symmetry

MDPI

Article

An Efficient OCT Fingerprint Antispoofing Method Based on ResMamba

Xinyan Mai [1], Miaohua Chen [1], Zhaodong Lu [1], Shengkai Yang [1], Gongpu Lan [1,2], Yanping Huang [1,2], Jia Qin [2], Lin An [2,3], Jingjiang Xu [1,2,*] and Jing Cai [1,*]

[1] Guangdong-Hong Kong-Macao Joint Laboratory for Intelligent Micro-Nano Optoelectronic Technology, School of Physics and Optoelectronic Engineering, Foshan University, Foshan 528000, China; 2112205032@fosu.edu.cn (X.M.); 2112205006@fosu.edu.cn (M.C.); 2112455013@fosu.edu.cn (Z.L.); 2112455031@fosu.edu.cn (S.Y.); langongpu@fosu.edu.cn (G.L.); yale.huangyp@fosu.edu.cn (Y.H.)

[2] Innovation and Entrepreneurship Teams Project of Guangdong Provincial Pearl River Talents Program, Guangdong Weiren Meditech Co., Ltd., Foshan 528015, China; wrqinjia@weirenmeditech.com (J.Q.); wranlin@weirenmeditech.com (L.A.)

[3] School of Computer Science, Hangzhou Dianzi University, Hangzhou 310018, China

* Correspondence: xujingjiang@fosu.edu.cn (J.X.); caijing@fosu.edu.cn (J.C.)

Abstract: Optical coherence tomography (OCT), known for its noncontact and 3D imaging capabilities, has found widespread application in fingerprint antispoofing detection. However, the existing methods rely heavily on single-frame B-scan images, underutilizing the 3D spatial information inherent in OCT volume data. High computational costs further limit its practical applications. Thus, this study proposes an efficient fingerprint antispoofing method which leverages the spatial continuity of OCT volume data to enhance both the accuracy and computational efficiency. Using an OCT system, we collected 320 real fingerprints and 320 spoofed fingerprints. Then, to distinguish between genuine and spoofed fingerprints, we developed the proposed ResMamba model, which is based on an enhanced 3D convolutional network integrated with a state space model (SSM). We extracted regions of interest (ROIs) from B-scan images and segmented them into volume slices for training and classification. The experimental results demonstrate that ResMamba achieved a 0.56% error rate (ERR) and 99.22% area under the curve (AUC), with an inference time of just 11 ms. Furthermore, compared to the existing models, ResMamba effectively balances its accuracy, inference speed, and model size. Ablation studies confirm that integrating the SIC module enhances the model's robustness. Overall, ResMamba offers an efficient and reliable fingerprint antispoofing solution, outperforming the traditional methods in terms of its accuracy and performance.

Keywords: optical coherence tomography; fingerprint antispoofing; state space model

Citation: Mai, X.; Chen, M.; Lu, Z.; Yang, S.; Lan, G.; Huang, Y.; Qin, J.; An, L.; Xu, J.; Cai, J. An Efficient OCT Fingerprint Antispoofing Method Based on ResMamba. *Symmetry* **2024**, *16*, 1603. https://doi.org/10.3390/sym16121603

Academic Editor: Zhixun Su

Received: 11 November 2024
Revised: 21 November 2024
Accepted: 27 November 2024
Published: 1 December 2024

1. Introduction

Biometric technology has revolutionized personal identity verification in real-world applications. This technology leverages unique biological traits, such as fingerprints and palm prints, to significantly enhance the accuracy and user-friendliness of identity authentication. Its broad range of applications ranges from smartphone unlocking to managing access at high-security facilities, highlighting its crucial role in ensuring personal and information security [1–3]. Currently, over 40% of biometric authentication systems worldwide employ fingerprint recognition [4] owing to its efficiency, ease of use, and ability to reliably differentiate between identities, even in the rare cases of identical twins.

Despite its advantages, fingerprint recognition technology now faces significant challenges [5,6]. To date, security vulnerabilities have emerged, particularly concerning the creation of fake fingerprints, as their use has become more widespread [7,8]. Fake fingerprints, made from materials such as silicone or capacitive gels [9], can deceive recognition systems, granting unauthorized access and posing a direct threat to privacy and data security [10,11].

These issues highlight the limitations of traditional optical and capacitive fingerprint recognition technologies in distinguishing real fingerprints from counterfeits [12,13]. As a result, researchers are now exploring new methods and technologies to enhance system security and resistance to spoofing, thus ensuring that biometric technology can continue to fulfill its critical role in real-world applications [14].

Fingerprint characteristics, such as minutiae types, ridge features, and the shape and spacing of ridge valleys, are commonly used to detect fake fingerprints in presentation attacks [15,16]. Marcialis et al. [17] analyzed high-resolution fingerprint images to calculate the sweat pore density and average spacing, enabling them to distinguish real fingers from artificial ones. To assess the authenticity of fingerprints, Galbally et al. [18] collected various fingerprint features, including ridge strength, direction, and continuity. Additionally, dynamic fingerprint features have become a central focus of antispoofing research. Park et al. [19] proposed a small fully convolutional neural network (FCN) that integrates with fingerprint systems to classify real, fake, and background fingerprint information, thus facilitating antispoofing detection. Wang et al. [20] divided fingerprint images into small segments, which they then inputted into a fully connected network for classification and authenticity determination.

Hardware-based liveness detection methods have also been explored. For example, Martin et al. [21] found that heart-induced blood flow changes slightly alter the finger contact volume—a variation detectable by sensors and subsequently analyzed by control systems. Reddy et al. [22] assessed blood oxygen levels by measuring the light absorption characteristics of fingers and artificial membranes at various wavelengths, thus enabling automatic antispoofing detection.

Recently, optical coherence tomography (OCT) has been applied to fingerprint acquisition tasks. First proposed by David Huang in 1991 [23], OCT is a noncontact, noninvasive 3D imaging technique based on low-coherence light interference [14]. With its high resolution (approximately 10 μm) and depth of 1–2 mm, OCT has been successfully employed in clinical ophthalmology and cardiovascular diagnostics and has broad application potential in fields such as brain science, dermatology, and dentistry [24]. OCT can also capture 3D volumetric data within a subcutaneous range of 1–2 mm. After processing, it can generate clear surface fingerprints [25], internal fingerprint structures [26], and sweat gland distributions [27]. Figure 1 presents a typical OCT B-scan image of a human finger obtained through OCT imaging.

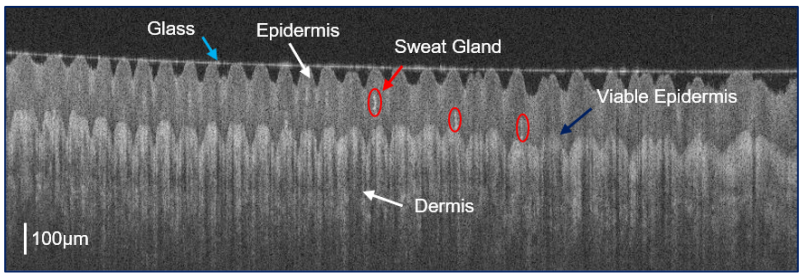

Figure 1. Example of finger OCT imaging data.

Cheng et al. [28] used an A-line autocorrelation analysis to distinguish the optical properties of real skin from those of artificial fingerprint materials. Bossen et al. [29] focused on extracting the internal fingerprint structures, specifically the dermal papillae, using B-scan OCT imaging. Similarly, Liu et al. [30] used spectral domain OCT (SD-OCT) to map the sweat gland distribution within the fingertips, providing robust tertiary biometric features for forgery detection. Darlow et al. [13] combined OCT with an autocorrelation analysis and deep feature extraction to identify counterfeit fingerprints and adhesive layers. Chugh et al. [3] also used deep convolutional neural networks (CNNs) to analyze the structural differences in OCT depth profiles to improve the detection accuracy. Liu et al. [31] developed a method based on dual-peak and sub-peak features derived from A-line OCT

depth profiles to classify real and fake fingerprints. Sun et al. [32] proposed the integration of total internal reflection (TIR) with OCT for simultaneous acquisition of external and internal fingerprint features, coupled with grid calibration to correct optical distortion. Liu et al. [33] introduced an autoencoder network to model the reconstruction errors and weighted activation maps to improve the robustness of counterfeit detection. Sun et al. [34] extracted external and internal fingerprint features from OCT data and incorporated hand-crafted features such as self-matching scores (SMSs) and sweat-gland-related metrics for classification. Zhang et al. [35] used OCT volume data and a 3D convolutional neural network to exploit spatial continuity for antispoofing. Table 1 shows a direct comparison of these methods.

