SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I12P117

Volume 12 Issue 12, 201-217, December 2025

Original Article

Novel Approach of Offline Signature Verification Using Online Signature Database and Pre-Trained Deep Convolution Neural Network: SqueezeNet

Bhimraj Prasai Chetry[1], Gunajyoti Das[2], Biswajit Kar[3]

[1,3]*Department of Instrumentation Engineering, Central Institute of Technology Kokrajhar, Assam, India.*
[2]*Department of Chemistry, Central Institute of Technology Kokrajhar, Assam, India.*

[1]*Corresponding Author : bp.chetry@cit.ac.in*

Received: 17 October 2025 Revised: 17 November 2025 Accepted: 16 December 2025 Published: 27 December 2025

Abstract *- Signature is a vital behavioral biometric trait. It has been used for secure authentication for centuries. An innovative framework that converts dynamic online signature data from the SVC 2004 database into offline grayscale images has been proposed here. And finally, offline signature verification is done using a pre-trained lightweight CNN, SqueezeNet. Essential signer-specific patterns are preserved in the process of online-to-offline conversion. Before feeding the SqueezeNet input, the signature images undergo a preprocessing step that includes grayscale-to-RGB conversion and resizing. Subsequently, transfer learning is used to distinguish between genuine and forged signatures. By adopting this strategy, the model can be efficiently deployed in resource-constrained environments without sacrificing accuracy. It uniquely integrates online and offline signature verification. It also provides extensive threshold-based evaluation using various fundamental classification metrics, biometric-specific performance metrics, and ROC curve analysis. User-specific and Global Youden Thresholds, User-specific and global EER threshold, Equal Error Rate (EER), and analysis of False Acceptance Rate (FAR) and False Rejection Rate (FRR) versus threshold are included in this study. Global ROC provides a Global Youden Threshold. And the average FAR and FRR curves vs threshold gives the global EER threshold. Offline signature verification under raw threshold, user-specific Youden threshold, and user-specific EER thresholds is performed here. Excellent accuracy, flexibility, and robustness are seen here. The idea of offline signature verification derived from online data, when combined with compact CNN architectures, SqueezeNet, can bridge the gap between online and offline signature verification systems. This work contributes toward scalable, cross-domain biometric verification solutions and opens up ways towards unified signature recognition systems. This first-of-its-kind, cross-domain framework delivers a scalable, accurate, and resilient signature verification solution for both random and skilled forgeries. The proposed Offline Signature Verification system using online signature database achieves the best average testing accuracy of 99.81% (With User Specific Youden Thresholding) for random forgeries and 94.81% (With User Specific Youden Thresholding) for skilled forgeries across all 40 users. Here, the testing accuracy of random forgeries ranges from (92.50-100.00) %, and skilled forgeries ranges from (72.50-100.00) %. Hence, the proposed system yielded very good accuracy in comparison to existing state-of-the-art results, offering a practical solution to real-world applications.*

Keywords *- Behavioral Biometric, CNN, Offline Signature Verification, SqueezeNet, SVC 2004 Database.*

1. Introduction

Biometric authentication has emerged as a critical technology for ensuring secure access to digital and physical systems, with handwritten signature verification remaining one of the most socially accepted and legally recognized methods [1]. Traditional signature verification is categorized into two primary modes: online and offline verification. Online verification uses dynamic features such as writing speed, pen pressure, and stroke order, whereas offline verification relies only on static images of signatures [2, 3]. Offline Signature Verification has significant challenges due to the absence of temporal information, making systems susceptible to intra-class variability and skilled forgeries [4].

Recent advancements in deep learning and transfer learning have substantially enhanced the accuracy of Offline Signature Verification systems. Pre-trained Convolutional Neural Networks (CNNs), particularly lightweight architectures such as SqueezeNet, offer compact models that can be efficiently fine-tuned for binary signature verification tasks [5]. SqueezeNet has demonstrated remarkable performance in recent studies, achieving identification

accuracies above 99.79% on multiple datasets, including BHSig260-Bengali, BHSig260-Hindi, CEDAR, and UTSig, with training times under 3 minutes per dataset [6]. However, a major challenge that remains underexplored is bridging the gap between online and offline verification domains for cross-domain biometric verification.

Existing Offline Signature Verification methods predominantly focus on static signature datasets without integrating the rich dynamic cues present in online data [7, 8]. Research done by Cairang et al. [9] has shown that cross-domain verification using Siamese networks with Triplet loss and Cross Entropy loss can improve model generalization across different domains. So, closing this gap opens the door for building unified verification systems. Regardless of how the signatures were originally acquired, these systems can authenticate signatures. As the latest techniques for cross-layer weakly supervised data augmentation demonstrated this [10].

Offline signature verification is done using SqueezeNet after the online signature data has been converted into offline signature images. This novel technique facilitates cross-domain verification as online data has been used in offline models. It is seen that it improves flexibility, robustness, and scalability across real-world scenarios. As a result, it can be a promising research direction to develop an integrated, scalable, and highly precise signature verification solution.

Evaluation of advanced metrics such as Youden's J statistic for threshold determination, Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR) has been done. Performance evaluation is done through FAR and FRR vs. threshold curves, average ROC curves, and global Youden thresholds derived from global ROC curves. To analyze verification performance, we have done verification using raw thresholding, user-specific Youden thresholds, and EER thresholds, with global EER assessment through average FAR/FRR curves. Performance metrics such as Accuracy, Precision, Recall, and F1-Scores are comprehensively evaluated for analysis [11-16].

2. Literature Review

Generally, handwritten signature verification can be classified into online and offline modes, each having distinct data acquisition and processing techniques used. In online signature verification, temporal dynamics are captured using devices like tablets or styluses, whereas offline signature verification relies on static images scanned from paper documents [17]. Usually, Online Signature Verification gives higher accuracy than Offline Signature Verification due to its rich temporal data. But it is seen that Offline Signature Verification is more commonly used in practical applications where only scanned or photographed signatures are available for verification [18, 19].

Major challenges that an Offline Signature Verification system has to go through are Signature forgeries. Forgeries are generally classified into three types as shown below [7, 20]:

- Random Forgeries – Signer produces the signatures without any prior knowledge of the genuine signature, so the signatures produced differ significantly in appearance.
- Simple Forgeries – Imitators produce signatures who know the signer's name but have not seen the genuine signature.
- Skilled Forgeries – An Imposter produces highly deceptive signatures after observing or practicing the genuine signature multiple times. This is the most challenging category for Offline Signature Verification systems.

Hand-crafted features such as Histogram of Oriented Gradients (HOG), Local Binary Patterns (LBP), or Geometric Descriptors [18, 21, 22] are used in conventional Offline Signature Verification techniques. Deep learning has transformed the field by automatically learning discriminative features from raw signature images. Various CNN architectures in Offline Signature Verification tasks have shown superior performance when done with transfer learning [23, 24].

Çiftçi and Tekin [25] compared five different deep learning methods: GoogLeNet, MobileNet-V3 Large, Inception-V3, ResNet50, and EfficientNet-B0, where GoogLeNet and Inception-V3 achieved an accuracy of 98.77%.

SqueezeNet is a lightweight CNN architecture. It has the advantage of remarkably reduced model size without compromising accuracy [5]. It is highly suitable for resource-constrained biometric applications because of its efficiency. Purbanugraha et al. [6] developed an optimized SqueezeNet with ADAM backpropagation, demonstrating good results across multiple datasets with identification accuracies above 99.79% and training times under 3 minutes per dataset.

Siamese networks have become a powerful architecture for signature verification tasks. Tehsin et al. [26] developed a Triplet Loss Siamese Similarity Network (tSSN) while combining with Manhattan distance measures, which gives better performance. The approach was evaluated on several datasets, including 4NSigComp2012, SigComp2011, 4NSigComp2010, and BHSig260, showing enhanced verification accuracy in scenarios with close signature similarity. Cross-domain verification is still an underexplored area. However, lots of research has been done to improve Offline Signature Verification and Online Signature Verification separately. Cairang et al. [9] proposed a novel approach for learning generalizable representations using Siamese networks combined with Triplet loss and

Cross Entropy loss. Their method has given better performance in cross-domain than single-domain applications using Instance Normalization and a module called Inference Layer Normalization Neck (ILNNeck) to improve model generalization across various domains.

As per recent research, transforming online signature data into offline signature images can enhance Offline Signature Verification, allowing models to learn from both static and dynamic characteristics [27, 28]. However, few methods have systematically integrated online datasets with compact CNNs for unified verification. Our research addresses this gap by introducing a SqueezeNet-based framework that uses online signature data in offline verification, providing enhanced robustness and scalability.

