applied sciences

MDPI

Article

Signed Fingermark Liveness Detection Method Based on Deep Residual Networks and Multimodal Decision Fusion

Yongliang Zhang *, Zihan Zhou, Jiahang Wang and Zipeng Chen

College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China; 2112112019@zjut.edu.cn (Z.Z.)
* Correspondence: titanzhang@zjut.edu.cn

Abstract: Fingermarks play an important role in document identification. At the same time, fingermarks on paper documents are often accompanied by signatures and background text, which introduce noise to the original fingermark textures and increase the difficulty of detection. A signed fingermark detection method based on deep residual networks and a decision-level fusion strategy was proposed to defend against spoofing attacks from fake fingermarks. Firstly, the multi-scale structure was introduced in the residual module, which improved the network's depth and breadth without increasing the parameters. Then, the multi-probability label strategy was refined and employed to enhance the local encoding ability of the feature extraction. A score fusion strategy was designed, with weights allocated based on the difference in signed interference levels of local image blocks. Finally, a model fusion strategy based on evidence theory was suggested, which improved detection accuracy by leveraging complementarity between models. A large-scale fingermark database was established, which included real fingermarks made from real fingers and fake fingermarks made from various materials, and this was divided into two sub databases: signed and unsigned. The experimental results show that the proposed method achieves 96.16% accuracy based on the fingerprint dataset of the global liveness detection competition called LivDet2017 and achieves 99.30% accuracy based on the signed fingermark database, while it has good resistance to spoofing attacks from unknown materials.

Keywords: biometric recognition; signed fingermark; liveness detection; deep residual network; decision-level fusion

Citation: Zhang, Y.; Zhou, Z.; Wang, J.; Chen, Z. Signed Fingermark Liveness Detection Method Based on Deep Residual Networks and Multimodal Decision Fusion. *Appl. Sci.* **2024**, *14*, 1998. https://doi.org/10.3390/app14051998

Academic Editor: Chilukuri K. Mohan

Received: 13 February 2024
Revised: 21 February 2024
Accepted: 26 February 2024
Published: 28 February 2024

1. Introduction

Biometric technology is extensively used in modern society. With the advancements in science and technology, biometric identification has gradually replaced traditional authentication methods such as keys and passwords for personal identity authentication. Fingerprint authentication is highly reliable, easily accessible, unique, and constant, making it the most widely used and trusted method on the market [1]. Fingerprint identification technology has matured, and it is a reliable method of identification. However, it is important to acknowledge that it also presents security risks. The easy accessibility of fingerprints, compared to irises and other biometric features, is both an advantage and a vulnerability. It is crucial to address this susceptibility to spoofing attacks in order to enhance the security of identification systems. Spoofing attacks, particularly those involving artificial fingerprint replicas created using mold-making materials, pose the biggest threat to fingerprint identification systems. It is important to be aware of this common and convenient means of spoofing attack. This is due to the ease with which counterfeiters can imitate the fingerprint image by creating the corresponding fingerprint negative mold. Fingerprint liveness detection technology is a proven solution to the growing problem of spoofing attacks. Extensive research has been conducted on this technology and it is widely implemented.

Since antiquity, fingermarks, generally formed by dipping a finger in pigment or sealing clay and pressing it on paper documents, have often appeared on documents with legal

effect. In particular, fingermarks have been employed in private lending and borrowing, such as on the occasion of financing between two natural persons, based on concerns regarding the easy imitation of and the uniqueness of fingermarks, often in accordance with the traditional custom of the mixed use of signatures and fingermarks. This type of fingermark is often accompanied by signatures, text and other background noise interference, also known as signed fingermarks, and the detection of signed fingermarks is thus more difficult. Fake fingermarks can lead to false convictions, not only causing personal losses, but also affecting the credibility of justice. Traditional fingerprint authentication mainly uses manual identification methods based on expert experience, which is highly subjective and time-consuming. The existing literature on computer-based fingermark liveness detection methods is sparse, and the detection accuracy is relatively low. Based on this status quo, it is necessary to further investigate high-performance signed fingermark liveness detection methods.

The main aims of this paper are as follows:

(1) To propose a network model, SFNet (Signed Fingermark Net), based on deep residual networks and a multi-probability label classification strategy, which achieves the purpose of signed fingermark liveness detection and achieves high accuracy on a fingermark dataset.
(2) To design and combine a multi-score fusion strategy based on the quality weights of local blocks of fingermark and a model fusion strategy based on evidence theory to further improve the detection accuracy.

2. Related Works

Liveness detection methods for fingerprints can be classified as hardware-based or software-based. Hardware-based methods use additional hardware devices to obtain the biological features unique to real fingers, such as sensors that detect skin temperature [2] or bioelectrical signals [3]. However, fingermarks lack these vital features. Software-based methods use machine learning or deep learning algorithms to extract dynamic or static features from fingerprint images [4]. These methods determine the liveness of the images and are suitable for various applications, including real-time fingerprint detection and verification. They are highly compatible, cost-effective, and allow for algorithm updates at any time, without requiring additional hardware equipment. Fingermark liveness detection is better suited to static features rather than dynamic features. This is because dynamic features are easily influenced by factors such as finger pressure and skin condition, which are continuous and uncontrollable physiological changes. It is impractical to extract dynamic information from fingermarks on paper documents. Therefore, it is recommended to focus solely on static features for fingermark liveness detection.

The ridge texture is the most commonly used static feature for detecting the authenticity of fingermarks. Authentic and fake fingermarks can be distinguished based on differences in continuity, clarity, and ductility. These characteristics provide a strong foundation regarding physical properties for effective liveness detection [5–10]. It is crucial to recognize that traditional texture-based liveness detection methods heavily depend on expert knowledge of manually labeled features. However, as science and technology advance, new means of forgery emerge, making it increasingly challenging to define the characteristics of liveness in fingermark standards. If the manual features used to define the standard are targeted and avoided, these types of liveness detection methods will inevitably become ineffective.

Convolutional neural networks [11] have been widely used in computer vision. Researchers have applied deep learning to the field of fingerprint liveness detection, providing better robustness and higher performance than detection methods using manual features. Biometric methods applying deep neural networks can be combined with various score fusion strategies [12] to improve recognition accuracy. MobileNet, proposed in [13], significantly reduces the model parameters compared to VGG-19 [14]. CNN-based cross-layer fusion and multi-model voting strategies were proposed in [15] to achieve a better average

performance of the network. The DRN designed in [16] achieved good accuracy based on the benchmark dataset LivDet2017 [17,18].

