

# Spooing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise

Bozhao Tan, Stephanie Schuckers\*

*Department of Electrical and Computer Engineering*

*Clarkson University*

*8 Clarkson Ave. Potsdam, NY 13699 USA*

---

## Abstract

Biometric fingerprint scanners are positioned to provide improved security in a great span of applications from government to private. However, one highly publicized vulnerability is that it is possible to spoof a variety of fingerprint scanners using artificial fingers made from Play-Doh, gelatin and silicone molds. Therefore, it is necessary to offer protection for fingerprint systems against these threats. In this paper, an anti-spoofing detection method is proposed which is based on ridge signal and valley noise analysis, to quantify perspiration patterns along ridges in live subjects and noise patterns along valleys in spoofs. The signals representing gray level patterns along ridges and valleys are explored in spatial, frequency and wavelet domains. Based on these features, separation (live/spoof) is performed using standard pattern classification tools including classification trees and neural networks. We test this method on a larger dataset than previously considered which contains 644 live fingerprints (81 subjects with 2 fingers for an average of 4 sessions) and 570 spoof fingerprints (made from Play-Doh, gelatin and silicone molds in multiple sessions) collected from the Identix fingerprint scanner. Results show that the performance can reach 99.1% correct classification overall. The proposed anti-spoofing method is purely software based and integration of this method can provide protection for fingerprint scanners against gelatin, Play-Doh and silicone spoof fingers.

---

\*Phone: (1)315-2686536

\*\*Fax: (1)315-2687600

*Email addresses:* tanb@clarkson.edu, sschucke@clarkson.edu (Bozhao Tan, Stephanie Schuckers)

*Key words:* fingerprint scanner, anti-spoofing, fingerprint ridge and valley, decision tree, neural network.

---

## 1. Introduction

Fingerprints are graphical ridge-valley patterns on human fingers. Fingerprint recognition is considered as the most widely used and efficient technique for biometric authentication, which utilizes physiological or behavioral characteristics for personal identification or verification[1]. While fingerprint systems may have an excellent performance and improve security, fingerprint systems are found to be vulnerable to attacks at the sensor level, replay attacks on the data communication stream, and attacks on the database [2]. For example, previous studies have shown that it is not difficult to make molds of latent fingerprints left by legitimate users and to create fake fingers made from Play-Doh, gelatin and silicone materials to fool a variety of fingerprint scanners [3, 4, 5, 7]. From a security and accountability perspective, fingerprint recognition systems should have the ability to detect when fake finger samples are presented. Liveness detection (or vitality detection) is proposed to defeat this kind of spoof attack. Liveness detection is an anti-spoofing method ensuring that only the biometric from a live, authorized person is submitted for enrollment, verification and identification [6].

In order to prevent fraudulent attacks by artificial fingers, several solutions have been proposed. The first method uses extra hardware to acquire life signs. Previously developed approaches measure fingertip temperature, pulse, pulse oximetry, blood pressure, electric resistance, odor, or ECG [7, 8, 9, 10, 11, 12]. These methods require dedicated hardware integrated with the fingerprint system. This is expensive and in some cases bulky and inconvenient. For example, the electrocardiogram requires two points of contact on opposite sides of the body. 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. Also, translucent spoofs may fool pulse oximetry as it relies on infrared light absorption to measure oxygen content of the blood. One commercially available fingerprint sensor which may provide spoof detection is from Lumidigm [17]. 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. This method while commercially viable requires purchase of a specific scanner not applicable to standard readers.

The second method uses the information already captured by traditional fingerprint systems to detect life signs, for example, skin deformation, pores, power spectrum or perspiration pattern. Skin deformation techniques use the information regarding how the fingertip’s skin deforms when pressed against the scanner surface [13] [14] [15] [47] [49]. The studies showed that when a real finger moves on a scanner surface, it produces a significant amount of non-linear distortion. However, fake fingers are more rigid than skin and the deformation is lower even if they are made of highly elastic materials. One approach quantifies this by considering multiple frames of clockwise motion of the finger [15]. The problem of this method is that the users need to have special training or have to control pressure while rotating the fingers. Second, the performance of this method still needs to be improved with an equal error rate of 11.24% using 45 live subjects and 40 fake fingers. A second method considers the deformation in a single image compared to a template [14]. This study achieved 82% recognition for a small dataset (32 gummy fingers). More research is needed to assess the viability of this approach.

Analysis of skin coarseness [16] 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 a wavelet based approach. The noise residue (original image minus denoised image) is then calculated. Authors show that the standard deviation of fake finger tips is much higher than the live finger tips. This method still needs to be tested on other types of scanners and spoof materials. The method proposed here takes advantage of similar characteristics of the noise along valleys.

Image power spectrum is also selected as an effective feature for vitality detection [19]. The authors hypothesize that the difference between live and spoof images is mainly due to the stamp fabrication process which causes an alteration of frequency details between ridge and valleys. The proposed Fourier transform feature can quantify the difference in terms of high frequency information loss. This approach is tested for a single scanner and silicone spoof material with 97.3% recognition. The performance of this method still needs to be tested on other sensors and other spoof materials.

