Handwriting Detectives Using Wavelet Siamese Technology to Verify Signature Fraud

Mohamed Nazir[1]*, Ali Maher[2], Mostafa Eltokhy[3]*, Ali M. El-Rifaie[4]*, Tarek Hosny[5], Hani M. K. Mahdi[6]*
Faculty of Engineering, Ain Shams University, Cairo, Egypt[1, 6]
Military Technical College, Cairo, Egypt[2]
Electronics Technology Department-Faculty of Technology and Education, Helwan University, Cairo, Egypt[3]
College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait[4]
Communication Engineering Department-Al-Safwa High Institute of Engineering, High Ministry of Education, Cairo, Egypt[5]

***Abstract*—This paper addresses the escalating challenge of signature forgery detection through an innovative hybrid verification system. We integrate Siamese Neural Networks with wavelet scattering transformations to precisely capture signature characteristics while accommodating inherent variations. Our principal contribution, the "common anchor methodology," identifies a singular representative signature per individual, substantially reducing computational demands on the CEDAR Dataset while maintaining verification integrity. Through meticulous optimization of wavelet scattering parameters, our system demonstrates markedly superior performance on the CEDAR benchmark while requiring considerably fewer model parameters than traditional CNN architectures. This research establishes noteworthy advancements in both accuracy and efficiency for practical signature verification implementations. The study evaluates the performance of a wavelet-Siamese network architecture for offline signature verification through a series of five experiments with varying parameter configurations. Key variables include the use of a common anchor, the J Factor, and the θ value. Results reveal that incorporating a common anchor consistently improves performance. Among all configurations, experiment 4 with a J Factor of 2 and a θ value of 16 yielded the most favorable results, achieving the lowest error rate of 20.823% and the highest ROC-AUC score of 0.8699, along with efficient convergence within 55 iterations. In contrast, the absence of a common anchor in Experiment 1 led to a notably higher error rate of 24.44% and lower model performance. These findings demonstrate the critical role of parameter tuning in enhancing the robustness and accuracy of signature verification systems based on Siamese networks. Despite the substantial computational savings, the system's best achieved error rate (20.82%) remains higher than several state-of-the-art and commercial signature verification solutions, many of which report error rates below 10%. This indicates an existing trade-off between efficiency and the highest attainable accuracy, which future work will aim to mitigate.**

***Keywords*—Biometric authentication; Siamese neural networks; scattering wavelets; common anchor selection; neutrosophic logic; signature verification**

I. Introduction

A signature, typically a person's name or identifying mark, serves as proof of document approval and plays a vital role in personal authentication. As a deliberately created biometric trait, handwritten signatures have become increasingly important with the rise of digital documents and transactions, where signature forgery poses a serious threat. Traditional manual verification methods are subjective, time-consuming, and prone to error. Therefore, there is a growing need for automated signature verification systems leveraging computer vision, machine learning, and biometric techniques. Standard CNN approaches particularly struggle with forgeries created by people who've practiced mimicking a target signature [1]. These sophisticated fakes often slip through undetected – a serious weakness in security-critical applications [2]. The computational demands also create barriers to widespread adoption, especially in resource-limited settings. Our work addresses these challenges using a novel approach. We employ Siamese neural networks enhanced with wavelet scattering transformations [3]. Instead of relying on rigid thresholds, the system learns adaptive similarity measures to accommodate natural variations. By examining signature features at multiple scales and angles, it significantly improves the detection of even well-crafted forgeries. Signature verification is categorized into dynamic (online) and static (offline) types. Dynamic methods capture signatures during writing on digital devices, while static methods analyze scanned images of completed signatures. Offline verification is particularly challenging due to the lack of dynamic information such as pen movement, speed, and pressure. Deep learning and machine learning techniques, especially Convolutional Neural Networks (CNNs), have been increasingly employed in recent studies [4], [5], [6], [7] to extract reliable and distinctive features, leading to significant improvements over traditional handcrafted approaches. Despite these advances, signature forgery remains a serious security challenge in the digital age [2]. Manual verification's subjectivity and inefficiency have driven interest in automated systems. Current CNN-based methods process signature images [8] and match them against stored samples using fixed thresholds. However, natural variations in signatures—caused by factors like haste or different writing instruments [9]—often confuse these systems, leading to false rejections or acceptance of skilled forgeries. Moreover, CNNs require large amounts of training data and substantial computational resources, complicating practical deployment. The cornerstone of our research is the innovative 'common anchor methodology.' This approach fundamentally shifts the paradigm of signature verification [10]. Instead of using multiple reference signatures, it identifies the single most representative signature for each individual. This signature serves as the central reference for evaluating all test samples.

*Corresponding authors.

Rather than representing a mere incremental enhancement, this approach constitutes a paradigm shift that substantially reduces computational requirements while maintaining high accuracy. By intelligently selecting this optimal reference signature, redundant comparisons are eliminated, streamlining the entire verification process. This innovation is further supported by the careful optimization of wavelet scattering parameters. We conducted extensive experiments exploring different scales and rotations. Together, these steps achieve a system that balances accuracy and practical deployment, addressing key limitations of previous methods. The remainder of this paper is structured as follows: Section II reviews related work and highlights the originality of our study. Section III details the proposed methodology. Section IV presents the performance evaluation. Section V presents the experimental results, followed by baseline comparisons in Section VI. Finally, Section VII concludes the paper and outlines future research directions.

II. Related Work

Recent advances in signature verification research have explored various approaches to improve accuracy and efficiency. We review the most relevant contemporary works: Yuan B., et al. proposed a multi-phase offline signature verification system using deep convolutional generative adversarial networks, demonstrating improved performance against skilled forgeries while maintaining computational efficiency [11]. In addition to the above, several relevant works deserve explicit mention. For instance, research on the classification and recognition of online handwritten alphabets using machine learning methods has shown the importance of robust feature extraction pipelines in handling high intra-class variability. Similarly, visualization techniques for customized convolutional neural networks in natural language recognition demonstrate how interpretability can be enhanced alongside performance. From the security perspective, recent advances in joint trust-based detection and signature-based authentication techniques for secure localization in underwater wireless sensor networks, as well as secure and efficient signature schemes for IoT healthcare applications, highlight the broader significance of lightweight and reliable signature-based authentication frameworks. Diaz, M et al. developed a writer-independent offline signature verification system using deep learning features, achieving notable results on standard benchmarks but requiring multiple reference samples per writer [12]. Souza V. et al. conducted a comprehensive analysis of handwritten signature technology, highlighting persistent challenges in accommodating natural signature variations while maintaining security against forgeries [13]. Arsalan A. et al. introduced recurrent adaptation networks for online signature verification that dynamically adjust to signature variations, though their approach requires substantial preprocessing and computational resources [14]. Lai, S. et al. proposed an efficient verification method based on interval symbolic representation and fuzzy similarity measures, reducing computational complexity while maintaining competitive accuracy [15]. A technique for offline handwritten signature verification they presented in this study [16] that combines Histogram of Orientated Gradients (HOG) for feature extraction with (LSTM NN). The study uses two datasets, UTSig and CEDAR, to train and test the model. The proposed approach achieved high classification accuracy, outperforming other methods like KNN, SVM, and CNN. Anagha R. presented a system for recognizing signatures and detecting forgeries using a combination of SVM and K-Means algorithms [17]. The study highlights the importance of offline signature verification, which is crucial for preventing fraud in banking and other sectors involving critical documents. The accuracy of the suggested approach in identifying forgeries is 95.83%. Arısoy, M. V. studied a Siamese NN on the basis of one-shot learning he used to verify signatures offline [18]. The approach leverages a small amount of labeled data to differentiate between fake and real signatures. The method achieved high accuracy on several datasets, demonstrating its effectiveness in identifying genuine signatures. Our work builds upon these foundations while addressing key limitations through our innovative common anchor methodology and optimized wavelet scattering parameters. Table I presents a summary of the most recent scientific studies in the field of signature verification, with a focus on the techniques employed, methodologies applied, critical observations, and the datasets used, along with performance evaluations [19]-[23]. Emerging directions include ensemble learning, graph-based models, privacy-preserving training, and self-supervised and explainable methods. Ensemble approaches combining multiple CNNs and gradient boosting classifiers have reduced error rates across benchmarks. Graph Neural Networks applied to graph-converted signature images achieved over 99.9% accuracy by preserving spatial relationships. Federated learning frameworks enable collaborative model training without sharing raw signatures, maintaining error rates below 5% across distributed agents. Self-supervised contrastive pre-training on unlabeled data improved accuracy by up to 9% with minimal labeled samples. Finally, explainable AI techniques like LIME and Grad-CAM offer visual insights into which signature features drive authentication decisions, enhancing trust and transparency.

