A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis

Jia Jia, Lianhong Cai, Kaifu Zhang, and Dawei Chen

Key Laboratory of Pervasive Computing (Tsinghua University), Ministry of Education
Beijing 100084, P.R. China
jiajia@mails.tsinghua.edu.cn,
clh-dcs@tsinghua.edu.cn,
zkf03@mails.tsinghua.edu.cn,
RunningOn9@gmail.com

Abstract. This work introduces a new approach to fake finger detection, based on the analysis of human skin elasticity. When a user puts a finger on the scanner surface, a sequence of fingerprint images which describes the finger deformation process is captured. Then two features which represent the skin elasticity are extracted from the image sequence: 1) the correlation coefficient of the fingerprint area and the signal intensity; 2) the standard deviation of the fingerprint area extension in x and y axes. Finally the Fisher Linear Discriminant is used to discriminate the finger skin from other materials such as gelatin. The experiments carried out on a dataset of real and fake fingers show that the proposed approach and features are effective in fake finger detection.

1 Introduction

Fingerprint authentication (verification/identification) is one of the most important biometric technologies [1]. A fingerprint is the pattern of ridges and valleys (furrows) on the surface of the finger. As the fingerprint of a person is unique and immutable, the automatic fingerprint authentication system can be widely used in both anti-criminal and civilian applications. However, the security of fingerprint scanners has been questioned. Previous studies have shown that fingerprint scanners can be fooled with artificial fingerprints, i.e. copies of real fingerprints [2, 3]. Some approaches have been recently presented to deal with the above problem which is often referred to as "fake finger detection", i.e. the discrimination of a fake fingerprint from real ones [4, 5, 6]. Some of them use extra hardware to acquire life signs such as epidermis temperature, pulse oximetry, blood pressure and electric resistance [2, 5, 7]. Unfortunately, due to the inherent variability of such characteristics, the performance achieved by most of these methods is not satisfactory [6]. Furthermore, the equipments are usually expensive. Another fake finger detection method has been recently proposed in [8]. The user is required to move the finger once it touches the scanner surface, and a sequence of DistortionCodes [9] is captured from the fingerprint frames acquired during the finger movement and further analyzed to determine the nature of the finger. However, the way how the images are acquired is not user friendly.

S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, pp. 309–318, 2007.
© Springer-Verlag Berlin Heidelberg 2007

This paper introduces a novel approach which is based on the elasticity analysis of human skin. When a user puts a finger on the scanner surface as normal fingerprint authentication system required, a sequence of fingerprint images which describes the finger deformation process is captured (explained by Fig. 1). Two features representing the skin elasticity are extracted from the image sequence. As fake finger detection is actually a two-class classification problem, the Fisher Linear Discriminant [10] is finally used to label the feature vectors with "real" or "fake".

Fig. 1. A sequence of fingerprint images which describes the deformation of a real finger

The proposed approach has the following advantages: 1) the sequence of fingerprint images used for fake finger detection is also used for fingerprint authentication. The whole sequence is used for fake finger detection while one or more of them can be used for fingerprint authentication. It's an effective way to prevent the attacker from using artificial fingerprint and real fingerprint for fake finger detection and authentication steps respectively; 2) the way how the image sequences are acquired is user friendly. The approach requires no extra hardware or special finger movement. The experiments carried out on a dataset of real and fake fingers show that the proposed approach and features are effective in fake finger detection.

The rest of this paper is organized as follows. Section 2 introduces the related work. And section 3 describes the proposed approach in detail. In section 4, we give the experimental results and discussion. Finally, we wrap up with the conclusions and future work in section 5.

2 Related Work

Fake finger detection in a fingerprint authentication system means the capability for the system to detect, during enrollment and authentication, whether the fingerprint presented is alive or not [11]. Fake finger detection can be performed either at the fingerprint acquisition stage, or at the fingerprint processing stage [12].

There are essentially three different ways to introduce liveness detection into a biometric system [5]:

- Using extra hardware to acquire life signs [3, 6, 13]. In this way, the liveness detection takes place at the acquisition stage.
- Using the information already captured by the system to detect life signs [7, 8, 14]. In this way, the liveness detection takes place at the processing stage.
- Using liveness information inherent to the biometric [15].

