 CMC, vol.53, no.4, pp.357-372, 2017

Fingerprint Liveness Detection from Different Fingerprint Materials Using Convolutional Neural Network and Principal Component Analysis

Chengsheng Yuan[1, 2, 3], Xinting Li[3], Q. M. Jonathan Wu[3], Jin Li[4,5] and Xingming Sun[1,2]

Abstract: Fingerprint-spoofing attack often occurs when imposters gain access illegally by using artificial fingerprints, which are made of common fingerprint materials, such as silicon, latex, etc. Thus, to protect our privacy, many fingerprint liveness detection methods are put forward to discriminate fake or true fingerprint. Current work on liveness detection for fingerprint images is focused on the construction of complex handcrafted features, but these methods normally destroy or lose spatial information between pixels. Different from existing methods, convolutional neural network (CNN) can generate high-level semantic representations by learning and concatenating low-level edge and shape features from a large amount of labeled data. Thus, CNN is explored to solve the above problem and discriminate true fingerprints from fake ones in this paper. To reduce the redundant information and extract the most distinct features, ROI and PCA operations are performed for learned features of convolutional layer or pooling layer. After that, the extracted features are fed into SVM classifier. Experimental results based on the LivDet (2013) and the LivDet (2011) datasets, which are captured by using different fingerprint materials, indicate that the classification performance of our proposed method is both efficient and convenient compared with the other previous methods.

Keywords: Fingerprint liveness detection, CNNs, PCA, SVM, ROI, LivDet 2013, LivDet 2011.

[1] School of Computer and Software, Nanjing University of Information Science & Technology, Ning Liu Road, No. 219, Nanjing, China, 210044

[2] Jiangsu Engineering Center of Network Monitoring, Ning Liu Road, No. 219, Nanjing, China, 210044

[3] Department of Electrical and Computer Engineering, University of Windsor, 401 Sunset Avenue, Windsor, ON, Canada N9B 3P4

[4] School of Computer Science, Guangzhou University, Yudongxi Road 36, Tianhe District, Guangzhou, China, 510500.

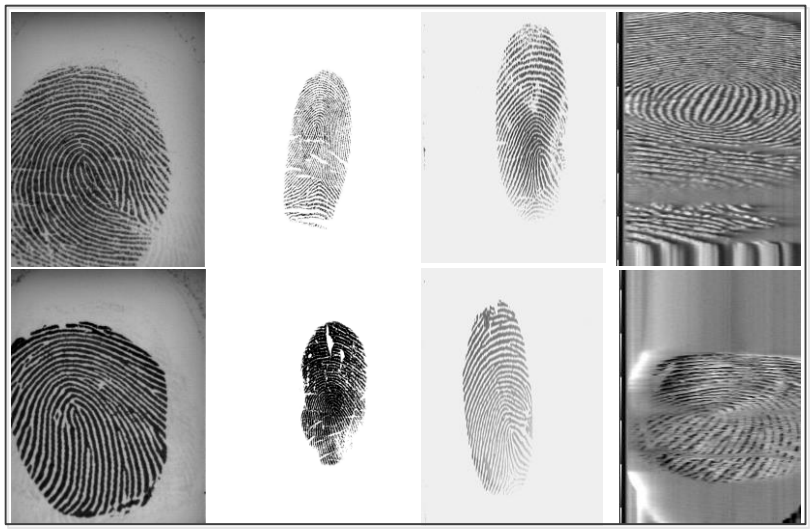
[5] The corresponding author: Jin Li, E-mail: jinli71@gmail.com

1 Introduction

Benefiting from the high-speed development of computer multimedia technology, current image sensors can acquire large number of fingerprints images with high resolution. In addition, the information of protecting users' identity and data has become crucial, since users' devices are filled with various sensible data. Therefore, accurate discrimination using such massive fingerprints has become urgent need in fingerprint recognition or authentication. In traditional authentication schemes knowledge-based, passwords or special tokens are used to verify users' identities and privacy information. On the one hand, we admit that these methods bring much convenience for personal privacy information; on the other hand, nowadays many studies have found that those traditional recognition methods are easy to suffer from illegal attacks, such as stolen, forgotten or lost attacks. Because of several of inherent properties: universality, uniqueness and durability, biometric identity techniques have aroused widespread concern in recent years [Ghiani et al. (2013); Zhou (2017); Wang (2016)]. Passwords in the traditional schemas can be reset once being lost or stolen, while the biometric characteristics cannot be reset as well as assessing users' identities by analyzing their behavioral or physiological traits. Most notably, biometric recognition technology based on fingerprint traits is the longest time and the most extensively used methods due to higher security and more convenience. Unfortunately, Marcialis, Lewicke, Tan et al. (2009) pointed out those fingerprint recognition systems are easy to suffer from spoofing attacks by fake fingerprints produced from general materials such as silicon, silicone or latex, under cooperative or non-cooperative scenarios using different methods in Kim et al. (2016). These artificial fingerprints try to fuse these fingerprint recognition systems when touching fingerprint sensors, thus, an outstanding fingerprint recognition system must correctly discriminate a spoof fingerprint from authentic ones prior to authentication. For this reason, how to prevent spoofing attacks becomes a huge challenge in the research filed of fingerprint authentication.

