International Journal of Grid and Distributed Computing
Vol. 9, No. 10 (2016), pp.65-78
http://dx.doi.org/10.14257/ijgdc.2016.9.10.06

Fingerprint Liveness Detection Using Gray Level Co-Occurrence Matrix Based Texture Feature

Chengsheng Yuan[1,2], Zhihua Xia[1,2], Xingming Sun[1,2], Decai Sun[3] and Rui Lv[1,2]

[1]School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China
[2]Jiangsu Engineering Center of Network Monitoring, Nanjing 210044, China
[3]College of Information Science and Technology, Bohai University, Jinzhou 121013, China
ycs_nuist@163.com, xia_zhihua@163.com, sunnudt@163.com, sdecai@163.com, lrain_nuist@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 using an accurate imitation of a real fingerprint such as an artificially made fingerprint. In this paper, we propose a novel software-based fingerprint liveness detection algorithm based on gray level co-occurrence matrix (GLCM), from which we can calculate the texture features of fingerprint images and obtain satisfactory results. For the first time, we extract texture features by constructing four-direction GLCMs in an image, and then quantization operation and normalization operation are adopted. After these, we detected whether a fingerprint image belongs to a real fingerprint or an artificial replica of it. A trained RBF SVM (support vector machine) classifiers scheme is used to make the final live/spoof decision via training and testing feature vectors. The experimental results reveal that our proposed method can discriminate between live fingerprints and fake ones with high classification accuracy.

***Keywords**: Fingerprint-based recognition Systems, Fingerprint liveness detection, Support Vector Machine, Gray Level Co-Occurrence Matrix, quantization, normalization*

1. Introduction

Nowadays, fingerprint has been used as biometric characteristics in forensic practice and science, but personal information safety has been an important issue. Because biometric recognition is considered to be more reliable than traditional passwords, increasingly more biometric recognition systems have been deployed in civilian and government applications [1], such as attendance systems, access control for recreation areas or fitness-centers, and so on [3]. Among these, the fingerprint recognition systems account for the vast majority part [2].

However, it is possible to deceive fingerprint recognition systems by presenting a well-duplicated artificial fingerprint [4]. Artificial fingerprints, which carry the identity of enrolled users and created to attempt to gain unauthorized access, are referred as spoof [4]. The attackers can make a spoof fingerprint to achieve unauthorized access.

In order to prevent the fraudulent attempts of fake fingers and judge whether a fingerprint is acquired from a real user or not, many fingerprint liveness detection techniques have been proposed. Among these, there are two major kinds of liveness detection methods: hardware-based methods applied at acquisition stage, and software-based methods applied at processing stage [3-5]. The hardware-based methods use some specific devices installed on the sensors to detect fingerprint liveness characteristics, such

ISSN: 2005-4262 IJGDC

as fingerprint sweat, pulse and electric resistance. These methods can achieve the fingerprint image liveness detection, but they can lead to a higher fake detection rate. What is more, these methods are more expensive and more complex, since you do need extra devices which raise the cost of the fingerprint liveness detection. In contrast, the software-based methods which have become active in recent year and not need additional sensor devices are cheaper and more convenient to realize fingerprint liveness detection. The fingerprint liveness detection techniques could be embedded in the feature extractor module which makes them distinguish the fake fingerprint by analyzing images features without extra hardware devices, and they are more flexible to the future fingerprint image research.

In this paper, we propose a novel software-based texture feature fingerprint liveness detection algorithm. In our method, we divide the fingerprint liveness detection into two processes: training process and testing process. During the two processes, feature extraction is critical step for judging the fingerprint liveness. For the first time, feature vectors are composed by constructing four gray level co-occurrence matrices which is the number of occurrences of pixels pair of a fingerprint image in a specified direction and distance between two appointed pixels to detect whether a fingerprint image belongs to a real fingerprint or an artificial replica of it. Specifically, we construct four gray level co-occurrence matrices in the four directions 0 degree, 45 degree, 90 degree and135 degree. After these, five texture parameters are obtained using gray level co-occurrence matrix formed a new characteristic of the fingerprint image to represent the different textural information. Quantization operation, which reduces the dimensionality of feature vector without reducing the classification accuracy of recognition for the fingerprint image, is introduced. Finally, the extracted texture features are tested by using the SVM classifiers.

The rest of the paper is structured as follows. Some of the relevant concepts in software-based fingerprint liveness detection methods are presented in Section II. Section III describes our proposed method about the feature vector extraction process. The result and comparison for the fingerprint liveness detection appear in Section IV. The basic questions posed above are then discussed and conclusions are finally drawn in Section V.

2. Related Work

The software-base fingerprint liveness detection methods show that the real and spoof fingerprints can be distinguished by analyzing the features extracted from fingerprint images. Sweat pores, perspiration, image quality, skin elasticity, image texture and so on. These properties are all considered as image features. As in Figure 1, in order to illustrate these concepts, we divide the software fingerprint liveness detection methods into five categories: Perspiration-based, Skin Deformation-based, Image Quality-based, Sweat Pore-based and Texture Feature-based.