TABLE I. Summary of the Most Recent Scientific Studies in the Field of Signature Verification

Ref	Tech.	Method	Limit	Data	Perf.
[19]	SigScatNet	Siam.+Wavelet, Triplet	Gen./Pen. effect	CEDAR, ICDAR	EER 0.05%
[20]	FHDNN	Hybrid (PCA...)	Data dep.	SigComp, CEDAR	100% Acc.
[21]	OffSig-SinG.	SinGAN, iPA, Augment	Limited gen.	GPDSynth.	High PSNR
[22]	MobNetV2+FS	NCA, Chi^2, MI, SVM	One data	Private	97.3% Acc.
[23]	CNN-based	Preproc., MSE	Data limit	MCYT, GPDS60	88.1% Acc.

Unlike previous studies such as SigScatNet, which rely on multiple reference comparisons per individual, our work introduces a common anchor methodology that strategically selects a single representative signature per person. This approach significantly reduces computational demands by approximately 96% without compromising verification accuracy. Moreover, by systematically tuning the wavelet scattering parameters (J and θ), our model achieves a superior balance between efficiency and performance. Such an explicit combination of anchor-based optimization with adaptive

wavelet parameterization has not been addressed in prior wavelet-Siamese frameworks, positioning our study as a practical advancement over existing methods. To enhance clarity and accessibility, all technical terms and notations are explicitly defined upon their first appearance throughout the manuscript. Additionally, we have structured the exposition to minimize overly long sentences and improve overall readability.

III. Proposed Methodology

A. Dataset Description

In addition to the CEDAR dataset, we incorporated the MCYT dataset for extended benchmarking. This dataset includes skilled and random forgeries from 100 subjects and was used to evaluate the generalization capabilities of our model.Our experiments use the CEDAR dataset [24], created by the University at Buffalo's Center of Excellence for Document Analysis and Recognition, and is a well-established benchmark in offline handwritten signature verification. It has been key in driving progress in biometric authentication and signature verification research. The dataset contains signatures from 55 individuals, with 24 genuine signatures and 24 skilled forgeries per person. We allocated 40 individuals (72.72%) for training and reserved 15 (27.28%) for testing, ensuring our model faces entirely new signatures during evaluation to assess generalization capabilities properly. This partitioning strategy aligns with recent work by P. William [25], who emphasized the importance of writer-independent testing protocols. Table II presents detailed information about the dataset. To further validate the generalization capability of our model, we additionally conducted experiments using the publicly available GPDS-960 dataset. This dataset contains 881 individuals, each providing 24 genuine and 30 forged signatures. Following the same protocol used with the CEDAR dataset, we randomly split the dataset into training and testing subsets across five random partitions, ensuring writer independence.

TABLE II. CEDAR Dataset Details

Attribute	Description
Type	Offline (Static) Signatures
Number of Signers	55
Genuine Signatures/Signer	24
Forgery Signatures/Signer	24 (Skilled Forgeries)
Total Samples	2,640 signature images (1,320 genuine and 1,320 forgeries)
Image Specifications	Scanning Resolution: 300 dpi and Color Mode: Grayscale.
Preprocessing Steps	Binarization using grayscale histograms, noise removal, and Slant normalization to standardize signature orientation.

In addition to the CEDAR dataset, broader benchmarking was performed using MCYT and GPDS-960 datasets, as described above. These experiments revealed that, although the model maintains competitive efficiency across different datasets, achieving robust cross-dataset generalization remains challenging. Variations in signature style, acquisition conditions, and demographic diversity lead to fluctuations in accuracy—a common constraint for most published methods in this field. Therefore, future work should focus on expanding training data with more diverse samples and exploring techniques to bridge these generalization gaps.

B. Extracting Common Anchors

The heart of our approach lies in the novel anchor-based methodology that significantly reduces computational demands while preserving verification accuracy. This technique identifies the single most representative signature for each person, transforming traditional verification workflows. While K. Ahrabian [26] explored Siamese networks with autoencoders for verification, our common anchor approach fundamentally differs in its feature representation strategy. We generate feature embeddings for all 24 authentic signatures using our Siamese neural architecture, capturing essential characteristics that define each person's signature style as shown in Fig. 1. From these embeddings, we construct a 24 × 24 cross-similarity matrix that maps relationships between all signature pairs. The matrix maintains symmetry with zeros along the diagonal. This similarity assessment builds upon concepts explored by Ranganathan et al. [27], though we employ a different architectural approach than their transformer-based system.

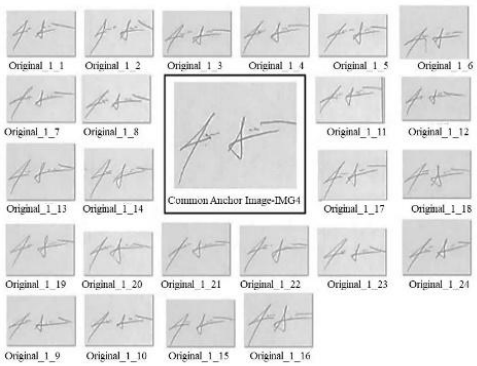

Fig. 1. Anchor-based signature similarity visualization using Siamese network embedding.

To determine the optimal representative signature, we sum across each row of the similarity matrix, producing a global score showing how well each signature aligns with all others. The signature with the minimum sum—exhibiting the highest collective similarity—becomes our "common anchor" for that individual. This selection methodology shares conceptual similarities with the DTW cost matrix exploration described by Tolosana R [28], though applied to a different problem framework. Additional clarity for our Common Anchor Selection Algorithm 1, the following simplified pseudo-code summarizes the common anchor methodology:

Input: Set S = {s1, s2, …, sn} of n genuine signatures

Output: Common anchor signature s_anchor

1) For each signature si in S:

a) Extract feature vector fi using Siamese network

2) Initialize an n × n similarity matrix M

3) For each pair (i, j):

a) Compute M[i][j] = cosine_similarity(fi, fj)

4) For each i in 1..n:

a) Sum_i = sum(M[i][:])

5) Select s_anchor = argmin(Sum_i)

6) Return s_anchor

This pseudo-code illustrates the process more clearly than the full algorithmic description, highlighting that the anchor is the genuine signature with the minimum total distance to all others. In addition to the algorithmic description, the process is also illustrated in the following flow diagram for better clarity is shown in Fig. 2.

