Fake-fingerprint detection using multiple static features

Heeseung Choi
Raechoong Kang
Kyoungtaek Choi
Andrew Teoh Beng Jin
Jaihie Kim
Yonsei University
School of Electrical and Electronic Engineering
Biometrics Engineering Research Center (BERC)
134 Shinchon-dong, Seodaemun-gu
Seoul 120-749, Korea
E-mail: jhkim@yonsei.ac.kr

Abstract. Recently, fake fingerprints have become a serious concern for the use of fingerprint recognition systems. We introduce a novel fake-fingerprint detection method that uses multiple static features. With regard to the usability of the method for field applications, we employ static features extracted from one image to determine the aliveness of fingerprints. We consider the power spectrum, histogram, directional contrast, ridge thickness, and ridge signal of each fingerprint image as representative static features. Each feature is analyzed with respect to the physiological and statistical distinctiveness of live and fake fingerprints. These features form a feature vector set and are fused at the feature level through a support vector machine classifier. For performance evaluation and comparison, a total of 7200 live images and 9000 fake images were collected using four sensors (three optical and one capacitive). Experimental results showed that proposed method achieved approximately 1.6% equal-error rate with optical-based sensors. In the case of the capacitive sensor, there was no test error when only one image was used for a decision. Based on these results, we conclude that the proposed method is a simple yet promising fake-fingerprint inspection technique in practice.
[DOI: 10.1117/1.3114606]

Subject terms: fake-fingerprint detection; fingerprint recognition; multiple static features; SVM (support vector machine).

Paper 080905R received Nov. 19, 2008; revised manuscript received Feb. 5, 2009; accepted for publication Feb. 6, 2009; published online Apr. 3, 2009.

1 Introduction

Fingerprint recognition systems have been widely used for user authentication on account of their reliable performance and usability compared to other biometric systems. Moreover, due to the development of low-cost acquisition devices, these systems have been utilized in a wide range of forensic and commercial applications, e.g., criminal investigation, e-commerce, and access control.[1] Although the interest in fingerprint recognition systems has been increasing, some researchers have reported that the systems may be vulnerable to certain threats. Ratha et al.[2,3] analyzed eight possible kinds of attacks on fingerprint systems and proposed some general guidelines to protect them from these attacks. Although all these attacks are serious from a security viewpoint, the use of fake fingers is the most critical according to several researchers.[4–10]

1.1 *Related Works and Motivation*

Putte and Keuning[4] introduced two duplication methods one with and one without the user's cooperation, for making fake fingers. They used fake silicone fingers to attack six conventional fingerprint sensors. Experimental results showed that all these sensors were deceived on the first or second attempt. Furthermore, Matsumoto et al.[5] introduced fake gelatin fingers (called gummy fingers) and used them to attack eleven different fingerprint recognition systems. It was found that the fake fingers were enrolled in all systems. The acceptance rates ranged from 67% to 100%.

Existing methods for detecting fake fingerprints use additional hardware to acquire signs of aliveness. These methods include the use of temperature,[4] pulse oximetry,[11] blood flow,[12] electrical characteristics,[13] spectral characteristics,[14] odor,[15] and heartbeat.[16] All of these methods use explicit characteristics of live fingers, which are not present in fake fingers. However, the implemented systems are bulky and costly due to the additional hardware. Apart from that, the process of acquiring life signals usually takes several seconds or minutes; this might cause inconvenience to the users.

This situation invites research on software-based approaches, since they do not require additional hardware, and they work with the images captured by existing sensors. Accordingly, many existing fingerprint systems can easily adopt these software-based approaches by simply modifying their embedded software.

The software-based approaches can be roughly grouped into dynamic and static, according to the kinds of features used. Dynamic approaches exploit features extracted from a sequence of fingerprint images, such as skin perspiration[17–24] and skin distortion.[25–28] Skin-perspiration-based approaches have been the most widely researched for fake-fingerprint detection. Such an approach utilizes the inherent perspiration of fingers. As perspiration persists, the sweat diffuses along the ridges and the image becomes

0091-3286/2009/$25.00 © 2009 SPIE

darker. Hence, several images are captured over a period of a few seconds and compared to search for the signs of that effect.

Another approach uses skin distortion analysis. Due to the different elasticities of live and fake fingers, they show different elastic tension when pressed on a sensor surface. The resulting skin distortion features can be obtained by having the user rotate a finger on the sensor surface.

Experimental results are promising under controlled environments for the two preceding approaches. However, these approaches have limitations in that they require users' cooperation. For example, users have to keep their fingers on the sensor for a few seconds (for perspiration analysis) or rotate their fingers on the sensor surface (for distortion analysis). Furthermore, the degree of perspiration may be greatly dependent on both skin and environmental conditions, such as temperature and air humidity. Skin distortion patterns can also be affected by the characteristics of the user's movements. For precise finger movement recording, the system needs special sensors[25] to guarantee a high frame rate. These requirements may be cumbersome for users and may not be suitable in practice.

Some researchers have suggested static approaches to overcome these drawbacks. These approaches used features that were extracted from a single image. The features include pores,[17,29] the power spectrum,[30] surface coarseness,[31] morphological characteristics,[32] and statistical properties.[33] The reasons for using these features are as follows. Firstly, the materials used for making fake fingers are typically composed of large organic molecules; thus making high-quality fake fingers is not an easy task.[25] For example, small features such as pores are usually not perfectly imitated, and the surface of fake fingers is coarser than that of live fingers. Secondly, the fake-fingerprint images appear different to live fingerprint images in various features because of the casting and molding processes.[30,33] Even though the static approach is useful in practice, it falls short of the dynamic approach in that it has to make a decision based only a single image. This deteriorates the classification performance.

1.2 *Contributions*

Based on the preceding considerations, we introduce a novel fake-finger detection method using multiple static features from a single image and satisfying requirements of users' convenience, time, and performance. Specifically, we study and utilize various features, including the power spectrum, directional contrast, ridge thickness, ridge signal, and first-order histogram, of the fingerprint images. These features encode the differences between live and fake fingerprints in terms of physiology and statistics. The feature vector sets formed by multiple static features are combined at the feature level through a support vector machine (SVM) classifier.

Two other significant contributions made by this paper are:

1. A total of 7200 live images and 9000 fake images were collected using four sensors on the market (three 500-dot/in. optical and one 508-dot/in. capacitive dc type, hereafter called optical_1, optical_2, optical_3, and capacitive.), taking various variabilities of live and fake fingerprints into account. The data set contains a large number of data compared to the data sets used in other researches. The detailed description of the database is presented in Sec. 3.1.
2. The proposed method can be used with various sensors easily, since only simple feature extraction and one session of offline training are involved.

The rest of this paper is organized as follows: in Sec. 2, feature analysis and feature vector extraction are explained. In Sec. 3, we describe the data acquisition process and present experimental protocols and results. Finally, conclusions are drawn in Sec. 4.

2 Extraction of Static Feature Vectors

To the best of our knowledge, there is no single static feature that is absolutely superior to all others in fake-detection performance. This is because sensor characteristics vary and the characteristics of both live and fake fingerprint images depend on user skin conditions, operating environments, fabrication materials, etc. Static features also contain less useful information than features extracted from dynamic approaches, because they are extracted from only a single image. In order to obtain better performance, it is desirable to select useful static features and combine them by means of an effective method. In this section, we analyze and select several representative static features, using image analysis. We then convert these features to vectors for classification.

2.1 *Image-Based Feature Analysis*

We observed some visual differences between the live and fake images, as shown in Fig. 1. As is seen, some micro-details differ in the fake images. These differences were mainly attributed to the stamping process and the characteristics of the materials used to create the fake images. The following categories explain the detectable microchanges that sometimes appeared in the fake images.