In the past decades, many researchers and scholars have devoted considerable effort to research and explore more efficient countermeasures against spoofing attacks to address the above issues [Zhou (2016); Wang (2016); Tian and Chen (2017)]. Most predominantly, fingerprint liveness detection is one of the many countermeasures to prevent fake fingerprint spoofing attacks. Fingerprint liveness detection can be thought of as a pattern-recognition and classification task analyzing unstructured data for purposes towards improving recognition accuracy of fingerprint detection. After study and analysis of the existing liveness detection methods, several anti-spoofing methods have been proposed in the fingerprint liveness detection, which are broadly categorized into two groups: hardware-based and software-based methods. With the help of specific sensor devices, in general, hardware-based methods need to measure intrinsic properties of given fingerprints, such as oxygen saturation, skin distortion or odor, etc. Added fingerprint sensor devices for measurement are the key to measure properties of given fingerprints in these methods of Marasco and Sansone (2012); Chen, Sun, Tobe et al. (2017); Sumon (2017); Yuan, Xia and Sun (2017). Nevertheless, fingerprints are extremely influenced by the external environment and captured devices, so classification performance based on these methods is still not satisfied with the requirements of current

fingerprint recognition systems [Jia, Cai, Zhang et al. (2007); Pereira and Pinheiro (2013)]. To provide a much lower cost and higher detection performance, software-based detection methods are popularly studied for more flexible, much cheaper and less invasive, which are used in this paper. Fake fingerprints in the latter methods are distinguished from authentic ones by using image processing technique to extract and analyze dynamic or static features of given fingerprint images. Meanwhile only one or a few fingerprints in these methods rather than fingerprints sequences [Yuan and Xia, (2016)] used to discriminate the fingerprint liveness compared with hardware-based detection methods. Besides, texture features extraction of given fingerprints in the software-based methods is the key step to distinguish real or fake fingerprints.



(a) (b) (c) (d)

Figure 1: Fingerprint samples from live (above) and fake (below) fingerprints acquired with 4 different sensors. (a) Biometrika. (b) Crossmatch. (c) Italdata. (d) Swipe.

Since texture features of real fingerprints in continuity, clarity and ridge strength are different from fake ones [Galballym, Marcel and Fierrez (2014); Manivanan, Memon and Balachandran (2010); Choi, Kang, Choi et al. (2011); Marcialis, Roli and Tidu (2010)]. Thus, many feature descriptors based on texture feature have been proposed and used to detect the fingerprint liveness. LBP (Local Binary Pattern) is a gray-scale and rotation invariant feature descriptors [Yuan and Sun (2016)], and it has been widely explored in the fields of computer vision, such as camera identification [Celiktutan, Sankur and Avcibas (2008)], face recognition, etc. Fingerprint liveness detection based on LBP method firstly was used in Nikam and Agarwal (2008), whose energy features of wavelet-domain are complemented by the LBP descriptor. Discriminative feature vector representations, composed of orientation component and differential excitation of each pixel value, are computed by using Weber Local Descriptor (WLD) in Gragnaniello, Poggi, Sansone et al. (2013). WLD is a robust to illumination change and powerful

texture features descriptor, and it is adapted for high-contrast patterns. Finally, feature representative vectors based on statistical joint histograms of orientation components and differential excitation are fed into SVM classifier. A novel local feature vector associated with liveness detection is proposed in Gragnaniello, Poggi, Sansone et al. (2015), and a bi-dimensional contrast-phase histogram is built by statistical information on the phase (frequency domain) and the local amplitude contrast (spatial domain). The local phase for the purpose of fingerprint liveness detection was used to detect the fingerprint liveness in Ghiani, Marcialis and Roli (2012), whose theory is similar to LBP. Binaried Statistical Image Features (BSIF) was presented in Ghiani et al. (2013), in which the features were represented through counting fingerprint patches and maximizing the statistical independence of the filter responses rather than a fixed set of filters. A combined method, including convolutional neural networks (CNN) with random weights and Local Binary Patterns (LBP), was used to detect the fingerprint liveness in Nogueira, Lotufo and Machado (2014). Then, extracted feature representations are fed into a RBF support vector machine (SVM) classifier. We found that most of the aforementioned feature extraction detection methods are handcrafted features, which heavily depend on the experience and domain knowledge of experts, meanwhile, these methods ignore spatial information. Thus, the representative power of the extracted features based on hand-crafted is limited, and the classification performance is not satisfactory. Furthermore, the traditional approach of fingerprint liveness detection is based on the cost of heavy burden of manual annotation. The workload of manual annotation will also increase when the number of images increases. Meanwhile, manual annotation is influenced by subjective factors, resulting in inaccurate classification. With the development of deep learning technology, more and more people start to focus on how to learn those discriminate features directly from original natural image without any image processing. Moreover, feature extraction methods based on deep learning, such as convolutional neural network technology (CNN), have made great achievements in computer vision and pattern recognition including image classification because of its strong feature self-learning capabilities, so this paper focuses on how to apply the convolutional neural networks to the field of fingerprint liveness detection. In Nogueira, Lotufo and Machado (2014); Wu and Li (2016), convolutional neural network technology is for the first time to be used to detect the fingerprint liveness, and the detection result is satisfactory. Through the research and study of above paper, we think that the convolutional operation process is regarded as process of feature extraction. Then, the learned features based on CNN are fed into SVM classifier to obtain a classification result in this paper, and this is the main idea of our paper. Different from above paper, an improved CNN with PCA method after convolutional and pooling operation is proposed in this paper. PCA operation is applied into this paper to reduce the dimensionality of learnt features between each convolutional and each pooling operations. Besides, another advantage based on ROI preprocessing operation in this paper is to get rid of the impact of invalid region. After above operations, high-level semantic features of fingerprint images have been automatically learnt from preprocessed labeled fingerprints images, and then SVM classifier is used for the classification of these extracted features. Next, a classifier model is established by using training fingerprint images. Finally, the performance of model is estimated by using