To ensure comprehensive performance assessment, modern signature verification systems employ multiple threshold-based and curve-based metrics [11-16] below:

- Youden Threshold: Determined by maximizing Youden's J statistic (TPR - FPR), providing an optimal trade-off between sensitivity and specificity.
- Equal Error Rate (EER): The point at which FAR matches FRR, representing balanced system performance.
- FAR and FRR vs. Threshold: Graphical representation to evaluate trade-offs at different thresholds, also used to determine global EER and its corresponding threshold.
- Average ROC Curves: Averaged True Positive Rate (TPR) across users for common FPR values to evaluate overall discriminative ability.
- Global Youden Threshold from Global ROC: A single threshold derived from all scores for cross-user performance optimization.
- Average FAR and FRR vs. Threshold: Used to calculate global EER and global EER threshold, showing system behavior under collective evaluation.

Current state of research in offline signature verification is the integration of cross-domain capabilities, lightweight architectures like SqueezeNet, and thorough evaluation of frameworks addressing both theoretical advances and practical deployment requirements in real-world biometric systems.

This research is the first to unify online and offline signature verification in a single framework using SqueezeNet. By converting online signatures into offline representations and integrating user-specific and global thresholding (Youden and EER) with comprehensive ROC and FAR/FRR analysis, our system achieves scalable, cross-domain verification. Unlike prior works, it simultaneously provides raw, user-specific, and global evaluations, offering robust, flexible, and practical solutions for real-world biometric applications using raw thresholding, user-specific Youden and EER thresholds, and global EER evaluation through average FAR/FRR curves.

3. Proposed Model

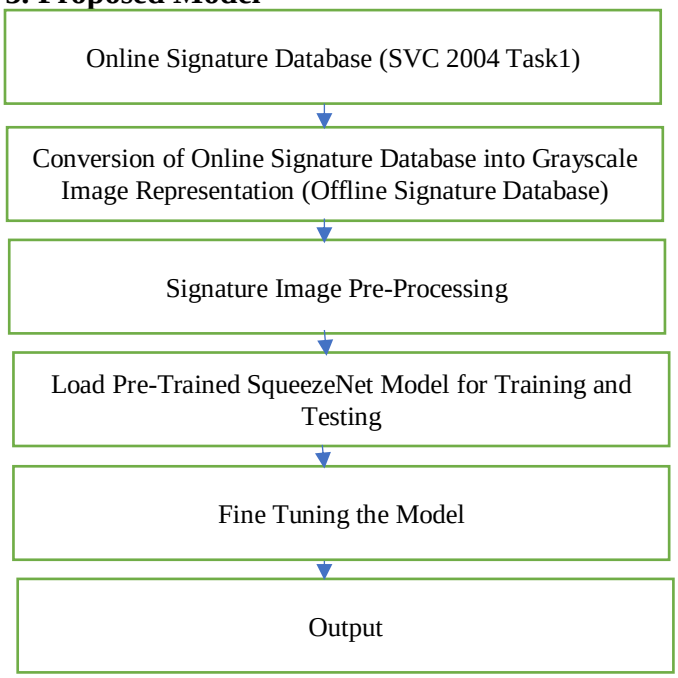

Fig. 1 Block diagram for offline signature verification using an online signature database and deep learning pretrained squeezenet network

The block diagram in Figure 1 shows how a pretrained SqueezeNet model can be used for offline signature verification using an online signature database. The process has multiple steps, from loading the Pretrained SqueezeNet Network to final verification. Below is the description of the blocks:

3.1. Block Diagram Description

The following steps outline how a pretrained SqueezeNet model can be used for offline signature verification:

Step 1: About the Database

We have used the SVC2004 Task 1 dynamic signature dataset, as referenced in [29], which includes signature data collected from 40 individual users. Each user contributed a total of 40 signature samples, stored in text files named using the format "UxSy.txt", where 'x' represents the user ID and 'y' denotes the specific signature instance as given in Equation (1) below.

$$x \in \{1,2,3,\ldots..40\},\ y \in \{1,2,3,\ldots..40\} \quad (1)$$

The first 20 signatures (i.e., y = 1 to 20) in each user's folder are genuine, while the remaining 20 samples (i.e., y = 21 to 40) are skilled forgeries, created by other individuals attempting to replicate the genuine signatures. In total, the

dataset contains 1600 signature files (40 users x 40 samples each), as cited in [30]. In every file, the signature is described by a sequence of points. Each signature file begins with a single number indicating the total number of points in the signature sequence.

Following this, each line represents a data point comprising four features, namely, X-coordinate, Y-coordinate, Time stamp, and Button status (indicating whether the pen is pressed or lifted) as shown in Figure 2. Here, we have converted all the 1600 signature files into offline signature images to perform offline signature verification using an online signature database. The shape of the offline converted signature images from the online Signature database is shown in Figure 3.

X-Coordinate	Y-Coordinate	Time Stamp	Button Status
148			
635	5541	31077710	0
618	5431	31077720	1
600	5443	31077730	1
575	5515	31077740	1
575	5515	31077750	1
608	5515	31077760	1
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.

Fig. 2 First genuine signature instance of User1 of the SVC2004 Task1 online signature database in text file format

User	Genuine Signatures	Skill Forgery Signatures
1		
2		
3		
4		
5		

Fig. 3 Some sample offline converted signatures of the SVC 2004 task 1 online signature database

Step 2: Conversion of the Online Signature Database into an Offline Database.

In every file, the signature here in the SVC 2004 online signature database is described by a sequence of points. Each line represents a data point comprising four features, namely, X-coordinate, Y-coordinate, Time stamp, and Button status (indicating whether the pen is pressed or lifted) as shown in Figure 2. Here we have converted the entire 1600 signature files, i.e., the entire database, into offline signature images without any background using MATLAB programming to perform offline signature verification. The shape of the offline converted signature images from the online/dynamic signature database is shown in Figure 3.

Step 3: Signature Image Pre-processing

The initial step in utilizing SqueezeNet for offline signature verification involves preprocessing the signature images and resizing them to align with SqueezeNet's input requirements. Specifically, all images in the dataset were resized to a consistent dimension of 227x227 pixels prior to being fed into the network's input layer. The converted signature images, originally sourced from the SVC 2004 database, were in grayscale JPG format. To ensure compatibility with SqueezeNet's input specifications, these grayscale images were converted to RGB format. Once converted, the images were processed through SqueezeNet to extract feature maps from its intermediate layers. These extracted features effectively capture critical characteristics of a signature, such as stroke dynamics, shape structures, and other distinctive signature traits [31].

Step 4: Pretrained Model (SqueezeNet)

SqueezeNet is a lightweight Convolutional Neural Network (CNN) architecture that is well-suited for applications with limited computational resources. It offers performance comparable to larger models such as ResNet and VGG, but with significantly fewer parameters. Numerous pretrained versions of SqueezeNet are available in popular Deep Learning frameworks and can be fine-tuned for specific tasks, including signature verification [32]. Designed to maintain a balance between model size and accuracy,

SqueezeNet proves beneficial in scenarios where computational efficiency and rapid inference are crucial, making it an optimal choice for offline signature verification systems, particularly in resource-constrained environments.

Key Features of SqueezeNet:

- Compact Structure: SqueezeNet delivers a small model size while maintaining accuracy comparable to larger CNN architectures like VGG and ResNet, using considerably fewer parameters.
- Fire Modules: The architecture introduces Fire Modules, each composed of a squeeze layer with 1x1 convolutions succeeded by an expansion layer that includes both 1x1 and 3x3 convolutions. This structure helps reduce the number of parameters while preserving performance.
- Pre-trained Weights: Like many CNNs, SqueezeNet supports fine-tuning through pretrained weights on large-scale datasets such as ImageNet. This allows for adaptation to more specific tasks, including offline signature verification.

Using a pretrained SqueezeNet model for offline signature verification is particularly effective in scenarios where a fast, lightweight solution is necessary. By using transfer learning, SqueezeNet, a deep CNN, can be adapted to distinguish between genuine and forged signatures by identifying key distinguishing features [33]. Transfer learning in this context refers to the process of starting with a model pretrained on a large dataset (such as ImageNet) and then fine-tuning it using a domain-specific dataset, like one for offline signature verification.

Signatures exhibit unique characteristics such as stroke patterns, curvature, and writing speed, which require the model to adjust from recognizing general visual features to more specific handwriting traits [34].

Once features are extracted from the input signature, the next step involves comparing them with features from known genuine signatures. This comparison is performed using similarity measures like Euclidean distance or cosine similarity.

Based on the similarity score, a classification mechanism such as thresholding or a SoftMax classifier is then used to determine whether the signature is genuine or forged [35].

Step 5: Fine-Tuning the Model

Fine-tuning plays a crucial role in effectively adapting the pretrained model to the signature dataset. This process typically involves freezing the initial layers of the network because these layers represent basic visual features such as edges and textures, which are generally transferable across tasks. The later layers of the model are then retrained using the signature dataset, allowing the network to learn high-level, signature-specific features. Through this approach, the model is able to leverage existing low-level representations while adapting to the unique patterns and characteristics found in signature data, such as lines and textures, which are often influenced by biases that make signature verification a complex task [36]. SqueezeNet pre-trained network has a total of 68 layers, having 1.2M total learnables.

