A New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis

Bozhao Tan and Stephanie Schuckers

Department of Electrical and Computer Engineering, Clarkson University

Potsdam, NY 13699

87.57.Nk, 87.17.Aa

ABSTRACT

Recently, research has shown that it is possible to spoof a variety of fingerprint scanners using some simple techniques with molds made from plastic, clay, Play-Doh, silicone or gelatin materials. To protect against spoofing, methods of liveness detection measure physiological signs of life from fingerprints ensuring only live fingers are captured for enrollment or authentication. In this paper, a new liveness detection method is proposed which is based on noise analysis along the valleys in the ridge-valley structure of fingerprint images. Unlike live fingers which have a clear ridge-valley structure, artificial fingers have a distinct noise distribution due to the material's properties when placed on a fingerprint scanner. Statistical features are extracted in multiresolution scales using wavelet decomposition technique. Based on these features, liveness separation (live/non-live) is performed using classification trees and neural networks. We test this method on the dataset which contains about 58 live, 80 spoof (50 made from Play-Doh and 30 made from gelatin), and 25 cadaver subjects for 3 different scanners. Also, we test this method on a second dataset which contains 28 live and 28 spoof (made from silicone) subjects. Results show that we can get approximately 90.9-100% classification of spoof and live fingerprints. The proposed liveness detection method is purely software

based and application of this method can provide anti-spoofing protection for fingerprint scanners.

Keywords: Liveness detection, Biometrics, Wavelet signal processing, Classification tree, Neural network

1. INTRODUCTION

Biometric systems are an emerging technology that enables the authentication of an individual based on physiological characteristics including face, fingerprint, iris, hand geometry, palm, or behavioral characteristics including voice, gait, keystroke dynamic and handwriting signature, etc [1]. While biometrics may improve security, biometric systems are found to be vulnerable to attacks at the biometric sensor level, replay attacks on the data communication level, and attacks on the database [2]. For example, previous studies have shown it is possible to fool a variety of fingerprint scanners using a well-duplicated synthetic finger made of silicone rubber, Play-Doh, wax, clay, gelatin, or in the worst cased, dismembered fingers [3, 4, 5, 6]. These materials are moisture based and most fingerprint scanners are able to image them. Some examples are showed in Figure 1 and Figure 2. Face or iris recognition systems can be spoofed by static facial or iris images. To improve security for the biometric systems, liveness detection (or vitality detection) is proposed to defeat this kind of spoof attacks. Liveness detection is an anti-spoofing method ensuring that only the biometric from a live, authorized person is submitted for enrollment, verification and identification [7]. In our work, we focus on the research of liveness detection in fingerprint scanners.

There are two different ways to introduce liveness detection into fingerprint recognition systems: at the acquisition stage or at the processing stage. The first method uses extra hardware to acquire life signs. For example, measuring fingertip temperature, pulse, pulse oximetry, blood pressure, electric resistance, odor, or ECG [8, 9, 10, 11, 12, 27]. These methods introduce difficulties because it is expensive and bulky. Furthermore, it may still be possible to present an artificial fingerprint to the fingerprint sensor and utilize the real fingerprint of the intruder for the hardware to detect liveness. The second method uses the information already captured by the system to detect life signs, for example, skin deformation, pores or perspiration pattern. Skin deformation technique uses the information about how the fingertip's skin deforms when pressed against the scanner surface [13, 25, 26]. However, using a thin artificial fingerprint glued on a live finger may still generate a similar non-linear deformation as a live finger would [8, 13]. By using a fingerprint sensor with a high resolution, it may be possible to use the pore's detail [13] and skin coarseness [28] as a liveness detection method. However, the work by Matsumoto et al. [4] has shown that a coarse reproduction of intra-ridge pores is feasible with gelatin artificial fingerprints.

2. PREVIOUS WORK IN OUR LABORATORY

In the previous research, our laboratory has demonstrated that the time-varying perspiration pattern in the fingerprint images can be used as a purely software based measure to detect liveness. Unlike spoof and cadaver fingers, live fingers have a distinctive spatial phenomenon both statically and dynamically [14].

In live fingers, perspiration starts from the pores, either completely covering them which makes them wet or leaving the pores as a dry dot. Statically the live fingerprint

looks patchy compared to spoof and cadaver fingerprints due to this special phenomenon specific to live fingers [14]. Dynamically, the live fingers have a distinct changing moisture pattern. Based on this principle, a ridge signal algorithm, a wavelet algorithm and an intensity based algorithm have been developed to detect the time-series perspiration pattern for liveness detection. Details about these methods are found in [14, 15, 16, 17, 29].

In addition, a method to quantify this phenomenon has been developed for a single image. This method is based on the gray levels along the ridges in live fingers which have a distinctive difference in the frequency pattern due to the presence of perspiration and pores, compared to the spoof and cadaver fingers [18]. The underlying process is to extract the ridge signal which represents the gray level values along a ridge mask and use wavelet transform to decompose this signal into multiscales. Statistical features are extracted on each scale which quantifies the perspiration pattern to discriminate between live and non-live fingerprints.

These methods are capable of producing classification rates in the range of 84%~100% for the three scanners tested.

Some methods which quantify the perspiration pattern rely on two time series images [14, 15, 16, 17, 29]. One method relies on only one image [18]. More research is needed to reduce the time and improve the performance of these algorithms. In addition, it is clear that the variation between the sensors and live/spoof fingers varies dramatically from technology to technology. More research is needed to develop approaches which are optimal for a particular technology.

Figure 1 shows a typical example of the first image captured from live, Play-Doh, gelatin and cadaver fingers using capacitive DC scanner in our database, respectively. Figure 2 shows a typical example of the first image captured from live, silicon fingers using optical scanner in another database. As can be observed, compared to live fingerprints with a clear ridge-valley structure, the spoof and cadaver fingerprint have much noise along the valleys. The reason is either because the spoof materials are easily transmuted or because there are many granules between the ridges due to the property of the spoof materials.

FIG. 1 HERE

FIG. 2 HERE

In our new approach, the basis of this method is simple and straightforward. We apply image processing technique to quantify the noise difference along valleys between live and non-live fingers.

The underlying process is to extract the valley signal, that is the gray level values along a mask which detects the valley. The wavelet transform is used to analyze the valley signal in multiscales. Statistical features are extracted on each scale are used to quantify the noise difference in order to discriminate between live and non-live fingerprints. Here we should note that the fingerprint images in our database are 0 second images immediately after the placement of the fingers.