testing fingerprint images. Predominantly, the major contributions of our paper can be summarized as follows:

1) Different from traditional fingerprint liveness detection method, the original fingerprint image is regarded as the input data. As shown in Figure 1, we found that the original fingerprint images are made up of ridge and valley alternation, which are caused by the contact of a fingertip with the sensor. The other region is regarded as no effective information except ridge and valley alternation, affecting the final trained model. Thus, ROI is performed to remove those invalid areas of given fingerprint images, then preprocessed images and given labels are as the input data of the following layers rather than the original fingerprint image including invalid information.

2) The representative power of the extracted features based on hand-crafted is limited in the traditional method, and the classification performance is not satisfactory. Besides, the cost of manual annotation is heavy burden for fingerprint liveness detection in the traditional method. Thus, it limits the development of traditional detection method. However, deep learning can automatically learn the high-level semantic features from the original images. The process of convolutional operation and pooling operation is considered as feature extraction, but the vast majority of learnt features are invalid (which means that there are many zero elements in the feature maps, and they are invalid). PCA operation is introduced for each convolutional operation or pooling operation (PCA is only operated for pooling operation in the first three layers) to get rid of useless elements and reduce the dimensionally of features vectors.

3) Besides above advantages, our method can solve the overfitting issues through using PCA, which remove useless features and reduce the number of parameter pairs between two adjacent layers. Finally, greatly accelerate the training process and improve the classification performance of fingerprint liveness detection. Our method was evaluated on the LivDet 2013 and LivDet 2011 databases without dataset augmentation, and experimental results show that our method are superior to other latest methods using SVM classifier.

The remainder of this paper is organized as follows. In Section 2, Methodology is presented at first, including our designed model structure and the basic theoretical foundation of CNN. The experimental results and analysis is reported in Section 3. Conclusions are finally drawn in Section 4.

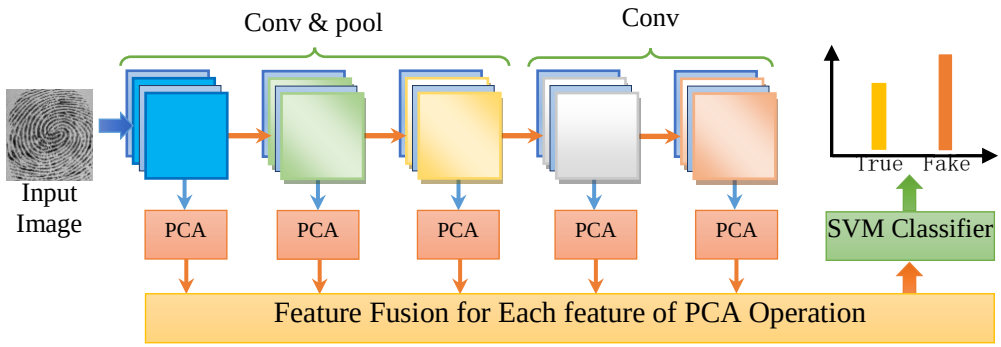


Figure 2: Flowchart of our method. (Conv denotes convolution operation, and pool denotes pooling operation)

2 Methodology

The goal of this paper provides a detection approach to correctly discriminate fake fingerprint from given ones prior to fingerprint recognition. Most of the traditional algorithms are designed by using handcrafted features, in which the experience and professional knowledge of image processing is the key to classification. Additionally, there is no actual value for researchers by statistic and computing features of pixel level. Deep learning (DL), such convolutional neural network, is able to automatically learn some structural feature representations from raw pixel values by combining low-level features to yield high-level semantic features, in which it overcomes the defect of conventional detection methods. Figure 2 shows the flowchart of our proposed method network, in which the dotted line window is the core of our method. In this paper, we for the first time introduce the PCA technique to convolutional neural network frame to handle the problem of fingerprint liveness detection, and achieved a state-of-the-art detection performance in LivDet 2013 and LivDet 2011 datasets.