3.2. Verification

3.2.1. Training

Here, training is done with randomly selected 60% offline converted signature images for every 40 users of the SVC 2004 online signature database, once with random forgery and subsequently with skill forgery. Combined Training Confusion Matrix for all Users using random forgery and using skill forgery are shown in Figures 4 and 5, respectively. Training accuracy and training time elapsed for each user using random forgery and skill forgery are displayed in Tables 1 and 3, respectively. Further average training accuracy and average training time elapsed are calculated for all 40 signers in both cases and displayed in Tables 1 and 3.

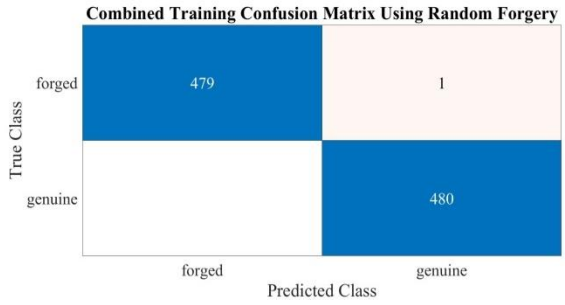

Fig. 4 Combined training confusion matrix using random forgery

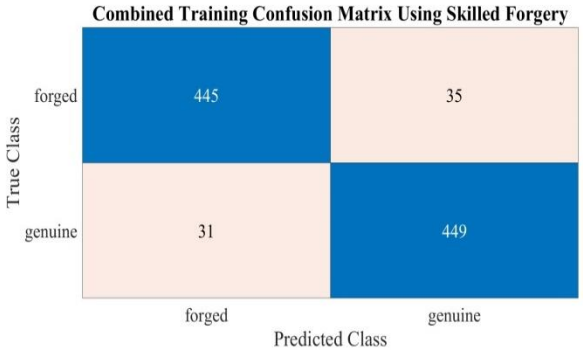

Fig. 5 Combined training confusion matrix using skilled forgery

3.2.2. Testing

Here, testing was done with all the 100% signatures data because of limited resources twice, as follows, once with offline converted skill forgery data given in the SVC 2004 online signature database. And subsequently, with the offline converted random forgery created using various users' signature images. Here, it is pertinent to mention that testing was done on Raw Thresholding, Best User-specific/

Individual EER Thresholding, and Best User-specific/ Individual Youden Thresholding for both the Random Forgery and Skill Forgery. Each User Testing Accuracy at different thresholds and other parameters, such as best individual EER Threshold, Youden threshold, AUC, and Equal Error Rate are shown in Table 1 and Table 3. Combined Testing Confusion Matrix of Raw, Individual EER thresholded, and Youden thresholded using Random forgery are shown in Figures 6, 7, and 8, respectively. Similarly, for skill forgery, it is shown in Figures 9, 10, and 11, respectively. Moreover, the average, highest, and lowest testing accuracy are calculated and shown in Table1 and Table 3 for both cases. Here we have also found out the Precision, Recall, and F1-Score for each user at the Youden threshold for both random and skill forgery, and are noted in Table 2 and Table 4, respectively.

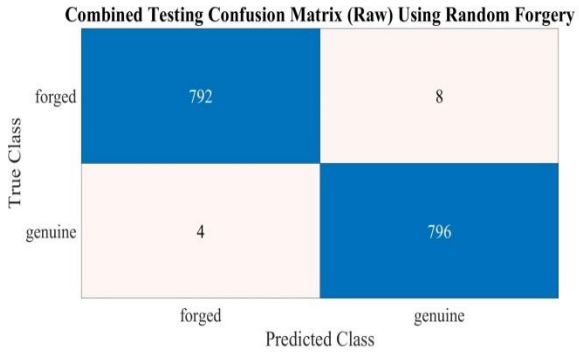

Fig. 6 Combined testing confusion matrix raw thresholded using random forgery

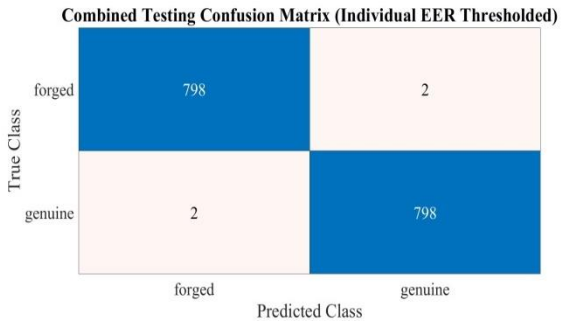

Fig. 7 Combined testing confusion matrix individual EER thresholded using random forgery

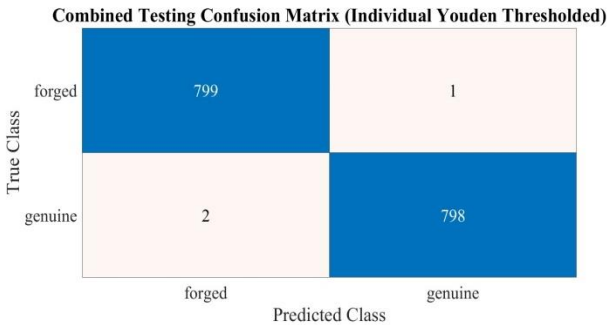

Fig. 8 Combined testing confusion matrix individual youden thresholded using random forgery

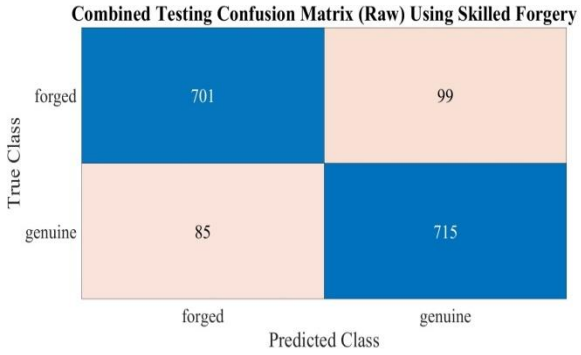

Fig. 9 Combined testing confusion matrix raw thresholded using skilled forgery

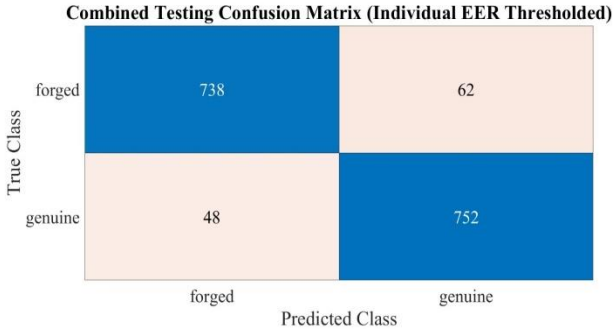

Fig. 10 Combined testing confusion matrix individual EER thresholded using skilled forgery

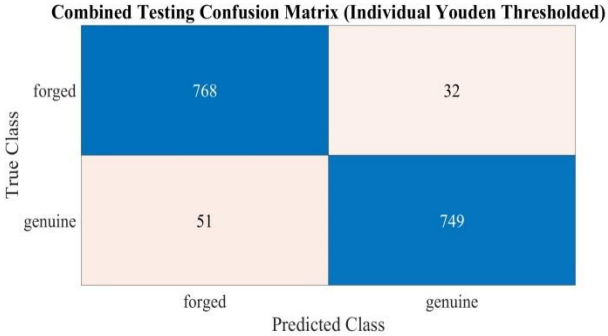

Fig. 11 Combined testing confusion matrix individual youden thresholded using skilled forgery

4. Verification Results and Performance Evaluation

The performance evaluation of offline signature verification systems is based on the confusion matrix components: True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), representing correctly/incorrectly classified genuine and forged signatures, respectively [11].

Fundamental Classification Metrics are given in [11] as follows:

Accuracy: It measures overall system correctness. The formula for it is given in Equation (2) below:

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})} \quad (2)$$

Precision: It quantifies the proportion of correctly identified genuine signatures among all accepted signatures. The formula for it is given in Equation (3) below:

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP})} \quad (3)$$

Recall (Sensitivity): It measures the proportion of genuine signatures correctly identified. The formula for it is given in Equation (4) below:

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

F1-Score: It provides the harmonic mean of precision and recall. The formula for it is given in Equation (5) below:

$$\text{F1} - \text{Score} = 2 \times \frac{(\text{Precision} \times \text{Recall})}{(\text{Precision} + \text{Recall})} \quad (5)$$

Biometric-Specific Performance Metrics are given in [12] as follows:

False Acceptance Rate (FAR): It represents the probability of incorrectly accepting a forged signature. The formula for it is given in Equation (6) below:

$$\text{FAR} = \frac{\text{FP}}{(\text{FP} + \text{TN})} \quad (6)$$

False Rejection Rate (FRR): It indicates the probability of incorrectly rejecting a genuine signature. The formula for it is given in Equation (7) below:

$$\text{FRR} = \frac{\text{FN}}{(\text{FN} + \text{TP})} \quad (7)$$

Equal Error Rate (EER): It represents the operating point where FAR equals FRR. It is depicted in Equation (8) below:

$$\text{EER} = \text{FAR} = \text{FRR (at optimal threshold } \tau\_\text{EER}) \quad (8)$$

EER provides a threshold-independent performance measure, with lower values indicating superior discrimination capability.

