A Writer Stability-Based Approach for Offline Signature Verification

Dr. Annapurna H
Associate Professor and HoD, Department of Computer Science, Yuvaraja's College, University of Mysore, Mysuru, Karnataka, 570005, India

Abstract—**Offline signature verification is a widely used biometric authentication technique; however, its performance is often affected by intra-writer variability and skilled forgeries. This paper proposes a Writer Stability-Based Approach for Offline Signature Verification, which exploits the consistency of writer-specific signature characteristics to improve verification reliability. Initially, signature images are preprocessed through grayscale conversion, median filtering, Otsu's thresholding, noise removal, cropping, and normalization. Deep feature vectors are then extracted using a pre-trained ResNet18 network. A Writer Stability Model (WSM) is constructed for each writer by estimating the median feature prototype and the corresponding feature stability using the median absolute deviation. Stability-based weights are assigned to emphasize consistent features during matching. The similarity between a questioned signature and the writer's stability model is computed using weighted cosine similarity, followed by threshold-based decision making. The proposed method is evaluated on the CEDAR offline signature dataset using four training-testing split ratios (40:60, 50:50, 60:40, and 70:30). Experimental results demonstrate that the proposed approach achieves the highest verification accuracy of 80.06% with the 40:60 split. The results indicate that incorporating writer-specific feature stability provides a simple, effective, and computationally efficient solution for offline signature verification.**

Index Terms—**Offline signature verification, writer stability model, ResNet18, deep feature extraction, weighted cosine similarity, biometric authentication.**

I. INTRODUCTION

Handwritten signatures remain one of the most widely accepted behavioral biometric traits for personal authentication due to their legal acceptance and extensive use in banking, financial transactions, commercial documents, and administrative applications. However, offline signature verification remains a challenging task because genuine signatures of the same individual often exhibit considerable intra-writer variations, while skilled forgeries closely resemble authentic signatures [1], [2]. These factors make accurate discrimination between genuine and forged signatures a significant research problem.

Offline signature verification determines the authenticity of a scanned signature image using only its static visual information, without access to dynamic characteristics such as pen pressure, writing speed, or stroke sequence. Consequently, the verification system relies entirely on image-based features extracted from the signature. Earlier studies primarily employed handcrafted geometric, statistical, and texture descriptors combined with conventional machine learning classifiers such as Support Vector Machines (SVM), Hidden Markov Models (HMM), and k-Nearest Neighbors (k-NN) [1],[3]. Although these methods achieved satisfactory performance, their effectiveness was highly dependent on manually designed features and their ability to capture complex signature variations.

Recent advances in deep learning have significantly improved offline signature verification by enabling automatic extraction of discriminative feature representations. Convolutional Neural Networks (CNNs), particularly Residual Networks (ResNet), have demonstrated superior capability in learning robust hierarchical features directly from signature images, thereby reducing the reliance on handcrafted feature engineering [4],[5]. Despite these improvements, most existing approaches treat all extracted feature dimensions equally during the verification process, without considering their consistency across multiple genuine signatures of the same writer.

In practice, certain signature characteristics remain relatively stable across genuine samples of an individual, whereas others exhibit greater variability due to natural writing fluctuations. Assigning equal importance to all feature dimensions may therefore reduce verification reliability. Exploiting writer-specific feature stability provides an opportunity to emphasize consistent characteristics while minimizing the influence of unstable features, leading to more robust signature matching.

Motivated by this observation, this paper proposes a Writer Stability-Based Approach for Offline Signature Verification. The proposed approach is evaluated on the CEDAR offline signature dataset.

The main contributions of this work are summarized as follows:

- A novel Writer Stability Model (WSM) is proposed to characterize stable writer-specific deep feature representations.
- A robust feature stability estimation method based on the Median Absolute Deviation (MAD) is introduced.
- Stability-guided weighted cosine similarity is employed to improve offline signature verification.
- The proposed framework is comprehensively evaluated on the CEDAR dataset using multiple training-testing split ratios.

The remainder of this paper is organized as follows. Section 2 reviews the related work on offline signature verification. Section 3 presents the proposed Writer Stability-Based Offline Signature Verification framework, including image preprocessing, deep feature extraction, writer stability estimation, stability-based feature weighting, signature verification, and decision making. Section 4 describes the experimental setup and discusses the obtained results. Finally, Section 5 concludes the paper and outlines directions for future research.

