Received August 25, 2020, accepted September 25, 2020, date of publication October 1, 2020, date of current version October 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3027846

A Score-Level Fusion of Fingerprint Matching With Fingerprint Liveness Detection

YONGLIANG ZHANG[1,2], CHENHAO GAO[1], SHENGYI PAN[1], ZHIWEI LI[2], YUANYANG XU[1], AND HAOZE QIU[3]

[1]College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China
[2]Hangzhou Jinglianwen Technology Comapny Ltd., Hangzhou 310014, China
[3]College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China

Corresponding author: Yongliang Zhang (titanzhang@zjut.edu.cn)

This work was supported by the Public Welfare Technology Research Program of Zhejiang Province under Grant LGF18F030008.

ABSTRACT Fingerprint-based recognition is widely deployed in different domains. However, the traditional fingerprint recognition systems are vulnerable to presentation attack, which utilizes an artificial replica of the fingerprint to deceive the sensors. In such scenarios, Fingerprint Liveness Detection (FLD) is required to ensure the actual presence of a live fingerprint. In this paper, a fingerprint matching method fused with liveness detection is proposed. Firstly, the similarity between two fingerprint images is calculated based on Octantal Neatest-Neighborhood Structure (ONNS), where the closest minutia to the central minutia is found from each sector of octant. Secondly, the FLD score of the fingerprint image is obtained by using the modified Residual Network (Slim-ResCNN). Finally, a score-level fusion is performed on the results of fingerprint matching and FLD by generating interaction features and polynomial features as the score feature vector. To classify whether a fingerprint image is a genuine live fingerprint or a spoof attack (including impostor live and fake fingerprints), the score feature vector is processed using logistic regression (LR) classifiers. The proposed method won the first place in the Fingerprint Liveness Detection Competition 2019 with an overall accuracy of 96.88%, which indicates it can effectively protect the fingerprint recognition systems from spoof attacks.

INDEX TERMS Fingerprint matching, fingerprint liveness detection (FLD), spoof attacks, score fusion.

I. INTRODUCTION

Compared with the traditional identity authentication, such as key, card, and password, biometrics are neither easy to steal nor easy to lose. Among many biometric authentication methods, such as face, iris, sound, fingerprint and gait, fingerprint has become one of the most popular and reliable identity authentication methods because of its uniqueness, invariance and universality [1]. At the same time, the security of fingerprint recognition systems has become especially important and gradually raised public's attention, because some studies have shown that fingerprint recognition systems have multiple security threats, such as using fake fingerprints to attack fingerprint sensors, communication modules, software modules, and data storage [2].

Among these attack threats, spoof attack is the most urgent problem that fingerprint recognition systems need to solve, because unlike other attacks, using fake fingerprints to attack the fingerprint sensors does not require any knowledge of the fingerprint recognition system. Previous researches have shown that fingerprint sensor can be easily deceived by fake fingerprints [3], which encourages researchers to aware the harmful of fake fingerprint attacks and devote to developing solutions for these spoof attacks. There are two methods to counterfeit fingerprint: cooperation and non-cooperation methods [4]. In cooperation method, the fake fingerprint is obtained by directly acquiring the fingerprint mold from the real finger. In non-cooperation methods, however, the fingerprint mold is indirectly formed by extracting the latent fingerprint, which is hard to fabricate for non-professional people. Then the fake fingerprint mold is filled with some materials, such as silica gel, gelatin, plasticine, and wood glue [5]. With the development of fake fingerprint attacks, the security of fingerprint recognition systems has been seriously challenged. The success rate of fake fingerprint attacks is varied from different types of sensors. For a fingerprint

The associate editor coordinating the review of this manuscript and approving it for publication was Shiping Wen.

recognition system with a capacitive sensor, only the fake fingerprint with conductive materials can be used to attack successfully. For the fingerprint recognition system with optical sensors, only 3D fake fingerprints can successfully attack. For the unlocking of mobile phones based on photoelectric screen fingerprints, both 2D and 3D fake fingerprints can be utilized to attack successfully.

Recently, many anti-spoofing methods have emerged in the field of fingerprint-based identity authentication. In literatures, there are many methods to detect whether a fingerprint is live or fake source, and the existing FLD methods can be divided into two categories: hardware-based and software-based methods [6]. The hardware-based methods try to measure fingerprint properties, such as temperature, pulse, pulse oximetry, conductivity, and blood pressure by auxiliary sensor devices. The hardware-based solutions can indeed prevent spoof attacks to some extent. However, the hardware-based methods need some professional devices to measure the inherent properties of real fingerprint, which increases the overall expenses of fingerprint recognition systems. Moreover, the additional device complicates the fingerprint recognition system, and the time of user authentication becomes longer, resulting in bad user experience. Last but not least, these hardware devices are difficult to update further once the adversary (people with ulterior motives) successfully attacks. In summary, the hardware-based methods are not the most ideal solution for FLD. The software-based methods only detect spoof behaviors by analyze the fingerprint image captured by fingerprint sensor. Compared with the hardware-based method, the software-based methods are less expensive and are more flexible to update at the software level further [7]. The software-based methods have attracted more and more scholars' attention because they are more convenient, fast, user-friendly and cost-effective. The software-based methods can be considered as a binary classification problem where a fingerprint image is classified either as a live or a spoof source.

The researches on fingerprint recognition system with anti-counterfeiting function have begun in application in market, especially integrating the anti-counterfeiting algorithm into the fingerprint recognition system. Based on the hypothesis that live and fake fingerprint images possess different textures, the score fusion approach is proposed between the score of fingerprint matching and the score of FLD by generating interaction features and polynomial features as the score feature vector. The fusion scheme effectively prevents spoof attacks on the surface of fingerprint sensor by integrating software- based FLD into fingerprint recognition system, avoiding expensive expenses by integrating additional hardware devices. Firstly, the necessity of liveness detection for fingerprint recognition system has been proved when spoof attacks appear in experiments. Secondly, the paper demonstrates how the proposed score-level fusion approach affects the performance of fingerprint recognition system. Lastly, the influence of increasing the dimensionality of the score feature vector has been analyzed in the paper. Although, the integrated fingerprint recognition system increase the False Reject Rate (FRR) of clients to some extent, it can not only reject the imposter, but also effectively prevent the spoof attack to ensure the security of fingerprint recognition system.