ROC curve analysis is given in [13, 14] as follows:

Receiver Operating Characteristic (ROC) curves: It is the plot of True Positive Rate against False Positive Rate across different threshold values, and their formula are given in Equations (9) and (10):

$$\text{TPR}(\tau) = \frac{\text{TP}(\tau)}{(\text{TP}(\tau) + \text{FN}(\tau))} \quad (9)$$

$$\text{FPR}(\tau) = \frac{\text{FP}(\tau)}{(\text{FP}(\tau) + \text{TN}(\tau))} \quad (10)$$

Area Under the ROC Curve (AUC): It provides a threshold-independent performance measure as given in Equation (11) below:

$$\text{AUC} = \int_0^1 \text{TPR}(\text{FPR}^{-1}(\text{x}))\text{dx} \quad (11)$$

Global ROC curves: It gives the aggregate performance across all test samples as represented in Equations (12) and (13) below:

$$\text{TPR}_{\text{global}} = \frac{\sum_\text{i} \text{TP}_\text{i}}{\sum_\text{i}(\text{TP}_\text{i} + \text{FN}_\text{i})} \quad (12)$$

$$\text{FPR}_{\text{global}} = \frac{\sum_\text{i} \text{FP}_\text{i}}{\sum_\text{i}(\text{FP}_\text{i} + \text{TN}_\text{i})} \quad (13)$$

Average ROC curves: It computes the mean performance across individual user ROC curves as given in Equations (14) and (15) below:

$$\text{TPR}_{\text{avg}(\tau)} = \frac{\sum_{\text{i}=1}^{\text{N}} \text{TPR}_\text{i}(\tau)}{\text{N}} \quad (14)$$

$$\text{FPR}_{\text{avg}(\tau)} = \frac{\sum_{\text{i}=1}^{\text{N}} \text{FPR}_\text{i}(\tau)}{\text{N}} \quad (15)$$

Threshold Selection Methods, as given in [15, 16], are as follows:

Youden Index: It maximizes the sum of sensitivity and specificity. It is given by the formula in Equation (16) below:

$$\text{J} = \text{Sensitivity} + \text{Specificity} - 1 = \text{TPR} - \text{FPR} \quad (16)$$

The optimal threshold maximizes the Youden Index and is given by Equation (17) below:

$$\tau\_\text{Youden} = \text{argmax}_\tau\,[\text{TPR}(\tau) - \text{FPR}(\tau)] \quad (17)$$

EER Threshold: It minimizes the difference between FAR and FRR, providing a balanced security-usability trade-off. It is given by the formula in Equation (18) below:

$$\tau_{\text{EER}} = \text{argmin}_\tau|\text{FAR}(\tau) - \text{FRR}(\tau)| \quad (18)$$

In offline signature verification, accuracy is a commonly used metric to assess the effectiveness of a system. The formula presented in Equation (2) was employed by the authors to measure the accuracy of the offline signature verification system, emphasizing its significance alongside complementary metrics such as False Acceptance Rate

(FAR) and False Rejection Rate (FRR) in assessing overall system performance [35-37]. Similarly, the same formula was utilized in the study by [31] to evaluate the performance of offline signature verification using discrete wavelet transforms and other machine learning approaches. Here, training accuracy, testing accuracy (at Raw, Youden User Specific Threshold, EER User Specific Threshold), EER, AUC, and training time for all 40 individual Users are recorded in Table 1 for random forgery and in Table 3 for skill forgery. Precision, Recall, and F1-Score while Testing Using Random Forgery for all 40 Users at Youden Threshold is shown below in Table 2, and similarly, while testing using Skill Forgery is shown in Table 4. Although we have done testing/verification using raw threshold, individual/user-specific Youden threshold, and individual/user-specific EER threshold. But we have also determined the Global ROC Curve using Random Forgery with Youden Threshold as shown in Figure 12 and the Global ROC Curve using skilled Forgery with Youden Threshold as shown in Figure 15. It is the plot of False positive rate vs. True positive rate which gives the overall/ global Youden point threshold of 0.5389 and 0.4926 in case of random forgery and skill forgery, respectively. Average FAR and FRR Curves vs Threshold for Random Forgery and Average FAR and FRR Curves vs Threshold for Skilled Forgery, which determine Global EER and Threshold, are shown in Figure 13 and Figure 16, respectively. This gives Global EER=0.75%, threshold=0.543 in case of random forgery, and Global EER=11.25%, threshold=0.508 in case of skilled forgery. The average ROC Curve across all 40 Users is shown in Figures 13 and 17, respectively, for random forgery and skilled forgery. Our Pretrained SqueezeNet model is trained and tested on the offline converted Signature images from SVC 2004 Task 1 online signature database for all forty users yielding excellent average testing accuracy of (99.25% for raw thresholding, 99.81% for Youden user specific thresholding and 99.75% for EER user specific thresholding) using Random Forgeries as shown in Table 1 and average testing accuracy of (88.50% for raw thresholding, 94.81% for youden specific thresholding and 93.13% for EER user specific thresholding) using Skilled Forgeries as shown in Table 3. From the results, it can be seen that this type of offline signature verification using an online signature database has shown excellent results; therefore, it can bridge the gap between offline and online signature verification systems, leading to an excellent cross-domain biometric verification solution. For random forgeries, testing accuracy ranges from (90%-100%) for all forty users; similarly, for skilled forgeries, testing accuracy ranges from (47.50%-100%). Average training time elapsed is observed to be 14.98 sec, with a highest of 18.92 sec and a lowest of 13.66 sec in the case of random forgery. Similarly, the average training time elapsed for skill forgery is 15.32 sec, with a highest of 22.02 sec and a lowest of 13.81 sec. The highest training accuracy for random as well as skill forgery is 100%. The lowest testing accuracy is 90 % and 47.50 % respectively, for random forgery and skill forgery. Use of a pretrained SqueezeNet Deep Learning Model for offline signature verification is seen to be an effective methodology, particularly when there is a necessity for a lightweight model that can deliver strong performance in resource-constrained environments with limited signature data. It can be seen that testing accuracy with random forgery is consistently higher than testing accuracy with skill forgery. Moreover, the training time elapsed for random forgery is lower than that of skill forgery.

Table 1. Training and verification results using random forgery (training 60% randomly and testing with all 100%)

User	Training Accuracy (%)	Using Random Forgeries			Training Elapsed Time (S)	Best Youden Threshold (User Specific)	Best EER Threshold (User Specific)	Equal Error Rate (EER) %	Area Under the Curve (AUC)
		Testing Accuracy (Raw) (%)	Testing Accuracy (Youden User Specific Thresholded) (%)	Testing Accuracy (EER User Specific Thresholded) (%)					
User1	100.00	100.00	100.00	100.00	18.92	0.9998	0.0553	0	1
User2	100.00	92.50	100.00	100.00	13.90	0.2157	0.0251	0	1
User3	100.00	100.00	100.00	100.00	13.66	0.8818	0.0050	0	1
User4	100.00	100.00	100.00	100.00	14.25	0.9592	0.3116	0	1
User5	100.00	100.00	100.00	100.00	14.19	0.5465	0.2563	0	1
User6	100.00	100.00	100.00	100.00	13.81	0.9990	0.0050	0	1