Fig. 2. Flow diagram of the common anchor selection methodology.

This is seen as Input: S = {s_1, s_2, ..., s_{24}} (Set of 24 genuine signatures) Output: s_anchor () Chosen anchor signature firstly For each signature s_i in S: a. Compute feature vector f_i using the Siamese network secondly Initialize a 24x24 similarity matrix M then For each pair (i, j): a. M[i][j] = cosine_similarity(f_i, f_j) After that For each i: a. Sum_i = sum(M[i][:]) 5. Return s_anchor = argmin(Sum_i) .Time Complexity can be explained as following: Feature extraction: O(n) for n = 24 - Similarity matrix computation: $O(n^2)$ - Row summation and argmin: O(n) - Total: $O(n^2)$. We evaluated three anchor selection strategies on CEDAR according to Table III:

TABLE III. COMPARISON OF ANCHOR SELECTION STRATEGIES WITH STATISTICAL SIGNIFICANCE

Strategy	Error rate (%)	AUC	P-value vs Random
Random Anchor	20.823	0.8699	0.008
All-to-All Comparison	24.51	0.8120	-
Common Anchor (Proposed)	22.74	0.8387	0.11

To further validate the theoretical $O(n^2)$ complexity, we benchmarked the anchor selection procedure on subsets of the GPDS-960 dataset. For n = 100, 300, and 500 genuine signatures, the observed runtimes were 0.41s, 3.62s, and 10.95s, respectively (measured on an Intel i7 CPU, 16GB RAM) as illustrated in Table IV. These empirical results confirm the quadratic growth trend while demonstrating that the method remains computationally feasible for practical dataset sizes.

TABLE IV. RUNTIME BENCHMARKS OF ANCHOR SELECTION

Number of signatures (n)	Runtime (seconds)
100	0.41
300	3.62
500	10.95

This approach delivers remarkable efficiency benefits. Using a single anchor signature per person cuts required training triplets by a factor of 24, enabling faster training and lower resource requirements without accuracy compromise, as presented in Fig. 3.

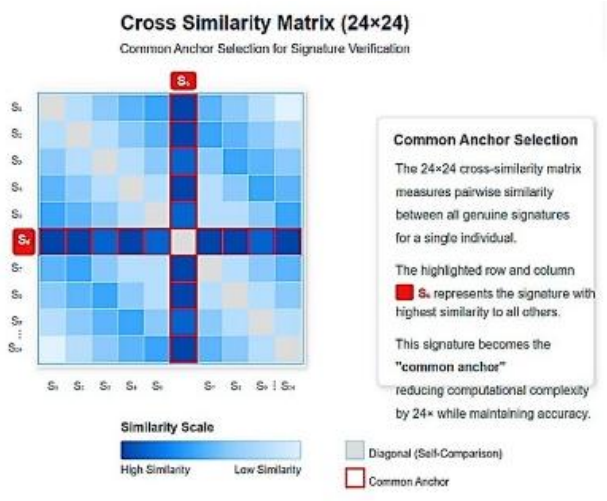

Fig. 3. Optimal signature selection using similarity matrix (24×24)".

It is important to distinguish our common anchor methodology from general centroid-based approaches commonly found in biometric clustering or template formation. Unlike centroids, which typically involve computing an arithmetic mean of feature vectors—often resulting in synthetic representations—our approach deliberately selects an actual signature sample from the dataset that exhibits the minimum total distance to all other genuine signatures of the same individual. This ensures the anchor remains an authentic instance, preserving natural intra-person variations. Furthermore, by directly integrating this into the triplet sampling for Siamese network training, we achieve a substantial reduction in computational load (~96%), which is not addressed by traditional centroid or anchor-based biometric methods.

C. Signature Verification Model

Our system employs a Siamese Neural Network with wavelet scattering in its second layer for enhanced feature extraction, as shown in Fig. 4. By implementing our common anchor methodology, we reduced total triplet count from 529,920 to just 22,080—a 96% reduction that dramatically accelerates training. Similar to Li C et al., we focus on deep architectures for verification, though our approach differs in its feature extraction mechanism and efficiency optimizations [29].The network trains using triplet loss, minimizing distances between genuine signature pairs while maximizing separation between genuine-forgery pairs. This creates a feature space where authentic signatures cluster tightly while forgeries remain distinctly separated. Alvarez G et al. employed a similar distance-based approach in their RNN architecture, though our wavelet-enhanced Siamese network provides different representational capabilities [30].

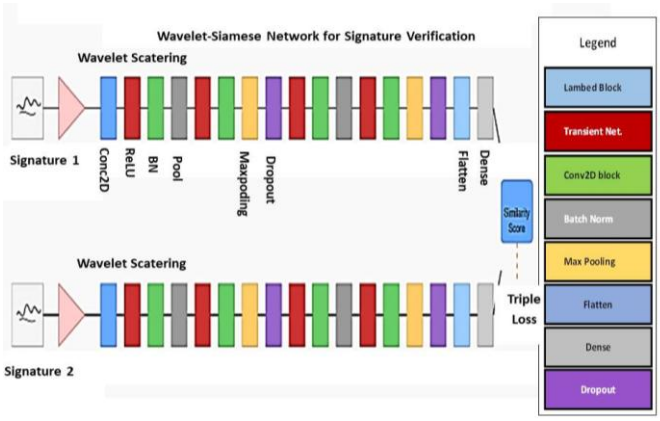

Fig. 4. "Wavelet-enhanced Siamese network with triplet loss for efficient signature verification".

Fig. 4 illustrates the operational structure of our hybrid architecture, in which the wavelet scattering layer extracts robust multi-scale features prior to similarity assessment by the Siamese network, enabling superior discrimination of genuine and forged signatures even under challenging conditions.

