

Signature Fraud Detection Using Deep Learning

G. Swetha¹, C. Umadevi², M. Govardhan³,
V. Tharun⁴, M. C Bhanu Prasad⁵

Department of CSE, Tadipatri Engineering College, Tadipatri.

Abstract:

Signature verification is commonly used for the signature is real or fake. Signatures are used in banks, offices, and legal documents. Fraudulent signatures can cause serious financial loss. Manual signature verification is not always reliable. Human errors may occur during verification. Therefore, an automatic signature fraud detection system is needed. This project focuses on signature fraud detection using deep learning methods. The system works with offline handwritten signature images. Signature samples are collected from different individuals. These samples are converted into digital image format. Image preprocessing is performed to remove noise. Image resizing and normalization are also applied. Convolutional Neural Network (CNN) is used for feature extraction. CNN helps in identifying important signature patterns. It learns features such as shape, curves, and strokes. CNN improves accuracy in image classification tasks. It reduces the need for manual feature selection. Siamese Neural Network is used for signature comparison. It compares two signature images at a time. The network checks similarity between input signatures. It determines whether the signatures belong to the same person. Siamese network is effective for verification problems. The system compares test signatures with stored reference signatures. Based on similarity score, the signature is verified. The output shows whether the signature is genuine or forged. The model is trained using labeled signature data. Testing is done using unknown signature samples. The performance is measured using accuracy and error rate. The system provides fast and reliable results. It reduces dependency on manual verification. This method improves security in authentication systems. It is suitable for banking and document verification applications.

Keywords: Signature Fraud Detection, Deep Learning, Siamese Neural Network, Biometric Authentication, Kaggle Dataset, Image Verification.

I.INTRODUCTION

Signature fraud detection is used to verify whether a signature is genuine or forged. Signature play an important role in banks, legal documents and identify verification. Manual checking of signatures is difficult and may lead to mistakes. Therefore, automated systems using deep learning are preferred. This approach, a kaggle signature dataset is used, which contains genuine and forged signature images. Image processing techniques such as re-sizing, grayscale conversion and normalization are applied to improve image quality and make all signatures uniform. These processed images are then used for training the model. A Siamese Neural Network is a special type of deep learning model that compares two signatures images at a time. It learns measure the similarity between signatures instead of classifying them directly. If the similarity score is high the signature is considered genuine method improves accuracy and works well even with limited training data. This system provides a reliable, fast and accuracy way to detect signature fraud and reduces dependence on manual verification.

Deep Learning is a subset of machine learning that uses multi layered neural networks to learn complex patterns in data. Signature fraud detection using deep learning has become an effective solution. Deep learning modules can automatically learn important features from signature images, such as shape, stroke patterns, and writing style. These features help the system distinguish between genuine and forged signatures with high accuracy. Siamese Neural Network takes two input images at a time and compress both, check whether they belong to same or not. A Siamese Neural Network uses two identical CNN's with shared weights to extract feature vectors to determine similarity. If the distance is below a threshold, the signature is genuine otherwise it is considered forged.

II. LITERATURE REVIEW

In [1] P. P. K., A. J. S. P., and B. B., “Advanced Deep Learning Algorithm for Offline Signature Fraud Detection” (ICCES, 2024) studies offline handwritten signature verification for fraud detection. The research uses scanned signature images and applies preprocessing like noise removal, normalization, and feature enhancement. A convolution-based model is proposed to learn discriminative signature patterns and classify signatures as genuine or forged. Experimental results show improved accuracy of 92.5%, with higher precision and recall than traditional machine learning methods. Limitations include small dataset size, no cross-dataset validation, and lack of real-world deployment analysis, affecting generalization.

[2] N. Shetty, S. Shetty, and N. Shetty, “Deep Learning-Powered Signature Authentication: The Signature Verify CNN Model” (ICAISS, 2025) studies offline handwritten signature verification. The research uses scanned signature images with preprocessing steps like noise reduction, normalization, and feature enhancement. Experimental results demonstrate high accuracy is 90.6%, precision, and recall compared to traditional machine learning methods. Limitations include small dataset size, lack of cross-dataset validation, and no real-world deployment analysis, which may affect generalization across diverse signatures.