Despite notable advances in OCT-based fingerprint antispoofing techniques, several limitations remain. Many of the existing approaches rely heavily on specific features such as the optical properties [28], sweat gland distribution [30], or depth profiles [3,13], which may prove inadequate when dealing with complex or anomalous spoofing materials. In addition, the application of OCT data is often limited to two-dimensional slices or superficial depth features [29,35], which does not account for the extensive spatial continuity present in volumetric data. Methods that rely on deep learning models, such as convolutional neural networks (CNNs) and 3D CNNs [3,35], typically require extensive labeled datasets, which are scarce in this domain. This can lead to overfitting problems in small-sample scenarios. In addition, the high computational complexity of these models hinders their use in real-time or resource-constrained environments. Finally, modern spoofing techniques, such as multi-layered or biomimetic materials, pose significant challenges to the robustness of the existing methods [33,34].

Table 1. Existing studies on OCT-based fingerprint antispoofing.

Study	Approach	OCT Data Types Used
Cheng et al., 2006 [28]	Using an A-line autocorrelation analysis	A-line
Bossen et al., 2010 [29]	Extraction of the internal papillary layer structure of fingerprints	B-scan
Liu et al., 2010 [30]	Extraction of fingertip sweat gland distribution as an antispoofing feature.	B-scan
Darlow et al., 2016 [13]	Combining OCT autocorrelation analysis and deep feature extraction	B-scan
Chugh et al., 2019 [3]	Detecting structural differences with a CNN based on B-scans	B-scan
Liu et al., 2019 [31]	Utilization of B-scan bimodal and sub-peak characteristics	A-line
Sun et al., 2020 [32]	Combining TIR and OCT to synchronize the collection of external and internal fingerprint information for comparison	B-scan
Liu et al., 2021 [33]	Reconstruction errors are detected using a self-encoder network.	B-scan
Sun et al., 2023 [34]	Extraction of OCT external and internal features based on manual feature detection.	B-scan
Zhang et al., 2023 [35]	Detection of forgeries based on OCT volumetric data and the 3DCNN method.	Volume data
Proposed method	Extracting the spatial continuity features of volumetric data using ResMamba, a 3D convolutional network with an integrated state space model (SSM)	Volume data

In order to address these challenges, we introduce a lightweight network model, which fully leverages OCT volume data and their 3D spatial continuity. This approach enhances fingerprint antispoofing detection while minimizing the computational overhead. The fingertip volume data obtained through OCT contain rich biometric features with inherent three-dimensional consistency, offering a significant advantage over the traditional fingerprint collection methods. This study develops the ResMamba architecture, specifically for OCT-based fingerprint antispoofing tasks, with the objective of maximizing the potential of OCT data while simultaneously reducing the computational costs. In contrast to existing methodologies that depend on particular features (e.g., optical characteristics or the sweat gland distribution), ResMamba integrates global spatial continuity with local fine-grained details, enabling the effective detection of anomalies and subtle differences between genuine and imitated fingerprints. In fully leveraging the three-dimensional nature of OCT data, ResMamba incorporates a state space model (SSM) to preserve the critical spatial continuity across the entire volume, thereby ensuring a comprehensive analysis of the fingerprint's structure. The lightweight architecture of the system minimizes the dependency on extensive labeled datasets, thereby mitigating the risk of overfitting, particularly in scenarios involving a limited number of samples. Moreover, the efficient design of ResMamba markedly reduces its computational complexity, thereby enabling its real-time deployment in resource-constrained environments. The integration of these capabilities allows ResMamba to maintain robust performance, even against advanced spoofing techniques such as multilayered or biomimetic materials, thus making it a reliable and practical solution for OCT-based fingerprint antispoofing.

In this work, we propose a lightweight antispoofing network model based on OCT 3D volume data implemented through the following steps: First, we collected 320 sets of OCT fingerprint data from real fingers and 320 sets from artificial fingerprint materials, which could be detected by traditional fingerprint recognition systems. Next, we developed an algorithm to accurately extract region of interest (ROI) volume slices from the OCT cross-sectional images (B-scans). Subsequently, we introduced the ResMamba network model to classify each 3D volume slice as either belonging to a real finger or an artificial one. In this step, we applied a symmetry-based approach to transforming the 3D data into a 1D representation, which was then fed into the SSM module for modeling. We then designed a strategy to prevent artificial fingerprints from being falsely identified as real ones. This allowed us to address the challenge posed by certain artificial fingerprint membranes that closely resemble real fingerprints in specific local regions and that may potentially lead to misclassification.

After testing on a database containing OCT data from various artificial materials, the results demonstrate that the proposed technology exhibits exceptional antispoofing performance, thus confirming its feasibility and robustness.

2. The Proposed Method

2.1. Preliminaries

2.1.1. State Space Models

A state space model (SSM), which has time-invariant properties, is a linear system that maps the input $x(t) \in \mathbb{R}^L$ to the output $y(t) \in \mathbb{R}^L$. Mathematically, this system is represented by a set of linear ordinary differential equations (ODEs), as shown in Equations (1) and (2). For a system with state dimension N, the model parameters are represented by $A \in \mathbb{C}^{N\times N}$, $B, C \in \mathbb{C}^{N\times L}$, and the skip connection $D \in \mathbb{C}^L$. In this paper, $\mathbb{R}$ and $\mathbb{C}$ represent the sets of real and complex numbers, respectively. The derivative of the state and the output signal are described by the following equations:

$$h'(t) = Ah(t) + Bx(t) \tag{1}$$

$$y(t) = Ch(t) + Dx(t) \tag{2}$$

2.1.2. Discretization

In the process of integrating the SSM method into the design of deep learning networks, the continuous nature of its structure presents certain challenges to the computational process. Therefore, discretization is required.

The primary objective of discretization is to transform continuous ordinary differential equations into discrete functions. This conversion is essential to aligning the model with the sampling rate of the input data, thus enabling efficient computation [36]. For a given output $x_k \in \mathbb{R}^{L \times B}$, which represents a sampled vector from a signal sequence of length L, Equations (1) and (2) can be discretized using the zero-order hold method as follows [37]:

$$h_k = A_d h_{k-1} + B_d h_k \tag{3}$$

$$y_k = C_d h_k + D x_k \tag{4}$$

where $A_d = e^{A\Delta}$, $B_d = (e^{A\Delta} - I)A^{-1}B$, and $C_d = C$. In these equations, $B, C \in \mathbb{R}^{D \times N}$, and $\Delta \in \mathbb{R}^D$. According to [38], B can be approximated by its first-order Taylor series expansion:

$$\overline{B} = (e^{A\Delta} - I)A^{-1}B \approx (\Delta A)(\Delta A)^{-1}\Delta B = \Delta B \tag{5}$$

2.1.3. A Selective Scan Mechanism

Unlike mainstream methods that primarily focus on linear time-invariant SSMs, the proposed ResMamba incorporates the selective scanning mechanism (S6) [38] as a core operator. In the S6 mechanism, the matrices $B \in \mathbb{R}^{B \times L \times N}$, $C \in \mathbb{R}^{B \times L \times N}$, and $\Delta \in \mathbb{R}^{B \times L \times D}$ are derived from the input $x \in \mathbb{R}^{B \times L \times D}$ where B refers to the batch size, L is defined as the sequence length of the input, D represents the feature dimension of the input, and N denotes the state dimension of the hidden states within the state space model. This design facilitates the extraction of contextual information embedded within the input, thereby ensuring the dynamic nature of the weights within the S6 mechanism. For a more comprehensive understanding of S6, a detailed explanation is provided in [39].