The rest of the paper is organized as follows. The related works are summarised in Section II. Section III describes the fusion between fingerprint matching and fingerprint liveness detection. The experimental results and analysis are shown in Section IV. Finally, we draw conclusions in Section V.

II. RELATED WORKS

As we mentioned in Section I, the paper focus on software-based FLD methods, since they are the most cost efficient. Furthermore, the software-based FLD methods can be divided into five categories, including sweat-pores based, perspiration based, skin-elasticity based, image-quality based, and texture-feature based methods [8].

Some researchers supposed that sweat pores were difficult to be reproduced in the fake fingerprints. Based on this consideration, FLD can be performed by analyzing the structure of sweat pores in the ridge line of the fingerprint image. Marcialis *et al.* [9] believed that even though some sweat pores may be retained during the fabrication process of fake fingerprints, the frequency of sweat pores in fake fingerprints was much lower than the frequency of sweat pores in live fingerprints. Therefore, they used this difference as a feature to distinguish the true and fake fingerprints. Choi *et al.* [10] used the distance feature between sweat pores as the basis for judging the authenticity of fingerprints. Manivanan *et al.* [11] proposed an automatic feature extraction based on sweat pores. They used Correlation Filters to locate the location of sweat pores in the fingerprint image, and used High-Pass Filter to extract effective sweat pore characteristics.

Some researchers observed that perspiration was a typical phenomenon of live fingers. perspiration started from the sweat pores and spread along the fingerprint ridge line with time, so that the area between the pores became black in the fingerprint image. The spatial humidity pattern can be obtained by observing multiple fingerprint images acquired in a short time. However, the fake fingerprints did not have a similar perspiration phenomenon. Schuckers *et al.* [12] proposed FLD method based on perspiration changes. Live fingerprints made the grayscale of the fingerprint ridge line uneven due to the permeability of perspiration, which was more prominent with the passage of time. However, the fake fingerprints were even in a period of time. It also showed high uniformity over time. Derakhshani *et al.* [13] proposed a method for detecting perspiration patterns. They measured the gray level between the first image and the last image in the image sequence by considering the local maximum and minimum values of the ridge signal change to measure the evolution of perspiration. The fluctuation of live fingerprints was usually higher than fake fingerprints. Because perspiration was a physiological phenomenon, it varied greatly between different subjects. In addition, it also had certain sensitivity to the environment, finger pressure, time interval, and skin condition.

The sequence of image collected on the fingerprint sensor would change due to the deformation of the finger during the pressing process. However, the skin-elasticity caused by fake fingerprint was not as good as that caused by the real fingerprint, because the skin of the real fingerprint was more elastic. Based on this observation, some researchers had proposed FLD methods based on skin-elasticity. Antonelli *et al.* [14] demonstrated that live fingerprints had better elasticity than fabricated ones, and proposed two dynamic methods based on skin distortion. In perspiration-based methods, the user was required to move the fingers while pressing it on the sensor surface to deliberately exaggerate the skin distortion. During the finger movement, a sequence of fingerprint images was acquired, and then features are extracted from the multiple fingerprint images. Jia and Cai *et al.* [15] used a series of fingerprint images to analyze the skin elasticity of the fingerprint generated during the fingerprint deformation process. Based on the greater flexibility of the live fingerprint, the live fingerprint was distinguished from the fake fingerprint. Zhang *et al.* [16] used the Thin Plate Spline model to model the distortion of live fingerprints and fake fingerprints, and the elasticity of the skin affected the way the fingers deform. Because fake fingerprints were usually much harder than human skin, the deformation of the fake fingerprint was smaller under the same deformation conditions caused by pressure in the same direction.

The material used to make the fake fingerprint was composed of organic molecules that are easy to polymerize, so the surface of the live fingerprint was usually smoother the the surface of the fake fingerprint. Some researchers assumed that fake fingerprints always produce low-quality fingerprint images. Moon *et al.* [17] claimed that the surface of fake fingerprints are likely to be coarser than live fingerprint, and utilized the wavelet transformation to analyze the coarseness of image to detect the liveness of fingerprint. Galbally *et al.* [18] evaluated the quality of fingerprint images by ridge-strength, ridge-clarity, and ridge-continuity, and effectively combined these features for liveness detection.

The above four types of FLD methods have demonstrated that various types of differences are existing between the real and spoof fingerprint. The theory of these methods can be easily explained, but the liveness detection performance needs to be further improved. In addition, these methods have some other disadvantages. In perspiration-based and skin-elasticity based approaches, features discriminating the live or fake fingerprints can be lost if the pressure was not applied correctly or the finger was not kept a fixed amount of time on the surface of sensor [19]. They both required more user cooperations to capture multiple fingerprint images and cannot be used for real-time applications. The major limitation of sweat-pore based methods is that it requires high-precision devices to capture tiny pores accurately, which was more expensive to collect high-precision fingerprint images.

Among these software-based methods, texture-feature based FLD methods have become one of the most widely studied methods. The basic idea behind this kind of methods is that spoof fingerprint images have different texture distribution from the live ones despite it is indistinguishable to human eyes. Nikam [20] applied Local Binary Pattern (LBP) histograms based on gradient to FLD for the first time and obtained good detection results where the different texture details were acquired by comparing the value of the center pixel with its adjacent pixels. The local phase quantization (LPQ) descriptor [21] is acquired by short time Fourier transform (STFT) to discriminate the differences between live samples from fake ones due to the loss of information which may occur during the replica fabrication process. Inspired by the Weber's law, Gragnaniello *et al.* [22] proposed the weber local descriptor (WLD) to prevent presentation attacks on fingerprint sensors, where the input fingerprint image is represented by extracting two-dimensional histogram features from differential excitation and square bipartite. Further, Gragnaniello *et al.* [23] proposed a new local contrast phase descriptor (LCPD) that combines gradient with local phase information together, achieving a commendable detection result on FLD. Inspired by weber local descriptor, Xia *et al.* [24] proposed a new local descriptor, named Weber local binary descriptor, which consists of the local binary differential excitation component that extracts intensity-variance features and the local binary gradient orientation component that extracts orientation features. The majority of software-based FLD methods are based on hand-crafted features where feature engineering needs to possess professional domain knowledge to extract desired feature representation. In addition, texture descriptors, a kind of shallow feature, only reflect the surface properties of the fingerprint image, but leave the intrinsic properties not extracted [25].