[3] E. F. Rudico, J. M. Y. Armocilla, and M. V. C. Caya, “Detection of Offline Handwritten Signature Forgery Using InceptionV4 with Sobel Edge Detection” (DSPA, 2025) focuses on offline signature forgery detection. It employs an InceptionV4-based deep learning model to learn distinctive signature patterns and classify signatures as genuine or forged. Experimental results show high accuracy is 96.9%, precision, and recall, outperforming conventional machine learning approaches. Limitations include limited dataset size, absence of cross-dataset validation, and no real-world deployment testing, affecting generalization across diverse signatures.

[4] A. S. M., S. Suvarna, and R. K. T., “Online Digital Cheque Signature Verification using Deep Learning Approach” (ICECAA, 2023) focuses on online digital cheque signature verification. The study uses digital signature data captured during signing and applies preprocessing such as normalization and noise reduction. Experimental results demonstrate high accuracy is 93.9%, precision, and recall compared to traditional machine learning methods. Limitations include limited dataset size, no cross-dataset validation, and absence of real-world deployment testing, affecting generalization across diverse signatures.

[5] O. Tarek and A. Atia, “Forensic Handwritten Signature Identification Using Deep Learning” (SETIT, 2022) focuses on forensic offline handwritten signature identification. A deep learning-based model is employed to extract discriminative features for identifying and verifying signatures. Experimental results demonstrate improved accuracy is 91.8% , precision, and recall compared to conventional techniques.

Limitations include limited dataset size, lack of cross-dataset validation, and absence of real-world forensic deployment analysis, which may affect generalization.

[6] O. Tarek and A. Atia, “Forensic Handwritten Signature Identification Using Deep Learning” (SETIT, 2022) focuses on forensic offline handwritten signature identification. The study uses scanned handwritten signature images and applies preprocessing such as noise removal and normalization. A deep learning-based model is employed to extract discriminative features for identifying and verifying signatures. Experimental results demonstrate improved accuracy is 95.7%, precision, and recall compared to conventional techniques. Limitations include limited dataset size, lack of cross-dataset validation, and absence of real-world forensic deployment analysis, which may affect generalization.

[7] G. K. Pandey, V. Raj, A. Agarwal, M. Dixit, S. S. Chauhan, and S. Srivastava, “Offline Signature Verification: An Extensive Survey of Deep Learning Methods” (ICSADL, 2025) presents a comprehensive survey of offline signature verification. It analyzes various deep learning architectures, including CNN's and hybrid models, used for signature verification and forgery detection. The survey highlights performance improvements in accuracy is 97.2%, precision, and recall achieved by deep learning methods over traditional approaches. It discusses strengths and challenges of existing models in handling skilled and random forgeries.

[8] C. A. Krishna and R. Bhuvanewari, “Offline Signature Forgery Detection using Multi-Layer Perceptron” (ASIANCON, 2023) focuses on offline handwritten signature forgery detection. A Multi-Layer Perceptron (MLP) model is employed to learn signature features and classify signatures as genuine or forged. Experimental results show improved accuracy is 95.4%, precision, and recall compared to traditional rule-based approaches. Limitations include limited dataset size, lower performance compared to deep CNN-based models, and lack of cross-dataset validation and real-world testing, affecting generalization.

[9] S. Bhirud, S. Bijwe, T. Chavan, A. Bhonsle, S. Rukhande, and D. G., “Deep Transfer Learning for Authenticating Handwritten Signatures” (EAIC, 2025) focuses on offline handwritten signature authentication. Experimental results demonstrate improved accuracy is 95.8%, precision, and recall compared to traditional machine learning methods. Limitations include dependency on pre-trained models, limited dataset size, lack of cross-dataset validation, and absence of real-world deployment analysis, affecting generalization.

[10] R. N. Mistry, N. More, S. Patil, and C. Desai, “Multilingual Signature Verification Using Deep Learning: A Three-Phase Modular Approach” (ICCUBE, 2025) focuses on offline multilingual handwritten signature verification. It proposes a three-phase modular deep learning framework for feature extraction, verification, and classification of signatures. Experimental results show high accuracy is 96.7%, precision, and recall across different language scripts compared to traditional approaches. Limitations include increased system complexity, limited cross-dataset validation.