2.2. The SSM in the Convolution Module

In recent years, Transformer-based deep learning methods have achieved remarkable success in image processing tasks. However, these methods are heavily reliant on powerful computational resources, with both memory and spatial complexity scaling as $O(N^2)$. Such heavy reliance imposes substantial demands on the training environment and application scenarios. Moreover, medical image datasets are often small (fewer than 1000 samples), and Transformer-based methods typically underperform on such datasets compared to large-scale datasets (e.g., ImageNet) containing over one million images. In these cases, convolutional neural networks (CNNs) tend to yield better results. However, CNNs are limited by their relatively small receptive fields, which hinder their ability to effectively capture global information and model long-range dependencies.

Inspired by the strong performance of the SSM in visual tasks and the Mamba model's ability to handle long-sequence tasks [40], we explored the process of integrating the SSM into CNNs to enhance the model's capacity to capture long-range dependencies. We also introduced the SSM as a parallel module within the CNN framework to expand the network's global receptive field, as illustrated in Figure 2.

Once the input data underwent initial encoding and feature extraction through the Stem layer, it was passed to the SIC (SSM in Convolution) module. This module consists of two layers, including 1×1 convolutions, along with batch normalization and ReLU activation functions. The feature map, with dimensions $B \times C \times H \times W \times D$, is reshaped into $B \times C \times L$, where $L = H \times W \times D$. In this process, we converted the 3D data into a 1D representation by employing a symmetrical flattening method. This method involved linearizing the spatial diagonal of the data, thus preserving the symmetry of the feature structure. The flattened data were then passed to the SSM module for global modeling,

thereby enhancing the network's ability to capture long-range dependencies and improving its overall global context awareness.

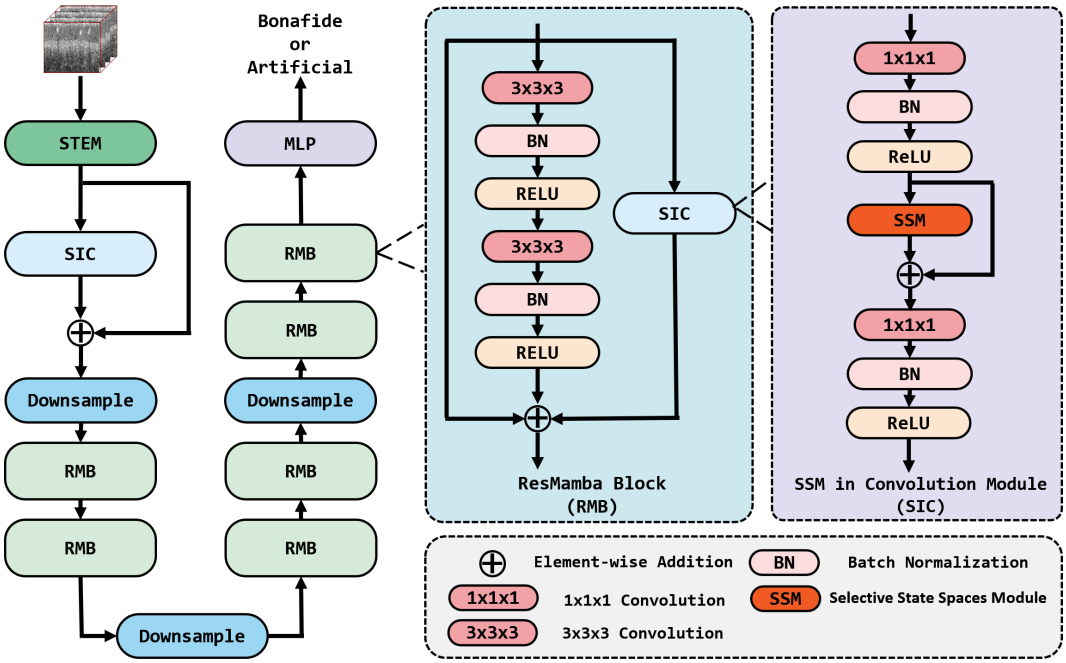

Figure 2. The architecture of the ResMamba model.

2.3. The ResMamba Block

We adopted a core architecture based on a residual encoder, as shown in Figure 2. This novel architectural unit was designed to integrate the SSM-based SIC (SSM in Convolution) module into traditional 3D CNNs for sequence modeling, thus enhancing the network's global perception capabilities. The ResMamba block consisted of two 3D convolutional layers, each followed by batch normalization to stabilize the training and ReLU activation to introduce nonlinearity. At the heart of the architecture is the SIC module, which serializes the input data by flattening them into a 1D form for sequential processing, facilitating the capture of spatially continuous information.

Moreover, residual connections bypass the entire block to mitigate the vanishing gradient problem, allowing the network to more effectively learn from the feature data. This design also enhances the network's ability to learn complex spatial features, which is critical for the OCT fingerprint antispoofing detection task. The experimental results show that compared to traditional network units, the ResMamba block excels at capturing features from OCT volume data, thus demonstrating its potential to improve the performance of 3D convolutional networks in handling serialized information.

2.4. ResMamba for OCT Fingerprint Antispoofing

This antispoofing task is fundamentally a classification task, for which we have adopted a residual-based encoder as the core network architecture, as shown in Figure 2. Based on the assumption that reducing the feature map size enhances the capture of long-range dependencies, we strategically introduced the SIC module after the Stem layer to optimize the data flow through residual connections. The input data were then processed by three ResMamba blocks, with the final output passed through a multilayer perceptron (MLP) to produce the classification result.

As shown in Figure 2, the ResMamba block was designed specifically to handle input data with a reduced resolution. The data were first downsampled using a convolutional layer, which reduced the dimensionality, lightened the computational load, and facilitated the extraction of higher-level features. The data then passed through two ResMamba blocks,

each equipped with skip connections that improved the gradient flow during training, thus mitigating the vanishing gradient problem and enabling the model to learn more effectively at greater depths.

To augment the training dataset, we applied the method proposed by Sun et al. [34]. Specifically, we performed peak detection along the vertical direction of the B-scan, extracted the curves representing the glass surface, and selected 100 pixels (based on empirical findings) below this curve as the ROI for OCT volume data. This ROI was then sliced into smaller volumes. A region of size $300 \times 600 \times 100$ can be sliced into 18 volumes of size $100 \times 100 \times 100$, which were subsequently used for the network training. This slicing process enhanced the data diversity and improved the robustness of the model.

2.5. The Antispoofing Method

To confirm the authenticity of the OCT volume data, we began by flattening each collected volume and randomly selecting 8 slices, each with a size of $100 \times 100 \times 100$. These slices were then inputted into the trained classifier for evaluation. If any of the 8 slices were classified as fake, the entire volume was considered counterfeit; otherwise, the volume was classified as coming from a real finger. The number of slices selected was empirically determined to ensure sufficient coverage for reliable classification. This process guarantees that even if part of the volume data is compromised, the system can still accurately identify counterfeit samples. Figure 3 illustrates a diagram outlining the process of the proposed antispoofing method.