2.1 Region of interest and principal component analysis

In the traditional deep learning, it can automatically learn more abstract high-level semantic feature representations layer-by-layer combination of low-level features from these original images. For those fingerprint images, alternating ridges and valleys of fingerprints are valid information, and other regions are invalid information. Region of interest is introduced in this paper, which can reduce the calculation time and remove those invalid regions. As shown in Figure 1, we list some fingerprint examples. In many research areas and applications, multivariate large samples will undoubtedly provide a wealth of detailed information, but also to a certain extent, increase the workload of data collection, more importantly; there may be a number of variables between the correlations in most cases. The computational complexity of the problem analysis increases, while the analysis is inconvenient. Therefore, it is necessary to find a reasonable way to reduce the need to analyze the indicators at the same time, as far as

possible to reduce the original index contains information loss in order to achieve a comprehensive analysis of the collected data purposes. Because there is a certain correlation between the variables, it is possible to synthesize the various types of information in each variable with fewer comprehensive indexes. Principal component analysis and factor analysis fall into this dimensionality reduction approach. Principal component analysis (PCA) is a statistical method, in which main function refers that reduces data redundancy and convert a set of variables that may be relevant by orthogonal transform into a set of linearly irrelevant variables. At the same time, PCA can eliminate the impact of assessment indicators. In the principal component analysis, the principal components are arranged in order according to the size of the variance. When the problem is analyzed, some zero elements of the feature maps are discarded, and only some effective components with large variance used to represent the original feature vectors, thus reducing the computational workload. Thus, PCA can solve the problem of high-dimensional data, which can reduce these dimensionalities of feature vector sets and cost of calculation and storage.

2.2 Convolutional neural network

Five layers, which are input layer, convolutional layer, pooling layer, full connection layer and output layer, are included in the traditional convolutional neural network. The convolutional layer can be described as the feature representations of these given images, and it can generate abstract high-level deep features by combining some low-level features. Thus, it has been widely used in computer vision, pattern recognition, etc. Because images have static attribute, it means that some useful features in an image area are most likely applied equally for adjacent to above image region, pooling operation is implemented after each convolutional operation to reduce the dimensionality of features vectors and prevent over-fitting. During this pooling operation, it can represent the region feature by calculating the average (or maximum) of region pixels. After above operation, the number of trained parameters is reduced. Following is full connection layer, and it is used to classify the extracted features. Different from it, the target of this paper extracts the features of given fingerprints, then the preprocessed features are fed into SVM classifier. The architecture of this paper is shown in Figure 2. In Figure 3, we visualize a feature map by using convolutional operation and the pooling operation. Convolutional features are obtained through computing the convolutional operation of original image and sliding window, and the process of convolutional operation is regarded as the process of feature extraction. During this, ReLU is chosen as the activation function to compute feature maps. After the convolution operation, pooling operation based on max-pooling is performed to reduce the dimensionality of feature maps and prevent over-fitting. The max-pooling operation principle counts the maximum in the sliding windows as the value of pooling layer. Such as the green solid line window in Figure 3, the size of green solid line window is 2×2, and the value of window is calculated as a new value (it is the maximum in the green solid line window) after max-pooling operation.

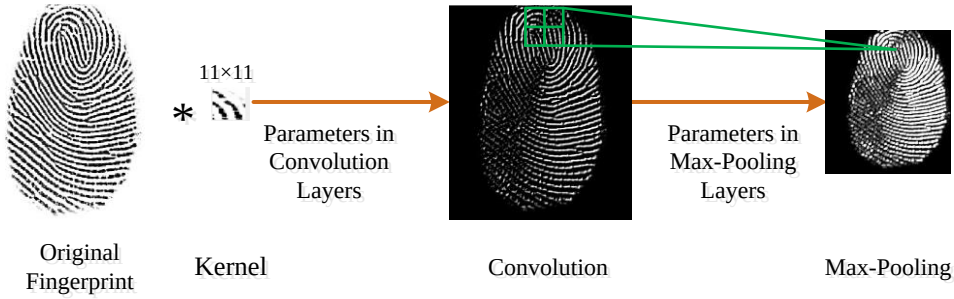


Figure 3: Architecture of the single layer convolutional neural network feature extraction process

2.3 Support Vector Machine

Support Vector Machine (SVM) has many unique advantages in solving small sample, nonlinear and high dimensional pattern problems. Thus, it is widely used in the research field of computer vision, pattern recognition and bioinformatics, etc. Vector set is usually difficult to be segmented in the low dimensional space, but it is linearly separable by constructing a hyperplane in a high-dimensional space. In other words, SVM clearly solve the problem by mapping vector set of low-dimensional space to high-dimensional space. Besides, affected by the mapping vector set, introduced kernel function in the SVM can solve the classification problem of computational complexity. What we need is to find an optimal hyperplane for a given two classes of samples, the hyperplane can correctly split two classes of samples, at the same time, and the sorting interval must be maximum value. The decision function is defined as follows:

$$f(x) = sign(\sum_i \alpha_i K(x_i^v, x) + b) \tag{1}$$

where α_i represent Lagrange multiplier determined during the process of SVM training, and the parameter b, which representing the shift of the hyperplane, is determined during SVM training when K (xv I, x) denotes the kernel function (Yuan and Xia 2016). Figure 4 presents the optimal line of classification in a linear separable case. H represents the optimal line in the high-dimensional space by computing the largest distance $max_{margin}=w/2$ between H_1 and H_2. LIBSVM software package [Ghiani, Marcialis and Roli (2012); Jia, Yang, Zhang et al. (2013)] is a most commonly used classification tool. In this tool, two key issues need to be noted when splitting two classes of samples using SVM.

