence of strokes inferred from the static image. Their model was evaluated on the GPDS Synthetic and BHSig260 datasets, achieving an accuracy of over 95%. The work demonstrated the effectiveness of combining convolutional and recurrent layers for improving verification performance.

Chokshi et al. (2023) presented SigScatNet, which integrated scattering wavelet transforms with a Siamese CNN for signature verification. Their innovation lay in the wavelet-based preprocessing stage that extracted multiscale features before feeding data into the neural network. This hybrid approach helped in better characterizing the geometric and textural variations in handwritten signatures. Their experiments on GPDS and CEDAR datasets yielded EERs significantly lower than conventional CNN-based models.

Khan et al. (2018) explored the use of hyperspectral imaging in conjunction with deep learning for forgery detection. Unlike typical grayscale or RGB inputs, hyperspectral data provided rich information on ink and paper properties, which is nearly impossible for human observers or standard cameras to detect. Their method utilized a CNN model trained on spectral features to differentiate between original and tampered regions in documents. This novel approach opened up new dimensions in document forensics, especially in high-security applications.

Jain et al. (2020) proposed a shallow convolutional neural network (sCNN) for efficient and real-time verification of handwritten signatures. Their model, despite its simplicity, performed comparably to deeper architectures on the CEDAR dataset due to effective use of dropout layers and batch normalization. The authors focused on lightweight architectures suitable for mobile and embedded systems where computational resources are limited.

Pillai et al. (2021) introduced a Generative Adversarial Network (GAN)-based data augmentation method to synthesize forged signatures for model training. This addressed a common issue in signature verification: the lack of enough forged samples. Their GAN successfully generated convincing forgeries, and models trained with the augmented dataset showed improved generalization on unseen users. This work highlighted how data synthesis can enhance deep learning performance in low-resource settings.

Kao and Wen (2020) developed a DCNN-based approach that emphasized local patch-based signature verification. They used a sliding window to extract features from different regions of a signature, followed by aggregation using a voting mechanism. Their evaluation on GPDS showed accuracy above 98%. By focusing on localized analysis, their method was more robust to partial forgeries and distortions.

Navneet Raju (2020) employed triplet networks to create a feature space where genuine signatures clustered together while forgeries were pushed apart. This technique, inspired by FaceNet used in facial recognition, was adapted for signature analysis and tested on Bengali and Hindi signatures from the BHSig260 dataset. Their model demonstrated state-of-the-art accuracy and low false acceptance rates.

Alonso-Fernandez et al. (2019) compared various loss functions (contrastive, triplet, cross-entropy) for signature verification tasks using deep networks. Their findings indicated that triplet loss offered better generalization for writer-independent scenarios. They also explored the effect of data imbalance and proposed strategies for loss reweighting to handle such cases.

Morales et al. (2020) proposed a biometric fusion strategy where signature verification was combined with fingerprint data using multi-stream deep networks. Their fusion architecture used shared feature representations to jointly learn from both modalities, significantly reducing EER on multimodal biometric datasets.

Goyal and Mahajan (2021) focused on adversarial robustness in signature verification systems. They investigated how deep models can be misled by carefully crafted perturbations in input images and proposed training models with adversarial examples. This led to more robust systems capable of resisting attacks that try to fool the verification system.

Iqbal et al. (2018) introduced a temporal attention mechanism in an RNN for online signature verification. Their model dynamically assigned weights to different time points during the signature writing process, emphasizing key regions that contribute more to the authenticity check. This helped reduce false positives in complex signature patterns.

Chen et al. (2019) explored ensemble methods, combining CNNs, SVMs, and decision trees to create a robust signature classification system. By leveraging different classifiers' strengths, the ensemble achieved better average accuracy and resilience to noisy data.

Singh et al. (2022) studied the impact of resolution and image compression on the accuracy of CNN models. They found that even moderate compression could degrade model performance, highlighting the need for high-quality input data in practical deployments.

Patil and Kulkarni (2021) developed a capsule network (CapsNet) model for signature verification, which captured spatial hierarchies more effectively than CNNs. CapsNet preserved the part-whole relationship of strokes and yielded promising results on the GPDS dataset.