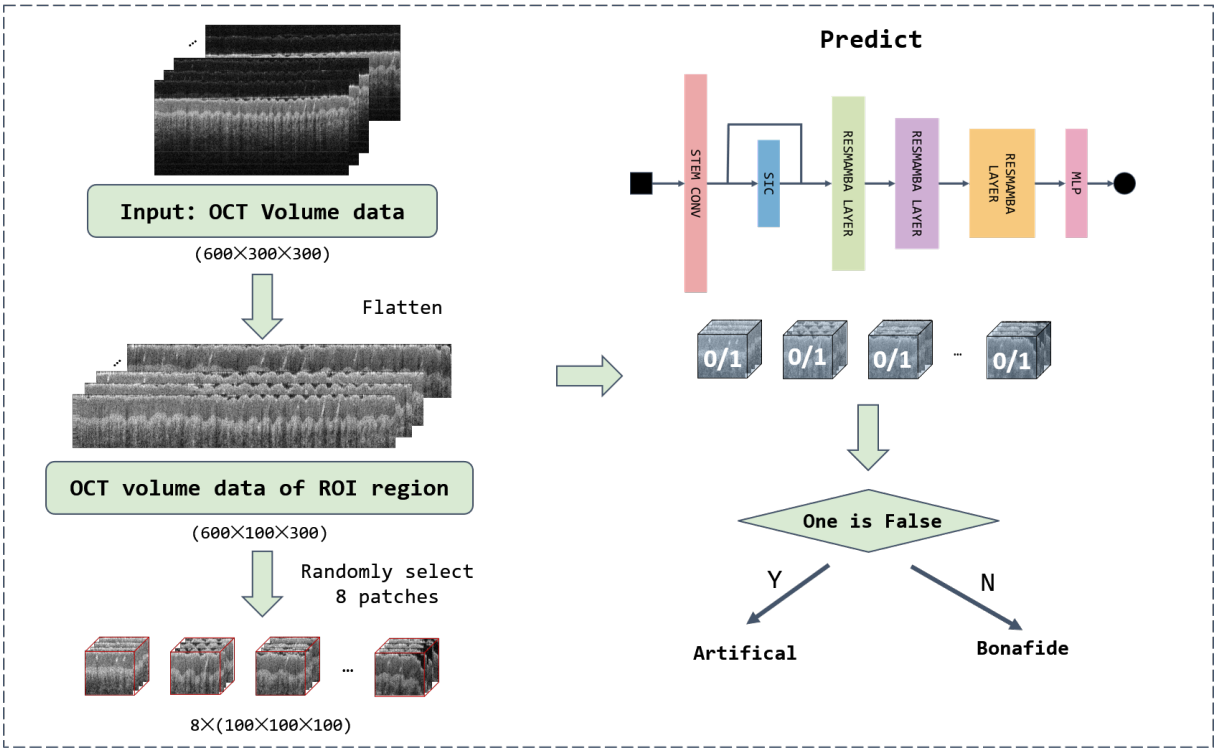

Figure 3. Our proposed antispoofing method.

3. Experiments and Analysis

3.1. OCT Systems and Data Acquisition

OCT is a noninvasive imaging technique used to scan the fingertip and capture volumetric data consisting of multiple cross-sectional slices. In this study, a swept-source OCT system was employed for fingerprint image acquisition, using a light source with a central wavelength of 1310 nm. Each B-scan image contained 300 pixels in the axial (Z) direction and 600 pixels in the lateral (X) direction. The OCT volume dataset con-

sisted of 300 individual B-scan images, which, together, formed a 3D representation of the scanned area.

In this study, we simulated artificial fingerprints using various common materials, such as transparent silicone, flesh-colored silicone, and ELMER's glue. These samples were categorized into two groups: one simulating only the external fingerprint features and the other simulating the external and internal features. All of the fabricated fingerprints were verified by traditional optical fingerprint recognition systems. Figure 4 illustrates the typical scanning outcomes for real fingers and artificial fingerprints.

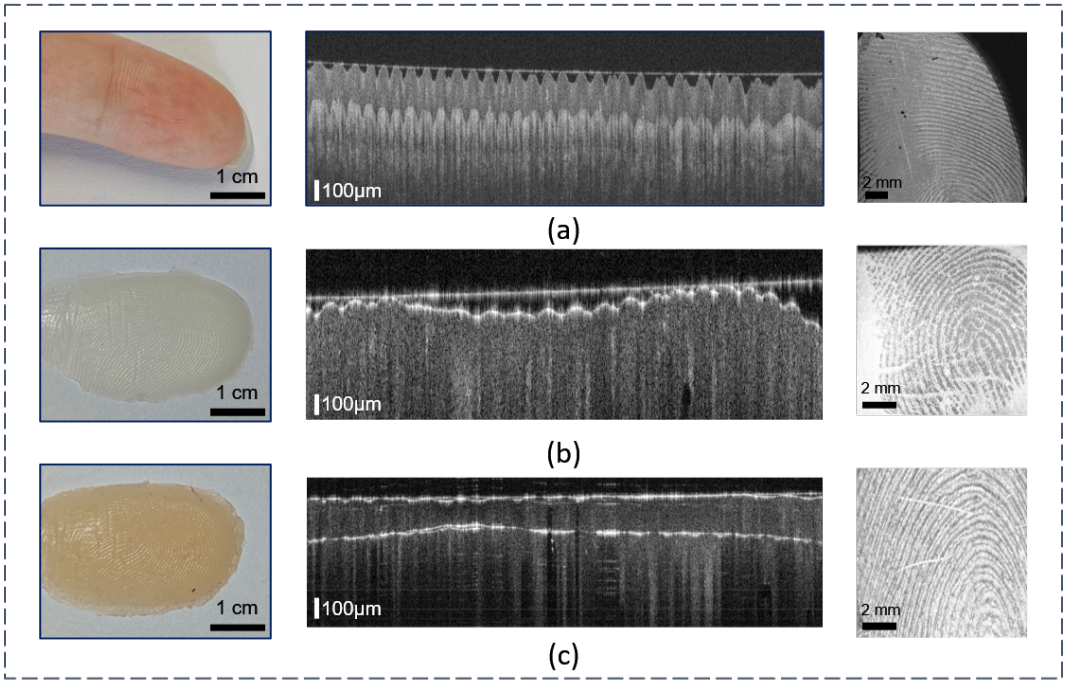

Figure 4. Samples of various types of fingerprint data. (**a**) Real finger fingerprints and corresponding B-scan images. (**b**) Artificial fingerprints (silicone) with only the outer-layer fingerprint features and corresponding B-scan images. (**c**) Artificial fingerprints with the outer- and inner-layer features (double-layer silicone overlay) and corresponding B-scan images.

In most cases, real fingers and artificial fingerprints that simulate only the external features can be differentiated easily in B-scan images. However, artificial fingerprints that simulate the external and internal features are more likely to be misclassified by the recognition system. Existing OCT-based fingerprint anticounterfeiting systems typically rely on single-frame B-scans for recognition; however, such systems fail to fully utilize the 3D spatial information available in the OCT data. Although some OCT-based anticounterfeiting detection networks have begun to incorporate volumetric data, these approaches often incur a significant computational overhead and require extensive computational resources and memory, thus limiting their practical efficiency.

To address these challenges, we propose an OCT fingerprint anticounterfeiting detection method based on ResMamba. This method fully leverages the features in OCT volumetric data to more accurately extract and identify fingerprint characteristics while simultaneously reducing the computational costs and enhancing the overall system efficiency.

3.2. Experimental Settings

3.2.1. Datasets

In this study, we employed a custom-built OCT system to collect both real fingerprint data and data from artificial fingerprint prostheses, allowing us to accurately evaluate the anticounterfeiting performance of each model. The training and testing datasets were selected from this data collection. For the real fingerprint data, we sampled 80 fingers from

10 individuals of various age groups (primarily students), with each finger sampled 4 times, resulting in 320 sets of real OCT volumetric data. For the artificial prosthesis data, we used 10 common prosthetic materials to fabricate 20 types of fingerprint prostheses, which included various combinations: 10 types simulating internal fingerprint features and 10 types simulating internal and external features. Each prosthesis type had 8 samples each sampled 4 times, thus producing a total of 320 sets of artificial prosthetic OCT fingerprint data.