3. Valley Noise Analysis

The main steps of this algorithm include:

1). Fingerprint enhancement;

2). Valley mask and signal extraction;

3). Wavelet analysis;

4). Statistical feature extraction;

5). Classification.

3.1. Fingerprint Enhancement

To improve the clarity of ridge and valley structures in fingerprint images, a number of techniques have been proposed to enhance gray-level images because the ridge and valley structures in a local neighborhood form a sinusoidal-shaped wave with well-defined frequency and orientation [19, 20]. Here, we use the enhancement algorithm proposed in Hong et al. [19], which applies a bank of bandpass Gabor filters on the normalized fingerprint image using estimated orientation and frequency information. Instead we will focus on the extraction of a valley mask, not a ridge mask as many methods have used for fingerprint recognition.

3.1.1. Pre-processing

To segment the foreground region of interest, the whole image is divided into blocks of small size and the variance of each block is computed. If the variance of a block is less than a threshold value, then it is removed from original image. Usually an elliptical shape of fingerprint foreground is kept and the corner parts are removed.

3.1.2. Local Orientation Estimation

The fingerprint has a consistent structure of ridges and valleys in a local neighborhood. The local ridge orientation is commonly used to tune the filter parameters for enhancement. In the Hong et al. enhancement algorithm, a least mean square orientation estimation method is used. The local orientation in an image can be computed by

$$V_x(i,j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} 2\sigma_x(u,v)\sigma_y(u,v) \quad (1)$$

$$V_y(i,j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} (\sigma_x^2(u,v) - \sigma_y^2(u,v)) \quad (2)$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{V_y(i,j)}{V_x(i,j)}\right) \quad (3)$$

where θ(i, j) is the least square estimate of the local ridge orientation at the block centered at pixel (i, j). σ_x and σ_y represent the horizontal and vertical gradients. w is the window width for the block wise calculation. Here this method is processed at a block size of 16x16.

3.1.3. Local Frequency Estimation

The local ridge frequency is another important property in a fingerprint image. To get the local ridge frequency, X-signatures of each block are computed along the direction perpendicular to the orientation angle in each block. The oriented window used for this purpose is of size 32×16 ($\ell \times w$). The frequency is then computed by the distance between the peaks obtained in the X-signatures. The X-signature for this is given by the formula

$$X[k] = \frac{1}{w}\sum_{d=0}^{w-1} \mathrm{I}(u,v), k = 0,1,...,l-1 \quad (4)$$

$$u = i + (d - \frac{w}{2})\cos O(i,j) + (k - \frac{l}{2})\sin O(i,j) \quad (5)$$

$$v = j + (d - \frac{w}{2})\sin O(i,j) + (\frac{l}{2} - k)\cos O(i,j) \quad (6)$$

where I is the input image and O is the orientation image.

Based on experiments, we find that a median frequency of all blocks can be used to represent the whole frequency image for further Gabor filter processing.

3.1.4. Filtering using Gabor filer

Gabor filters consider both the frequency components as well as the spatial coordinates, which make it an excellent non-linear tool in spatial and frequency domains. After getting local orientation angle and frequency, a bank of Gabor filters is applied as a band-pass filter which removes the noise and enhances the ridge and valley structures. The even-symmetric Gabor filter has the general form.

$$h(x,y:\phi,f) = \exp\{-\frac{1}{2}[\frac{(x\cos\phi)^2}{\delta_x^2} + \frac{(y\sin\phi)^2}{\delta_y^2}]\}\cos(2\pi fx\cos\phi) \quad (7)$$

where ϕ is the orientation, f is the frequency, δ_x and δ_y are the parameters of Gaussian function along x and y axis.

To estimate the local orientation and frequency block wise, we need to take into consideration corrupted ridge and valley structures and the existence of minutiae in the fingerprint images. In these kinds of situations, low pass filtering and interpolation techniques can be used to reduce its negative effects. For the details about this algorithm, we can refer to [19]. Figure 3 shows the outcome of performing orientation estimation, frequency estimation and Gabor filtering.

FIG. 3 HERE

3.2. Valley Mask and Signal Extraction

After the input fingerprint image is enhanced with Gabor filtering, a binary image is extracted by comparison with a pre-defined threshold. Compared to other fingerprint enhancement algorithm extracting the ridge mask, a valley mask is extracted. A standard thinning algorithm using morphological operations can be used to obtain one pixel thin valleys. Y-junctions and some short curves shorter than a typical pore-to-pore distance are discarded using a simple non-overlapping neighbor operation. Then the final contour along the valleys can be used as a mask to generate signals corresponding to the actual gray level changes along the valleys. Figure 4 shows the binary output image, the extracted valley masks superimposed on the original fingerprint and the valley signal is extracted.

FIG. 4 HERE

3.3. Wavelet Analysis

As observed from the extracted valley signal (Figure 4), it is a non-stationary signal. The Fourier Transform (FT) would not be effective, because FT may not provide appropriate information when analyzing non-stationary signals. Although short time Fourier Transform (STFT) can map the signal into time and frequency domain, it may not be effective because it only uses a fixed window technique. Compared to FT and STFT,

the wavelet transform, provides a powerful tool for non-stationary signal processing because it can analyze the signal at different scales. From an algorithmic point of view, the 1-D multiresolution analysis leads to dyadic pyramidal implementations using filter banks [21]. It applies an orthogonal filter bank to compute a discrete-time wavelet transform when iterated on the lower band.

The procedure of multiresolution decomposition of a signal is schematically shown in figure 5. Each stage of this analysis consists of a highpass and lowpass filter followed by scale two downsampling. In this scheme, the scaling function and mother wavelet function can be calculated by:

$$\phi(n) = 2\sum_{n} h_n \phi(2x - n) \tag{8}$$

$$\psi(n) = 2\sum_{n} g_n \phi(2x - n) \tag{9}$$

where h_n and g_n are conjugate mirror filters, as in,

$$h[L-1-n] = (-1)^n g[n] \tag{10}$$

where L is the length of filters.

The output of the first high-pass and low-pass filters provide the detail D1 and the approximation A1, respectively. The first approximation, A1 is then decomposed to the second level detail D2 and approximation A2, and so on.

FIG. 5 HERE

Daubechies wavelet is selected as the mother wavelet [22, 23]. They are a family of orthogonal wavelets indexed by N, where N is the number of vanishing wavelet

moments. They are supported on an interval of length 2N-1. Their regularity increases linearly with N and is approximately equal to 0.2075N for large N. Figure 6 is the generated Daubechies low pass and high pass filter, in which *N* is 16. These filters lead to a scale and wavelet function, as shown in figure 7. The Daubechies solution comes from a selection of filters with maximum number of vanishing moments and minimum phase. The choice of minimum phase leads to the most asymmetric scale function, as you can observe in the above figure.