User7	95.83	92.50	92.50	90.00	13.86	0.5781	0.5628	10	0.955
User8	100.00	100.00	100.00	100.00	14.05	0.8846	0.0302	0	1
User9	100.00	100.00	100.00	100.00	14.16	0.9971	0.2513	0	1
User10	100.00	100.00	100.00	100.00	14.18	0.7439	0.0653	0	1
User11	100.00	100.00	100.00	100.00	14.24	0.8997	0.0050	0	1
User12	100.00	100.00	100.00	100.00	14.55	0.9961	0.0050	0	1
User13	100.00	100.00	100.00	100.00	14.94	0.9996	0.1759	0	1
User14	100.00	100.00	100.00	100.00	15.39	0.8215	0.0201	0	1
User15	100.00	97.50	100.00	100.00	15.41	0.8502	0.5528	0	1
User16	100.00	100.00	100.00	100.00	15.13	0.9857	0.0553	0	1
User17	100.00	100.00	100.00	100.00	15.41	0.8463	0.1206	0	1
User18	100.00	97.50	100.00	100.00	15.15	0.9904	0.6131	0	1
User19	100.00	100.00	100.00	100.00	15.21	0.7837	0.3618	0	1
User20	100.00	100.00	100.00	100.00	15.17	0.7566	0.2161	0	1
User21	100.00	100.00	100.00	100.00	14.87	0.9513	0.0151	0	1
User22	100.00	100.00	100.00	100.00	15.05	0.9993	0.0050	0	1
User23	100.00	100.00	100.00	100.00	15.10	0.9231	0.0201	0	1
User24	100.00	100.00	100.00	100.00	15.01	0.9975	0.1608	0	1
User25	100.00	100.00	100.00	100.00	14.91	0.5751	0.4422	0	1
User26	100.00	100.00	100.00	100.00	15.22	0.9334	0.1608	0	1
User27	100.00	100.00	100.00	100.00	15.53	0.8620	0.2915	0	1
User28	100.00	97.50	100.00	100.00	15.04	0.3806	0.0201	0	1
User29	100.00	95.00	100.00	100.00	15.17	0.7461	0.6382	0	1
User30	100.00	100.00	100.00	100.00	14.93	0.9924	0.0050	0	1
User31	100.00	100.00	100.00	100.00	15.44	0.9776	0.2613	0	1
User32	100.00	100.00	100.00	100.00	15.19	0.9858	0.2111	0	1
User33	100.00	100.00	100.00	100.00	15.10	0.8880	0.1256	0	1
User34	100.00	100.00	100.00	100.00	15.76	0.9667	0.0050	0	1
User35	100.00	100.00	100.00	100.00	15.30	0.9878	0.2563	0	1
User36	100.00	100.00	100.00	100.00	15.06	0.7923	0.3668	0	1
User37	100.00	97.50	100.00	100.00	14.95	0.8481	0.5176	0	1
User38	100.00	100.00	100.00	100.00	15.20	0.6589	0.1156	0	1
User39	100.00	100.00	100.00	100.00	16.02	0.9780	0.0101	0	1
User40	100.00	100.00	100.00	100.00	14.92	0.9500	0.1256	0	1
Average	99.90	99.25	99.81	99.75	14.98	0.8532	0.1862	0.25	0.999
Highest	100.00	100	100	100	18.92	0.9998	0.6382	10	1
Lowest	95.83	92.50	92.50	90.00	13.66	0.2157	0.0050	0	0.955

Table 2. Precision, Recall, and F1-Score while testing using random forgery for all 40 users at youden threshold

User	Using Random Forgeries (At Youden's Threshold)						
	TP	TN	FP	FN	Precision(%)	Recall(%)	F1-Score(%)
User1	20	20	0	0	100.00	100.00	100.00
User2	20	20	0	0	100.00	100.00	100.00
User3	20	20	0	0	100.00	100.00	100.00
User4	20	20	0	0	100.00	100.00	100.00
User5	20	20	0	0	100.00	100.00	100.00
User6	20	20	0	0	100.00	100.00	100.00
User7	18	19	1	2	94.74	90.00	92.31
User8	20	20	0	0	100.00	100.00	100.00
User9	20	20	0	0	100.00	100.00	100.00
User10	20	20	0	0	100.00	100.00	100.00

User11	20	20	0	0	100.00	100.00	100.00
User12	20	20	0	0	100.00	100.00	100.00
User13	20	20	0	0	100.00	100.00	100.00
User14	20	20	0	0	100.00	100.00	100.00
User15	20	20	0	0	100.00	100.00	100.00
User16	20	20	0	0	100.00	100.00	100.00
User17	20	20	0	0	100.00	100.00	100.00
User18	20	20	0	0	100.00	100.00	100.00
User19	20	20	0	0	100.00	100.00	100.00
User20	20	20	0	0	100.00	100.00	100.00
User21	20	20	0	0	100.00	100.00	100.00
User22	20	20	0	0	100.00	100.00	100.00
User23	20	20	0	0	100.00	100.00	100.00
User24	20	20	0	0	100.00	100.00	100.00
User25	20	20	0	0	100.00	100.00	100.00
User26	20	20	0	0	100.00	100.00	100.00
User27	20	20	0	0	100.00	100.00	100.00
User28	20	20	0	0	100.00	100.00	100.00
User29	20	20	0	0	100.00	100.00	100.00
User30	20	20	0	0	100.00	100.00	100.00
User31	20	20	0	0	100.00	100.00	100.00
User32	20	20	0	0	100.00	100.00	100.00
User33	20	20	0	0	100.00	100.00	100.00
User34	20	20	0	0	100.00	100.00	100.00
User35	20	20	0	0	100.00	100.00	100.00
User36	20	20	0	0	100.00	100.00	100.00
User37	20	20	0	0	100.00	100.00	100.00
User38	20	20	0	0	100.00	100.00	100.00
User39	20	20	0	0	100.00	100.00	100.00
User40	20	20	0	0	100.00	100.00	100.00
Average					99.87	99.75	99.81
Highest					100	100	100
Lowest					94.74	90.00	92.31

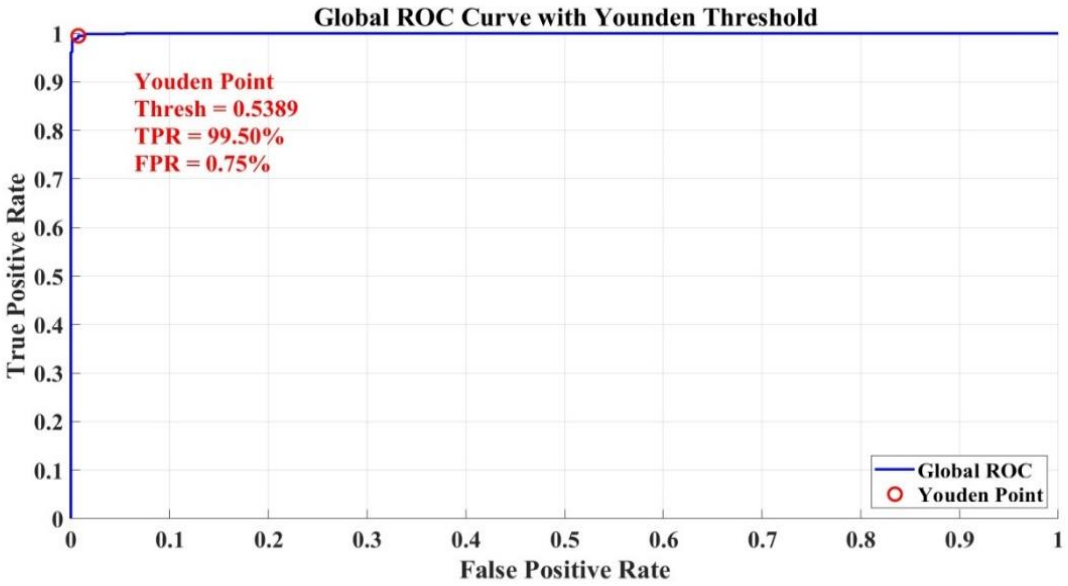

Fig. 12 Global ROC curve using random forgery with youden threshold

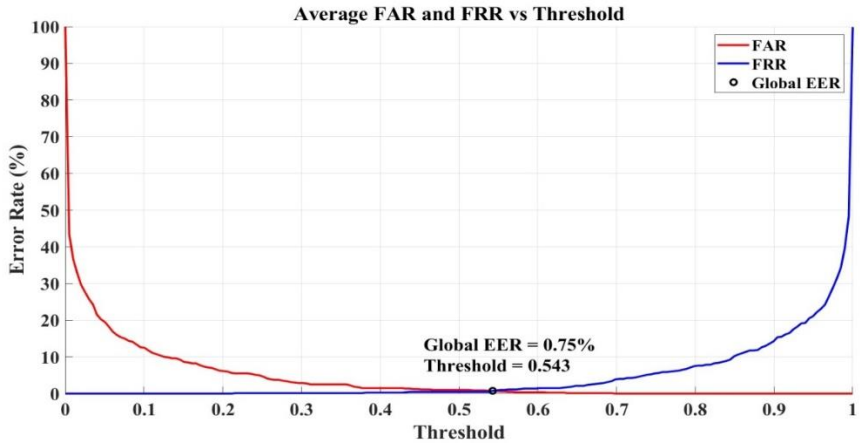

Fig. 13 Average FAR and FRR Curves vs Threshold for random forgery

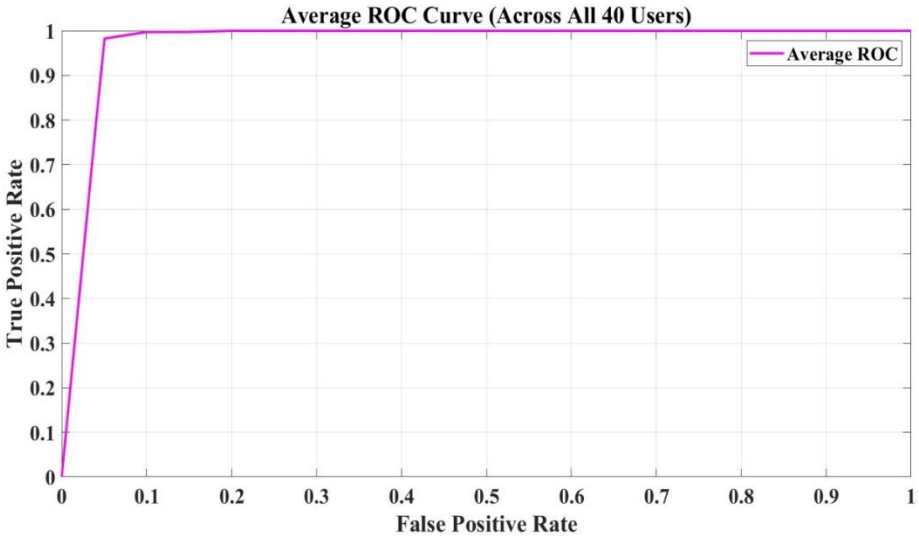

Fig. 14 Average ROC curve across all 40 users for random forgery

Table 3. Training and verification results using skilled forgery (training 60% randomly and testing with all 100%)