The first way introduces a few other problems: 1) it is expensive; 2) it is bulky; and 3) it could still be possible to present the artificial fingerprint to the fingerprint scanner and the real fingerprint of the intruder to the hardware that detects liveness. Also, in some cases it is still possible to fool the additional hardware with a wafer-thin artificial fingerprint. The second method does not have these disadvantages, except maybe that it is a bit more complicated to extract the life signs using no additional hardware. Furthermore, special finger movement is usually required to acquire life signs in this kind of methods. The third method is not applicable to fingerprint recognition. Other biometric systems including face recognition, gait recognition, etc. use this however. These technologies are not widely implemented and still need to be validated as reliable biometric identifiers [11, 15].

The proposed approach performs fake finger detection at the image processing stage. We adopt the second way which uses the information already captured by the system to detect life signs. No special finger movement is required in our approach.

3 A New Approach to Fake Finger Detection

When a user puts a finger on the scanner surface, our scanner captures a sequence of fingerprint images at a certain frame rate. For example, when the frame rate is 20 fps (frames per second) and the capturing duration is 1.5s, the image number of every sequence is 30. The image sequence is used for fake finger detection. One or more of them can be used for fingerprint authentication. Let $\{F_1, F_2, \ldots\ldots, Fn\}$ be the sequence of n images. For each image sequence, we compute two features:(1) the correlation coefficient of the fingerprint area and the average signal intensity; (2) the standard deviation of the fingerprint area extension in x and y axes. Finally the Fisher Linear Discriminant is used to determining the final "real" or "fake" results.

In order to show the ability of the presented two features in discriminating fake fingers from real ones, we used one-way analysis of variance□ANOVA□and Multiple Comparison Method to do the statistical tests on the dataset of real and fake fingers. As the material humidity has great effects on the elasticity of fake fingers and the signal intensity of gray-level image, we collected 4 different data groups in ANOVA and Multiple Comparison tests:

- R Real finger group (Real): 30 real fingers;
- Wet gelatin fake finger group (Wet): 47 gelatin fake fingers with high humidity;
- Medium gelatin fake finger group (Medium): 47 gelatin fake fingers with normal humidity;
- Dry gelatin fake finger group (Dry): 47 gelatin fake fingers with low humidity.

We used capacitive scanner Veridicom FPS200 to record the image sequences. For each finger, only one image sequence was recorded. The humidity of different groups of fake fingers compared with real ones is shown in Table 1.

Table 1. The humidity of fake fingers compared with real ones

	Wet gelatin	Medium gelatin	Dry gelatin
Humidity	>> Real	Approximately = Real	< Real

3.1 Computing the Correlation Coefficient of Fingerprint Area and Signal Intensity

For a sequence $\{F_i (i=1, 2,\ldots\ldots, n)\}$, the following steps are performed on each frame F_i (i=1, 2,……, n):

Extracting the fingerprint area: let S_i (i=1, 2,……, n) represents the fingerprint area of F_i (i=1, 2,……, n). We first divide F_i into blocks of size $w \times w$ (16×16). The variance of each block is computed by Eq.1.

$$VAR = \frac{1}{w^2}\sum_{i=0}^{w-1}\sum_{j=0}^{w-1}(I(i, j) - M)^2, \quad M = \frac{1}{w^2}\sum_{i=0}^{w-1}\sum_{j=0}^{w-1} I(i, j) \tag{1}$$

where $I(i, j)$ represents the intensity (0-255) of the pixel at the ith row and jth column in one block. M represents the mean value of the block intensity. The fingerprint area S_i is obtained by Eq.2.

$$S_i = N_i \times w \times w \tag{2}$$

where N_i is the number of blocks whose VAR is greater than a certain threshold.

Computing the average signal intensity of the fingerprint area: the average signal intensity $AvgInt_i$ (i=1, 2,……, n) of the fingerprint area is computed by Eq.3.

$$AvgInt_i = \sum_{I(x,y)>\varepsilon} I(x, y) / S_i \tag{3}$$

where $I(x, y)$ is the intensity of the pixel in fingerprint area of F_i.$\varepsilon$is a threshold which is used to separate the pixels in fingerprint area from the ones in background.

