

SpooF Fingerprint Detection based on Co-occurrence Matrix

Yujia Jiang and Xin Liu

*College of Architecture and Artistic Design, Hunan Institute of Technology,
Hengyang, 421001, China
jiangyujiacaad@163.com, liuxin7890@163.com*

Abstract

Fingerprint-based recognition systems have been widely deployed in numerous civilian and government applications. However, the fingerprint recognition systems can be deceived by commonly used sensors with the artificially fake fingerprint made using materials like gelatin or silicon. In this paper, spooF fingerprint detection is considered as a two-class classification problem and co-occurrence matrix is constructed from image gradients to extract features. In feature extraction process, the quantization operation is firstly applied with the fingerprint images. Secondly, the horizontal and vertical differences at each pixel are calculated. Thirdly, the differences of large absolute values are truncated into a reduced range. Finally, the co-occurrence matrix is constructed from the truncated differences, and the elements of the co-occurrence matrix are directly used as features. The features are separately utilized to train support vector machine classifiers on two databases. The experimental results have demonstrated that the proposed method outperform the state-of-the-arts.

Keywords: *Biometrics; spooF fingerprint detection; image difference; co-occurrence matrix*

1. Introduction

Fingerprint-based recognition systems have been widely deployed in numerous civilian and governments applications. . However, fingerprint-based systems are vulnerable to spooF attacks, as the spooF fingerprint can be easily made using cheap materials such as gelatin and silicon. The attackers could clandestinely retrieve a user's fingerprint and make a spooF one to achieve illegal access. In another way, a user may make a spooF fingerprint for himself to deceive attendance system.

In order to address the above problem, many spooF fingerprint detection techniques have been proposed to judge whether a fingerprint image is captured from an actual user or not. The existing methods can be divided into two classes: hardware-based and software-based methods [1, 2] .

The hardware-based methods add new hardware to obtain life signs of the finger such as temperature, pulse, and blood pressure. Then, spooF fingers can be detected from real ones by analyzing these signs. The hardware-based solutions can discover spooF attacks to some degree. However, this type of techniques requires the support of additional devices which increases the expenses of the fingerprint identification system. On the other hand, the software-based methods distinguish the live fingers from the spooF ones by analyzing the images obtained from the existing fingerprint sensors. This type of methods is less expensive than hardware-based one.

The software-based spooF fingerprint detection methods can be further divided into five categories: sweat pores based, perspiration based, skin elasticity based, image quality based, and texture feature based. Generally, the sweat pores based methods have a high requirement for the resolution of the fingerprint images. The perspiration based and the skin elasticity based methods require capturing two or more images to extract

dynamic features. They are time-consuming and user-unfriendly. The image quality based and texture feature based methods require no special demands from users and sensors, and hence have been researched widely.

In this paper, a novel software-based spoof fingerprint detection method is proposed. We regard the liveness detection as a two-class classification problem, i.e. classifying a test fingerprint image into either a living or a spoof one. Feature extraction is a crucial step for classification problem. This paper for the first time extracts discriminant features by calculating co-occurrence matrix from image gradient. Specifically, the horizontal and vertical gradients are calculated from the adjacent pixels. Then, co-occurrence matrix is calculated from the differences to form texture features. Quantization and truncation operations are designed and applied to reduce the dimensionality of feature vector.

In the rest of the paper, Section II presents some related works. Section III describes the feature extraction process. Experiments are presented in Section IV, and conclusions are drawn in Section V.

2. Related Works

The software-based methods show that live and spoof fingerprints can be discriminated by analyzing the features extracted from fingerprint images. The features can be based on sweat pores, perspiration, skin elasticity, image quality, image texture and so on. To clarify, we classify the software-based spoof fingerprint detection methods into five categories: sweat pores based, perspiration based, skin elasticity based, image quality based, and texture feature based methods.

Sweat pores based methods. The sweat pores are of very small circular structures in the fingerprint ridges. Some researchers assumed that such small structures would be very difficult to reproduce in high quality. Marcalis *et al.* [3] claimed that the frequency of pores in spoof fingerprint was less than that in living fingerprints. This difference was used as a discriminating feature in liveness detection. Manivanan *et al.* [4] proposed a method to automatically extract and locate the sweat pores in a fingerprint image by using high-pass and correlation filtering techniques. It is an important preliminary work of sweat pores based spoof fingerprint detection methods.