[11] A. A. Lakshmi, G. S. Reddy, M. S. Reddy, and N. Kathirisetty, “Offline Signature Forgery Detection Based on Geometric Measures Using Tensorflow Model” (ASSIC, 2024) focuses on offline handwritten signature forgery detection. Experimental results demonstrate improved accuracy is 98.5%, precision, and recall compared to traditional machine learning techniques.

Limitations include dependence on geometric feature quality, and absence of real-world deployment evaluation, which may affect generalization.

[12] S. C. Nossam, R. A. Katakam, G. Pulastya, and S. Jayan, "Signature Forgery Detection and Verification using Deep Learning Techniques" (ICCCNT, 2024) focuses on offline handwritten signature forgery detection and verification. The study utilizes scanned signature images with preprocessing steps such as noise removal and normalization. Experimental results demonstrate improved accuracy is 98.2%, precision, and recall compared to conventional machine learning approaches. Limitations include limited dataset size, lack of cross-dataset validation, which may affect generalization.

[13] N. B. Emberi, A. Mohan, C. A. Naphade, and R. Ransing, "Harnessing Deep Neural Networks for Accurate Offline Signature Forgery Detection" (ICICCS, 2023) focuses on offline handwritten signature forgery detection. Deep neural network models are employed to extract discriminative features and classify signatures as genuine or forged. Experimental results show high accuracy is 92.7%, precision, and recall, outperforming traditional machine learning methods. Limitations include limited dataset size, lack of cross-dataset validation, and absence of real-world deployment analysis affecting generalization.

[14] G. P., S. G., K. R. K., K. N. K. J., and K. N., "Real Time Signature Forgery Detection Using Machine Learning" (ICAECT, 2022) focuses on real-time offline handwritten signature forgery detection. The study uses scanned signature images with preprocessing steps such as noise removal and normalization. Experimental results show good accuracy is 95.8%, precision, and recall compared to traditional approaches. Limitations include small dataset size, lack of cross-dataset validation, and no real-world deployment analysis affecting generalization.

[15] S. Lodha and H. Malani, "A Unique Approach to Efficient Fraudulent Signature Detection Using Deep Convolutional Neural Network, Xception, and EfficientNet" (AIVR, 2022) focuses on offline handwritten signature forgery detection.

Deep learning models including CNN, Xception, and EfficientNet are employed to extract features and classify signatures as genuine or forged.

Experimental results demonstrate high accuracy is 98.3%, precision, and recall compared to traditional machine learning methods.

Limitations include limited dataset size, affecting generalization.

III. PROPOSED METHODOLOGY

The system is to detect signature fraud by comparing a test signature with a genuine signature using deep learning techniques. It is based on a Siamese Neural Network architecture combined with Convolutional Neural Networks (CNN's) to effectively learn and compare signature patterns.

First, a signature dataset containing both genuine and forged signatures is collected from kaggle. The dataset may include offline (scanned) handwritten signatures. All signature images are preprocessed to improve quality. Preprocessing steps include image resizing, noise removal, normalization, and binarization to reduce variations caused by scanning conditions.

Next, pairs of signature images are created. Each pair consists of either two genuine signatures one genuine and one forged signature. These pairs are used as input to the Siamese Network, which is designed to learn similarity rather than classification.

Each branch of the Siamese Network uses a Convolutional Neural Network (CNN) with shared weights. The CNN automatically extracts meaningful features such as stroke shape, texture, curves, and writing style from the signature images. Because both branches share parameters, the network learns consistent feature representations.

The extracted feature vectors from both branches are then compared using a distance metric. An Euclidean distance is used to minimize the distance between genuine signature pairs and maximize the distance between genuine–forged pairs.

During training, the model learns to differences between genuine and forged signatures. Once trained, the system can evaluate a new signature by comparing it with a stored genuine signature and producing a similarity score.

Finally, a decision threshold is applied to classify the signature as genuine or forged. This deep learning–based approach provides a reliable solution for signature fraud detection.

6.1 Deep Learning:

Signature fraud detection is used to identify fake or forged signatures. It helps in verifying whether a signature is genuine or not. Deep learning models automatically learn important features from signature images. The system compares a new signature with stored genuine signatures. If the signature pattern does not match, it is marked as fraudulent. This method reduces human errors in signature verification. It improves accuracy compared to traditional verification methods.