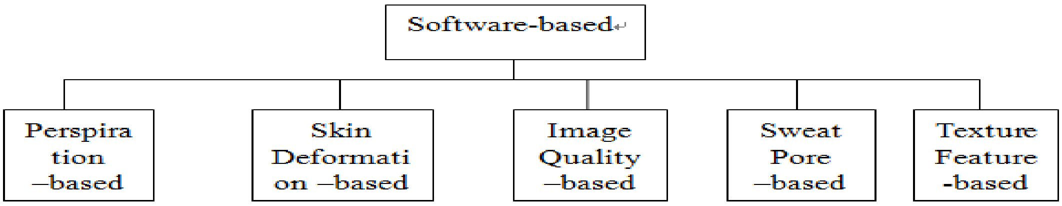


Figure 1. Software-Based Fingerprint Liveness Detection Method

Perspiration-Based Methods: Because only real fingerprints can perspire, we can detect the fingerprint through analysis of image sweat. However, many scholars have shown that this method is unsafe via experiment research. Since this method is easily affected by a series of characteristic factors including pressure sensitive finger, environment and time interval, etc. Derakhshai *et. al.,* [10] proposed a method which is based on wavelet to detect fingerprint liveness through analyzing perspiration feature using two fingerprints captured at zero second and after five seconds [11-12] in 2004, in order to improve the accuracy of this method, Abhyankar *et. al.*, further research via increasing the datasets and decreasing the time between capturing images. After that, Tan and Schuckers [14] claimed that a new method based on perspiration pattern detect the fingerprint liveness was proposed using only one fingerprint image. The downside, of course, is that perspiration of moisture structure of skin around sweat pores is easy to cause static and dynamic patterns change.

Skin Deformation-Based Methods: Compared with the fake fingerprints, the real fingerprints can have a better skin elasticity. When fingers press and rotate on the fingerprint sensor, different hardness materials will generate different fingerprint deformation. Therefore, we can detect the fingerprint liveness by compare and test the distortion. The key to method material lies in the differences of hardness. Zhang *et. al.,* [13] conducted an experiment that the user was asked to rotate his finger in four angles 0, 90, 180, 270 to capture different direction images when he placed his finger into the scanner surface. From capturing finger distortion images, using Thin-plate Spline model extract relevant features related to skin distortion. However, Tan and Schuckers [7] observed and pointed out deformation-based method, in which some disadvantages that testers have been trained.

Image Quality-Based Methods: In fact, it is difficult to forge a living fingerprint image with the same or better quality fingerprint images. In general, fake fingerprint image quality is not as good as the living fingerprint image. Choi *et. al.,* [20] proposed method which extracted many static features. It is a highly competitive detection accuracy compared with the state-of-the-arts. In 2005, Maltoni *et. al.*, [2] detected the liveness through using some high resolution fingerprint images (1000 dpi), which were based on fingerprint surface coarseness feature. And Maltoni *e.t al.*, [2] treated the coarseness that is arisen by the ridge and valley in the fingerprint.

Sweat Pore-Based Methods: Generally speaking, when the fingerprint images are magnified several times under a microscope, living fingerprints can be seen small holes with pore shape, while in the fake fingerprints we cannot observe small holes. Manivanan *et. al.*, [15] proposed a new method to detect fingerprint liveness based on pores as a sign of fingerprint. The key to the method that this paper applies two filtering techniques: highpass filter which was used to extract active sweat pore and correlation filter which was used to locate the position of pores. Espinoza *et. al.,* [9]claimed that they can use pores as a liveness sign and research the possibility of generating pores in spoof fingers. And this method is based on comparing pore quantity which was between query image and the recorded one at time 0 second and 5 seconds. Marcialis *et. al.*, [16] proposed a new fingerprint liveness detection method, this is an important work of sweat pores.

Texture Feature-Based Methods: Texture feature is a kind of important visual clues, which is widespread in the image. However, it is difficult in describing the texture features of fingerprint images. In 2006, Abhyankar and Schuckers [17] proposed a fingerprint liveness detection method, which is used to minimize the energy associated with phase and orientation maps, multiresolution texture analysis techniques are used. Besides, cross ridge frequency analysis of fingerprint images is performed through statistical measures and weighted average phase. These different features along with ridge reliability or ridge center frequency are given as inputs to a fuzzy c-means classifier. Jhat *et. al.*, [18] extractd texture features by an algorithm based on the spatial gray level dependence method, which proposed use of the statistical texture analysis of a fingerprint using spatial gray level dependence method (SGLDM) for personal verification and discrimination. Nikam and Agarwal [19] proposed a fingerprint liveness detection texture-based method, where the fundamental basis of this paper is that real fingerprint exhibits different textural characteristics from a fake fingerprint using the anti-spoofing method.

3. Feature Extraction

Fingerprint liveness detection can be considered as a two-class classification problem, which divides an input fingerprint into either a set of living or a fake one. Therefore, it is important for us to extract a suitable features detecting the vitality of a given fingerprint image using SVM classifier. The general diagram of our method is shown in Figure 2, which mainly include two parts: the training process and the testing process. In this paper, based on the hypothesis that the live and fake fingerprint images have different textures, we proposed a fingerprint liveness detection method based on GLCM. GLCM is applied to the images to extract minute texture features. It is described by second-order statistics, such as the probability of the pair of two adjacent pixels having particular gray levels at particular spatial relationships. Firstly, we obtain probability that the two adjacent pixels having particular gray levels at particular directions (We can work out four gray level co-occurrence matrices in four directions 0 degree, 45 degree, 90 degree and 135 degree). Secondly, we treat the values of five texture feature parameters (Angular Second Moment, Entropy, Inverse Differential Moment, Moment of Inertia and Correlation) as the image texture features using GLCM. Then, quantization operation and normalization are used to reduce the grayscale and remove the influence of abnormal values. Finally, the texture feature parameters are trained using SVM classifier.