Perspiration based methods. When a live finger is put on the surface of a fingerprint sensor, the obtained fingerprint images will change slightly in a short time span due to the moisture produced by the sweat glands. However, the spoof fingers do not produce a similar phenomenon when scanned by the sensor. Derakhshani *et al.* [5] proposed a detection method which acquired two fingerprint images at different time points (0 and 5 seconds). This method maps the two-dimensional fingerprint images into one-dimensional gray values along the ridges. It is observed that the middle ridge signal of the second fingerprint image is of a much more wavy nature because of the spreading of moisture. One static feature and four dynamic features are extracted based on this difference. Schuckers and Abhyankar [6] also observed perspiration pattern of images acquired in two different time points. Their method decomposes the low-frequency content of the image using the multi-resolution analysis and decomposes the high-frequency content using the wavelet analysis. The features are extracted based on the energy of the coefficients. Tan and Schuckers [7] proposed a liveness detection method which quantified perspiration patterns along ridges and noise patterns along valleys. The signals representing gray level patterns along ridges and valleys were explored in spatial, frequency and wavelet domains. Marasco and Sansone [8] combined perspiration and morphology-based static features to detect spoof fingerprints. Their perspiration based features are extracted by observing the individual pore spacing and the intensity of the image.

Skin elasticity based methods. Generally, live fingers have better elasticity than spoof ones. Antonelli *et al.* [9, 10] proposed a dynamic method based on skin distortion. In their method, the user is required to move the finger while pressing it on the scanner surface to deliberately exaggerate the skin distortion. During the finger movement, a sequence of fingerprint images are acquired. Then, features are extracted from the multi-stage images. Zhang *et al.* [11] also proposed a detection method which required the user to apply some pressure in four different directions when putting the finger on the sensor surface. This method extracts features by observing the minutiae of distorted fingerprint images and the undistorted one. The change of minutiae positions is used to calculate the thin-plate spline model, and then the bending energy vectors are calculated as features. Jia and Cai [12] proposed a method which did not require any special behavior from the user. In this method, a time-series sequence of fingerprint images are captured when a user put a finger onto the sensor. Five features are extracted from the image sequence. Two of the features represent the skin elasticity, and the other three represent the physiological process of perspiration. Finally support vector machine classifier is trained to discriminate the live fingers from spoof ones.

Image quality based methods. Moon *et al.* [13] claimed that the surface of a spoof fingertip was much coarser than that of a living one, and utilized the wavelet analysis to extract noise residue. The standard deviation of the noise residue was used as the distinguishable feature. Jin *et al.* [14] utilized three effective quality measures, namely spectral band energy, middle ridge line and middle valley line, to extract features. The support vector machine and quadratic discriminant analysis classifiers were trained. Galbally *et al.* [15] proposed an image quality based liveness detection method. The quality features were extracted by ridge-strength, ridge-clarity and ridge-continuity measures. In 2013, Pereira *et al.* [16] measured the coarseness of fingerprint through the estimation of the residual Gaussian white noise of the image. The noise was divided into several parts, and each part of the noise was used to calculate a histogram. The bins of these histograms were used as features. Galbally *et al.* [17] proposed an image quality based liveness detection method for iris, fingerprint and face recognition. The authors applied twenty five image quality assessment measures to extract features. It is a highly competitive liveness detection method compared with other advanced ones.

Texture feature based methods. Spoof fingerprint images possess different texture compared with the living ones despite the difference is hard to tell by human eyes. Abhyankar and Schuckers [18] developed a method based on multi-resolution texture features and local ridge frequency features. Their texture features include: 1) the first order features, i.e. energy, entropy, median, and variance of the histogram, and 2) the second order features, i.e. cluster shade and cluster prominence of the co-occurrence matrix. Coli *et al.* [19] claimed that the high frequency details of the spoof fingerprint images were greatly reduced, and extracted features from the power spectrum for the classification. Nikam and Agarwal proposed several liveness detection methods based on the texture analysis of the fingerprint images. The authors extracted many distinguishable features through various texture measure methods such as, the curvelet transform [20, 21], the Gabor filters [22], the Ridgelet transform [23], and the wavelet transform [24]. All of these features can successfully address spoof fingerprint detection problem to some degree. Jin *et al.* [25] proposed a spoof fingerprint detection method based on band-selective Fourier spectrum. The authors revealed that the live fingerprint images showed stronger Fourier spectrum in the ring patterns than the spoof ones, and classified live and spoof fingerprint images by analyzing the band-selective Fourier spectral energies. Lee *et al.* [26] transformed the fingerprint image through 2D fast Fourier transform, and detected values along a specific line in the spectrum image. The line was transformed into the fractional Fourier domain. The standard deviation of the fractional Fourier domain coefficient was used as feature. Jia *et al.* [27] considered that the multi-scale local binary pattern (LBP) could reflect the texture of fingerprint images

more adequately than original LBP, and proposed a spoof fingerprint detection method by using two kinds of multi-scale LBP. Their method achieves good detection accuracy.