Let $Corr$ represents the correlation coefficient of the fingerprint area $\boldsymbol{S}=\{S_i\}$ (i=1,2,……, n) and the signal intensity $\boldsymbol{AvgInt}=\{AvgInt_i\}$($i$=1,2,……, n). The $Corr$ is obtained by Eq.4.

$$Corr(\boldsymbol{S}, \boldsymbol{AvgInt}) = \frac{Cov(\boldsymbol{S}, \boldsymbol{AvgInt})}{\sqrt{D(\boldsymbol{S}) \times D(\boldsymbol{AvgInt})}} \tag{4}$$

where $Cov(\boldsymbol{X}, \boldsymbol{Y})$ is the covariance of $\boldsymbol{X}$ and $\boldsymbol{Y}$, and $D(\boldsymbol{X})$ is the squared deviation of $\boldsymbol{X}$.

The signal intensity captured by a capacitive sensor is effected by to two factors: the pressing pressure and the humidity of finger skin (or other materials). For a real finger, with the increase of pressure, the fingerprint area S and the signal intensity $AvgInt$ increases both, which means they have a positive correlation. Fig. 2 shows the relation of S and $AvgInt$ of a real finger and a gelatin finger. For real finger, with the increase of fingerprint area from 3.5 to 5.5 ($\times 10^4$), the average intensity monotonically increases from 100 to 170. But for fake finger, with the increase of fingerprint area, the average intensity presents a random fluctuation, which means they have no obvious correlation.

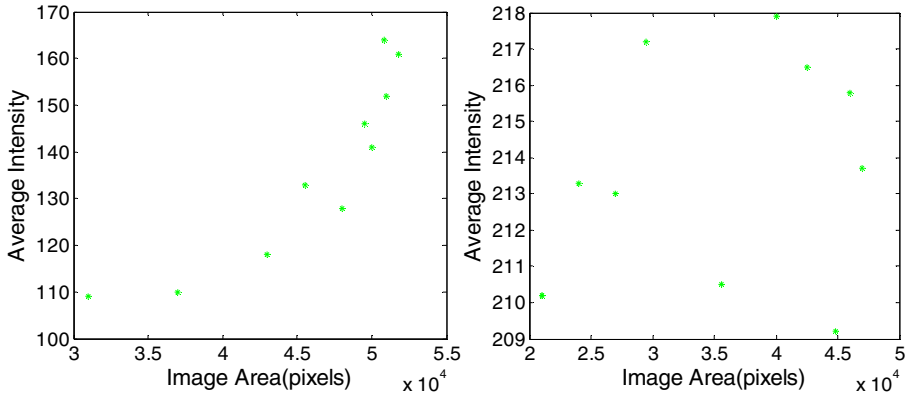


Fig. 2. The average intensity as a function of the fingerprint area. (a) a real finger, (b) a gelatin finger.

Table 2 gives the ANOVA results of the feature *Corr*. The Multiple Comparison results of *Corr* are shown in Fig.3(a). The *p* value of ANOVA is 2.77e-008, which indicates that this feature is effective in discriminating samples of different groups. The Multiple Comparison results shows that although the humidity of the finger skin (or other materials) can affect the image signal intensity, the *Corr* value can still clearly separate the real finger group from other three fake finger groups.

Table 2. ANOVA Table of feature *Corr*

ANOVA Table			
Source[1]	Groups	Error	Total
SS	15.1235	22.6909	37.8144
d.f.	3	74	77
MS	5.0412	0.30663	
F	16.4403		
p>F	2.77e-008		

3.2 Computing the Standard Deviation of Fingerprint Area Extension in x and y Axes

For each frame F_i and its next frame F_{i+1} in a image sequence $\{F_i\ (i=1, 2,\ldots\ldots, n)\}$, we compute the fingerprint area extension Ho_i (i=1, 2,……, n-1) in x axis and Ver_i (i=1, 2,……, n-1) in y axis, shown in Eq.5.

[1] The notations in ANOVA: 1. SS: Sum of Squares; 2. d.f.: degrees of freedom; 3. MS: Mean Square; 4. F ratio = (found variation of the group averages)/ (expected variation of the group averages); 5. p: probability.

$$Ho_i = abs(\max x_{i+1} - \min x_{i+1}) - abs(\max x_i - \min x_i)$$
$$Ver_i = abs(\max y_{i+1} - \min y_{i+1}) - abs(\max y_i - \min y_i) \quad (5)$$

where x_i and y_i indicate the pixel coordinate of F_i, and $abs(x)$ is the absolute value of x.

Let *Std* presents the mean value of the standard deviation of $\boldsymbol{H}=\{Ho_i\}$and $\boldsymbol{V}=\{Ver_i\}$ (i=1,2,……, n-1), as shown in Eq.6.