In this method, the scale selected is 5 because further decomposition detail does not contain much useful frequency content.

FIG. 6 HERE

FIG. 7 HERE

Figures 8, 9 and 10 show examples of decomposed wavelet transform on the valley signal from a typical live, spoof (Play-Doh), and cadaver finger. As can be observed from the comparison, spoof and cadaver fingerprints have higher amplitude and variance on the approximation and detail scales than that from live fingerprints, because non-live fingers are very noisy along the valleys but the live fingers are very clean, oppositely.

FIG. 8 HERE

FIG. 9 HERE

FIG. 10 HERE

3.4. Statistical Feature Extraction

The transformed wavelet coefficients provide a compact representation that shows the energy distribution of the signal both in time and frequency. To extract the feature vectors, mean and standard deviation of the wavelet coefficients in each scale are used. Besides the two parameters, mean and standard deviation, from the original signal, totally we extract 14 parameters including 10 from the 5 detail scales (D1~D5) and 2 from the last approximation A5. After investigating each parameter on the training and validation dataset, efficient statistical features are retained.

Figures 11 and 12 show an example of the comparison of mean and standard deviation in the 2nd detail level D2 between live, spoof and cadaver fingerprints, respectively. The comparison verifies our hypothesis that the mean and variance of the spoof and cadaver fingers are much higher than live subjects, except few cadaver samples.

FIG. 11 HERE

FIG. 12 HERE

3.5. Classification

After efficient features are extracted, classification trees and neural network are used to separate the non-live subjects from the live subjects. The non-live category includes the spoof data made from Play-Doh, gummy and cadaver fingers.

Classification trees derive a sequence of if-then-else rules using the training set in order to assign a class label to the input data. The user can see the decision rules clearly

to verify if the rules match their understanding about the classification. In our samples, while there are general trends, there are also few cadaver fingers look like live fingers but still have grey level differences in some subbands compared with live fingerprints. The classification tree works efficiently taking into consideration these situations. In our case, an Excel tool was applied to generate the classification tree automatically [24]. The training, validation and test data is randomly selected. Figure 13 shows the classification tree selected for the capacitive DC scanner. In this example, it only selects one feature and uses one rule to form a single level decision tree. In this decision tree, the enrolled subject is classified as live if the feature C (mean of detail D2) is larger than 0.015393 and it is classified as non-live if C is less than 0.015393, which matches our observation in the former discussion. Support means how many percent of the training data are supported by this rule and confidence means the confidence level about this specific decision rule. Figure 14 shows the classification tree selected for the optical1 scanner.

FIG. 13 HERE

FIG. 14 HERE

Neural network is another popular pattern classification method for non-linear problems. Multilayer perceptrons (MLPs) are feedforward neural networks trained with the standard back-propagation algorithm. They are supervised networks so they require a desired response to be trained. They learn how to transform input data into a desired response, so they are widely used for pattern classification. The multilayer perceptron is capable of learning a rich variety of nonlinear decision surfaces. It has been proven that

the standard MLPs with a single non-linear hidden layer (sigmoidal neurons) can approximate the performance of optimal statistical classifiers in difficult problems. In this case, a two-layer feed-forward network is created. The network's input is the extracted statistical features. The first hidden layer has 3 tansig neurons, the second layer has one purelin neuron. The trainlm network training function is to be used. For convenience of training, bipolar targets (+1,-1) are chosen to denote live and non-live categories, respectively. Here we use neural network toolbox from WEKA software [30].

4. DATA COLLECTION

To test our liveness algorithms, three types of fingerprint scanners were used to collect data in our laboratory: capacitive DC (Precise Biometrics, 100sc, 500dpi), optical1 (Secugen, EyeD hamster model #HFDUO1A, 500dpi) and electro-optical (Ethentica, USB2500, 403dpi). These systems were selected based on considerations of technology diversity, availability and flexibility of the SDK. We made 38 casts from live subjects using dental materials and made molds using Play-Doh and gelatin. Furthermore, we collected cadaver fingerprint images using these scanners. For each device, fingerprints images were collected from live, spoof and cadaver fingers. Only the fingerprints that can be enrolled and verified (at least once in six trials) are kept in the database. The dataset contains approximately 58 different live subjects (from different races, ages and balanced number of males and females with one image per person from right thumb or index finger), 80 spoof (made from 38 casts) and 25 cadaver fingerprints (from 10 subjects, multiple images from different fingers of the same subjects). For the spoof data, it includes 50 Play-Doh images including 10 images with changing pressure, and 30 gelatin images including 10 images with normal pressure, 10 images with changing pressure and

10 images with sprinkling water. All the images were collected in a single session. Only the images collected at 0 second, right after placing the fingers on the scanners, were used for our test in this approach.

Also we test this new method on the dataset collected by the group of Dr. Marcialis and Dr. Roli from University of Cagliari in Italy. They collect live and gummy fingerprints using an optical (optical2) scanner from Biometrika (FX2000) with a resolution of 569 dpi. They adopt a cooperative method for the collection of fake fingers, making the finger stamps using plastiline and then making the molds using liquid silicone. The gummy fingerprints they collected are after 1 hour when the silicone dries.

Table 1 summarizes the number of subjects used for each device and category. The spoof and cadaver fingerprints are included in the "non-live" category. The image utilized in this paper is the first image immediately after placement on the scanner in time-series collection.

TAB. 1 HERE

5. RESULTS

To evaluate this algorithm objectively, the dataset is divided into training (1/3), validation (1/3) and test (1/3) datasets. The randomly selected training and validation data is used to generate and determine the best classification tree and neural network. The decision tree or neural network which has the least FAR and FRR scores is chosen as the one most likely performing well on the unseen test data.

Figure 15 presents the test results for live and non-live fingerprints using classification trees method. For the test dataset, capacitive DC (Precise) scanner demonstrates a correct classification rate of 100% for live and 98.4% for non-live subjects. Optical1 scanner (Secugen) in our dataset demonstrates a correct classification rate of 100% for live and 91% for non-live subjects. The electro-optical scanner (Ethentica) in our dataset demonstrates a correct classification rate of 100% for live and 92.6% for non-live subjects. Optical2 scanner (Biometrika) demonstrates a correct classification rate of 90.9% for live and 100% for non-live subjects.

