Fingerprint Liveness Detection Using Histogram of Oriented Gradient Based Texture Feature

Chengsheng Yuan[1,2,3], Xingming Sun[1,2]

[1] School of Computer and Software, Nanjing University of Information Science and Technology, China
[2] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, China
[3] Department of Electrical and Computer Engineering, University of Windsor, Canada
{ycs_nuist, sunnudt}@163.com

Abstract

Fingerprint authentication systems are widely used in civilian applications and governments. However, current problem is that fingerprints are easy to be imitated by artificial materials. Thus, spoof fingerprint detection has become increasingly significant. To solve the problem, a anti-spoofing mechanism, called FLD (fingerprint liveness detection), is used to discriminate spoof fingerprints from authentic fingerprints. In this paper, a new detection method using the histogram of oriented gradient with gamma correction is proposed. Firstly, gamma correction operation is used to eliminate the effects of poor quality fingerprints due to bad light and high brightness. Next, the sizes of captured images using different sensors are various, so images are zoomed to same scales through a bi-linear difference method. Then, features descriptors are described by the calculation of histogram of oriented gradient of pixels. Normalization operation is performed to remove the influence of abnormal features. Finally, the features representations are fed into SVM classifier with RBF. Experimental results on LivDet 2013 indicate that our method can yield a better classification performance compared with other methods.

Keywords: Fingerprint liveness detection, SVM, Gamma Correction, Histogram of oriented gradient, Normalization

1 Introduction

With the rapid development of digital and network technology, the demand of security and confidentiality of personal identification become high gradually. Therefore, identity authentication techniques attract the attention of researchers and scholars. However, traditional access methods (PIN, Password, Key, Card, etc.) are easy to be damaged, lost or cracked. Therefore, traditional identity authentication methods do not meet the needs of security [1]. In order to solve above problem, identity recognition techniques based on biological features, which are more effective, reliable and safer, are developed [2]. Among all biometric features recognition techniques, the fingerprint Fingerprints are not only used for identity recognition, but also the most skilled biometric identification techniques [3]. Because fingerprints are made up of valley lines and ridge lines, fingerprint recognition can verify the identity of the testers by fingerprint comparison. However, the fingerprints are easy to be imitated by using common materials, such as silicone, gelatin, or latex. Thus, these systems are vulnerable to spoof attacks [4]. To handle the problem, fingerprint liveness detection technology has been proposed.

Fingerprint liveness detection refers to ability that fingerprint authentication system can distinguish between authentic fingerprints and artificial fingerprints. In recent years, various fingerprint liveness detection methods have been proposed [17-24], which are divided into two categories: hardware-based methods applied at acquisition stage, and software-based methods applied at processing stage. The hardware-based detection methods use specific sensor devices and tools to measure fingerprint traits, such as sweat, pulse and electric resistance, etc. Though hardware-based methods can detect fingerprint liveness detection as well [8], these detection methods can yield higher error affected by influence of external environment or devices themselves. Compared with the hardware-based methods, software-based detection error is low, and fake traits are detected only by using image processing algorithms to extract dynamic or static texture features of fingerprints.

In this paper, we propose a novel fingerprint liveness detection algorithm to handle vulnerability of artificial fingerprints. For the first time, we construct the feature vectors by using histogram of oriented gradient. Firstly, to eliminate the effects of lights, gamma correction is proposed in this paper. In addition, the sizes of collected fingerprints using different sensors are various, thus, the fingerprint images are zoomed to the same scales using bi-linear difference

*Corresponding Author: Xingming Sun; E-mail: sunnudt@163.com
DOI: 10.3966/160792642018091905021

method. Then, features representations are constructed by using histogram of oriented gradient. Normalization operation is performed to remove the influence of abnormal gradient values. Finally, classifier model are trained by using SVM with RBM classifier. Parameter optimization for feature vectors is essential through using gnuplot.exe in SVM classifier before training [13].

The rest of the paper is structured as follows. Some of relevant concepts in software-based fingerprint liveness detection methods are presented in Section 2. Section 3 describes our method about the feature extraction process. The result and comparison of the fingerprint liveness detection appear in Section 4. Finally, the conclusions and future works are drawn in Section 5.