Through testing, it is found that the accuracy of the method originally used for fingerprint liveness detection is not ideal after migrating to signed fingermark liveness detection. Compared with the fingerprint images obtained by a fingerprint capture device, the fingermarks obtained from paper documents through a document scanner have to pass through multiple layers of media, with relatively fuzzy texture details and noise interference, such as text, signatures, and other elements, and the influence of signatures on liveness detection is still not clear. Exploring this issue is the goal of this paper.

In order to cope with these challenges brought about by signed fingermark spoofing attacks, this paper proposes a network model, SFNet, based on a deep residual network structure and combining a multi-probability label classification strategy, designing and combining a multi-score fusion strategy based on the quality weights of the local blocks of fingermarks and a model fusion strategy based on the theory of evidence, in order to achieve the liveness detection of signed fingermarks and to achieve a higher precision based on the fingermark dataset.

3. Proposed Method

3.1. Input Data Preprocessing

The network input uses local blocks from the original fingermark image after preprocessing. This approach avoids introducing incorrect information into the network, which could result in the loss of discriminative information required for effective network training. Signed fingermarks' local blocks are preferred over those with rich textures to ensure network training effectiveness. Signed fingermark preprocessing involves foreground extraction, local block extraction, and image enhancement. The foreground region is extracted from the original fingermark image file using the color space method. An average color threshold per unit area is used to identify the effective area of the fingermark, filtering out interference items that may be similar in color to the fingermark (e.g., stamps).

The center of gravity of the foreground region, which represents the original image of the fingermark, is calculated and positioned as the central point. A sliding window with a fixed size of p × p (p = 300 pixels) is then used to intercept the local blocks by sliding in steps of 50 pixels, as illustrated in Figure 1.

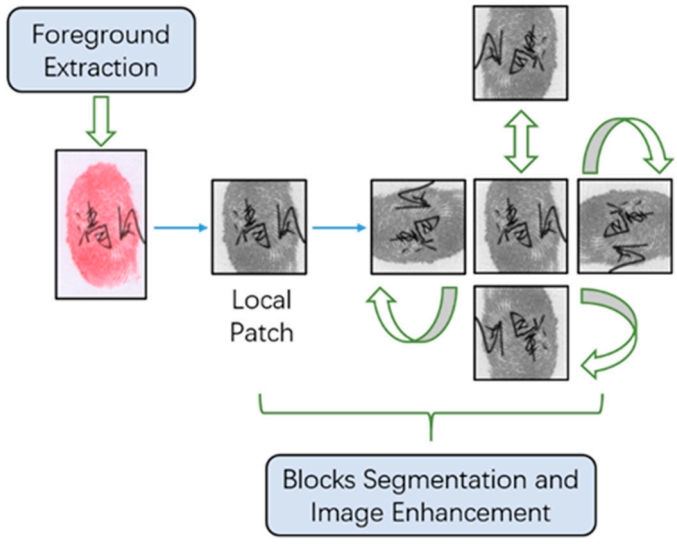


Figure 1. Local blocks and image enhancement with a sliding window, which shows a fingermark with Chinese signature.

To ensure the continuity and consistency of strokes, a larger window size should be selected for signed fingermarks, as they have complex stroke lines. This will avoid limiting

the characteristics of stroke lines and reduce the risk of accuracy reduction in liveness detection. It is important to ensure that the training data contains sufficient fingermark information and does not have a large number of blank areas. The accuracy of signed fingermark liveness detection is significantly reduced when the size of the localized blocks is too small or too large. To increase diversity and enrich the data, the intercepted local blocks are augmented with random-direction mirror flipping and random-angle rotation (rotation angles of 0°, 90°, 180°, and 270°) before being sent to the network for training. To enhance network efficiency, we convert local blocks to single-channel grayscale maps without color information. We then perform contrast enhancement based on the grayscale histogram, using the formula given in Equation (1).

$$F(s) = \text{round}\left(\frac{cdf(s) - cdf_{min}}{(w \times h) - cdf_{min}}\right) \times 255 \quad (1)$$

where w and h refer to the width and height of the image, respectively; cdf is the cumulative distribution function; s is the original gray value; and round represents the rounding function.

Enhancement of the image contrast is performed using grayscale stretching to increase the grayscale difference between the texture of the fingermark and the blank background and to reduce the effect of some of the fingermarks not being visible in the curve of the line due to too light a press.

3.2. SFNet

Figure 2 illustrates the main structure of the proposed signed fingermark liveness detection network, which consists of convolutional layers, average pooling layers, and residual blocks. The fingermark image's local features are obtained through convolutional layers. The average pooling layer downsamples the image, removes redundant information, and compresses the number of parameters to prevent overfitting. The enhanced residual structure improves the network's ability to extract high-dimensional features and filter effective features. Batch normalization layers and activation units are added after all of the convolutional layers in the network. This reduces the difference in the distribution of the training data, accelerates data convergence, improves network generalization ability, reduces parameter interdependence, and mitigates possible overfitting. The prediction results are confidently achieved through the classification layer, utilizing the feature maps of the localized blocks to accurately detect the liveness of signed fingermarks.

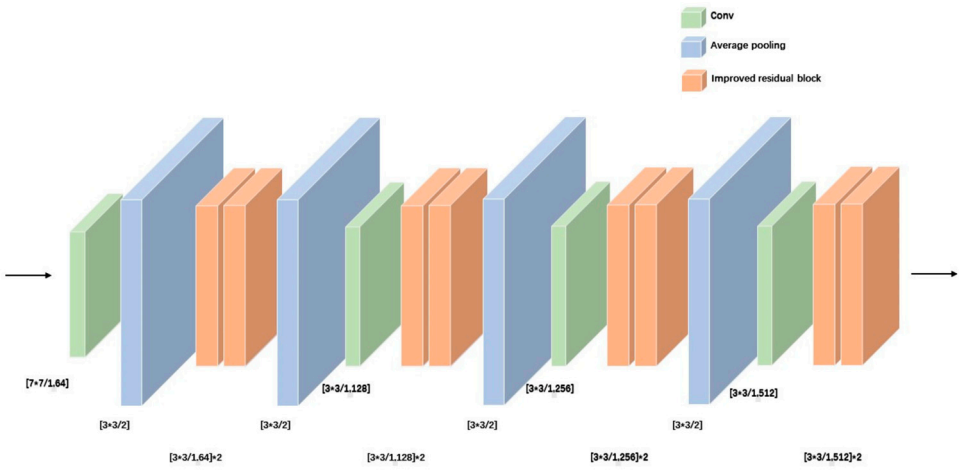


Figure 2. Structure of SFNet.