Also researchers investigate the characteristics of spoof and live fingers, like perspiration pattern [46], band-selected Fourier Spectrum [50], valley noise [25], gray-level profile and frequency patterns [48], integration of multiple static features [51], or curvelet texture difference [52].

Previously, our laboratory has demonstrated that pattern of perspiration

on fingerprint image can be used as a measure of liveness detection for fingerprint biometric systems. Unlike spoof and cadaver fingers, live fingers demonstrate a distinctive spatial moisture pattern when in physical contact with the capturing surface of the fingerprint scanner. The pattern in fingerprint images begins as 'patchy' areas of moisture around the pores spreading across the ridges over time. Image/signal processing and pattern recognition algorithms have been developed to quantify this phenomenon using wavelet and statistical approaches [20, 21, 22, 23].

A disadvantage of this method is that it requires two time-series images, which might be not convenient for users. In our previous research, 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 [24]. 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 extracted on each scale are used by neural network or classification trees to discriminate between live and non-live fingerprints. The capacitive DC (Precise) scanner demonstrates between 90-100% (for live and non-live, respectively) correct classification rate. The optical scanner (Secugen) shows 89-92% correct classification.

The motivation of this work is to further develop and improve performance of live/spoof separation using a single image. In this approach we extend the work of ridge signal [20, 24] and valley noise [25] by improving the features selected and fusing the information to improve performance. We test our new approach using a new larger dataset of live and spoof images than previously tested. For live fingerprints, the dataset contains multiple visits from the subjects (average 4 returns, range 1 to 13). The purpose is to capture the variability of a single subject. For spoof fingerprints, the dataset contains spoof fingers of varying materials (gelatin, silicone and Play-Doh) with varying levels of moisture (captured over time as the spoof dries). We utilize the term anti-spoofing as our method considers both the characteristics of the live fingers (liveness) and characteristics of the spoof.

The organization of the paper is as follows: Section II describes the database collected for this study. Section III introduces a new approach to detect liveness by fusing ridge signal and valley noise analysis. Section IV gives the experiment results of the new method on the new dataset, which is also compared with ridge signal and valley noise analysis alone. Section V

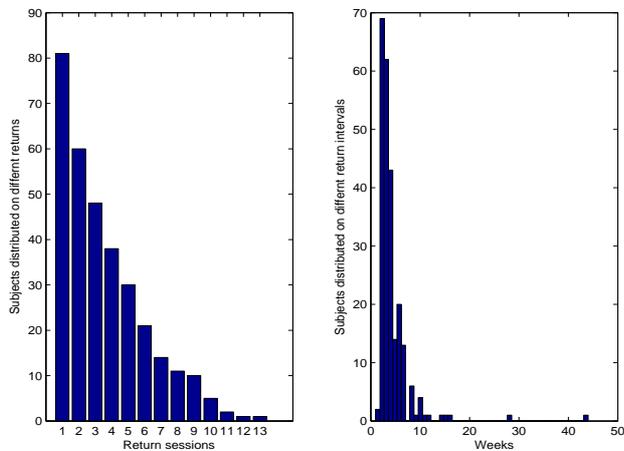


Figure 1: Histogram of number of return live subjects (left) and weeks between visits (right)

discusses the advantages and limitations of the new method and future work. Finally, Section VI gives a conclusion of this work.

## 2. Data Collection

Identix DFR2100 fingerprint scanner, used to collect data for this research is an optical scanner with a resolution of 686 dpi and size of 720x720 (forensic mode). The manufacturer provided a software developer kit (SDK). The software was modified to collect a time series of sensor raw images. Three time-series images (at 0, 1 and 2 seconds) are used for this study. To test our algorithm, cross validation was applied on 0, 1 and 2 second images separately. In addition, all of the time-series images were mixed and tested together also using cross validation. Each liveness decision was based on a single fingerprint image. For comparison, we also implemented the previous ridge signal algorithms [20, 24]. For ridge signal algorithm [20], we only selected the static feature from the first image. Protocols for data collection from the subjects were approved by Clarkson University Institutional Review Board (IRB).

Fingerprint images were collected from live, Play-Doh, gelatin and silicone fingers. The live fingerprints were collected from 81 subjects, representing a wide range of ages (18-50 years), ethnicities (Caucasian, Black, Asian), and both sexes. Live subjects usually returned voluntarily at intervals of at least

two weeks. The average return interval was 4.2 weeks and the standard deviation was 3.8. The maximum return interval was 44 weeks. Some subjects came back more often (13 times) than others (1 time only), resulting in a total of 322 visits across 81 subjects. The purpose is to capture the variability of a single subject. In our live data collection, it has the subjects with all kinds of variabilities, like wet finger, dry finger, dirty finger, pressure change, etc.