3. Feature Extraction Process

In this paper, the spoof fingerprint detection is considered as a two-class classification problem, *i.e.* classing a test fingerprint image into either a living or a spoof one. The framework of our method includes two parts: the training process and the testing process, as is illustrated in Figure 1. In the training process, a classifier is trained using the two classes of feature vectors. Then, the trained classifier is used to make the judgment. Feature extraction is a crucial step for classification problem. Based on the hypothesis that live and spoof fingerprint images possess different textures, a novel spoof fingerprint detection method based on image texture features is proposed. The second-order and third-order co-occurrence arrays are applied to extract texture features from the image gradients. Quantization operation and truncation operation are used to reduce the number of features. The features are utilized to compose the feature vector to train the classifier.

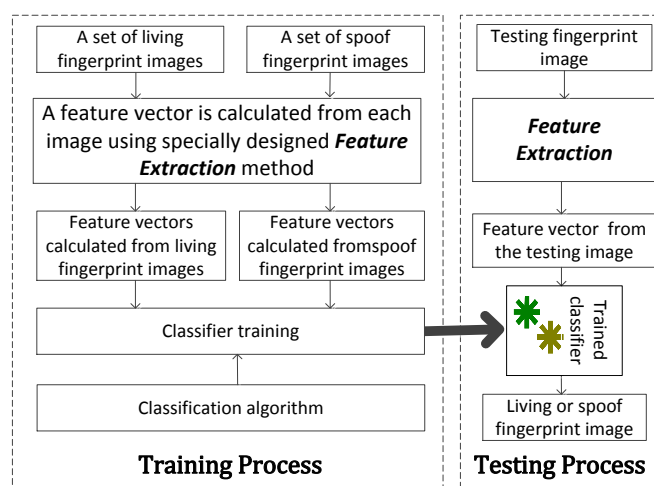


Figure 1. The Framework of the Proposed Method

In this paper, the symbol $\mathbf{X} = (X_{i,j}) \in \{0, \dots, 255\}^{n_1 \times n_2}$ represents an 8-bit grayscale image. The symbol $X_{i,j}$ denotes the grayscale value of the pixel located at (i, j) . The process of the feature extraction includes the following four steps. Firstly, the image is quantized by a quantization factor. Secondly, the horizontal and vertical differences are calculated from the adjacent quantized pixels. Thirdly, we truncate the differences of large absolute values into a reduced range. Finally, the co-occurrence matrix is calculated from the gradients. The elements of the co-occurrence matrix are used as the features.

3.1. Quantization

In the process of feature extraction, the image pixel values are firstly quantized as:

$$X_{i,j} \leftarrow \left\lfloor \frac{X_{i,j}}{Q} \right\rfloor, \quad (1)$$

where $Q \geq 1$ is a quantization factor. The quantization operation will cause the loss of image information, but will not affect the overall texture of a fingerprint image. The quantization operation can largely reduce the dynamic range of $X_{i,j}$, and thus help to reduce the dimensionality of the feature vector.

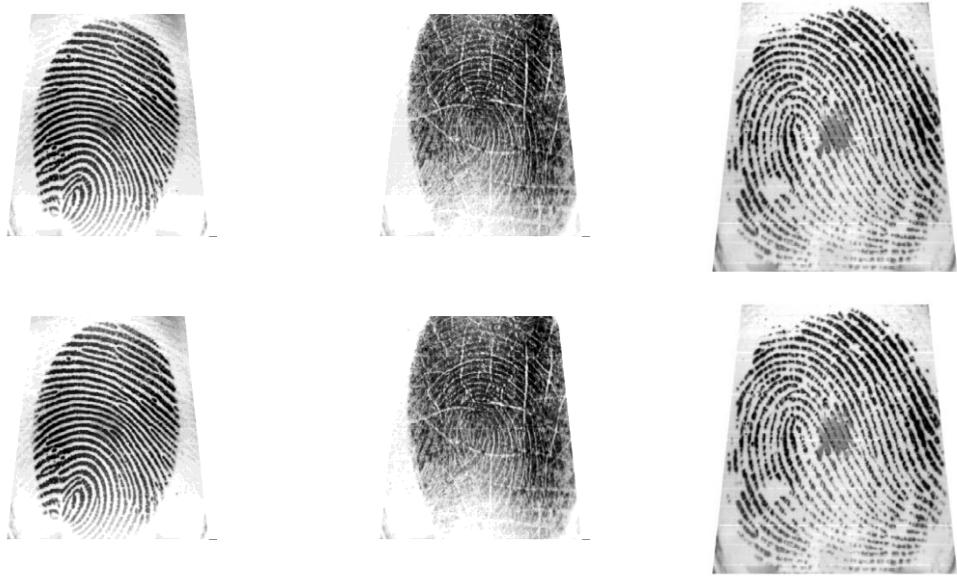


Figure 2. The Examples of Original Fingerprint Images (in the first row) and their Corresponding Quantized Images (in the second row, the quantization factor $Q = 16$)