During the network training phase, we used 60 sets of real fingerprint data and 60 sets of artificial prosthesis data as the training dataset. In the testing phase, the types of prosthetics included in the training dataset were excluded to ensure robustness in antispoofing detection. While real fingerprint data were included in the testing dataset, they were collected from individuals who were not part of the training dataset, thereby ensuring no overlap in subjects between the training and testing datasets.

We tested the model with the prosthetic types excluded in the training phase to ensure the robustness of the anticounterfeiting detection. This strategy aimed to evaluate the model's ability to generalize previously unseen prostheses, thus providing a more comprehensive assessment of its generalization performance and anticounterfeiting effectiveness in real-world applications.

The collection of human fingerprint data for this study was approved by the Ethics Committee of Foshan University (Project Identification Code: FUME2022001) and adhered to the ethical principles outlined in the Declaration of Helsinki for research involving human participants. All of the participants were fully informed about the research objectives, procedures, and potential risks before the data collection and voluntarily signed an informed consent form. This study ensured the privacy and security of the participants' data, which were anonymized and used exclusively for research purposes.

3.2.2. Evaluation Metrics

We compared the proposed method with other approaches using several evaluation metrics, including the ERR, AUC, TPR@FPR = 0.1, and BCPER_{20}.

Error rate (ERR) is a commonly used metric for assessing classification accuracy, representing the probability of making an incorrect prediction. The ERR is calculated as follows:

$$\text{EER} = \frac{FP + FN}{TP + TN + FP + FN} \tag{6}$$

where TP (true positive) refers to the number of positive instances correctly identified as positive, TN (true negative) refers to the number of negative instances correctly identified as negative, FP (false positive) indicates the number of negative instances incorrectly classified as positive, and FN (false negative) refers to the number of positive instances misclassified as negative. These metrics are fundamental for evaluating the performance of binary classification models and their ability to correctly distinguish between positive and negative samples.

AUC is another commonly used metric to assess a model's overall performance across all possible thresholds. This metric quantifies the model's ability to discriminate between positive and negative samples. A higher AUC (closer to 1) indicates a stronger discriminative power.

TPR@FPR measures the percentage of TP samples identified at a fixed FP rate (FPR). This metric helps evaluate the model's performance under specific FPR conditions. For example, when the FPR is fixed at 0.1, TPR@FPR represents the percentage of true samples correctly identified by the presentation attack detection (PAD) model when the FP rate is 0.1. A higher TPR@FPR indicates a better model performance under the given FPR.

BPCER (Biometric Presentation Classification Error Rate) is a critical metric in the field of biometric antispoofing. It evaluates the accuracy of biometric systems, such as those used for facial recognition, in distinguishing between legitimate and spoofed biometric data. A higher BPCER indicates a higher likelihood of misclassifying legitimate users as spoof attempts, which negatively impacts the user experience and system usability. Ideally,

the BPCER should be as low as possible to ensure legitimate users can pass through the biometric verification process smoothly.

BCPER$_{20}$ (Bona Fide Presentation Classification Error Rate at 20% APCER) is a key performance indicator that measures the misclassification rate for legitimate users (Bona Fide Presentations) when the attack presentation classification error rate (APCER) is set to 20%. This metric evaluates a model's security and reliability, ensuring that the model can effectively differentiate between legitimate samples and spoofed attempts, even when faced with a fixed attack error rate.

3.2.3. Optimization

The algorithm was implemented in PyTorch, utilising the Adam optimizer due to its capacity for adaptive learning rate adjustments, which is well suited to deep learning tasks. The initial learning rate was set to 0.001, a value determined following a series of hyperparameter search experiments. During the course of these experiments, the efficacy of the learning rates within the range of $[10^{-4}, 10^{-2}]$ was evaluated. It was established that a rate of 0.001 demonstrated the optimal equilibrium between the convergence stability and performance.

The training process was conducted on an NVIDIA RTX 3080 GPU with 10 GB of VRAM, thereby ensuring the availability of sufficient computational resources for the experiments. The batch size was set to 32, selected following an evaluation of values of 16, 32, and 64. A batch size of 32 proved to be the optimal compromise between the computational efficiency and the model performance. Increasing the batch size to 64 resulted in a slight decline in the convergence speed, while reducing it to 16 increased the gradient noise without conferring notable gains in accuracy.

The cross-entropy loss function was selected on the grounds of its suitability for classification tasks. The training process was conducted for a maximum of 100 epochs, with an early stopping criterion designed to halt training if no improvement in the validation performance was observed for 10 consecutive epochs. This criterion was subsequently validated through testing of stopping patience values of 5, 10, and 15 epochs, wherein 10 epochs were identified as providing an optimal balance between preventing overfitting and avoiding premature termination of training.

The finalization of these hyperparameter values was based on systematic experimentation and a grid search on a validation set. Each parameter was tuned independently while the others were held constant, and combinations were subsequently tested to confirm their compatibility. This process ensured the stability and reliability of the training pipeline while maximizing the model's performance.

3.3. The Antispoofing Performance Experiment

In this section, we compared the proposed method with several leading 3D CNN architectures. All of the networks utilized the processing techniques outlined in Figure 3, with the only difference being the prediction network used. The test set consisted of 260 instances of real fingerprint volume data and 260 instances of artificial fingerprint volume data. The experimental results for the different methods are presented in Table 2.

Table 2. Comparison of results in OCT fingerprint antispoof detection.

Model	AUC	ERR	TPR@FPR = 0.1	BCPER$_{20}$
MobileNet [41]	0.991	0.044	0.804	0.582
ResNet [42]	0.997	0.023	0.973	0.051
DenseNet [43]	0.997	0.016	0.975	0.091
ResMamba	**0.998**	**0.002**	**0.990**	**0.004**

Note: The bold numbers represent the best evaluation metrics.

Notably, our method demonstrates superior performance, achieving an error rate of only 0.2%, validating its excellent antispoofing capabilities. Compared to other supervised networks, our proposed method effectively captures subtle differences in internal struc-tures, even with a limited training set. The training set comprised data from only 10 individuals with real fingerprints and 10 types of artificial materials simulating external fingerprint features. These results further prove our method's strong generalization ability in detecting synthetic samples.

As shown in Table 2, which compares the performance of MobileNet, ResNet, DenseNet, and our proposed ResMamba model, ResMamba achieves the best performance across several metrics. In particular, it shows significant advantages in terms of the AUC, error rate (ERR), and TPR at a fixed FPR (TPR@FPR = 0.1). Notably, ResMamba scored just 0.004 on the $BCPER_{20}$ metric. These results highlight that ResMamba outperforms the other methods in terms of its accuracy and antispoofing capabilities, thus underscoring its practical value for fingerprint recognition tasks.

3.4. The Runtime Performance Experiment

We evaluated the runtime performance of several CNN models using an NVIDIA GeForce RTX 3080 GPU. Table 3 presents the key metrics, including the number of parameters, GFLOPs, and inference time per volume dataset, for MobileNet, ResNet, DenseNet, and the proposed ResMamba model. In the OCT fingerprint antispoofing detection task, the full volume data must be processed to make a final decision. To ensure consistent timing, we averaged the inference time over 100 sets of OCT volume data, which consisted of 50 sets of artificial fingerprints and 50 sets of real fingerprints.

Table 3. Comparison of model parameters.

Model	Param (M)	GFLOPs	Inference Time (ms)
MobileNet [41]	3.3	1.34	2.7
ResNet [42]	33.2	43.76	24.3
DenseNet [43]	25.38	55.3	59.9
ResMamba	13.62	22.91	11

As detailed in Table 3, MobileNet is the lightest model, with just 3.3 million parameters, 1.34 GFLOPs, and the fastest inference time of 2.7 ms. Furthermore, its compact architecture reduces the model's complexity, making it more suitable for resource-constrained environments. ResNet, with 33.2 million parameters and 43.76 GFLOPs, has a more complex structure and an inference time of 24.3 ms. DenseNet, known for its dense connectivity, has 25.38 million parameters. However, its GFLOPs are the highest at 55.3, and it requires the longest inference time (59.9 ms), thus indicating its high computational demand.

