machine learning & knowledge extraction

MDPI

Article

TL-Efficient-SE: A Transfer Learning-Based Attention-Enhanced Model for Fingerprint Liveness Detection Across Multi-Sensor Spoof Attacks

Archana Pallakonda [1], Rayappa David Amar Raj [2], Rama Muni Reddy Yanamala [3], Christian Napoli [4,5] and Cristian Randieri [4,6,*]

[1] Department of Computer Science and Engineering, National Institute of Technology Warangal, Warangal 506004, India; ap23csr1r06@student.nitw.ac.in
[2] Amrita School of Artificial Intelligence, Amrita Vishwa Vidyapeetham, Coimbatore 641112, India; rd_amarraj@cb.amrita.edu
[3] Department of Electronics and Communication Engineering, Indian Institute of Information Technology Design and Manufacturing (IIITD&M) Kancheepuram, Chennai 600127, India; yanamalamunireddy@iiitdm.ac.in
[4] Department of Computer, Control, and Management Engineering "Antonio Ruberti", Sapienza University of Rome, 00185 Rome, Italy; cnapoli@diag.uniroma1.it
[5] Department of Artificial Intelligence, Czestochowa University of Technology, ul. Dqbrowskiego 69, 42-201 Czestochowa, Poland
[6] Department of Theoretical and Applied Sciences, eCampus University, Via Isimbardi 10, 22060 Novedrate, Italy
* Correspondence: cristian.randieri@uniecampus.it

Abstract

Fingerprint authentication systems encounter growing threats from presentation attacks, making strong liveness detection crucial. This work presents a deep learning-based framework integrating EfficientNetB0 with a Squeeze-and-Excitation (SE) attention approach, using transfer learning to enhance feature extraction. The LivDet 2015 dataset, composed of both real and fake fingerprints taken using four optical sensors and spoofs made using PlayDoh, Ecoflex, and Gelatine, is used to train and test the model architecture. Stratified splitting is performed once the images being input have been scaled and normalized to conform to EfficientNetB0's format. The SE module adaptively improves appropriate features to competently differentiate live from fake inputs. The classification head comprises fully connected layers, dropout, batch normalization, and a sigmoid output. Empirical results exhibit accuracy between 98.50% and 99.50%, with an AUC varying from 0.978 to 0.9995, providing high precision and recall for genuine users, and robust generalization across unseen spoof types. Compared to existing methods like Slim-ResCNN and HyiPAD, the novelty of our model lies in the Squeeze-and-Excitation mechanism, which enhances feature discrimination by adaptively recalibrating the channels of the feature maps, thereby improving the model's ability to differentiate between live and spoofed fingerprints. This model has practical implications for deployment in real-time biometric systems, including mobile authentication and secure access control, presenting an efficient solution for protecting against sophisticated spoofing methods. Future research will focus on sensor-invariant learning and adaptive thresholds to further enhance resilience against varying spoofing attacks.

Keywords: adaptive thresholds; multi-sensor; presentation attack detection; squeeze and excitation mechanism; transfer learning

check for updates

Academic Editor: Danial Javaheri

Received: 15 July 2025
Revised: 15 September 2025
Accepted: 22 September 2025
Published: 1 October 2025

Citation: Pallakonda, A.; Raj, R.D.A.; Yanamala, R.M.R.; Napoli, C.; Randieri, C. TL-Efficient-SE: A Transfer Learning-Based Attention-Enhanced Model for Fingerprint Liveness Detection Across Multi-Sensor Spoof Attacks. *Mach. Learn. Knowl. Extr.* **2025**, *7*, 113. https://doi.org/10.3390/make7040113

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Fingerprint recognition systems have evolved as a cornerstone of contemporary biometric authentication due to their uniqueness, ease of usage, and broad relevance in protected access control. Nevertheless, these systems are susceptible to presentation attacks (PAs) [1], where fake replicas such as silicone or gelatin fingerprints are utilized to mislead the sensor. To resolve this, fingerprint spoof detection or presentation attack detection (PAD) [2] has arisen as a vital area of investigation aimed at determining real (live) fingerprints from fake ones. With the growing sophistication of spoof materials (Figure 1) and the need for real-time, strong authentication, this work studies the development of fingerprint spoof detection techniques, from conventional machine learning techniques to cutting-edge deep learning and unified models, concentrating on their implementation, adaptability, and generalization to anonymous attacks [3].

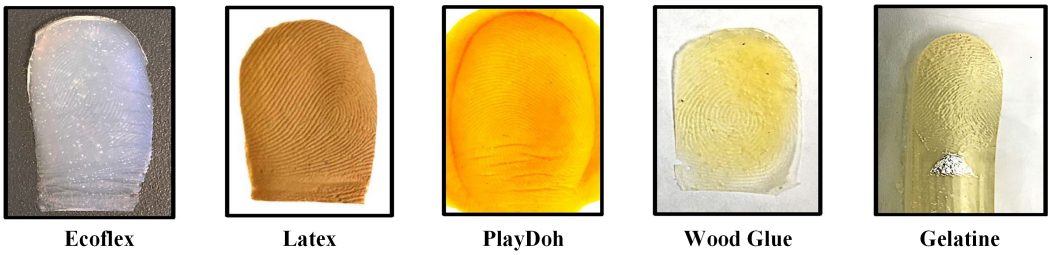


Figure 1. Spoofed fingerprints created using various materials.

Fingerprint liveness detection has undergone a considerable transition over the past decade, transitioning from handcrafted and ensemble-based approaches to unified, adaptive, and transformer-driven solutions. Initial measures primarily concentrated on using traditional machine learning methods, notably ensemble and incremental learning. Kho et al. [4] proposed an early method based on incremental learning employing support vector machine (SVM) ensembles. Their strategy presented expert classifiers incrementally trained on new spoof types utilizing the Learn++.NC algorithm, which presents scalability without needing retraining of the whole system. Building on this, Agarwal and Chowdary [5] presented adaptive ensemble techniques—A-Stacking and A-Bagging—which formed disjoint experts tailored to distinctive data subsets, enhancing robustness on imbalanced datasets. With the growing popularity of deep learning concepts, Jung et al. [6] proposed a dual-CNN architecture that combines template and probe fingerprints, thereby improving liveness detection while incurring some computational burden. Alshdadi et al. [7] later developed feature engineering by integrating Level-1 (ridge orientation) and Level-3 (ridge contours) features through a novel descriptor called Quantized Fundamental Fingerprint Features (Q-FFF), resulting in decreased error rates on LivDet datasets. Meanwhile, Sharma and Selwal [8] contributed an exhaustive review of fingerprint PAD techniques, discussing the development from classical hardware-based approaches to current deep learning-based techniques, along with datasets, protocols, and open challenges.

To additionally lower computational intricacy while preserving high accuracy, Zhang et al. [9] proposed FLDNet, a lightweight dense CNN with attention pooling. It exhibited robust performance across cross-material, intra-sensor, and cross-sensor evaluations. Nevertheless, generalization to anonymous spoof materials remained a continuous challenge. To address this, Chugh and Jain [10] presented the Universal Material Generator, a style-transfer-based approach that enhanced generalization by synthesizing new spoof deviations. Moreover, González-Soler et al. [11] concentrated on encoding both local and global features into a common space, gaining state-of-the-art performance across LivDet 2011–2019 datasets, especially in unfamiliar attack scenarios. Above traditional classifi-

cation, the domain initiated to investigate few-shot and one-shot learning paradigms to manage data scarcity. Tian et al. [12] proposed the Coupled Patch Similarity Network, which extracted fine-grained, part-level similarities employing patch-wise attention, applying the groundwork for fine-grained spoof detection with very low data. Tang et al. [13] expanded this with a bidirectional pyramidal attention mechanism for few-shot fine-grained recognition, additionally improving model sensitivity to slight divergences.

As the demand for adaptability became more critical, Agarwala et al. [14] developed AiLearn, an adaptive incremental learning model that maintained knowledge across learning phases without retraining, achieving substantial improvements in performance on evolving spoof materials. Rattani and Ross [15] presented a novel material detection module that automatically retrained the liveness detector when encountering unknown spoof images, gaining a 46% performance improvement over non-adaptive strategies. Recent research has shifted towards integrating spoof detection directly within recognition systems. A unified model proposed in [16] exhibited that spoof detection and fingerprint recognition can be simultaneously achieved without degrading performance, reducing memory and computational overhead by up to 50%. This technique was additionally examined by [17], which presented a simulation framework for examining PAD integration in verification systems under diverse operating conditions. Similarly, ref. [18] highlighted the constraints of binary evaluation parameters for PAD and proposed modified procedures that mirror the pseudo-ternary nature of spoof detection in real-world biometric systems. The most progressive evolution in this line of research is ViT Unified [19], which employs a Vision Transformer-based architecture to jointly execute fingerprint recognition and spoof detection. This unified model attains high accuracy while greatly lessening latency and parameter count, marking a milestone in the design of effective and protected biometric systems. The Squeeze-and-Excitation attention mechanism enhances computational efficiency compared to Vision Transformer models, which need high memory and computation due to self-attention across all input patches. SE operates at the channel level, recalibrating feature maps to concentrate on key channels, hence lowering computational overhead. Unlike ViT, which requires large datasets and substantial resources, SE can be combined into existing networks like EfficientNetB0, allowing faster convergence and efficient performance, making TL-Efficient-SE more appropriate for real-time fingerprint liveness detection in resource-constrained environments.