3.2. Differences and Truncation

Image gradient measures a directional change in the intensity of an image, which can be used for robust and effective texture feature extraction. Here, the horizontal and vertical gradient arrays G_H and G_V are defined by calculating the differences between the adjacent pixels as

$$\begin{cases} D_H(i,j) = X_{i,j} - X_{i,j+1}, & \text{for } i \in \{0, \dots, n_1 - 1, j \in \{0, \dots, n_2 - 2, \} \\ D_V(i,j) = X_{i,j} - X_{i+1,j}, & \text{for } i \in \{0, \dots, n_1 - 2, j \in \{0, \dots, n_2 - 1, \} \end{cases} \quad (2)$$

In this paper, the elements of the co-occurrence matrix are directly used as features which are arranged to compose a feature vector. The dimensionality of the feature vector is depended on the dynamic range of the differences. As shown in Figure 3, the differences calculated from the quantized images have a narrower dynamic range than that from the original images. A large quantization factor could help to reduce the dimensionality of the feature vector. In addition, the histogram of the differences can be approximated by Laplacian distribution. Thus, we can truncate differences to a small range $[-T, T]$ without losing much useful information while largely reducing the dimensionality of the feature vector. The truncation operation is defined as

$$D(i,j) \leftarrow \text{trunc}_T(D(i,j)), \quad (3)$$

where $D(i,j)$ denotes the difference calculated according to Formula (2) along horizontal or vertical direction. If $D(i,j) > T$, $\text{trunc}_T(D(i,j)) = T$; if $D(i,j) < -T$, $\text{trunc}_T(D(i,j)) = -T$; if $D(i,j) \in [-T, T]$, $\text{trunc}_T(D(i,j)) = D(i,j)$.

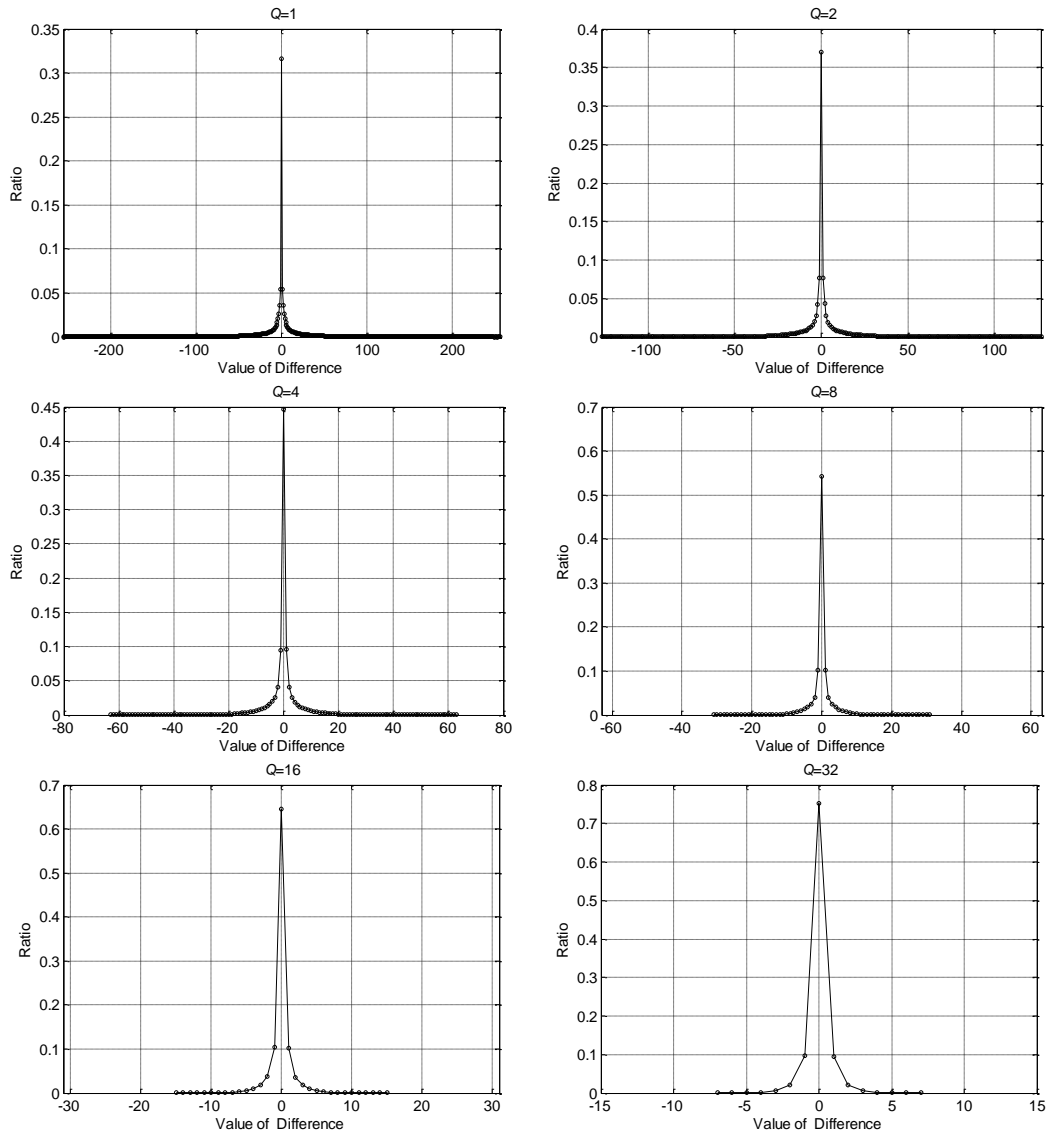


Figure 3. Histogram of Differences Calculated from Quantized Fingerprint Images along the Horizontal Direction, $Q = 1, 2, 4, 8, 16, 32$