- Broken ridges and blowholes: As shown in Fig. 1(a), fake fingerprints may have more broken ridges and blowholes because of deficiencies in casting at the surface of fake fingers.
- Noise components in valleys: As shown in Fig. 1(b), fake fingerprints may show random noise components in valleys, since incomplete stamping can arise in valleys when making molds.
- Nonclarity of ridge-valley structures: Even though fake images have similar geometrical structures to live images, ridge and valley shapes are not perfectly reproducible in all duplications and sometimes crumble as shown in Fig. 1(c).
- Thick ridges: To create fake fingers, users must imprint their fingers on molding materials, or latent fingerprints on sensing surface must be captured. Hence ridge widths can be altered depending on the amount of pressure the user exerts. Besides that, due to the stamping process, the ridge-to-valley depth of fake fingers can be lower than that of live fingers. Consequently, most fake images have thicker ridges than live images, as shown in Fig. 1(d).

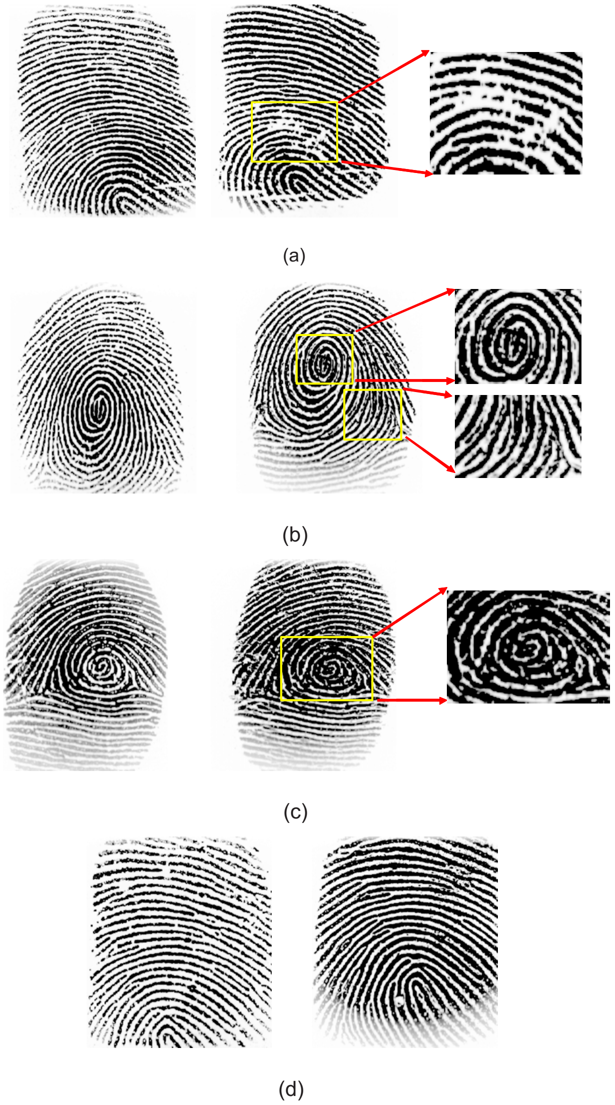


Fig. 1 Visual differences between live (left) and fake (right) images. (a) Broken ridges and blowholes. (b) Noise components in valleys. (c) Nonclarity of ridge and valley structure. (d) Thick ridges.

2.1.1 *Extraction of the global image-based feature vector*

In this sub-subsection, we explain the detection of live and fake images by using power spectrum analysis. Power spectrum analysis has been widely used in fingerprint image enhancement, quality checking, and matching.[34] Generally, a fingerprint image is composed of ridges and valleys of specific frequencies. For instance, the ridge-to-ridge distance in 500-dot/in. fingerprint images ranges from 7 to 10 pixels. Hence, its corresponding frequency bands contain more energy than other frequency bands and generate ring patterns in the specific spectrum area.[34] In our observation, the power spectra of live and fake images exhibit similar ring patterns, since their overall geometric structures are alike, as shown in Fig. 2.

However, the power spectra of live and fake images have distinct energy distributions due to microchanges that show in the fake fingerprint images. The differences can be analyzed and a power spectrum feature vector can be elicited through the following procedure:

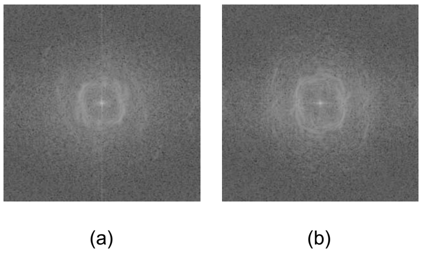


Fig. 2 The power spectra of (a) live and (b) fake fingerprint images.

1. An image is first transformed using the discrete Fourier transform (DFT)

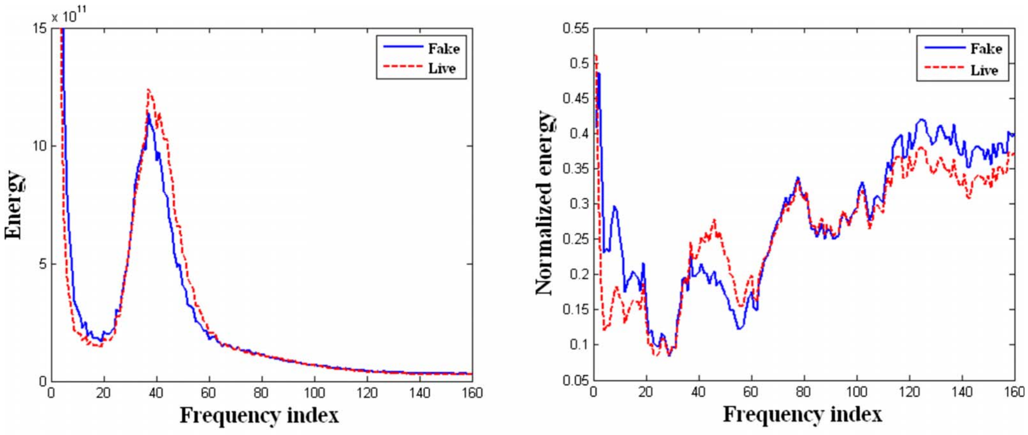
$$F(u,v)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\exp\left[-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right], \tag{1}$$

   where $f(x,y)$ represents an image of size $M\times N$ in the spatial domain.
2. A transformed image is tessellated according to concentric rings to alleviate the rotation problem. Each ring's radius differs from that of its neighbors by one frequency unit. This means that two adjacent rings are one pixel apart in the frequency domain.
3. We compute the energy values of pairs of adjacent rings. The numbers of rings were different among the sensors, since the sizes of the images vary. If two adjacent rings are denoted as $R(i-1)$ and $R(i)$, the sum of all energy values of pairs of adjacent rings, $V(i)$, is obtained from the following equation:

$$V(i)=\sum_{(u,v)\in P_i}|F(u,v)|^2, \tag{2}$$

   where P_i represents the set of all (u,v) pairs between $R(i-1)$ and $R(i)$.
4. For all adjacent rings, we repeat step 3.
5. Finally, the sums of all energy values for the frequency indices are computed and grouped to form a feature vector.

Figure 3 shows a comparison of the energy distributions that were calculated according to this procedure. We notice that live fingerprint images had higher energy concentrations in ridge-and-valley frequencies. Fake images had more diffused energy distribution because of microdetail changes such as broken ridges and valley noise described earlier. Also, the random noise components were distributed so that the high-frequency components of the fake images had more energy than those of the live images. Based on these differences, we used the energy values calculated by the procedure described to obtain the feature vector. Hereafter we denote by SFV_1 the power spectrum feature vector (static feature vector 1).



(a) (b)

Fig. 3 A comparison of the energy concentration of live and fake fingerprint images. (a) Energy concentration of live and fake images. (b) Normalized energy concentration.

As mentioned in Refs. 21 and 33, live and fake fingerprints are visually different. For example, fake fingerprint images look darker and have less contrast than their corresponding live fingerprints. Therefore, to analyze the visual differences between live and fake images, we used the seven first-order histogram features that were suggested in Ref. 33 (energy, entropy, median, variance, skewness, kurtosis, coefficient of variation) as another set of representative features. These seven features formed a feature vector called SFV_2.