Fig. 1 summarizes the distribution of live subjects of a number of returns and interval of return. Each time the subject’s right thumb (R1) and right index (R2) fingerprints are collected. Table 1 summarizes the number of subjects and total fingerprints collected using Identix scanner.

Categories	Live	Play-Doh	Gelatin	Silicone
Subjects	81	38	38	38
Sessions	1-13	5	5	5
Total	644	190	190	190

Table 1: Summary of live and spoof fingers collection

To generate spoof fingerprint images, artificial finger molds made from Play-Doh, gelatin and silicone were created from 38 casts made from dental impression materials. We have chosen to make casts from cooperative users. When we prepared spoofs, we always tried to make the highest quality spoofs to mimic live fingerprints, which look like live fingerprints. We collected spoofs with different moisture levels to mimic wet and dry fingerprints.

The apparatus required to make the cast is as follows: Acquasil easy mix putty smart wetting impression material of type 0 from Dentsply Caulk, Extrude polyvinylsiloxane impression material of type 2, mixing tips large teal, and extruder gun from Kerr corporation, and film-can. First, the subject mixes type 0 base and catalyst evenly and puts the mix in a film-can to make outer supportive shell. Then, the subject pushes finger in paste and hold it that position for 2-3 minutes until the mix gets hardened. This creates a base imprint for the finger cast. Next, the subject takes the finger out of the paste and fills the mold with the type 2 extrude using extruder gun. Then the subject puts back finger back onto the molding, in a similar manner as

previously done and holds the finger in a still position for 3 minutes until it becomes hardened. The cast is ready when the subject removes the finger.

To make gelatin finger molds, gelatin (Knox Gelatine) was mixed with water and heated in the microwave until the solution was thick enough to pour into the casts. Silicone finger molds are made by Sylgard 184 Silicone Elastomer Kit, manufactured by DOW Corning Corporation [27]. The kit includes two items: silicone elastomer base and curing agent which are mixed at the ratio of 10:1. Play-Doh finger molds were created by simply press Play-Doh into the cast. After pouring into finger casts, we wait at least 3 hours for gelatin solutions and at least 12 hours for silicone solutions to harden before beginning collection on the fingerprint sensor. Silicone spoof fingerprints were collected after 12 hours for 5 sessions with 1 hour intervals. Gelatin spoof fingerprints were collected after 3 hours for 5 sessions with 1-hour intervals. Play-Doh spoof fingerprints were collected for 5 sessions with 20-minute intervals. The purpose of the time between samples is to achieve a dataset of spoofs with a variable amount of moisture. In addition, to make the highest quality spoofs, Play-Doh fingers were placed in the air for 5 minutes, as fresh Play-Doh fingerprints displayed a very wet pattern, they are very easy to detect, and thus considered as spoof. The gelatin fingers were placed at air for about 3 hours to make sure they did not show a smudged pattern on the scanner. To make the highest quality of silicone fingers, we tried different ratio to mix the materials in the kit. Higher ratio silicone fingers are so sticky that they the scanner dirty and display a noise pattern on the scanner, while lower ratio silicone fingers are too stiff. We selected an optimal ratio to make a flexible silicone finger and get the best image quality.

Fingerprint image quality is a valuable tool in determining a fingerprint matcher’s ability to match a fingerprint against other fingerprints [28]. It has been shown that as fingerprint image quality degrades so does matcher performance. To investigate the image quality of our database, NFIQ [28], an implementation of the NIST Fingerprint Image Quality algorithm, was used as a standard measure to evaluate the fingerprint quality distribution for both live and spoof images. It computes a feature vector using the quality image map and minutiae quality statistics produced by the MINDTCT minutiae detection algorithm [28]. The feature vector is then used as input to a Multi-Layer Perceptron (MLP) neural network classifier, and the output activation level of the neural network is used to determine the fingerprint’s image quality value. There are five quality levels with 1 being the highest quality and 5

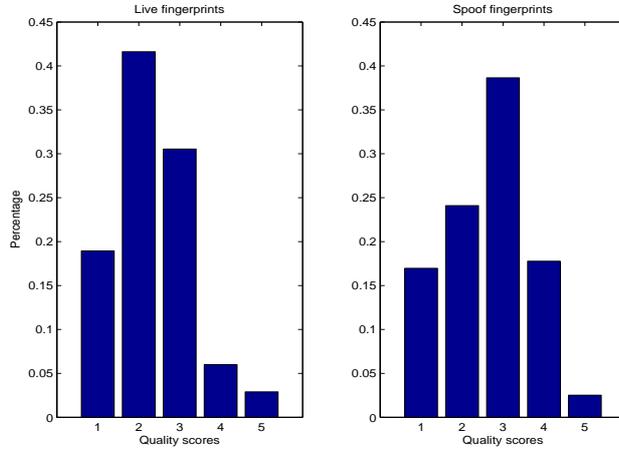


Figure 2: NFIQ quality score distribution of live fingerprints (left) and spoof fingerprints (right)

being the lowest quality. Fig. 2 is a comparison of image quality histogram distribution for both live and spoof fingerprints. X-axis is the NFIQ quality scores from high to low. Y-axis is the percentage distribution for different quality scores. As can be seen, most live and spoof fingerprints have a quality score of 4 or better, which is similar to the quality distribution of FVC2004 fingerprint database [29]. The NFIQ scores of spoof fingerprints are slightly lower than live ones, which is not unexpected due to the difficulty of creating spoofs. However, over 79.7% of spoof images are of quality 3 or better. In addition, it should be noted that not all live images were of the highest quality, reflecting variable conditions (wet, dry, high pressure, etc.).