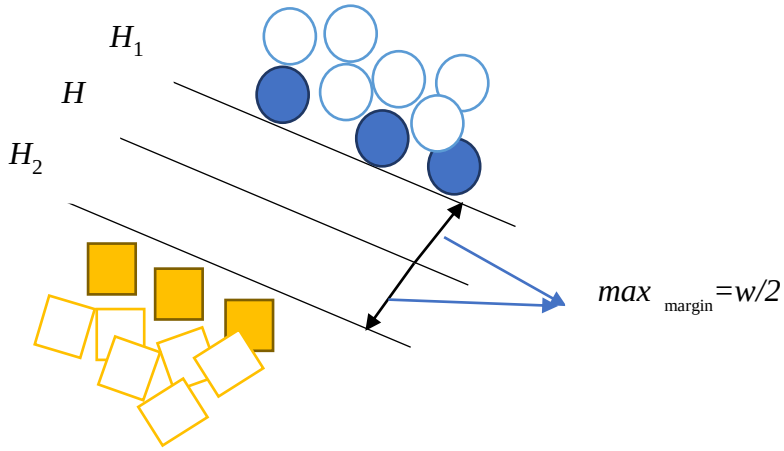


Figure 4: The optimal line of classification in linear separable cases.

One question is how to choose an appropriate kernel function of SVM. The goal of kernel function is that the two classes of samples is linearly separable by selecting an appropriate transformation in high-dimensional space, however, the two classes of samples for some problems are linearly non-separable in low dimensional space. According to the problem of linear separable and linear inseparable, different kernel functions are defined. It notes that the classification labels and samples are all nonlinear. Simplify, *RBF* kernel function is selected in this paper, mapping linear inseparable vector set of low-dimensional space to high-dimensional space. Another problem is how to set parameter pairs. A parameter pair is necessary in SVM with the *RBF* kernel function: including C andγ. To train a better classifier model, parameter optimization operation is necessary. In libsvm, gnuplot.exe is an executable file, which is used to find the optimal parameter pair C andγ. The goal of the parameter optimization is to classify the unknown data. Finally, we can search the results of the optimal parameter pair by using the "Grid-search and Cross-validation".

3 Experimental results

To evaluate the efficiency of our algorithm, our experimental results are compared with several state-of-the-art methods based on two public fingerprint datasets LivDet 2013 [Ghiani et al. (2013)] and LivDet 2011 [Yambay, Ghiani and Denti (2011)]. Firstly, a brief description about the two public datasets and experimental setup is given in this subsection. Next, performance assessment and experimental operating environment are described. Finally, we carry out experiments using the two public datasets, and we also have listed and compared our results with the state-of-the art works.

Table 1: The distribution of the LivDet 2011 set and LivDet 2013 set

Database ID	Sensor Device	Res.(dpi)	Image Size	Samples in Training Set		Samples in Testing Set	
				Real	Fake	Real	Fake
Liv2011-1	Biometrika	500	315×372	1000	1000	1000	1000
Liv2011-2	Digital	500	355×391	1004	1000	1000	1000
Liv2011-3	Italdata	500	640×480	1000	1000	1000	1000
Liv2011-4	Sagem	500	352×384	1008	1008	1000	1036
Liv2013-1	Biometrika	569	352×384	1000	1000	1000	1000
Liv2013-2	CrossMatch	500	800×750	1250	1000	1250	1000
Liv2013-3	Italdata	500	480×640	1000	1000	1000	1000
Liv2013-4	Swipe	96	1500×208	1221	979	1153	1000

3.1 Datasets description and experimental environment

Because fingerprint scanner systems are vulnerable to an artificial replica of real fingerprint, many fingerprint liveness detection methods are presented to prevent them being circumvented by counterfeit fingerprint images. The target of fingerprint liveness competition is to provide a standardized sample database for all academic and industrial institutions to compare their different detection methods. In addition, the assessments of the performance of our method are based on and LivDet 2013 and LivDet 2011, which are publicly available and widely used for evaluating fingerprint liveness detection.