In comparison, the proposed ResMamba model achieves an optimal balance between the parameter count and computational efficiency, with 13.62 million parameters, 22.91 GFLOPs, and an inference time of 11 ms. These results indicate that the ResMamba model falls between ResNet and DenseNet in terms of its performance. Furthermore, due to its optimized architectural design and the inclusion of the SIC module, it can enhance feature learning without significantly increasing the parameter count.

In summary, ResMamba offers an ideal balance between speed and model complexity, making it a competitive choice for applications that require high accuracy and computational efficiency.

3.5. The Ablation Experiment

Table 4 summarizes the results of ablation studies conducted with different SIC module configurations to evaluate its contribution to the ResMamba model's performance. The configurations were assessed using AUC, EER, TPR@FPR = 0.1, and $BCPER_{20}$.

Table 4. Ablation experiment results.

Introduction Location	AUC	ERR	TPR@FPR = 0.1	$BCPER_{20}$
No introduction	0.977	0.056	0.908	0.140
Only introduced at the model's early stage	0.986	0.015	0.983	0.009
Only in the first ResMamba layer	0.988	0.021	0.973	0.082
Only in the second ResMamba layer	0.988	0.030	0.953	0.051
Only in the third ResMamba layer	0.994	0.023	0.982	0.022
Only in all three ResMamba layers	0.981	0.070	0.866	0.224
Model's early stage + first ResMamba layer	0.992	0.034	0.869	0.649
Model's early stage + second ResMamba layer	0.994	0.014	0.971	0.033
Model's early stage + third ResMamba layer	0.986	0.005	**0.993**	0.009
Model's early stage + all three ResMamba layers	**0.995**	**0.002**	0.990	**0.004**

Note: The bold numbers represent the best evaluation metrics.

No SIC module: When the SIC module was not introduced at any stage, the model achieved an AUC of 0.977, an EER of 0.056, and a TPR@FPR = 0.1 of 0.908. However, the relatively high $BCPER_{20}$ of 0.140 indicates a limited ability to handle challenging cases and an elevated error rate.

The SIC module at specific layers: Introducing the SIC module into individual ResMamba layers yielded the following outcomes:

- **First layer only** : With an AUC of 0.988 and a TPR@FPR = 0.1 of 0.973, this configuration provided moderate improvements. However, an EER of 0.021 and a $BCPER_{20}$ of 0.082 suggest the model still struggles in certain scenarios.
- **Second layer only** : This achieved an AUC of 0.988 and an EER of 0.030, with a TPR@FPR = 0.1 of 0.953 and a $BCPER_{20}$ of 0.051, indicating strong performance in feature extraction but occasional misclassifications.
- **Third layer only** : This demonstrated the best performance among the single-layer integrations, with an AUC of 0.994, an EER of 0.023, and a TPR@FPR = 0.1 of 0.982. The $BCPER_{20}$ of 0.022 highlights its effectiveness in reducing the number of false positives and improving reliability.

SIC module in all ResMamba layers: When the SIC module was introduced across all ResMamba layers, the model achieved an AUC of 0.981 but showed increased errors, with an EER of 0.070 and a TPR@FPR = 0.1 of 0.866. The $BCPER_{20}$ of 0.224 reflects a trade-off in performance due to redundancy in feature extraction.

SIC module at the model's early stage only: Introducing the SIC module solely at the early stage resulted in significant gains. The model achieved an AUC of 0.986, an EER of 0.015, and a TPR@FPR = 0.1 of 0.983, with a $BCPER_{20}$ of 0.009, showcasing the early stage's critical role in enhancing the feature representation and robustness.

Combined configurations: The integration of the SIC module at the model's initial stage combined with specific ResMamba layers further improved the model's performance:

- **Early stage + first ResMamba layer** : Achieved an AUC of 0.992 and an EER of 0.034, with a lower TPR@FPR = 0.1 of 0.869 and a higher $BCPER_{20}$ of 0.649, indicating limited improvement in error control.
- **Early stage + second ResMamba layer** : Showed an AUC of 0.994, an EER of 0.014, and a TPR@FPR = 0.1 of 0.971, with a $BCPER_{20}$ of 0.033, reflecting a balanced trade-off between accuracy and error control.
- **Early stage + third ResMamba layer** : Demonstrated excellent performance, with an AUC of 0.987, an EER of 0.005, a TPR@FPR = 0.1 of 0.993, and a $BCPER_{20}$ of 0.009, highlighting this configuration's robustness.
- **Early stage + all ResMamba layers** : Produced the best overall results, with an AUC of 0.995, an EER of 0.002, and a TPR@FPR = 0.1 of 0.990. The lowest $BCPER_{20}$ of 0.004 emphasizes this configuration's superiority in enhancing the stability and predictive accuracy.

The experimental results demonstrate that introducing the SIC module at the model's initial stage is essential for boosting the feature extraction and overall robustness. Moreover, combining early-stage integration with selective placement in the ResMamba layers significantly enhances the model's performance. The best results are achieved with a dual-module approach involving the model's initial stage and all three RMB layers, effectively reducing the error rates, improving the performance on complex tasks, and ensuring the ResMamba model's stability and reliability.

3.6. Visualization

Figure 5 shows the results of applying the GRAD-CAM technique to visualize the features learned by the network, thus providing insights into the key information it utilizes for prediction. In particular, Figure 5a displays a volumetric slice of a real finger. The network predominantly focuses on the internal structures, as well as the surface fingerprint patterns and sweat gland features. The model's predictions demonstrate spatial continuity, indicating smooth feature representation across neighboring regions. Meanwhile, Figure 5b illustrates a spoof fingerprint that includes the internal and external structures. The network focuses on the seams formed during the fabrication, which are key indicators of fake fingerprints. By capturing these distinctive details, the network is able to make more accurate identifications. Figure 5c presents a spoof fingerprint containing only external structures. In this case, the network focuses on the contact area between the fake fingerprint and the glass surface. Given that the characteristics of these regions differ significantly from those of a real finger, the results provide important cues for the network to make accurate classifications.

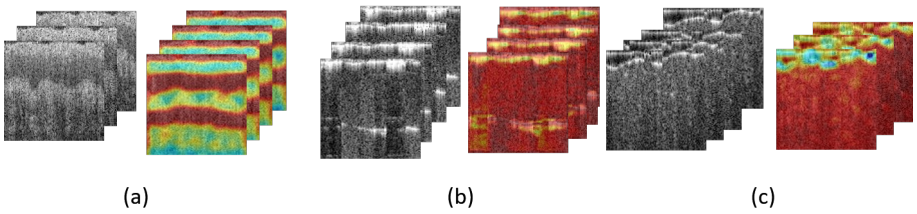

Figure 5. Grad-CAM [44]: Visualization of cross-sectional slices. (**a**) Heatmap of a cross-sectional image of a real finger. (**b**) Heatmap of a cross-sectional image of an artificial fingerprint with external fingerprint features. (**c**) Heatmap of a cross-sectional image of an artificial fingerprint with simulated internal fingerprint features (cool-toned regions indicate the neural network's focus areas).

4. Discussion

The proposed ResMamba model evinces considerable advancement in the performance of OCT-based fingerprint antispoofing detection through the integration of the selective state space module (SSM). In comparison to the most recent approaches, including ResNet, DenseNet, and MobileNet, the ResMamba model demonstrates superior results across a range of evaluation metrics. In particular, the model achieves an AUC of 0.998 and a TPR@FPR = 0.1 of 0.99 while simultaneously reducing the ERR and BCPER20 to 0.002 and 0.004, respectively. These results serve to validate the exceptional capabilities of the proposed approach in the context of fingerprint antispoofing. Moreover, the model exhibits an optimal trade-off between its inference speed and computational complexity, with an inference time of merely 11 ms and a parameter count of 13.62 M. These characteristics render ResMamba particularly well suited to resource-constrained environments.