2 Related Works

The sweat gland of true fingerprint can generate moisture, while artificial fingerprints do not have this phenomenon. Because the fingerprint sensors are sensitive to this moisture, detection methods based on moisture are exploited. In the method [10], two fingerprints images are captured at zero second and after five seconds [11-12], then, some static features are constructed by using FFT and calculating total energy corresponding to spatial frequency. In 2006, Tan [14] proposed a new method based on wavelet transform, and ridge signal along the ridge mask was extracted. In their method, biometric features from fingerprints are captured for enrollment or authentication, which can detect the moisture phenomenon using only a single image. Unfortunately, Tan [7] observed and pointed out that skin deformation-based method has some disadvantages, and testers have been trained to capture fingerprints. Kim proposed a detection method by obtaining image quality scores from multiple local regions [20], and the extracted features are fed into the SVM with RBF classifier to verify whether the given fingerprints are artificial fingerprints or not. The advantage is that it can accurately verify vitality of fingerprints even with small partial distortions. In 2010, a method based on features of multiple images quality-based is proposed to handle fake attacks in [15]. In their method, three effective spoof and true quality measures are extracted and fused to discriminate spoof fingerprints from true ones. Espinoza [9] exploited essential features of ridge skin: pores to detect spoofing attacks, and proposed a method using the number of pores. Then, these features are fed into linear classifier, and the performance was evaluated through using the differences of pore quantity. Marcialis [16] also detected the fingerprint spoofing attacks by using the analysis of fingerprint pores location as the features of fingerprints, and this is an important research about sweat pores. A novel liveness detection method through using minimize the energy associated with phase and orientation maps was proposed in [5-6], and multi-resolution texture analysis techniques are also exploited [23-24]. In addition, cross ridge frequency analysis is performed through calculating statistical measures and weighted average phase. These features along ridge reliability or ridge center frequency are input into a fuzzy c-means classifier. In Yuan [18], SIFT is used to be extracted the local feature of given image, and the experimental results are satisfactory.

3 Feature Extraction

Liveness detection is a binary classification problem, distinguishing true fingerprints from spoof ones. Therefore, the key to fingerprint detection is how to extract a better feature. The flow diagram of our method is presented in Figure 1, and two processes are included: the training process and the testing process. The former is used to obtain a model classifier, and the latter is used to evaluate the performance of model. Before feature extraction, preprocessing operation is necessary.

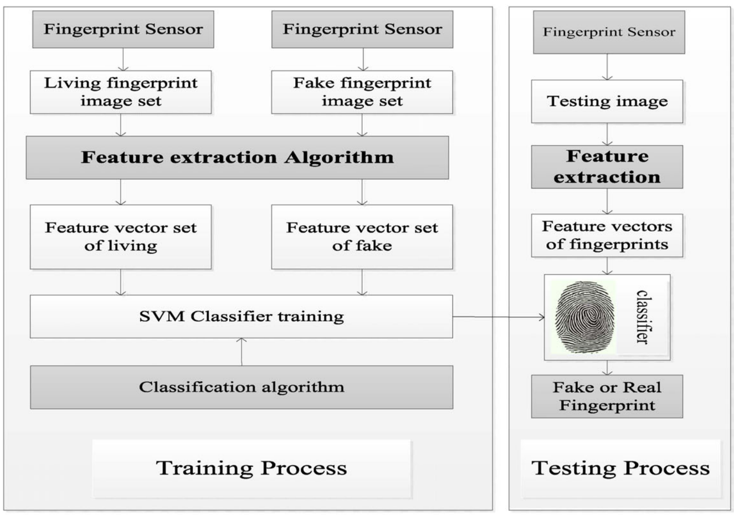


Figure 1. The flow diagram of our proposed method

3.1 Preprocessing Operation

Before liveness detection, fingerprint images are captured by using fingerprint sensors. Affected by devices and external environment, the quality of fingerprint images is bad, and the classification error rate is higher. Therefore, preprocessing operations for captured images are implemented to prevent false detection and leak detection. The the color information of fingerprint images is not effective, so image graying operation for captured RGB image is firstly implemented. Then, the sizes of captured images are various due to the influence of fingerprints devices themselves, and high scale fingerprint images can increase the liveness detection correct rate. Therefore, all captured image are scaled to the same size to make dimension of the features of captured fingerprint images based on different fingerprint devices consistent. Finally, segmentation correction for captured images based on Gamma operation is proposed, which reduce the influence of shadow and strong lights. Gamma correction is executed in this paper using $\gamma < 1$ if the pixel values are small; Otherwise, Gamma correction executes $\gamma > 1$. After Gamma correction operation, the small gray-scale pixels are ranged to high gray-scale pixels, and high gray-scale pixels are ranged to small gray-scale pixels.