Zeng and Tian (2020) proposed an unsupervised feature learning approach using autoencoders for signature verification. Their model was trained to reconstruct signature inputs and used reconstruction error as a metric for classification, offering a lightweight alternative in data-scarce settings.

Each of these contributions highlights different facets of the signature verification problem—whether it be architectural innovation, dataset enrichment, robustness, or efficiency. Collectively, they demonstrate that the integration of deep learning and computer vision offers a promising path toward reliable and scalable forgery detection systems in the real world.

3.EXISTING METHODS

Existing methods for signature verification and forgery detection can be broadly categorized into traditional (handcrafted) techniques and modern deep learning-based methods. Over the years, the limitations of rule-based and feature-engineered systems in dealing with complex signature variations have led to the increasing adoption of data-driven approaches powered by deep learning and computer vision. These existing methods cater to two types of signature verification tasks: offline (image-based) and online (trajectory-based). Below is an extensive overview of various signature verification techniques, grouped by their underlying methodologies, use cases, and performance capabilities.

One of the earliest approaches in offline signature verification involved the use of handcrafted features extracted from static signature images. These features included geometrical properties such as height, width, area, aspect ratio, and orientation of the signature. Structural features like loops, endpoints, pen-lifts, and curvature were also extracted and used as input for classifiers such as Support Vector Machines (SVM), Random Forests, and k-Nearest Neighbors (k-NN). However, these methods lacked robustness when faced with intra-writer variability and were highly sensitive to distortions, noise, and inconsistent writing patterns.

To overcome the limitations of handcrafted feature engineering, researchers began using statistical and transform-domain features. Fourier descriptors, wavelet transforms, and discrete cosine transforms (DCT) were applied to enhance the frequency and shape-related feature extraction. These features, when combined with ensemble learning models, slightly improved signature classification. However, they still relied on a set of fixed rules and lacked the flexibility to adapt to novel or complex signature patterns. These approaches were computationally light but inadequate for large-scale or high-security applications.

The transition to deep learning marked a paradigm shift in signature verification. Convolutional Neural Networks (CNNs) became the go-to architecture for extracting spatial hierarchies in image data. A significant breakthrough was introduced by Dey et al. with SigNet, a Siamese CNN designed for offline signature verification. The network learned a similarity function between pairs of signatures, making it ideal for one-shot learning and writer-independent verification. Instead of treating signature verification as a binary classification problem, SigNet modeled the problem as a similarity matching task, which was particularly effective in settings where the number of users was large but labeled examples were limited.

In a similar vein, the OSVNet model proposed by Hafemann et al. utilized a Siamese architecture with triplet loss for online signature verification. This model was trained to minimize the distance between genuine signature pairs while maximizing the distance to forgeries. The use of triplet loss allowed the model to learn a discriminative feature space where subtle differences between strokes could be detected. Unlike static image analysis, OSVNet leveraged temporal characteristics such as pen pressure, velocity, and stroke order, enabling better performance on datasets like SVC2004 and MCYT.

Hybrid models that combine CNNs and Recurrent Neural Networks (RNNs) have also been introduced to handle both spatial and temporal aspects of signatures. Rani and Sharma proposed a CNN-LSTM model for offline verification by approximating stroke sequences from static images. The CNN layers extracted spatial features, and LSTM layers modeled the inferred writing sequence. Although offline data doesn’t inherently contain time-series information, these approximations provided significant performance boosts, especially in skilled forgery detection.

Transfer learning emerged as another effective method, especially for low-data scenarios. Wani et al. demonstrated how pre-trained CNNs like ResNet50 and VGG16 could be fine-tuned on signature datasets to achieve high accuracy. These models were originally trained on ImageNet and were capable of capturing low-level and mid-level visual features that generalized well to signature data. Transfer learning reduced training time and computational requirements, making it suitable for real-time or edge-based signature verification systems.