In contrast, the existing methods were found to exhibit distinct limitations. While ResNet and DenseNet achieve strong accuracy, they are both computationally intensive and challenging to deploy in real-time applications. MobileNet offers a lightweight alternative with faster inference but lacks the precision required to handle complex spoofing scenarios. Additionally, conventional algorithms relying on single-frame B-scan images fail to leverage

the rich 3D spatial information of OCT data, resulting in reduced robustness against sophisticated spoofing techniques, such as multilayered or biomimetic materials.

While ResMamba offers a number of advantages, it is not without limitations that warrant further investigation. The model is contingent upon the availability of high-quality 3D OCT datasets, which are costly to acquire and label, thereby constraining its scalability. While the incorporation of the SSM facilitates long-range dependency modeling, the resilience of this approach to highly intricate or unconventional spoofing materials necessitates further assessment. Moreover, while ResMamba has been optimized for OCT fingerprint antispoofing, its performance in multitasking environments, such as its integration with other biometric recognition systems, remains to be investigated.

To address these limitations and enhance the model's capabilities further, a number of research avenues are proposed. Future work should concentrate on increasing the diversity and size of the training datasets in order to enhance the model's generalization across different spoofing materials and conditions. Furthermore, the development of more efficient architectures or the utilization of compression techniques could assist in reducing the computational overhead while maintaining high accuracy. The integration of OCT data with other biometric modalities, such as thermal or capacitive imaging, represents a promising avenue for enhancing the robustness of detection. Moreover, the model's application could be extended to other biometric tasks, such as palm print or iris recognition, in order to explore its adaptability across a range of domains.

Overall, the ResMamba model provides a robust and efficient solution for OCT fingerprint antispoofing, demonstrating superior accuracy and computational efficiency compared to those of the existing methods. By addressing its current limitations through data diversification, architectural refinements, and application extensions, this model's potential will be further unlocked, paving the way for the development of advanced biometric security solutions.

5. Conclusions

This study introduced the ResMamba model, a lightweight and efficient framework for OCT-based fingerprint antispoofing. It leveraged the 3D spatial continuity of volume data and a novel SIC module to address the limitations of the existing methods. The experimental results highlight several critical findings.

- **Enhanced detection accuracy and efficiency**: The ResMamba model achieved state-of-the-art performance, with an ERR of 0.2% and an AUC of 99.8%, significantly surpassing that of the traditional methods. Its lightweight architecture ensures an inference time of only 11 ms, making it suitable for real-time applications in resource-constrained environments.
- **Robustness against advanced spoofing techniques**: By fully exploiting OCT volumetric data, the model effectively distinguishes genuine fingerprints from those created using complex multilayered materials, demonstrating strong generalization capabilities even with a limited training dataset.
- **Model limitations**: Despite its advantages, the model's reliance on OCT volume data increases the computational requirements compared to those of 2D-image-based approaches. Additionally, the robustness to rare or highly sophisticated spoofing materials, such as biomimetic polymers, requires further evaluation. The model's reliance on labeled data also poses challenges for its scalability to diverse fingerprint datasets.
- **Future directions**: Future work will focus on dataset diversity, architectural optimization, and the integration of multimodal biometric data to further enhance the robustness and scalability of the proposed model.

To summarize, the ResMamba model effectively balances accuracy, efficiency, and robustness in OCT-based fingerprint antispoofing. The proposed approach demonstrates significant potential for addressing the current challenges in the field, with room for further optimization and broader dataset exploration to enhance its applicability across diverse biometric authentication systems.

Author Contributions: Conceptualization, X.M., L.A., and J.X.; data curation, X.M., Z.L., and S.Y.; formal analysis, X.M., G.L., Y.H., J.Q., and L.A.; funding acquisition, G.L., Y.H., J.Q., L.A., J.X., and J.C.; methodology, X.M., L.A., and J.X.; software, X.M., M.C., and Z.L.; validation, X.M.; visualization, X.M., L.A., and J.X.; writing (original draft), X.M.; writing (review and editing), X.M., G.L., Y.H., J.Q., L.A., J.X., and J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (62005045, and 61975030); Guangdong Basic and Applied Basic Research Foundation (2024A1515011344); Research Project of the Department of Education of Guangdong Province (2022ZDZX2055); Innovation and Entrepreneurship Team Project of the Guangdong Pearl River Talent Program (2019ZT08Y105); and Research Fund of the Guangdong–Hong Kong–Macao Joint Laboratory for Intelligent Micro–Nano-Optoelectronic Technology (No. 2020B1212030010).

Institutional Review Board Statement: The protocol was approved by the Ethics Committee of Medical Ethics Committee, Foshan University of Science and Technology (FUME2022001).

Informed Consent Statement: Informed consent for participation was obtained from all subjects involved in the study.

Data Availability Statement: The data that support the findings of this study are available upon request from the corresponding author.

Conflicts of Interest: Gongpu Lan, Yanping Huang, and Jingjiang Xu are consultants at Weiren Meditech Co., Ltd. Jia Qin, and Lin An are currently working at Weiren Meditech Co., Ltd. The remaining authors declare no conflicts of interest. The funders had no role in the design of this study; in the collection, analyses, or interpretation of the data; in the writing of this manuscript; or in the decision to publish the results.

References

1. Das, A.; Galdi, C.; Han, H.; Ramachandra, R.; Dugelay, J.L.; Dantcheva, A. Recent advances in biometric technology for mobile devices. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; IEEE: New York, NY, USA, 2018; pp. 1–11.
2. Khan, T.M.; Bailey, D.G.; Khan, M.A.; Kong, Y. Efficient hardware implementation for fingerprint image enhancement using anisotropic Gaussian filter. *IEEE Trans. Image Process.* **2017**, *26*, 2116–2126. [CrossRef] [PubMed]
3. Chugh, T.; Jain, A.K. OCT Fingerprints: Resilience to Presentation Attacks. *arXiv* **2019**, arXiv:1908.00102. [CrossRef]
4. Meissner, S.; Breithaupt, R.; Koch, E. Defense of fake fingerprint attacks using a swept source laser optical coherence tomography setup. In Proceedings of the Frontiers in Ultrafast Optics: Biomedical, Scientific, and Industrial Applications XIII, San Francisco, CA, USA, 2–7 February 2013; SPIE: New York, NY, USA, 2013; Volume 8611, pp. 49–52.
5. Ametefe, D.S.; Sarnin, S.S.; Ali, D.M.; Zaheer, M. Fingerprint liveness detection schemes: A review on presentation attack. *Comput. Methods Biomech. Biomed. Eng. Imaging Vis.* **2022**, *10*, 217–240. [CrossRef]
6. Zukarnain, Z.A.; Muneer, A.; Ab Aziz, M.K. Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. *Symmetry* **2022**, *14*, 821. [CrossRef]
7. Gamassi, M.; Lazzaroni, M.; Misino, M.; Piuri, V.; Sana, D.; Scotti, F. Quality assessment of biometric systems: A comprehensive perspective based on accuracy and performance measurement. *IEEE Trans. Instrum. Meas.* **2005**, *54*, 1489–1496. [CrossRef]
8. Xiao, Q. Technology review-biometrics-technology, application, challenge, and computational intelligence solutions. *IEEE Comput. Intell. Mag.* **2007**, *2*, 5–25. [CrossRef]
9. Sousedik, C.; Busch, C. Presentation attack detection methods for fingerprint recognition systems: A survey. *Iet Biom.* **2014**, *3*, 219–233. [CrossRef]
10. Aum, J.; Kim, J.H.; Jeong, J. Live acquisition of internal fingerprint with automated detection of subsurface layers using OCT. *IEEE Photonics Technol. Lett.* **2015**, *28*, 163–166. [CrossRef]
11. Memon, N. How biometric authentication poses new challenges to our security and privacy [in the spotlight]. *IEEE Signal Process. Mag.* **2017**, *34*, 196-194. [CrossRef]
12. Marasco, E.; Ross, A. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Comput. Surv. (CSUR)* **2014**, *47*, 1–36. [CrossRef]
13. Darlow, L.N.; Webb, L.; Botha, N. Automated spoof-detection for fingerprints using optical coherence tomography. *Appl. Opt.* **2016**, *55*, 3387–3396. [CrossRef] [PubMed]
14. Sedik, A.; El-Latif, A.A.A.; El-Affendi, M.; Mostafa, H. A Cancelable Biometric System Based on Deep Style Transfer and Symmetry Check for Double-Phase User Authentication. *Symmetry* **2023**, *15*, 1426. [CrossRef]
15. Lee, H.S.; Maeng, H.J.; Bae, Y.S. Fake finger detection using the fractional Fourier transform. In Proceedings of the Biometric ID Management and Multimodal Communication: Joint COST 2101 and 2102 International Conference, BioID_MultiComm 2009, Madrid, Spain, 16–18 September 2009; Proceedings 2; Springer: Berlin/Heidelberg, Germany, 2009; pp. 318–324.