LivDet 2011 fingerprint dataset, released in 2011, contains total 16056 fingerprints of both real and fake captured with four different flat optical sensors. As shown in Table 1, two classes of fingerprint datasets are included: training set with a total of 8020 images and testing set with a total of 8036 images. Both training set and testing set, which are all divided into two parts: true fingerprints and fake fingerprints. Moreover, there is no overlap between training set and testing set. The real fingerprints are captured by using four optical sensors, and the fake fingerprints are generated by using common materials with the help of tester' cooperation or no cooperative process. The detailed distribution of the LivDet 2011 dataset is listed in Table 1. LivDet 2013 dataset consists of total

16853 fingerprints, including 8874 real fingerprints and 7979 fake fingerprints. Both of them are captured based on four different flat optical sensors, which are Biometrika, CrossMatch, Italdata and Swipe, respectively. Some fingerprint samples from four different datasets are listed in Figure 1, and we can find that it is difficult to observe any slight difference between real and fake fingerprints only by the naked eyes. Similar to the introduction in LivDet 2011, two types of fingerprint samples are divided: Training set with a total of 8450 images and Testing set with a total of 8403 images. For the fingerprint liveness detection, Training set is used to learn and obtain a trained model, and the performance of the trained model is assessed by using Testing set. The detailed distribution of the LivDet 2013 dataset is presented in Table 1. Besides, we find that the ratio of the number of real or fake fingerprints is approximately 1:1. The sizes/scales of given fingerprints are various from 315×372 to 1500×208. The average classification errors (*ACE*) of our methods on LivDet 2013 dataset and LivDet 2011 dataset are presented in Table 2 and Table 3, respectively. By contrast, we can find that the average classification error of our method is superior to other methods.

3.2 Performance assessment and experimental environment

All classification results and performance metrics are in terms of Average Classification Error (*ACE*) formula (1) stated by Yuan and Sun (2016) to ensure consistency when compared with other methods in this paper, which is similar to (Nogueira, Lotufo and Machado 2014).

$$ACE = (FAR + FRR) / 2 \tag{2}$$

where in formula (2), *FAR* (False Accept Rate) represents the percentage of misclassified real fingerprints and *FRR* (False Reject Rate) represents the percentage of misclassified as fake ones. The detection accuracy of the testing samples is indicated by a value between 0 to 100 according to LivDet 2013 set and LivDet 2011 set. The better is the value of liveness detection, and the better is the performance of given methods.

Our operating environment is based on the open source code of cuDNN and Tensor flow deep learning framework. The operating system is Linux Mint 18 version, and all the experiments are all implemented by python 3.5.2 programming on a single GeForce GTX 1080 GPU (8 G memory) with two days. About the operational environment, two conditions are necessary, which are hardware condition and software condition. The detailed requirements for operational environment are demonstrated in Table 3.

Table 2: The hardware requirements of our experimental operating environment.

Hardware Condition	Software Condition
CPU: Intel@ Core i7-6700 Memory: 32G GPU: NVIDIA@ GeForce GTX 1080 8GB	Operating System: Linux Mint 18 Version Run environment: Python 3.5.2 + Cuda 8.0

3.3 Implementation Process, Detection Results and Comparison

Fingerprint image classification performance based on convolutional neural network is obviously superior to traditional detection methods, thus we consider that the key point is the extracted features by analyzing the difference between traditional detection methods and detection methods based on convolutional neural network. Moreover, we also observe that many elements of feature maps are zero or close to zero after convolutional operation or pooling operation. At the same time, we know that these feature maps are as the input data of next convolution layer or pooling layer. If we do not handle these zero elements, then it increases the computational complexity and affects the final classification performance to a certain extent. Based on above discussion, PCA is introduced into our method for each convolution layer or pooling layer, and the detailed description and structure of our method are shown in Figure 2. In this paper, only the convolution layer and pooling layer are used. Before feature extraction, preprocessing operation for fingerprint images is necessary due to the impact of invalid areas. In this paper, ROI is implemented by using built-in ROI function in OpenCV tool. Next, the features are extracted by using convolutional operation and pooling operation. PCA for the extracted features has also been implemented after convolutional operation or pooling operation. Note that only the first three pooling layer need to implement PCA, and there is no need to implement PCA operation for the first three convolutional layer. Then, until the last layer, the extracted features after PCA operation is regarded as the input data of next convolutional layer or pooling layer. Finally, all the extracted features after PCA operation are stitched together, which are fed into SVM classifier.

To verify the performance of our proposed method, our experimental results are compared with several state-of-the-art methods, including MSDCM [Yuan and Xia (2016)], MBLTP [Jia, Yang, Zhang et al. (2013)], Pore Analysis [Johnson and Schuckers (2015)], SURF [Dubey, Goh and Thing (2016)], and SURF+PHONG [Dubey, Goh and Thing (2016)]. Table 3 and Table 4 list detailed experimental results. In Table 3 and Table 4, the average classification error of our method is the best, which are highlighted in bold.

Table 3: The comparisons of the classification error ratio of different algorithms in LivDet 2013 dataset.

Methods	The Average Classification Error ACE (%)				
	Bimometrika	CrossMatch	Italata	Swipe	Average
Our method	**3.14**	**3.82**	**1.36**	9.95	**4.57**
PHONG (Dubey 2016)	3.87	9.92	6.7	9.05	7.24
CN (Nogueira 2014)	4.55	5.2	47.65	5.97	15.84
SURF (Dubey 2016)	5.75	6.08	4.6	**4.6**	5.26
MSDCM (Yuan and Xia, 2016)	3.55	20.84	2.35	5.25	7.59
HIG Dense Block Packing Combined (Gottschlich 2014)	3.9	28.76	1.7	14.4	12.19
Winner (Ghiani 2013)	4.7	31.2	3.5	14.07	13.37

Table 4: The comparisons of the classification error ratio of different algorithms in LivDet 2011 dataset.