Recent examinations emphasize the effectiveness of attention mechanisms [20] in progressing fingerprint and biometric recognition. Query2Set presents a single-to-multiple partial fingerprint matching technique that adaptively combines features from distinct partial prints, surpassing traditional fusion and mosaicking techniques [21]. AFR-Net integrates vision transformers with CNN embeddings, attaining superior recognition across intra-sensor, cross-sensor, and latent-to-rolled datasets, even outperforming commercial systems [22]. For reconstruction, attention-based and multi-kernel autoencoders restore damaged or incomplete fingerprints with high accuracy (93.81%), enhancing biometric dependability in experimental settings [23]. Advancing to multimodal systems, an Attention-Based Multimodal Biometric Recognition (AMBR) framework with Federated Learning guarantees privacy-preserving training while gaining low error rates on benchmark datasets [24]. Concurrently, these works show that attention-driven models improve recognition, reconstruction, and secure multimodal authentication. Prior techniques like Slim-ResCNN [25] and HyFiPAD [26] suffer certain limitations that restrict their effectiveness in real-world applications. Slim-ResCNN struggles with cross-sensor generalizability as it is trained on a specific sensor, making it not adaptable to data from other sensors, which restricts its deployment in various environments. Furthermore, HyFiPAD depends on local binary features that are manually crafted, potentially restricting its capability to

efficiently capture complex fingerprint textures and adjust to new spoof materials, thereby decreasing its generalization across evolving spoofing methods. These restrictions are overcome by the TL-Efficient-SE framework, which uses EfficientNetB0 for robust feature extraction and combines the Squeeze-and-Excitation mechanism to enhance adaptability and generalization across various spoof materials and sensors. The comparison of the propsoed TL-Efficient-SE with the notable existing works is given in Table 1. Some studies highlight the effectiveness of Vision Transformers in fingerprint recognition, such as [27], which achieves high accuracy in contactless fingerprint classification. The work in [28] introduces the Finger Recovery Transformer (FingerRT) for recovering incomplete fingerprints, improving recognition accuracy. The authors in [29] focuses on adversarial attacks in multimodal biometric systems, showing input fusion offers better security. The authors in [30] reviews unimodal and multimodal fingerprint systems, emphasizing fusion and template protection. Previous studies predominantly utilized conventional machine learning techniques; however, contemporary approaches have transitioned to deep learning and attention mechanisms. This development highlights the increasing necessity for adaptive models that can manage various spoofing materials and sensor discrepancies. Conversely, our suggested TL-Efficient-SE framework amalgamates transfer learning with the Squeeze-and-Excitation attention mechanism, providing superior feature extraction and cross-sensor generalization, distinguishing it from conventional techniques. This work proposes a deep learning framework integrating EfficientNetB0 with a Squeeze-and-Excitation (SE) attention mechanism to improve fingerprint liveness detection by enhancing feature extraction and focusing on key fingerprint areas. The major contributions of the proposed work are as follows.

Table 1. Comparison of TL-Efficient-SE with referenced methods.

Method	Accuracy (%)	Computational Complexity	Cross-Sensor Performance
Incremental SVM Ensembles [4]	85.00%	High (Ensemble of SVMs)	Low (Sensor-specific training)
A-Stacking and A-Bagging [5]	90.00%	Moderate (Ensemble Learning)	Moderate (Expert classifiers tailored to subsets)
Dual-CNN Architecture [6]	92.00%	High (Dual-CNN network)	Moderate (Requires paired data)
Q-FFF [7]	93.50%	Moderate (Feature engineering + CNN)	High (Improved feature extraction with Q-FFF)
FLDNet [9]	95.00%	Moderate (Dense CNN)	Moderate (Performance varies across spoof types)
Universal Material Generator [10]	94.50%	High (Style transfer-based method)	High (Synthesizes new spoof types for generalization)
Feature Encoding [11]	96.00%	Moderate (Feature encoding and CNN)	High (State-of-the-art across multiple datasets)
Coupled Patch Similarity Network [12]	95.50%	High (Patch-based attention mechanism)	Moderate (Low data handling but good for fine-grained spoofing)
A-iLearn [14]	97.00%	Moderate (Incremental learning)	Moderate (Maintains knowledge over learning phases)
Material Detection Module [15]	96.50%	Moderate (Adaptive retraining)	Moderate (Retrains detector for unknown spoof types)
TL-Efficient-SE (Proposed)	**98.50–99.50%**	**Low (EfficientNetB0 + SE + Transfer Learning)**	**High (Adaptable across sensors and spoof materials)**

- The work proposes a strong deep learning framework integrating EfficientNetB0 and a Squeeze-and-Excitation (SE) attention mechanism to improve feature extraction, enhancing the capability to discriminate live and spoofed fingerprints. The attention

mechanism effectively highlights significant fingerprint areas, thereby augmenting classification accuracy.

- By using transfer learning with a pre-trained EfficientNetB0 model, the proposed approach facilitates convergence and effectively extracts features from limited training data, providing high performance without needing vast retraining.
- The proposed model is tested on the LivDet 2015 dataset across distinct sensors like Green Bit, CrossMatch, and HiScan, consistently delivering high accuracy and adaptability making the model feasible for real-world applications where sensor diversity is common.
- Gaining greater than 98.50% accuracy, high AUC, and perfect recall, the model provides accurate liveness detection with fewer false positives or negatives, essential for preserving secure and seamless user experiences in biometric systems.
- The SE attention mechanism enhances feature discrimination by concentrating on essential fingerprint details and lessening the influence of insignificant relevant features, thereby greatly enhancing the model's robustness against spoof attacks.

2. Datasets Description

The LivDet 2015 dataset [31] is an extensively utilized benchmark for assessing fingerprint liveness detection algorithms and biometric security systems. It comprises live and spoof fingerprint images captured utilizing four different optical fingerprint scanners: Green Bit, Biometrika, Persona, Digital, and Crossmatch. The dataset is split into two primary parts: *Algorithm Testing*, which evaluates the performance of software-based liveness detection models, and *System Testing*, which assesses whole hardware-integrated fingerprint recognition systems. The individual dataset comprises over 4000 images featuring spoof fingerprints constructed from diverse materials, including Ecoflex, Latex, Play-Doh, Gelatine, and Wood Glue (Figure 2). Moreover, unknown spoof materials were contained in the test set to estimate the generalization capability of detection models. Live fingerprint images were received from multiple subjects under differing conditions, including normal, wet, dry, high-pressure, and low-pressure environments.

The dataset is created to deliver natural fingerprint spoofing conditions, providing a strong evaluation of anti-spoofing methods. The performance assessment is based on key parameters, including correct classification rates for live and spoof fingerprints ($F_{corrlive}$ and $F_{corrfake}$), false classification rates ($F_{errlive}$ and $F_{errfake}$), and failure-to-enroll rates (F_{rej}). The classification threshold for distinguishing between live and spoof fingerprints was fixed at 50 out of 100. The fixed classification criterion of 55/100 was selected for uniformity; however, it may not be ideal in every instance. Future study will investigate adaptive thresholding, which dynamically adjusts according to prediction scores or sensor attributes, to enhance performance and resilience in practical applications. The System Testing dataset contains fingerprint images from 51 human subjects and spoof attempts employing five distinct spoof materials. The LivDet 2015 competition results exhibit considerable advancement in biometric security, emphasizing the resilience and drawbacks of diverse liveness detection techniques. Table 2 outlines the fundamental features of the dataset.

The LivDet 2015 dataset is highly suitable for assessing multi-sensor spoof detection due to its inclusion of fingerprint images from diverse optical sensors, such as Green Bit, CrossMatch, and HiScan, under various conditions. It includes both live and spoofed fingerprints, with the spoof images constructed employing materials like Play-Doh, Ecoflex, and gelatin, symbolizing various spoofing strategies. This diversity makes the dataset a perfect standard for evaluating a model's capability to generalize across numerous

sensors and spoof materials, which is critical for real-world applications in multi-sensor biometric systems.