Image gray scale operation formula is defined as follows:

$$Gray = 0.3R + 0.6G + 0.1B \tag{1}$$

Where Gray denotes gray scale image after a gray, components of color RGB are multiplied by a weight value. Gamma correction is implemented by using formula as follows:

$$GC(x, y) = I(x, y)^{\gamma} \tag{2}$$

I (x, y) is the pixel values of original images, which is located (x, y). GC (x, y) denotes pixel values after Gamma correction operation. γ refers to the parameter of Gamma correction. In this paper, γ is 0.5. Based on formula 2, low gray image, whose pixel values are stretched, has better correction effect. However, the captured images under strong light are more bright and whiter after the formula 2 operation, which is bad for liveness detection. Therefore, to reduce the influence of strong lights, two Gamma correction operations for low gray images and high gray images are proposed respectively. Gamma correction is executed when the pixels' values are low through using parameter γ, which satisfies with $0< \gamma < 1$, and another correction has been done for the high pixels' values using parameter γ, $\gamma > 1$. After above operations, the low gray-scale pixels are stretched to high gray-scale pixels, the high gray-scale pixels range to small gray-scale pixels. Defined formulas for low gray images and high gray images are following:

$$\begin{cases} GC(x,y)=[I(x,y)/0.5]^{\gamma}*0.5 \\ \qquad\qquad I(x,y)\le 0.5,\ 0<\gamma<1 \\ GC(x,y)=\{[I(x,y)-0.5]/0.5\}^{\gamma}*0.5+0.5 \\ \qquad\qquad I(x,y)>0.5,\ \gamma>1 \end{cases} \tag{3}$$

In formula (3), $I(x, y)$ denotes the pixel values of fingerprint images, which are double images. And the range of $I(x, y)$ is [0, 1]. $GC(x, y)$ are pixels values of fingerprint images after Gamma correction operation. In this paper, the value of γ is 0.5 when $0< \gamma < 1$, and the value of γ is 2 when $\gamma >1$.

3.2 Normalization

The key to fingerprint liveness detection is extracted features, but the size and dimension of image are various. Therefore, data normalization operation is necessary to increase the classification accuracy of trained model. Data normalization refers to the operation that makes different scale data adjust to a small range, such as in [0, 1] or [-1, 1]. Normalization operation can make image resist geometry transformation, and it can identify the invariant image. In this paper, feature extraction based on HOG in different cells and blocks, and the size and range of extracted features are various because of different fingerprint image. Therefore, normalization operation is implemented to eliminate the influence of illumination changes and shadow. Classification accuracy using SVM classifier will be huge impact on detection results if the data scale is not unified.

In our method, the normalization operation is defined as follows:

$$F_{\text{norma}} = \frac{F(i, j) - F_{\min}}{F_{\max} - F_{\min}} \tag{4}$$

In the formula, $F(i, j)$ denotes the pixel values corresponding location (i, j). And $F_{\min}$ and $F_{\max}$ respectively denote the minimum value and maximum value in the original fingerprint images. F_{norma} is processed data after normalization operation. After this operation, the entire pixel values or features vectors are mapped in the range of [0, 1].

3.3 Histogram of Oriented Gradient

Histogram of oriented gradient method firstly derived from SIFT algorithm. Due to the stronger description for images, the features method based on HOG presents more superior in object detection, which is better local texture descriptor. The process of feature extraction based on HOG is shown in Figure 2.

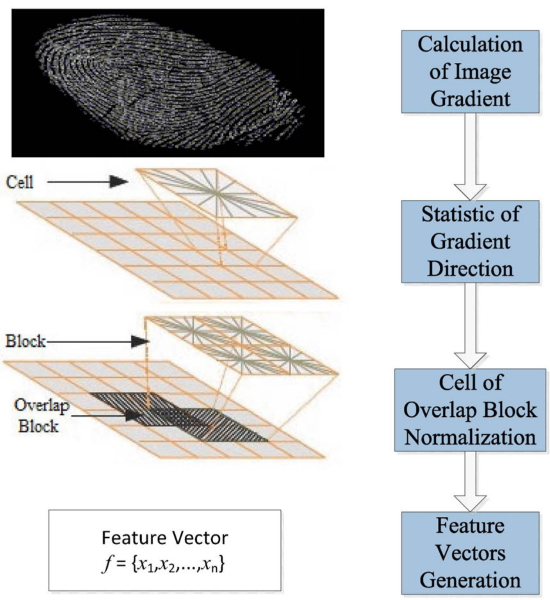


Figure 2. The diagram of feature extraction based on HOG

The size of fingerprint image $F(x, y)$ is $M \times M$, and the images are divided into n equal squares, whose sizes are M/n, $n<=M$. If M/n is a non-integer, $\lfloor M/n \rfloor$ is implemented for M/n, and $\lfloor\rfloor$ denotes floor operation. Figure 3, which is part of the given fingerprint image, shows the relationship of cell and block for fingerprint image. In the 3×3 squares of the upper left corner, Purple square of 3×3 squares denote cell (note: each cells composed of $M/n \times M/n$ pixels), and the block consist of Purple cell and surrounded by eight adjacent cells. The adjacent blocks can be overlapped, and they are also can overlap. Then, each pixel horizontal and vertical gradients are computed by using gradient operator. In this paper, the formula of each pixel horizontal and vertical gradients is defined as follows:

$$\begin{cases} G_x(x,y)=F(x+1,y)-F(x-1,y) \\ G_y(x,y)=F(x,y+1)-F(x,y-1) \end{cases} \quad \textbf{(5)}$$