User	Training Accuracy (%)	Using Skilled Forgeries			Training Elapsed Time (S)	Best Youden Threshold (User Specific)	Best EER Threshold (User Specific)	Equal Error Rate (EER) %	Area Under the Curve (AUC)
		Testing Accuracy (Raw) (%)	Testing Accuracy (Youden User Specific Thresholded) (%)	Testing Accuracy (EER User Specific Thresholded) (%)					
User1	100.00	92.50	95.00	95.00	16.70	0.4744	0.5276	5.00	0.98
User2	100.00	85.00	90.00	87.50	22.02	0.4293	0.4171	12.50	0.9425
User3	100.00	95.00	95.00	95.00	17.06	0.5084	0.4975	5.00	0.965
User4	95.83	87.50	92.50	90.00	13.81	0.6897	0.6382	10.00	0.95
User5	50.00	47.50	72.50	72.50	14.17	0.4926	0.4925	27.50	0.695
User6	100.00	100.00	100.00	100.00	14.41	0.6335	0.0503	0.00	1
User7	70.83	62.50	87.50	87.50	14.43	0.4762	0.4724	12.50	0.9225
User8	95.83	92.50	95.00	95.00	14.17	0.5346	0.4925	5.00	0.9725
User9	95.83	90.00	92.50	90.00	14.69	0.4914	0.3467	10.00	0.9525
User10	100.00	87.50	92.50	90.00	14.80	0.2466	0.2513	10.00	0.9725

User11	95.83	87.50	92.50	90.00	14.81	0.5644	0.5678	10.00	0.955
User12	95.83	87.50	100.00	100.00	15.24	0.2000	0.1256	0.00	1
User13	100.00	100.00	100.00	100.00	15.09	0.9910	0.3166	0.00	1
User14	100.00	97.50	100.00	100.00	15.04	0.4960	0.4824	0.00	1
User15	95.83	90.00	95.00	90.00	15.26	0.7620	0.5427	10.00	0.9875
User16	100.00	97.50	97.50	95.00	15.30	0.5365	0.5377	5.00	0.995
User17	75.00	72.50	95.00	92.50	14.94	0.5317	0.5226	7.50	0.965
User18	100.00	100.00	100.00	100.00	15.13	0.7750	0.4724	0.00	1
User19	83.33	72.50	80.00	77.50	14.95	0.4826	0.4874	22.50	0.8625
User20	91.67	87.50	92.50	90.00	14.96	0.3975	0.2261	10.00	0.97
User21	91.67	87.50	87.50	85.00	14.96	0.5674	0.2764	15.00	0.9275
User22	100.00	95.00	97.50	95.00	15.02	0.6203	0.3618	5.00	0.9975
User23	95.83	90.00	95.00	90.00	15.11	0.5116	0.5075	10.00	0.9825
User24	100.00	92.50	97.50	95.00	14.97	0.7067	0.5126	5.00	0.995
User25	100.00	100.00	100.00	100.00	15.02	0.5740	0.4975	0.00	1
User26	91.67	85.00	90.00	87.50	15.30	0.5888	0.5377	12.50	0.9625
User27	87.50	77.50	97.50	92.50	15.26	0.6087	0.5678	7.50	0.98
User28	87.50	87.50	95.00	90.00	15.06	0.6333	0.5678	10.00	0.9825
User29	87.50	90.00	90.00	87.50	15.78	0.5266	0.5226	12.50	0.9625
User30	100.00	100.00	100.00	100.00	15.12	0.7261	0.0905	0.00	1
User31	100.00	95.00	97.50	95.00	14.99	0.8695	0.4523	5.00	0.995
User32	100.00	100.00	100.00	100.00	14.85	0.5247	0.4121	0.00	1
User33	100.00	92.50	100.00	100.00	15.14	0.9579	0.7588	0.00	1
User34	58.33	57.50	100.00	100.00	16.02	0.6741	0.6533	0.00	1
User35	100.00	97.50	100.00	100.00	14.94	0.9840	0.5528	0.00	1
User36	83.33	75.00	87.50	80.00	14.91	0.7525	0.6683	20.00	0.93
User37	95.83	95.00	100.00	100.00	14.88	0.5947	0.5276	0.00	1
User38	100.00	95.00	95.00	95.00	17.54	0.5421	0.4824	5.00	0.9775
User39	100.00	95.00	97.50	95.00	15.98	0.6831	0.4121	5.00	0.9975
User40	100.00	100.00	100.00	100.00	15.05	0.6247	0.3769	0.00	1
Average	93.13	88.50	94.81	93.13	15.32	0.5996	0.4552	6.88	0.9694
Highest	100	100	100	100	22.02	0.9910	0.7588	27.50	1
Lowest	50	47.50	72.50	72.50	13.81	0.2000	0.0503	0.00	0.695

Table 4. Precision, Recall, and F1-Score while testing using skilled forgery for all 40 users at youden threshold

User	Using Skilled Forgeries (At Youden Threshold)						
	TP	TN	FP	FN	Precision(%)	Recall(%)	F1-Score(%)
User1	20	18	2	0	90.91	100.00	95.24
User2	18	18	2	2	90.00	90.00	90.00
User3	19	19	1	1	95.00	95.00	95.00
User4	18	19	1	2	94.74	90.00	92.31
User5	18	11	9	2	66.67	90.00	76.60
User6	20	20	0	0	100.00	100.00	100.00
User7	17	18	2	3	89.47	85.00	87.18
User8	18	20	0	2	100.00	90.00	94.74
User9	17	20	0	3	100.00	85.00	91.89
User10	19	18	2	1	90.48	95.00	92.68
User11	19	18	2	1	90.48	95.00	92.68
User12	20	20	0	0	100.00	100.00	100.00
User13	20	20	0	0	100.00	100.00	100.00
User14	20	20	0	0	100.00	100.00	100.00

User15	18	20	0	2	100.00	90.00	94.74
User16	20	19	1	0	95.24	100.00	97.56
User17	18	20	0	2	100.00	90.00	94.74
User18	20	20	0	0	100.00	100.00	100.00
User19	17	15	5	3	77.27	85.00	80.95
User20	18	19	1	2	94.74	90.00	92.31
User21	15	20	0	5	100.00	75.00	85.71
User22	19	20	0	1	100.00	95.00	97.44
User23	18	20	0	2	100.00	90.00	94.74
User24	19	20	0	1	100.00	95.00	97.44
User25	20	20	0	0	100.00	100.00	100.00
User26	17	19	1	3	94.44	85.00	89.47
User27	19	20	0	1	100.00	95.00	97.44
User28	18	20	0	2	100.00	90.00	94.74
User29	18	18	2	2	90.00	90.00	90.00
User30	20	20	0	0	100.00	100.00	100.00
User31	19	20	0	1	100.00	95.00	97.44
User32	20	20	0	0	100.00	100.00	100.00
User33	20	20	0	0	100.00	100.00	100.00
User34	20	20	0	0	100.00	100.00	100.00
User35	20	20	0	0	100.00	100.00	100.00
User36	15	20	0	5	100.00	75.00	85.71
User37	20	20	0	0	100.00	100.00	100.00
User38	19	19	1	1	95.00	95.00	95.00
User39	19	20	0	1	100.00	95.00	97.44
User40	20	20	0	0	100.00	100.00	100.00
Average					96.36	93.63	94.78
Highest					100	100	100
Lowest					66.67	75	76.60