Figure 16 presents the test results for live and non-live fingerprints using neural network classification method. To the test dataset, capacitive DC (Precise) scanner demonstrates a correct classification rate of 100% for live and 93.5% for non-live subjects. Optical1 scanner (Secugen) in our dataset demonstrates a correct classification rate of 95.5% for live and 95.5% for non-live subjects. The electro-optical scanner (Ethentica) in our dataset demonstrates a correct classification rate of 85.7% for live and 88.1% for non-live subjects. The optical2 scanner (Biometrika) demonstrates a correct classification rate of 90.9% for live and 91.7% for non-live subjects.

Compared these two classification methods, we find the classification tree performs better than the neural network to this non-linear case. Classification tree automatically chooses that features from our set of 14 features. Sometimes only one or two features have efficient classification for the classification tree. Neural networks are sensitive to cases where too many features are used as inputs. Therefore, we choose five or six features based on separation achieved by visually assessing the scatter plots of each feature alone.

FIG. 15 HERE

FIG. 16 HERE

Figure 17 shows some examples where the algorithm fails in the capacitive DC scanner. When the live fingers are very wet (perspiration saturated) and the subjects enroll the fingers with pressure, some parts are smudged or the ridges merged together, this method will fail for the live subjects. In this kind of situation, quickly wiping the clothes and placing with normal pressure is an effective way to avoid this phenomenon. We also find this method is very efficient to separate these fake fingers made from Play-Doh, gelatin and silicone materials. This method can reach 100% correct classification for this kind of data. In the cases of failure, most non-live subjects are from the cadaver data. When the cadaver fingers have a clear ridge-valleys structure, it becomes a more difficult to make the correct classification.

FIG. 17 HERE

6. DISCUSSION

This research demonstrates that the vitality of fingerprints can be determined by a novel noise analysis method processing only a single image. The results show that this method compares with previous perspiration pattern detection methods. The system can become "spoof-proof" just by a simple software update.

The main problems of liveness detection methods based on extra hardware, is that the system is bulky and expensive. They are still vulnerable to attacks when impostors use a wafer-thin artificial fingerprint glued on a live finger. In these kinds of spoof attacks, detecting temperature, optical properties, pulse oximetry, blood pressure, electric resistance, etc. will lose their efficiency [8]. It is inconvenient for the users when using extra hardware, i.e. combining ECG, pulse oximetry, and temperature [3, 8]. Another method utilizing extra hardware is based on the acquisition of the odor by means of electronic sensor, which can detect the presence of human skin compared to artificial fingers [27]. One commercially available fingerprint sensor which includes spoof detection is from Lumidigm [31]. They use a multispectral sensor, from which multiple wavelengths of light and different polarizations allow new data to be captured which is unavailable from a conventional optical fingerprint reader. Based on the multiple spectral images, they have developed a spoof detection method.

One approach using existing fingerprint information is based on the difference of skin deformation between live and non-live fingers. The studies showed that when a real finger moves on a scanner surface, it produces a significant amount of non-linear distortion. However, the fake fingers are more rigid than skin and the deformation is lower even if they are made of highly elastic materials [13, 25, 26]. First, the problem of this method is that the users need to have a special training or have to know exactly how to apply pressure while rotating the fingers. Second, it requires the scanners are capable of delivering frames at a proper rate. However, only few scanners have this ability. Third, and the most important problem is that using a thin artificial fingerprint

glued on a live finger may still produce similar non-linear deformations as a live finger would [8, 13].

Another approach for liveness detection is to detect the sweat pores [13] using a fingerprint sensor with a very high resolution (up to 1000dpi). These fine details might be difficult to copy in artificial fingerprints. However, according to the work by Matsumoto et al., it showed that a coarse reproduction of intra-ridge pores is feasible with gelatin gummy fingerprints, even though it is difficult to reproduce the exact size and position of the pores on the mold [4].

Analysis of skin coarseness [28] is another approach for future second generation high resolution scanners. Standard deviation of the noise residue is used as an indicator to the texture coarseness. A fingertip image is first denoised using wavelet based approach. The noise residue (original image - denoised image) is then calculated. It showed the standard deviation of fake finger tips is much higher than the live finger tips. We tried the similar procedure of denoising the image using wavelet shrinkage and compared the standard deviation on our current used fingerprint scanners with resolution of 500 dpi. It did not show similar results as was shown in [28]. We use the results of testing on Capacitive DC scanner as an example. There is no difference using skin coarseness analysis between cadaver and live fingers and only a small difference between live and spoof fingers made of gelatin and Play-Doh, as shown in Figure 18. We think the reason of failure of this approach for our database is because of low resolution of scanners we used and the different properties of the spoof materials compared to the original published report.

FIG. 18 HERE

In our new method, the images used are the first image immediately upon placement on the fingerprint scanner. Because this method is based on detection of noise along the valleys, wiping the clothes before scanning and placing the finger with normal pressure is a necessary way to demonstrate a live pattern. In addition, to obtain a good quality fingerprint image with clear ridge-valley pattern, the scanner surface should be kept clean continuously. Oppositely, it is more difficult to defeat this method using the fake fingers because they will most likely display noise patterns when placing on the scanner due to the material's properties. It is necessary then that live fingerprint images are clean in order to prevent false rejections. This formulates a trade-off between usability (requiring clean fingerprint images) versus security (incorporating liveness). More research is needed to explore this relationship and its limits. It is important to note in ours (and others) collection there were no special cleaning procedures required besides wiping finger on clothes in a normal office environment.

Compared to the previous method using wavelet ridge analysis [18], which was tested using the same dataset as here, this method has improved performance. For example, the ridge results were 80% (live) and 92% (non-live) correct for Secugen scanner compared to 100% (live) and 91% (non-live) correct for this new approach using valley noise analysis. The two approaches are quite distinct. The ridge wavelet approach looks for pattern of increased variability along the ridges seen only in live fingers, while the valley wavelet approach considers pattern of increased variability in the valley of spoof fingers. The variability of noise for spoof is quite distinct in valley compared to the signature of a spoof along ridges.

Another issue of this method is that it is device-dependent because the fingerprint images vary across different technologies. Different features and classification approaches will be needed for different scanners when applying this method. Spoof/live fingers interact differently across devices. Furthermore, our methods show variability in performance across technologies. This may be due to the variability of quality of fingerprint images from different scanners. Little research has looked at this question [32]. For example, in our observation, Ethentica scanner shows more noise for all images, especially spoof images. Therefore, this enhances the ability to detect liveness. More variability in quality of live fingers needs to be studied.