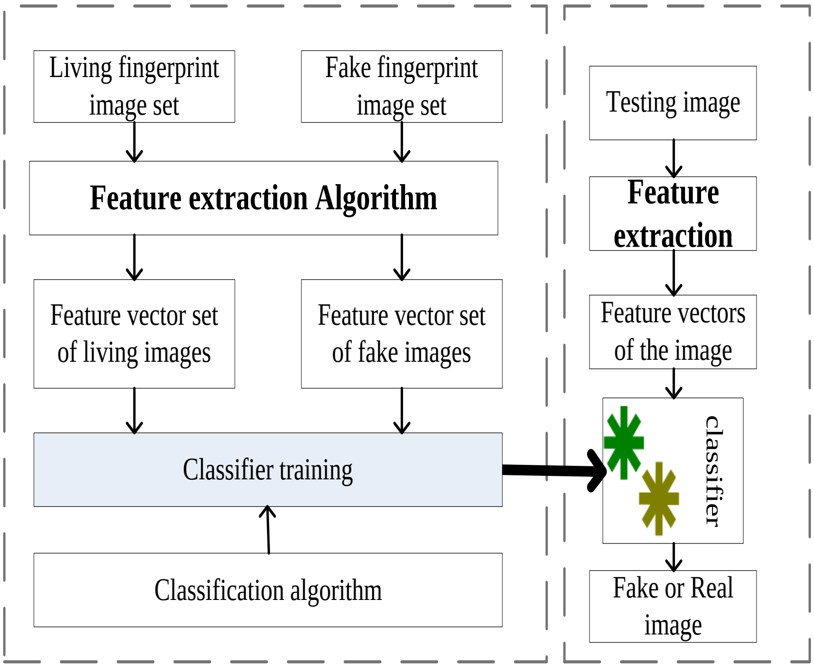

Living fingerprint image set
Fake fingerprint image set
Feature extraction Algorithm
Feature vector set of living images
Feature vector set of fake images
Classifier training
Classification algorithm
Testing image
Feature extraction
Feature vectors of the image
classifier
Fake or Real image

Figure 2. The General Diagram of Our Proposed Method

In this paper, we use a symbol X representing an 8-bit gray image, and the equation X is:

$$X = (X_{i,j}) \in \{0,..,255\}^{n_1 \times n_2} \tag{1}$$

In the Equation (1), $X_{i,j}$ denotes the gray value of the pixel which is located at (i, j). The range of $X_{i,j}$ is $\{0,..,255\}$, and $n_1 \times n_2$ denotes the size of the image. The feature extraction operations are as follows. Firstly, in order to reduce the dimensionality of gray level, we use the specified quantization factor to quantify images. Secondly, at the same distance (the distance is 1), we obtain four directions(in the 0 degree, 45 degree, 90 degree and the 135 degree) co-occurrence matrices. Thirdly, four co-occurrence matrices are normalized respectively. Finally, five different values of parameters, which compose feature vectors of images, are calculated according to the GLCM. The experiment results reveal that our method, compared with the state-of-the-arts, makes the classification accuracy enhance.

3.1. Quantization

In general, the number of gray levels is so large (such as 8 bit for level 256), which makes the calculation complex. In order to reduce the amount of calculation and the dimensionality of the feature vectors, meanwhile, improve the accuracy of classification, the quantization operation is taken into account. For instance, we can make grayscale level reduce from 256 levels to 16 levels using the Equation (2). The quantization operation substantially decreases the computational cost through reducing the range of $X_{i,j}$. In the meantime, it also helps to reduce the dimensionality of the feature vector and maintains an optimal performance in terms of the classifier of the feature vector. Quantization formula is:

$$G_{i,j} \leftarrow \lfloor G_{i,j} / Q \rfloor \tag{2}$$

The symbol $G_{i,j}$ denotes the grayscale value of the pixel which is located at (i, j), and the scope of grayscale value of $G_{i,j}$ is $\{0,..,255\}$.In formula (2) Q is a quantization factor, and the value of which is greater than or equal to 1. Though quantization operation can reduce the quality of the images, the influence of the image texture is really low.

3.2. Normalization

Normalization refers to the image moment invariant which finds a set of parameters to eliminate the influence of other transformation function of image transformation. Image normalization makes image resist geometry transform attack, and it can identify the invariant in the image. Through it, we can learn that these images either are as same as the original one, or a same series.

In our method, the normalized operation is following:

$$M(i,j) = G(i,j) / \sum_{i=1}^{k} \sum_{j=1}^{k} G(i,j) \tag{3}$$

In Equation (3), a molecule denotes the grayscale value after normalization. And the first $G(i,j)$ is the grayscale value after a given pixel value of quantification, denominator is the summation of image pixel values. After quantification, the entire pixel values are mapped in the interval [0- 1].

3.3. Gray Level Co-Occurrence Matrixes

Usually, GLCM is a matrix function of pixel distance and angle, which can not only reflect the distribution characteristics of brightness, but also describe the texture feature of given images. GLCM can be computed for the whole image, or for small windows around pixel values. The size value of image $F(x,y)$ of is $M \times N$, and the gray level of images is K. Though the given image gray is 256, in the calculation of the gray level co-occurrence matrix derived texture features, gray level of the image is much less than 256. Mainly because the matrix dimension is larger and the window size is smaller, gray level co-occurrence matrix is not good texture representation; meanwhile, the amount of calculation is greatly increased. So before computing the gray level co-occurrence matrix, it is necessary to make the histogram of the image, so as to reduce the gray level of the image, and the gray level of the image is 8 or 16. The formula of construction of gray level co-occurrence matrix of given image is following:

$$P(i,j,d,\theta)=\#\{(x_1,y_1),(x_2,y_2)\in M\times N \mid f(x_1,y_1)=i,\ f(x_2,y_2)=j,\\ d\in Z,\theta\in\{0^{\circ},45^{\circ},90^{\circ},135^{\circ}\}\} \tag{4}$$