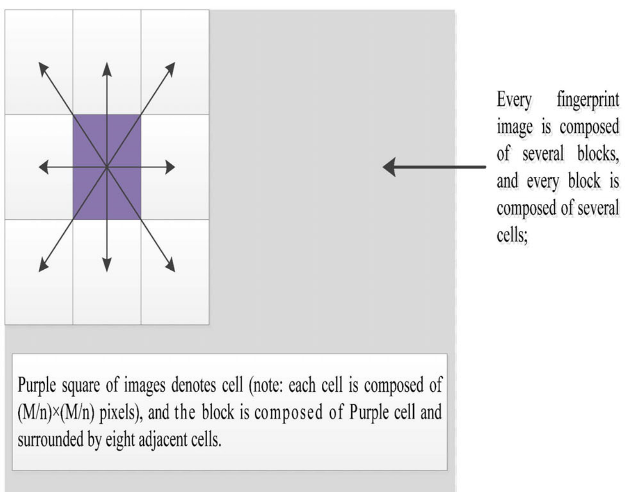


Figure 3. The relationships of cell and block in HOG

Where G_x(x, y), G_y(x, y) and $F(x, y)$ denote respectively horizontal gradient, vertical gradient and original fingerprint image when the coordinates of the pixel is (x, y). Derivation operation for pixel values not only capture the edges, breakpoints and bifurcation points on the ridge and valley lines, but also weaken the influence of strong lights. Next, each pixel gradient amplitudes and directions are calculated by using horizontal and vertical gradients $G_x(x, y)$ and $G_y(x, y)$. And the formulas of gradient amplitudes and directions are defined as following:

$$\begin{cases} A(x,y)=\sqrt{G_x(x,y)^2+G_y(x,y)^2} \\ D(x,y)=\tan^{-1}\left(\dfrac{G_y(x,y)}{G_x(x,y)}\right) \end{cases} \quad \textbf{(6)}$$

Where in formula (6), $A(x, y)$ is the size of the gradient for pixel values, located in (x, y), and $D(x, y)$ is the direction of the gradient for pixel values. $D(x, y)$ scope is 0 degree to 180 degree, and it is divided into 9 bins. Figure 4 denotes the distribution of bin blocks using HOG. Then, histograms of 9 bins for each cell are computed using gradient directions and gradient amplitudes, and each cell is composed of 9 features vectors. Block consists of four cells, therefore, features vectors of four cells are connected to 36 features vectors. That is to say, the dimensionality of a block is 36 features vector. Next, features vectors based on HOG are obtained by connecting the entire feature vectors corresponding blocks. Finally, trained model is learned by using SVM with RBF classifier, and the trained model is used as the standard classification function for testing samples.

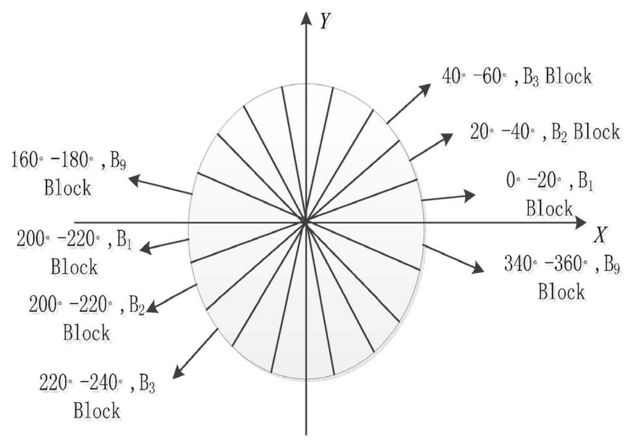


Figure 4. The distribution of bin blocks based on HOG

4 Experimental Results

4.1 Fingerprint Database and Validation Criterion

The performance of our proposed method is evaluated on LivDet 2013 [6], which comprising more than

18,000 true and spoof fingerprint images. The fingerprint set is used in Fingerprint Liveness Detection Competition 2013, which was held a Competition by the Department of Electrical and Computer Engineering of the Clarkon University (USA) and the Department of Electronic Engineering of the University of Cagliari (Italy). The fingerprint set comprises four data sets of true and spoof fingerprints, which are captured through using four optical sensors: 1) Biometrika (569 dpi), 2) CrossMatch (500 dpi), 3) Italdata (500 dpi), 4) Swipe (96 dpi). The detailed descriptions about four fingerprint sets are listed in Table 1. And the fake fingerprint can be generated using five kinds of materials: Ecoflex, Gelatin, Latex, Modasi and WoodGlue. Figure 5 lists some typical samples of real and spoof fingerprint images coming from LivDet 2013. We also list some common fake fingerprints which using different materials as well. It is difficult to distinguish the true fingerprints from artificial spoof fingerprint images, and even the expert cannot distinguish the real and fake fingerprint images. For the fingerprint set of liveness detection, it is divided into two unbiased sets: the goal of training sets is used to obtain and learn classifier model, and another set is testing set, which is used to validate the performance of classifier model.