2.1.2 *Extraction of the local image-based feature vector*

As shown in Fig. 1, ridges and valleys in fake images are less conspicuous than those in live images. Moreover, valleys in fake images often contain noise components. In practice, when creating fake fingers, ridge widths are easily increased and also ridge-to-valley depths are decreased with respect to the corresponding live fingers. Therefore we identify two additional representative static features for fake fingerprint detection: directional contrast and ridge thickness (SFV_3). Directional contrast was used to measure the distinctness and clarity between the ridges and the valleys. This is because the blocks near to ridges and valleys in live images are well separated and display high directional contrast. The following procedure was devised to measure the level of directional contrast:

1. A fingerprint image is partitioned into 8×8 blocks.
2. A 3×3 four-directional mask is created as shown in Fig. 4 to extract each directional value. The function $S_j(x,y)$ $(j=1,2,3,4)$ at the (x,y) position as described

$$S_j(x,y)=\sum_{k=1}^{2} I(P_{jk}), \qquad j=1,2,3,4, \tag{3}$$

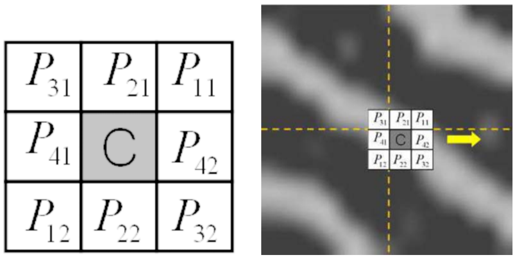
   where $I(P_{jk})$ denotes the intensity value of the pixel that corresponds to the position P_{jk} in the filter.
3. For each block, the local directional gray value D_j is calculated as

$$D_j=\sum_{x=1}^{8}\sum_{y=1}^{8} S_j(x,y). \tag{4}$$

4. We average each four-directional contrast value over all the blocks, and the four resulting values are then used as directional contrast features.

In general, the ridge thickness measures the width of the ridges. The ridge thickness was computed in each 16×16 block.[35] Figure 5 shows the gray-level plot of a fingerprint image. The ridge thickness is calculated using the gray-level values of each block in a direction normal to the ridge orientation. Ridge orientation is calculated using the method suggested in Ref. 36. The threshold value that separates the ridges and valleys is determined by averaging the local maximal and local minimal gray-level values in each block.[35] Then, the average ridge thickness value is computed using all blocks. Table 1 shows the average values of the ridge thickness of the live and fake fingerprints using our data set. In Table 1, it is clear that the ridges of the fake images were thicker than those of the live images.

Finally, we consider the average four-directional contrast values and the ridge thickness values to be representative static features. These features also formed a feature vector (denoted as SFV_3 hereafter).



(a) (b)

Fig. 4 Measuring directional contrast. (a) Mask for eight-directional filter. (b) Windowing operation for measuring directional contrast.

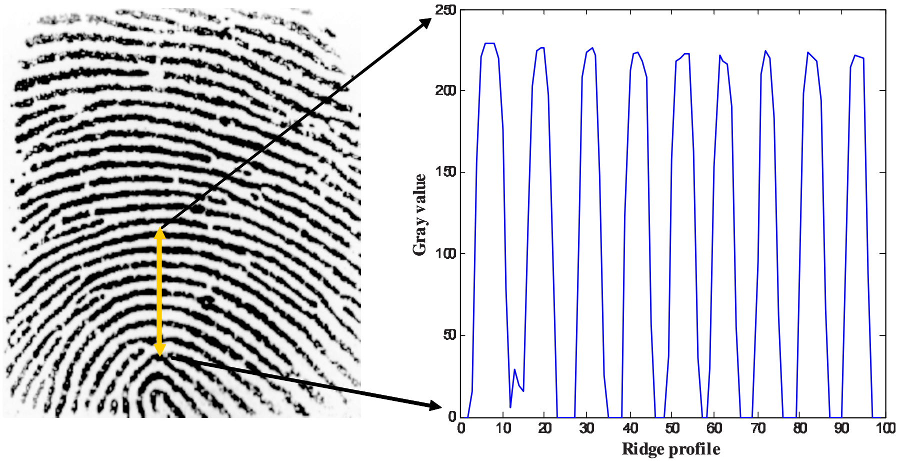


Fig. 5 The gray-level plot of a fingerprint image.

2.2 *Ridge-Based Feature Analysis*

Pores are usually considered to be one of the most useful static features for fake-fingerprint detection,[17,29] since typical materials used for making fake fingers are composed of large organic molecules. Therefore, miniature features such as pores are not reproduced exactly. Derakhshani et al.[17] analyzed the periodicity of sweat pores along ridges. Their algorithm was used to transform a two-dimensional fingerprint image into one-dimensional signals denoting the gray-level values along ridges (called the ridge signals). The fast Fourier transform (FFT) was used to analyze the gray-value variability due to the occurrence of pores. The total ridge signal energy was then calculated using 11 to 33 FFT points, which took account of pore periodicity.[17] Then, these energy values were used as static features, in that the energy extracted from live fingerprints is higher than that from fake fingerprints. However, in our observation, we found that pores could be detected in fake fingerprints even though the pores of live fingerprint images are invisible, as shown in Fig. 6. This is because pore presence in live images can be greatly affected by environmental conditions (such as temperature and humidity) and user's skin conditions (dry or wet).

Besides that, pore spacing may not be useful depending on the sensor's characteristics. Fig. 7 shows the energy distributions of live and fake images using this method.[17] As shown in this figure, discrimination may be difficult when using only 11 to 33 points for pore the spacing. The following procedure was then applied to rectify this problem:

1. A binary image is produced and skeletonized using the Gabor filter.[36]
2. A 1-D gray-value signal is acquired along each thinned ridge.[17]
3. 256 FFT values from each ridge signal are computed and averaged.
4. An average power ridge signal is formed using the FFT coefficients from 1 to 127 points.

To analyze the usefulness of ridge signals, Fisher's linear discriminant was used. Fisher's linear discriminant is well known as a measure of separability among classes and is expressed as follows[37]:

$$\text{Fisher ' s linear discriminant} = \frac{|\mu_{\text{Live}} - \mu_{\text{Fake}}|^2}{\sigma^2_{\text{Live}} + \sigma^2_{\text{Fake}}} \qquad (5)$$

where μ_{Live} and σ_{Live} (μ_{Fake} and σ_{Fake}) represent the mean and variance of the live (fake) class. Fisher's linear discriminant analysis is performed for all frequency components of the average power ridge signal in each data set. Figure 8 shows the Fisher discriminant values of all the frequency components in each data set.

We notice that the dominant frequency region depends on the sensor characteristics. The dominant frequency bands in the ridge signal show higher discrimination power than that in the frequency bands (11 to 33 points for 256 FFT values) corresponding to the pore spacing. Furthermore, their relative discrimination values are distinctively different. Thus, we consider all the 127 frequency components of the average power ridge signal, denoted as SFV_4.

Table 1 Comparison of average ridge thickness.

	Ridge thickness (pixels)			
Image	Optical_1 sensor	Optical_2 sensor	Optical_3 sensor	Capacitive sensor
Live	6.44	8.33	7.98	3.95
Fake	9.55	12.88	11.00	4.22

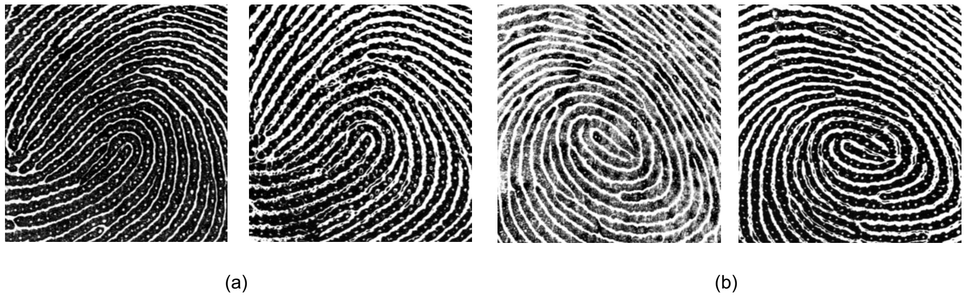


Fig. 6 Two sets, (a) and (b), of live and fake fingerprint images captured with a 1000-dot/in. high-resolution optical sensor (CrossMatch Co. Ltd). Left: live image; right: corresponding fake image.