In Equation (4), the size of gray level co-occurrence matrix of appointed image is $K\times K$, and $\#(x)$ denotes the number of the set of x. For example, $P(i,j)$ denotes that the pair of gray value i and gray value j which is located with an inter sample distance d and a direction θ. Firstly, we randomly select a point in the image (x_1,y_1), where the pixel value is $f(x_1,y_1)$. Secondly, selecting different point (x_2,y_2), which deviates from point (x_1,y_1), we can get the different pixel values. The gray level of image is k, so there are k^2 kinds of combinations of f_1 and f_2 (f_1 denotes the grayscale value of point (x_1,y_1), f_2 denotes the grayscale value of point (x_2,y_1)). Last but not least, we can compute each gray value (f_1,f_2) the number of occurrences in the whole image, and get a size of $K\times K$ GLCM. The distance between (x_1,y_1) and (x_2,y_2) is d, and the angle of two different pixels is θ. Therefore, we can describe the GLCM using symbol $P(i,j,d,\theta)$. In this symbol, (i,j) denotes position of gray level, d denotes the distance between two different pixels, θ denotes the angle of them. In our method, we set the value of distance d as 1 and θ as 0 degree, 45 degree, 90 degree and 135 degree respectively. In order to make readers better understand the structure of the gray level co-occurrence matrix, we did a demonstration of a part of image. Table 1 shows an example of the calculation of GLCM. The Table 1 (a), is the part of a given image, and the gray level of the image is processed from 64 to 4. In the case of (0, 1), the value of $P(0,1,1,0^{\circ})$ is 10 in Table 1 (b). That is to say, the frequency of occurrences of pair of gray value 0 and gray value 1 when the distance is 1 and the direction is 0° is 10 in the Table 1 (a). Similarly, the value of $P(1,2,1,0^{\circ})$ is 11. While the θ changes from 0° to 45°, $P(1,1,1,45^{\circ})$ denotes the number of occurrences of adjacent pixel gray values $P(1,1)$ in the Table 1 (a), on the direction of 45 degree when the distance is 1 between two pixels, after that, writing the results of calculation on the corresponding coordinates in Table 1 (c).

According to the above process, we can compute four GLCMs when the angle is 0 degree, 45 degree, 90 degree and 135 degree respectively. Next, using GLCM, we can calculate texture features reflecting the state of GLCM. In our method, compared with some parameters [26], we select some typical and universal characteristics as the fingerprint image texture features, such as Angular Second Moment, Entropy, Inverse Differential Moment, Moment of Inertia and Correlation.

Since angular second moment is the sum of the squares of the gray level co-occurrence matrix elements, we also consider it as energy. The function is that reflects the fingerprint image grayscale distribution uniformity and the degree of texture thickness. The bigger values of the angular second moment indicate a relatively homogenous texture patterns and the change of image textures. And ASM is defined as:

$$ASM=\sum_{i=1}^{k}\sum_{j=1}^{k}(P(i,j))^2\ , \tag{5}$$

Entropy is the measurement of the information of image. From the value of the entropy, we can see the degrees of non-uniform or complexity of the image texture and the more elements of CLCM scatters, the larger the value of the image entropy. The Entropy is defined as:

$$E = -\sum_{i=1}^{k}\sum_{j=1}^{k} P(i, j)logP(i, j) \tag{6}$$

Inverse differential moment reflects the homogeneity of image texture, so we can compute the change of image textures. If the value of it is big, indicating the different regions of image texture lack of change and changing very evenly in local area. And the inverse differential moment is defined as:

$$I = \sum_{i=1}^{k}\sum_{j=1}^{k}\frac{P(i, j)}{1+(i - j)^2} \tag{7}$$

Moment of inertia reflects the degree of clarity and texture grooving depth of images. The more the pixel gray level difference, the greater the CON. And the CON is defined as:

$$CON = \sum_{i=1}^{k}\sum_{j=1}^{k}(i - j)^2 * P(i, j) \tag{8}$$

Correlation measures the similar degree of spatial GLCM elements of the row or column direction, and the size of the correlation reflects the local gray correlation. When matrix element values are equal in the image, the correlation is relatively large. If there is a level direction texture, the horizontal COR is greater than the rest of matrices COR values. And Correlation is defined as:

$$C = \sum_{i=1}^{k}\sum_{j=1}^{k}\frac{(i \cdot j)P(i, j) - u_i u_j}{s_i s_j} \tag{9}$$

Where in Equation (8), u_i, u_j, s_i^2 and s_j^2 represent as respectively:

$$u_i = \sum_{i=1}^{k}\sum_{j=1}^{k} i \cdot P(i, j), \qquad u_j = \sum_{i=1}^{k}\sum_{j=1}^{k} j \cdot P(i, j),$$

$$s_i^2 = \sum_{i=1}^{k}\sum_{j=1}^{k} P(i, j)(i - u_i)^2, \qquad s_j^2 = \sum_{i=1}^{k}\sum_{j=1}^{k} P(i, j)(j - u_i)^2$$

In our paper, we can calculate five different parameter values using GLCM. Five different parameter values can be considered as texture features corresponding to GLCM. Because our method needs to compute four directions GLCMs, each fingerprint image can calculate 20 parameters, and 20 parameter values can form a feature vector of image.