The rectified linear unit (ReLU) activation function is employed in the network's activation unit to enhance its expressive power. The loss function of the network is represented by Equation (2) and is expressed as cross entropy.

$$L = \frac{1}{N}\sum_{i} -[y_i \cdot \log(p_i) + (1 - y_i) \cdot \log(1 - p_i)] \quad (2)$$

where y_i denotes the label of sample i, p_i denotes the probability that sample i is predicted to be true, and $1 - p_i$ is the probability that sample i is predicted to be false.

The residual block in the fingermark liveness detection network combines the residual structure proposed in [19] with the multiscale backbone structure proposed in [20]. This fusion results in a structure that is better suited for the signed fingermark liveness detection network. The improved residual block structure is shown in Figure 3. The features are decomposed into multiple groups of equal-length sub-features equally by the decomposition layer, and the class residual structure is introduced between the multi-scale sub-features to deepen the chunking depth. The multiscale residual structure [20] accurately represents multiscale features at a finer granularity level, ensuring consistency in the depth of sub-features across scales. This improvement has been extended to multiple scales through the class residual structure, resulting in a significantly larger sensory field. The connection layer is successfully reorganized into a single feature and connected with the input feature residuals to form a residual block embedding network. This approach effectively improves the depth and breadth of the network without increasing the number of parameters.

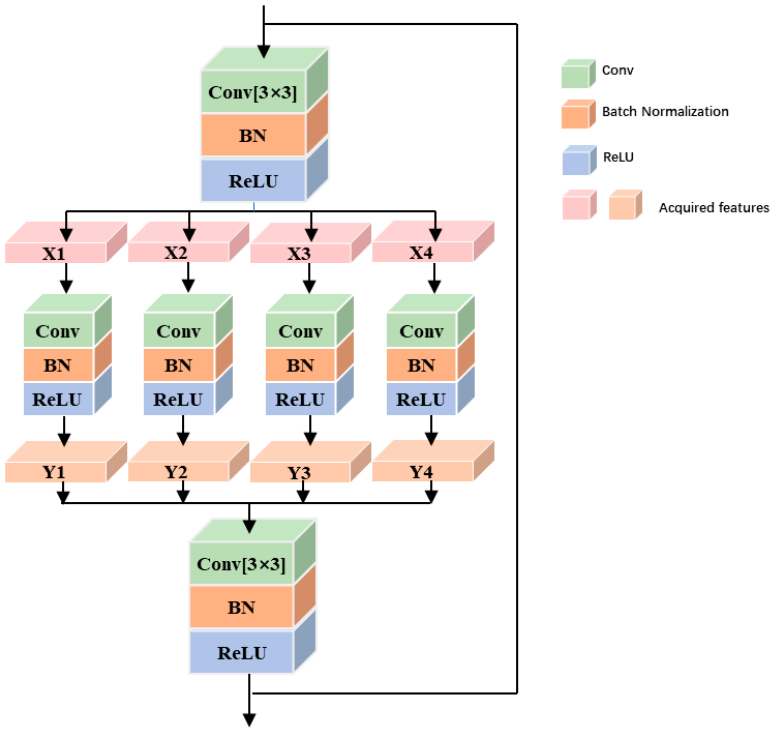


Figure 3. Improved residual block.

3.3. Multimodal Decision-Level Fusion Approach

This paper presents an improved method for detecting the liveness of signed fingermarks. The method uses a multimodal decision-level fusion approach, which includes a score fusion strategy that takes into account the quality weights of the localized blocks of the fingermarks and a model fusion strategy based on the theory of evidence. This approach is highly effective in accurately detecting the liveness of signed fingermarks.

3.3.1. Multi-Probability Labeling Strategy

The traditional classification task performs the final classification through the fully connected layer. As shown in Figure 4a, the classification label confidence prediction of the input fingermark image is performed by the fully connected layer based on the features obtained from the network.

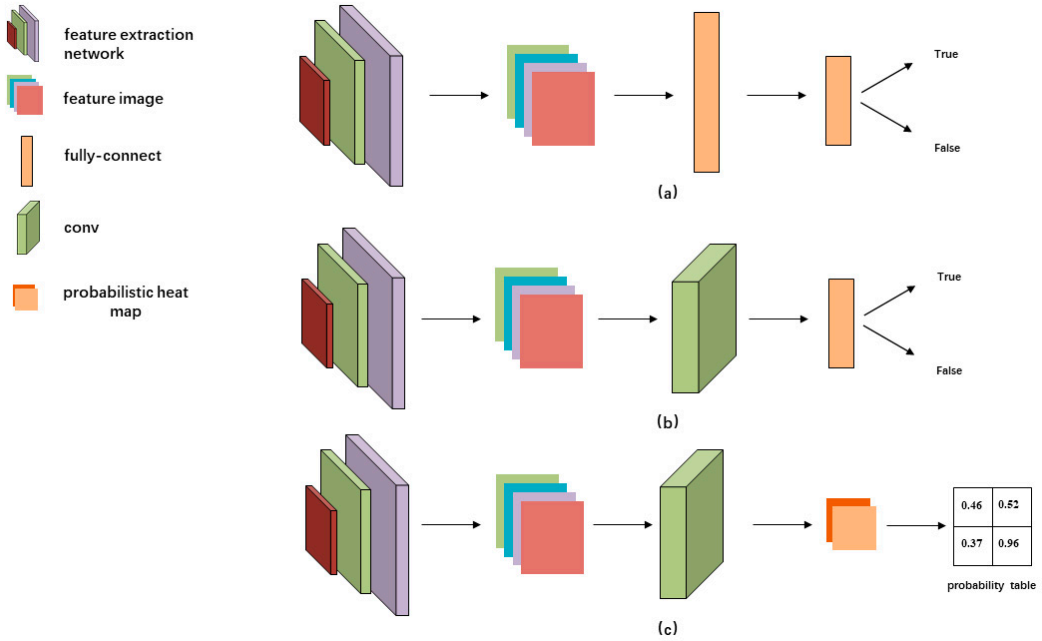


Figure 4. Different classification strategies. Where (**a**) represents Original classification strategy, (**b**) represents Improved classification strategy and (**c**) means Multi-probability labeling strategy.

SFNet replaces the first fully connected layer with a convolutional layer for dimensionality reduction prior to final classification, as illustrated in Figure 4b. This technique significantly reduces the number of parameters and computations required without sacrificing network performance.