### 3. Ridge signal and valley noise analysis

Fig. 3 shows two typical examples of images captured from live, Play-Doh, gelatin and silicone fingers using Identix DFR2100 scanner. The fingerprint pattern is comprised of ridges touching the sensor plane and valleys not touching the sensor plane. For normal live fingers, it is very easy to get a clear ridge-valley structure when touching the sensor plane with normal pressure. As can be observed, the live and spoof fingerprints look different considering both ridges and valleys. Reasons include the perspiration pattern of live fingers and differences in the properties of the spoof materials compared to human skin.



Figure 3: Example of live and non-live fingerprints captured by Identix DFR2100 scanner: (a) live fingerprint; (b) Play-Doh spoof sample; (c) Gelatin spoof sample; (d) Silicone spoof sample.

First, live fingers have sweat, but spoof fingers do not. On the surface of human skin, there are about 600 sweat glands per square inch and the sweat (a dilute sodium chloride solution) diffuses from the sweat glands through small pores [26]. Skin pores do not disappear, move, or spontaneously change over time. Sweat has a very high dielectric constant and electrical conductivity compared to lipid-soluble substances absorbed by the outmost layer of the skin. The perspiration starts from the pores, either completely covering them or leaving the pore as a dry dot. Due to this reason, the live fingerprint looks "patchy" compared with spoof subjects. From the ridge perspective, the gray level along ridges in live fingers has distinctive characteristics due to the presence of perspiration and pores, compared to spoof fingers.

Second, the properties of spoof materials are different than human skin. The intensity along the ridges is very uniform for spoof images because the impostor must apply pressure to the spoof for a proper image. While it is difficult to reproduce the variability along the ridges seen in live images even with reduced pressure, spoofs as they dry may produce this variability where the drying is not uniform over the spoof. We attempt to create this with our dataset. Also there are many granules in the valleys due to the properties of the spoof materials, which result in more noise along the valleys in fingerprint images.

Based on these investigations, we apply image processing techniques to quantify moisture patterns along ridges and noise along valleys to discriminate between live and spoof fingers. The underlying process is to create separate ridge and valley masks, single pixel lines tracking the ridge and valley. From this mask, ridge and valley signals are gray level values along the ridge and valley masks. Wavelet transform and Fourier transform are used to analyze ridge and valley signal in wavelet and frequency domain, respectively. Spatial, frequency and wavelet features are extracted to quantify perspiration and noise difference in order to discriminate between live and spoof fingerprints. Based on these features, standard pattern classifiers are used to make the final decision whether to accept or reject the input fingers.

The basic steps are listed as follows:

- *Ridge, valley mask and signal extraction*
- *Feature extraction*
- *Classification*

### 3.1. Ridge, valley mask and signal extraction

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 [30, 31]. Here, a software module from Veridicom SDK was used to segment the fingerprint and get the binary ridge-valley image, as seen in Fig. 4-b.

A standard thinning algorithm using morphological operations was used to obtain one pixel thin ridges. Y-junctions and some short curves shorter than a typical pore-to-pore distance are discarded using a simple non-overlapping neighbor operation. Individual strings are connected to form a signal, which represents the gray levels of contours passing through middle of the ridges. Similar methods are used to extract the valley signal corresponding to the actual gray level changes along the valleys. Fig. 4(b) shows the binary ridge-valley fingerprint image, Fig. 4(c) and 4(d) show the extracted ridge and valley masks appear superimposed on original fingerprint. Fig. 5 shows ridge and valley signal samples from partial signals extracted from a typical live and spoof fingerprints, respectively. The ridge signal from live fingerprints appears more periodic than spoof and the signal intensity is different, as can be seen from Fig. 5(a). From Fig. 5(b), we can see that the valley signal from live fingerprints appears more stable than spoof fingerprints due to the existence of more noise along the spoof valleys.

### 3.2. Feature extraction

After extracting ridge and valley signals, features are extracted to quantify the difference between live and spoof fingerprints in spatial, frequency and wavelet domain, respectively.