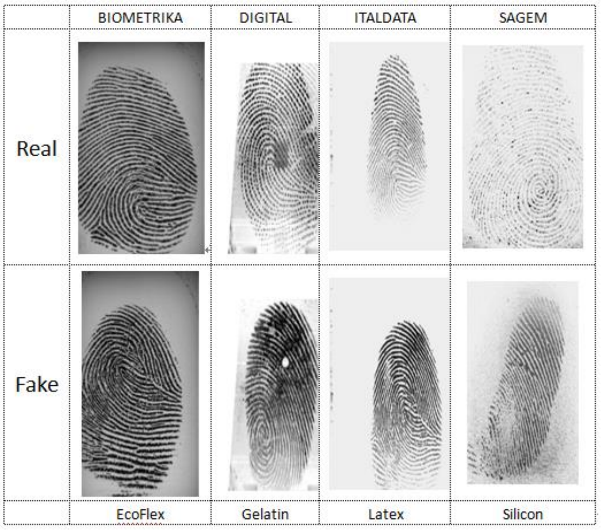
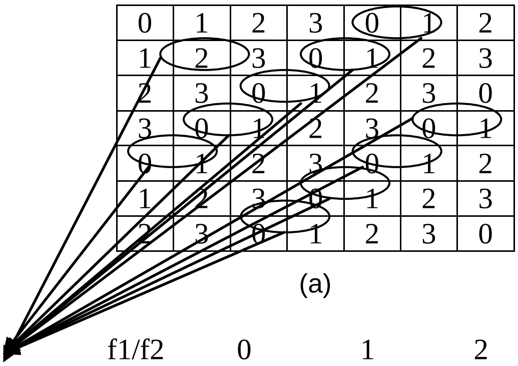


Figure 3. Samples of Real and Spoof Fingerprint Images That Can Be Found in the LivDet Public Database

Table 1. Fingerprint Image Matrix: (a) Grayscale Value of the Fingerprint Image Matrix, (b) Gray Level Co-Occurrence Matrix when $d = 1, \theta = 0^{\circ}$, (c) Gray Level Co-Occurrence Matrix when $d = 1, \theta = 45^{\circ}$



0	1	2	3	0	1	2
1	2	3	0	1	2	3
2	3	0	1	2	3	0
3	0	1	2	3	0	1
0	1	2	3	0	1	2
1	2	3	0	1	2	3
2	3	0	1	2	3	0

(a)

f1/f2	0	1	2	3
0	0	10	0	0
1	0	0	11	0
2	0	0	0	11
3	10	0	0	0

(b)

f1/f2	0	1	2	3
0	8	0	0	0
1	0	9	0	0
2	0	0	10	0
3	0	0	0	9

(c)

4. Experiment

The performance of the proposed fingerprint liveness detection method is achieved by using two different databases: the publicly available dataset provided in the Fingerprint Liveness Detection Competition, LivDet 2009 [6] and LivDet 2011 [21]. In this section, firstly, we will present a brief introduction about the two databases and estimate the performance of our proposed method using the Average Classification Error (ACE). Secondly, the support vector machine is also introduced. Finally, we conduct experiment results on LivDet2011 database [21], besides we will compare the state-of-the art works with our proposed method.

4.1. Database and Validation Criterion

For the fingerprint liveness detection, the performance of our method is tested using LivDet 2009 [6], which comprising over 18,000 real and fake samples and LivDet 2011 [21], which comprising over 16,000 real and fake samples. The two databases are used in Fingerprint Liveness Detection Competition 2009 and 2011 respectively. The former database comprises three datasets of real and spoof fingerprints which are captured using three different flat optical sensor: 1) Biometrika FX2000 (569 dpi), 2) CrossMatch Verifier 300LC (500 dpi), 3) Indentix DFR2100 (686 dpi). Details are described in Table 2. And the fake fingerprint can be generated using three different kinds of materials: gelatin, playdoh and silicone. Figure 3 presents some typical samples of real and fake fingerprint images which can be found in the LivDet Public Dtabase 2011. At the same time, we also list some common fake fingerprints which use different materials. In Figure 3, we can find that it is difficult to distinguish the differences between different fingerprint images, and even the expert cannot distinguish the real and fake fingerprint images. While the latter database images are composed of four different optical sensors

(Sagem, Biometrika, ItlData and Digital Person). For instance, the fake images in the LivDet 2011 dataset (Biometrika and Italdata) were created using the non-cooperative method. The fake fingerprint can be generated using four different kinds of materials: gelatin, playdoh, silicone ecoflex and wood glue. Due to some reasons, the original fingerprint images may be color images or RGB images. Therefore, we should transform all the images into gray images before experiment. In the fingerprint liveness detection experiment, every database has been divided into totally unbiased two parts: train sets which can be obtained using the train classifier and another test set, which is used to validate the performance of our method.

In this paper, the Average Classification Error (ACE) of classification error of the method is defined as ACE = (FAR+FRR)/2, in which the False Accept Rate(FAR) accounts for the proportion of the fake fingerprints being incorrectly accepted, and the False Reject Rate (FRR) that accounts for the proportion of the real fingerprints being considered as incorrectly rejected.

4.2. Support Vector Machine

SVM, a kind of machine learning algorithm, is used to solve classification and regression [30] problems. In this paper, we use the SVM as training classifier. SVM kernel function maps the raw data into a high dimensional space, and achieves the linear classification in high-dimensional space. Classification algorithms are based on classification of boundaries aims, and we can find the classification of the boundary for multidimensional data through training. The data are the point of the N dimensional space, and the classification boundary is called super surface in N dimensional space.

Libsvm of SVM is an open source library and realizes four basic kernels. The radial basis function (RBF) kernel is widely used among the four basic kernels. In our method, we will choose the RBF kernel function. Besides that, the libsvm also provides other functions, such as to seek the most suitable kernel parameter g and penalty parameter c for an RBF kernel. Through the tool “Grid-search and Cross-validation”, we can search the results of the optimal.