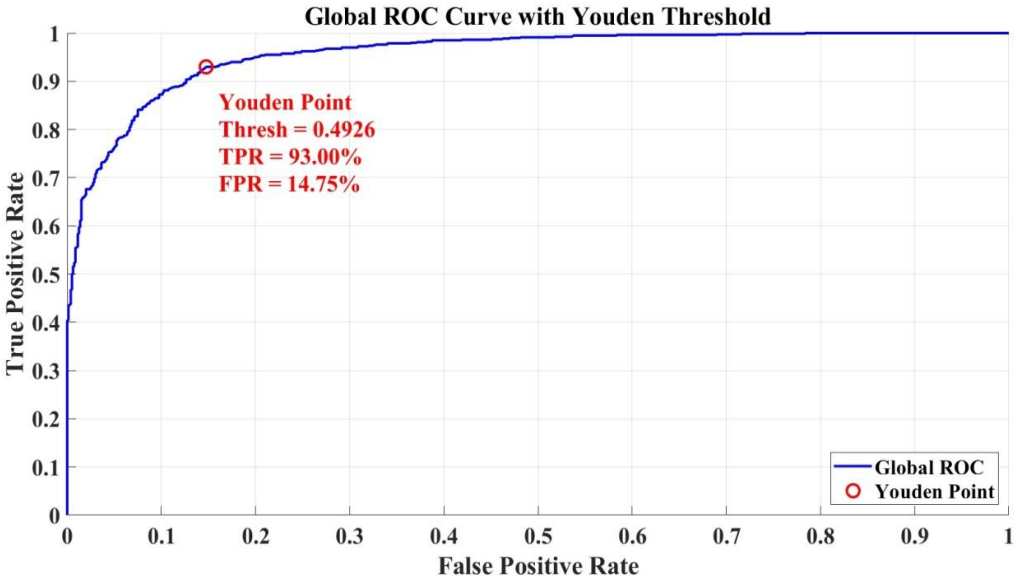

Fig. 15 Global ROC curve using skilled forgery with youden threshold

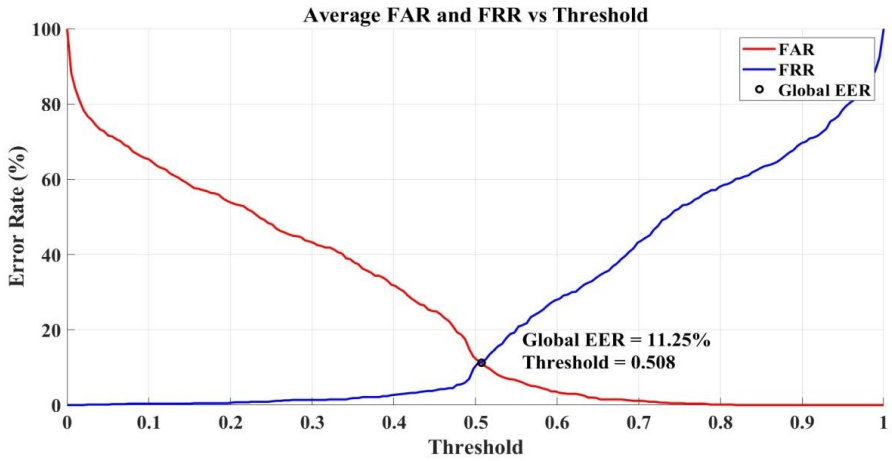

Fig. 16 Average FAR and FRR curves vs Threshold for skilled forgery

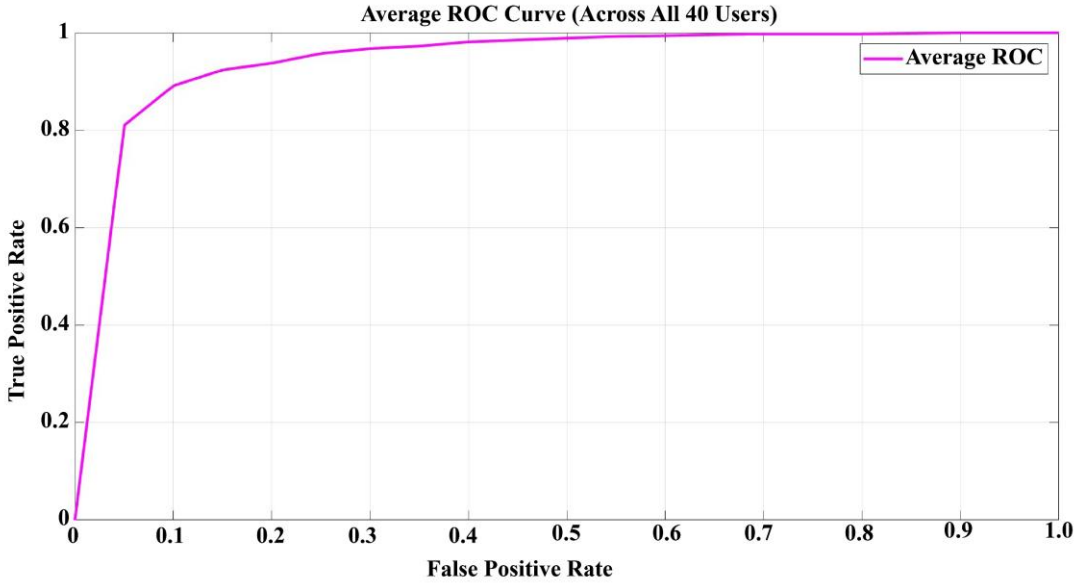

Fig. 17 Average ROC curve across all 40 users for skilled forgery

Table 5. Verification report of proposed method

Performance Parameters	Results Obtained	
	Random Forgery	Skilled Forgery
Average Testing Accuracy(Raw Thresholded)	99.25%	88.50%
Average Testing Accuracy(Youden Thresholded)	99.81%	94.81%
Average Testing Accuracy(EER Thresholded)	99.75%	93.13%
Average Precision(Youden Thresholded)	99.87%	96.36%
Average Recall(Youden Thresholded)	99.75%	93.63%
Average F1-Score(Youden Thresholded)	99.81%	94.78%
Average Best Youden Threshold	0.8532	0.5996
Average Best EER Threshold	0.1862	0.4552
Global EER	0.75%	11.25%
Threshold at Global EER	0.543	0.508
Global Youden Point Threshold	0.5389	0.4926

The performance analysis report of our proposed offline signature verification system using the SVC 2004 online signature database in terms of Testing Accuracy, Precision, Recall, and F1-Score using Random Forgery and Skilled Forgery, which performs remarkably well, is shown in Table 5 above.

5. Results and Conclusion

5.1. Results and Discussions

Our Pretrained SqueezeNet is trained and tested on the offline converted images of online signature database SVC 2004 for all forty users, yielding average testing accuracy of (99.25% for Raw Thresholding, 99.81% for Youden Thresholding and 99.75% for EER Thresholding) using Random Forgeries and (88.50% for Raw Thresholding, 94.81% for Youden Thresholding and 93.13% for EER Thresholding) using Skilled Forgeries as shown is Table 1, Table 3 and Table 5. For random forgeries, testing accuracy ranges from (90%-100%) for all forty users; similarly, for skilled forgeries, testing accuracy ranges from (47.50%-100%). Average training time elapsed is observed to be 14.98 sec, with a highest 18.92 sec and lowest 13.66 sec in case of random forgery similarly average training time elapsed for skill forgery is 15.32 sec with highest 22.02 sec and lowest 13.81 sec.

The verification report of our proposed model in terms of performance parameters is depicted clearly in Table 5. It is clear that the model's performance is best with an average testing accuracy of 99.81% for Youden thresholding (Using Random Forgery) and 94.81% for Youden thresholding (Using Skill Forgery), which indicates great overall efficiency. Average precision of 99.87% (Using Random Forgery) and 96.36% (Using Skill Forgery) shows that the model effectively reduces false positives. With an average recall of 99.75% (Using Random Forgery) and 93.63% (Using Skill Forgery), the model minimizes false negatives. Moreover, a well-balanced tradeoff between recall and precision, known as F1-Score, comes out to be 99.81% (Using Random Forgery) and 94.78% (Using Skill Forgery). All the above findings suggest the model's dependability, its high degree of accuracy, and very careful handling of false positives and false negatives.

Hence, the values of Average Testing Accuracy, Average Precision, Average Recall, Average F1-Score, etc. from Table 5 indicate that our proposed system performs remarkably well in line with the state-of-the-art results presented to date. For our proposed model, training accuracy, testing accuracy (at Raw, Best Youden User Specific Threshold, Best EER User Specific Threshold), EER, AUC, and training time for all 40 individual Users are recorded in Table 1 for random forgery and in Table 3 for skill forgery. Precision, Recall, and F1-Score while Testing Using Random Forgery for all 40 Users at Youden Threshold is shown in Table 2, and similarly while Testing using Skill Forgery is shown in Table 4. We have determined the Global ROC curve using Random Forgery with Youden Threshold as shown in Figure 12 and the Global ROC curve using Skilled Forgery with Youden Threshold as shown in Figure 15. It is the plot of False positive rate versus True positive rate which gives a global Youden point threshold of 0.5389 and 0.4926 in case of random forgery and skill forgery, respectively. Average FAR and FRR Curves vs Threshold for Random Forgery and Average FAR and FRR Curves vs Threshold for Skilled Forgery, which determine Global EER and Threshold, are shown in Figures 13 and 16, respectively.

This gives Global EER=0.75% at threshold=0.543 in case of random forgery and Global EER=11.25% at threshold=0.508 in case of skilled forgery. The average ROC Curve across all 40 Users is shown in Figures 14 and 17, respectively, for random forgery and skilled forgery. Use of a pretrained SqueezeNet Deep Learning Model for offline signature verification is seen to be an effective approach, particularly when there is a necessity for a lightweight model that can deliver a strong performance in resource-constrained environments with limited signature data.