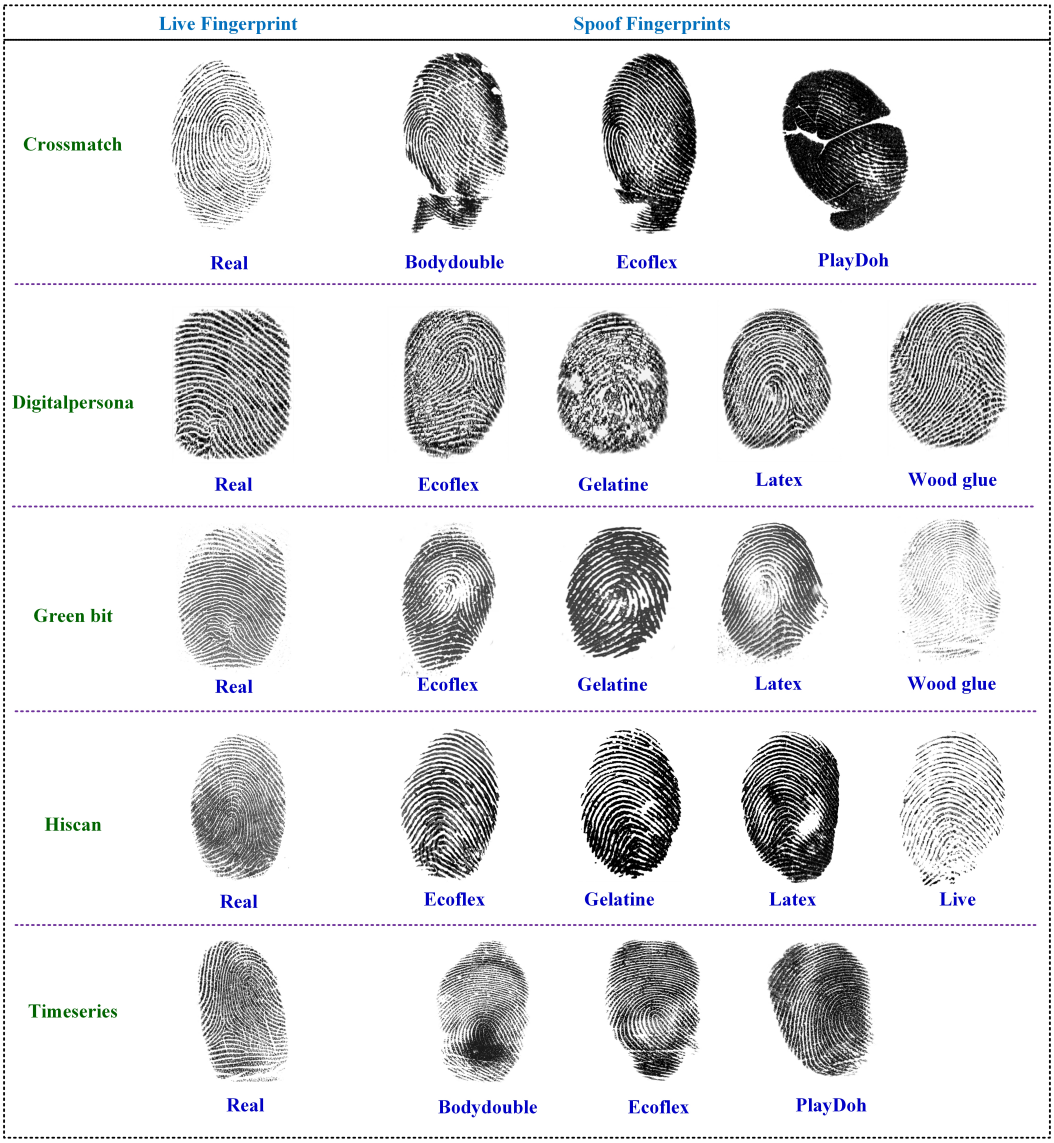


Figure 2. Fingerprint spoofs fabricated using different materials.

Table 2. Characteristics of optical fingerprint sensors.

Sensor Type	Resolution (dpi)	Image Size (px)	Format
Green Bit DactyScan26	500	500 × 500	PNG
Biometrika HiScan-PRO	1000	1000 × 1000	BMP
Digital Persona U.are.U 5160	500	252 × 324	PNG
Crossmatch L Scan Guardian	500	640 × 480	BMP

3. Proposed EfficientNetB0 with Attention Mechanism

The proposed framework (Figure 3) involves data preprocessing (resizing images to 224 × 224, normalization, with 80:20, 70:15:15, 70:20:10 splits). Feature extraction employs EfficientNetB0 with frozen layers and global average pooling. The Squeeze-and-Excitation mechanism applies channel attention through two fully connected layers. Fully connected layers with batch normalization and dropout are followed by a sigmoid output layer for bi-

nary classification. The model is trained with the Adam optimizer and binary cross-entropy loss, evaluated employing metrics like accuracy, AUC, precision, recall, and F1-score.

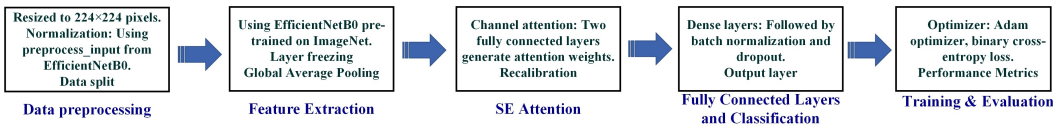


Figure 3. Pipeline of proposed workflow.

3.1. Data Preprocessing and Augmentation

The fingerprint dataset employed in this analysis is sourced from the LivDet 2015 competition, especially the CrossMatch sensor, which includes both live and spoofed fingerprint images manufactured employing diverse materials, including Ecoflex, Body Double, and Playdoh.

Individually, the fingerprint image is first loaded and resized to a specified resolution of 224 × 224 pixels to correspond to the input size of EfficientNetB0. Mathematically, considering an input fingerprint image be defined as follows:

$$I \in \mathbb{R}^{H \times W \times C} \tag{1}$$

where $H = 224$, $W = 224$, and $C = 3$ (RGB channels). The selection to resize fingerprint images to 224 × 224 pixels is predicated on compatibility with pre-trained models such as EfficientNetB0, which was trained on the ImageNet dataset utilizing this particular input dimension. Resizing optimizes feature extraction while reducing computational complexity and memory consumption. High-resolution sensors, such as the Biometrika HiScan-PRO (1000 dpi), record intricate fingerprints, but scaling to 224 × 224 pixels enables the model to concentrate on essential features like ridges and minutiae. While certain intricate details may be diminished during resizing, the Squeeze-and-Excitation (SE) attention mechanism within the TL-Efficient-SE framework mitigates this by augmenting the model's capacity to concentrate on essential features, thereby ensuring resilient performance even with resized images from high-resolution sensors. All the images are then normalized, employing EfficientNetB0's preprocessing function:

$$I' = \frac{I - \mu}{\sigma} \tag{2}$$

where μ and σ are mean and standard deviation values from the ImageNet dataset.

To guarantee a balanced dataset, stratified splitting is used:

$$\text{Train:Test} = 80\% : 20\% \tag{3}$$

where class distribution remains uniform across both training and testing datasets.

Equations (1), (2), and (3) describe the input formatting, normalization, and dataset splitting strategy, respectively.

3.2. Pre-Trained Model for Feature Extraction

The architecture is based on EfficientNetB0, a highly optimized convolutional neural network for image feature extraction as shown in Figure 4. The base feature extractor is set with pre-trained ImageNet weights:

$$F = f_\theta(I') \tag{4}$$

where f_θ denotes the convolutional layers of EfficientNetB0, and $F \in \mathbb{R}^{7 \times 7 \times D}$ is the extracted feature map with depth D.

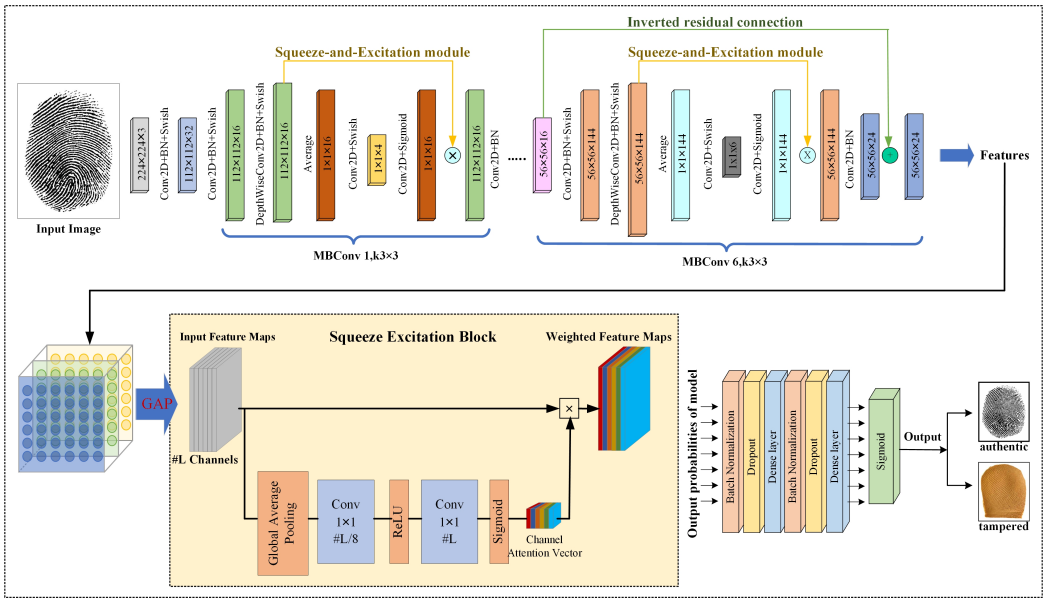


Figure 4. Overview of the proposed methodology.