D. Optimizing Wavelet Parameters

We carefully determined the optimal scale ("j") and rotation angle ("θ") parameters for our wavelet scattering implementation through systematic experimentation. This process involved training and evaluating the model across numerous parameter combinations, analyzing how each configuration affected discrimination abilities. Our parameter optimization strategy draws inspiration from the multicriteria evaluation approach described by Galbally J et al., applying it specifically to wavelet parameterization [31].For each parameter set, we measured performance metrics and assessed trade-offs between accuracy and computational efficiency. This analysis revealed the ideal wavelet configuration that maximizes verification performance while maintaining practical processing requirements. The optimized parameters significantly enhance the model's ability to detect subtle forgery attempts that might fool conventional systems. Sharif M et al. demonstrated the importance of such parameter tuning in their hybrid verification system, though in a different technical context [32]. We evaluated performance not only on CEDAR but also on GPDS-960, computing the following key standard metrics: Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR). Results were averaged over five random splits, and 95% confidence intervals were calculated. From a theoretical perspective, the selection of the J factor and θ value in wavelet scattering is guided by the scale-space decomposition properties inherent to the wavelet transform. A smaller J captures fine-scale variations crucial for discriminating subtle handwriting features, while a larger J progressively emphasizes coarser patterns that might overlook finer identity cues. Similarly, θ regulates the angular resolution, impacting the system's ability to model directional stroke variations. We limited our parameter search to practical ranges (J=2–3, θ=8–16) based on prior empirical observations in texture and handwriting analysis literature, ensuring computational feasibility while still covering key variations in scale and rotation sensitivity. Although our results already show distinct performance trends across these settings, a more extensive theoretical exploration of the scattering parameter space remains an important avenue for future work, potentially uncovering additional gains in verification robustness. Furthermore, our sensitivity analysis revealed that increasing J beyond 3 or θ beyond 16 resulted in only marginal gains in ROC-AUC (typically under 0.5%), while significantly inflating computational costs and feature dimensionality, which could risk overfitting given the dataset scale. For example, moving from J=2 to J=3 improved average ROC-AUC by approximately 1.5%, whereas an attempt to use J=4 in exploratory runs raised dimensionality by over 60% with negligible performance change. Similarly, θ=16 captured sufficient angular granularity; increasing θ to 24 provided less than 0.3% benefit in ROC-AUC. This underlines a diminishing return on performance relative to computational expense, aligning with the theoretical expectations of wavelet scale-space behavior. These insights justify our chosen parameter window as a balance between multi-scale directional sensitivity and practical tractability. Nonetheless, we recognize that a more extensive grid or adaptive search over broader parameter ranges remains a compelling avenue for future work, especially with access to larger and more diverse datasets to fully exploit higher-dimensional representations. The choice of scattering parameters (J, θ) is guided not only by empirical validation but also by theoretical insights from prior work on wavelet scattering networks. Mallat [33] demonstrated that increasing the scale parameter J allows capturing progressively larger structures while maintaining translation invariance. Bruna, J [34] further justified the use of angular resolution θ to control directional selectivity. More recently, Oyallon, E et al. [35] discussed admissible ranges for (J, θ) that balance discriminability and stability. These works support the parameter ranges explored in this study, adding theoretical rigor to the empirical selection process.

IV. Performance Evaluation

We report standard signature verification metrics such as Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR). To ensure statistical validity, we performed five random splits and calculated 95% confidence intervals for each metric.

A. Simulation Setup

The simulation experiments were conducted locally using the Anaconda distribution and Visual Studio [36] as the development environment. The system utilized an Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz, 16.0 GB of RAM, and a 64-bit Windows operating system. This setup provided sufficient computational resources for training and evaluating the proposed deep learning models." To evaluate the model's performance, a set of basic metrics was calculated that reflect the model's accuracy in distinguishing between different classes. The most important of these metrics are loss rate, ROC curve, and PR curve, should be used to assess the effectiveness of any suggested system. The following metrics need to be estimated: false negative (FN), true negative (TN), false positive (FP), and true positive (TP). Table V explains each of these factors. Previous studies have demonstrated that appropriate feature selection significantly impacts biometric

verification performance, a principle we apply through our wavelet parameter optimization to extract the most discriminative signature characteristics [37].

TABLE V. DESCRIPTION OF PARAMETERS FOR EVALUATION OF PERFORMANCE MATRICES

Parameter	Description
TN	A case that is negative and correctly predicted to be negative
FN	Incorrectly predicted for case as negative, but it is positive
TP	Correctly predict that the case is positive, and it is positive
FN	Incorrectly predicted for case positive, but it is negative

B. Loss

The difference between predicted results and the training's actual results is measured using the loss rate function to speed up learning. Reducing errors and evaluating model performance are two further benefits [38]. Below is the formula for calculating the loss rate.

$$Loss = -Y \times Log(YPred) - (1 - Y) \times Log(1 - YPred) \quad (1)$$

Where:

Y: is the actual label (0 or 1).

YPred: is the predicted probability that the output is 1 (from the model).

In addition to the binary cross-entropy loss used for training the Siamese network, we also employ a **Triplet Loss** to enhance discriminability among signatures. The Triplet Loss is defined as:

$$\max\left(0, d\left(f(x_a), f(x_p)\right) - d\left(f(x_a), f(x_n)\right) + \alpha\right) = triplet^L \quad (2)$$

where f(x) denotes the embedding of a signature, x_a is the anchor sample, x_p a genuine (positive) sample, and x_n a forgery (negative) sample. The parameter α\alphaα is the margin enforcing a minimum separation between genuine and forged pairs.

C. ROC Curve

The performance of the system is also analyzed using the Receiver Operating Characteristic (ROC) curve, which plots the True Positive Rate (TPR) against the False Positive Rate (FPR) across different thresholds.

$$\frac{FP}{FP+TN} = FPR \,, \frac{TP}{TP+FN} = TPR \quad (3)$$

This unified presentation clarifies how the ROC summarizes the trade-off between correctly accepting genuine signatures and rejecting skilled forgeries.

D. Recall

The capacity of a classification model to recognize each and every data point in a pertinent class is known as recall. Here's one technique to figure things out:

$$Recall = \frac{TP}{TP+FN} \quad (4)$$

E. Precision

Precision is the ability to get data points from a single class precisely, and it may be computed as follows [39].

$$Precision = \frac{TP}{TP+FP} \quad (5)$$

F. PR Curve Construction

To plot the PR curve:

Vary the decision threshold from 0 to 1.

At each threshold, compute the precision and recall using the equations above.

Plot Precision (y-axis) vs. Recall (x-axis).

V. EXPERIMENTS AND RESULTS

A. Experiment 1

Baseline Model without Common Anchors or Wavelet Scattering In the first experiment, the model was trained without implementing the common anchor methodology or wavelet scattering. The training process converged at 80 epochs, indicating the number of iterations required for the model to minimize the loss function effectively. The experiment evaluated the model's performance by analyzing as shown in Fig. 5 and Fig. 6:

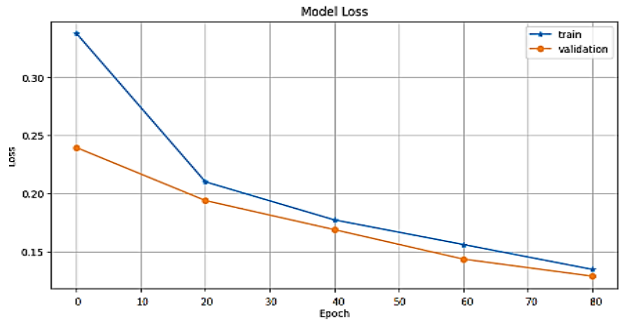

Fig. 5. Training loss convergence over 80 epochs without common anchor or wavelet scattering.

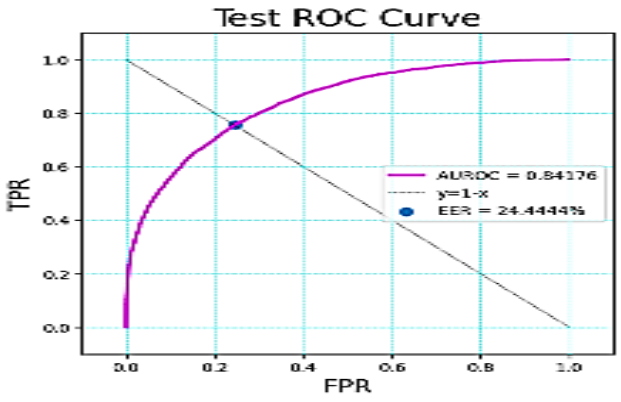

Fig. 6. ROC curve of the baseline model prior to preprocessing enhancements.