On this basis, the multi-probability labeling strategy is proposed in combination with the patch-label strategy in [21], as shown in Figure 4c. The patch-label strategy, described in [21], involves preprocessing the image and inputting it into the Inception network. The network performs dimensionality reduction using a fully connected layer and outputs the classification probability through the convolutional layer with confidence. SFNet employs an improved labeling strategy over the patch-label approach described in [21]. The fully connected layer is replaced with a convolutional layer that achieves the same effect. The SFNet subject network takes an image of size 300 $\times$ 300 pixels as the input to generate 10 $\times$ 10 $\times$ 512 feature maps, and the convolutional layer outputs probability distribution maps of size 10 $\times$ 10 $\times$ 2. The final prediction output of the network is obtained by taking the weighted average of the weights corresponding to the 10 $\times$ 10 probability table generated after the SoftMax operation, which is trained using the ground truth label. The probability table represents a local block at the corresponding position of the input image and is utilized to train the local coding capability of the feature extraction network.

3.3.2. Score Fusion Strategy

To ensure prediction accuracy, the network typically receives only a single localized block when classifying and predicting fingermark images. This input strategy, however, can introduce randomness and reduce the robustness of the results. For this reason, we propose the multi-input score fusion strategy. We use a sliding window in the image preprocessing step to intercept multiple local blocks and feed them into the network. This results in multiple independent prediction probabilities, which we combine using the score fusion

method to calculate the final classification prediction probability, as shown in Figure 5. The final classification prediction probability of the input fingermark image is determined by utilizing the voting results of multiple prediction inputs. Equation (3) presents the calculation formula for the classification prediction probability.

$$P_{predict} = \frac{1}{N}(P(y_1|x_1) + P(y_2|x_2) + \ldots + P(y_N|x_N)) = \frac{1}{N}\sum_{i=1}^{N} p^{y_i}(1-p)^{1-y_i} \quad (3)$$

where $P(y_i|x_i)$ denotes the prediction score of the current local block, x_i denotes the current local block input to the network for prediction, y_i is the prediction label of the corresponding local block output by the network, and P is the confidence level corresponding to y_i.

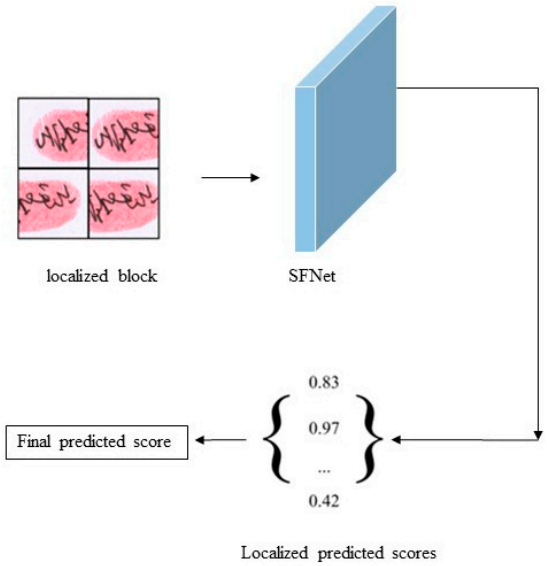


Figure 5. Score fusion via the multiple input strategy. Which shows a fingermark with Chinese signature.

However, considering that the local blocks obtained from the sliding window intercepts have an uneven texture distribution and are affected by signatures, the score fusion strategy with equal weights cannot reflect individual differences. The effective area contained in the localized block has large individual differences, and too large a background area will lead to performance degradation of the detection algorithm. In addition, the region impacted by the signed lines will affect the performance of the detection algorithm, i.e., the proportion of the signed lines in the local block is negatively correlated with the credibility of the detection results of the local block. Therefore, in this paper, we design the score fusion method based on the quality weight of fingermark localized blocks and propose the quality score calculation method based on the effective region and the proportion of signed lines, and the calculation formula is shown in Equation (4):

$$Q = \sigma Q_{ROI} + \tau Q_{Signature} = \sigma \frac{1}{w \times h}\sum_{i=1}^{w}\sum_{j=1}^{h} \varepsilon[p(i,j) - P_{ROI}] + \tau \frac{1}{w \times h}\sum_{i=1}^{w}\sum_{j=1}^{h} \varepsilon\left[p(i,j) - P_{Signature}\right] \quad (4)$$

where $\varepsilon(t - t_0)$ is the step function whose value is 1 at $t - t_0 \geq 0$ and 0 vice versa; w and h are the width and height of the localized block, respectively; $p(i, j)$ is the pixel value of the current coordinate; P_{ROI} is the threshold for distinguishing between the valid area of the fingermark and the blank background, $P_{signature}$ is the threshold for distinguishing between the signed line and the valid area; and σ and τ are correction coefficients for effective region

weights and signed line weights. From this, the quality weight of the current localized block ω can be obtained, and the calculation formula is shown in Equation (5):

$$\omega_i = Q_i / \sum_{j=1}^{n} Q_j \tag{5}$$

where Q_i is the mass fraction Q calculated from the current localized block *i*. The final prediction probability formula is obtained by improving Equation (3) by using the localized block mass fraction of the fingermark as the weight of the fraction fusion, as shown in Equation (6):

$$P_{predict} = \sum_{i=i}^{N} \{\varpi_i \cdot [P(y_i|\ x_i) - threshold]\} + threshold \tag{6}$$

where *threshold* denotes the liveness probability judgment threshold. The score fusion strategy takes into account the variation in quality distribution of the fingermark image when making liveness detection decisions using local block quality weights. This approach leverages the individual differences in local blocks to a greater extent, resulting in improved network classification performance.

3.3.3. Model Fusion Strategies Based on Evidence Theory

Fingermark liveness detection accuracy is influenced by various factors, such as the raw material type of the fingermarks and the liveness detection methods employed. Additionally, the accuracy can be affected by the use of models with different classification strategies. This paper argues that network models with different classification strategies have their own strengths and that there is a degree of complementarity between them. The accuracy of forgery detection can be further improved through the method of model fusion. Evidence theory provides a powerful tool for characterizing and fusing uncertain information for decision making. Model fusion strategies based on evidence theory are designed and used to coordinate the complementarities between different models to achieve optimal results. The experiments in this paper only address the fusion of two models.

For a problem, all possible outcomes constitute a discriminative framework denoted by θ, where θ is a non-empty set. The problem in this paper is fingermark liveness discrimination, so $\theta = \{A, B\}$, where A is true and B is false. Its power set is $2^\theta = \{\varnothing, \{A\}, \{B\}, \{A, B\}\}$.