6.2 Siamese Neural Network:

Siamese Neural Network compares two signatures instead of classifying just one. It learns the similarity between an original signatures and a test signature. Both signatures are passed through identical neural networks with shared weights. The model measures how closely the two signatures match. If the similarity score is high, the signatures is considered genuine. If the similarity score is low, the signature is marked as forged.

6.3 Biometric Authentication:-

Signature fraud detection using biometric authentication is a security technique used to verify a persons identity based on their handwritten signature. Since every individuals signature has a unique patterns, it can be treated as a behavioral biometric.

6.4 Image Verification

It works by comparing a scanned signature image with an original stored signature image preprocessing techniques are used to extract important features from the signature. Machine learning models analyze shape, strokes and patterns of the signatures. The system checks whether the new signature matches the genuine one.

IV. SYSTEM ARCHITECTURE DIAGRAM

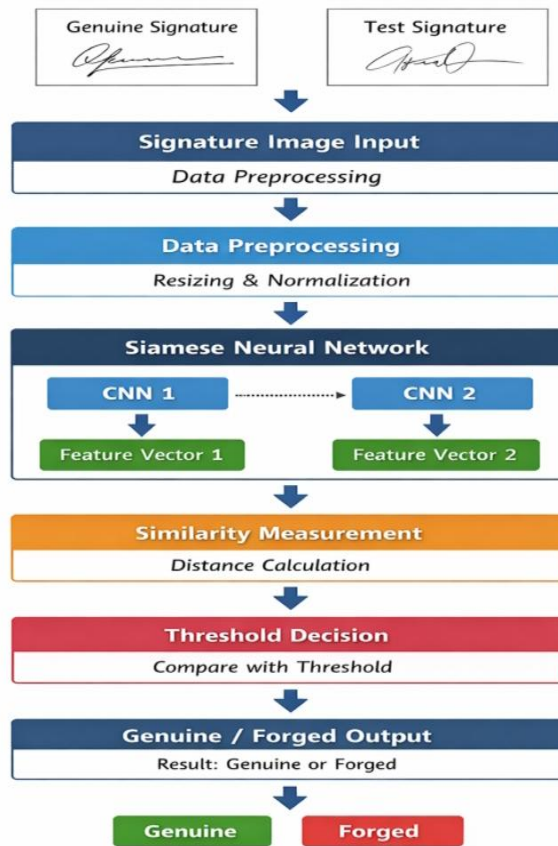


Fig:1: SIGNATURE FRAUD DETECTION USING DEEP LEARNING

The system takes a genuine signature and a test signature as image inputs. Both images are preprocessed by re sizing and normalizing them for consistency. The processed images are fed into a Siamese Neural Network. Each side of the network (CNN 1 & CNN 2) extracts important signature features. Two feature vectors are compared using a distance or similarity measure. This distance is checked against a predefined threshold. If the distance is small the signature is Genuine, otherwise the signature is Forged.

V. RESULTS & DISCUSSION

The system was tested using genuine and forged signature images. The dataset was divided into training and testing sets. CNN was used to extract important signature features. It identified stroke patterns and signature shapes effectively. CNN achieved good accuracy in classification. Siamese Neural Network compared pairs of signatures. It measured similarity between reference and test signatures. SNN correctly identified forged signatures. The combined approach reduced verification errors. The system proved reliable for signature authentication.