Further research for this work is to investigate this method on a larger dataset. Our plan is to collect more live subjects with different skin conditions and quality to detect the efficiency of this method. Also we plan to collect more spoof data using gelatin, Play-Doh and silicone rubber materials to see if we can use these materials to make clean, life-like finger images without noise. For example, we will explore different moistness levels of the spoof fingers because wetness is a primary source of noise. Second, to improve this method, more analysis of effective features on the multiresolution scales is needed to optimize this method and improve its efficiency. Thirdly, we can combine this method with the previous perspiration pattern detection methods at the feature or decision level, for example, multi-modal fusion to improve the liveness classification confidence.

7. CONCLUSION

A new method which is based on the noise analysis along the fingerprint valleys is proposed to detect liveness for fingerprint sensors. Results show that it is very efficient (90.9% ~100%) for the capacitive DC, optical and electro-optical scanners to detect

vitality using a single fingerprint based on the noise pattern specific to the fake fingers. The method is purely software based and application of this liveness detection method can protect fingerprint scanners from spoofing attacks.

ACKNOWLEDGMENT

This work is funded by NSF ITR grant #0325333 and Center for Identification Technology Research (CITeR) at West Virginia University. We also thank Dr. G.L. Marcialis and Dr. F. Roli from University of Cagliari in Italy for providing their liveness test database.

REFERENCES

[1] A. Jain, R. Bolle, S. Pankanti, Biometrics: Personal Identification in Networked Society, Springer, 1999.

[2] N.K. Ratha, Enhancing security and privacy in biometric-based authentication systems, IBM Systems Journal, vol. 40, no.3, pp.614-634, 2001.

[3] S.A.C. Schuckers, Spoofing and anti-spoofing measures, Information Security Technical Report, Vol. 7, No. 4, pages 56 – 62, 2002.

[4] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, Impact of artificial 'gummy' fingers on fingerprint systems, Proceedings of SPIE, vol. 4677, Jan. 2002.

[5] T. Matsumoto, Gummy Finger and Paper Iris: An Update, Workshop on Information Security Research, Fukuoka, Japan, Oct. 2004.

[6] H. Kang, B. Lee, H. Kim, D. Shin, J. Kim, A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules, KES 2003, pp. 1245-1253, 2003.

[7] Liveness Detection in Biometric Systems, International biometric group white paper, available at http://www.ibgweb.com/reports/public/reports/liveness.html

[8] M. Sandstrom, Liveness Detection in Fingerprint Recognition Systems, Master thesis, http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf

[9] D. Osten, H. M. Carim, M. R. Arneson, B. L. Blan, "Biometric, personal authentication system", Minnesota Mining and Manufacturing Company, U.S. Patent #5,719,950, February 17, 1998.

[10] K. Seifried, "Biometrics - What You Need to Know," Security Portal, 10 January 2001.

[11] P. D. Lapsley, J. A. Less, D. F. Pare, Jr., N. Hoffman, "Anti-fraud biometric sensor that accurately detects blood flow", SmartTouch, LLC, U.S. Patent #5,737,439, April 7, 1998.

[12] P. Kallo, I. Kiss, A. Podmaniczky, and J. Talosi, "Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus", Dermo Corporation, Ltd. U.S. Patent #6,175,64, January 16,2001.

[13] D.Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, Nu, USA, 2003.

[14] R. Derakhshani, S. A. C. Schuckers, L. Hornak, and L. O'Gorman, Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition Journal, Vol. 36, No.2, 2003.

[15] Schuckers SAC, Abhyankar A, A Wavelet Based Approach to Detecting liveness in Fingerprint Scanners, Proceedings of Biometric Authentication Workshop, ECCV, Prague, May, 2004.

[16] Parthasaradhi S, Derakhshani R, Hornak L, Schuckers SAC, Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 35, pp. 335- 343, 2005.

[17] B. Tan, S. Schuckers, Liveness detection using an intensity based approach in fingerprint scanner, Proceedings of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21 2005

[18] B. Tan, S. Schuckers, Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing, IEEE 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), 2006.

[19] L. Hong, Y. Wang and A. Jain: Fingerprint image enhancement: Algorithm and Performance Evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 8, pp.777–789,Aug. 1998.

[20] M. Kawagoe and A. Too. Fingerprint pattern classification. Patern Recognition, 17(3):295-303, 1984.

[21] M. B. Ruskai et. al., Wavelets and Digital Signal Processing in Wavelets and Their Applications (pp. 105-121), 1992.

[22] I. Daubechies, Orthonormal bases of compactly supported wavelet, Comm. Pure Appl. Math., 41(1988), pp. 909-996.

[23] Ten lectures on Wavelets, No. 61 in CBMS-NSF Series in Applied Mathematics, SIAM, Philadelphia, 1992.

[24] A. Saha, Classification Tree in Excel, Available at http://www.geocities.com/adotsaha/CTree/CtreeinExcel.html

[25] Y. Chen, A. Jain, and S. Dass, Fingerprint Deformation for Spoof Detection, Proc. Of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21 2005

[26] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis", IEEE Transactions on Information Forensics and Security, vol.1, no.3, pp.360-373, September 2006.

[27] D. Baldisserra, A. Franco, D. Maio and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis", in proceedings International Conference on Biometric Authentication (ICBA06), Hong Kong, January 2006.

[28] Y.S. Moon, J.S. Chen, K.C. Chan, K. So and K.C. Woo, Wavelet based fingerprint liveness detection, Electronic Letters, Vol. 41, Issue: 20, pp. 1112-1113, 2005.

[29] Schuckers, SAC, Abhyankar A., A Wavelet Based Approach to Detecting Liveness in Fingerpritn Scanners, Proc. Of Biometric Authentication Workshop, ECCV, Prague, May. 2004.

[30] I. H. Witten and E. Frank, Data Mining: Parctical machine learning tools and techniques, 2nd Edition, Morgan Kaufmann, San Francisco, 2005.

[31] K. A. Nixon, R. K. Rowe, Spoof detection using multispectral fingerprint imaging without enrollment, Proceedings of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21, 2005

[32] R. Cappelli, M. Ferrara, and D. Maltoni. The quality of fingerprint scanners and its impact on the accuracy of fingerprint recognition algorithms. Proc. Multimedia Content Representation, Classification and Security (MRCS) 2006.