II. LITERATURE REVIEW

Offline signature verification has been extensively studied owing to its importance in biometric authentication and document security. Unlike online verification, offline methods rely solely on the static image of a signature, making them more susceptible to intra-writer variations and skilled forgeries [6], [10]. Consequently, robust feature extraction and reliable verification techniques remain essential for improving system performance.

Earlier studies mainly employed handcrafted geometric, structural, statistical, and texture features combined with conventional classifiers such as Support Vector Machines (SVM), Hidden Markov Models (HMM), and Artificial Neural Networks (ANN) for signature verification [6]. Although these approaches achieved reasonable performance, their dependence on manually designed features limited their ability to capture complex variations in handwriting.

Recent advances in deep learning have significantly improved offline signature verification by enabling automatic feature learning from signature images. Convolutional Neural Networks (CNNs), particularly ResNet, have demonstrated superior capability in extracting robust and discriminative feature representations while reducing the reliance on handcrafted descriptors [4], [5]. Consequently, CNN-based feature extraction has become the dominant approach in modern offline signature verification systems.

Several recent studies have further enhanced deep learning-based verification frameworks. Muhtar *et al.* [7] integrated an attention mechanism with ResNet to improve multilingual offline signature verification. Diaz *et al.* [8] proposed an explainable verification framework to enhance the interpretability of deep learning decisions in forensic document examination. Zois *et al.* [9] employed similarity distance learning for writer-independent verification, while Sharma and Singh [10] demonstrated the effectiveness of transfer learning for improving feature extraction from limited training samples.

Despite these advances, most existing approaches focus primarily on learning discriminative feature representations and optimizing classification performance, while assigning equal importance to all extracted features during verification. However, genuine signatures contain both stable and variable characteristics, and treating all feature dimensions equally may reduce verification reliability.

To address this limitation, the present work proposes a Writer Stability Model (WSM) that explicitly models the stability of deep features extracted from genuine signatures. The stability of each feature dimension is estimated using the Median Absolute Deviation (MAD), and the resulting stability weights are incorporated into a weighted cosine similarity measure. By emphasizing stable writer-specific characteristics while suppressing unstable features, the proposed framework aims to improve the robustness and reliability of offline signature verification.

III. PROPOSED FRAMEWORK

This section presents the proposed Writer Stability-Based Offline Signature Verification framework. The framework is designed to improve verification performance by emphasizing stable writer-specific characteristics extracted from genuine signatures. It consists of the following sequential stages. The overall workflow of the proposed framework is illustrated in Fig. 1.

A. Training–Testing Data Partition
B. Image Preprocessing
C. Deep Feature Extraction
D. Writer Stability Estimation
E. Writer Stability Model Construction
F. Stability-Based Feature Weighting
G. Signature Verification
H. Decision Making
I. Performance Evaluation

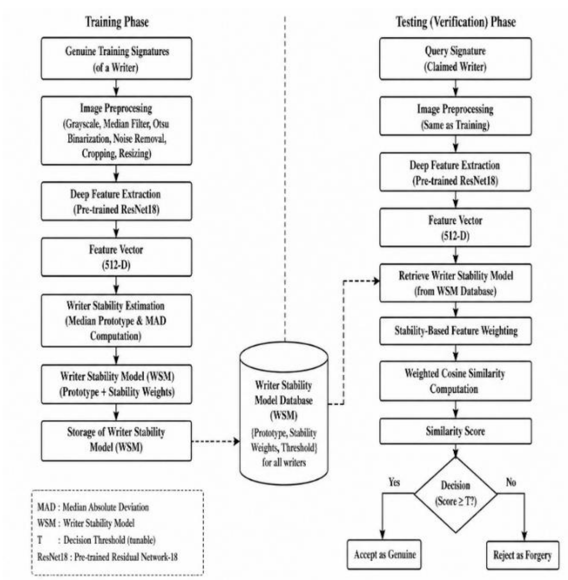

Fig.1. Proposed Writer Stability-Based Offline Signature Verification framework

A. Training–Testing Data Partition

The CEDAR offline signature dataset [11] is divided into training and testing sets using four predefined split ratios: 40:60, 50:50, 60:40, and 70:30. For each writer, only genuine signatures are used to construct the Writer Stability Model (WSM) during training, while the remaining genuine signatures and the corresponding skilled forgeries are used for testing. This evaluation protocol enables the performance of the proposed framework to be assessed under different enrollment conditions.