#### 3.2.1. Spatial domain features

Mean and standard deviation of ridge and valley signals are extracted spatially. For the ridge signal representing gray level intensities along ridge mask, gelatin and silicone fingerprints usually have a higher value of mean because they look darker than live fingerprints. However, the mean value of live and Play-Doh fingerprints are usually similar. Because the spoof materials also have artificial pores or other artifacts, the standard deviation does not have a big difference between live and non-live fingerprints. For the valley signal representing gray level intensities along valley mask, usually

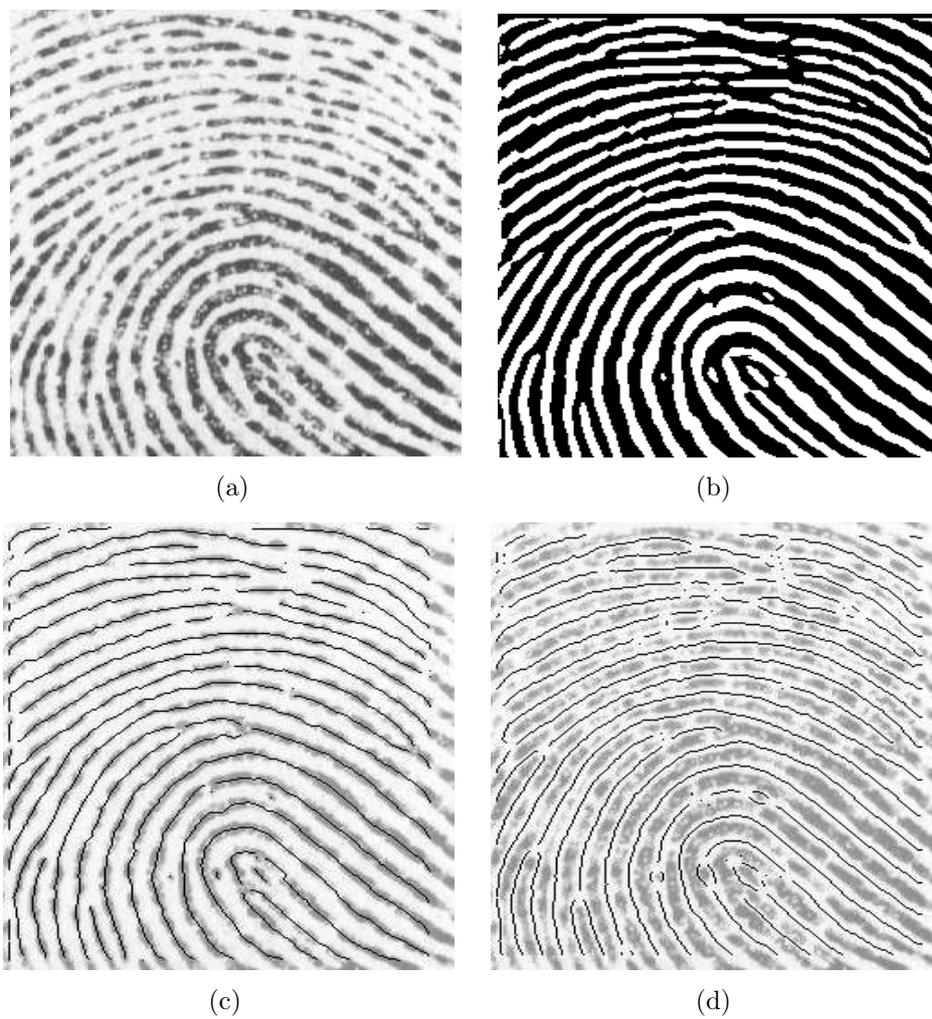
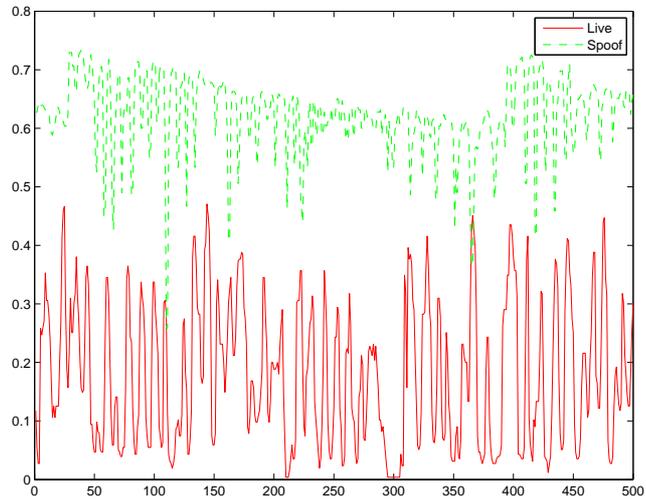
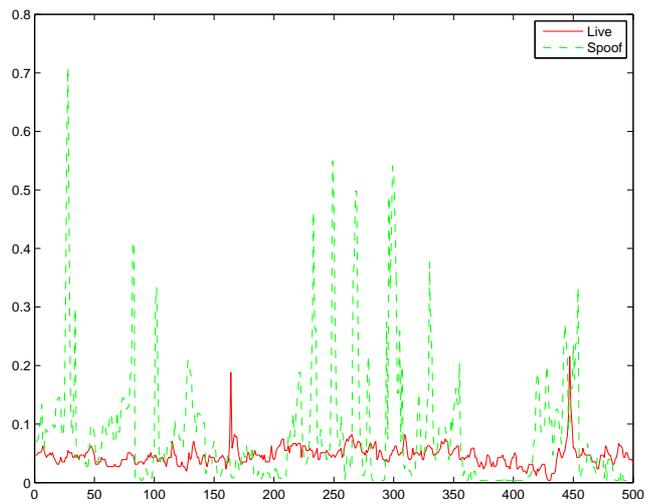