GRAPH

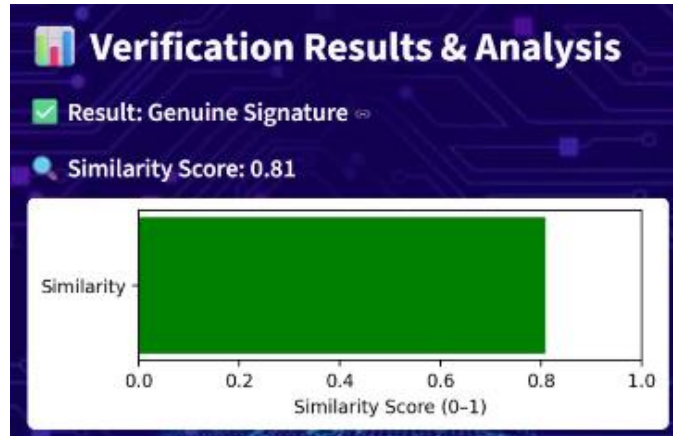


FIG 2. GRAPH

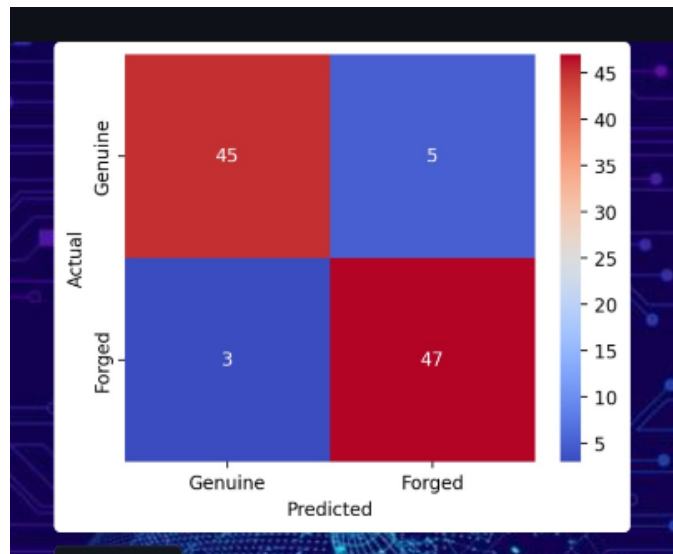


FIG 3. CONFUSION MATRIX

SCREENSHOTS



FIG 4. INEDX PAGE

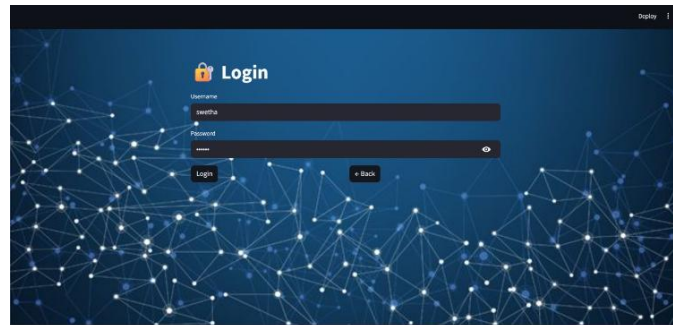


FIG 5. LOGIN PAGE

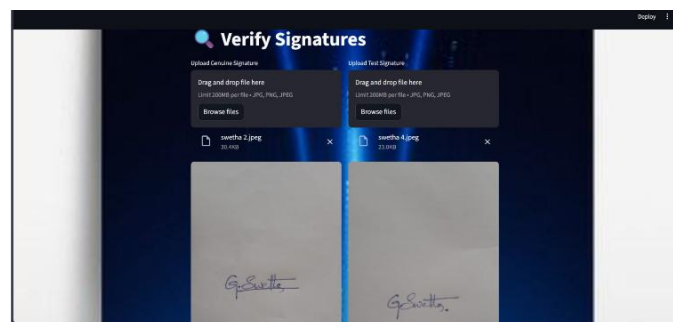


FIG 6. VERIFY PAGE

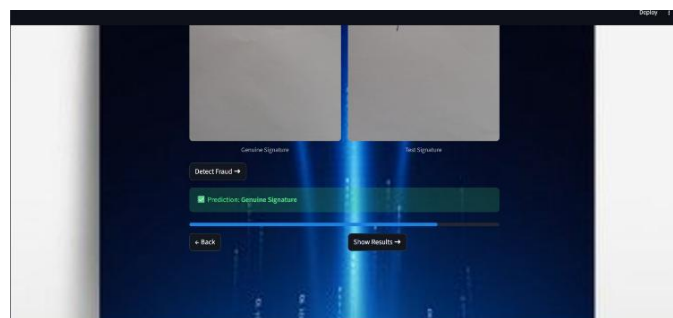


FIG 7. PREDICTION PAGE

VI. CONCLUSION & FUTURE SCOPE

This project presented a signature fraud detection system using deep learning methods. CNN was used to extract important features from signature images. It effectively captured shape and stroke patterns of signatures. Siamese Neural Network was used to compare genuine and test signatures. The system successfully identified forged signatures. It reduced errors compared to manual verification. The results showed reliable and consistent performance. This method can be used in banking and document verification systems. In the future, the system can be trained using larger datasets. More variations of signatures can be included. Real-time signature verification can be implemented. Performance can be improved for complex forgery cases. The system can be integrated with online authentication platforms