B. Image Preprocessing

Image preprocessing is performed to improve the quality and consistency of the signature images prior to feature extraction. Initially, each signature image is converted to grayscale to eliminate redundant color information. A 3×3median filter is then applied to suppress impulsive noise while preserving the structural characteristics of the handwritten strokes [12].

The filtered image is binarized using Otsu's thresholding algorithm, which automatically determines an optimal threshold to separate the signature from the background [13]. Small isolated foreground components introduced during scanning or thresholding are subsequently removed using connected component analysis. The signature region is then localized by computing its bounding rectangle, and a small margin is retained to avoid clipping the boundary strokes.

The cropped signature is resized while preserving its original aspect ratio and centered on a 224×224white canvas to obtain a standardized input representation. Finally, the pixel intensities are normalized to the range $[0, 1]$, producing consistent signature images suitable for deep feature extraction. This preprocessing stage reduces background interference, preserves the structural characteristics of the handwritten signature, and provides reliable input for the subsequent writer stability-based verification process.

C. Deep Feature Extraction

Following preprocessing, deep feature extraction is performed to obtain a compact and discriminative representation of each signature. In this work, a pretrained ResNet18 model is employed as the feature extraction backbone due to its lightweight architecture, residual learning capability, and proven effectiveness in various image recognition tasks [14]. The use of transfer learning enables the model to extract meaningful visual features without requiring extensive training on large-scale signature datasets.

The preprocessed signature images of size 224×224pixels are provided as inputs to the network. Since ResNet18 expects three-channel images, each grayscale signature image is replicated across the three input channels before being forwarded through the network. The pretrained weights obtained from the ImageNet dataset are retained, while the final fully connected classification layer is removed. Consequently, the output of the global average pooling layer is used as the feature representation of the input signature.

For each signature image, ResNet18 produces a 512-dimensional deep feature vector, which captures both low-level and high-level visual characteristics, including stroke patterns, local textures, and structural information. To improve numerical stability and reduce variations in feature magnitude, each feature vector is normalized using L2 normalization, as expressed in Eq. (1):

$$\hat{\mathrm{f}} = \frac{\mathrm{f}}{\|\mathrm{f}\|_2} \qquad (1)$$

where f denotes the extracted feature vector and $\hat{\mathbf{f}}$ represents the normalized feature vector.

The normalized deep feature vectors are subsequently used as inputs to the proposed writer stability estimation stage, where the consistency of each writer's genuine signatures is analyzed to identify stable and discriminative writing characteristics.

D. Writer Stability Estimation

The proposed Writer Stability Estimation (WSE) stage identifies the deep feature dimensions that remain consistent across multiple genuine signatures of a writer. Although genuine signatures naturally exhibit intra-writer variations, several discriminative features remain relatively stable and can provide reliable information for signature verification. These stable features are identified by analyzing the deep feature vectors extracted from the genuine training signatures. Let

$$F = \{\mathrm{f}_1, \mathrm{f}_2, \ldots, \mathrm{f}_N\}$$

represent the set of Nnormalized deep feature vectors extracted from the genuine signatures of a writer, where each feature vector

$$\mathrm{f}_i \in \mathbb{R}^{512}$$

is obtained from the pre-trained ResNet18 network.

A representative feature prototype is first computed by taking the component-wise median of all genuine feature vectors:

$$\mathrm{p} = \mathrm{median}(\mathrm{f}_1, \mathrm{f}_2, \ldots, \mathrm{f}_N) \qquad (2)$$

where pdenotes the representative feature prototype. The median is adopted because it is less sensitive to outliers and natural variations than the mean.

The consistency of each feature dimension is then estimated using the Median Absolute Deviation (MAD):

$$\mathrm{MAD}_j = \mathrm{median}_{i=1}^{N}(\mid f_{ij} - p_j \mid), j = 1,2, \ldots, 512 \qquad (3)$$

where f_{ij}represents the j^{th}feature of the i^{th}genuine signature and $p_j$is the corresponding component of the representative prototype. Lower MAD values indicate greater consistency of the corresponding feature dimension across genuine signatures.

The stability score of each feature dimension is subsequently computed as

$$s_j = \frac{1}{\mathrm{MAD}_j + \varepsilon} \qquad (4)$$

where $\varepsilon$is a small positive constant introduced to avoid division by zero. Higher stability scores correspond to more reliable feature dimensions.