Recently, Convolutional Neural Networks(CNNs) have been widely used in computer vision. CNNs makes outstanding performance in image classification [26], object detection [27] and many other tasks [28], attributing to the impressive ability of extracting local features. CNNs avoid the feature engineering and can learn the high-level semantic features of image using multiple layers neural network structure. The FLDs using convolutional neural networks have gained increasing attention because of their high detection rates. This powerful tool was also employed in FLD field and achieved good detection performances. The winner of the Fingerprint Liveness Detection Competition 2015 firstly introduced pre-trained VGG model to determine whether an input fingerprint image was from live or fake [29]. However, it is difficult to optimize the feature extraction and classification simultaneously since they are designed into two separate parts. Many approaches based on CNNs have been proposed for FLD, such as MobileNet-v1 [30], VGG-19 [31], CaffeNet and GoogLeNet [32].

In order to improve the security of biometric systems, some researches combine liveness detection technology

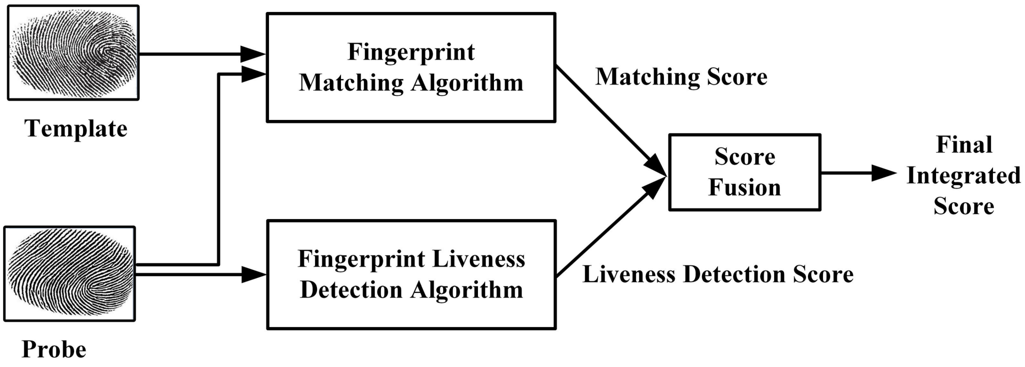


FIGURE 1. The diagram of integrated recognition system.

with biometric technology (such as fingerprints and faces). In literature [33], a countermeasure against such attacks was enhanced, where a wavelet-based liveness detection approach was integrated into the fingerprint matcher. Marfella *et al.* [34] devised proper approaches to integrate liveness detection into biometric system at score or decision level, and then tested them to assess which benefit can be obtained by smartly using vitality information in multi-biometric systems. In literature [35], Chingovska *et al.* studied techniques for decision level and score-level fusion to integrate a recognition and anti-spoofing systems, using an open-source framework that handled the ternary classification problem (clients, impostors and attacks) transparently.

However, most existing software-based FLDs only focus on FLD itself, ignoring links (integration) to fingerprint recognition systems. FLD as an independent anti-spoofing system does not have practical application value, but should be integrated into the fingerprint recognition system. The fingerprint recognition system with FLD can complete liveness detection while carrying out identity authentication. It not only maximizes the application value of FLD, but also ensures safety and efficient operation of a fingerprint recognition system.

III. PROPOSED METHOD

The application scenarios of traditional fingerprint recognition system only involve live fingerprints. The traditional recognition system is only capable of distinguishing two classes: valid users and impostors. Valid users represent registered users in the fingerprint recognition system and are regarded as positive class. Impostors represent non-registered users in the fingerprint recognition system and are regarded as negative class. With the appearance of spoof attacks, the recognition system is now confronted with three classes: valid users, impostors and spoof attacks. spoof attacks refer to artificial replicas made of commonly available materials (e.g., silicone, gelatin and plasticine) through molding, casting, or even complex 3D printing technologies. The fake fingerprints have the same texture information of valid users, which can easily deceive the traditional fingerprint recognition system and achieve the purpose of illegally entering the authorized recognition system. The fingerprint liveness detection system can only detect spoof attacks, but cannot reject impostors.

The system that we are interested in should be able to reject both impostors and spoof attacks at the same time. The impostors and spoof attacks can be merged into one enhanced negative class. When the replicas are of good quality, their score distribution may be close to, or even overlap the distribution of the valid users. It will result in a worse separability between the positive class and the enhanced negative class. To remedy this problem, the paper proposed a score-level fusion of fingerprint recognition system with anti-spoofing system. The diagram of the integrated system that we proposed is shown in Figure 1.

A. FINGERPRINT MATCHING BASED ON ONNS

The purpose of fingerprint matching is to determine whether the two fingerprint images come from the same finger by calculating the similarity of two images. Minutiae based fingerprint matching algorithms are currently widely employed, and the specific minutiae types are limited to two: endings and bifurcations (Figure 2). They can be described using parameters such as coordinates, direction and type. However, minutiae-based matching algorithms face a series of challenges, such as the location and orientation errors of detected

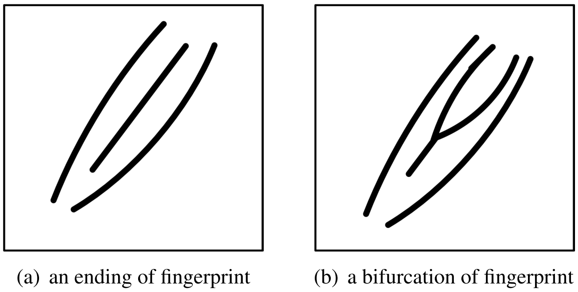

(a) an ending of fingerprint (b) a bifurcation of fingerprint

FIGURE 2. The minutiae of fingerprint image.

minutiae, the presence of spurious minutiae and the absence of genuine minutiae.