To improve the discriminative ability of the architecture model, we combine an attention mechanism utilizing Squeeze-and-Excitation blocks. The attention mechanism refines the feature representation by computing channel-wise importance scores as follows:

$$z_c = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} F_{i,j,c} \tag{5}$$

where z_c denotes the global average-pooled feature for channel c.

This vector is then passed through a fully connected bottleneck transformation:

$$s = \sigma(W_2 \cdot \mathrm{ReLU}(W_1 \cdot z)) \tag{6}$$

where $W_1 \in \mathbb{R}^{\frac{D}{r} \times D}$ and $W_2 \in \mathbb{R}^{D \times \frac{D}{r}}$ are learnable weights, r is the reduction ratio (set to 2 in our case), and $\sigma(x) = \frac{1}{1+e^{-x}}$ is the sigmoid activation function.

Finally, the re-weighted feature maps are obtained by element-wise multiplication:

$$F' = s \cdot F \tag{7}$$

where F' represents the enhanced feature representation with improved discriminatory power. The pseudocode of Deep Feature Extraction (EffB0-Feature) is given in Algorithm 1.

Algorithm 1 Deep Feature Extraction (EffB0-Feature)

Require: Raw fingerprint image set $X = \{x_1, x_2, \ldots, x_N\}$
Ensure: Feature map set $F = \{f_1, f_2, \ldots, f_N\}$
Define backbone model: EffNetB0 pre-trained on ImageNet
Initialize the full model: model ← EffNetB0 backbone
Remove top (dense) layers from the model
Freeze all convolutional layers in the model to preserve pre-trained weights
for each image $x_i \in X$ **do**
    Resize x_i to $224 \times 224 \times 3$
    Apply normalization using `preprocess_input`
    Extract feature map: $f_i \leftarrow \mathrm{EfficientNetB0}(x_i) \in \mathbb{R}^{7 \times 7 \times 1280}$
    Append f_i to feature map set F
end for
    return $F = \{f_1, f_2, \ldots, f_N\}$

3.3. Squeeze-and-Excitation (SE) Block–Attention Mechanism

A Squeeze-and-Excitation (SE) block is incorporated into the architecture to augment the discriminative capacity of the derived features. This block executes adaptive recalibration of channel-specific feature responses by explicitly modelling inter-channel interdependencies. The objective is to highlight informative features and diminish less important ones.

TheSE block improves feature discrimination by adaptively recalibrating channel-wise feature responses. The process is as follows.

3.3.1. Squeeze Operation (Global Average Pooling)

Global average pooling is employed to the feature map F to yield a channel descriptor z_c for each channel c:

$$z_c = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} F_{i,j,c} \tag{8}$$

where H and W denote feature map spatial dimensions, and $F_{i,j,c}$ denotes the feature map values.

3.3.2. Excitation Phase (Fully Connected Layers)

The channel descriptor z_c is passed through two pointwise convolutions (fully connected layers):

$$s_1 = \delta(W_1 \cdot z + b_1) \tag{9}$$

where W_1 denotes the learnable weight matrix, δ denotes the ReLU activation function, and b_1 is the bias term.

The second convolution regains dimensionality and applies a sigmoid activation function to produce attention weights:

$$s = \sigma(W_2 \cdot s_1 + b_2) \tag{10}$$

where W_2 is another learnable weight matrix, σ is the sigmoid activation function, and b_2 is the bias term.

In the proposed TL-Efficient-SE framework, the SE block enahnces the model's capability to focus on essential fingerprint features like ridges and minutiae, improving both accuracy and robustness, especially in handling diverse spoof materials and sensor types.

3.3.3. Recalibration (Element-Wise Multiplication)

The attention weights s are implemented to the original feature map F through element-wise multiplication to recalibrate the features:

$$F' = s \cdot F \tag{11}$$

where F' represents the recalibrated feature map with improved discriminatory power.

This mechanism helps the model focus on important features while suppressing less relevant ones, thereby improving feature representation and classification accuracy.

Consider the feature map output from EfficientNetB0 as a 3D tensor specified as follows:

$$\mathbf{U} \in \mathbb{R}^{H \times W \times C}, \quad \text{where } H = 7,\ W = 7,\ C = 1280 \tag{12}$$

The squeeze operation employs global average pooling to reduce spatial dimensions and generate a channel descriptor:

$$z_c = \frac{1}{H \cdot W} \sum_{i=1}^{H} \sum_{j=1}^{W} U_{i,j,c}, \quad \text{for } c = 1, 2, \ldots, C \tag{13}$$

$$\mathbf{z} \in \mathbb{R}^C = \mathbb{R}^{1280} \tag{14}$$

The excitation phase employs two fully connected layers to describe channel-wise relationships. The initial layer lowers dimensionality and applies a ReLU activation:

$$\mathbf{s}_1 = \delta(\mathbf{W}_1 \mathbf{z} + \mathbf{b}_1), \quad \mathbf{W}_1 \in \mathbb{R}^{\frac{C}{r} \times C}, \ \mathbf{s}_1 \in \mathbb{R}^{640} \tag{15}$$

The second layer regains dimensionality and applies a sigmoid activation function to produce attention weights:

$$\mathbf{s} = \sigma(\mathbf{W}_2 \mathbf{s}_1 + \mathbf{b}_2), \quad \mathbf{W}_2 \in \mathbb{R}^{C \times \frac{C}{r}}, \ \mathbf{s} \in \mathbb{R}^C \tag{16}$$

The weights are subsequently employed to rescale the original feature map by channel-wise multiplication:

$$\tilde{U}_{i,j,c} = s_c \cdot U_{i,j,c}, \quad \text{for all } i, j, c \tag{17}$$

$$\tilde{\mathbf{U}} = \mathbf{U} \odot \mathbf{s} \in \mathbb{R}^{H \times W \times C} \tag{18}$$

where $\odot$ represents element-wise multiplication implemented across the channels of the feature map. The detailed pseudocode of EfficientNetB0 with Squeeze-and-Excitation Attention (EffB0-SE) is given in Algorithm 2.

Algorithm 2 EfficientNetB0 with Squeeze-and-Excitation Attention (EffB0-SE)

Require: Fingerprint images X, binary labels C
Ensure: Trained classifier M
Define backbone model: EffNetB0 pre-trained on ImageNet with no top layers
Initialize the full model: model $\leftarrow$ EffNetB0 backbone
Freeze all convolutional layers in EfficientNetB0
for each image $x \in X$ **do**
    Resize x to 224×224, apply `preprocess_input`
    Extract features using EfficientNetB0 backbone: $f \in \mathbb{R}^{1280}$
    Apply Global Average Pooling: $z \leftarrow \text{GAP}(f)$
    Apply Squeeze-and-Excitation block:
        $z_s \leftarrow \text{Dense}(640, \text{ReLU})(z)$
        $z_e \leftarrow \text{Dense}(1280, \text{Sigmoid})(z_s)$
        $z_{\text{att}} \leftarrow z \times z_e$ ▷ Attention-weighted feature
end for
Define classification head:
    $h_1 \leftarrow \text{Dense}(256, \text{ReLU}) \rightarrow \text{BatchNorm} \rightarrow \text{Dropout}(0.4)$
    $h_2 \leftarrow \text{Dense}(128, \text{ReLU}) \rightarrow \text{BatchNorm} \rightarrow \text{Dropout}(0.4)$
    Output layer: $y \leftarrow \text{Dense}(1, \text{Sigmoid})(h_2)$
Compile model M with Binary Cross-Entropy loss and Adam optimizer
Train model on (X, C) with 80:20 split for N epochs
Evaluate using Accuracy, Precision, Recall, F1-score, and ROC AUC **return** Hypothesis: $\hat{y}(x) = \arg\max_{y \in \{0,1\}} \text{sigmoid}(M(x))$

3.4. Fully Connected Layers and Classification

Subsequent to attention-based recalibration, the enhanced feature map is subjected to global average pooling to diminish its spatial dimensions:

$$\mathbf{x} = \frac{1}{H \cdot W} \sum_{i=1}^{H} \sum_{j=1}^{W} \tilde{U}_{i,j} \tag{19}$$

This feature vector $\mathbf{x}$ is passed through a series of fully connected layers. The first layer implements a ReLU activation:

$$\mathbf{h}_1 = \text{ReLU}(\mathbf{W}_1 \mathbf{x} + \mathbf{b}_1) \tag{20}$$

This is succeeded by another ReLU-activated dense layer:

$$\mathbf{h}_2 = \text{ReLU}(\mathbf{W}_2 \mathbf{h}_1 + \mathbf{b}_2) \tag{21}$$

To enhance generalization and avoid overfitting, batch normalization and dropout (with a rate of 0.4) are employed:

$$\mathbf{h}_3 = \text{BatchNorm}(\mathbf{h}_2) \tag{22}$$

$$\mathbf{h}_4 = \text{Dropout}(\mathbf{h}_3,\ p = 0.4) \tag{23}$$

The final classification is performed employing a single sigmoid neuron:

$$\hat{y} = \sigma(\mathbf{W}_{\text{out}} \mathbf{h}_4 + b_{\text{out}}) \tag{24}$$

where $\hat{y} \in [0, 1]$ is the predicted probability of the fingerprint being spoofed. The detailed model architecture summary is given in Table 3, and the training configuration summary is given in Table 4.