Figure 4: Fingerprint ridge-valley mask generation and signal extraction: (a) Original fingerprint image; (b) Binary ridge-valley image; (c) Thinned ridges overlaid on fingerprint image; (d) Thinned valleys overlaid on fingerprint image.



(a)



(b)

Figure 5: Examples showing ridge signal and valley signal difference between live (solid line) and spoof (dotted line) fingerprints: (a) Ridge signal; (b) Valley signal.

the mean and standard deviation of spoof fingerprints are higher than live fingerprints because the spoof fingerprints have much more noises.

### 3.2.2. Frequency domain feature

The ridge signal is also analyzed in the frequency domain. For the ridge signal, the peaks denote the moist locations and the valleys denote the dryer regions usually between two pores. For live fingerprints, the peak to peak distance is typically periodical corresponding a pore to pore distance. The variations in the spoof ridge signal do not have a specific periodicity because they do not have evenly spaced pores. The frequency feature is the average Fourier transform of the signal segments where the energy related to typical pore spacing is used. Before Fourier transform, the mean of the signal is removed to eliminate the spike around zero frequency. A 256-point FFT is performed. The procedure can be mathematically calculated as

$$FE = \sum_{k=256/pl}^{2*256/pl} \frac{\sum_{i=1}^n \left| \sum_{p=1}^{256} R_i(p) e^{-j2\pi(k-1)(p-1)/256} \right|}{n}; \quad (1)$$

where  $pl$  is the spatial period (around 25 pixels using this scanner under its highest resolution condition), and  $R_i$  is ridge signal after DC removal.

### 3.2.3. Wavelet domain features

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 [32]. An orthogonal filter bank is applied to compute the discrete-time wavelet transform when iterated on the lower band. For wavelet multiresolution decomposition, 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:

$$\phi(n) = 2 \sum_n h_n \phi(2x - n) \quad (2)$$

$$\psi(n) = 2 \sum_n g_n \phi(2x - n) \quad (3)$$

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

$$h[L - 1 - n] = (-1)^n g[n] \quad (4)$$

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. Daubechies wavelet is selected as the mother wavelet [33] and the scale selected is 5 because further decomposition detail does not contain much useful frequency content.

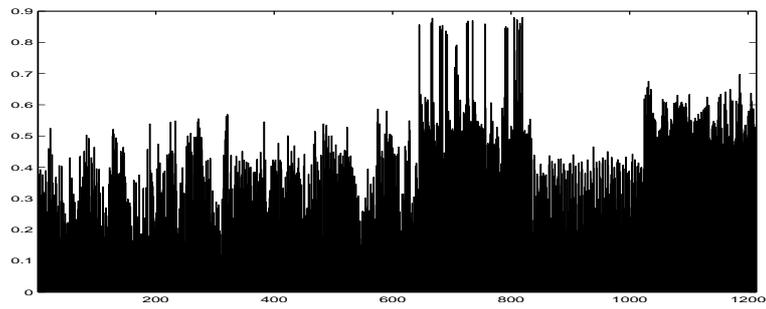
To extract the feature vectors, mean and standard deviation of the wavelet coefficients in each scale are used. For ridge signal, 6 features (mean only) are extracted from 5 detail scales and the last approximation scale because variance on each scale does not have demonstrated a large difference between live and spoof ridge signals. For valley signal, 12 features (mean and standard deviation) are extracted from 5 detail scales and the last approximation scale. There are a total of 19 features in the spatial, frequency and wavelet domain.

Fig. 6 shows the comparison of four features between live, Play-Doh, gelatin and silicone fingerprints over the whole dataset. On the X axis, subjects 1-644 represent live fingers, subjects 645-834 represent Play-Doh fingers, subjects 835-1024 represent gelatin fingers and subjects 1025-1214 represent silicone fingers.