3.3. Co-occurrence Matrix

In this paper, the co-occurrence matrix is calculated from the differences between adjacent pixels. And the dimensionality of co-occurrence matrix can be efficiently reduced by the proposed quantization and truncation operation. Thus, the elements of co-occurrence matrix can be directly used as features. Formally, the difference co-occurrence matrix ($DCoM$) is defined along horizontal and vertical directions as

$$\begin{cases} DCoM_H(s, t) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-3} \gamma(D_H(i, j), s) \times \gamma(D_H(i, j + 1), t) \\ DCoM_V(s, t) = \sum_{i=0}^{n_1-3} \sum_{j=0}^{n_2-1} \gamma(D_V(i, j), s) \times \gamma(D_V(i + 1, j), t) \end{cases} \quad (4)$$

where $s, t \in \{-T, \dots, T\}$, and $\gamma(x, y) = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{if } x \neq y \end{cases}$

In order to eliminate the effect caused the image size, the elements of the co-occurrence arrays can be normalized as

$$\begin{cases} DCoM_H(s, t) \leftarrow \frac{DCoM_H(s, t)}{\sum_{s=-T}^T \sum_{t=-T}^T DCoM_H(s, t)} \\ DCoM_V(s, t) \leftarrow \frac{DCoM_V(s, t)}{\sum_{s=-T}^T \sum_{t=-T}^T DCoM_V(s, t)} \end{cases}, \quad (6)$$

In this paper, the elements of co-occurrence matrix are directly used as texture features. Then, the dimensionality of the proposed feature vector ($DCoM$) equals to $2 \times (2T + 1)^2$.

4. Experiments

The performance of the proposed method is tested on two databases named LivDet09DB [28] and LivDet11DB [29]. In this section, we firstly present a brief introduction to these two databases and the support vector machine. Secondly, the comparative experiments are conducted on LivDet11DB to choose a proper quantization factor Q and truncation factor T . Finally, the proposed method with the chosen parameters is compared with the state-of-the-art works.

4.1. Databases and Evaluation Criterion

The proposed detection methods are tested on two databases, named LivDet09DB and LivDet11DB. The LivDet09DB is the database used in Spoof fingerprint Detection Competition 2009 [28]. It consists of images taken from three different sensors: Biometrika, Identix and Crossmatch. The spoof fingers are generated using three different materials: silicone, gelatin and playdoh. The LivDet11DB is the database used in Spoof fingerprint Detection Competition 2011 [29]. It consists of images from four different sensors: Biometrika, Digital Persona, Italdata and Sagem. The spoof fingers are generated using six different materials: gelatin, latex, PlayDoh, silicone, ecoflex and wood glue. All of the fingerprint images are transformed into gray images before being used. Each of the datasets has been divided into two non-overlapping parts: training and testing sets, which are used respectively in the training and testing processes of the classification. The general information of the databases are presented in Table 1. For the two databases, images captured from each sensor are tested separately.

Table 1. The Information of LivDet09DB and LivDet11DB

Database	Sensor	Resolution (dpi)	Image size	Number of images in Training set		Number of images in Testing set	
				live	spoof	live	spoof
LivDet09DB#1	Biometrika	569	312×372	520	520	1473	1480
LivDet09DB#2	Crossmatch	500	480×640	1000	1000	3000	3000
LivDet09DB#3	Identix	686	720×720	750	750	2250	2250
LivDet11DB#1	Biometrika	500	315×372	1000	1000	1000	1000
LivDet11DB#2	Digital Persona	500	355×391	1004	1000	1000	1000
LivDet11DB#3	ItalData	500	640×480	1000	1000	1000	1000
LivDet11DB#4	Sagem	500	352×384	1008	1008	1000	1036

In the experiment, the average classification error (ACE) of the trained classifier is defined as the evaluation criterion

$$ACE = (FAR + FRR)/2 \quad (9)$$

where FAR (False Accept Rate) is the proportion of spoof fingerprints being incorrectly accepted, and FRR (False Reject Rate) is the proportion of real fingerprints being incorrectly rejected.