Another important concept in the theory of evidence is the basic probability assignment (BPA), whose mass function m satisfies the following condition, as shown in Equation (7):

$$\begin{cases} m(A) \geq 0, \text{for all } A \subseteq 2^\theta \\ m(\varnothing) = m(A, B) = 0 \\ \sum\limits_{A \subseteq 2^\theta} m(A) = 1 \end{cases} \tag{7}$$

where $m(A)$ denotes the extent to which the evidence supports Proposition A. There are two mass functions, m1 and m2, in this paper. If $m(A)! = 0$, then *A* is said to be a focal element. Assuming that the focal elements are $\{A_1, A_2, \ldots, A_n\}$ and $\{B_1, B_2, \ldots, B_n\}$, in each decision, the two models are two sources of evidence, and the confidence output of their dichotomization is the evidence. In this paper, uncertainty weights are introduced to synthesize m_1 and m_2 into a new probability assignment function m_{12} according to the Dempster–Shafer combination rule, whose synthesis rule is shown in Equation (8):

$$\begin{aligned} &m_1 \oplus m_2 = m_{12}(A) = \\ &\tfrac{1}{1-K} \sum_{A_i \cap B_j = A} \alpha \cdot m_1(A_i) \cdot \beta \cdot m_2(B_j); \\ &A \neq \varnothing, K = m_1(A)m_2(A) + m_1(B)m_2(B) \end{aligned} \tag{8}$$

where α and β represent the uncertainty weights of the two models, while K is the conflict coefficient, which represents the degree of conflict between the evidence, and the size of K is positively correlated with the degree of conflict. After the BPA calculation, the joint support $m_{12}(A)$ and $m_{12}(B)$ of the two models for the classification results can be obtained. If $m_{12}(A) > m_{12}(B)$, the input image decision can then be categorized as a real fingermark, or otherwise a fake one.

4. Experiments

4.1. Database

Publicly available open source fingerprint databases are widely used in liveness detection, such as LivDet2017, FVC2002 and ATVS [22]. To verify the effectiveness of the proposed network for unsigned fingermarks, this paper first tests it on the publicly available fingerprint activity detection dataset LivDet2017, the details of which are shown in Table 1.

Table 1. Details of LivDet2017 database.

LivDet2017	Train				Test			
	Live	Ecoflex	Body Double	WoodGlue	Live	Gelatine	Latex	Liquid Ecoflex
Green Bit	1000	400	400	400	1700	680	680	680
Orcanthus	1000	400	400	400	1700	680	658	680
Digtial Persona	999	400	399	400	1700	679	670	679

However, there is no publicly accessible database of signed fingermarks. For this reason, the research team in this paper created a fingermark database containing two subsets: the unsigned fingermark dataset and the signed fingermark dataset. The original fingermarks were made from real fingers or fake fingermarks dipped in sealing clay and pressed onto paper documents. In order to simulate the real scenario, the signed fingermark data were created using paper documents with different types of signed pens, and then fingermarks were pressed, in line with the habit of signing first and pressing later. The original document was scanned by a document scanner at a resolution of 600 dpi, the original fingermark image was obtained and then cropped to a fingermark image of 500 × 300 pixels in size, and the corresponding real value label was created and categorized according to attributes (attributes include: liveness, raw material, date of collection, gender and age of the provider, etc.).

The database of fingermarks includes both live and fake fingermarks. The materials used to make fake fingermarks included all kinds of common chemical raw materials, and the specific types and quantities are shown in Table 2.

Table 2. Details of fingermark database.

Type		Train		Test	
		Signed	Unsigned	Signed	Unsigned
Live Fingermarks		32,667	25,511	8649	6459
Fake Fingermarks	Conductive silicone	6637	7500	1618	2124
	Skin color silicone	6322	3930	1440	1220
	Wood glue	5393	600	1365	160
	Clear silicone	7453	8790	1885	2343
	Fingerprint seals	5141	2280	1256	550
	Total	63,613	48,611	16,213	12,856

The fake fingermark materials include conductive silicone, skin-color silicone, wood glue, clear silicone and fingerprint seals, all of which are commonly used in previous spoofing attacks. Because it is usually difficult to distinguish between fingermarks made

using different materials with the naked eye, as shown in Figure 6, it is necessary to ensure the diversity of materials in the dataset.

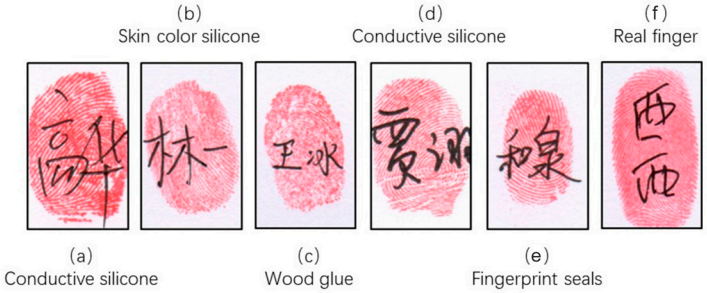


Figure 6. Fake signed fingermarks formed from different materials. Which shows a fingermark with Chinese signature.

4.2. Experimental Environment and Evaluation Indicators

In this paper, stochastic gradient descent with a batch size of 64 samples was used to train the model. The initial learning rate was set to 0.01, which dynamically reduced as the number of iterations increased. Based on the PyTorch framework with version number 1.1.0.

The experiments in this paper were evaluated in terms of test sample detection accuracy, i.e., the rate of correctly classifying the test set samples (live and fake fingermarks). In this paper, the probability scoring threshold for liveness of fingermarks was set to 0.5, and fingermark images greater than or equal to the threshold were considered as live fingermarks, otherwise they were considered as fake fingermarks.

The training samples of the network with live fingermarks and fake fingermarks were randomly distributed and fed into the network to ensure that the training data were randomized. Each fingermark had a corresponding correct label: the label of the live fingermark was set to 1, and the label of the fake fingermark was set to 0. The test samples were fed into the trained network model to obtain the prediction probabilities corresponding to the two types of data, and the prediction labels were judged according to the probability score threshold. If the predicted label of the test sample was the same as the label of the real value, the prediction was correct; otherwise, the prediction was wrong.

4.3. Analysis of Experimental Results

4.3.1. Fingerprint Verification

Although the fingermark liveness detection method is proposed for signed fingermarks, it still needs to have the basic ability to detect the liveness of unsigned fingerprints. In this paper, the SFNet model was tested on the public fingerprint dataset LivDet2017 to verify the effectiveness of the proposed network structure, and the experimental results are shown in Table 3, and the other four sets of models were from the results of the LivDet2017 competition [23]. It can be seen that compared with the four best performing algorithms in the LivDet2017 competition, SFNet achieves the optimal results in terms of detection accuracy on all sub-datasets, which indicates that SFNet has a better fingerprint liveness detection capability.