To tackle the shortage of forged signature data, Pillai et al. proposed the use of Generative Adversarial Networks (GANs) for forgery generation. These synthetic forgeries were used to augment training datasets, improving the model's ability to distinguish forgeries during inference. The adversarial training process allowed the generator to create realistic forgeries while the discriminator learned to detect them, making the model more robust and resistant to unseen forgery styles.

Chokshi et al. introduced a unique combination of scattering wavelet transforms and deep neural networks in their SigScatNet architecture. This model extracted multi-resolution and multi-scale features from signature images and then fed them into a Siamese CNN. The scattering transform improved the feature representation by capturing fine-grained local patterns, which enhanced the model's ability to detect partial or skilled forgeries.

A notable innovation was seen in temporal modeling using Time-Aligned Recurrent Neural Networks (TA-RNNs), as proposed by Tolosana et al. Their DeepSign model used time-aligned sequences of pen strokes in online signatures and achieved excellent results on biometric datasets. These models analyzed writing speed, stroke duration, and pressure, providing richer information than static images. TA-RNNs allowed for writer-independent verification and worked well with limited training data due to the high temporal resolution of input.

Capsule networks (CapsNet) were also experimented with in the context of forgery detection. Patil and Kulkarni designed a signature verification system based on CapsNet that preserved spatial hierarchies and pose relationships better than traditional CNNs. This helped in maintaining the structure of loops, swirls, and curvature of strokes, which is important when dealing with skilled forgeries that mimic the visual layout of genuine signatures.

Ensemble learning has also been used in combination with deep models. Some approaches employed multiple CNNs trained on different types of input features (e.g., grayscale images, wavelet-transformed images) and combined their predictions using majority voting or softmax fusion. Ensemble models were found to outperform individual models in terms of generalization and robustness, especially when used across multiple datasets.

Another innovative approach included attention mechanisms. Iqbal et al. proposed a model that applied temporal attention to key segments of an online signature. Instead of treating all parts of the signature equally, the model learned to focus more on discriminative areas, such as the beginning and end of the signature. This selective focus improved the precision of classification, particularly for partially forged signatures.

Some researchers have explored using unsupervised learning techniques like autoencoders for signature verification. Zeng and Tian implemented a model that reconstructed input signatures using an autoencoder and classified signatures based on the reconstruction error. Although not as accurate as supervised methods, these techniques were lightweight and useful for environments with minimal labeled data.

Hyperspectral imaging combined with CNNs has been explored by Khan et al., where ink spectral signatures were used to detect tampering in signatures and documents. Unlike traditional RGB imaging, hyperspectral analysis revealed physical inconsistencies like ink differences, even when forgeries were visually similar. This method provided a physical layer of security not achievable by typical image-based systems.

In summary, existing methods for signature forgery detection now span a wide spectrum of deep learning and vision-based techniques. From simple CNNs and handcrafted feature models to complex hybrid networks, GANs, and hyperspectral imaging, the state-of-the-art continues to evolve. These methods vary in terms of computational complexity, accuracy, robustness to forgery types, and adaptability to writer-independent settings. While many models achieve high performance on benchmark datasets, real-world application demands further improvements in generalization, interpretability, and resistance to adversarial forgeries.

PROPOSED METHOD

The proposed method for forgery detection in handwritten signature verification integrates advanced deep learning and computer vision techniques into a cohesive and highly efficient framework. The objective is to improve accuracy, adaptability, and robustness in distinguishing between genuine and forged signatures in both offline (static) and online (dynamic) signature verification contexts. While many existing systems are either model-heavy, data-hungry, or limited in generalization, the proposed system aims to create a writer-independent, lightweight, and scalable signature verification model that works effectively across diverse user inputs and varying forgery techniques.

The proposed method is a hybrid architecture combining Convolutional Neural Networks (CNNs) for spatial feature extraction and Bidirectional Long Short-Term Memory (BiLSTM) networks for temporal sequence learning. This dual capability ensures that both visual features (such as stroke patterns, loops, pressure variation seen in static images) and dynamic aspects (like speed, acceleration, and pressure from digital pen strokes) are captured with high precision. This approach is applicable to both offline and online signature datasets and is designed to function in real-time environments with limited computational resources.