4.2. Support Vector Machine (SVM)

SVM is utilized to train the classifier with feature vector in this paper. Treating the data as two sets of points in an n -dimensional space, SVM builds an separating hyperplane by Lagrangian multipliers to differentiate the negative data points from the positive ones [30]. Intuitively, a good separation is achieved when a separating hyperplane has the largest distance to the boundary points of both classes.

LIBSVM [31] is a free software for support vector classification. LIBSVM implements four basic kernels, among which the radial basis function (RBF) kernel is widely suggested as the best choice by the users. LIBSVM also provides a tool named “Cross-validation and Grid-search” to search the appropriate penalty parameter C and kernel parameter γ for RBF kernel. In this paper, the LIBSVM with RBF kernel is used to train classifiers in the experiments, and the tool “Cross-validation and Grid-search” is utilized to search the penalty parameter C and kernel parameter γ .

4.3. Selection of Parameters

It is needed to select a good pair of quantization factor Q and truncation factor T for a compact feature vector and good detection accuracy. Here, we conduct a comparison experiment on LivDet11DB to find out the better choice. First, we set $Q = 1, 2, 4, 8, 16, 32$ to quantize the images. Under each of the quantization step, we compute the average percentages of differences that fall into the range $[-T, T]$, which then help us to choose the truncation factor T . Generally, we want to take as many differences into consideration as possible in constructing feature vector. However, a larger T will lead to a feature vector of larger dimensionality. By compromising on the percentages of covered differences and the dimensionality of feature vector, we choose $T = 10$ when Q is set to 1, 2 and 4, $T = 5$ when Q is set to 8, and $T = 4$ when Q is set to 16 and 32. For each parameter pair (Q, T) , the dimensionality of *DCoM* feature vector and the average percentages of covered differences are listed in Table 2. Note that, it is not ensured that the parameters used here are the best choices.

Table 2. Dimensionality of *DCoM* Feature Vector and Ratio of Covered Differences when Different Parameter Pair (Q, T) is Chosen

(Q, T)	(1,10)	(2,10)	(4,10)	(8,5)	(16,4)	(32,4)
Dimensionality of <i>DCoM</i> feature vector	882	882	882	242	162	162
ratio of covered differences (%)	70.73	81.23	91.43	90.67	96.05	99.74

The different parameter pair (Q, T) produces different types of feature vectors. Each type of feature vector is used to train SVM classifiers separately. The detection accuracies of the classifiers are listed in Table 3. The parameter pairs (C, γ) used in the training process of classifiers are presented in Table 4

As shown in Table 3, the *DCoM* feature vectors extracted with the parameter pairs (8, 5) and (16, 4) achieve the best average detection result. When the quantization factor Q is set to 4, we need to set the truncation factor T to 10 so as to cover 91.43% of gradients, generating 882 features. When the quantization factor Q is set to 8, we need to set the truncation factor T to 5 so as to cover 90.67% of gradients, generating only 242 features. However, the feature vectors extracted with the parameter pair (8, 5) achieve better detection accuracy than that with (4, 10). This tells us that the quantization operation with a suitable factor will help to extract better features and reduce the dimensionality of the feature vector.

Table 3. The Average Classification Error (ACE) of DCoM Features Calculated with different Parameter Pair (Q, T)

Parameter pair (Q, T)	Average classification error (ACE) (%)				
	LivDet11DB#1	LivDet11DB#2	LivDet11DB#3	LivDet11DB#4	Average
(1,10)	15.70	15.40	16.50	5.50	15.78
(2,10)	12.25	17.50	22.35	5.45	14.39
(4,10)	8.95	13.65	20.95	4.91	12.12
(8,5)	8.00	14.15	16.90	4.86	10.98
(16,4)	8.45	15.35	14.85	5.26	10.98
(32,4)	10.45	15.90	18.15	7.56	13.02

Table 4. The Parameter Pair (C, γ) used in Training Process with DCoM Features Calculated with Different Parameter Pair (Q, T)

Parameter pair (Q, T)	Parameter pair (C, γ)			
	LivDet11DB#1	LivDet11DB#2	LivDet11DB#3	LivDet11DB#4
(1,10)	(2048,16)	(8192,16)	(524288,2)	(262144,8)
(2,10)	(524288,4)	(1024,256)	(2097152,4)	(1024,16)
(4,10)	(262144,1)	(4096,16)	(524288,16)	(16777216,0.5)
(8,5)	(8192,32)	(131072,16)	(262144,16)	(65536,8)
(16,4)	(262144,2)	(2097152,4)	(2097152,4)	(262144,4)
(32,4)	(2097152,4)	(2097152,4)	(524288,4)	(4096,16)

4.4. Comparison with Previous Methods

According to the results in Table 3 we choose the parameter pair (16,4) to compare with the previous methods.

As shown in Table 5 and 6, the proposed method outperforms the previous methods. Note that, in the training process of our classifier on LivDet09DB, the penalty and kernel parameter pair (C, γ) are set to (262144, 1), (8192,0.5) and (65536,1) for LivDet09DB#1, #2 and #3, respectively.