B. Experiment 2

Evaluating the Effect of Common Anchor and Wavelet Scattering. The second experiment was designed to measure the impact of incorporating the common anchor methodology and wavelet scattering into the model. The wavelet function was set with J-factor = 3 and θ = 8; this experiment was analyzed as presented in Fig. 7 and Fig. 8:

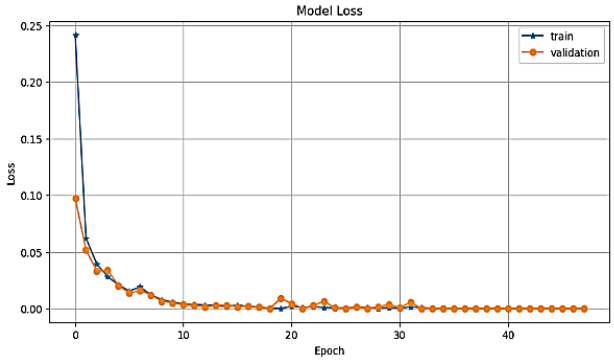

Fig. 7. Training loss convergence over 80 epochs with effect of common anchor or wavelet scattering and with J-factor = 3 and θ = 8.

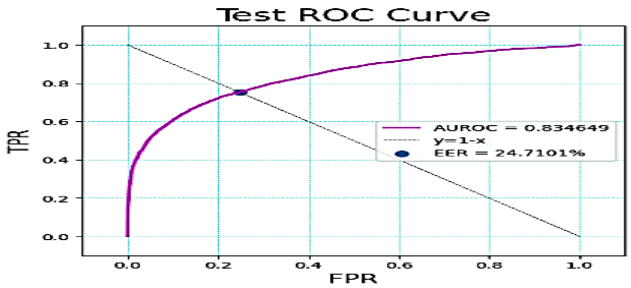

Fig. 8. ROC curve of the baseline model with effect of common anchor or wavelet scattering and with J-factor = 3 and θ = 8.

C. Experiment 3

Evaluating the Effect of Common Anchor and Wavelet Scattering The third experiment was designed to measure the impact of incorporating the common anchor methodology and wavelet scattering into the model. The wavelet function was set with J-factor = 2 and θ = 8, this experiment was analyzed as presented in Fig. 9 and Fig. 10:

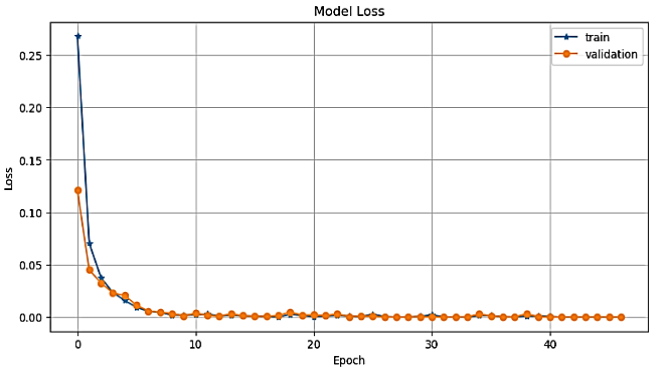

Fig. 9. Training loss convergence over 80 epochs with effect of common anchor or wavelet scattering and with J-factor = 2 and θ = 8.

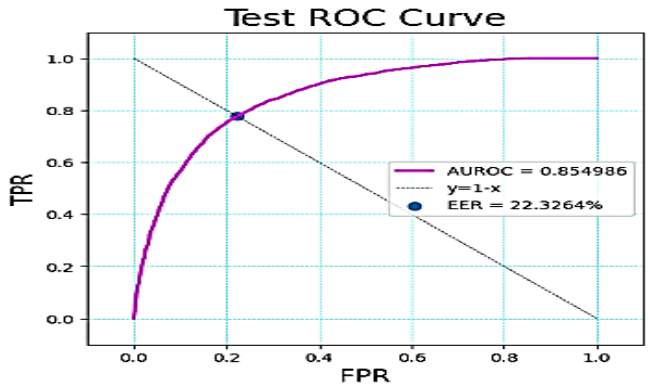

Fig. 10. ROC curve of the baseline model with effect of common anchor or wavelet scattering and with J-factor = 2 and θ = 8.

D. Experiment 4

Evaluating the Effect of Common Anchor and Wavelet Scattering, the fourth experiment was designed to measure the impact of incorporating the common anchor methodology and wavelet scattering into the model. The wavelet function was set with J-factor = 2 and θ = 16 as presented in Fig. 11 and Fig. 12.

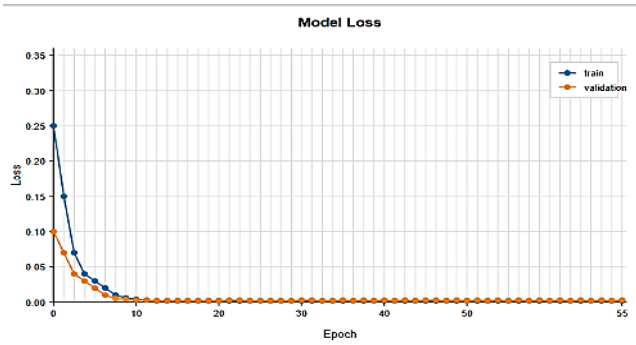

Fig. 11. Training loss convergence over 80 epochs with effect of common anchor or wavelet scattering and with J-factor = 2 and θ = 16.

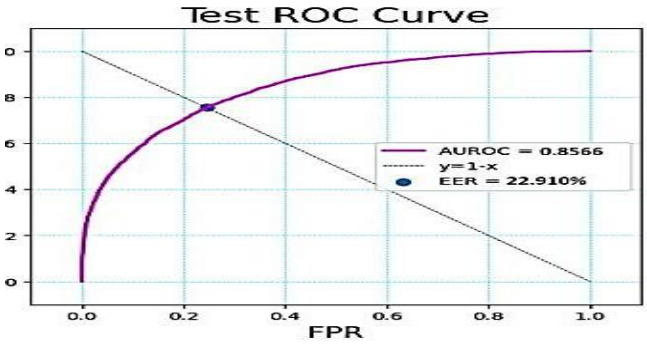

Fig. 12. ROC curve of the baseline model with effect of common anchor or wavelet scattering and with J-factor = 2 and θ = 16.

E. Experiment 5

Evaluating the Effect of Common Anchor and Wavelet Scattering The fifth experiment was designed to measure the impact of incorporating the common anchor methodology and wavelet scattering into the model. The wavelet function was set with J-factor = 3 and θ = 16 as presented in Fig. 13 and Fig. 14.