4.3. Results

The LivDet 2011DB derives from 2011 Fingerprint Liveness Detection Competition, where the quality of the spoof fingerprints has greatly improved, and they are distributed through the website of the competition. We have discussed the detailed information of the LivDet 2011DB in Part A. The performance of our proposed method is estimated using the Average Classification Error (ACE), which is defined as ACE = (FAR+FRR)/2. As described above, the validation process in this paper presents two successive parts (the train process and the test process). The database is divided into train set which comprising 4012 real images and corresponding 4008 spoof fingerprint images, and test set with the rest of 4000 real fingerprint and fake fingerprint images coming from the rest of 4036 fingerprint images. To avoid generating a wrong result, dataset cannot have non-overlapping parts between them.

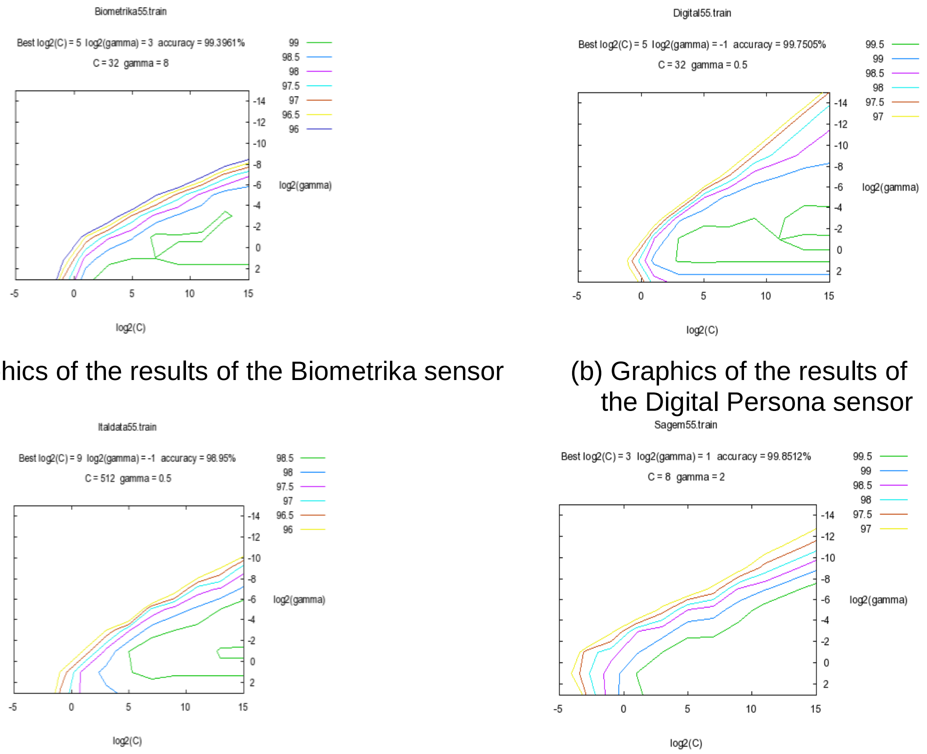
Table 2. The General Information of LivDet2009DB and LivDet2011DB

Database	Sensor	Model NO.	Resolutio n(dpi)	Image size
LivDet20 09#1	Biome trika	FX2000	569	312×372
LivDet20 09#2	Cross match	Verfier 300 LC	500	480×680

LivDet2009#3	Identix	DFR200	686	720×720
LivDet2011#1	Biometrika	FX200	500	315×372
LivDet2011#2	Digital Persona	4000B	500	355×391
LivDet2011#3	ItalData	ET10	500	640×480
LivDet2011#4	Sagem	MSO30	500	352×384

Using each GLCM can compute five different texture feature vectors, and we can obtain 20 parameter features for each GLCM when θ are four different degrees respectively. Next, use the train SVM classifier to train the obtained feature vectors. In order to get better classification accuracy, we need to carry out parameters optimization using LIBSVM. Figure 4 shows the graphics of the results of the parameter optimization. Different color lines show different test precision, and the same color lines show the same accuracy value. We use the parameter pair (C, g) to estimate the accuracies of the SVM classifier in the training process, where the parameter *C* denotes the cost, parameter g denotes parameter gamma. In Figure 4 (a), we can find that the parameters optimization can obtain the highest accuracy when the *C*=32, and g=8. Similarity, we can find the best accuracy responding the (b), (c), (d) respectively. Table 3, lists the detection accuracies of the train SVM classifier. The average error rate is shown in the last column. The process average error rate is measured on a 32-bit Operating system Windows7-PC with a 2.83 GHz processor and 4G RAM, running MATLAB R2010a. The results of fingerprint liveness detection are shown in Table 3. From the table, we can see that our approach is obviously able to correctly classify. Compared with the mentioned [23] method for the different liveness detection solutions, our approach classification error rates are also clearly lower than those reported in [23]. And the detection results of using SVM classifier are listed in Table 3. As shown in Table 3, we can compute the accuracies of the four different sensors with the help of SVM classifier. For the clarity, only the best accuracy achieved on the LivDet2011 DB for each of the individual sensor dataset is given. In order to facilitate comparison of different accuracy, the best accuracy obtained using our proposed method is highlighted in bold, and the same description is described in Table 4, which using LivDet2009 database. We can find that the average error rate of our method is obviously superior to others.

Jia X *et. al.*, [24] proposed an excellent fingerprint liveness detection method based on multi-scale block local ternary patterns and conducted the comparison experiments on LivDet2011DB. In this paper, we cite the experiment data results listed in [6] for the performance comparison on the LivDet2009DB, which can not only adapt to different biometric attacks, but also perform better than well known approaches of cited works.