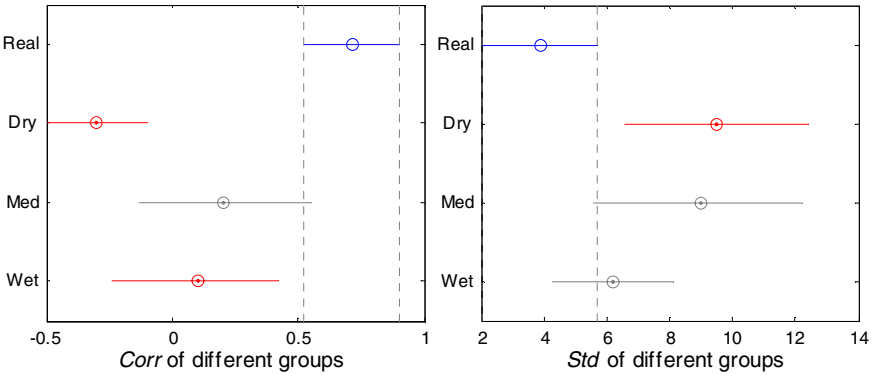
$$Std(\boldsymbol{H},\boldsymbol{V}) = \frac{1}{2}\sqrt{D(\boldsymbol{H}) \times D(\boldsymbol{V})} \quad (6)$$

where $D(\boldsymbol{X})$ is the squared deviation of $\boldsymbol{X}$.

The *Std* feature indicates the skin extension in finger deformation process. Table 3 gives the ANOVA results of the feature *Std*. And the Multiple Comparison results of *Std* are shown in Fig.3(b). The p value of ANOVA is 0.0062, which indicates this *Std* feature can discriminate fake fingers from real ones for most cases. But it has a lower discriminating ability than feature *Corr*. The Multiple Comparison results shows that the *Std* feature can clearly separate the real finger group from medium/dry fake finger groups, while it still has limitation in discriminating the real finger group and the wet fake finger group.

Table 3. ANOVA Table of feature *Std*

ANOVA Table			
Source	Groups	Error	Total
SS	351.88	1946.27	2298.14
d.f.	3	74	77
MS	117.292	26.301	
F	4.46		
p>F	0.0062		



(a) (b)

Fig. 3. The Multiple Comparison results in four different groups. (a)feature Corr, (b)feature Std.

3.3 Determining Results by the Fisher Linear Discriminant

We define a 2-tuple vector $\boldsymbol{V}$=($Corr$, Std) to describe the elasticity features of each sequence. Where $Corr$ is the correlation coefficient of the fingerprint area $\boldsymbol{S}$=$\{S_i\}$ (i=1,2,……, n) and the average signal intensity $\boldsymbol{AvgInt}$=$\{AvgInt_i\}$(i=1,2,……, n); Std is the mean value of the standard squares of $\boldsymbol{H}$=$\{Ho_i\}$and $\boldsymbol{V}$=$\{Ver_i\}$ (i=1,2,……, n-1).

As fake finger detection is actually a two-class classification problem, the Fisher Linear Discriminant is chosen as the classifier. The Fisher Linear Discriminant is a classification method that projects high-dimensional data onto a line and performs classification in this one-dimensional space. The projection maximizes the distance between the means of the two groups while minimizing the variance within each group. The decision function of the Fisher Linear Discriminant is explained by Eq.7.

$$\begin{aligned} Group(\boldsymbol{X}) &= \text{real finger} \quad \text{for } \boldsymbol{W} \times \boldsymbol{X} + b >= c \\ &= \text{fake finger} \quad \text{for } \boldsymbol{W} \times \boldsymbol{X} + b < c \end{aligned} \tag{7}$$

where b is a constant, c is the threshold and W is the regression coefficients matrix.

The flowchart of our fake finger detection approach is shown as Fig. 4. This paper focuses on the parts with gray-background.