Fig. 1. Example of live and non-live fingerprints captured by Capacitive DC scanner: (a) live finger; (b) spoof finger made from Play-Doh; (c) spoof finger made from gelatin; (d) cadaver finger

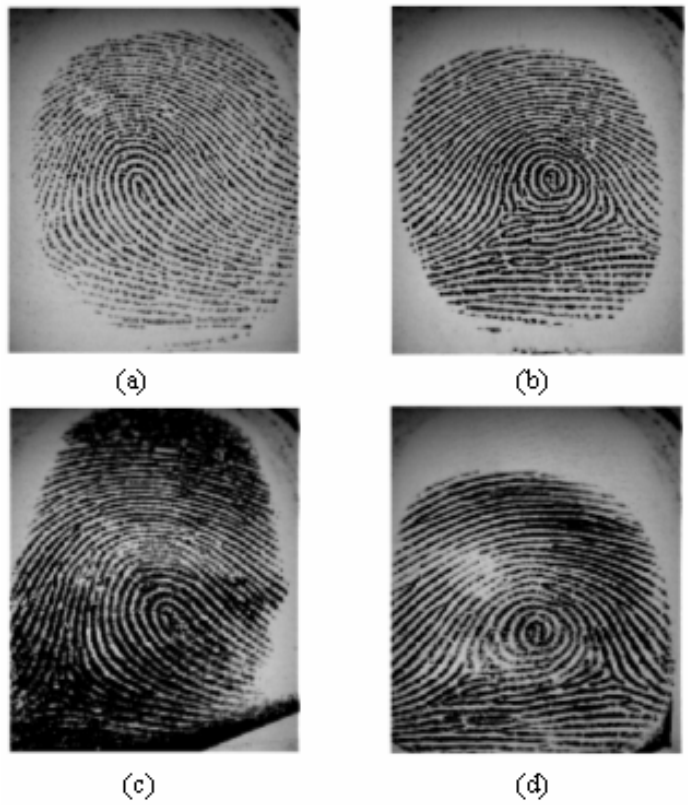


Fig. 2. Example of live and non-live fingerprints captured by optical scanner: (a) live finger 1; (b) live finger 2; (c) silicon finger 1; (d) silicon finger 2

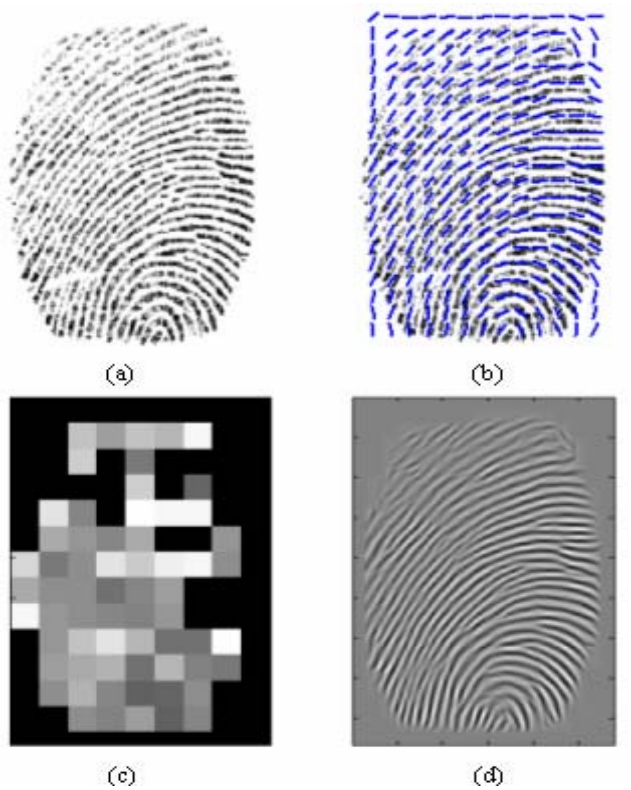
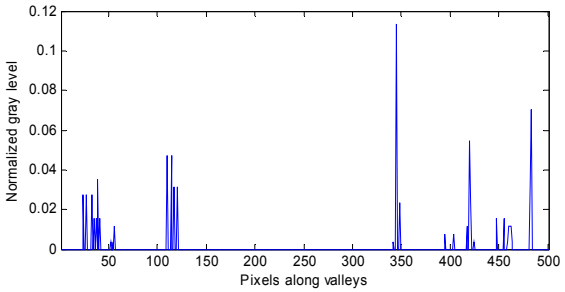


Fig.3. The process of fingerprint enhancement: (a) original image; (b) orientation estimation; (c) frequency estimation; (d) enhanced by Gabor filter

(a) (b)



(c)

Fig. 4. Ridge signal extraction: (a) binary image; (b) thinned valleys laid on the original image; (c) portion of enlarged valley signal

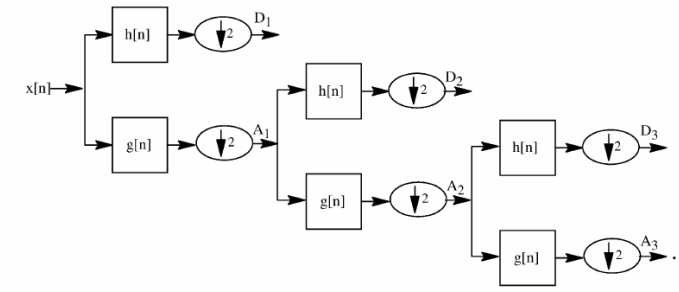
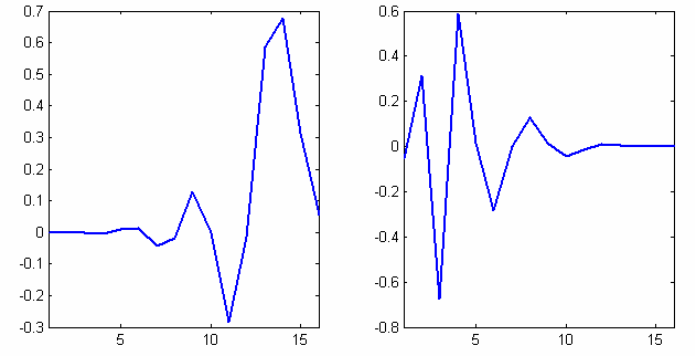
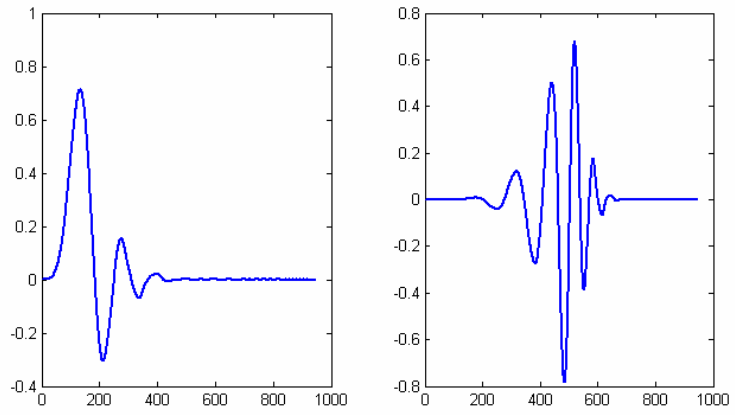