(a) Graphics of the results of the Biometrika sensor

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

(c) Graphics of the results of the ItalData sensor

(d) Graphics of the results of the Sagem sensor

Figure 4. Graphics of the Results of the Parameter Optimization using Different Sensors

5. Conclusion

The research of the fingerprint liveness detection against spoof attacks, where the attackers could use a spoof fingerprint to achieve illegal access, has been widely researched for hundreds of years. Facing all kinds of attacks, we design an advanced detection method against known attacks. In this paper, a novel fingerprint liveness detection method based on the gray level co-occurrence matrix has been proposed, and the image textural feature sets can be obtained using the gray level co-occurrence matrix. Moreover, it is the first time that values of the gray level co-occurrence matrix has been used to construct the feature vector through computing different texture parameters. Our proposed method adopts a software-based approach which can distinguish the spoof fingerprint from real ones. The performance of the proposed method is evaluated on two publicly available databases: the fingerprint database used in the 2011 LivDet competition [21] and 2009 LivDet competition [6]. The experimental results present that our proposed method can discriminate between live fingerprint and fake fingerprint. Compared with other fingerprint liveness detection method, our proposed method can realize fingerprint liveness detection and achieves better classification accuracy.

In the experiment, without the effect of noise, our method can achieve better classification accuracy. On the contrary, when people introduce the noises or other factors, the accuracy of fingerprint liveness detection classification algorithm is proposed in this paper would be reduced. However, it can be solved by constructing different noise filters to remove these different noises, using idea from Jin *et. al.*, [29]. Besides, we will also select and calculate different parameter values for GLCMs to detect the vitality of fingerprint image. These will be done in our future works.

Table 3. Performance Comparison in Terms of ACE in Database of the LivDet 2011

Methods	The Average Classification Error ACE in (%)				
	LivDet2011 #1	LivDet2011 #2	LivDet2011 #3	LivDet2011 #4	Average
Our method	16.18	9.2	**6.15**	**1.6**	**8.28**
Jia’s method[24]	**10**	**7.1**	16.3	6.4	9.95
Original LBP [19]	13	10.8	24.1	11.5	14.85
Power Spectrum [25]	30.6	27.1	42.8	31.5	33
Dermalog [21]	20	36.1	21.8	13.8	22.93
Federico [21]	40	8.9	40	13.4	25.57
Curvelet GLCM [26]	22.9	18.3	30.7	28	24.98
CASIA [21]	29.70	16.10	50.60	22.10	29.63
Walvelet Energy[20]	50.2	14	46.8	22	33.25
Rideges Wavelet [14]	38.8	27.5	56.9	20.5	35.93
Curvelet energy [26]	45.2	21.9	47.9	28.5	35.88
Best Result in LivDet2011[21]	20	36.1	21.8	13.8	22.93

Table 4. Performance Comparison in Terms of ACE in Database of the LivDet 2009

Methods	The Average Classification Error ACE in (%)			
	LivDet2009#1	LivDet2009#2	LivDet2009#3	Average
Our method	23.01	**3.6**	**1.98**	**9.53**
Moon *et al.,* [8] reported in [4]	23	23.5	38.2	28.2
Marasco *et al.,* [23]	**12.6**	15.2	9.7	12.5
Abhyankar *et al.,* [27] reported in [4]	31.7	31.5	47.2	36.8
Nikam *et al.,* [28]reported in [4]	28.3	18.7	30.3	25.8
Best LivDet09 [6]	18.2	9.4	2.8	10.1

Acknowledgements

This work is supported by the NSFC (61232016, 61103141, 61070195, 61070196, 61173141, 61173142, 61173136, 61103215, 61373132, 61373133, and 61073191), National Basic Research Program 973 (2011CB311808), 2011GK2009, GYHY201206033, 201301030, 2013DFG12860, SBC201310569, Research Start-Up fund of NUIST (20110428), and PAPD fund.

References

[1] X. Jia, X. Yang, K. Cao, Z. Yali, Z. Ning, D. Ruwei, Z. Xinzhong and T. Jie, "Multi-scale local binary pattern with filters for spoof fingerprint detection", Information Sciences: an International Journal, vol. 268, no. 6, **(2014)**, pp. 91-102.

[2] D. Maltoni, D. Maio, A. K. Jain and S. Prebhakar, "Handbook of fingerprint recognition", springer,

(2009).

[3] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey", Iet Biometrics, vol. 3, no. 4, **(2014)**, pp. 219-233.

[4] 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.

[5] I. I. 19792:2009, "Information Technology—Security Techniques—Security Evaluation of Biometrics," vol. ISO/IEC Standard 19792, **(2009)**.

[6] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli and S. Schuckers, "First international fingerprint liveness detection competition—livdet 2009", Image Analysis and Processing–ICIAP 2009, Springer Berlin Heidelberg, **(2009)**, pp. 12-23.

[7] B. Tan and S. Schuckers, "New approach for liveness detection in fingerprint scanners based on valley noise analysis", Journal of Electronic Imaging, vol. 17, no. 1, **(2008)**.

[8] Y. S. Moon, J. S. Chen, K. C. Chan, K. C. So and K. C. Woo, "Wavelet based fingerprint liveness detection", Electronics Letters, vol. 41, no. 20, **(2005)**, pp. 1112-1113.

[9] M. Espinoza and C. Champod, "Using the number of pores on fingerprint images to detect spoofing attacks", Hand-Based Biometrics (ICHB), 2011 International Conference on. IEEE, **(2011)**, pp. 1-5.

[10] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak and O'G. Lawrence, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners", Pattern recognition, vol. 32, no. 2, **(2003)**, pp. 383-396.