In our preliminary study [36], [37], the minutiae matching algorithm based on local feature structure, Octantal Neatest-Neighborhood Structure (ONNS), is utilized for obtaining the matching score of two fingerprint images. The fingerprint matching algorithm based on ONNS has relatively lower computational complexity and higher distortion tolerance. The algorithm constructs an ONNS for each minutia by equally dividing the area centered at the minutia into 8 sectors (angle of each sector is 45°), and the direction (θ_i) of the minutia (M_i) is considered as the initial angle. Next, the closest minutia to the central minutia is found from each sector. The ONNS of a minutia is shown in Figure 3. The local features are selected based on ONNS to measure the similarity of two fingerprint images. For more details, please refer to our preliminary work [36]. The algorithm achieves a good tradeoff between the template size and the matching accuracy, hence it is suitable for the application of real-time systems.

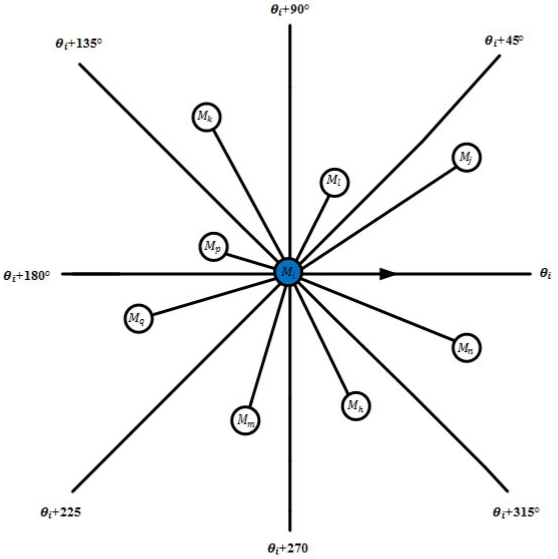
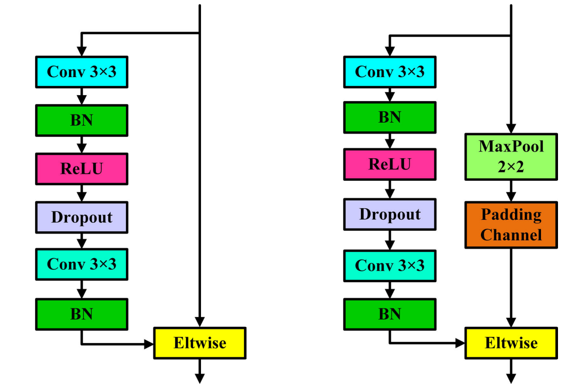


FIGURE 3. The ONNS structure of a minutia on the fingerprint image.

B. FINGERPRINT LIVENESS DETECTION BASED ON IMPROVED Slim-ResCNN MODEL

The Slim-ResCNN structure [38] in our preliminary study is used for obtaining the liveness score of input fingerprint image. The Slim-ResCNN is a relatively lightweight CNN structure. It consists of several improved residual blocks where the dropout layer is added to each pair of kernels of original residual block [39] to prevent overfitting (Figure 4 (a)). When the dimensions increase, the convolutional layer of the original residual block is replaced by padding channel with zero entries, to avoid bringing in extra parameters. Experiments had demonstrated that the Slim-ResCNN structure provided high classification accuracy for fingerprint liveness detection. More details of the Slim-ResCNN model can be found in our preliminary work [38].



(a) Improved residual block_a. (b) Improved residual block_b.

FIGURE 4. The improved residual blocks of Slim-ResCNN.

C. SCORES FUSION

The scores of the fingerprint matching and liveness detection are obtained by using the fingerprint matching algorithm based on ONNS and the liveness detection algorithm based on Slim-ResCNN respectively. To determine whether the tested fingerprint is from a legitimate user, it is necessary to weigh the confidence of the fingerprint matching $score_1$ and the liveness detection $score_2$. We construct a score feature vector based on these two scores to predict the validity of the input fingerprint image. However, simply using the matching score $score_1$ and the liveness detection score $score_2$ potentially prevents the classifier achieving high accuracy. In order to increase the post-classification performance of the classifier, we build a high-dimensional eigenvector using interaction features and polynomial features of the $score_1$ and $score_2$, which provides abundant and sufficient feature information for the classifier to enhance the separability of fingerprint images.

According to the above feature construction strategy, a 13-dimensional score feature vector can be constructed by generating interaction features and polynomial features which come from the fingerprint matching score $score_1$ and the fingerprint liveness detection score $score_2$. The 13-dimensional score feature vector F is calculated as follows:

$$\begin{aligned} F = [&score_1^{0.5}, score_2^{0.5}, score_1^{0.5} \times score_2^{0.5}, score_1, \\ &score_2, score_1^{0.5} \times score_2, score_1 \times score_2^{0.5}, \\ &score_1 \times score_2, score_1^2, score_1 \times score_2^2, \\ &score_2^2, score_1^2 \times score2, score_1^2 \times score_2^2] \end{aligned} \tag{1}$$

Although higher-dimensional score feature vectors can be utilized to achieve a better performance, this paper uses the above constructed 13-dimensional score feature vectors F to obtain a good trade-off between the performance and

TABLE 1. Device characteristics of LivDet2015 datasets.

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

TABLE 2. Device characteristics of LivDet2019 datasets.