Table 3. Comparison results of detection accuracy of different models based on the LivDet2017 dataset. Unit: %.

Model	Green Bit	Digital Persona	Orcanthus	Overall
JLW_A	95.08	94.09	93.52	94.23
JLW_B	96.44	95.59	93.71	95.25
ganfp	95.67	93.66	94.16	94.50
ZYL_2	96.26	94.73	93.17	94.72
SFNet	96.82	96.64	95.27	96.16

4.3.2. Signed Fingermark Verification

Experiments were conducted in the database established in this paper to verify the effectiveness of the proposed SFNet and multi-probability labeling strategy for signed fingermarks. The network was confidently trained with unsigned fingermark data to ensure its ability to detect the liveness of unsigned fingermarks, without any interference from signed noise. SFNet models and an SFNet model incorporating a multi-probability labeling strategy were trained on a comprehensive fingermark dataset containing both signed and unsigned fingermarks (SFNet_1). The test results in Table 4 demonstrate that the signed fingermark liveness detection network has a detection accuracy of over 98%, indicating that SFNet exhibits superior liveness detection performance on both signed and unsigned fingermark datasets. The method that incorporated the multi-probability labeling strategy had higher accuracy on both signed and unsigned fingermark datasets, with 99.00% and 99.26%, respectively. This confirms that the multi-probability labeling strategy significantly improves the accuracy of liveness detection and enhances network performance.

Table 4. Detection accuracy results for SFNet and multi-probability label strategy. Unit: %.

Model	Train	Live	Fake	Overall
SFNet	Signed	98.41	98.68	98.54
	Unsigned	98.96	98.84	98.90
SFNet_1	Signed	98.49	99.00	98.73
	Unsigned	98.97	99.26	99.13
SFNet_2	Signed	70.62	67.96	69.35
	Unsigned	97.98	97.79	97.89

In order to verify the existence of signatures interfering with the liveness detection of fingermarks, a set of SFNet models incorporating a multi-probability labeling strategy is trained on the unsigned fingermark training set (SFNet_2). The model's recognition accuracy for the signed fingermark test set is significantly lower than its performance on the unsigned test set, demonstrating a failure to meet the requirements of liveness detection. This confirms that the presence of a signatures has a negative impact on the accuracy of liveness detection, underscoring the need for a signed fingermark database to be established.

The original purpose of signed fingermark liveness detection algorithms is to defend against spoofing attacks. Therefore, the ability to resist attacks from fake fingermarks made from different materials is one of the important criteria for a liveness detection method. In this paper, we test the accuracy of a signed fingermark dataset made from different materials, as shown in Table 5. It can be seen that SFNet has good detection results for all five materials in the dataset, which indicates that SFNet has high recognition accuracy for known materials and can withstand spoofing attacks from most known materials. In addition, latex was tested as an unknown material, and compared to the known materials, the number of fake signed fingermarks obtained from latex production is lower, but also has a high recognition accuracy, which indicates that SFNet has a certain degree of robustness to unknown materials.

Table 5. The performance of the network on the signed fingermark database made using different materials. Unit: %.

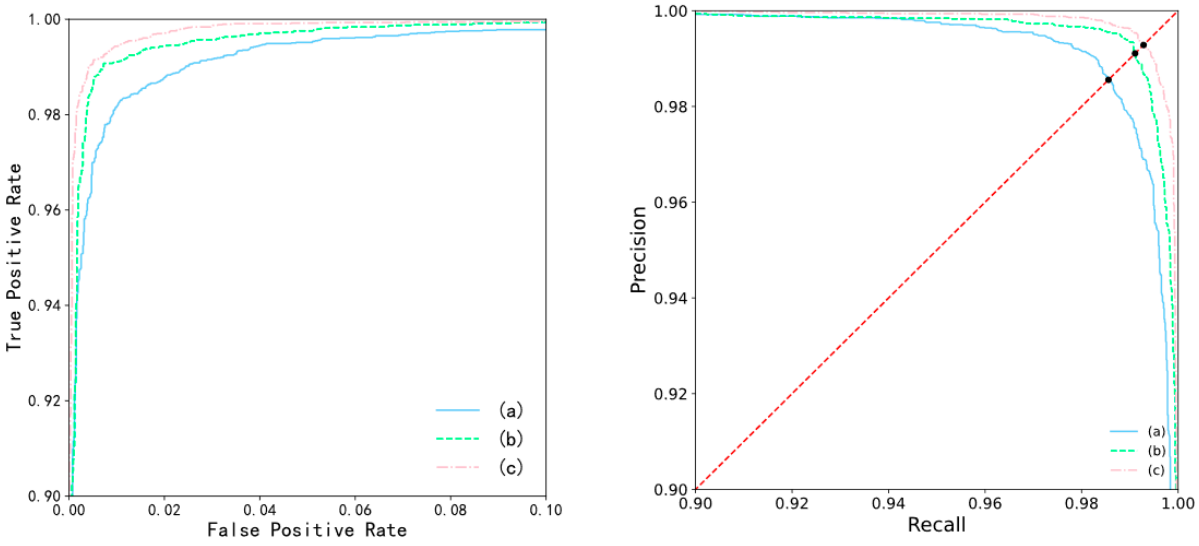
	Type	SFNet	SFNet_1
Fake	Conductive silicone	98.76	99.07
	Skin color silicone	98.68	98.12
	Wood glue	99.12	99.19
	Clear silicone	98.62	98.99
	Fingerprint seals	99.52	99.28
	Live	98.41	98.49

To verify the effectiveness of the proposed local block quality-based score fusion strategy, the effect of SFNet combined with the score fusion strategy was tested on the signed fingermark test set, and the experimental results are shown in Table 6. SFNet_3 represents the SFNet combining the multi-probability labeling strategy with the equal-weight score fusion strategy, and SFNet_4 represents the SFNet combining the multi-probability labeling strategy with the image quality-weight score fusion strategy. It can be seen that SFNet_4, which is based on the quality weight score fusion strategy, significantly improves the detection performance of the proposed method compared to SFNet without the score fusion strategy and SFNet_3, which is based on the equal weight score fusion strategy.

Table 6. Comparison of detection performance of SFNet combined with the score fusion strategy. Unit: %.