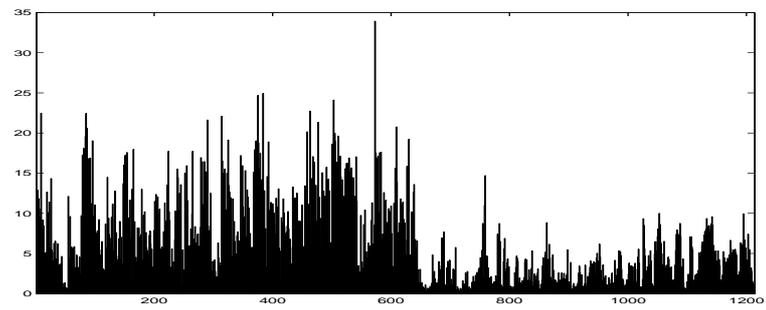
As can be observed from Fig. 6-a, gelatin and silicone fingerprints generally have a higher intensity along the ridges than live fingerprints. Live fingerprints have a higher Fourier energy than the three types of spoof fingerprints due to the presence of perspiration points and pores along the ridges, as shown in Fig. 6-b. Also, along the valleys, spoof fingerprints have a higher intensity and higher variation than live fingers because of the existence of noise, as shown in Fig. 6-c and Fig. 6-d. From the feature comparison, we utilize these features for decision logic to make the liveness classification.

#### 3.2.4. System fusion

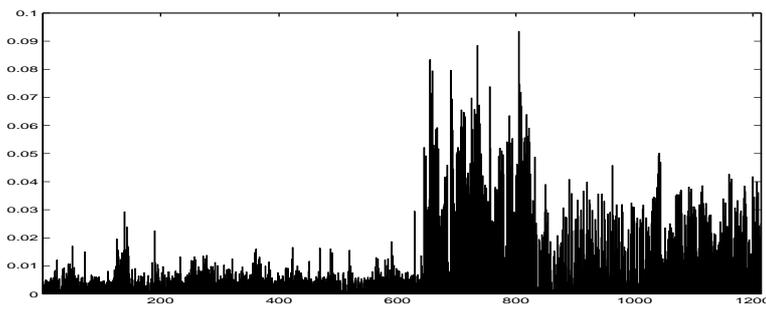
Each of our proposed ridge signal and valley noise approaches can be used individually or together via system fusion. It is worthwhile to carry out the comprehensive feasibility study of these different strategies since each has different complexity and may behave differently under different real application scenarios for the fingerprints with varying quality. Through this



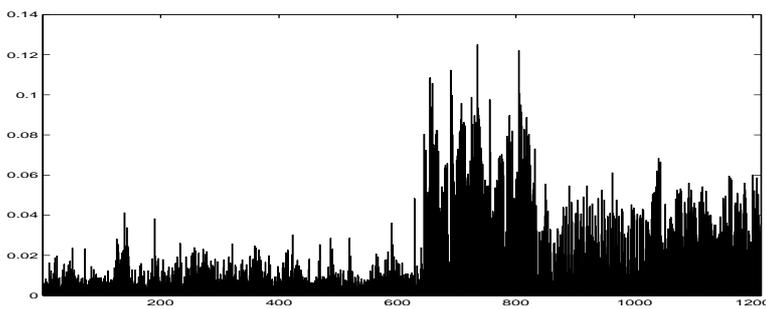
(a) Mean of ridge signal



(b) Fourier energy of ridge signal



(c) Mean of valley signal on wavelet detail scale 3



(d) Standard deviation of valley signal on wavelet detail scale 3

Figure 6: Feature comparison between live and spoof fingerprints; For subjects on X axis: live subjects are 1-644; Play-Doh: 645-834; ~~pl~~atin: 835-1024; silicone: 1025-1214

study we will gain expertise in liveness detection or anti-spoofing protection for fingerprint scanner, which will allow us to suggest the best solution for different real-world downstream applications and scenarios. We can either do the system fusion at feature level, match score or decision level [45]. In this case, we focus on feature level fusion. For feature level fusion, we combine the features extracted from each approach, into a unique feature vector, because the features extracted from each approach are independent between them.

### 3.3. Classification

After statistical features are extracted, standard pattern classification tools (neural network, nearest neighbour, classification tree, etc.) are used to separate non-live subjects from the live subjects. The non-live category includes the spoof data made from Play-Doh, gelatin and silicone fingers. The software we used for classification is from WEKA (Waikato Environment for Knowledge Analysis) software tool [34] that provides different classification techniques for large data sets.

For neural network we chose a multilayer perceptrons (MLPs) with supervised feedforward neural networks trained with the standard back-propagation algorithm. In this case, a two-layer feed-forward network is created where the inputs are the extracted statistical features. The first hidden layer has 3 tan-sig 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.

Nearest Neighbour classifier [35] is another supervised statistical pattern recognition method. Training was performed with both positive and negative cases. A new sample is classified by calculating the normalized Euclidean distance to the nearest training case.

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. Several learning and searching strategies are utilized to train the models, including ADTree [36], J48 [37], Random Forests [38], and Bagging Tree [39]. For example, Random Forests, a meta-learner comprised of many individual trees, was designed to operate quickly over large datasets and more importantly to be diverse by using random samples to build each tree in the forest. The randomly selected training data is sampled to create an in-bag portion to construct the tree, and a smaller out-of-bag portion

to test the completed tree to evaluate its performance. This performance measure is known as the out-of-bag error estimate.