Table 1. The detailed description of four sets from LivDet 2013

ID	Sensor	Res.(dpi)	Image Size	Samples in Training Set		Samples in Testing Set	
				Real	Fake	Real	Fake
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

(a) Biometrika(b) Crossmatch (c) Italdata (d) Swipe

Figure 5. Samples of real and spoof fingerprint images from the LivDet 2013

In this paper, the performance measurement of liveness detection is defined as follows. Average Classification Error (*ACE*), which is similar to [21], is used as a standard metric to ensure consistency when compared with other methods.

$$ACE = (FAR + FRR)/2 \quad \textbf{(7)}$$

where in formula (7), the *FAR* (False Accept Rate) represents the percentage of fake fingerprints misclassified as real fingerprint, and the *FRR* (False Reject Rate) denotes the percentage of real fingerprints misclassified as fake ones.

$$FAR = \frac{Total\ Number\ Imposter\ Fingerprints\ Accepted\ as\ Genuine}{Total\ Number\ of\ Forgery\ Tests\ Performed}, \quad \textbf{(8)}$$

$$FRR = \frac{Total\ Number\ Genuine\ Fingerprints\ Accepted\ as\ Imposter}{Total\ Number\ of\ Genuine\ Matching\ Tests\ Performed}, \quad \textbf{(9)}$$

4.2 Support Vector Machine (SVM)

After deeply study of statistical learning theory and structural risk minimization theory, Vapnik proposed a new kind of machine learning algorithm: Support Vector Machine (SVM). SVM is usually used to solve classification and regression problems, and it is a better tool to solve small sample, high latitudes, and nonlinear challenging problems in pattern recognition field. In addition, SVM is used as optimal two classification classifiers, which can separate the two types of problems as far as possible as well as make the structural risk minimization. Machine learning theory refers that a trained classifier is learned by using known classification samples. Once the classifier is learned, the classification for the test samples is implemented with the help of the learned classifier.

The goal of SVM is to learn a classifier using some way when the trained samples are small, and the trained model has also a good classification performance for the unknown testing samples. Another advantage is that the early SVM classifier only supports the linear separable two problems, while current SVM classifier is also suitable for nonlinear classification by introducing SVM kernel function. That is to say, the samples are linearly inseparable in low latitude space, however, they can achieve linear separation in high-dimensional space by mapping the samples into a higher dimensional space. LibSVM is an open source program library, and several basic kernels are included. Among these basic kernels, radial basis function (RBF) kernel function can solve the non-separable in low dimensional by mapping samples into high dimensional. Therefore, RBF kernel function is chosen in our method. Through the Grid-search and Cross-validation function, we can search for the optimal parameters to train and learn an optimal classifier.