5.2. Conclusion

With the introduction of deep learning, offline signature verification has advanced significantly. In terms of accuracy and resilience, models like CNNs, RNNs, and GANs have surpassed conventional methods. However, issues like bridging the gap between online and offline signature verification have not been addressed to date for cross-domain biometric verification solutions.

This problem is resolved here, where online collected signatures can be verified with offline collected signatures and offline signatures can be verified with online collected signatures in real-time with excellent accuracy, leading to a cross-domain biometric verification solution. By altering a pretrained SqueezeNet model for offline signature verification, we have taken advantage of deep learning's power while keeping a lightweight and efficient model appropriate for deployment on devices with limited computational resources.

Here in our proposed model, we have obtained the best average testing accuracy of 99.81% (With user-specific Youden Thresholding) using Random Forgery and 94.81% (With user-specific Youden Thresholding) using Skilled Forgery, which is excellent and is in line with the state-of-the-art results. Here, we have also calculated the Global Youden Threshold and Global EER Threshold across all forty users, but verification using them and their analysis is a promising direction for future research. We often observed that, in practical applications, offline signature verification systems encounter significant challenges due to various distortions, such as stamps, overlapping text, smudges, and background noise, factors that lie beyond the scope of the

current study. We cannot perform accurate verification and authentication of signatures in the presence of these types of interferences. Therefore, the development of robust methods for the detection, removal, or mitigation of these distortions constitutes a promising research direction for the future. Progress in this area has the potential to significantly improve the reliability and accuracy of automated offline signature verification systems.

References

[1] Moises Diaz et al., "A Perspective Analysis of Handwritten Signature Technology," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1-39, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Rajesh Kumar, J.D. Sharma, and Bhabatosh Chanda, "Writer-Independent Off-line Signature Verification using Surroundedness Feature," *Pattern Recognition Letters*, vol. 33, no. 3, pp. 301-308, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[3] Amir Soleimani, Babak N. Araabi, and Kazim Fouladi, "Deep Multitask Metric Learning for Offline Signature Verification," *Pattern Recognition Letters*, vol. 80, pp. 84-90, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[4] C.R. Divyashri, and V. Nischitha, "Beyond the Pen: Deep Learning Advances in Offline Signature-Based Writer Identification and Verification," *International Journal on Science and Technology*, vol. 16, no. 2, pp. 1-9, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Forrest N. Iandola et al., "SqueezeNet: AlexNet-level Accuracy with 50x Fewer Parameters and <0.5MB Model Size," *arXiv Preprint*, pp. 1-13, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yosepin Petra Purbanugraha, Adian Fatchur Rochim, and Iwan Setiawan, "Improvement Accuracy Identification and Learning Speed of Offline Signatures Based on SqueezeNet with ADAM Backpropagation," *2022 9th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, Semarang, Indonesia, pp. 248-253, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira, "Offline Handwritten Signature Verification — Literature Review," *2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*, Montreal, QC, Canada, pp. 1-8, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[8] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira, "Learning Features for Offline Handwritten Signature Verification using Deep Convolutional Neural Networks," *Pattern Recognition*, vol. 70, pp. 163-176, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Xianmu Cairang et al., "Learning Generalisable Representations for Offline Signature Verification," *2022 International Joint Conference on Neural Networks (IJCNN)*, Padua, Italy, pp. 1-7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yongliang Zhang et al., "Cross Layer Weakly Supervised Data Augmentation Network for Offline Signature Verification," *2024 International Joint Conference on Neural Networks (IJCNN)*, Yokohama, Japan, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Muhammad Azi Saputra, and Ida Nurhaida, "Signature Originality Verification Using A Deep Learning Approach," *Electronic Journal of Education Social Economics and Technology*, vol. 5, no. 1, pp. 19-29, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Neha Sharma, Sheifali Gupta, and Puneet Mehta, "A Comprehensive Study on Offline Signature Verification," *Journal of Physics: Conference Series: International Virtual Conference on Intelligent Robotics, Mechatronics and Automation Systems 2021*, Chennai, India, vol. 1969, pp. 1-17, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Tom Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861-874, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jack Hogan, and Niall M. Adams, "On Averaging ROC Curves," *Transactions on Machine Learning Research*, pp. 1-12, 2023. [Google Scholar] [Publisher Link]

[15] S. Rashidi, A. Fallah, and F. Towhidkhah, "Estimation of the Youden Index and its Associated Cutoff Point," *Biometrical Journal: Journal of Mathematical Methods in Biosciences*, vol. 47, no. 4, pp. 458-472, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[16] S. Rashidi, A. Fallah, and F. Towhidkhah, "Feature Extraction based DCT on Dynamic Signature Verification," *Scientia Iranica*, vol. 19, no. 6, pp. 1810-1819, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ibtisam Ghazi Nsaif et al., "A Review of Online Signature Recognition System," *Fusion: Practice and Applications*, vol. 18, no. 1, pp. 130-144, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Donato Impedovo, and Giuseppe Pirlo, "Automatic Signature Verification: The State of the Art," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 609-635, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[19] Jiaxin Lu et al., "Research on Authentic Signature Identification Method Integrating Dynamic and Static Features," *Applied Sciences*, vol. 12, no. 19, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Aman Singla, and Ajay Mittal, "Exploring Offline Signature Verification Techniques: A Survey Based on Methods and Future Directions," *Multimedia Tools and Applications*, vol. 84, pp. 2835-2875, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mustafa Berkay Yilmaz et al., "Offline Signature Verification using Classifier Combination of HOG and LBP Features," *2011 International Joint Conference on Biometrics (IJCB), Washington*, DC, USA, pp. 1-7, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[22] Srikanta Pal et al., "Performance of an Off-Line Signature Verification Method Based on Texture Features on a Large Indic-Script Signature Dataset," *2016 12th IAPR Workshop on Document Analysis Systems (DAS)*, Santorini, Greece, pp. 72-77, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[23] S. Singh, S. Chandra, and Agya Ram Verma, "Enhancing Offline Signature Verification via Transfer Learning and Deep Neural Networks," *Augmented Human Research*, vol. 9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] S.D. Bhavani, R.K. Bharathi, and R.J. Anil Kumar, "Offline Signature Verification using Pre-Trained Deep Convolutional Neural Network," *AIP Conference Proceedings: Emerging Trends in Signal Processing, Instrumentation, Power, Control, and Automation Systems*, Subang Jaya, Malaysia, vol. 2966, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Bahar Ciftçi, and Ramazan Tekin, "Deep Learning Based Offline Handwritten Signature Recognition," *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi*, vol. 13, no. 3, pp. 871-884, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] Sara Tehsin et al., "Enhancing Signature Verification Using Triplet Siamese Similarity Networks in Digital Documents," *Mathematics*, vol. 12, no. 17, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Victor K.S.L. Melo et al., "Deep Learning Approach to Generate Offline Handwritten Signatures Based on Online Samples," *IET Biometrics*, vol. 8, no. 3, pp. 215-220, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[28] Huan Li, Ping Wei, and Ping Hu, "Static-Dynamic Interaction Networks for Offline Signature Verification," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 35, no. 3, pp. 1893-1901, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Dit-Yan Yeung et al., "SVC2004: First International Signature Verification Competition," *Biometric Authentication*, pp. 16-22, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[30] Dawid Najda, and Khalid Saeed, "Impact of Augmentation Methods in Online Signature Verification," *Innovations in Systems and Software Engineering*, vol. 20, pp. 477-483, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Suvarna Joshi, and Abhay Kumar, "Feature Extraction Using DWT with Application to Offline Signature Identification," *Proceedings of the Fourth International Conference on Signal and Image Processing 2012 (ICSIP 2012)*, pp. 285-294, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[32] Saeeda Naz, Kiran Bibi, and Riaz Ahmad, "DeepSignature: Fine-Tuned Transfer Learning Based Signature Verification System," *Multimedia Tools and Applications*, vol. 81, no. 26, pp. 38113-38122, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[33] Min Hao et al., "SqueezeNet: An Improved Lightweight Neural Network for Sheep Facial Recognition," *Applied Sciences*, vol. 14, no. 4, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[34] Yash Gupta et al., "Handwritten Signature Verification Using Transfer Learning and Data Augmentation," *Proceedings of International Conference on Intelligent Cyber-Physical Systems*, Jaipur, India, pp. 233-245, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[35] Shih-Yin Ooi, Andrew Beng-Jin Teoh, and Thian-Songa Ong, "Offline Signature Verification through Biometric Strengthening," *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, Alghero, Italy, pp. 226-231, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[36] Transfer Learning and Fine-Tuning, TensorFlow. [Online]. Available: https://www.tensorflow.org/tutorials/images/transfer_learning

[37] Oona Rainio, Jarmo Teuho, and Riku Klén, "Evaluation Metrics and Statistical Tests for Machine Learning," *Scientific Reports*, vol. 14, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]