Table 3. Model architecture summary.

Layer (Type)	Output Shape	Param #	Connected to
input_layer_1 (InputLayer)	(None, 224, 224, 3)	0	-
efficientnetb0 (Functional)	(None, 7, 7, 1280)	4,049,571	input_layer_1[0][0]
global_average_pooling2d (GlobalAvgPool2D)	(None, 1280)	0	efficientnetb0[0][0]
dense (Dense)	(None, 640)	819,840	global_average_pooling2d[0][0]
dense_1 (Dense)	(None, 1280)	820,480	dense[0][0]
multiply (Multiply)	(None, 1280)	0	global_average_pooling2d[0][0], dense_1[0][0]
dense_2 (Dense)	(None, 256)	327,936	multiply[0][0]
batch_normalization (BatchNorm)	(None, 256)	1024	dense_2[0][0]
dropout (Dropout)	(None, 256)	0	batch_normalization[0][0]
dense_3 (Dense)	(None, 128)	32,896	dropout[0][0]
batch_normalization_1 (BatchNorm)	(None, 128)	512	dense_3[0][0]
dropout_1 (Dropout)	(None, 128)	0	batch_normalization_1[0][0]
dense_4 (Dense)	(None, 1)	129	dropout_1[0][0]
Total params: 6,052,388 (23.09 MB) **Trainable params:** 2,002,049 (7.64 MB) **Non-trainable params:** 4,050,339 (15.45 MB)			

Table 4. Training configuration summary.

Component	Configuration (as per Code)
Framework	TensorFlow 2.x (with Keras API)
Model Backbone	EfficientNetB0 (pretrained on ImageNet, include_top=False)
Attention Mechanism	Squeeze-and-Excitation (SE) applied after GlobalAveragePooling2D
Input Image Size	224 × 224 × 3
Data Preprocessing	`efficientnet.preprocess_input` applied to all input images
Train/Test Split	80% training, 20% testing (stratified split)
Batch Size	32
Epochs	30
Optimizer	Adam (`learning_rate = 0.0001`)
Loss Function	Binary Crossentropy
Metrics Monitored	Accuracy (training and validation)
Regularization	Batch Normalization + Dropout (`rate = 0.4`)

3.5. Loss Function and Optimization

The model is trained by Binary Cross-Entropy loss defined as follows:

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}(y_i \log \hat{y}_i + (1 - y_i)\log(1 - \hat{y}_i)) \tag{25}$$

where y_i is the ground truth label, $\hat{y}_i$ is the predicted probability, and N is the number of samples.

The Adam optimizer is used for optimization, which adapts learning rates for diverse parameters dynamically. The learning rate is set to the following:

$$\alpha = 10^{-4} \tag{26}$$

Figure 4 presents an overview of the proposed fingerprint liveness detection methodology, integrating an EfficientNet-inspired structure with Squeeze-and-Excitation (SE) modules and Mobile Inverted Bottleneck Convolution (MBConv) blocks for effective and discriminative feature extraction. The pipeline initiates with a fingerprint image of size $224 \times 224 \times 3$, which passes through preliminary convolutional layers that integrate batch normalization and Swish activation to augment feature expressiveness.

The image subsequently spans a series of MBConv blocks, each containing depthwise separable convolutions to reduce computational complicatedness, along with a Squeeze-and-Excitation block that captures inter-channel reliances. The SE block uses Global Average Pooling to lower spatial dimensions, followed by two pointwise convolutions activated by ReLU and sigmoid functions to generate channel attention weights. These weights are later used to the feature maps utilizing channel-wise multiplication, thereby intensifying principal features and attenuating noise.

The second MBConv block features an inverted residual connection, facilitating gradient flow and enabling feature reuse. The collected and weighted feature maps are subsequently refined and processed through a deep classification network comprising fully connected layers, batch normalization, and dropout regularization. The ultimate sigmoid-activated output categorizes the fingerprint as either genuine (live) or manipulated (spoof), showcasing a resilient end-to-end solution for fingerprint spoof detection.

The proposed TL-Efficient-SE framework diverges from conventional CNN designs by incorporating EfficientNetB0 alongside a Squeeze-and-Excitation attention mechanism. In contrast to conventional CNNs that depend exclusively on convolutional layers, the SE mechanism adaptively recalibrates channel-wise feature responses, enabling the model

to concentrate on more salient information. This modification augments discriminative capability, enhances generalization across various sensors and spoof materials, and bolsters robustness, rendering the model more adept for practical fingerprint liveness detection applications.

4. Results and Discussion

This section gives an in-depth investigation of the fingerprint liveness detection results acquired utilizing the EfficientNetB0-based deep learning model with an attention mechanism on the LivDet 2015 dataset. The assessment was performed on diverse fingerprint sensors, including Time Series, Cross Match, Green Bit, HiScan, and Digital Persona for various data splits such as 80:20, 70:15:15, 70:20:10 (train–validation–test). The performance of the architecture is evaluated utilizing fundamental classification metrics, namely, accuracy, F1-score, AUC-ROC score, precision, and recall. The obtained results exhibit the robustness of the proposed technique in effectively differentiating live and faked fingerprint images across diverse sensor types.

4.1. Performance Evaluation Across Sensors

The model's performance differs negligibly across diverse sensors due to divergences in fingerprint acquisition approaches, image resolution, spoofing material varieties, and sensor noise. Nevertheless, the proposed model invariably gains high accuracy, AUC, F1-score, precision, and recall across all the considered datasets, exhibiting its generalizability and effectiveness in real-world scenarios. As noted in the Table 5, the proposed model achieves near-perfect AUC-ROC scores across all fingerprint sensors, indicating outstanding discrimination between live and faked fingerprints. The confusion matrixes obtained for all the sensor types Figure 5. The training and validation accuracy and loss, ROC curves (shown in Figure 6), high precision, F1-score, and recall values additionally validate the model's effectiveness.

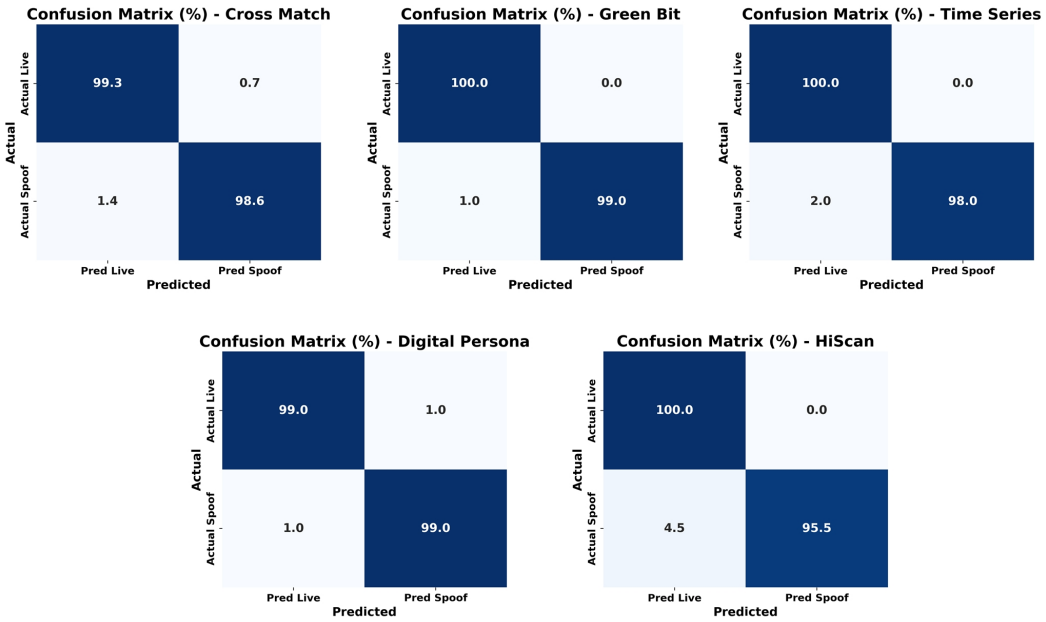


Figure 5. Confusion matrixes obtained for all the sensor types.