Methods	The Average Classification Error ACE (%)				
	Bimometrika	Digital	Italata	Sagem	Average
Our method	10.8	**4.32**	9.91	**3.95**	**7.25**
MBLTP (Jia 2013)	9.7	7.0	16.0	5.8	9.62
Winner (Yambay 2011)	20	36.1	21.8	13.8	22.9
LPQ+PCA (Yuan and Sun, 2016)	**7.1**	9.7	10.5	7.2	8.63
Pore Analysis (Johnson 2015))	26.6	31.4	23.4	22.0	25.9
Baseline (Johnson 2015)	20.6	14.0	8.4	8.4	12.9
Fusion (Johnson 2015)	18.4	15.2	7.8	6.7	12
LASP (Kim 2016)	22.6	27.1	17.6	17.58	21.22
WLD (Chen 2010)	13.3	13.8	27.7	6.7	15.4
SURF+PHONG ([Dubey 2016)	8.76	6.9	**7.4**	6.23	7.32

4 Conclusions

In the traditional fingerprint liveness detection, extracted features are the key to obtain a higher classification performance. Existing features extraction algorithms are based on

hand-crafted features, which heavily depend on the experience and domain knowledge of experts. Because of its strong feature self-learning capabilities, feature extraction methods based on CNN (convolutional neural network technology) have been widely used in computer vision and pattern recognition including image classification. This paper mainly focuses on how to apply CNN to the research field of fingerprint liveness detection. Through the research of Nogueira, Lotufo and Machado (2014), we think that the convolutional process is regarded as process of feature extraction. Therefore, the extracted features based on CNN are fed into SVM classifier in this paper. PCA technique is also used to reduce the dimensionality of feature maps after each convolutional or pooling operation. Moreover, ROI preprocessing operation has been implemented in this paper to get rid of the impact of anomalous region. After above operations, high-level semantic features of fingerprint images have been automatically learnt from preprocessed fingerprints images, and then these extracted features are fed into SVM classifier. Next, a classifier model is trained by using training fingerprint images. Finally, the performance of model is evaluated by using testing fingerprints.

Acknowledgments: This work is supported by the NSFC (61672294, U1536206, 61502242, U1405254, 61602253), BK20150925. Fund of MOE Internet Innovation Platform (KJRP1403), Fund of Jiangsu Postgraduate Research and Innovation Program Project (KYCX17_0899), State Scholarship Fund (201708320316), CICAEET, and PAPD fund.

References

Celiktutan, O.; Sankur, B.; Avcibas, I. (2008): Blind Identification of Source Cell-Phone Model. *Information Forensics & Security IEEE Transactions on*, vol. 3, no. 3, pp. 553-566.

Chen, J.; Shan, S.; He, C.; Zhao, G.; Pietikainen, M.; Chen, X.; Gao, W. (2010): WLD: A Robust Local Image Descriptor. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 32, no. 9, pp. 1705-1720.

Chen, X.; Sun, H.; Tobe, Y.; Sun, X. (2017): Coverless Information Hiding Method Based on the Chinese Mathematical Expression. *Journal of Internet Technology*, vol. 18, no. 2, pp. 133-143.

Choi, H.; Kang, R.; Choi, K.; Kim, J. (2011): Aliveness detection of fingerprints using multiple static features. *Proceedings of World Academy of Science Engineering & Technology*, pp. 200-205.

Dubey, R. K.; Goh, J.; Thing, V. L. L. (2016): Fingerprint Liveness Detection from Single Image Using Low-Level Features and Shape Analysis. *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 7, pp. 1461-1475.

Galballym J.; Marcel, S.; Fierrez, J. (2014): Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition. *IEEE transactions on image processing: a publication of the IEEE Signal Processing Society*, vol. 23, no. 2, pp. 710-724.

Ghiani, L.; Yambay, D.; Mura, V.; Tocco, S.; Marcialis, G. L.; Roli, F.; Schuckers, S. (2013): LivDet 2013 Fingerprint Liveness Detection Competition 2013. *Iapr International Conference on Biometrics*, pp. 208-215.

Gragnaniello, D.; Poggi, G.; Sansone, C.; Verdoliva, L. (2013): Fingerprint Liveness Detection based on Weber Local Image Descriptor. *2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, pp. 46-50.

Gragnaniello, D.; Poggi, G.; Sansone, C.; Verdoliva, L. (2015): Verdoliva, Local contrast phase descriptor for fingerprint liveness detection. *Pattern Recognition*, vol. 48, no. 4, pp. 1050-1058.

Ghiani, L.; Hadid, A.; Marcialis, G. L.; Roli, F. (2013): Fingerprint Liveness Detection using Binarized Statistical Image Features. *IEEE Sixth International Conference on Biometrics: Theory*, vol. 2071, pp. 1-6.

Ghiani, L.; Marcialis, G. L.; Roli, F. (2012): Fingerprint liveness detection by local phase quantization. *International Conference on Pattern Recognition*, pp. 537-540.