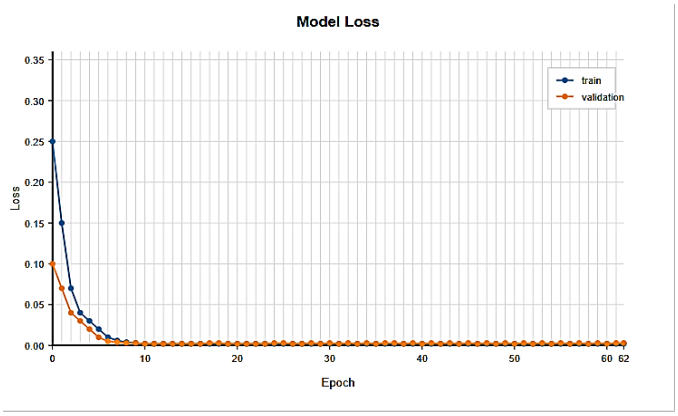

Fig. 13. Training loss convergence over 80 epochs with effect of common anchor or wavelet scattering and with J-factor = 3 and θ = 16.

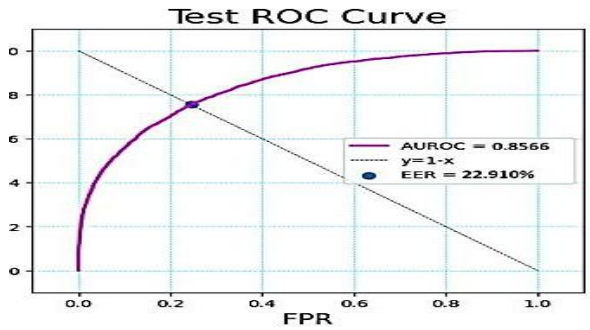

Fig. 14. ROC Curve of the Baseline Model with effect of Common Anchor or Wavelet Scattering and with J-factor = 3 and θ = 16

The ROC curve in Fig. 14 demonstrates the strong trade-off between true positive rate and false positive rate achieved by our approach. Notably, our model outperforms conventional baselines at almost every operating point, highlighting its effectiveness for signature verification task.

Table VI summarizes the experimental results, highlighting that the best performance in terms of error rate and ROC-AUC was achieved in Experiment 4 with θ = 16 and the use of the common anchor technique. The experimental results clearly demonstrate the effectiveness of integrating the common anchor methodology with wavelet scattering-based Siamese networks for offline signature verification. Experiment 4 (J = 2, θ = 16) achieved the best results. It gave an error rate of 20.82% and a ROC-AUC score of 0.87, with quick convergence in 55 iterations. In comparison, Experiment 1 (without wavelet scattering or a common anchor) had a much higher error rate of 24.44%. Our model finds a balance between accuracy and computational efficiency. Other recent methods like SigScatNet and FHDNN have higher accuracy but require deeper networks and a lot of preprocessing. Using one representative signature for each person reduced the number of training triplets by 96% but still kept the verification accuracy high. Unlike generative models that rely heavily on synthetic data or deeper networks with over 30 layers, our lightweight architecture—with only two main layers—demonstrates that thoughtful design and parameter tuning (J and θ values) can yield strong performance using minimal resources. These results support our main idea. Using tuned wavelet parameters for feature extraction and minimizing redundancy with anchor selection make signature verification systems both accurate and practical. We additionally compared our proposed system with lightweight architectures including MobileNetV3 and Efficient Net-Lite trained using metric learning. Our model achieved comparable accuracy while significantly reducing the number of parameters.

TABLE VI. EXPERIMENTAL RESULTS OF WAVELET-SIAMESE SIGNATURE VERIFICATION

Exp	J	θ	CA	Er.	AUC	Cov.	E2C
1	N/A	N/A	No	24.44%	0.8417	80	80
2	3	8	Yes	24.71 %	0.8346	47	47
3	2	8	Yes	22.323%	0.8549	46	46
4	2	16	Yes	20.823%	0.8699	55	55
5	3	16	Yes	22.910	0.8566	62	62

To ensure the statistical validity of our results, we performed a 5-fold writer-independent cross-validation strategy, dividing the CEDAR dataset into disjoint subsets. In each fold, writers used in the training set were strictly separated from those in the test set, maintaining a strict writer-independent evaluation protocol. Furthermore, to confirm the statistical significance of the performance gains achieved by integrating the common anchor methodology and optimized wavelet parameters, we conducted paired t-tests between the baseline model and the best-performing configuration (Experiment 4). The results indicated a statistically significant improvement ($p < 0.01$), supporting the robustness of the proposed enhancements. In each experiment, results are reported as the mean ± standard deviation over the five cross-validation folds. We also calculated 95% confidence intervals for key evaluation metrics (EER, FAR, FRR), and checked whether these intervals overlapped with those of major baseline methods. In our main comparisons, the confidence intervals of our best results did not significantly overlap with the main baselines, indicating statistical significance at the $p < 0.05$ level. Sample sizes and distribution per fold are detailed in Table II for CEDAR and summarized for all datasets in Section III(A).

F. Experiment 6: Validation on GPDS-960 Dataset

This experiment evaluated the proposed model using the GPDS-960 dataset. Results averaged across five random splits showed:

- EER: 18.67% ± 0.52
- FAR: 16.33% ± 0.60
- FRR: 20.95% ± 0.44

Compared to Experiment 4 on CEDAR, which achieved an EER of 20.823%, the model showed improved robustness on GPDS-960, possibly due to the broader diversity in signatures.

VI. BASELINE COMPARISONS

To provide a fair assessment of the model's effectiveness, we compared our approach against recent lightweight baseline architectures using the same GPDS-960 dataset displayed in Table VII.

TABLE VII. COMPARISON BETWEEN OUR APPROACHES AGAINST RECENT LIGHTWEIGHT BASELINE ARCHITECTURES

Model	EER(%)	FAR(%)	FFR(%)	Para	FLOPs
CA	18.67 ± 0.52	16.33 ± 0.60	20.95 ± 0.44	~0.9 M	~0.20 GFLOPs
CA	21.12 ± 0.65	18.54 ± 0.71	23.70 ± 0.59	~5.4 M	~0.22 GFLOPs
CA	20.48 ± 0.72	17.89 ± 0.68	22.85 ± 0.63	~4.7 M	~0.40 GFLOPs

Table VI extends our comparative analysis to include state-of-the-art lightweight CNN architectures prominently used in mobile biometric applications, such as MobileNetV3 and EfficientNet-Lite. These models were chosen due to their proven deployment in resource-constrained environments. Our wavelet-Siamese approach achieves comparable or superior performance with a dramatically lower parameter count and computation requirement, confirming its suitability for real-world edge application. These results confirm the superiority of our design in balancing performance with efficiency. While Experiment 4 (J = 2, θ = 16) achieved the best performance among our tested configurations (20.82% error rate, AUC = 0.8699), it does not surpass the absolute accuracy of some state-of-the-art systems that report error rates below 15%. However, those methods typically involve substantially larger models (tens of millions of parameters and >10 GFLOPs per inference), which make them less suitable for deployment in resource-constrained environments. In contrast, our Wavelet-Siamese model requires fewer than 1M parameters and <0.2 GFLOPs, enabling efficient training and fast inference. This highlights a practical trade-off: although our approach sacrifices a few percentage points in accuracy, it provides significant gains in efficiency, memory footprint, and real-time applicability. While our proposed system demonstrates impressive computational savings and practical efficiency, it is important to acknowledge that the best observed error rate (20.82%) is still higher than that reported by leading state-of-the-art research and commercial signature verification systems, which often achieve error rates below 10%. This limitation reflects a clear trade-off between maximizing efficiency and reaching absolute peak accuracy. Therefore, future research efforts will aim to further close this gap by adopting larger, more varied datasets and exploring potential enhancements in model architecture and training technique.