3 Experiments

3.1 *Data Acquisition*

As mentioned in Sec. 1, producing good-quality fake fingers is not an easy task, and most fake-fingerprint databases are made for in-house testing. This means that there is no public database for benchmarking. Moreover, to generalize the method by analyzing the selected features and evaluate their performance, various kinds of live and fake images should be considered. In this work, we collected a larger number of live and fake fingerprint images than in previous works.[18–31] Four fingerprint sensors on the market were considered: three 500-dot/in. optical sensors (the IZZIX FD 1000 from Digent Co. Ltd.,[38] the HFDU04 from Nitgen Co. Ltd.,[39] and the VIRDI FPR02 from Unioncomm Co. Ltd.[40]) and one 508-dot/in. capacitive dc sensor (the SFM3050-TC1 from Suprema Co. Ltd.[41]). We named these sensors optical_1, optical_2, optical_3, and capacitive, respectively. With each sensor, we collected fingerprint images from live and fake fingers. By considering various characteristics of live fingerprints, 60 volunteers were gathered: 30 males and 30 females. Their ages are ranged from 6 to 60 years. For each volunteer, thumbs and index fingers were used to capture 15 impressions at various pressure levels (low, medium, and high). Exact pressure values were recorded using our special pressure gauge (CAS CI-1500A[42]) during the capturing process. When making fake fingerprints, we only used the silicone and gelatin, because these two types of materials are generally regarded as the most critical and able to produce higher-quality fake fingerprint images than other materials such as paper, film,

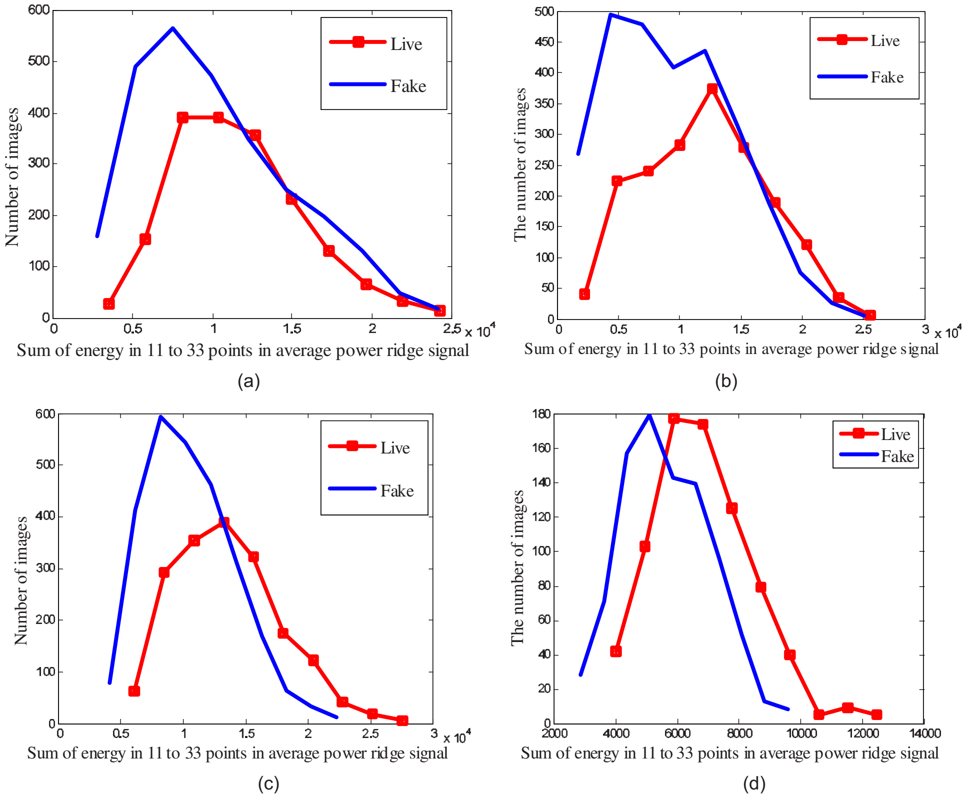
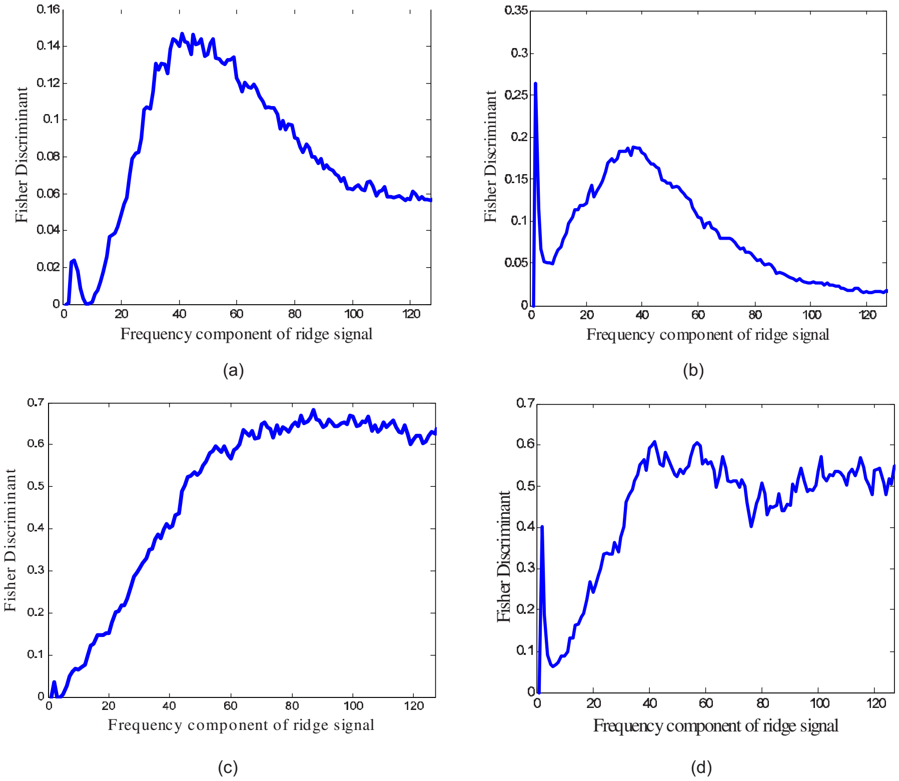


Fig. 7 The energy distribution of each data set: obtained from (a) the optical_1 sensor, (b) the optical_2 sensor, (c) the optical_3 sensor, (d) the capacitive sensor.



(a)

(b)

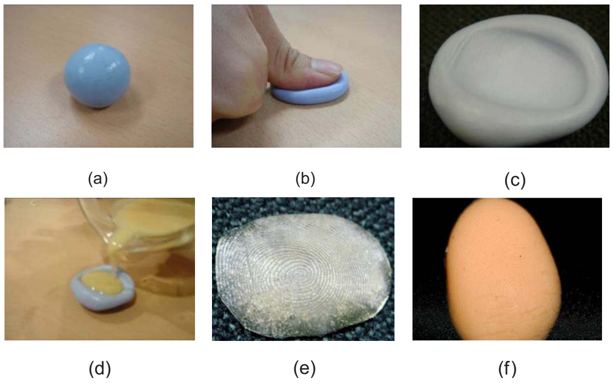
(c)

(d)

Fig. 8 The Fisher discriminant values with average power ridge signals in each data set: obtained from (a) the optical_1 sensor, (b) the optical_2 sensor, (c) the optical_3 sensor, (d) the capacitive sensor.

and rubber. To generalize the fake-fingerprints creation procedures, 60 volunteers cooperated with five instructors and followed the same basic steps to make their fake fingerprints. Figure 9 shows the steps in our fake-finger generation process.