Finally, the stability scores are normalized to obtain the writer-specific feature weights:

$$w_j = \frac{s_j}{\sum_{k=1}^{512} s_k}, \sum_{j=1}^{512} w_j = 1 \qquad (5)$$

where $w_j$denotes the normalized weight assigned to the j^{th}feature dimension. These normalized stability weights quantify the relative importance of the extracted deep features and are subsequently utilized for constructing the Writer Stability Model in the next stage.

E. Writer Stability Model Construction

The Writer Stability Model (WSM) is constructed using the representative feature prototype and the corresponding normalized stability weights obtained from the Writer Stability Estimation stage. The model provides a compact writer-specific representation by capturing both the characteristic deep features and their relative stability across multiple genuine signatures.

The Writer Stability Model for each enrolled writer is defined as

$$\mathrm{WSM} = \{\mathrm{p}, \mathrm{w}\} \qquad (6)$$

where **p** denotes the representative feature prototype computed from the genuine signatures, and **w** represents the corresponding normalized stability weight vector. The prototype characterizes the writer's typical signature pattern, while the stability weights quantify the relative importance of individual feature dimensions.

The constructed WSM is stored as the reference model for the corresponding writer and is subsequently used during the signature verification stage. By jointly representing the writer's characteristic deep features and their stability, the WSM provides a robust and compact template for reliable signature matching.

F. Stability-Based Feature Weighting

The stability-based feature weighting stage assigns greater importance to feature dimensions that remain consistent across the genuine signatures of a writer. The normalized stability weights obtained from the Writer Stability Estimation stage are incorporated during signature comparison to emphasize reliable features while reducing the influence of highly variable ones. Consequently, feature dimensions exhibiting greater stability contribute more significantly to the final similarity score.

Let $\mathrm{q} \in \mathbb{R}^{512}$ denote the normalized feature vector of the questioned signature and **p**represent the prototype stored in the corresponding Writer Stability Model. The similarity between the two feature vectors is computed using the normalized stability weights, where each feature dimension is weighted according to its estimated stability. This weighting strategy improves the robustness of the verification process by focusing on the most representative writer-specific characteristics and minimizing the effect of natural signature variations.

The weighted feature vectors are subsequently used in the signature verification stage to compute the similarity score between the questioned signature and the enrolled writer's reference model.

G. Signature Verification

During the verification stage, the questioned signature undergoes the same preprocessing and deep feature extraction procedures as those applied during training. The extracted feature vector is then compared with the corresponding Writer Stability Model (WSM) of the claimed writer. To improve matching reliability, the comparison is performed using weighted cosine similarity, where the normalized stability weights assign greater importance to consistent feature dimensions.

The weighted cosine similarity between the questioned signature feature vector q and the writer prototype p is computed as

$$S(\mathrm{q}, \mathrm{p}) = \frac{\sum_{j=1}^{512} w_j\, q_j p_j}{\sqrt{\sum_{j=1}^{512} w_j\, q_j^2}\sqrt{\sum_{j=1}^{512} w_j\, p_j^2}} \qquad (7)$$

where q_j and p_j denote the j^{th} components of the questioned signature and the writer prototype, respectively, and $w_j$represents the corresponding normalized stability weight. The resulting similarity score reflects the degree of correspondence between the questioned signature and the enrolled writer while emphasizing stable writer-specific characteristics. Higher similarity scores indicate a greater likelihood that the questioned signature is genuine.

H. Decision Making

The final verification decision is made by comparing the weighted cosine similarity score with a predefined decision threshold. Let $S(\mathrm{q}, \mathrm{p})$denote the similarity score obtained from the signature verification stage and Trepresent the decision threshold. A questioned signature is classified as genuine if its similarity score is greater than or equal to the threshold; otherwise, it is classified as forged. This decision rule is expressed as

$$D = \begin{cases} \text{Genuine}, & \text{if } S(\mathbf{q}, \mathbf{p}) \geq T, \\ \text{Forged}, & \text{if } S(\mathbf{q}, \mathbf{p}) < T. \end{cases} \qquad (8)$$

where Ddenotes the verification decision and $T$is the predefined similarity threshold determined during the training phase. This threshold-based decision mechanism enables the proposed framework to effectively distinguish genuine signatures from skilled forgeries by utilizing the writer-specific stability information incorporated into the similarity computation.