Scanner	Model	Resolution(dpi)	Image Size(px)	Format	Type
Creen Bit	DactyScan84C	500	500×500	BMP	Optical
Orcanthus	Certis2 Image	500	$300 \times n$	PNG	Thermal swipe
Digital Personal	U.are.U 5160	500	252×324	PNG	Optical

TABLE 3. Number of samples for each scanner and each part of LivDet2015 dataset.

dataset	Live	Ecoflex	Gelatine	Latex	Wood Glue	Liquid Ecoflex	RTV
Green Bit	1000	250	250	250	250	250	250
Orcanthus	1000	250	250	250	250	250	250
Digital Persona	1000	250	250	250	250	250	250
	Live	Gelatine	Ecoflex	Playdoh	OOMOO	Body Double	
Crossmatch	1500	300	270	281	297	300	

the response delay of the fingerprint system. The Logistic Regression(LR) is further utilized to determine whether the fingerprint comes from a legitimate user. The LR, a liner model, can make our fingerprint recognition system more suitable for real-time applications. The specified training sets $\{X, Y\}$ are used to derive the weight θ of the LR classifier model; where X is a set of score feature vectors composed of F and Y is a set of discrete labels composed of "0" or "1." The formula for calculating the final integrated score $score_f$ of the fingerprint sample pair as positive sample is presented as follow:

$$score_f(y = 1|F; \theta) = \frac{1}{1 + e^{-\theta^T F}} \tag{2}$$

$score_f$ in formula (2) ranges from [0, 1], and represents the probability that the fingerprint sample pair is classified as a positive sample ($y = 1$). A higher score indicates that the fingerprint is more likely to belong to a legitimate user, otherwise the fingerprint is from an illegal intruder which may be a real fingerprint of a non-registered users or a fake fingerprint of a registered or non-registered user.

The linear models have good performance in high-dimensional datasets, but they perform poorly in low-dimensional datasets. In this paper, the original score feature vector consisting of two socres is increased into high-dimensional score feature vector by introducing interactive features and polynomial features. To some extend, it solves the problem of insufficient fitting of linear models on low-dimensional datasets and improves the separability of linear models.

IV. EXPERIMENTS

A. DATASETS

The LivDet2015 [40] dataset and the training set of LivDet2019 [41] are used in this paper. The LivDet2015 database contains four different optical devices: Biometrika, Digital Persona, Green Bit, and Crossmatch. The training set of LivDet2019 dataset is composed by sub-sets of the previous LivDet editions: the Orcanthus and Green Bit are from LivDet2017 [42] trainning set, and the Digital Persona is from LivDet 2015 trainning set. The detailed scanner characteristics of LivDet2015 and LivDet2019 datasets are reported in Table 1 and Table 2, respectively. It is worth to note that the dimensions of the images acquired with the three sensors are very different from each other, which allows us to evaluate the performance of the algorithms on the basis of the output images shape of different sensors.

For each sub-dataset in the LivDet2015 dataset, there were more than 4000 images. Live images came from multiple acquisitions of all fingers of different subjects. The entire datasets were divided into training set and testing set by using images from different subjects. The sample distribution of live and fake fingerprints in LivDet2015 dataset was shown in Table 3. The sample distribution of the training set was similar to the testing set. It was worth noting that the testing sets included spoof images of unknown materials, i.e. materials which were not included in the training set. The unknown materials are liquid Ecoflex and RTV for Green Bit, Biometrika and Digital Persona datasets, and OOMOO and Gelatin for Crossmatch dataset. This practice has been adopted to assess the reliability of algorithms under attack by unknown materials. The fake fingerprint images of LivDet2019 were collected using the cooperative method. Live image came from multiple acquisitions of at least six fingerprints of different subjects. Each dataset contains two parts. The first part is the training set and the second one is the test set. Because the test set of LivDet2019 has not been published so far, the training set is is re-divided into training set and validation set. Furthermore, the fake fingerprints on the test set were fabricated using materials different

TABLE 4. Number of samples for each scanner and each part of LivDet2019 dataset.

	Train						Test			
Dataset	Live	Wood Glue	Ecoflex	Body Double	Latex	Gelatine	Live	Mix 1	Mix 2	Liquid Ecoflex
Green Bit	1000	400	400	400	-	-	1020	408	408	408
Orcanthus	1000	400	400	400	-	-	990	384	308	396
Digital Persona	1000	250	250	-	250	250	1019	408	408	408

TABLE 5. When there are fake fingerprint attacks, the comparisons of the success rate of fingerprint recognition systems with and without fingerprint liveness detection on three test sets (%).

Datasets	Attack success rate without liveness detection	Attack success rate with liveness detection
Digital Persona	56.93	0.00
Green Bit	59.60	0.41
Orcanthus	41.30	1.94
Average	52.61	0.78

from those used in the training set. The training set consists of 6400 images, while the test set contains 6565 images. The number of samples for each scanner is shown in Table 4.

B. EXPERIMENTAL RESULTS AND ANALYSIS

In order to simulate a real scenario, all the comparisons were made with the template fingerprints belonging to live fingerprints, while the probes could be live or fake fingerprints. Only when the template fingerprint and the predicted fingerprint come from the same genuine finger, the label of the fingerprint image is marked as "1," otherwise the label is "0" in other cases.

Firstly, the necessity of liveness detection for fingerprint recognition system has been proved by simulating the scenario of spoof attacks. The traditional fingerprint recognition system can only reject the true fingerprint of the impostor live fingerprints but it is difficult to resist the fake fingerprints. In three test sets, the average success rate of fake fingerprint attacks on existing templates is as high as 52.61%, which is enough to reveal that the existing fingerprint recognition system on the market is vulnerable to fake fingerprints in real life. To protect the fingerprint recognition system from spoof attacks, this paper integrates the fingerprint liveness detection into the fingerprint recognition system. When the probe is compared with the template, the liveness detection score of the probe is calculated by the fingerprint liveness detection model trained on the corresponding fingerprint sensor. In the training set, we traine three models for liveness detection on three sub training sets. The three models were used to compute the score of fingerprint liveness detection, which means the probability that the fingerprint image belongs to genuine live fingerprints. After obtaining the scores of fingerprint matching and fingerprint liveness detection, they are merged using the fusion strategy mentioned in the previous chapter to obtain a final integrated score. The optimal threshold is selected when obtaining the highest accuracy on the training set.