Gottschlich, C.; Marasco, E.; Yang, A. Y.; Cubic, B. (2014): Fingerprint liveness detection based on histograms of invariant gradients. *IEEE International Joint Conference on Biometrics*, pp. 1-7.

Johnson, P.; Schuckers, S. (2015): Fingerprint pore characteristics for liveness detection. *Biometrics Special Interest Group. IEEE*, pp. 1-8.

Jia, J.; Cai, L.; Zhang, K.; Chen, D. (2007): A new approach to fake finger detection based on skin elasticity analysis. *In Advances in Biometrics*, vol. 4642, pp. 309-318.

Jia, X.; Yang, X., Zang, Y.; Zhang, N.; Dai, R. et al. (2013): Multi-scale block local ternary patterns for fingerprints vitality detection. *International Conference on Biometrics*, pp. 1-6.

Kim, S.; Park, B.; Song, B. S.; Yang, S. (2016): Deep belief network based statistical feature learning for fingerprint liveness detection. *Pattern Recognition Letters*, vol. 77, pp. 58-65.

Kim, W., Jung, C. (2016): Local accumulated smoothing patterns for fingerprint liveness detection. *Electronics Letters*, vol. 52, no. 23, pp. 1912-1914.

Manivanan, N.; Memon, S.; Balachandran, W. (2010): Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering. *Electronics letters*, vol. 46, no. 18, pp. 1268-1269.

Marasco, E.; Sansone, C. (2012): Combining perspiration- and morphology-based static features for fingerprint liveness detection. *Pattern Recognition Letters*, vol. 33, no. 9, pp. 1148-1156.

Marcialis, G. L.; Roli, F.; Tidu, A. (2010): Analysis of fingerprint pores for vitality detection. *International Conference on Pattern Recognition*, pp. 1289–1292.

Marcialis, G. L.; Lewicke, A.; Tan, B.; Coli, P.; Grimberg, D. et al. (2009): First international fingerprint liveness detection competition-livdet 2009. *In Image Analysis and Processing–ICIAP 2009*, pp. 12-23.

Nikam, S. B.; Agarwal, S. (2008): Texture and Wavelet-Based Spoof Fingerprint Detection for Fingerprint Biometric Systems. *First International Conference on Emerging Trends in Engineering and Technology*, pp. 675-680.

Nogueira, R. F.; Lotufo, R. D. A.; Machado, R. C. (2014): Evaluating software-based fingerprint liveness detection using Convolutional Networks and Local Binary Patterns. *Biometric Measurements and Systems for Security and Medical Applications*, pp. 22-29.

Pereira, L. F. A.; Pinheiro, H. N. B.; Cavalcanti, G. D. C.; Ren, T. I. (2013): Spatial surface coarseness analysis: technique for fingerprint spoof detection. *Electronics Letters*, vol. 49, no. 4, pp. 260-261.

Susom, D. A.; Ramachandra, M.; Dookie, K.; Pijush, S. (2017): Prediction of Compressive Strength of Self-Compacting Concrete Using Intelligent Computational Modeling. *Computers, Materials & Continua*, vol. 53, no. 2, pp. 167-185.

Tian, Q.; Chen, S. (2017): Cross-heterogeneous-database age estimation through correlation representation learning. *Neurocomputing*, vol. 238, pp. 286-295.

Wang, B.; Gu, X.; Ma, L.; San, Y. (2016): Temperature Error Correction Based on BP Neural Network in Meteorological Wireless Sensor Network. *International Conference on Cloud Computing and Security*, pp. 117-132.

Wang, J.; Li, T.; Shi, Y. Q.; Lian, S.; Ye, J. (2016): Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics. *Multimedia Tools & Applications*, pp.1-17.

Wu, C.; Li, W. (2016): Three-Dimensional Static Analysis of Nanoplates and Graphene Sheets by Using Eringen's Nonlocal Elasticity Theory and the Perturbation Method. *Computers, Materials & Continua*, vol. 52, No. 2, pp. 73-103.

Yambay, D.; Ghiani, L.; Denti, P. (2011): LivDet 2011-Fingerprint liveness detection competition 2011. *Iapr International Conference on Biometrics*, pp. 208-215.

Yuan, C.; Sun, X.; Lv, R. (2016): Fingerprint liveness detection based on multi-scale LPQ and PCA. *China Communications*, vol. 13, no. 7, pp. 60-65.

Yuan, C.; Xia, Z.; Sun, X. (2017): Coverless Image Steganography Based on SIFT and BOF. *Journal of Internet Technology*, vol. 18, no. 2, pp. 435-442.

Yuan, C.; Xia, Z.; Sun, X.; Sun, D.; Lv, R. (2016): Fingerprint liveness detection using multiscale difference co-occurrence matrix. *Optical Engineering*, vol. 55, no. 6, pp. 063111.

Zhou, Z.; Wang, Y.; Wu, Q. M. J.; Sun X. (2016): Effective and Efficient Global Context Verification for Image Copy Detection. *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 1, pp. 48-63.

Zhou, Z.; Wu, Q. J.; Huang, F; Sun, X. (2017): Fast and accurate near-duplicate image elimination for visual sensor networks. *International Journal of Distributed Sensor Networks*, vol. 13, no. 2.