Fig. 5. The wavelet multiresolution decomposition



(a) **(b)**

Fig. 6. (a) Daubechies lowpass filter (b) highpass filter



(a) **(b)**

Fig. 7. (a) Daubechies scale function (b) wavelet function

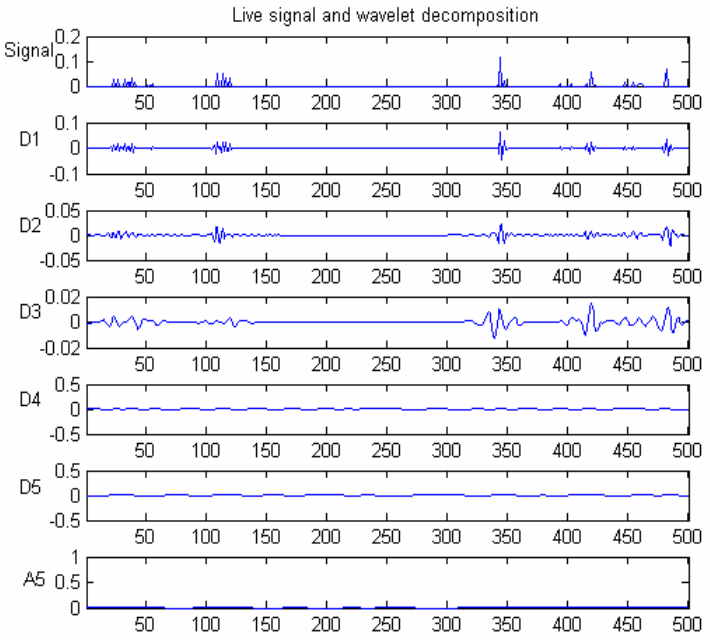


Fig. 8. Live signal and wavelet decomposition example

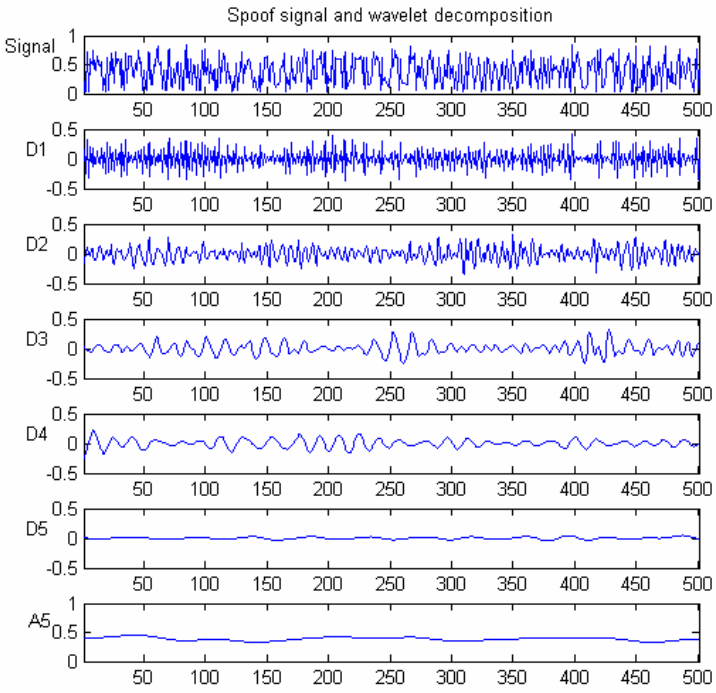


Fig. 9. Spoof signal and wavelet decomposition example

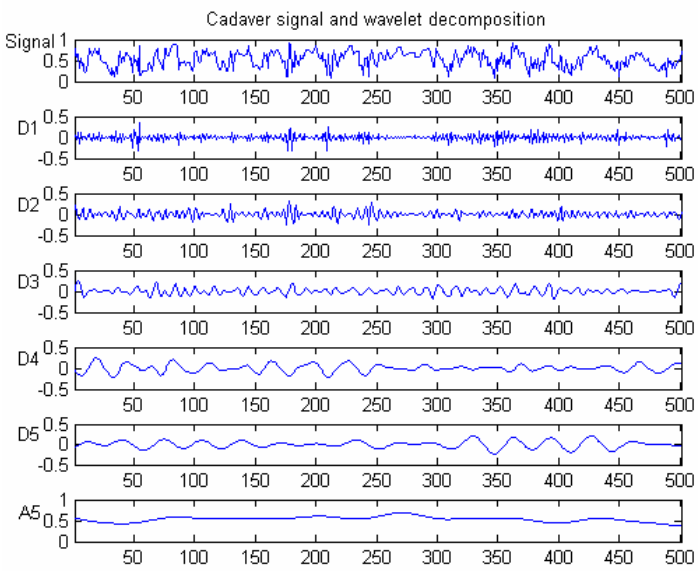


Fig. 10. Cadaver signal and wavelet decomposition example

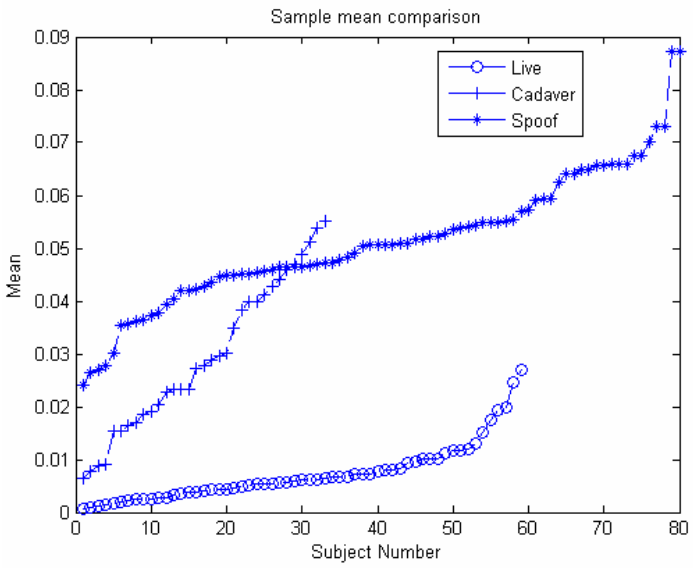


Fig. 11. D2 mean comparison in capacitive DC scanner

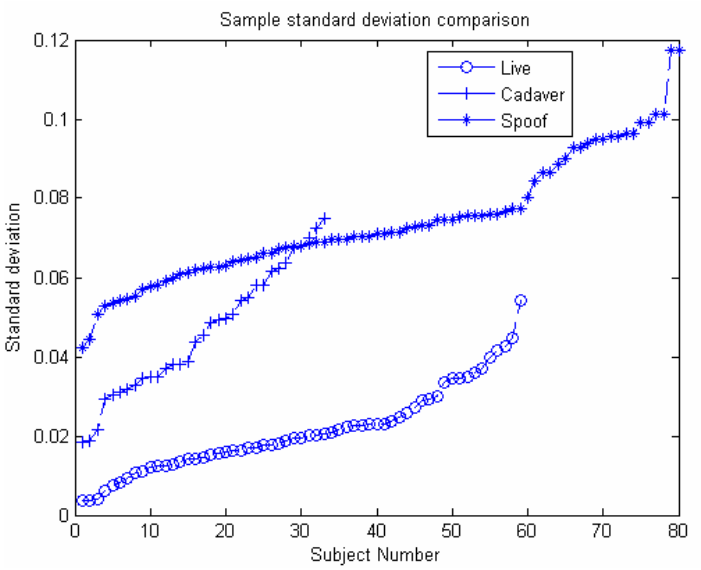


Fig. 12. D2 standard deviation comparison in capacitive DC scanner

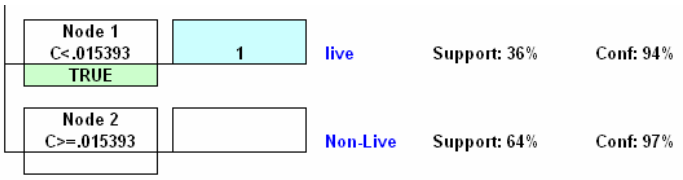