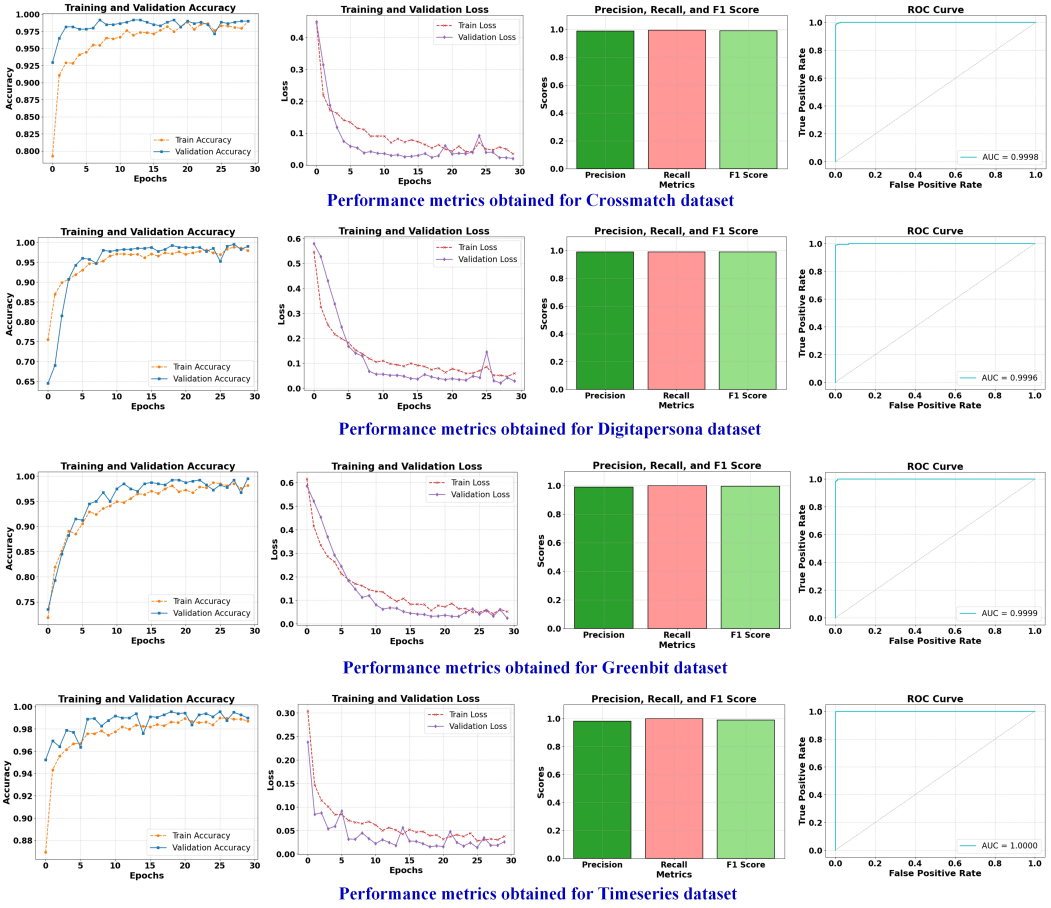


Figure 6. Performance metrics obtained by proposed model for various datatsets.

Table 5. Performance metrics obtained by proposed model for 80:20 data split.

Sensor Type	Accuracy (%)	AUC	F1-Score	Precision	Recall
Time Series	98.99	1.0000	0.9901	0.9804	1.0000
Green Bit	99.50	0.9999	0.9950	0.9901	1.0000
Cross Match	98.99	0.9998	0.9899	0.9865	0.9932
Digital Persona	99.00	0.9996	0.9900	0.9900	0.9900
HiScan	97.75	0.9986	0.9780	0.9569	1.0000

4.2. Sensor-Wise Performance Analysis

4.2.1. Analysis on Time Series Sensor

The proposed model architecture, when tested with time series sensor data, achieves 99.89% accuracy with a perfect AUC-ROC score of 1.0000, exhibiting the model's capability to distinguish between live and fake fingerprints perfectly. The F1-score of 0.9901 and recall of 1.0000 indicate that the model accurately categorizes all live fingerprints, resulting in no false negatives. Nevertheless, the precision value of 0.9804 exhibits a negligible misclassification of fake fingerprints as live due to overlapping texture similitudes between particular spoof materials and real fingerprints.

4.2.2. Analysis on Green Bit Sensor

On the Green Bit sensor dataset, the model attains the highest accuracy (99.50%) among all sensor types, with an AUC of 0.9999. The F1-score of 0.99 and recall value of 1.00 exhibit no false negatives, signifying all live fingerprints are precisely categorized. The precision of 0.99 demonstrates the model's capability to classify most fake fingerprints accurately. The remarkable performance on Green Bit indicates that the image quality

and texture differentiation are well-captured by the EfficientNetB0 feature extraction and attention mechanism.

4.2.3. Analysis on Cross Match Sensor

The Cross Match sensor yields a high accuracy of 98.99% and an AUC of 0.99. The F1-score of 0.9899 and precision value of 0.9865 exhibit that while the model functions competently, it encounters slight confusion in categorizing fake fingerprints, as contemplated by the precision being slightly lesser than the recall value of 0.9932. This disparity may be attributed to spoof materials in the dataset that simulate real fingerprints more efficiently, making categorization more challenging.

4.2.4. Analysis on Digital Persona Sensor

The Digital Persona sensor exhibits high invariant performance, attaining accuracy and AUC of 99.00% and 0.9996, respectively, and equal precision and recall values of 0.99. This proportion indicates a consistent classification of both live and faked fingerprints. The slightly lesser value of AUC corresponding to other sensors could be due to variability in sensor-specific distortions and fingerprint ridges, yet the overall performance stays highly resilient.

4.2.5. Analysis on HiScan Sensor

The HiScan sensor demonstrates the lowest accuracy, at approximately 97.75%, and an AUC of 0.99 among all tested sensors. While the recall remains at 1.00, the precision declines to 0.9569, exhibiting a higher false positive rate (live fingerprints misclassified as fake), suggesting that HiScan fingerprints have lower quality, more noise, or divergences in ridge patterns, making feature extraction and categorization narrowly less effective.

4.2.6. Dataset Split Strategy and Validation Approach

We conducted tests with various train–validation–test splits to assess the model's robustness and generalization capabilities. Table 6 presents the results of the 70:15:15 train–validation–test split, illustrating performance across multiple fingerprint sensors, including Time Series, Green Bit, Cross Match, Digital Persona, and HiScan. The metrics, including accuracy, AUC, F1-score, precision, and recall, indicate the model's robust performance on various sensors. Additionally, to verify the consistency of the results, we conducted trials utilizing a 70:20:10 train–validation–test split, as noted in Table 7. This table contrasts the model's performance on the 2011 and 2013 LivDet datasets, encompassing Biometrica, Digital, and CrossMatch sensors. The 70:20:10 division was employed to assess the model's performance with varied data partitions, hence reinforcing the robustness of the TL-Efficient-SE architecture across diverse datasets and sensors.

Table 6. Model performance on different sensors with 70:15:15 train–validation–test split.

Sensor	Accuracy	AUC	F1-Score	Precision	Recall
Time Series	0.9940	0.9999	0.9941	0.9926	0.9956
Green Bit	0.9900	0.9993	0.9900	0.9868	0.9933
Cross Match	0.9867	0.9987	0.9866	0.9932	0.9800
Digital Persona	0.9700	0.9968	0.9705	0.9548	0.9867
HiScan	0.9700	0.9962	0.9701	0.9669	0.9733

Table 7. Model performance on different sensors with 70:20:10 train–validation–test split.

Sensor	Accuracy	AUC	F1-Score	Precision	Recall
HiScan	0.9700	0.9968	0.9697	0.9796	0.9600
GreenBit	0.9900	0.9994	0.9900	0.9868	0.9933
CrossMatch	0.9911	0.9998	0.9909	0.9954	0.9864
Digital Persona	0.9800	0.9973	0.9800	0.9800	0.9800
Time Series	0.9933	0.9998	0.9933	0.9955	0.9911

4.2.7. Comparison with Baseline Models

The comparison of model performance across different sensors obtained by the proposed and existing approaches is noted in Table 8. The proposed EfficientNetB0 architecture, enhanced with channel-wise attention through SE blocks, successfully handles several inherent constraints discovered in previous fingerprint liveness detection approaches. In contrast to Slim-ResCNN [25], which is both computationally demanding due to its training-from-scratch approach and deficient in cross-sensor generalisability, our approach has significant practical benefits. Utilizing pretrained ImageNet weights markedly enhances convergence speed and guarantees the transferability of low-level features, facilitating domain-specific adaption in the deeper layers. Moreover, Slim-ResCNN's implementation of basic score-level fusion [32], such as average pooling, inadequately addresses the non-linear interdependencies among features derived from various fingerprint areas. Our model overcomes this limitation by utilizing SE-based internal feature reweighting, which automatically learns optimal fusion hierarchies in a distinguishable way. In contrast to HyFiPAD [26], which relies on superficial classifiers and manually crafted features such as local adaptive binary features and binary statistical image features, rendering it less adaptable to new fake textures or acquisition conditions, our end-to-end trainable workflow acquires hierarchical and generalizable representations straight from data. The attention mechanism promotes robustness to ambiguous or overlapping spoof qualities by emphasizing salient feature maps contextually. The design considerations together ensure constant, high-fidelity performance across all five sensors in the LivDet2015 benchmark, affirming the model's cross-domain robustness and its suitability for implementation in dynamic, real-world biometric verification systems.