When the classification accuracy on the training set is the highest, the classification threshold is recorded at this time. In the verification sets, the probe fingerprint can be judged as a genuine live fingerprint fingerprint when the final integrated score is greater than the threshold, otherwise it will be judged as impostor live fingerprint or genuine fake fingerprint. As can be seen from the Table 5, the average success rate of spoof attacks on existing templates is as low as 0.78% in the same databases. The experimental results demonstrated the fingerprint recognition is necessary to fuse the liveness detection to resist external fake fingerprint attacks.

TABLE 6. When there is no fake fingerprint attack, the impact of the fingerprint comparison on the algorithm performance with the anti-counterfeiting algorithm and without the fingerprint anti-counterfeiting algorithm on the validation sets of LivDet2019(%).

Fingerprint recognition system without liveness detection				
Database	Accuracy	Precision	TPR	FPR
Digital Persona	93.02	93.93	90.43	4.84
Green Bit	98.13	97.32	98.64	2.30
Orcanthus	93.89	94.00	92.74	5.12
Average	95.01	95.08	93.94	4.09

Fingerprint recognition system with liveness detection				
Database	Accuracy	Precision	TPR	FPR
Digital Persona	94.30	94.60	88.30	2.30
Green Biit	98.61	98.58	96.90	0.00
Orcanthus	93.98	94.48	87.60	0.50
Average	95.63	95.89	90.93	0.93

TABLE 7. The IMG_acc, IMI_acc and Total_acc of four databases on LivDet2015 dataset.(%).

database	IMG_acc	IMI_acc	Total_acc
Creen Bit	95.38	99.60	98.62
Biometrika	78.40	98.04	93.43
Digital Personal	84.47	97.50	94.46
Crossmatch	99.20	96.73	98.57

Secondly, this paper demonstrates how the fingerprint liveness detection affects the performance of fingerprint recognition system. To simulate the traditional environment without spoof attacks, the templates come from genuine liveness fingerprints, and the probe come from genuine live fingerprint or impostor live fingerprint. When the fingerprint recognition system has no liveness detection, the classification Accuracy, Precision, TPR (True Positive Rate), FPR (False Positive rate) are used to evaluate the performance of the fingerprint

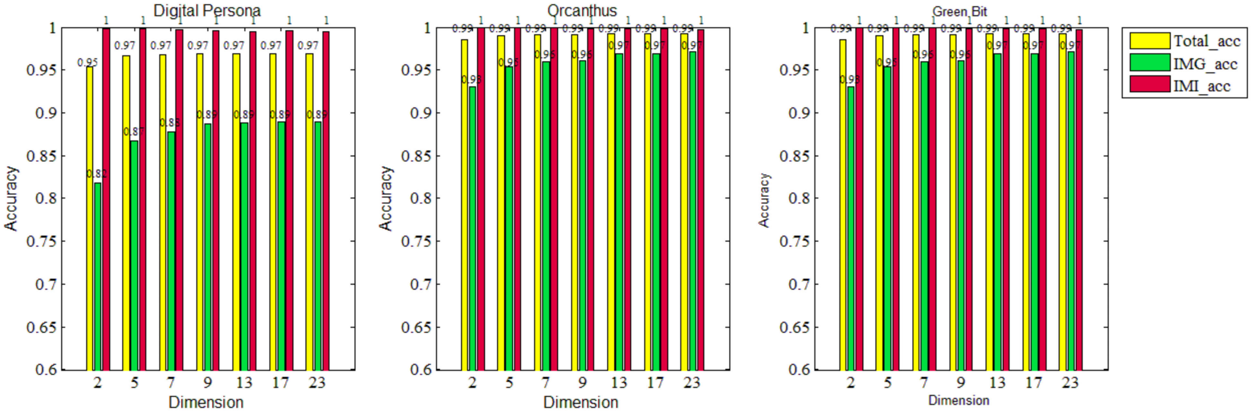


FIGURE 5. The accuracies (Total_acc, IMI_acc and IMG_acc) of score feature vectors of different dimensions (2,5,7,9,13,17 and 23) in the three validation datasets of LivDet2019 (%).

TABLE 8. IMS accuracy of the algorithms on the test sets. For each dataset the rate of correctly classified genuine live fingerprints (IMG) and the rate of correctly classified impostor live or genuine fake fingerprints (IMI) are reported. The last column is relative to the average of the total accuracy on the three datasets of LivDet2019(%).

Algorithm	Green Bit			Digital Persona			Orcanthus			Average
	IMG_acc	IMI_acc	Total_acc	IMG_acc	IMI_acc	Total_acc	IMG_acc	IMI_acc	Total_acc	
LivDet19_CNN	82.16	99.96	95.67	67.34	98.30	90.84	67.35	100.00	91.78	92.77
Unina	88.36	97.81	95.54	71.37	92.78	87.62	76.69	99.58	93.82	92.32
JLWa	99.12	96.60	97.21	89.69	90.31	90.16	92.55	95.97	95.11	94.16
JLWs	99.24	98.72	98.85	88.48	95.75	94.00	91.84	99.80	97.80	96.88
halekim	93.43	82.43	85.08	82.32	96.84	93.35	61.72	96.57	87.80	88.74
JungCNN	98.46	98.26	98.31	96.66	85.98	88.56	96.97	98.33	97.99	94.95
ZJUT_Det_A	99.51	95.89	96.76	93.07	86.65	89.37	92.55	96.01	95.14	93.76
ZJUT_Det_S	99.66	30.24	46.97	92.76	58.43	66.70	96.67	64.50	72.60	62.09

recognition. At the same time, the fingerprint recognition system with liveness detection integrated has been performed. The experimental results presented in Table 6 indicates that Whether the liveness detection is integrated into fingerprint recognition system or not makes a significant difference.