[11] A. S. Abhyankar and S. C. Schuckers, "A wavelet-based approach to detecting liveness in fingerprint scanners", Defense and Security. International Society for Optics and Photonics, **(2004)**, pp. 278-286.

[12] S. Schuckers and A. Abhyankar, "Detecting liveness in fingerprint scanners using wavelets: Results of the test dataset Biometric Authentication", Springer Berlin Heidelberg, **(2004)**, pp. 100-110.

[13] Y. Zhang, J. Tian, X. Chen, X. Yang and P. Shi, "Fake finger detection based on thin-plate spline distortion model", Advances in Biometrics. Springer Berlin Heidelberg, **(2007)**, pp. 742-749.

[14] B. Tan and S. Schuckers, "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing", Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on. IEEE, **(2006)**.

[15] 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.

[16] G. L. Marcialis, F. Roli and A. Tidu, "Analysis of fingerprint pores for vitality detection", Pattern Recognition (ICPR), 2010 20th International Conference on. IEEE, **(2010)**, pp. 1289-1292.

[17] A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques", Image Processing, 2006 IEEE International Conference on. IEEE, **(2006)**, pp. 321-324.

[18] C. Jin, H. Kim and S. Elliott, "Liveness detection of fingerprint based on band-selective Fourier spectrum", Information Security and Cryptology-ICISC 2007. Springer Berlin Heidelberg, **(2007)**, pp. 168-179.

[19] S. B. Nikam and S. Agarwal, "Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems", Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on. IEEE, **(2008)**, pp. 675-680.

[20] H. Choi, R. Kang, K. Choi, C. Kyungtaek and K. Jaihie, "Aliveness detection of fingerprints using multiple static features", Proc. of World Academy of Science, Engineering and Technology, vol. 22, **(2007)**.

[21] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis and F. Roli, "LivDet 2011—Fingerprint liveness detection competition 2011", Biometrics (ICB), 2012 5th IAPR International Conference on. IEEE, **(2012)**, pp. 208-215.

[22] L. Ghiani, P. Denti and G. L. Marcialis, "Experimental results on fingerprint liveness detection", Articulated Motion and Deformable Objects. Springer Berlin Heidelberg, **(2012)**, pp. 210-218.

[23] J. Galbally, S. Marcel and J. Fierrez, "Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition", **(2013)**.

[24] X. Jia, X. Yang, Y. Zang, Z. Ning, D. Ruwei, T. Jie and Z. Jianmin, "Multi-scale block local ternary patterns for fingerprints vitality detection", Biometrics (ICB), 2013 International Conference on. IEEE, **(2013)**, pp. 1-6.

[25] P. Coli, G. L. Marcialis and F. Roli, "Power spectrum-based fingerprint vitality detection", Automatic Identification Advanced Technologies, 2007 IEEE Workshop on. IEEE, **(2007)**, pp. 169-173.

[26] S. Nikam and S. Agarwal, "Fingerprint liveness detection using curvelet energy and co-occurrence signatures. Computer Graphics", Imaging and Visualisation, 2008. CGIV'08. Fifth International Conference on. IEEE, **(2008)**, pp. 217-222.

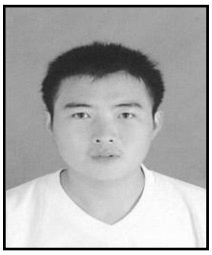
[27] A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques", Image Processing, 2006 IEEE International Conference on. IEEE, **(2006)**, pp. 321-324.

[28] S. B. Nikam and S. Agarwal, "Curvelet-based fingerprint anti-spoofing", Signal, Image and Video Processing, vol. 4, no. 1, **(2010)**, pp. 75-87.

[29] Q. Jin, I. Grama and Q. Liu, "Optimal weights mixed filter for removing mixture of Gaussian and impulse noises", arXiv preprint arXiv:1205.3999, **(2012)**.

[30] B. Gu, V. S. Sheng, K. Y. Tay, W. Romano and S.Li, "Incremental Support Vector Learning for Ordinal Regression", IEEE Transactions on Neural Networks and Learning Systems, vol. 8, no. 99, **(2014)**, pp. 1283-1291.

Authors



Chengsheng Yuan, he received his B.S. degree in Software Engineering from Nanjing University of Information Science and Technology, China in 2014. Currently he is studying for his M.S degree in Computer Science and Technology at the same university. His research interests include digital forensic, image processing and network security.

Zhihua Xia, Dr. Zhihua Xia received his BE in Hunan City University, China, in 2006, PhD in computer science and technology from Hunan University, China, in 2011. He works as an associate professor in School of Computer & Software, Nanjing University of Information Science & Technology. His research interests include cloud security, and digital forensic.

Xingming Sun, Prof. Xingming Sun received his BS in mathematics from Hunan Normal University, China, in 1984, MS in computing science from Dalian University of Science and Technology, China, in 1988, and PhD in computing science from Fudan University, China, in 2001. He is currently a professor in School of Computer & Software, Nanjing University of Information Science & Technology, China. His research interests include network and information security, digital watermarking.

Decai Sun, Dr. Decai Sun received his BE at Daqing Petroleum Institute, China, in 2002, M.S. degree at Hunan University, China, in 2009, PhD in computer science and technology from Hunan University, China, in 2012. He works as a lecturer at College of Information Science and Technology in Bohai University. His research interests include Computational Biology, Information Retrieval, and Approximate String Matching.

Rui Lv, he received his B.S. degree in Computer Science and Technology from Nanjing University of Information Science and Technology, China in 2014. Currently he is studying for his M.S degree in Computer Science and Technology at the same university. His research interests include digital watermark, image processing and network security.