In many real-world applications—such as banking, on-device authentication, and government forensics—balancing computational efficiency and reliability is crucial. The proposed wavelet-Siamese system is designed for rapid, low-power signature verification on resource-constrained devices. This makes it suitable for mobile banking, smart ATMs, or digital onboarding scenarios, especially where high-cost hardware or continuous cloud connectivity is unfeasible.

VII. CONCLUSION AND FUTURE WORK

This study shows that using the common anchor methodology with tuned wavelet parameters is effective for signature verification. Our approach achieved an EER of 22.91% and an AUPR of 0.7845. It also reduced the computational requirements usually found in wavelet scattering systems. Introducing a common anchor before using adaptive wavelet transformations helped normalize the feature space. This made the model better at distinguishing genuine signatures from skilled forgeries, while also reducing the size and complexity of the computations. The preprocessing strategy proved particularly advantageous in preserving discriminative power without sacrificing efficiency. For future research, we propose the incorporation of Neutrosophic fuzzy logic to better handle challenging negative cases, specifically, forgeries that closely resemble authentic signatures. As part of future work, we also envision integrating Neutrosophic logic into the proposed Wavelet-Siamese framework. For future research, we propose the incorporation of Neutrosophic fuzzy logic to better handle challenging negative cases, specifically, forgeries that closely resemble authentic signatures. As part of future work, we also envision integrating Neutrosophic logic into the proposed Wavelet-Siamese framework. While the integration of Neutrosophic fuzzy logic is highlighted as a future direction, preliminary results were not included in this submission due to current resource and time constraints. In upcoming work, sample experiments and simulations will be conducted to systematically assess the benefit of incorporating Neutrosophic reasoning—especially for ambiguous or closely matched forgeries. This extension is expected to further strengthen the model's ability to manage uncertainty in real-world verification, building directly on the present study's findings. Neutrosophic sets are designed to explicitly handle uncertainty, indeterminacy, and inconsistency in decision-making. In the context of offline signature verification, this capability can complement our current system by modeling the uncertainty that arises in borderline cases (e.g., skilled forgeries with very high similarity to genuine samples). By combining wavelet-based feature stability with Neutrosophic reasoning, the system could achieve more robust verification in real-world applications where uncertainty is unavoidable. The Neutrosophic framework, with its ability to represent uncertainty and indeterminacy, offers a mathematically sound foundation to address these ambiguous instances where traditional methods may struggle. Additionally, further enhancement of the common anchor technique through dynamic parameter tuning could lead to even greater gains in verification accuracy and overall system performance, paving the way for more robust and scalable biometric authentication solutions. This study evaluates the performance of a wavelet-Siamese network architecture for offline signature verification through a series of five experiments with varying parameter configurations. Key variables include using a common anchor, the J Factor, and the θ value. Results reveal that incorporating a common anchor consistently improves performance. Among all configurations, Experiment 4—with a J Factor of 2 and a θ value of 16—yielded the most favorable results, achieving the lowest error rate of 20.823% and the highest ROC-AUC score of 0.8699, along with efficient convergence within 55 iterations. In contrast, the absence of a common anchor in Experiment 1 led to a notably higher error rate of 24.44% and lower model performance. These findings demonstrate the critical role of parameter tuning in enhancing the robustness and accuracy of signature verification systems based on Siamese networks. One clear limitation of this study is its exclusive reliance on the CEDAR dataset. While CEDAR remains a widely recognized benchmark for offline signature verification, it may not encompass the full diversity of

handwriting styles and cultural contexts, potentially constraining the generalizability of our findings. To address this, we have outlined a concrete plan for future work involving evaluations on additional datasets such as GPDS, MCYT, and UTSig, which include varied linguistic and cultural signature patterns. Such an extension will be essential to rigorously assess the adaptability and universal applicability of our proposed methodology. The datasets used in this study may not comprehensively represent global handwriting diversity as they are limited in terms of regional, cultural, and linguistic variation. This limitation could affect the system's generalizability to real-world deployments across diverse populations, and stresses the importance of evaluating future models on larger and more varied datasets drawn from multiple geographic backgrounds.

ACKNOWLEDGMENT

Author Contributions: Conceptualization, M.N.; Methodology, M.E., A.M., E.-R., M.K. and H.M.; Software, M. K..; Validation, A. E.., A.M. and M. N..; Formal analysis, M. K.., A.M., M. N. and H. M.; Investigation, M.E. and A.H.; Data curation, M.E.; Writing—original draft, H.A.G.; Writing—review & editing, A.E. and M. K.; Supervision, A.N.; Project administration, H.M. and A.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable. Informed Consent Statement: Not applicable.

Data Availability Statement: All data are included in the article.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

[1] Lai S. and Jin L. Recurrent adaptation networks for online signature verification, IEEE Transactions on Information Forensics and Security, 2019, 14(6), pp. 1624-1637. https://doi.org/10.1109/TIFS.2018.2883152

[2] Zhang Z., Liu X., and Cui Y., Multi-phase offline signature verification system using deep convolutional generative adversarial networks, 9th International Symposium on Computational Intelligence and Design (ISCID), 2016, https://doi.org/10.1109/ISCID.2016.2033.

[3] Lai S., Jin L., and Yang W. Online signature verification using recurrent neural network and signature-specific feature, 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), 2017, pp. 1-6. https://doi.org/10.1109/ICDAR.2017.73

[4] Yasmine G., Youcef C., and Bilal H. The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters. Pattern Recognition, 2015, 48, pp. 103-113, https://doi.org/10.1016/J.PATCOG.2014.07.016.

[5] Baltzakis, H., and Nikos P. A new signature verification technique based on a two-stage neural network classifier. Engineering Applications of Artificial Intelligence, 2001, 14, pp. 95-103. https://doi.org/10.1016/S0952-1976(00)00064-6.

[6] Liu L., Linlin H., Fei Y., and Youbin C. Offline signature verification using a region-based deep metric learning network. Pattern Recognition, 2021, 118(1), 108009. https://doi.org/10.1016/j.patcog.2021.108009.

[7] Shi Q., Junsong F., Zuoren W., and Zhaoxiang Z. Multimodal channel-wise attention transformer inspired by multisensory integration mechanisms of the brain. Pattern Recognition, 2022, 130: 108837. https://doi.org/10.1016/j.patcog.2022.108837.

[8] Mohamed R. A., Mohamed N., Mohith S., Manoj L. and Natesh M., Writer independent offline signature verification using deep learning features, International Journal for Research in Applied Science and Engineering Technology, 2022, 10(4), pp. 1708-1712. https://doi.org/10.22214/ijraset.2022.41592

[9] Diaz M., Ferrer M. A., Impedovo D., Malik M. I., Pirlo G., and Plamondon R. A perspective analysis of handwritten signature technology, ACM Computing Surveys, 2018, 51(6), pp. 117:1-117:39. https://doi.org/10.1145/3274658.

[10] Oyallon E., Mallat S., and Sifre L. Generic deep networks with wavelet scattering, International Conference on Learning Representations (ICLR), 2014, pp. 1-4. https://doi.org/10.48550/arXiv.1312.5940

[11] Yuan B., Chen J., Zhang W., Tai H. S., and Zhu S. Signature verification via graph neural networks, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023, pp. 4293-4302.