By this process, 120 silicone and 60 gelatin fake fingers were collected. Since the color of a finger affects the image characteristics of optical sensors, we added an incarnadine pigment similar to finger skin color to the fake fingers. For each fake finger, 15 fake images were also captured at various pressure levels. Specifically, to obtain high-quality gelatin fake images, the time elapsed between the creation of the gelatin and its use is a critical factor, in particular with respect to the deformation. Hence we collected gelatin fake images from each individual within 30 min after creation. Our capacitive sensor did not respond to the fake silicone finger, because it produced too small an electrical charge. Eventually, 7200 live fingerprint images and 9000 fake fingerprint images (5400 silicone images, 3600 gelatin images) were acquired. Figure 10 shows some examples of live and fake fingerprint images.


(a)

(b)

(c)

(d)

(e)

(f)

Fig. 9 Steps of making a fake finger: (a) A mold is made of a dental impression material. (b) A finger is pressed on the mold. (c) A negative pattern of the fingerprint is formed on the mold. (d) Liquid silicone or gelatin is put over the mold. (e) A gelatin fake finger. (f) A silicone fake finger.

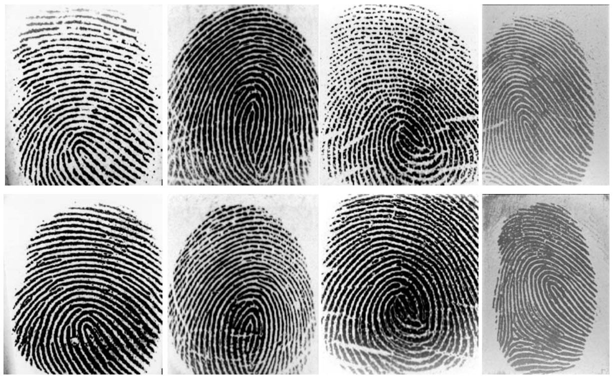


Fig. 10 Some examples of live and fake fingerprint images obtained from the four sensors: live fingerprint images (top row) and their corresponding fake fingerprint images (bottom row).

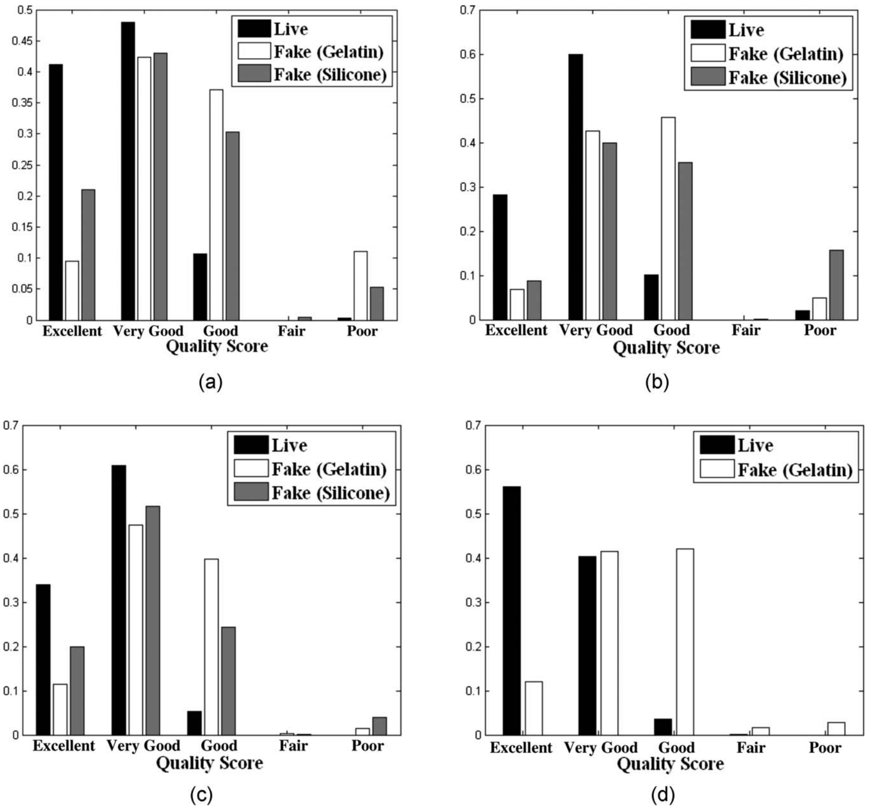


Fig. 11 The results of the NIST quality check on our database: obtained from (a) the optical_1 sensor, (b) the optical_2 sensor, (c) the optical_3 sensor, (d) the capacitive sensor.

There are some important things to notice in collecting fake images. For example, the fake fingers must be able to interact with fingerprint recognition systems. If a fake finger is of too low quality, it may be considered as a nonmatched finger and simply rejected. It is relatively easy not to accept fake fingers when using low quality fake fingerprints. In our experiments, to ensure the image quality was sufficiently high, we applied a fingerprint quality checking algorithm developed by the National Institute of Standards and Technology (NIST).[43] The quality measure is defined as the degree of separation between the matching and nonmatching distributions of a given fingerprint, which is predicted using neural networks.[43] Each fingerprint image was assigned to one of five quality levels (excellent, very good, good, fair, bad) according to the quality measure. Figure 11 shows the NIST quality-checking results for our database. It is observed that most of the fake fingerprint images were of good quality.

3.2 *Experimental Protocol*

Figure 12 shows the overall procedure of the proposed method. The representative static feature vectors included the power spectrum (SFV_1), seven histogram features (SFV_2), directional contrast and ridge thickness values (SFV_3), and ridge signals (SFV_4). After the feature extraction stage, each feature vector was normalized as follows:

Table 2 The dimensions of the feature vectors in each data set.

	Optical_1 sensor	Optical_2 sensor	Optical_3 sensor	Capacitive sensor
Image size:	320×280	292×248	292×265	360×256
SFV_1	160	146	146	180
SFV_2	7	7	7	7
SFV_3	5	5	5	5
SFV_4	127	127	127	127
Total	299	285	285	319

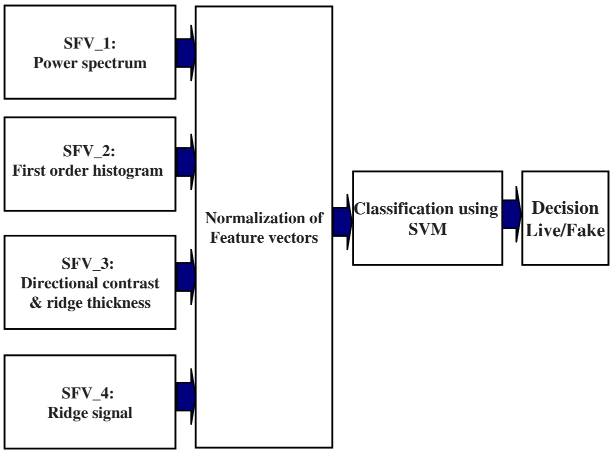


Fig. 12 Overall procedure of the proposed method.

$$f_{n\_i} = \frac{f_i - m_i}{\sigma_i}, \tag{6}$$

where f_{n_i} represents the i'th normalized feature, and m_i and σ_i represent the mean and standard deviations of f_i over all samples. Table 2 shows the dimensions of the feature vectors in each data set.