Table 8. Comparison of model performance across different sensors.

Ref.	Model	Sensor Type			
		Green Bit	**Cross Match**	**Digital Persona**	**HiScan**
[25]	**Slim-ResCNN**	97.81%	97.01%	95.42%	–
[26]	**HyFiPAD**	96.70%	95.00%	97.20%	–
[32]	**Score-Level Fusion**	98.62%	98.57%	94.46%	–
	Proposed	99.50%	98.99%	99.00%	97.75%

4.2.8. Effects of Sensor-Specific Distortions and Mitigation Approaches

The HiScan sensor, distinguished by its lowered resolution as well as potential distortions in fingerprint images, produced marginally inferior performance metrics (e.g., accuracy, precision) in comparison to superior sensors such as GreenBit and CrossMatch. Sensor-specific aberrations, including noise and diminished ridge clarity, might adversely affect feature extraction, complicating the model's capability to determinate fingerprints effectively. The model's performance, specifically regarding precision and F1-score, diminished when evaluated using HiScan data, highlighting the influence of sensor quality on overall efficacy. We proposed sensor-specific fine-tuning as a viable way to tackle that

challenge. By refining the model, especially on HiScan-acquired data, we can alter the model to understand and integrate the distinct attributes of the sensor.

This fine-tuning process would facilitate the model to more effectively manage sensor-specific distortions, such as reduced resolution or noise, thereby improving its capacity to distinguish between live and spoofed fingerprints across diverse sensor conditions. Fine-tuning on sensor-specific data can be a crucial strategy for improving the model's robustness and providing its efficacy across diverse fingerprint sensors employed in practical biometric systems.

5. Strengths and Limitations of Proposed Model

5.1. Strengths of Proposed Model

One of the main strengths of the proposed architecture lies in its improved generalization ability across diverse fingerprint sensors. It consistently achieves an accuracy of over 97% for all sensor types, emphasizing its robustness and adaptability to various input characteristics. Another substantial advantage is the near-perfect Area Under the Curve (AUC) scores, all of which are above 0.998, exhibiting an excellent capability to differentiate between live and faked fingerprints with high confidence. The architecture also aids greatly from the incorporation of the Squeeze-and-Excitation attention mechanism, which improves the discriminatory ability of the extracted features by concentrating on the considerable informative fingerprint regions. This attention mechanism plays a vital function in attaining higher precision and recall. Moreover, the model indicates extremely low false negative rates, with a perfect recall value of 1.00 in most cases, which is specifically valuable in biometric systems, as it provides that genuine users are not erroneously rejected, thereby enhancing user experience and system dependability. Comparable to previous work in medical imaging, where convolutional architectures were optimized for rapid and accurate diagnosis of COVID-19-related pathologies from X-rays while maintaining a lightweight design [33], our model similarly achieves high diagnostic performance with reduced computational overhead. The architecture also aids greatly benefits from the incorporation of the Squeeze-and-Excitation attention mechanism, which improves the discriminatory ability of the extracted features by concentrating on the considerably informative fingerprint regions. Similar attention-based strategies have also demonstrated effectiveness in other biometric domains, such as facial emotion recognition for Ambient Assisted Living systems [34]. This attention mechanism plays a vital function in attaining higher precision and recall. Moreover, the model indicates extremely low false negative rates, with a perfect recall value of 1.00 in most cases, which is specifically valuable in biometric systems as it prevents genuine users from being erroneously rejected, thereby enhancing user experience and system dependability.

5.2. Limitations of Proposed Model

Despite these advantages, the proposed architecture demonstrates certain constraints. Notably, it exhibits a higher false positive rate for specific sensors, like HiScan and Time Series, where the respective precisions decline to 0.9569 and 0.9804, suggesting that the model sometimes misclassifies high-quality spoof fingerprints as real, which could compromise the system's security. This is particularly evident with the HiScan sensor, where lower accuracy can be attributed to sensor-specific distortions such as lower resolution or noise in fingerprint images. To illustrate this, we provide failure case examples for both sensors, highlighting specific instances where the model struggled to differentiate live and spoofed fingerprints. Additionally, the performance deviates narrowly across diverse sensors, with Green Bit achieving 99.50% accuracy, while HiScan lags slightly behind at 97.75%. This variability indicates that sensor-specific artifacts may impact the

model's decision-making process. This observation aligns with findings from the field of image forensics, where CNN-based models for copy-move forgery detection have similarly demonstrated a strong dependency on dataset characteristics, with the performance varying significantly across different data sources due to class imbalance, manipulation complexity, and dataset size [35]. Visualizations of feature maps have been included to show how the model focuses on different fingerprint regions, helping to understand why certain instances lead to misclassifications. These visualizations provide insight into the model's feature extraction process, particularly for challenging spoof detection cases. Finally, although the employment of EfficientNetB0 with pre-trained ImageNet weights delivers a solid basis for feature extraction, it still depends on general-purpose pretraining, which may not fully capture the unique characteristics of fingerprints, such as ridges and minutiae. Domain-specific fine-tuning on larger and more diverse fingerprint datasets could significantly enhance the model's ability to address real-world spoofing techniques. Pre-training the model on extensive fingerprint-specific datasets such as LivDet 2015 will enable it to better capture essential fingerprint features, strengthening its ability to generalize across different sensors and spoof materials, ultimately improving its robustness and accuracy in fingerprint liveness detection.

5.3. Regulatory Considerations

We recognize the importance of compliance with biometric security standards such as ISO/IEC 30107 [36] for Presentation Attack Detection and ISO/IEC 19794-2 [37] for fingerprint data formats. Compliance with these standards is crucial for ensuring the security and reliability of fingerprint-based systems in real-world applications, particularly in sectors like banking and healthcare. In future work, we will explore how the TL-Efficient-SE framework can be adapted to meet these standards, ensuring its effectiveness and compliance with industry regulations for biometric systems.

6. Conclusions

This study proposes a practical deep learning framework for fingerprint liveness detection, integrating EfficientNetB0 with a Squeeze-and-Excitation attention mechanism. The integration improves feature extraction and enhances the model's capability to differentiate between live and spoofed fingerprints. By employing transfer learning, the model attains high performance with less data, making it well-suited for real-world requirements. The model shows robust generalization across diverse fingerprint sensors, including CrossMatch, Green Bit, and HiScan, acquiring high accuracy, AUC, and recall. The proposed model achieves 99.50% accuracy on the Green Bit sensor, significantly outperforming Slim-ResCNN, which achieved 97.81% accuracy. This highlights the superior performance and generalization ability of the TL-Efficient-SE framework. This adaptability guarantees its functional deployment across various biometric systems. Further, the SE attention mechanism improves feature discrimination, making the model resistant to spoof attacks. With its exceptional performance, the proposed model provides a potential solution for fingerprint liveness detection, making it well-suited for applications in mobile authentication and secure access control. This study paves the way for further advancements, such as sensor-invariant learning and dynamic thresholding, to handle complicated spoofing techniques better. Future development may also draw inspiration from recent embedded implementations of predictive models in real-time safety-critical environments, such as FPGA-accelerated LSTM architectures for UAV engine monitoring that leverage matrix compression techniques to achieve high accuracy with reduced latency and hardware resource usage [38]. Similarly, advancements in UAV obstacle and aircraft detection under adverse conditions highlight how deep learning and sensor fusion ap-

proaches can ensure robust performance in dynamic, real-time scenarios [39]. The proposed approach is highly applicable for real-world scenarios, particularly in secure access control inside sensitive domains like banking and healthcare, where effective fingerprint liveness detection is essential.

Author Contributions: Conceptualization, A.P., C.N. and C.R.; methodology, A.P., R.D.A.R. and C.N.; software, A.P., R.D.A.R. and C.N.; formal analysis, A.P. and R.M.R.Y.; investigation, A.P., R.D.A.R. and C.R.; resources, R.D.A.R. and R.M.R.Y.; data curation, A.P., R.D.A.R. and R.M.R.Y.; supervision, C.N. and C.R.; project administration, C.R. 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. This study did not involve humans or animals and therefore did not require ethical approval.

Informed Consent Statement: Not applicable. This study did not involve human participants.

Data Availability Statement: The datasets used in this study are publicly available and can be accessed through the original source cited in the manuscript. No new data were generated in this study.

Acknowledgments: The authors thank their respective institutions for providing computational resources and infrastructure. No external administrative or technical support was involved.