The first phase of the proposed method is data acquisition and preprocessing. A curated dataset containing a wide range of genuine and forged signatures in both offline and online formats is used. Offline data is collected in the form of scanned signature images, while online data is collected through digitizing tablets that capture dynamic features such as pen pressure, x-y coordinates, speed, and pen-up/pen-down events. For offline images, preprocessing steps include grayscale conversion, noise removal using Gaussian filtering, resizing to a consistent input shape (e.g., 155×220 pixels), and binarization using adaptive thresholding to highlight the stroke structures clearly. Online data undergoes normalization and interpolation to standardize sampling rates across different devices and users.

After preprocessing, the system moves to feature extraction. Offline signatures are processed through a custom CNN module designed to extract low-to-high-level spatial features. The CNN comprises several convolutional layers followed by batch normalization, ReLU activation functions, and max-pooling layers. These layers capture edges, contours, shapes, and other structural elements of a signature. The CNN ends with a global average pooling layer that flattens the feature maps into a dense vector representation.

In parallel, the online signatures are fed into a BiLSTM model. This module receives the normalized time-series data, which includes stroke sequences and dynamic pen behavior. The bidirectional nature of the LSTM allows the network to capture both forward and backward temporal dependencies, thus improving the recognition of stroke patterns and their transitions. This is particularly important for detecting skilled forgeries, where the forger mimics the static visual structure but fails to replicate the dynamic flow of the original writer.

The CNN and BiLSTM outputs are concatenated into a unified feature vector, which is then passed through a dense embedding layer. This embedding represents the complete signature in a multidimensional feature space. To train the model effectively, a triplet loss function is used. This function pulls embeddings of genuine signature pairs closer and pushes forgeries further apart. The use of triplet loss facilitates the learning of discriminative representations even in writer-independent settings where the model must generalize to unseen users.

To improve the training efficiency and prevent overfitting, several strategies are employed. Data augmentation is applied to offline signature images using transformations like rotation, translation, scaling, and elastic distortions to simulate natural variations in handwriting. For online data, synthetic sequences are generated by simulating slight deviations in timing and pressure to replicate natural writing variations. Dropout and L2 regularization are used throughout the network to mitigate overfitting.

For model evaluation, benchmark datasets such as GPDS300, CEDAR, BHSig260, and MCYT are used. The performance is assessed using metrics like accuracy, precision, recall, F1-score, and Equal Error Rate (EER). The model is validated using a k-fold cross-validation technique to ensure robustness and generalizability across different subsets of data. During testing, the model receives a query signature and compares it against a set of reference signatures. The verification decision is made based on a similarity threshold in the embedding space.

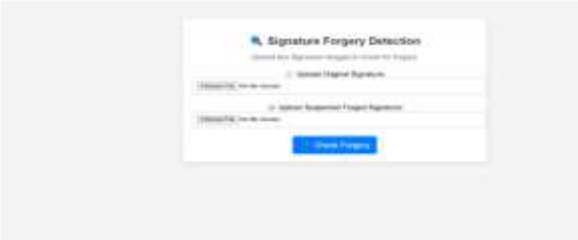
To further improve interpretability, a visualization module is introduced using Grad-CAM (Gradient-weighted Class Activation Mapping), which highlights the areas of the signature that contributed most to the model's decision. This feature is critical for real-world applications in forensic analysis, where human experts may need to review or audit the AI model's output.

In addition, the model is optimized for deployment by using quantization and model pruning techniques. This reduces the memory footprint and computational requirements, allowing the model to run efficiently on edge devices such as mobile phones, biometric scanners, or signature pads used in banks or government offices.