Based on the feature vectors described in Table 2, we discriminated the input fingerprint images as live or fake using a support vector machine (SVM). The SVM performed classification by determining the optimal linear decision hyperplane at the maximum distance to the closest points of the training vectors, called support vectors.[37] Generally, the SVM is given by[39]

$$f(x) = \mathrm{sgn}\left(\sum_{i=1}^{k} \alpha_i y_i K(x, x_i) + b \right), \tag{7}$$

where k represents the number of data points, and $y_i \in \{-1, 1\}$ represents the class label of the training point x_i. In the experiments, the coefficients α_i were found by solving a quadratic programming problem with linear constraints and b as the bias. Also, the SVM was extended to a nonlinear decision surface by using several kernel functions. We used both polynomial and radial basis function (RBF) kernels as follows:

$$\text{Polynomial kernel:} \qquad K(x,y) = (Gxy + 1)^d, \tag{8}$$

Table 3 Parameter ranges used in the experiments.

	Parameter range		
Kernel	Degree *d*	Gamma *G*	Cost of constraint violation
Polynomial	1 to 6	0.01 to 1	1 to 100
RBF	N/A	0.01 to 1	100 to 10,000

Table 4 Performance comparison of each feature set using the optical_1 database.

	EER (%)	
Static features	Polynomial kernel	RBF kernel
SFV_1 (power spectrum feature vectors)	5.8	1.78
SFV_2 (first-order histogram feature vectors)	9.81	10.63
SFV_3 (directional contrast and ridge thickness feature vectors)	12.23	11.6
SFV_4 (ridge signal feature vectors)	22.95	20.9
Fused feature vectors	3.5	1.08

Table 5 Performance comparison of each feature set using the optical_2 database.

	EER (%)	
Static features	Polynomial kernel	RBF kernel
SFV_1 (power spectrum feature vectors)	4.9	1.78
SFV_2 (first-order histogram feature vectors)	19.34	18.26
SFV_3 (directional contrast and ridge thickness feature vectors)	13.62	13.88
SFV_4 (ridge signal feature vectors)	19.41	18.45
Fused feature vectors	3.12	1.6

Table 6 Performance comparison of each feature set using the optical_3 database.

	EER (%)	
Static features	Polynomial kernel	RBF kernel
SFV_1 (power spectrum feature vectors)	4.03	1.63
SFV_2 (first-order histogram feature vectors)	17.01	16.38
SFV_3 (directional contrast and ridge thickness feature vectors)	12.99	13.43
SFV_4 (ridge signal feature vectors)	20.15	18.62
Fused feature vectors	3.13	1.16

Table 7 Performance comparison of each feature set using the capacitive database.

	EER (%)	
Static features	Polynomial kernel	RBF kernel
SFV_1 (power spectrum feature vectors)	0.5	0.98
SFV_2 (first-order histogram feature vectors)	13.86	13.64
SFV_3 (directional contrast and ridge thickness feature vectors)	12.66	14.84
SFV_4 (ridge signal feature vectors)	20.68	22.86
Fused feature vectors	0.49	0

$$\text{RBF kernel:}\qquad K(x,y)=\exp(-G\|x-y\|^2). \tag{9}$$

To find the optimal parameters of the polynomial and RBF kernel, we first divided the data sets into training, validation, and test sets with an equal number of images. Using the training and validation sets, we adjusted the optimal parameters of the kernels. The ranges of the parameters are shown in Table 3. In each experiment, we found the optimal parameters and applied them to the test set.

3.3 *Experimental Results*

The performance of the proposed method was evaluated using the false-acceptance rate (FAR) and the false-rejection rate (FRR). The FAR is the probability of accepting a fake fingerprint as a live one, and the FRR is the probability of rejecting a live fingerprint as a fake one. The equal error rate (EER) is the value when the FAR and the FRR are equal.

3.3.1 *Performance evaluation of each feature set and fused feature set*

Next, we evaluated the performance of each feature set and fused feature set. Tables 4–7 show the comparative EER performance using each feature set in each database. Experimental results evidenced that all representative feature sets discriminate well between live and fake fingers. It is noted that the performance of the power spectrum feature set was favorable across all databases. This suggests that this feature set is generic in a sense and can be applied to optical and capacitive sensors for fake-fingerprint detection. We also observed that the performance of other feature sets, except SFV_1, differed because the image characteristics were all different. We repeat that useful feature sets are diverse with respect to individual sensor characteristics, and this research is useful for determining the dominant feature sets of each database and sensor.

Table 8 EER ranges obtained with a polynomial kernel.

	EER (%)		
		Using bootstrap method	
Sensor	Using all test data	Maximum	Minimum
Optical_1	3.5	5.21	1.51
Optical_2	3.12	5.21	1.51
Optical_3	3.13	5.22	0.88
Capacitive	0.49	0.74	0

Table 9 EER ranges obtained with an RBF kernel.

	EER (%)		
		Using bootstrap method	
Sensor	Using all test data	Maximum	Minimum
Optical_1	1.08	2.38	0
Optical_2	1.6	3.25	0
Optical_3	1.63	2.39	0
Capacitive	0	0	0

When these feature sets are fused, performance is improved, as shown in Tables 4–7. Specifically, we achieved an EER of approximately 1.6% in the optical-based sensors and an EER of 0% in the capacitive sensor (when we used the RBF kernel). However, this does not necessarily mean that the proposed method is more advantageous when using the capacitive sensor than when using an optical sensor. The database of the capacitive sensor was only composed of gelatin fake fingerprint images, and so direct comparison is impossible. Nonetheless we can conclude that our approach is useful in both optical and capacitive-based sensors according to the results.

3.3.2 *Confidence interval test results*

As mentioned in Sec. 3.3.1, the proposed method produced some promising results for detecting fake fingerprints. However, it is difficult to evaluate its performance, due to diverse databases and the evaluation method. It is also not easy to collect a test set that is sufficiently representative to cover all types of live and fake fingerprints from various environments. Therefore, it would be desirable if lower and upper bounds of the performance rate could be estimated. We adopted the bootstrap method,[44] which is a popular nonparametric statistical method to measure performance variations from a limited data set. For estimating the lower and upper bounds of the error rates, the following procedure was executed:

1. Using the test data set, which included 2400 live images and 3000 fake images from four sensors, the bootstrap sampling size was determined by the following equation[45]:

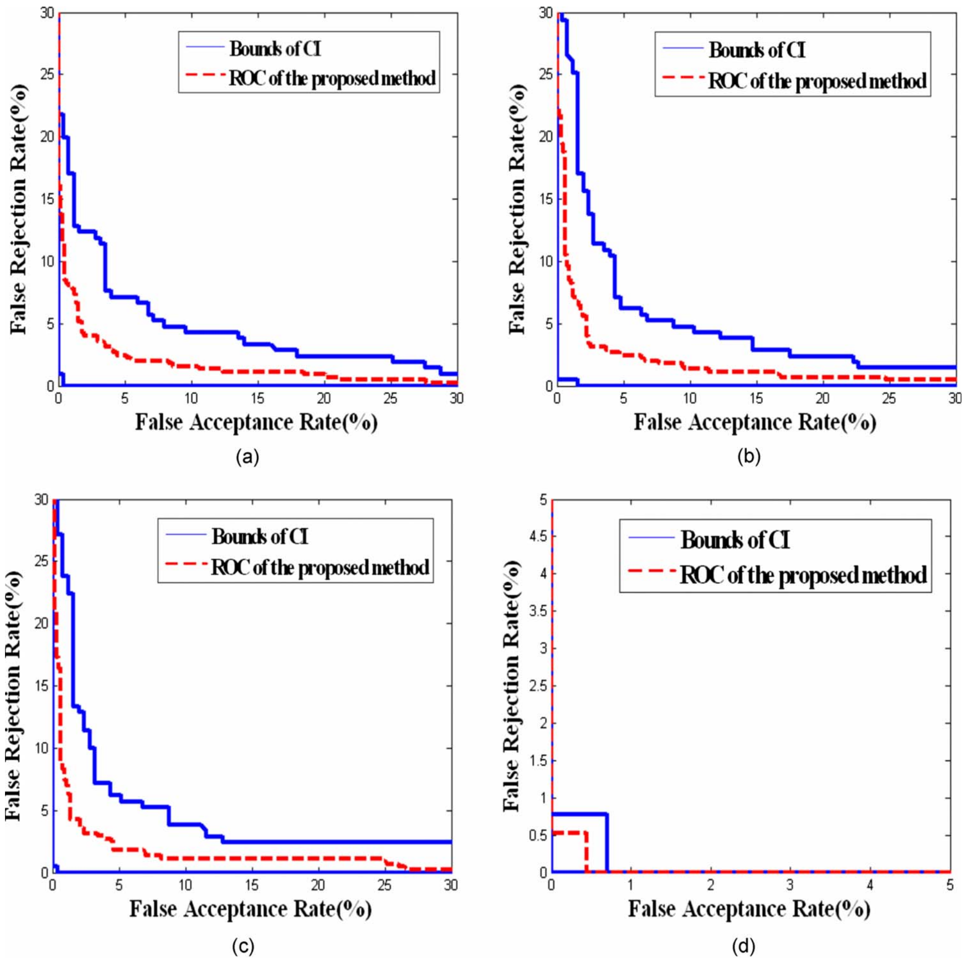


Fig. 13 Performance evaluation (polynomial kernel case) using the bootstrap method with 95% confidence intervals: database obtained from (a) the optical_1 sensor, (b) the optical_2 sensor, (c) the optical_3 sensor, (d) the capacitive sensor.

$$n = \frac{N}{1 + N(e)^2}, \tag{10}$$

where n is the determined sample size, N is the population size, and e is the level of precision. To satisfy the 95% confidence level, we set e at 0.05.

2. The FAR, FRR, and EER of the proposed method were computed using the randomly selected test set. The optimal parameters for the SVM were precalculated in the experiments as described in Sec. 3.2.
3. We repeated step 2 3000 times and then estimated the 95% confidence intervals of the FAR, FRR, and EER.

Figures 13 and 14 show the receiver operating characteristic (ROC) curves obtained from the bootstrap method by using the polynomial and the RBF kernel. The solid lines denote the confidence interval (CI) boundaries obtained by the bootstrap method, and the dashed lines are the ROC curves based on all the test images. As shown in these figures, the performance varied according to the data set used. However, the calculated confidence intervals were small, which suggests the robustness of the proposed method. (It is meaningless to find the confidence interval when we applied the RBF kernel to the capacitive sensor, since the EER is 0.) The EER ranges are also shown in Tables 8 and 9.

4 Conclusions

This paper describes a novel way of detecting fake fingers by using multiple static features. With usability in field applications in mind, static features from a single image rather than dynamic features were considered for discrimination between live and fake fingerprints. To improve the classification performance, we studied and extracted multiple static features and fused them at the feature level, using a SVM. Our representative features consist of a power spectrum, a histogram, the directional contrast, the ridge thickness, and fingerprint ridge signals, which can be easily obtained from fingerprint images. The experimental results were promising: The proposed method produced an EER of approximately 1.6% when using the optical sensors and 0% when using the capacitive sensor.

In addition, a total of 7200 live images and 9000 fake images were collected using four sensors (three optical and one capacitive) under various conditions.

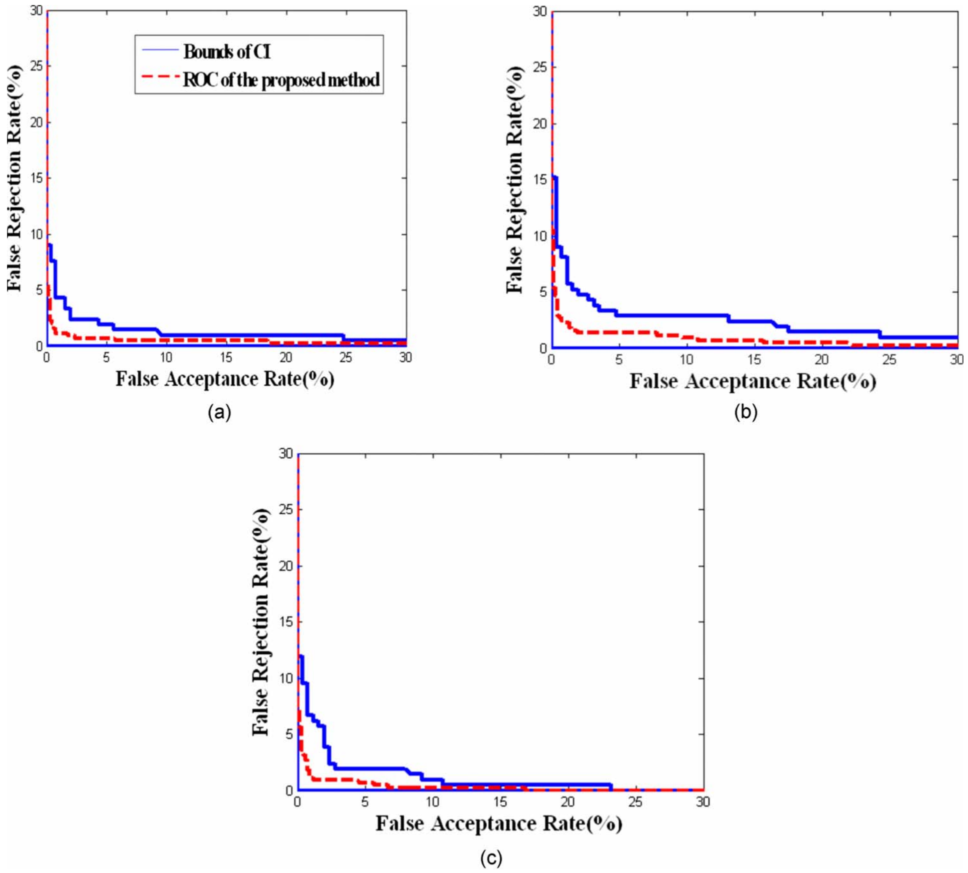


Fig. 14 Performance evaluation (RBF kernel case) using the bootstrap method with 95% confidence intervals: database obtained from (a) the optical_1 sensor, (b) the optical_2 sensor, (c) the optical_3 sensor.

The proposed method also can be easily integrated into various sensors, since it only uses simple feature extraction and offline training.

The proposed method has been proven effective, but several improvements can be pursued in future research. For example, larger databases collected in different environments (with varying temperatures and levels of humidity) can be used to analyze the usefulness of these features in various conditions. Feature enhancement methods will be further researched. Various types of sensors can also be used to analyze the correlation of the features. Furthermore, finding the optimal feature set and classification method is necessary to improve the classification performance.

Acknowledgment

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Biometrics Engineering Research Center (BERC) at Yonsei University, R112002105070010(2008).