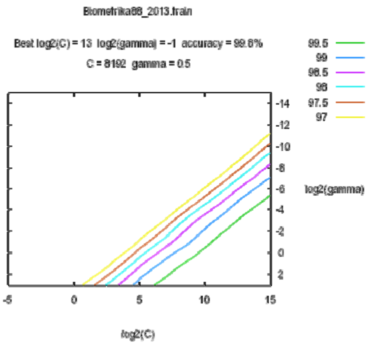
4.3 Experimental Results

The size of fingerprint image $F(x, y)$ is $M \times M$, and the images are divided into n equal squares, whose sizes are M/n, $n<=M$. Before experiments, fingerprint samples are necessary for the detection. The experiment is measured on a 32-bit Operating system Windows7-PC with a 2.83 GHz processor and 4 G RAM, running MATLAB R2010a. In order to avoid generating a wrong result, fingerprint set, including training set and testing set, can not have non-overlapping parts between data set. The LivDet 2013 derives from 2013 (FLDC) Fingerprint Liveness Detection Competition, whose quality of real or fake fingerprint has been greatly improved. The fingerprint set is downloaded from the website of the fingerprint liveness detection competition. The performance of our proposed method is evaluated by using the Average Classification Error (*ACE*). For obtaining the fingerprint image, the number of pixel values is huge. If the whole pixels of fingerprints are the input for the SVM classifier, the problems are that storage for system is large and computing time is long. Therefore, to deal with above problems, features extraction, representing the original fingerprint with minimum values and reducing the computation complexity, is the key to detection. In this paper, features are extracted by using HOG. Affected by the acquisition devices and lighting, the quality of captured images quality is poor. Thus, preprocessing operation for the captured images is firstly implemented. The preprocessing operation is including image graying, scale normalization and segmentation correction. Gamma correction is executed when the pixel values are low through using parameter γ, which satisfies with $0< \gamma < 1$, and another correction has been done for the high pixels values using parameter γ, $\gamma > 1$. It is executed according to the formula (2) and (3). Segmentation correction for captured images based on gamma operation can reduce the influence of shadow and strong lights as well as gradient orientations are easy to be computed. Then, the size and range of extracted features in different cells and blocks are various, so normalization operation is implemented. Next, the scope of gradient direction is 0 degree and 180 degree in our experiment. It is obvious that the livenss detection rate of fingerprints images will increase, but the trend of increase of detection rate is slow when the number of gradient direction is larger than 9 bins. Therefore, in this paper, the gradient direction is divided into 9 bins. Each pixel horizontal and vertical gradients are computed by using gradient operator, and the derivation operation for each pixel horizontal and vertical gradients is obtained by using formula (5). Pixel gradient amplitudes and directions are calculated by using horizontal and vertical gradients according to formula (6). Histograms of 9 bins for each cell are computed by using gradient directions and gradient amplitudes, and each cell is composed of 9 features vectors. Block consists of four cells, therefore, features vectors of four cells are connected to 36 features vectors. That is to say, the dimension of a block is 36 features vector. Next, features vectors based on HOG are obtained by connecting the entire feature vectors corresponding blocks. The dimension of feature vectors for whole image is $(n/2) \times (n/2) \times 36 = 9n^2$.

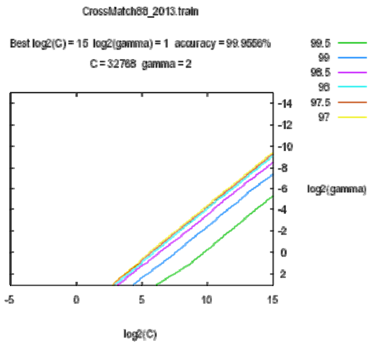
Finally, trained model is obtained based on conducted features vectors by using SVM classifier, and the trained model is used as the standard classification function for testing samples[11]. In order to learn a better classifier model and make the classification error minimum, parameter optimization is conducted for extracted features by using LIBSVM. Figure 6 shows the parameter pairs (C, g) of parameter optimization for four different sensors. From the Figure 6, parameter C denotes the cost, parameter g denotes parameter gamma. In Figure 4(a), the highest classification accuracy is obtained by parameters optimization when $C = 32$, and $g = 8$. Similarity, we can find the best classification accuracy responding the Figure 4(b), (c), (d) respectively. Table 2 lists the average detection error rate for different methods. The results of fingerprint liveness detection are shown in Table 2. From the table, our classification error rates are also clearly lower than other methods. To help observe the average detection errors of different methods, the best result obtained using our proposed method is highlighted in bold. The average error rate of our method is obviously superior to other methods.

5 Conclusions and Future Works

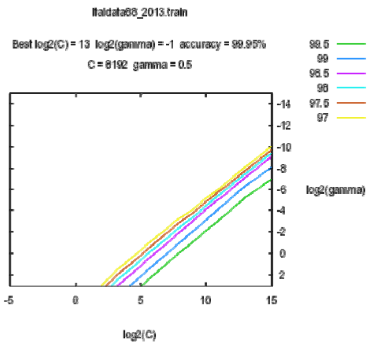
The security of fingerprint authentication systems is vulnerable by some artificial fake fingerprints, and the attackers can illegally access to real user's information. The risk of artificial spoof fingerprint attacks is becoming serious, which are handled by using various anti-spoofing mechanisms against known attacks. It is the first time that the gradient orientations and amplitudes are used to detect the fingerprint vitality. In this paper, image preprocessing operation is expected to improve the image quality. In order to eliminate the effects of shadow and strong lights as well as gradient orientations are easy to be computed, Gamma correction is proposed in this paper. Then, the size and range of extracted features in different cells and blocks are different, normalization operation is implemented. Next, the gradient direction of each pixel is divided into 9 bins. Each pixel horizontal and vertical gradients are computed by using gradient operator, and pixel gradient amplitudes and directions are calculated by using horizontal and vertical gradients. Histograms of 9 bins for each cell are computed by using gradient directions and gradient amplitudes, and each cell is