Compared with the fingerprint recognition system without fingerprint liveness detection integrated, the accuracy and precision of the fingerprint recognition system with liveness detection integrated is improved by less than 1% (Table 7). Besides, the TPRs and FPRs have dropped on three databases, which shows that the probability that positive instances are correctly predicted decreases, while the probability that negative instances are correctly predicted increases.

Thirdly, the performance of increasing the dimensionality of the score feature vector has been analyzed in the paper. It can be seen from Figure 5 that when the original feature dimensions increase, the performance is greatly improved, but after it is finally improved to a certain dimension, the change in recognition accuracy becomes stable. It can also be seen that the IMI_accuracy (Rate of correctly classified impostor or genuine fake fingerprints) is generally higher than IMG_accuracy (Rate of correctly classified genuine live fingerprint) on the three data sets. The classification accuracy of the positive samples in the GB database is generally higher than that of the other two databases. This may be because the size of fingerprint image on Green Bit database is larger, which contains abundant fingerprint information. The fusion method proposed in this paper can improve the fingerprint authentication system's resistance to spoof attacks to a certain extent, and at the same time it slightly affects the recognition performance of real fingerprints.

The effectiveness of the proposed algorithm has been evaluated on LivDet2015 and LivDet2019 datasets. Table 7 shows the IMI_acc, IMG_acc and Total_acc of the proposed algorithm on the LivDet2015. IMI_acc is generally higher than IMG_acc on the four databases of LivDet2015. Table 8 shows the results of the submitted integrated algorithm on the LivDet2019 competition, in particular the accuracy for each dataset related to correctly recognized impostors and genuine and the total accuracy calculated as an average between the three datasets. It can be seen that IMG_acc is higher than IMI_acc on the Green Bit scanner, and this trend has completely changed in the other two sensors. It may relate to the acquisition area of the sensors used: in particular, the Green Bit device has an area that covers the entire surface of the finger. A larger area allows to extract more minutiae and therefore have more points to for comparison. In particular, The Green Bit sensor has almost twice the size of captured images compared to other sensors. In LivDet2019 competition, the submitted algorithm called JLWs won the first place with an overall classification accuracy rate of 96.88%.

The final result may depend on various factors, but the fusion strategies of fingerprint matching and liveness detection score are very important. For those algorithms that perform well in fingerprint anti-counterfeiting, a better integrated algorithm may need to be designed to avoid major problems in fingerprint liveness detection, Research on integrated algorithms still requires a lot of effort. More details about LivDet2019 competition can be found in the LivDet2019 report [41].

V. CONCLUSION

FLD plays an important role in ensuring the security of the fingerprint recognition system. The paper proposes a score-level fusion method, which combines the score of fingerprint matching and the score of fingerprint liveness detection to generate a final integrated score for determination of whether the probe fingerprint is a genuine live fingerprint. Although the fake fingerprints inserted in the test set were created using materials different from those used in the training set, the experimental results show that the final integrated system we proposed achieved a compelling performance with an overall acuaracy of 96.88%. Besides, winning the first place of the International Fingerprint liveness Detection Competition (LivDet) 2019 further verify the effectiveness of our proposed fusion strategy.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[3] B. Tan and S. Schuckers, "Liveness detection using an intensity based approach in fingerprint scanner," in *Proc. Biometric Consortium Res. Symp.*, Crystal City, VA, USA, Sep. 2005, pp. 1–2.

[4] J. Domingo-Ferrer, D. Chan, and A. Watson, *Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned*. Springer, 2000, ch. 17, pp. 289–303, doi: 10.1007/978-0-387-35528-3.

[5] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics*, vol. 1, no. 1, pp. 11–24, Mar. 2012.

[6] P. Coli, G. L. Marcialis, and F. Roli, "Vitality detection from fingerprint images: A critical survey," in *Proc. Int. Conf. Biometrics*, 2007, pp. 722–731.

[7] A. S. Abhyankar and S. C. Schuckers, "A wavelet-based approach to detecting liveness in fingerprint scanners," in *Proc. Biometric Technol. for Human Identificat.*, Aug. 2004, doi: 10.1117/12.542939.

[8] Z. Xia, R. Lv, and X. Sun, "Rotation-invariant Weber pattern and Gabor feature for fingerprint liveness detection," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18187–18200, 2018.

[9] G. L. Marcialis, F. Roli, and A. Tidu, "Analysis of fingerprint pores for vitality detection," in *Proc. 20th Int. Conf. Pattern Recognit.*, Aug. 2010, pp. 1289–1292.

[10] H. Choi, "Fake-fingerprint detection using multiple static features," *Opt. Eng.*, vol. 48, no. 4, Apr. 2009, Art. no. 047202.

[11] N. Manivanan, S. Memon, and W. Balachandran, "Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering," *Electron. Lett.*, vol. 46, no. 18, pp. 1268–1269, 2010.

[12] S. A. C. Schuckers, S. T. V. Parthasaradhi, R. Derakshani, and L. A. Hornak, "Comparison of classification methods for time-series detection of perspiration as a liveness test in fingerprint devices," in *Biometric Authentication. ICBA* (Lecture Notes in Computer Science), vol. 3072, D. Zhang and A. K. Jain, Eds. Berlin, Germany: Springer, 2004. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-25948-0_36

[13] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recognit.*, vol. 36, no. 2, pp. 383–396, Feb. 2003.

[14] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 360–373, Sep. 2006.

[15] J. Jia and L. Cai, "Fake finger detection based on time-series fingerprint image analysis," in *Proc. Int. Conf. Intell. Comput.*, 2007, pp. 1140–1150.

[16] Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, "Fake finger detection based on thin-plate spline distortion model," in *Int. Conf. Biometrics*, 2007, pp. 742–749.

[17] Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, "Wavelet based fingerprint liveness detection," *Electron. Lett.*, vol. 41, no. 20, pp. 1112–1113, Sep. 2005.

[18] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710–724, Feb. 2014.

[19] E. Park, X. Cui, T. H. B. Nguyen, and H. Kim, "Presentation attack detection using a tiny fully convolutional network," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 3016–3025, Nov. 2019.