References

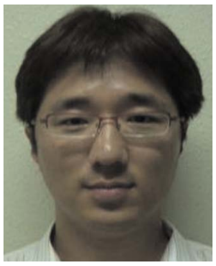
1. D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York (2003).
2. N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Third Int. Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pp. 223–228 (2001).
3. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.* **40**(3), 614–634 (2001).
4. T. Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Proc. 4th Working Conf. on Smart Card Research and Advanced Applications*, pp. 289–303 (2000).
5. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Optical Security and Counterfeit Deterrence Techniques IV*, *Proc. SPIE* **4677**, 275–289 (2002).
6. M. Sandstrom, "Liveness detection in fingerprint recognition systems," Master's Thesis, Linkoping Univ., Linkoping, Sweden (2004).
7. H. Kang, B. Lee, H. Kim, D. Shin, and J. Kim, "A study on performance evaluation of the liveness detection for various fingerprint sensor modules," in *Proc. KES*, pp. 1245–1253 (2003).
8. L. Thalheim and J. Krissler, "Body check: biometric access protection devices and their programs put to the test," *C't Mag.* (Nov. 2002).
9. D. Willis and M. Lee, "Biometrics under our thumb," *Net. Comput.* (June 1, 1998).
10. S. A. C. Schuckers, "Spoofing and anti-spoofing measures," *Inf. Security Tech. Rep.* **7**(4), 56–62 (2002).
11. D. Osten, H. M. Carim, M. R. Arneson, and B. L. Blan, "Biometric, personal authentication system," U.S. Patent No. 5,719,950 (1998).
12. P. D. Lapsley, J. A. Less, D. F. Pare, Jr., and N. Hoffman, "Anti-fraud biometric sensor that accurately detects blood flow," U.S. Patent No. 5,737,439 (1998).
13. D. R. Setlak, "Fingerprint sensor having spoof reduction features and related methods," U.S. Patent No. 5,953,441 (1999).
14. K. A. Nixon, R. K. Rowe, J. Allen, S. Corcoran, L. Fang et al., "Novel spectroscopy-based technology for biometric and liveness verification," *Proc. SPIE* **5404**, 287–295 (2004).
15. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *Proc. Int. Conf. on Biometric Authentication (ICBA)* (2006).
16. L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: a new approach in human identification," *IEEE Trans. Instrum. Meas.* **50**(3), 808–812 (2001).
17. R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, and L. O. Gor-

man, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recogn.* **36**, 383–396 (2003).

18. S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," *IEEE Trans. Syst. Man Cybern., Part C Appl. Rev.* **35**(3), 335–343 (2005).
19. A. Abhyankar and S. Schuckers, "Wavelet-based approach to detecting liveness in fingerprint scanners," in *Proc. SPIE Defense and Security Symp., Biometric Technology for Human Identification* (2004).
20. A. Abhyankar and S. Schuckers, "Characterization, similarity score and uniqueness associated with perspiration pattern," in *Proc. 5th Int. Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Vol. **5**, pp. 301–309 (2005).
21. B. Tan and S. Schuckers, "Liveness detection using an intensity based approach in fingerprint scanner," in *Proc. Biometrics Symp.* (2005).
22. S. Schuckers and A. Abhyankar, "Detecting liveness in fingerprint scanners using wavelets: results of the test dataset," in *Proc. Int. Biometric Authentication Workshop (BioAW 2004)*, pp. 100–110 (2004).
23. S. A. C. Schuckers, S. T. V. Parthasaradhi, R. Derakshani, and L. A. Hornak, "Comparison of classification methods for time-series detection of perspiration as a liveness test in fingerprint devices," in *Proc. Int. Conf. on Biometric Authentication (ICBA) 2004*, pp. 256–263 (2004).
24. R. Derakhshani, "Spoof-proofing fingerprint systems using evolutionary time-delay neural networks," in *Proc. IEEE Int. Conf. on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS)* (2005).
25. A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *IEEE Trans. Inf. Forensics Security* **1**(3), 360–373 (2006).
26. A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "A new approach to fake finger detection based on skin distortion," in *Proc. Int. Conf. on Biometric Authentication (ICB) 2006*, pp. 221–228 (2006).
27. Y. Chen and A. Jain, "Fingerprint deformation for spoof detection," in *Proc. Biometrics Symp.* (2005).
28. Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, "Fake finger detection based on thin-plate spline distortion model," in *Proc. Int. Conf. on Biometric Authentication (ICB) 2007*, pp. 742–749 (2007).
29. B. Tan and S. A. C. Schuckers, "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing," in *2006 Conf. on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, pp. 26–33 (2006).
30. P. Coli, G. L. Marcialis, and F. Roli, "Power spectrum-based fingerprint vitality detection," in *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 169–173 (2007).
31. Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, "Wavelet based fingerprint liveness detection," *Electron. Lett.* **41**(20), 1112–1113 (2005).
32. P. Coli, G. L. Marcialis, and F. Roli, "Analysis and selection of features for the fingerprint vitality detection," in *Proc. Joint IAPR Int. Workshop on Structural and Syntactical Pattern Recognition and Statistical Techniques in Pattern Recognition (SSPR/SPR)*, pp. 907–915 (2006).
33. A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques," in *2006 IEEE Int. Conf. on Image Processing*, pp. 321–324 (2006).
34. Y. Chen, S. Dass, and A. Jain, "Fingerprint quality indices for predicting authentication performance," in *Proc. Int. Conf. on Audio- and Video-Based Biometric Person Authentication*, pp. 160–170 (2005).
35. E. Lim, X. Jiang, and W. Yau, "Fingerprint quality and validity analysis," in *IEEE Int. Conf. on Image Processing (ICIP)*, Vol. **1**, pp. 469–472 (2002).
36. L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE Trans. Pattern Anal. Mach. Intell.* **20**(8), 777–789 (1998).
37. R. Duda, P. Hart, and D. Stork, *Pattern Classification*, John Wiley and Sons, Inc. (2001).
38. http://www.digent.com/product/fmfd.htm (accessed on Jan. 20, 2009).
39. http://www.nitgen.com/New_site/eng/product/product.asp (accessed on Jan. 20, 2009).
40. http://www.unioncomm.co.kr/eng/product/pro_detail.asp?prod_code=0000071 (accessed on Jan. 20, 2009).
41. http://www.supremainc.com/eng/product/em_13.php?mark=213 (accessed on Jan. 20, 2009).
42. http://www.globalcas.com/bemarket/shop/index.php?pageurl=page_goodsdetail&part_code=130004005&uid=324 (accessed on Jan. 20, 2009).
43. E. Tabassi, C. Wilson, and C. Watson, "Fingerprint image quality," NIST Research Report NISTIR7151 (2004).
44. B. Efron and R. Tibshirani, "Bootstrap methods for standard errors, confidence intervals, and other measures of statistical accuracy," *Stat. Sci.* **1**, 54–75 (1986).
45. http://edis.ifas.ufl.edu/PD006 (accessed on Jan. 20, 2009).

Heeseung Choi received the BS and MS degrees in electrical and electronic engineering from Yonsei University, Seoul, Korea, in 2004 and 2006, respectively. He is currently pursuing his PhD in electrical and electronic engineering. He has been a research member of BERC (Biometrics Engineering Research Center). His research interests include computer vision, biometrics, image processing, and pattern recognition.

Raechoong Kang received the BS and MS degrees in electrical and electronic engineering from Yonsei University, Seoul, Korea, in 2006 and 2008, respectively. His research interest is in biometrics, image processing, and pattern recognition.



Kyoungtaek Choi received the BS degree in electrical and electronics engineering from Chung-ang University, Seoul, Korea, in 2001, and the MS degree in electrical and electronic engineering from Yonsei University, Seoul, Korea, in 2003. He received the PhD degree in electrical and electronic engineering from Yonsei University. Currently he is a senior researcher at BERC (Biometrics Engineering Research Center) in Korea and has been researching fingerprint registration, touchless fingerprint recognition, and fake-fingerprint detection. His research interests include computer vision, biometrics, image processing, and pattern recognition.

Andrew Teoh Beng Jin obtained his BEng (electronics) in 1999 and his PhD degree in 2003 from National University of Malaysia. He is currently an assistant professor in the Electrical Engineering Department, College of Engineering, Yonsei University. His research interest is in biometric security, watermarking, and pattern recognition. He has published around 130 international journal and conference papers in his area.

Jaihie Kim received the BS degree in electronic engineering from Yonsei University, Seoul, Korea, in 1979, and the MS degree in data structures and the PhD degree in artificial intelligence from Case Western Reserve University, Cleveland, OH, in 1982 and 1984, respectively. Since 1984, he has been a professor in the School of Electrical and Electronic Engineering, Yonsei University. He is currently the Director of the Biometric Engineering Research Center in Korea. His research areas include biometrics, computer vision, and pattern recognition. Prof. Kim is currently the chairman of the Korean Biometric Association.