Model	Live	Fake	Overall
SFNet	98.49	99.00	98.74
SFNet_3	98.71	99.15	98.92
SFNet_4	99.08	99.27	99.17

To confirm the hypothesis that different network models enhance each other and boost the accuracy of the liveness detection method, we implemented a model fusion strategy based on the theory of evidence. We combined the original SFNet with the SFNet that integrates the multi-probability labeling strategy and the image quality weight score fusion strategy. The resulting ROC and P–R curves, depicted in Figure 7, demonstrate the success of our approach. This section compares three versions of SFNet: the original SFNet (curve a), SFNet_3 (curve b), and SFNet_4 (curve c). SFNet_3 combines the multi-probability labeling strategy and the equal weight score fusion strategy, while SFNet_4 combines the multi-probability labeling strategy and the image quality weight score fusion strategy. The figure clearly demonstrates that the AUC value and the equilibrium point value are significantly higher after fusion than the two curves before fusion, providing strong evidence for the superior performance of the fused model. These results unequivocally establish the complementarity between network models with different strategies and the effectiveness of the model fusion strategy.



(a) ROC (b) P-R

Figure 7. ROC and P–R curves after fusion.

4.3.3. Ablation and Migration

In order to demonstrate the effectiveness of the improved residual blocks, corresponding comparison experiments were conducted. The residual block in SFNet combining the multi-probability labeling strategy and the image quality weight score fusion strategy was replaced with a different residual module as the control group, and the replaced residual modules were the original residual block proposed in [19] and the Res2Net module proposed in [20], respectively. The results, as shown in Table 7, show that the test accuracies of the control group on the comprehensive test set are only 97.19% and 98.39%, while the test accuracy of SFNet combining the multi-probability labeling strategy and the image quality weight score fusion strategy using the improved residual block is 99.17%, which is a significant improvement. This result indicates that the improved residual block has higher performance in the signed fingermark liveness detection task and proves the effectiveness of the improvement.

Table 7. Comparison of detection performance of different residual blocks. Unit: %.

Model	Live	Fake	Overall
ResNet [19]	97.23	97.14	97.19
Res2Net [20]	98.23	98.58	98.39
Our work	99.08	99.27	99.17

This conclusion is based on the examination of the impact of local block sizes of training and test data on the network and showcases the importance of carefully selecting the appropriate block size for signed fingermarks. A local block size that is too small increases the effect of signatures in the image block on the fingermark texture. This paper argues that a larger localized block size is needed to obtain sufficient fingermark information and mitigate the negative effects of signed occlusion, which destroys the texture of the fingermarks. This paper presents two comparison experiments using localized block sizes of 112 × 112 pixels and 224 × 224 pixels, which are commonly used in fingermark-related studies. A control group using the original image size of 500 × 300 pixels is also included.

The results of the experiments are displayed in Table 8. It is evident that the effectiveness of the two comparison experiments with smaller sizes drops significantly, particularly for the signed fingermark test set. Notably, the accuracy falls below 90.0% when the local block size is 112 × 112 pixels. Using different local block sizes increases the interference of signatures on the texture of fingermarks in the image block, which affects the effectiveness of the algorithm for signed fingermark liveness detection. It is worth noting that the performance of the original image with a size of 500 × 300 pixels is lower than that of the image block of 224 × 224 pixels. This is due to the significant individual differences exhibited in the original images, with some samples containing numerous blank areas. Furthermore, the average effective information per unit area of the uncropped original images is much lower than that of other groups. The experiment results indicate that a larger size of localized fingermark block should be selected, as long as it contains sufficient valid information per unit area.

Table 8. The performance of the network under different local block sizes. Unit: %.

Block Size	Signed	Unsigned	Overall
112 × 112	91.02	96.13	93.26
224 × 224	95.09	97.68	96.23
300 × 300	99.08	99.27	99.17
500 × 300	93.97	95.12	94.47

Finally, other algorithms are migrated for comparison experiments with this paper's algorithm. Due to less research on fingermark liveness detection methods, this paper migrates two well-established fingermark liveness detection methods and one fingermark

liveness detection method: the Slim-ResCNN [24], the method in [25] based on the CNN architecture, and Inception [21], which combines the patch-label strategy, which is trained on a comprehensive fingermark dataset and tested on a signed fingermark dataset.

The results are shown in Table 9, and under the same conditions, the detection accuracy of these methods for signed fingermarks is not satisfactory, and the lowest accuracy is lower than 90.0%, while the SFNet proposed in this paper, which combines the multi-probability labeling strategy and the image quality weight score fusion strategy, achieves the optimal test accuracy.

Table 9. The performance of migration methods on signed fingermark database. Unit: %.

Model	Live	Fake	Overall
Slim-ResCNN [24]	92.36	91.03	91.73
An CNN architecture [25]	82.13	84.47	83.24
Inception with patch-label [21]	98.57	98.14	98.37
SFNet after model fusion	99.15	99.46	99.30

Counterfeiters may use novel materials to carry out spoofing attacks on the liveness detection algorithm. The ability of a liveness detection algorithm to resist attacks with unknown materials is also one of the criteria for judging the robustness of the algorithm. Unknown materials refer to materials that do not exist in the algorithm's training dataset. In this paper, a small dataset was created based on five unknown materials, including glass glue, vulcanized silicone, glue, emulsion, and a bionic finger. Among them, the bionic finger was made of mixed materials to simulate a real finger, which has a flexibility and ductility very close to those of real skin, and has a similar appearance and touch to a real finger.

The experimental results are shown in Table 10. It can be seen that SFNet can be effectively protected against attacks from unknown materials, which is better than other methods. It can be seen that SFNet shows a slight degradation in accuracy against bionic fingers, so further research will need to consider investigating how to defend against unknown materials with high ductility and flexibility.

Table 10. The performance of migration methods on unknown materials. Unit: %.

Type		SFNet after Model Fusion	Inception with Patch-Label [21]	Slim-ResCNN [24]
Fake	Glass glue	96.38	91.30	81.88
	Vulcanized Silicone	97.73	93.18	75.14
	Glue	98.96	91.67	83.32
	Emulsion	92.96	89.63	72.59
	Bionic finger	89.17	83.33	69.17

5. Conclusions

This paper proposes an effective method for detecting signed fingermark liveness to counter fingermark spoofing attacks and meet the needs of applications like judicial document authentication. The method is based on deep residual networks and multi-probability labels. The method combines the residual network structure and the multi-scale backbone structure to improve the accuracy of liveness detection. This is achieved through the use of a multi-probability label classification strategy, a multi-input score fusion strategy, and a model fusion strategy. The signed fingermark liveness detection method achieved a remarkable 99.17% success rate on the comprehensive dataset using different strategies, which was further improved to 99.30% after model fusion. These results demonstrate the method's high effectiveness. It is worth noting that the method can also handle signed fingermarks on special paper backgrounds, such as squares and stripes, in practical scenarios. In the future, we will study liveness detection algorithms for

signed fingermarks with complex backgrounds to significantly improve the practicality of fingermark liveness detection.