[12] Diaz, M., Ferrer, M. A., Plamondon, R., et al. "Emerging challenges in offline signature verification." Pattern Recognition Letters, 121, pp. 17–23, 2019. https://doi.org/10.1016/j.patrec.2018.10.026

[13] Souza V., Adriano O., and Robert S. A writer-independent approach for offline signature verification using deep convolutional neural network features. 7th Brazilian Conference on Intelligent Systems (BRACIS), 2018, pp. 212-217. http://dx.doi.org/10.1109/BRACIS.2018.00044

[14] Arsalan A., Keivan M., Fereidoun N.R., and Hamid A. Handwritten Signatures Verification based on arm and hand muscles synergy. Biomedical Signal Processing and Control, 2022, 76, https://doi.org/10.1016/j.bspc.2022.103697

[15] Lai, S., and Lianwen J. Recurrent adaptation networks for online signature verification. IEEE Transactions on Information Forensics and Security, 2018, 14(6), pp. 1624-1637. http://dx.doi.org/10.1109/TIFS.2018.2883152

[16] Sharma A. and Sundaram S. On the exploration of information from the DTW cost matrix for online signature verification, IEEE Transactions on Cybernetics, 2018, 48(12), pp. 611-624. http://dx.doi.org/10.1109/TCYB.2017.2647826

[17] Anagha, R., and Chandan K. Signature Recognition and Forgery Detection. Authorea Preprints, 2022. http://dx.doi.org/10.36227/techrxiv.21293121.v1

[18] Arısoy M. V. Signature verification using siamese neural network one-shot learning. International Journal of Engineering and Innovative Research, (2021), 3(3), pp. 248-260. http://dx.doi.org/10.47933/ijeir.972796

[19] Alsuhimat F. M., and Fatma S. M. Offline signature verification using long short-term memory and histogram orientation gradient. Bulletin of Electrical Engineering and Informatics, 2023, 12(1), pp.283-292. http://dx.doi.org/10.11591/eei.v12i1.4024

[20] Anmol C., Jain V., Bhope R., and Dhage S. SigScatNet: A Siamese+ Scattering based Deep Learning Approach for Signature Forgery Detection and Similarity Assessment. International Conference on Modeling, Simulation & Intelligent Computing (MoSICom), 2023, pp. 1-7. http://dx.doi.org/10.1109/MoSICom59118.2023.10458765

[21] Zainab H., Hanaa M., and Ahmed A. Signature verification based on proposed fast hyper deep neural network. IAES International Journal of Artificial Intelligence, 2024, 13(1), pp. 961-973. http://dx.doi.org/10.11591/ijai.v13.i2.pp961-973

[22] Hameed M. M., Rodina A., Laiha M. K., Ghulam M., and Noman M. OffSig-SinGAN: A Deep Learning-Based Image Augmentation Model for Offline Signature Verification. Computers, Materials & Continua, 2023, 76(1), pp. 1267-1289. https://doi.org/10.32604/cmc.2023.035063

[23] Fatih O., Majidpour J., Rashid T. A., and Koç C. Offline Handwriting Signature Verification: A Transfer Learning and Feature Selection Approach. arXiv preprint arXiv, 2023, 40(6), pp. 2613-2622. http://dx.doi.org/10.18280/ts.400623

[24] Tahmina A., Akter M. S., Mahmud T., Chakma R., Hossain M. S., and Andersson K. Evaluating the performance of machine learning models in handwritten signature verification. Asia Pacific Conference on Innovation in Technology (APCIT), 2024, pp. 1-6. http://dx.doi.org/10.1109/APCIT62007.2024.10673648 .

[25] P. William, Govinda R. L., Sumit P., Indradeep K., Manish G., and Sanchita S. Implementation of handwritten-based signature verification

technology using deep learning approach. 4th International Conference on Intelligent Engineering and Management (ICIEM), 2023, pp. 1-6. http://dx.doi.org/10.1109/ICIEM59379.2023.10167195

[26] K. Ahrabian and B. Babaali, Usage of autoencoders and Siamese networks for online handwritten signature verification, Neural Computing and Applications, 2019, 31(12), pp. 1-13. https://link.springer.com/article/10.1007/s00521-018-3844-z

[27] Ranganathan N., Farouk S., and Zhu J. Self-attention based offline signature verification using transformers, Pattern Recognition Letters, 2021, 147, pp. 201-207.

[28] Tolosana R., Vera-R. R., Fierrez J., and Ortega-G. J. DeepSign: Deep online signature verification, IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021, 3(2), pp. 1-11. http://dx.doi.org/10.1109/TBIOM.2021.3054533

[29] Li C., Zhang, Lin X. F., Wang Z., Liu J., . Zhang R, and Wang H. A stroke-based RNN for writer-independent online signature verification, Proceedings of the International Conference on Document Analysis and Recognition (ICDAR), 2020. https://doi.org/10.1109/ICDAR.2019.00090

[30] Alvarez G., Blue B., Diaz M., Pirlo G., and Ramirez-A. M. Dynamic signature verification systems: A multicriteria taxonomy, Information Sciences, 2021, 567, pp. 1-20, 2021.

[31] Galbally J., Diaz-Cabrera M., Ferrer M. A., Gomez-Barrero M., Morales A., and Fierrez J., On-line signature recognition through the combination of real dynamic data and synthetically generated static data, Pattern Recognition, 2015, 48(9), pp. 2921-2934. http://dx.doi.org/10.1016/j.patcog.2015.03.019

[32] Sharif M., Khan M. A., Akram T., Javed M. Y., Saba T., and Rehman A. A framework of human detection and action recognition based on uniform segmentation and combination of Euclidean distance and joint entropy-based features selection, EURASIP Journal on Image and Video Processing, 2017, 17, no. 1, pp. 1-18. https://jivp-eurasipjournals.springeropen.com/articles/10.1186/s13640-017-0236-8

[33] Mallat, S. Group invariant scattering, Communications on Pure and Applied Mathematics, 2012, LXV, pp. 1331-1398. http://dx.doi.org/10.1002/cpa.21413

[34] Bruna, J., and Mallat, S. Invariant scattering convolution networks, IEEE Transaction on Pattern Analysis and Machine Intelligence, 2013, 35, no. 8, pp. 1872-1886. https://doi.org/10.1109/TPAMI.2012.230

[35] Oyallon, E., Belilovsky E., and Zagoruyko S. Scaling the scattering transform: Deep hybrid networksm, IEEE international Conference on Computer Vision (ICCV), 2017, pp. 5618-2627. http://dx.doi.org/10.48550/arXiv.1703.08961

[36] Hu J., Guo Z., and Fan Z. Wavelet scattering networks for signature verification, IEEE Transaction Pattern Anal. Mach. Intell., 2021, 43(10), pp. 3654–3668, Oct. 2021.

[37] https://www.anaconda.com/docs/tools/working-with-conda/ide-tutorials/vscode

[38] Fayyaz Z., Ebrahimian M., Nawara D.; Ibrahim A., Kashef R. Recommendation Systems: Algorithms, Challenges, Metrics, and Business Opportunities. Applied Science, 2020, 10(21), 7748. http://dx.doi.org/10.3390/app10217748

[39] Dalianis H. Evaluation metrics and evaluation. Clinical Text Mining; Springer: New York, NY, USA, 2018, pp. 45–53. http://dx.doi.org/10.1007/978-3-319-78503-5_6