Table 5. Performance Comparison in Terms of Average Classification Error (ACE) on LivDet11DB

Methods	Average classification error (ACE) (%)				
	LivDet11DB#1	LivDet11DB#2	LivDet11DB#3	LivDet11DB#4	Average
DCoM	8.45	15.35	14.85	5.26	10.98
Best result in LivDet 2011 [29]	20.0	36.1	21.8	13.8	22.925
Original LBP[32] reported in [27]	13.0	10.8	24.1	11.5	14.85
Tan's method [7] reported in [27]	43.8	18.2	29.6	24.7	29.075
Valleys wavelet [33] reported in [34]	29.0	13.0	23.6	28.0	23.4
Curvelet GLCM [20] reported in [34]	22.9	18.3	30.7	28.0	24.975
Wavelet energy [24] reported in [34]	50.2	14.0	46.8	22.0	33.25

Table 6. Performance Comparison in Terms of Average Classification Error (ACE) on LivDet09DB

Methods	Average classification error (ACE) (%)			
	LivDet09DB#1	LivDet09DB#2	LivDet09DB#3	Average
DCoM	10.4	6.7	3.2	6.8
Best result in LivDet 2009 [28]	18.2	9.4	2.8	10.1
Marasco et al. [8]	12.6	15.2	9.7	12.5
Moon et al [13] reported in [8]	23.0	23.5	38.2	28.2
Nikam et al. [21] reported in [8]	28.3	18.7	30.3	25.8

5. Conclusions

In this paper, we regard the spoof fingerprint detection as a two-class classification problem, and have presented a novel software-based spoof fingerprint detection method which achieves good detection accuracy. Firstly, quantization operation is applied to reduce the dynamic range of pixel value, which not only helps to decrease the dimensionality of feature vector but also generates more useful features. Secondly, image differences are calculated from adjacent quantized pixels along horizontal and vertical directions. It is observed that most of the differences have an absolute value near to zero and the histogram of the differences can be approximated by Laplacian distribution. Therefore, we can truncate the differences into a reduced range with a properly selected threshold without losing much useful information. The experimental results have demonstrated that the proposed method outperform many state-of-the-art methods in general.

Acknowledgements

This work is supported the 12th five year programming of scientific research in education of Hunan Province (Design and Study of constructing Flipped Class Model teaching based on the "Instructed learning plan + microlecture, No. XJK015BGD018).

References

- [1] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey", *IET Biometrics*, vol. 2, no. 1, (2014), pp. 1-15.
- [2] A. Al-Ajlan, "Survey on fingerprint liveness detection", In *International Workshop on Biometrics and Forensics*, vol. (2013), pp. 1-5.
- [3] G. L. Marcialis, F. Roli and A. Tidu, "Analysis of Fingerprint Pores for Vitality Detection", In *International Conference on Pattern Recognition*, vol. (2010), pp. 1289 - 1292.
- [4] N. Manivanan, S. Memon and W. Balachandran, "Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering", *Electronics Letters*, vol. 46, no. 18, (2010), pp. 1268 - 1269.
- [5] R. Derakhshani, S. A. Schuckers, L. A. Hornak and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners", *Pattern recognition*, vol. 36, no. 2, (2003), pp. 383-396.
- [6] A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition", *Pattern recognition*, vol. 42, no. 3, (2009), pp. 452-464.
- [7] B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise", *Pattern recognition*, vol. 43, no. 8, (2010), pp. 2845-2857.
- [8] E. Marasco and C. Sansone, "Combining perspiration-and morphology-based static features for fingerprint liveness detection", *Pattern Recognition Letters*, vol. 33, no. 9, (2012), pp. 1148-1156.
- [9] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "A New Approach to Fake Finger Detection Based on Skin Distortion", In *International Conference on Advances in Biometrics*, vol. (2006), pp. 221-228.
- [10] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake finger detection by skin distortion analysis", *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 3, (2006), pp. 360-373.
- [11] Y. Zhang, J. Tian, X. Chen, X. Yang and P. Shi, "Fake finger detection based on thin-plate spline distortion model", In *International conference on Advances in Biometrics*, vol. (2007), pp. 742-749.
- [12] J. Jia and L. Cai, "Fake finger detection based on time-series fingerprint image analysis", In *International Conference on Intelligent Computing*, vol. (2007), pp. 1140-1150.
- [13] Y. S. Moon, J. Chen, K. Chan, K. So and K. Woo, "Wavelet based fingerprint liveness detection", *Electronics Letters*, vol. 41, no. 20, (2005), pp. 1112-1113.
- [14] C. Jin, S. Li, H. Kim and E. Park, "Fingerprint liveness detection based on multiple image quality features", In *International Workshop on Information Security Applications*, vol. (2011), pp. 281-291.
- [15] J. Galbally, F. Alonso-Fernandez, J. Fierrez and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features", *Future Generation Computer Systems*, vol. 28, no. 1, (2012), pp. 311-321.