Author Contributions: Conceptualization, Y.Z.; Methodology, Y.Z.; Software, Y.Z., Z.Z. and J.W.; Validation, Z.Z. and J.W.; Data curation, Y.Z.; Writing—original draft, Z.Z. and Z.C.; Writing—review & editing, Y.Z. and J.W.; Visualization, Z.Z. and Z.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, 62102364, and the Natural Science Foundation of Zhejiang Province, LY22F020016.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author. The data are not publicly available due to privacy.

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

References

1. Zhang, Y.; Liu, C.; Xiao, G.; Fang, S. Fake Fingerprint Detection Algorithm Based on Curvelet Texture Analysis and SVM-KNN Classification. *Comput. Sci.* **2014**, *41*, 303–308.
2. Jung, H.; Lee, H. Semi-transparent reduced graphene oxide temperature sensor on organic light-emitting diodes for fingerprint liveness detection of smartphone authentication. *Sens. Actuators A-Phys.* **2021**, *331*, 112876. [CrossRef]
3. Qin, W.; Yang, F.; Liu, Y.; Wang, Z. Research on the technology of fingerprints image pickup and true-false distinguish. *Microcomput. Inf.* **2007**, *19*, 287–289.
4. Zhang, Z. Research on Fingerprint Anti-counterfeiting Technology and Detection Method. *China Secur. Prot. Technol. Appl.* **2021**, *2*, 58–60.
5. Marcialis, G.L.; Roli, F.; Tidu, A. Analysis of Fingerprint Pores for Vitality Detection. In Proceedings of the 20th International Conference on Pattern Recognition, ICPR 2010, Istanbul, Turkey, 23–26 August 2010.
6. Espinoza, M.; Champod, C. Using the number of pores on fingerprint images to detect spoofing attacks. In Proceedings of the 2011 International Conference on Hand-Based Biometrics, Hong Kong, China, 17–18 November 2011; pp. 1289–1292.
7. Nikam, S.B.; Agarwal, S. Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems. In Proceedings of the 2008 International Conference on Emerging Trends in Engineering and Technology, Nagpur, India, 16–18 July 2008; pp. 675–680.
8. Ververidis, D.; Kotropoulo, S.C. Fast and accurate sequential floating forward feature selection with the Bayes classifier applied to speech emotion recognition. *Signal Process.* **2008**, *88*, 2956–2970. [CrossRef]
9. Lyu, R.; Xia, Z.; Chen, X.; Sun, X. Fingerprint liveness detection based on weber binarized perception features. *J. Appl. Sci.* **2016**, *34*, 616–624.
10. Chen, J.; Shan, S.; He, C.; Zhao, G.; Pietikäinen, M.; Chen, X.; Gao, W. WLD: A robust local image descriptor. *IEEE Trans. Pattern Anal. Mach. Intell.* **2010**, *32*, 1705–1720. [CrossRef] [PubMed]
11. Yang, X.; Ye, Y.; Li, X.; Lau, R.Y.; Zhang, X.; Huang, X. Hyperspectral image classification with deep learning models. *IEEE Trans. Geosci. Remote Sens.* **2018**, *56*, 5408–5423. [CrossRef]
12. Gao, Z.; Xuan, H.Z.; Zhang, H.; Wan, S.; Choo, K.K.R. Adaptive fusion and category-level dictionary learning model for multiview human action recognition. *IEEE Internet Things J.* **2019**, *6*, 9128–9293. [CrossRef]
13. Chugh, T.; Cao, K.; Jain, A.K. Fingerprint spoof buster: Use of minutiae-centered patches. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2190–2202. [CrossRef]
14. Simonyan, K.; Zisserman, A. Very deep convolutional networks for large-scale image recognition. *arXiv* **2022**, arXiv:1409.1556.
15. Luo, H.L.; Lu, F.; Yan, Y. Action recognition based on multi-model voting with cross layer fusion. *J. Electron. Inf. Technol.* **2019**, *41*, 649–655.
16. Yuan, C.; Xia, Z.; Sun, X.; Wu, Q.J. Deep residual network with adaptive learning framework for fingerprint liveness detection. *IEEE Trans. Cogn. Dev. Syst.* **2019**, *12*, 461–473. [CrossRef]
17. Yambay, D.; Schuckers, S.; Denning, S.; Sandmann, C.; Bachurinski, A.; Hogan, J. LivDet 2017-fingerprint systems liveness detection competition. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–9.
18. Casula, R.; Micheletto, M.; Orrù, G.; Delussu, R.; Concas, S.; Panzino, A.; Marcialis, G.L. LivDet 2021 fingerprint liveness detection competition-into the unknown. In Proceedings of the 2021 IEEE International Joint Conference on Biometrics (IJCB), Shenzhen, China, 4–7 August 2021; pp. 1–6.
19. 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 (CVPR), Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.

20. Gao, S.H.; Cheng, M.M.; Zhao, K.; Zhang, X.Y.; Yang, M.H.; Torr, P. Res2net: A new multi-scale backbone architecture. *IEEE Trans. Pattern Anal. Mach. Intell.* **2019**, *43*, 652–662. [CrossRef] [PubMed]
21. Zhang, Y.; Gao, C.; Li, Z.; Lv, Y.; Zhu, K. A method of fingermark anti-counterfeiting for forensic document identification. *Pattern Recognit. Lett.* **2021**, *152*, 86–92. [CrossRef]
22. Raj, S.; Pannu, J.S.; Fernandes, S.L.; Ramanathan, A.; Pullum, L.L.; Jha, S.K. Attacking NIST biometric image software using nonlinear optimization. *Pattern Recognit. Lett.* **2020**, *131*, 79–84. [CrossRef]
23. Mura, V.; Orrù, G.; Casula, R.; Sibiriu, A.; Loi, G.; Tuveri, P.; Ghiani, L.; Marcialis, G.L. LivDet 2017 fingerprint liveness detection competition. In Proceedings of the 2018 International Conference on Biometrics, Gold Coast, QLD, Australia, 20–23 February 2018; pp. 297–302.
24. 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]
25. Arun, K.T.K.; Vinayakumar, R.; Sajith, V.V.V.; Sowmya, V.; Soman, K.P. Convolutional neural networks for fingerprint liveness detection system. In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems, Madurai, India, 15–17 May 2019; pp. 243–246.