I. Performance Evaluation

The performance of the proposed Writer Stability-Based Offline Signature Verification framework is evaluated on the CEDAR offline signature dataset [11] using four training–testing split ratios: 40:60, 50:50, 60:40, and 70:30. The verification performance is assessed using standard evaluation metrics, including Accuracy (ACC), False Acceptance Rate (FAR), False Rejection Rate (FRR), Precision, Recall, and F1-score. These metrics provide a comprehensive assessment of the framework's ability to correctly identify genuine signatures while rejecting skilled forgeries under different enrollment conditions. The experimental results obtained for each split ratio are presented and discussed in the subsequent section.

IV. EXPERIMENTATION AND RESULTS

A. Experimental Setup

The proposed Writer Stability-Based Offline Signature Verification framework was evaluated using the CEDAR offline signature dataset [11], which contains genuine and skilled forged signatures from 55 writers. Signature images were preprocessed through grayscale conversion, median filtering, Otsu's thresholding, noise removal, cropping, and normalization before feature extraction. Deep feature vectors were extracted using a pre-trained ResNet18 network, resulting in 512-dimensional feature representations.

To evaluate the robustness of the proposed method, four training–testing split ratios (40:60, 50:50, 60:40, and 70:30) were considered. For each writer, only genuine signatures were used during the training phase to construct the Writer Stability Model (WSM), while the remaining genuine signatures and the corresponding skilled forgeries were used for testing. The verification performance was assessed using Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Precision, Recall, and F1-score.

B. Performance Evaluation Metrics

The performance of the proposed framework is evaluated using standard verification metrics, namely Accuracy (ACC), False Acceptance Rate (FAR), False Rejection Rate (FRR), Precision (P), Recall (R), and F1-score. These metrics collectively assess the capability of the proposed method to correctly classify genuine signatures while rejecting skilled forgeries.

The Accuracy (ACC) is defined as

$$\mathrm{ACC} = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \qquad (9)$$

where TP, TN, FP, and FNdenote the number of true positives, true negatives, false positives, and false negatives, respectively.

The False Acceptance Rate (FAR), which measures the percentage of forged signatures incorrectly accepted as genuine, is computed as

$$\mathrm{FAR} = \frac{FP}{FP + TN} \times 100 \qquad (10)$$

The False Rejection Rate (FRR), representing the percentage of genuine signatures incorrectly rejected, is given by

$$\mathrm{FRR} = \frac{FN}{TP + FN} \times 100 \qquad (11)$$

The Precision (P) is calculated as

$$\mathrm{Precision} = \frac{TP}{TP + FP} \times 100 \qquad (12)$$

The Recall (R) is defined as

$$\mathrm{Recall} = \frac{TP}{TP + FN} \times 100 \qquad (13)$$

Finally, the F1-score, which represents the harmonic mean of Precision and Recall, is computed as

$$\text{F1-score} = 2 \times \frac{\mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}} \qquad (14)$$

These evaluation metrics provide a comprehensive assessment of the effectiveness and robustness of the proposed Writer Stability-Based Offline Signature Verification framework under different training–testing split ratios.

C. Experimental Results

The proposed Writer Stability-Based Offline Signature Verification framework was evaluated on the CEDAR offline signature dataset using four training–testing split ratios (40:60, 50:50, 60:40, and 70:30). The quantitative results are presented in Table I, while the corresponding accuracy comparison is shown in Fig. 2.

The proposed method achieved its highest verification accuracy of 80.06% with the 40:60 split, followed by 79.56% for the 60:40 split. The 50:50 and 70:30 configurations yielded accuracies of 77.73% and

77.48%, respectively. These results demonstrate that the proposed Writer Stability Model (WSM) effectively captures stable writer-specific characteristics, resulting in reliable verification performance across different training–testing configurations.

Table I: Verification results of the proposed method for different training–testing split ratios.