REFERENCES:

1. P. P. K, A. J. S P and B. B, "Advanced Deep Learning Algorithm for Offline Signature Fraud Detection," 2024 9th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2024, pp. 2110-2115,doi:10.1109/ICCES63552.2024.10860056.
2. N. Shetty, S. Shetty and N. Shetty, "Deep Learning-Powered Signature Authentication: The Signature Verify CNN Model," 2025 Third International Conference on Augmented Intelligence and Sustainable Systems (ICAISS),Trichy ,India, 2025, pp. 1405-1410,doi : 10.1109/ICAISS61471.2025.11042173.
3. E. F. Rudico, J. M. Y. Armocilla and M. V. C. Caya, "Detection of Offline Handwritten Signature Forgery Using InceptionV4 with Sobel Edge Detection," 2025 27th International Conference on Digital Signal Processing and its Applications (DSPA), Moscow, Russian Federation,2025,pp.15,doi:10.1109/DSPA64310.2025.10977897.
4. A. S. M, S. Suvarna and R. K T, "Online Digital Cheque Signature Verification using Deep Learning Approach," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp.866871,doi:w10.1109/ICECAA58104.2023.10212410.
5. O. Tarek and A. Atia, "Forensic Handwritten Signature Identification Using Deep Learning," 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Hammamet, Tunisia, 2022, pp. 185-190, doi: 10.1109/SETIT54465.2022.9875697.
6. G. K. Pandey, V. Raj, A. Agarwal, M. Dixit, S. S. Chauhan and S. Srivastava, "Offline Signature Verification: An Extensive Survey of Deep Learning Methods," 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2025, pp.892898,doi:10.1109/ICSADL65848.2025.10933339.
7. N. Tiwari, J. Thakkar, O. Bansode and H. Magar, "Signature Forgery and Veracity Detection using Machine Learning,"2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETISIS), Manama, Bahrain, 2024, pp. 1756-1759,doi:10.1109/ICETISIS61505.2024.10459390.
8. C. A. Krishna and R. Bhuvanewari, "Offline Signature Forgery Detection using Multi-Layer Perceptron," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet IN,India,2023,pp.14,doi:10.1109/ASIANCON58793.2023.10269874.
9. S. Bhirud, S. Bijwe, T. Chavan, A. Bhonsle, S. Rukhande and D. G., "Deep Transfer Learning for Authenticating Handwritten Signatures," 2025 International Conference on Electronics, AI and Computing (EAIC), Jalandhar, India, 2025, pp.1-6,doi:10.1109/EAIC66483.2025.11101688.
10. R. N. Mistry, N. More, S. Patil and C. Desai, "Multilingual Signature Verification Using Deep Learning: A Three-Phase Modular Approach," 2025 9th International Conference on Computing, Communication, Control and Automation (ICCCBEA), Pune, India, 2025, pp. 17,doi:10.1109/ICCUBEA65967.2025.11283938.
11. A. A. Lakshmi, G. S. Reddy, M. S. Reddy and N. Kathirisetty, "Offline Signature Forgery Detection Based on Geometric Measures Using Tensorflow Model," 2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar,India,2024,pp.1-7,doi: 10.1109/ASSIC60049.2024.10507928.
12. S. C. Nossam, R. A. Katakam, G. Pulastya and S. Jayan, "Signature Forgery Detection and Verification using Deep Learning Techniques," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp.16,doi:10.1109/ICCCNT61001.2024.10726260.

13. N. B. Emberi, A. Mohan, C. A. Naphade and R. Ransing, "Harnessing Deep Neural Networks for Accurate Offline Signature Forgery Detection," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 619-626, doi: 10.1109/ICICCS56967.2023.10142593.
14. G. P, S. G, K. R. K, K. N K J and K. N, "Real Time Signature Forgery Detection Using Machine Learning," 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2022, pp. 1-5, doi: 10.1109/ICAECT54875.2022.9807905.
15. S. Lodha and H. Malani, "A Unique Approach to Efficient Fraudulent Signature Detection using Deep Convolutional Neural Network, Xception and EfficientNet," 2022 IEEE International Conference on Artificial Intelligence and Virtual Reality, CA, USA, 2022, pp. 4654, doi: 10.1109/AIVR56993.2022.0001.