[20] S. B. Nikam and S. Agarwal, "Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems," in *Proc. 1st Int. Conf. Emerg. Trends Eng. Technol.*, 2008, pp. 675–680, doi: 10.1109/ICETET.2008.134.

[21] L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," in *Proc. 21st Int. Conf. Pattern Recognit. (ICPR)*, 2012, pp. 537–540.

[22] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Fingerprint liveness detection based on weber local image descriptor," in *Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl.*, Sep. 2013, pp. 46–50, doi: 10.1109/BIOMS.2013.6656148.

[23] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Local contrast phase descriptor for fingerprint liveness detection," *Pattern Recognit.*, vol. 48, no. 4, pp. 1050–1058, Apr. 2015.

[24] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, and Y.-Q. Shi, "A novel weber local binary descriptor for fingerprint liveness detection," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 4, pp. 1526–1536, Apr. 2020.

[25] C. Yuan, Z. Xia, X. Sun, and Q. M. J. Wu, "Deep residual network with adaptive learning framework for fingerprint liveness detection," *IEEE Trans. Cognit. Develop. Syst.*, vol. 12, no. 3, pp. 461–473, Sep. 2020.

[26] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2012, pp. 1097–1105.

[27] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Columbus, OH, USA, Jun. 2014, pp. 580–587.

[28] N. Zhang, M. Paluri, M. Ranzato, T. Darrell, and L. Bourdev, "PANDA: Pose aligned networks for deep attribute modeling," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2014, pp. 1637–1644.

[29] R. F. Nogueira, R. de Alencar Lotufo, and R. Campos Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.

[30] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: Use of minutiae-centered patches," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2190–2202, Sep. 2018.

[31] E. Marasco, P. Wild, and B. Cukic, "Robust and interoperable fingerprint spoof detection via convolutional neural networks," in *Proc. IEEE Symp. Technol. Homeland Secur. (HST)*, May 2016, pp. 1–6, doi: 10.1109/THS.2016.7568925.

[32] Y. Li, J. Zhou, F. Huang, and L. Liu, "Sub-pixel extraction of laser stripe center using an improved gray-gravity method," *Sensors*, vol. 17, no. 4, p. 814, Apr. 2017.

[33] A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," *Pattern Recognit.*, vol. 42, no. 3, pp. 452–464, Mar. 2009.

[34] L. Marfella, E. Marasco, and C. Sansone, "Liveness-based fusion approaches in multibiometrics," in *Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl. (BIOMS)*, Sep. 2012, pp. 1–7, doi: 10.1109/BIOMS.2012.6345779.

[35] I. Chingovska, A. Anjos, and S. Marcel, "Anti-spoofing in action: Joint operation with a verification system," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2013, pp. 98–104, doi: 10.1109/CVPRW.2013.22.

[36] Z. Yongliang, "Research on algorithm of sliding fingerprint splicing and fingerprint matching," Ph.D. dissertation, Pattern Recognit. Inst., Shanghai Jiao Tong Univ., Shanghai, China, 2006.

[37] Y. Zhang, S. Fang, B. Zhou, C. Huang, and Y. Li, "Fingerprint match based on key minutiae and optimal statistical registration," in *Biometric Recognition. CCBR* (Lecture Notes in Computer Science), vol. 8833, Z. Sun, S. Shan, H. Sang, J. Zhou, Y. Wang, and W. Yuan, Eds. Cham, Switzerland: Springer, 2014, doi: 10.1007/978-3-319-12484-1_23.

[38] Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu, and Z. Li, "Slim-ResCNN: A deep residual convolutional neural network for fingerprint liveness detection," *IEEE Access*, vol. 7, pp. 91476–91487, 2019.

[39] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 770–778, doi: 10.1109/CVPR.2016.90.

[40] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition 2015," in *Proc. IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2015, pp. 1–6, doi: 10.1109/BTAS.2015.7358776.

[41] G. Orrù, R. Casula, P. Tuveri, C. Bazzoni, G. Dessalvi, M. Micheletto, L. Ghiani, and G. Luca Marcialis, "LivDet in action–fingerprint liveness detection competition 2019," 2019, *arXiv:1905.00639*. [Online]. Available: http://arxiv.org/abs/1905.00639

[42] V. Mura, G. Orru, R. Casula, A. Sibiriu, G. Loi, P. Tuveri, L. Ghiani, and G. L. Marcialis, "LivDet 2017 fingerprint liveness detection competition 2017," in *Proc. Int. Conf. Biometrics (ICB)*, Feb. 2018, pp. 297–302, doi: 10.1109/ICB2018.2018.00052.

YONGLIANG ZHANG received the B.S. and M.S. degrees from Jilin University, China, in 2000 and 2003, respectively, and the Ph.D. degree from Shanghai Jiao Tong University, China, in 2007. He is currently an Associate Professor with the College of Computer Science and Technology, Zhejiang University of Technology. His research interests include biometric identification, pattern recognition, and artificial intelligence.

CHENHAO GAO graduated from the School of Computer Science and Technology, Zhejiang University of Technology, China, in 2018, where he is currently pursuing the master's degree in software engineering. His research interests include biometric recognition and machine learning.

SHENGYI PAN was born in Hangzhou, China, in 1999. He is currently pursuing the B.E. degree in computer science with the Zhejiang University of Technology, China. His research interests include biometric recognition, computer vision, and machine learning.

ZHIWEI LI received the M.S. degree from the Center for Optics and Optoelectronics Research, College of Science, Zhejiang University of Technology, China, in 2016. He is currently an Algorithm Engineer with Hangzhou Jinglianwen Technology Company Ltd. His research interests include biometric recognition, machine learning, and digital forensic.

YUANYANG XU was born in Hangzhou, China, in 1999. He is currently pursuing the B.S. degree with the College of Computer Science and Technology, Zhejiang University of Technology, China. His research interests include image processing, biometric identification, and machine learning

HAOZE QIU is currently pursuing the bachelor's degree with Zhejiang University. He worked as an Intern with Jinglianwen Technology Company Ltd. His research interest includes biometric recognition.