Testing Set (%)	Testing Set (%)	FAR (%)	FRR (%)	Precision (%)	Accuracy (%)
40	60	21.59	17.12	69.16	80.06
50	50	24.39	18.03	62.69	77.73
60	40	22.27	16.03	61.06	79.56
70	30	23.79	18.18	50.08	77.48

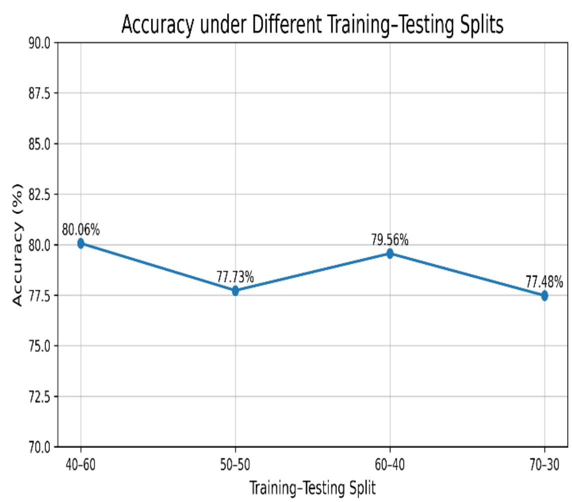

Fig. 2 Verification accuracy of the proposed Writer Stability-Based Offline Signature Verification method under different training–testing split ratios.

D. Discussion

The experimental results demonstrate the effectiveness of the proposed Writer Stability-Based Offline Signature Verification framework across different training–testing split ratios. The highest verification accuracy of 80.06% was achieved with the 40:60 split, indicating that the proposed Writer Stability Model (WSM) effectively captures stable writer-specific characteristics using a moderate number of genuine signatures. The consistent performance across all split ratios confirms that incorporating feature stability into the verification process improves the robustness and reliability of offline signature verification against skilled forgeries.

V. CONCLUSION

This paper presented a Writer Stability-Based Approach for Offline Signature Verification, which utilizes writer-specific feature stability to improve verification performance. The proposed framework combines image preprocessing, ResNet18-based deep feature extraction, writer stability estimation using the Median Absolute Deviation (MAD), and weighted cosine similarity for signature verification. Experimental results on the CEDAR offline signature dataset demonstrated a maximum verification accuracy of 80.06% using the 40:60 training–testing split. The results confirm that incorporating feature stability enhances the robustness and reliability of offline signature verification. Future work will focus on validating the proposed framework on larger benchmark datasets and exploring advanced deep learning models for further performance improvement.

REFERENCES

[1] D. Impedovo and G. Pirlo, "Automatic Signature Verification: The State of the Art," *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 38, no. 5, pp. 609–635, 2008.

[2] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline Handwritten Signature Verification—Literature Review," *Pattern Recognition*, vol. 74, pp. 278–292, 2018.

[3] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. Wiley, 2001.

[4] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.

[5] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning Features for Offline Handwritten Signature Verification Using Deep Convolutional Neural Networks," *Pattern Recognition*, vol. 70, pp. 163–176, 2017.

[6] M. A. Muhtar, M. A. Ismail, M. F. Nasrudin, and N. M. Tahir, "FC-ResNet: An Improved Residual Network with Attention Mechanism for Multilingual Offline Signature Verification,"

Applied Sciences, vol. 13, no. 14, Art. no. 8022, 2023.

[7] M. Diaz, M. A. Ferrer, A. Morales, and J. Fierrez, "Explainable Offline Signature Verification for Forensic Document Examination," *Neural Computing and Applications*, vol. 36, pp. 1605–1621, 2024.

[8] E. N. Zois, A. Alewijnse, and G. Economou, "Similarity Distance Learning on Symmetric Positive Definite Manifolds for Writer-Independent Offline Signature Verification," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1547–1561, 2024.

[9] A. Sharma and R. K. Singh, "Transfer Learning-Based Offline Signature Verification Using Deep Convolutional Neural Networks," *Expert Systems with Applications*, vol. 237, Art. no. 121512, 2024.

[10] S. N. Srihari, S.-H. Cha, H. Arora, and S. Lee, "Individuality of Handwriting: A Validation Study," *Pattern Recognition*, vol. 35, no. 11, pp. 2519–2527, 2002.

[11] S. N. Srihari, S.-H. Cha, H. Arora, and S. Lee, "Individuality of Handwriting," *Journal of Forensic Sciences*, vol. 47, no. 4, pp. 856–872, 2002.

[12] T. S. Huang, G. J. Yang, and G. Y. Tang, "A Fast Two-Dimensional Median Filtering Algorithm," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 27, no. 1, pp. 13–18, 1979.

[13] N. Otsu, "A Threshold Selection Method from Gray-Level Histograms," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 9, no. 1, pp. 62–66, 1979.

[14] K. He, X. Zhang, S. Ren, and J. Sun, *Deep Residual Learning for Image Recognition*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778, 2016.