Fig. 13. Classification tree for capacitive DC

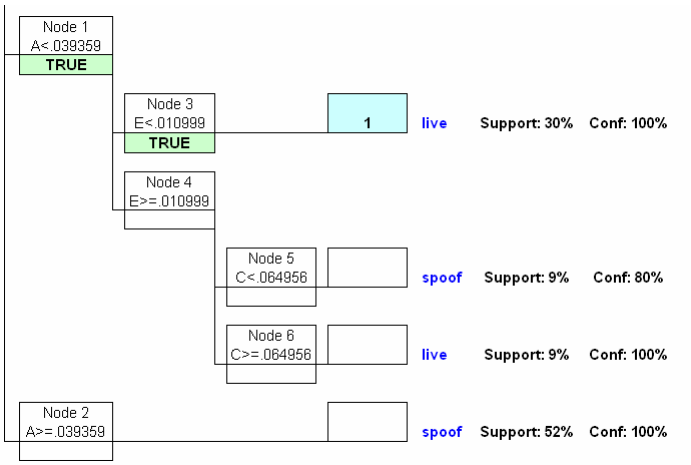


Fig. 14. Classification tree for optical1 scanner

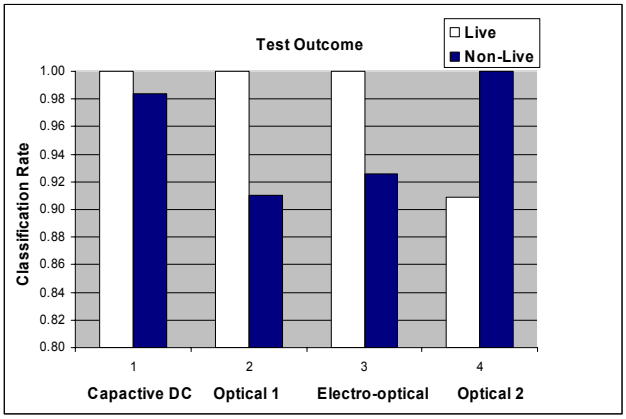


Fig. 15. Results on four different scanners using classification tree

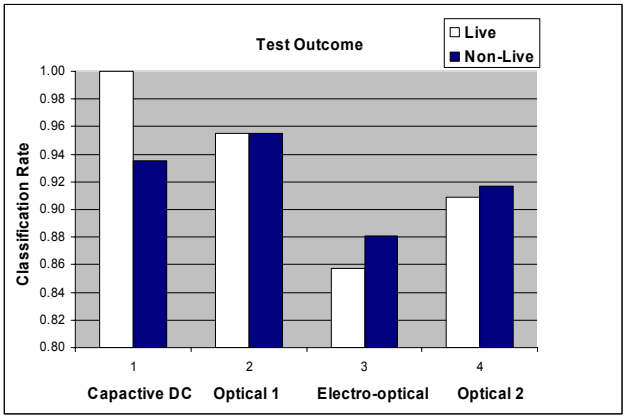


Fig. 16. Results on four different scanners using neural network

Fig. 17. Fail examples: (a) live fingers are classified as non-live fingers; (b) cadaver fingers are classified as live

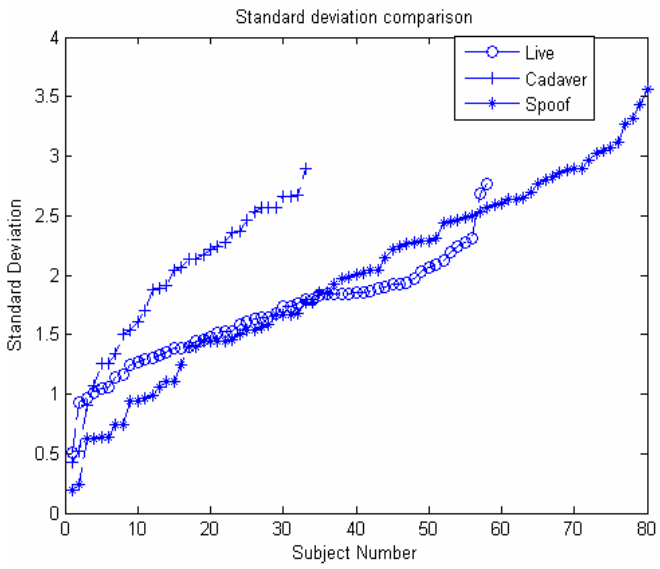


Fig. 18. Standard deviation comparison for Capacitive DC scanner (500dpi) using similar method as in [28].

Category	Precise	Secugen	Ethentica	Biometrika
Live	58	58	55	28
Spoof	80	80	80	28
Cadaver	33	25	22	

Table 1. Number of subjects used for each device and category