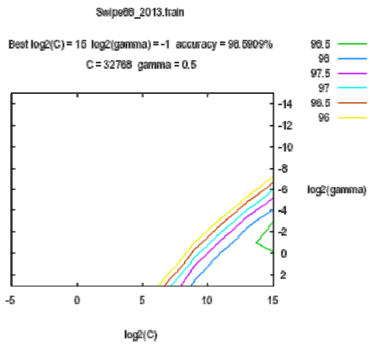
(a) Graphics of the results of the Biometrika sensor



(b) Graphics of the results of the CrossMatch Persona sensor



(c) Graphics of the results of the ItalData sensor



(d) Graphics of the results of the Swipe sensor

Figure 6. Graphics of the results of the Parameter optimization using different sensors

Table 2. Performance comparison in terms of ACE in database of the LivDet 2013

Methods	The Average Classification Error (ACE) (%) For Different Sensors				
	Biometrika	Digital	Italdata	Sagem	Average
Our method	2.75	7	7.05	4.27	5.27
WLD [25]	6.1	50	9.1	---	21.7
Winner 2013 [6]	4.7	31.2	3.5	14.07	13.53
HIG [21]	3.9	28.8	1.7	14.4	12.2
Anonym3 [6]	5.7	53.11	2.8	5.25	16.72
UniNap2 [6]	6.55	52.13	9.45	26.85	23.75
Anonym1 [21]	2.0	49.47	1.15	N.A	N.A
HIG-MC [21]	4.3	39.96	10.6	32.41	21.82
HIG-DBP [21]	3.9	34.13	8.3	14.44	15.19

composed of 9 features vectors. Block is made up of four cells, so the dimension of feature vectors for whole image is $(n/2) \times (n/2) \times 36 = 9n^2$ by concatenating entire feature vectors corresponding blocks. Finally, SVM classifier is used to train a model and verify the performance of the trained model. The experimental results show that our method can discriminate real fingerprints from spoof ones. Compared with other detection methods, our method can discriminate the live fingerprint from artificial spoof ones with a higher classification performance.

The error rates of fingerprint liveness detection based on texture features are extremely affected by the noise. Therefore, to reduce the influence of noise, median filter operation is applied in our future work and meanwhile features are extracted based on frequency domain to detect fingerprint liveness. In addition, extended experiments with different materials will be performed to demonstrate interoperability of our method. All these will be done in our future works.

Acknowledgements

This work is supported by the National Key R&D Program of China under grant 2018YFB1003205; by the National Natural Science Foundation of China under grant U1536206, U1405254, 61772283, 61602253, 61672294, 61502242; by the Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20150925, BK20181407 and

BK20151530; by the Jiangsu Postgraduate Research and Innovation Program under grant KYCX17_0899; by the State Scholarship fund 201708320316, China; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund; by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

References

[1] Z. Xia, R. Lv, Y. Zhu, P. Ji, H. Sun, Y. Shi, Fingerprint Liveness Detection using Gradient-based Texture Features, *Signal Image & Video Processing*, Vol. 11, No. 2, pp. 381-388, February, 2017.

[2] C. Yuan, X. Sun, R. Lv, Fingerprint Liveness Detection Based on MultiScale LPQ and PCA, *China Communications*, Vol. 13, No. 7, pp. 60-65, July, 2016.

[3] C. Sousedik, C. Busch, Presentation Attack Detection Methods for Fingerprint Recognition Systems: A Survey, *IET Biometrics*, Vol. 3, No. 4, pp. 219-233, December, 2014.

[4] C. Yuan, X. Li, Q. Wu, J. Li, X. Sun, Fingerprint Liveness Detection from Different Fingerprint Materials Using Convolutional Neural Network and Principal Component Analysis, *Computer Materials and Continua*, Vol. 53, No. 4, pp. 357-372, December, 2017.

[5] Z. Xia, C. Yuan, X. Sun, D. Sun, R. Lv, Combining Wavelet Transform and LBP Related Features for Fingerprint Liveness Detection, *IAENG International Journal of Computer Science*, Vol. 43, No. 3, pp. 290-298, August, 2016.

[6] D. Yambay, J. S. Doyle, K. W. Bowyer, A. Czajka, S. Schuckers, LivDet-iris 2013-Iris Liveness Detection Competition 2013, *IEEE International Joint Conference on Biometrics*, Clearwater, FL, 2014, pp. 1-8.

[7] B. Tan, S. C. Schuckers, New Approach for Liveness Detection in Fingerprint Scanners based on Valley Noise Analysis, *Journal of Electronic Imaging*, Vol. 17, No. 1, January, 2008.

[8] X. Chen, S. Chen, Y. Wu, Coverless Information Hiding Method Based on the Chinese Character Encoding, *Journal of Internet Technology*, Vol. 18, No. 2, pp. 313-320, March, 2017.