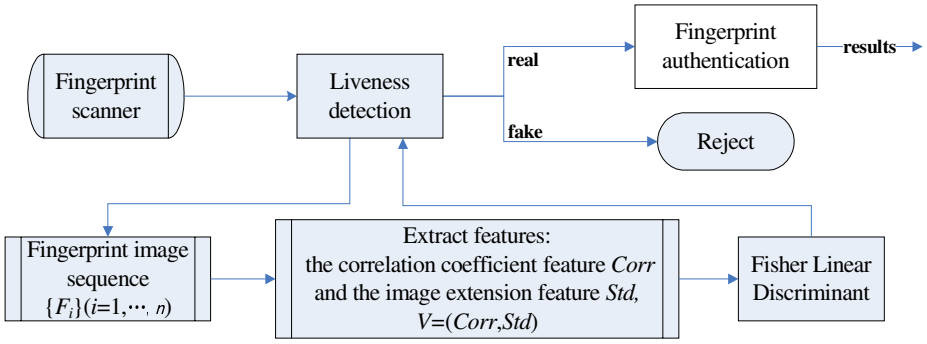


Fig. 4. A flowchart showing different phases of our approach

4 Experiments and Discussion

In this section we describe some experiments to evaluate the presented fake fingerprint detection approach.

4.1 Datasets

In order to evaluate the proposed approach, a dataset of image sequences was collected. The dataset was acquired from 15 volunteers, all of whom were graduates of the Computer Science and Technology Department, Tsinghua University. For real fingerprints, two fingers were collected from each volunteer; ten image sequences were recorded for each real finger. For fake fingerprints, 47 fake fingers were manufactured, all of which were made of gelatin and had medium humidity; ten image

sequences were recorded for each fake finger. The total number of the image sequences is 770. And the image sequences were acquired using the capacitive fingerprint scanner "Veridicom Fps200", which produces 250×300 fingerprint images at 500 DPI.

Table 4. The information of dataset

	Different fingers/ Image sequences	Sensors	Image size	Resolution
Real fingerprint	30/300	capacitive sensor	250×300	500 dpi
Fake fingerprint	47/470	capacitive sensor	250×300	500 dpi

4.2 Measures

Let FAR (False Accept Rate) be the proportion of fake fingers that are incorrectly accepted, and FRR (False Reject Rate) be the proportion of real fingers that are incorrectly rejected. The EER (that is the value such that FRR =FAR) is reported as a performance indicator. Note that FAR and FRR do not include verification/identification errors. The configuration of the running computer is Pentium 2.60 GHz, 1.00GB.

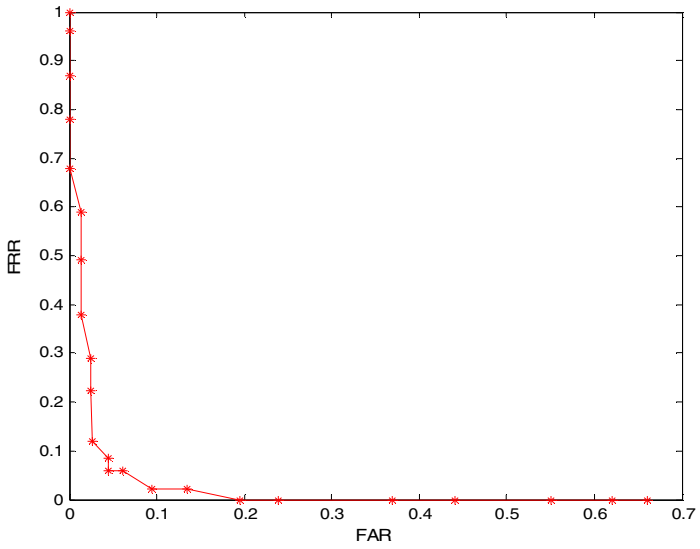


Fig. 5. The FRR as a function of FAR of the proposed approach

Table 5. The experimental result for fake finger detection of different systems

	Fake finger detection by odor analysis	Fake finger detection based on skin distortion	Our approach
EER	7.48%	4.90%	4.78%

4.3 Experimental Results and Discussion

For each fingerprint image sequence, we extracted the features and used the Fisher Linear Discriminant to determine the final results. In our experiments, the dataset was divided into two parts: a set (400 sequences, from 15 real fingers and 25 fake fingers) used for training the classification models; and a test set (370 sequences, from the other 15 real fingers and 22 fake fingers) used to measure the performance. We change the threshold parameter of the Fisher Linear Discriminant ($\boldsymbol{W} \times \boldsymbol{X} + b > c$, changed c) to get the FRR as a function of FAR. The experimental result is shown in Fig.5. And the EER of the proposed approach measured in the above described experimentation was 4.78%. The experimental results strongly suggest that the presented features and approach are effective in discriminating fake fingers from real ones. Although it is not fair to compare our approach with other fake finger detection systems due to the difference in experimental datasets, we also list the experimental results of three different systems in Table 5. The first system uses extra hardware to capture the odor signal to discriminate the finger skin odor from that of other materials [6]. The second system requires user to move the finger once it touches the scanner surface; and uses a sequence of DistortionCodes to determine the nature of the finger [8]. Obviously it is impossible for our approach to use the same datasets with the other two systems.