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

References

1. Ramachandra, R.; Busch, C. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 1–37. [CrossRef]
2. Shaheed, K.; Szczuko, P.; Kumar, M.; Qureshi, I.; Abbas, Q.; Ullah, I. Deep learning techniques for biometric security: A systematic review of presentation attack detection systems. *Eng. Appl. Artif. Intell.* **2024**, *129*, 107569. [CrossRef]
3. Gangarapu, B.S.; Yanamala, R.M.R.; Pallakonda, A.; Vardhan, H.R.; Raj, R.D.A. Lightweight spatial attention pyramid network-based image forgery detection optimized for real-time edge TPU deployment. *Comput. Electr. Eng.* **2025**, *128*, 110645. [CrossRef]
4. Kho, J.B.; Lee, W.; Choi, H.; Kim, J. An incremental learning method for spoof fingerprint detection. *Expert Syst. Appl.* **2019**, *116*, 52–64. [CrossRef]
5. Agarwal, S.; Chowdary, C.R. A-Stacking and A-Bagging: Adaptive versions of ensemble learning algorithms for spoof fingerprint detection. *Expert Syst. Appl.* **2020**, *146*, 113160. [CrossRef]
6. Jung, H.Y.; Heo, Y.S.; Lee, S. Fingerprint liveness detection by a template-probe convolutional neural network. *IEEE Access* **2019**, *7*, 118986–118993. [CrossRef]
7. Alshdadi, A.A.; Mehboob, R.; Dawood, H.; Alassafi, M.O.; Alghamdi, R.; Dawood, H. Exploiting Level 1 and Level 3 features of fingerprints for liveness detection. *Biomed. Signal Process. Control* **2020**, *61*, 102039. [CrossRef]
8. Sharma, D.; Selwal, A. FinPAD: State-of-the-art of fingerprint presentation attack detection mechanisms, taxonomy and future perspectives. *Pattern Recognit. Lett.* **2021**, *152*, 225–252. [CrossRef]
9. Zhang, Y.; Pan, S.; Zhan, X.; Li, Z.; Gao, M.; Gao, C. Fldnet: Light dense cnn for fingerprint liveness detection. *IEEE Access* **2020**, *8*, 84141–84152. [CrossRef]
10. Chugh, T.; Jain, A.K. Fingerprint spoof detector generalization. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 42–55. [CrossRef]
11. Gonzalez-Soler, L.J.; Gomez-Barrero, M.; Chang, L.; Pérez-Suárez, A.; Busch, C. Fingerprint presentation attack detection based on local features encoding for unknown attacks. *IEEE Access* **2021**, *9*, 5806–5820. [CrossRef]
12. Tian, S.; Tang, H.; Dai, L. Coupled patch similarity network for one-shot fine-grained image recognition. In Proceedings of the 2021 IEEE International Conference on Image Processing (ICIP), Anchorage, AK, USA, 19–22 September 2021; pp. 2478–2482.
13. Tang, H.; Yuan, C.; Li, Z.; Tang, J. Learning attention-guided pyramidal features for few-shot fine-grained recognition. *Pattern Recognit.* **2022**, *130*, 108792. [CrossRef]
14. Agarwal, S.; Rattani, A.; Chowdary, C.R. A-iLearn: An adaptive incremental learning model for spoof fingerprint detection. *Mach. Learn. Appl.* **2022**, *7*, 100210. [CrossRef]
15. Rattani, A.; Ross, A. Automatic adaptation of fingerprint liveness detector to new spoof materials. In Proceedings of the IEEE International Joint Conference on Biometrics, Clearwater, FL, USA, 29 September–2 October 2014; pp. 1–8.

16. Popli, A.; Tandon, S.; Engelsma, J.J.; Namboodiri, A. A unified model for fingerprint authentication and presentation attack detection. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*; Springer: Singapore, 2023; pp. 77–99.
17. Micheletto, M.; Marcialis, G.L.; Orrù, G.; Roli, F. Fingerprint recognition with embedded presentation attacks detection: Are we ready? *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 5338–5351. [CrossRef]
18. Chingovska, I.; Mohammadi, A.; Anjos, A.; Marcel, S. Evaluation methodologies for biometric presentation attack detection. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*; Springer: Cham, Switzerland, 2019; pp. 457–480.
19. Grosz, S.A.; Wijewardena, K.P.; Jain, A.K. ViT unified: Joint fingerprint recognition and presentation attack detection. In Proceedings of the 2023 IEEE International Joint Conference on Biometrics (IJCB), Ljubljana, Slovenia, 25–28 September 2023; pp. 1–9.
20. Aryan, P.; Yanamala, R.M.R.; Pallakonda, A.; Raj, R.D.A.; Prakasha, K.K. Lightweight End-to-End Patch-Based Self-Attention Network for Robust Image Forgery Detection. *IEEE Access* **2025**, *13*, 157674–157686. [CrossRef]
21. Chen, S.; Guo, Z.; Li, X.; Yang, D. Query2set: Single-to-multiple partial fingerprint recognition based on attention mechanism. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1243–1253. [CrossRef]
22. Grosz, S.A.; Jain, A.K. Afr-net: Attention-driven fingerprint recognition network. *IEEE Trans. Biom. Behav. Identity Sci.* **2023**, *6*, 30–42. [CrossRef]
23. Dhalia Sweetlin, J.; Bhuvaneshwari, R.; Bhagya, N.; Bavya Dharshini, N. Robust fingerprint reconstruction using attention mechanism based autoencoders and multi-kernel autoencoders. *Appl. Intell.* **2024**, *54*, 8262–8277. [CrossRef]
24. Lin, L.; Zhao, Y.; Meng, J.; Zhao, Q. A federated attention-based multimodal biometric recognition approach in IoT. *Sensors* **2023**, *23*, 6006. [CrossRef]
25. Zhang, Y.; Shi, D.; Zhan, X.; Cao, D.; Zhu, K.; Li, Z. Slim-ResCNN: A deep residual convolutional neural network for fingerprint liveness detection. *IEEE Access* **2019**, *7*, 91476–91487. [CrossRef]
26. Sharma, D.; Selwal, A. HyFiPAD: A hybrid approach for fingerprint presentation attack detection using local and adaptive image features. *Vis. Comput.* **2022**, *38*, 2999–3025. [CrossRef]
27. Kaplesh, P.; Gupta, A.; Bansal, D.; Sofat, S.; Mittal, A. Vision transformer for contactless fingerprint classification. *Multimed. Tools Appl.* **2025**, *84*, 31239–31259. [CrossRef]
28. Jia, Z.; Huang, C.; Wang, Z.; Fei, H.; Wu, S.; Feng, J. Finger recovery transformer: Toward better incomplete fingerprint identification. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 8860–8874. [CrossRef]
29. Alghamdi, S.M.; Jarraya, S.K.; Kateb, F. Enhancing security in multimodal biometric fusion: Analyzing adversarial attacks. *IEEE Access* **2024**, *12*, 106133–106145. [CrossRef]
30. Sumalatha, U.; Prakasha, K.K.; Prabhu, S.; Nayak, V.C. A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. *IEEE Access* **2024**, *12*, 64300–64334. [CrossRef]
31. Ghiani, L.; Yambay, D.A.; Mura, V.; Marcialis, G.L.; Roli, F.; Schuckers, S.A. Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015. *Image Vis. Comput.* **2017**, *58*, 110–128. [CrossRef]
32. Zhang, Y.; Gao, C.; Pan, S.; Li, Z.; Xu, Y.; Qiu, H. A score-level fusion of fingerprint matching with fingerprint liveness detection. *IEEE Access* **2020**, *8*, 183391–183400. [CrossRef]
33. Randieri, C.; Perrotta, A.; Puglisi, A.; Grazia Bocci, M.; Napoli, C. CNN-Based Framework for Classifying COVID-19, Pneumonia, and Normal Chest X-Rays. *Big Data Cogn. Comput.* **2025**, *9*, 186. [CrossRef]
34. Russo, S.; Tibermacine, I.E.; Randieri, C.; Rabehi, A.; H Alharbi, A.; El-kenawy, E.S.M.; Napoli, C. Exploiting facial emotion recognition system for ambient assisted living technologies triggered by interpreting the user's emotional state. *Front. Neurosci.* **2025**, *19*, 1622194. [CrossRef]
35. Dell'Olmo, P.V.; Kuznetsov, O.; Frontoni, E.; Arnesano, M.; Napoli, C.; Randieri, C. Dataset Dependency in CNN-Based Copy-Move Forgery Detection: A Multi-Dataset Comparative Analysis. *Mach. Learn. Knowl. Extr.* **2025**, *7*, 54. [CrossRef]
36. Gonzalez, S.; Tapia, J.E. Forged presentation attack detection for ID cards on remote verification systems. *Pattern Recognit.* **2025**, *162*, 111352. [CrossRef]
37. Sadhya, D. Achieving unlinkability in fingerprint templates via k-anonymity and random projection. *Sādhanā* **2024**, *49*, 224. [CrossRef]
38. Priya, S.S.; Sanjana, P.S.; Yanamala, R.M.R.; Amar Raj, R.D.; Pallakonda, A.; Napoli, C.; Randieri, C. Flight-Safe Inference: SVD-Compressed LSTM Acceleration for Real-Time UAV Engine Monitoring Using Custom FPGA Hardware Architecture. *Drones* **2025**, *9*, 494. [CrossRef]
39. Randieri, C.; Ganesh, S.V.; Raj, R.D.A.; Yanamala, R.M.R.; Pallakonda, A.; Napoli, C. Aerial Autonomy Under Adversity: Advances in Obstacle and Aircraft Detection Techniques for Unmanned Aerial Vehicles. *Drones* **2025**, *9*, 549. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.