16. Ding, Y.; Ross, A. An ensemble of one-class SVMs for fingerprint spoof detection across different fabrication materials. In Proceedings of the 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, United Arab Emirates, 4–7 December 2016; IEEE: New York, NY, USA, 2016; pp. 1–6.
17. Marcialis, G.L.; Roli, F.; Tidu, A. Analysis of fingerprint pores for vitality detection. In Proceedings of the 2010 20th International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; IEEE: New York, NY, USA, 2010; pp. 1289–1292.
18. Galbally, J.; Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. A high performance fingerprint liveness detection method based on quality related features. *Future Gener. Comput. Syst.* **2012**, *28*, 311–321. [CrossRef]
19. Park, E.; Kim, W.; Li, Q.; Kim, J.; Kim, H. Fingerprint liveness detection using CNN features of random sample patches. In Proceedings of the 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 21–23 September 2016; IEEE: New York, NY, USA, 2016; pp. 1–4.
20. Wang, C.; Li, K.; Wu, Z.; Zhao, Q. A DCNN based fingerprint liveness detection algorithm with voting strategy. In Proceedings of the Biometric Recognition: 10th Chinese Conference, CCBR 2015, Tianjin, China, 13–15 November 2015; Proceedings 10; Springer: Berlin/Heidelberg, Germany, 2015; pp. 241–249.
21. Drahansky, M.; Notzel, R.; Funk, W. Liveness detection based on fine movements of the fingertip surface. In Proceedings of the 2006 IEEE Information Assurance Workshop, West Point, NY, USA, 21–23 June 2006; IEEE: New York, NY, USA, 2006; pp. 42–47.
22. Reddy, P.V.; Kumar, A.; Rahman, S.; Mundra, T.S. A new antispoofing approach for biometric devices. *IEEE Trans. Biomed. Circuits Syst.* **2008**, *2*, 328–337. [CrossRef]
23. Huang, D.; Swanson, E.A.; Lin, C.P.; Schuman, J.S.; Stinson, W.G.; Chang, W.; Hee, M.R.; Flotte, T.; Gregory, K.; Puliafito, C.A.; et al. Optical coherence tomography. *Science* **1991**, *254*, 1178–1181. [CrossRef] [PubMed]
24. Aumann, S.; Donner, S.; Fischer, J.; Müller, F. Optical Coherence Tomography (OCT): Principle and Technical Realization. In *High Resolution Imaging in Microscopy and Ophthalmology: New Frontiers in Biomedical Optics*; Bille, J.F., Ed.; Springer: Cham, Switzerland, 2019.
25. Ding, B.; Wang, H.; Chen, P.; Zhang, Y.; Guo, Z.; Feng, J.; Liang, R. Surface and internal fingerprint reconstruction from optical coherence tomography through convolutional neural network. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 685–700. [CrossRef]
26. Darlow, L.N.; Connan, J. Efficient internal and surface fingerprint extraction and blending using optical coherence tomography. *Appl. Opt.* **2015**, *54*, 9258–9268. [CrossRef]
27. Sun, S.; Guo, Z. Sweat glands extraction in optical coherence tomography fingerprints. In Proceedings of the 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Shenzhen, China, 15–17 December 2017; IEEE: New York, NY, USA, 2017; pp. 579–584.
28. Cheng, Y.; Larin, K.V. Artificial Fingerprint Recognition by Using Optical Coherence Tomography with Autocorrelation Analysis. *Appl. Opt.* **2006**, *45*, 9238–9245. [CrossRef]
29. Bossen, A.; Lehmann, R.; Meier, C. Internal Fingerprint Identification With Optical Coherence Tomography. *IEEE Photonics Technol. Lett.* **2010**, *22*, 507–509. [CrossRef]
30. Liu, M.; Buma, T. Biometric Mapping of Fingertip Eccrine Glands With Optical Coherence Tomography. *IEEE Photonics Technol. Lett.* **2010**, *22*, 1677–1679. [CrossRef]
31. Liu, F.; Liu, G.; Wang, X. High-Accurate and Robust Fingerprint Anti-Spoofing System Using Optical Coherence Tomography. *Expert Syst. Appl.* **2019**, *130*, 31–44. [CrossRef]
32. Sun, H.; Zhang, Y.; Chen, P.; Wang, H.; Guo, Z.; He, Y.H.; Liang, R. Synchronous Fingerprint Acquisition System Based on Total Internal Reflection and Optical Coherence Tomography. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 8452–8465. [CrossRef]
33. Liu, F.; Liu, H.; Zhang, W.; Liu, G.; Shen, L. One-Class Fingerprint Presentation Attack Detection Using Auto-Encoder Network. *IEEE Trans. Image Process.* **2021**, *30*, 2394–2407. [CrossRef] [PubMed]
34. Sun, H.; Zhang, Y.; Chen, P.; Wang, H.; Liu, Y.P.; Liang, R. A new approach in automated fingerprint presentation attack detection using optical coherence tomography. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 4243–4257. [CrossRef]
35. Zhang, Y.; Yu, S.; Pu, S.; Wang, Y.; Wang, K.; Sun, H.; Wang, H. 3D CNN-based Fingerprint Anti-Spoofing through Optical Coherence Tomography. *Heliyon* **2023**, *9*, e20052. [CrossRef]
36. Gu, A.; Johnson, I.; Goel, K.; Saab, K.; Dao, T.; Rudra, A.; Ré, C. Combining recurrent, convolutional, and continuous-time models with linear state space layers. *Adv. Neural Inf. Process. Syst.* **2021**, *34*, 572–585.
37. Gupta, A.; Gu, A.; Berant, J. Diagonal state spaces are as effective as structured state spaces. *Adv. Neural Inf. Process. Syst.* **2022**, *35*, 22982–22994.
38. Gu, A.; Dao, T. Mamba: Linear-time sequence modeling with selective state spaces. *arXiv* **2023**, arXiv:2312.00752.
39. Gu, A.; Goel, K.; Ré, C. Efficiently modeling long sequences with structured state spaces. *arXiv* **2021**, arXiv:2111.00396.
40. Zhang, Y.; He, X.; Zhan, C.; Li, J. Visual State Space Model for Image Deraining with Symmetrical Scanning. *Symmetry* **2024**, *16*. [CrossRef]
41. Howard, A.G. Mobilenets: Efficient convolutional neural networks for mobile vision applications. *arXiv* **2017**, arXiv:1704.04861.
42. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.

43. Huang, G.; Liu, Z.; Van Der Maaten, L.; Weinberger, K.Q. Densely connected convolutional networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, HI, USA, 21–26 July 2017; pp. 4700–4708.
44. Selvaraju, R.R.; Cogswell, M.; Das, A.; Vedantam, R.; Parikh, D.; Batra, D. Grad-cam: Visual explanations from deep networks via gradient-based localization. In Proceedings of the IEEE International Conference on Computer Vision, Venice, Italy, 22–29 October 2017; pp. 618–626.