5 Conclusion

Our main contributions to fake finger detection are: 1) proposing a software-based fake finger detection approach. The approach uses a user friendly way to acquire a sequence of fingerprint images for each finger. The features are extracted from the image sequences and further analyzed by Fisher Linear Discriminant to determine the nature of the finger; 2) proposing two features representing the skin elasticity: the correlation coefficient of the fingerprint area and the average image signal intensity, and the standard deviation of the fingerprint area extension in x and y axes. The features have strong ability in discriminating the fake fingers from real ones. The experimental results show that the proposed features and approach are effective in fake finger detection.

Future work may include: acquiring a larger dataset to evaluate the performance of the proposed approach, and investigating more features that represent the skin elasticity.

Acknowledgements

This research was supported by China National Natural Science Foundation (60433030, 60418012), and the Special Funds for Major State Basic Research Program of China (973 Program) (No. 2006CB303101). And we would like to thank reviewers for their kindly review and helpful comments for this paper.

References

1. Newham, E.: The Biometric Report. SJB Services, New York (1995)
2. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of Artificial ”Gummy” Fingers on Fingerprint Systems. In: Proceeding of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275–289 (2002)
3. Putte, T.v.D., Keuning, J.: Biometrical Fingerprint Recognition: Don’t Get Your Fingers Burned. In: Proceeding of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pp. 289–303 (2000)
4. Derakhshani, R., Schuckers, S.A.C., Hornak, L., O’Gorman, L.: Determination of Vitality from a Non-invasive Biomedical Measurement for Use in Fingerprint Scanners. Pattern Recognition 36(2), 383–396 (2003)
5. Schuckers, S.A.C.: Spoofing and Anti-spoofing Measures. Information Security Technical Report 7(4), 56–62 (2002)
6. Baldisserra, D., Franco, A., Maio, D., Maltoni, D.: Fake Fingerprint Detection by Odor Analysis. In: Zhang, D., Jain, A.K. (eds.) Advances in Biometrics. LNCS, vol. 3832, pp. 265–272. Springer, Heidelberg (2005)
7. Parthasaradhi, S.T.V., Derakhshani, R., Hornak, L.A., Schuckers, S.A.C.: Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices. IEEE Transactions on Systems, Man, and Cybernetics-Part C:Applications and Reviews 35(3) (2005)
8. Antonelli, A., Cappelli, R., Maio, D., Maltoni, D.: A New Approach to Fake Finger Detection Based on Skin Distortion. In: Zhang, D., Jain, A.K. (eds.) Advances in Biometrics. LNCS, vol. 3832, pp. 221–228. Springer, Heidelberg (2005)
9. Cappelli, R., Maio, D., Maltoni, D.: Modeling Plastic Distortion in Fingerprint Images. In: Singh, S., Murshed, N., Kropatsch, W.G. (eds.) ICAPR 2001. LNCS, vol. 2013, pp. 369–376. Springer, Heidelberg (2001)
10. Fisher, R.A.: The Use of Multiple Measurements in Taxonomic Problems. Annals of Eugenics 7(partII), 179–188 (1936)
11. Sandstrom, M.: Liveness Detection in Fingerprint Recognition Systems. Master thesis (2004), http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf
12. International Biometric Group: Optical-silicon-ultrasound. White paper (2004), Available at http://www.biometricgroup.com/reports/public/reports/finger-scan optsilult.html
13. Lapsley, P.D., Lee, J.A., Pare Jr., D.F., Hoffman, N.: Anti-fraud biometric sensor that accurately detects blood flow. SmartTouch, LLC., US Patent #5737439 (April 1998)
14. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, New York (2003)
15. Woodward Jr., J.D., Orlands, N.M., Higgins, P.T.: Biometrics: Identity assurance in the information age. McGraw-Hill/Osborne, Berkeley, California, USA (2003)