- [16] L. F. A. Pereira, N. B. Pinheiro, G. D. C. Cavalcanti and T. I. Ren, "Spatial surface coarseness analysis: technique for fingerprint spoof detection", *Electronics Letters*, vol. 49, no. 4, (2013), pp.
- [17] J. Galbally, S. Marcel and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition", *IEEE Transactions on Image Processing*, vol. 23, no. 2, (2014), pp. 710-724.
- [18] A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques", In *International Conference on Image Processing*, vol. (2006), pp. 321-324.
- [19] P. Coli, G. L. Marcialis and F. Roli, "Power spectrum-based fingerprint vitality detection", In *IEEE Workshop on Automatic Identification Advanced Technologies*, vol. (2007), pp. 169-173.
- [20] S. Nikam and S. Agarwal, "Fingerprint Liveness Detection Using Curvelet Energy and Co-Occurrence Signatures", In *International Conference on Computer Graphics, Imaging and Visualisation*, vol. (2008), pp. 217-222.
- [21] S. B. Nikam and S. Agarwal, "Curvelet-based fingerprint anti-spoofing, *Signal, Image and Video Processing*", vol. 4, no. 1, (2010), pp. 75-87.
- [22] S. B. Nikam and S. Agarwal, "Gabor Filter-Based Fingerprint Anti-spoofing", In *International Conference on Advanced Concepts for Intelligent Vision Systems*, vol. (2008), pp. 1103-1114.
- [23] S. B. Nikam and S. Agarwal, "Ridgelet-based fake fingerprint detection", *Neurocomputing*, vol. 72, no. 10, (2009), pp. 2491-2506.
- [24] S. B. Nikam and S. Agarwal, "Texture and Wavelet-Based Spoof Fingerprint Detection for Fingerprint Biometric Systems", In *International Conference on Emerging Trends in Engineering and Technology*, vol. (2008), pp. 675-680.
- [25] C. Jin, H. Kim and S. Elliott, "Liveness detection of fingerprint based on band-selective Fourier spectrum", In *International Conference on Information Security and Cryptology*, vol. (2007), pp. 168-179.
- [26] H.-s. Lee, H.-j. Maeng and Y.-s. Bae, "Fake finger detection using the fractional Fourier transform", In *International Conference on Biometric ID Management and Multimodal Communication*, vol. (2009), pp. 318-324.
- [27] X. Jia, X. Yang, K. Cao, Y. Zang, N. Zhang, R. Dai, X. Zhu and J. Tian, "Multi-scale local binary pattern with filters for spoof fingerprint detection", *Information Sciences*, vol. 268, (2014), pp. 91-102.
- [28] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, F. Roli, D. Grimberg, A. Congiu, A. Tidu, S. Schuckers and t.L. Group, *First International Fingerprint Liveness Detection Competition-LivDet 2009*, In *International Conference on Image Analysis and Processing*, vol. (2009),
- [29] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli and S. Schuckers, "LivDet 2011—Fingerprint liveness detection competition 2011", In *International Conference on Biometrics*, vol. (2012), pp. 208-215.
- [30] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition", *Data Mining and Knowledge Discovery*, vol. 2, no. 2, (1998), pp. 121-167.
- [31] C.-C. Chang and C.-J. Lin, "LIBSVM: a library for support vector machines", In vol. 2010, (2001),
- [32] T. Ojala, M. Pietikäinen and D. Harwood, "A comparative study of texture measures with classification based on featured distributions", *Pattern recognition*, vol. 29, no. 1, (1996), pp. 51-59.
- [33] B. Tan and S.C. Schuckers, "New approach for liveness detection in fingerprint scanners based on valley noise analysis", *Journal of Electronic Imaging*, vol. 17, no. 1, (2008), pp. 9.
- [34] L. Ghiani, P. Denti and G. L. Marcialis, "Experimental results on fingerprint liveness detection", In *International Conference on Articulated Motion and Deformable Objects*, vol. (2012), pp. 210-218.

Authors



Yujia Jiang, she received her BS at Artistic Design Department of Jilin Teacher's College of Engineering and Technology, China, in 2001, MS at Artistic Design Department of Jilin Art College, China, in 2005. She works as a lecturer at College of Architecture and Artistic Design Department in Hunan Institute of Technology. Her research interests include information security, image processing, and artistic design.



Xin Liu, he received his BS at Artistic Design Department of Jilin Teacher's College of Engineering and Technology, China, in 2001, MS at Artistic Design Department of Jilin Art College, China, in 2004. He works as a lecturer at College of Architecture and Artistic Design Department in Hunan Institute of Technology. His research interests include information security, image processing, and animation production.