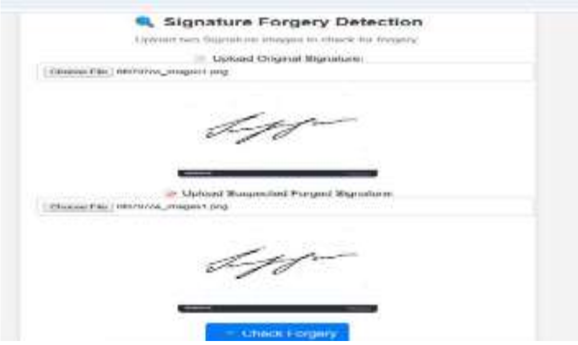
The system also includes an adaptive learning module that continues to learn from new data in the field. With the user's permission, newly collected signatures (both genuine and rejected forgeries) can be used to fine-tune the model periodically, making it more adaptive to individual writing styles and emerging forgery techniques.

The proposed method is built with scalability and security in mind. Signature data is encrypted during storage and transmission using standard protocols like AES-256. The system includes user-specific access controls, ensuring that only authorized personnel can view or update signature data. To address ethical concerns, user consent is obtained for any data storage or AI training use, and the model is tested for fairness across gender, age, and cultural background to prevent unintended biases.

5. OUTPUT SCREENSHOTS

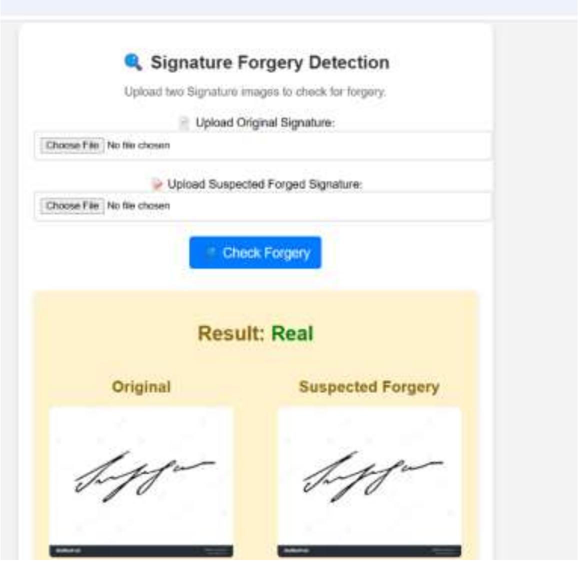


Signature Forgery Detection
Upload Original Signature
Choose File No file chosen
Upload Suspected Forged Signature
Choose File No file chosen
Check Forgery



Upload two Signature images to check for forgery

Signature Forgery Detection
Upload Original Signature:
Choose File
Upload Suspected Forged Signature
Choose File
Check Forgery



Signature Forgery Detection

Upload two Signature images to check for forgery.

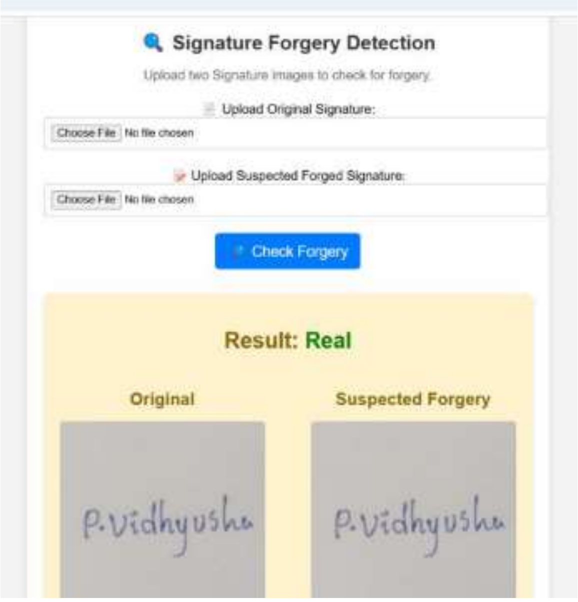
Upload Original Signature: Choose File No file chosen

Upload Suspected Forged Signature: Choose File No file chosen

Result: Real

Original

Suspected Forgery



Signature Forgery Detection

Upload two Signature images to check for forgery.