[9] M. Espinoza, C. Champod, Using the Number of Pores on Fingerprint Images to Detect Spoofing Attacks, *2011 International Conference on Hand-Based Biometrics (ICHB)*, Hong Kong, China, 2011, pp. 1-5.

[10] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, L. O'Gorman, Determination of Vitality from a Non-invasive Biomedical Measurement for Use in Fingerprint Scanners, *Pattern Recognition*, Vol. 36, No. 2, pp. 383-396, February, 2003.

[11] Y. Zheng, B. Jeon, D. Xu, Q. M. J. Wu, H. Zhang, Image Segmentation by Generalized Hierarchical Fuzzy C-means Algorithm, *Journal of Intelligent and Fuzzy Systems*, Vol. 28, No. 2, pp. 961-973, March, 2015.

[12] S. Schuckers, A. Abhyankar, Detecting Liveness in Fingerprint Scanners Using Wavelets: Results of the Test Dataset, *Biometric Authentication, ECCV 2004 International Workshop, BioAW 2004*, Prague, Czech Republic, 2004, pp. 100-110.

[13] Z. Xia, Y. Zhu, X. Sun, Z. Qin, K. Ren, Towards Privacy-preserving Content-based Image Retrieval in Cloud Computing, *IEEE Transactions on Cloud Computing*, Vol. 6, No. 1, pp. 276-286, January- March, 2018.

[14] B. Tan, S. Schuckers, Liveness Detection for Fingerprint Scanners based on the Statistics of Wavelet Signal Processing, *2006 Conference on. Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, New York, NY, 2006, pp. 1-8.

[15] N. Manivanan, S. Memon, W. Balachandran, Automatic Detection of Active Sweat Pores of Fingerprint using Highpass and Correlation Filtering, *Electronics letters*, Vol. 46, No. 18, pp. 1268-1269, September, 2010.

[16] G. L. Marcialis, F. Roli, A. Tidu, Analysis of Fingerprint Pores for Vitality Detection, *IEEE 2010 20th International Conference on Pattern Recognition (ICPR)*, Istanbul, Turkey, 2010, pp. 1289-1292.

[17] Z. Xia, X. Wang, X. Sun, Q. Wang, A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 27, No. 2, pp. 340-352, February, 2016.

[18] C. Yuan, Z. Xia, X. Sun, Coverless Image Steganography Based on SIFT and BOF, *Journal of Internet Technology*, Vol. 18, No. 2, pp. 435-442, March, 2017.

[19] R. Gurusamy, V. Subramaniam, A Machine Learning Approach for MRI Brain Tumor Classification, *Computer Materials and Continua*, Vol. 53, No. 2, pp. 91-108, 2017.

[20] W. Kim, S. Suh, Y. Kim, C. Choi, Fingerprint Liveness Detection Using Ensemble of Local Image Quality Assessments, *Electronic Imaging*, Vol. 2016, pp. 1-6, February, 2016.

[21] C. Gottschlich, E. Marasco, A. Y. Yang, B. Cukic, Fingerprint Liveness Detection based on Histograms of Invariant Gradients, *IEEE International Joint Conference on Biometrics*, Clearwater, FL, 2014, pp. 1-7.

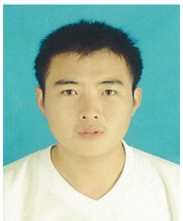
[22] C. Yuan, Z. Xia, X. Sun, D. Sun, R. Lv, Fingerprint Liveness Detection using Multiscale Difference Co-occurrence Matrix, *Optical Engineering*, Vol. 55, No. 6, June, 2016.

[23] A. Pradeep, S. Mridula, P. Mohanan, High Security Identity Tags Using Spiral Resonators, *Computer Materials and Continua*, Vol. 52, No. 3, pp. 185-195, 2016.

[24] C. Yuan, Z. Xia, X. Sun, D. Sun, R. Lv, Fingerprint Liveness Detection Using Gray Level Co-Occurrence Matrix Based Texture Feature, *International Journal of Grid and Distributed Computing*, Vol. 9, No. 10, pp. 65-78, October, 2016.

[25] D. Gragnaniello, G. Poggi, C. Sansone, L Verdoliva, Fingerprint Liveness Detection based on Weber Local Image Descriptor, *2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, Napoli, Italy, 2013, pp. 46-50.

Biographies



Chengsheng Yuan, received his B.S. degree in Software Engineering from Nanjing University of Information Science and Technology, China in 2014. At present, he is pursuing his Ph.D. degree in Meteorological Information Technology at the same university. His research interests include pattern recognition and digital forensic.

Xingming Sun, received his B.S. in Hunan Normal University, China, in 1984, M.S. in Dalian University of Science and Technology, China, in 1988, and his Ph.D. in Computing Science from Fudan University, China, in 2001. He is a Professor in NUIST. His research interests include network and information security.