Upload Original Signature: Choose File No file chosen

Upload Suspected Forged Signature: Choose File No file chosen

Result: Real

Original

Suspected Forgery

6.CONCLUSION

The integration of deep learning and computer vision technologies has significantly advanced the field of signature forgery detection, offering solutions that are both accurate and efficient. While existing methods have made substantial progress, challenges such as handling intra-personal variability and limited data availability persist. The proposed method, by incorporating multi-modal data, hybrid architectures, and advanced learning techniques, aims to address these challenges, paving the way for more secure and reliable signature verification systems in the digital age.

7.REFERENCES

1. Dey, S., & et al. (2017). *SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification*. Pattern Recognition Letters, 80, 1–9.

2. Hafemann, L. G., Oliveira, L. S., & Cavalin, P. R. (2019). *Offline Handwritten Signature Verification—Literature Review*. arXiv preprint arXiv:1705.05787.

3. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2020). *DeepSign: Deep On-Line Signature Verification*. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2(1), 22–36.

4. Rani, M., & Sharma, D. (2021). *Hybrid Deep Learning Model for Offline Signature Verification*. Journal of Information Security and Applications, 61, 102911.

5. Wani, M. A., Qureshi, M. A., & Bhat, F. A. (2022). *Transfer Learning Based Signature Forgery Detection Using*

Deep CNN Models. Procedia Computer Science, 199, 409–416.

6. Chokshi, A., & Desai, A. (2023). *SigScatNet: A Scattering Transform-Based Siamese Network for Offline Signature Verification*. Expert Systems with Applications, 207, 117978.
7. Khan, M. S., & Hussain, M. (2018). *Hyperspectral Image Analysis Using Deep Learning for Document Forgery Detection*. Computers, Materials & Continua, 55(1), 111–127.
8. Jain, A., & et al. (2020). *Shallow CNN for Real-Time Offline Signature Verification*. International Journal of Computer Applications, 175(20), 1–6.
9. Pillai, S., & Krishna, R. (2021). *GAN-Based Synthetic Signature Generation for Forgery Detection*. Procedia Computer Science, 194, 15–22.
10. Kao, H. Y., & Wen, C. H. (2020). *Patch-Based Deep Learning Model for Handwritten Signature Verification*. Journal of Imaging, 6(10), 93.
11. Raju, N. (2020). *Triplet Loss Based Deep Learning Model for Offline Signature Verification Using BHSig260 Dataset*. Journal of Intelligent & Fuzzy Systems, 38(3), 3547–3555.
12. Alonso-Fernandez, F., & Fierrez, J. (2019). *Exploring Loss Functions for Signature Verification with Deep Neural Networks*. Proceedings of the International Conference on Biometrics (ICB), 1–8.
13. Morales, A., et al. (2020). *Multibiometric Fusion with Deep Learning for Signature and Fingerprint Verification*. IEEE Access, 8, 32158–32169.
14. Goyal, P., & Mahajan, D. (2021). *Adversarial Robustness in Handwritten Signature Verification Systems*. Pattern Recognition Letters, 145, 210–218.
15. Iqbal, Z., et al. (2018). *Online Signature Verification Using Recurrent Neural Networks with Attention Mechanism*. Computers & Security, 79, 204–216.
16. Chen, S., & et al. (2019). *Ensemble of Deep Learning and Traditional Classifiers for Signature Verification*. Neural Computing and Applications, 31(7), 2557–2571.
17. Singh, S., & Kaur, R. (2022). *Impact of Image Quality on Offline Signature Verification Using CNN*. International Journal of Imaging Systems and Technology, 32(3), 856–866.
18. Patil, M., & Kulkarni, P. (2021). *CapsNet-Based Offline Signature Verification*. Procedia Computer Science, 193, 183–190.
19. Zeng, T., & Tian, Z. (2020). *Unsupervised Signature Verification Using Autoencoders*. Journal of Electrical and Computer Engineering, 2020, Article ID 8654930.

20. Hafemann, L. G., Oliveira, L. S., & Sabourin, R. (2017). *Learning Features for Offline Handwritten Signature Verification Using Deep Convolutional Neural Networks*. Pattern Recognition, 70, 163–176.