Last, support vector machines (SVM) are also used to make comparisons. John Platt’s sequential minimal optimization algorithm [40] is utilized for training a support vector classifier.

Ten-fold cross-validation test is used to test the proposed approach. The original dataset is partitioned almost evenly into 10 subsamples sets. Of the 10 subsamples, a single subsample set is retained as the validation data for testing the model, and the remaining 9 subsamples are used as training data. The cross-validation process is then repeated ten times. Results from 10 folds then can be averaged to produce a single estimation.

## 4. Experiments and Results

### 4.1. Performance Evaluation

To evaluate our system, we utilize terms for evaluating biometric identification or verification systems. Liveness classification is the process of determining whether the input finger is live or spoof.

Because of the threshold selection or decision logic, liveness classification makes two type of errors, i.e., *spoof false acceptance* (SFA), where a spoof finger is accepted as live and *live false rejection* (LFR), where a live finger is rejected. Two other terms are also often used, *true acceptance*, where a live finger is recognized as live and *true rejection*, where a spoof finger is recognized as spoof. Normalized SFA and LFR are used, which are called spoof false acceptance ratio (SFAR) and live false rejection ratio (LFRR), respectively. They can be calculated as

$$SFAR = \frac{SFA}{NS} \quad (5)$$

$$LFRR = \frac{LFR}{NL} \quad (6)$$

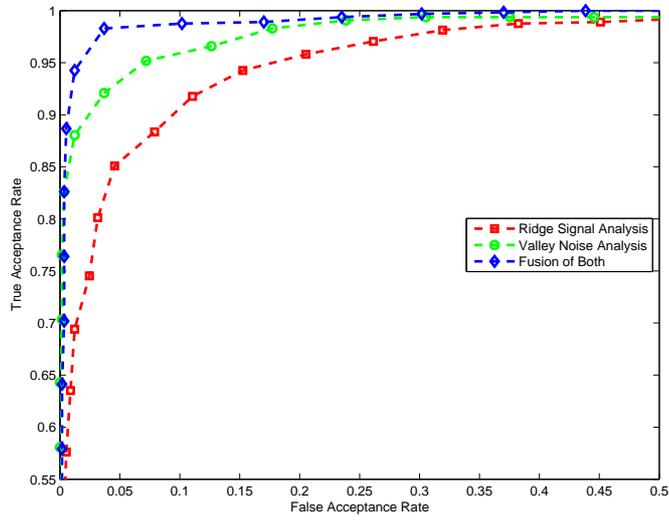
where SFA and LFR are the number of SFA and LFR samples, respectively; and NS and NL are the total number of spoof finger samples and live finger samples, respectively. Equal error rate (EER) is when SFAR equals LFRR. A lower EER value indicates a high accuracy of this system. To evaluate the performance of our system, we use Receiver Operator Characteristic (ROC) curve, which plots the change of true positive rate (1-LFRR) with SFAR for varying thresholds.

## 4.2. Results

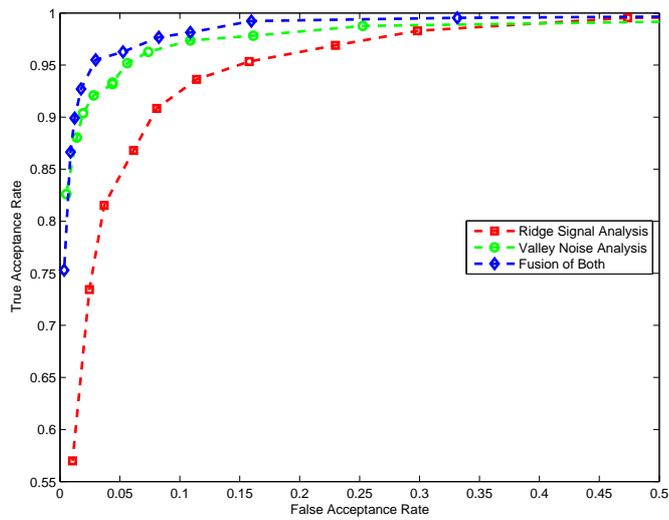
Performance of live/spoof separation is detected considering ridge signal features and valley noise features separately, and integration of both at feature level. In our approaches, both ridge signal algorithm and valley noise algorithms use wavelet decomposition to extract features. These features are inputs to classifiers: neural network and random forest tree. We compared the ROC for both ridge signal and valley noise algorithms. Fig. 7 shows the ROC curve for ridge signal analysis, valley noise analysis and integration of both methods using neural network and random forest classification tree for 0 second images, respectively. Different classifiers have different ROC curves, using NN, random tree, Bayes net or SVM, etc. Here we used the two best classifiers using NN and random forest tree. The performances are very close, that's why the ROC curves using these two methods are similar. But after fusion, the ROC from NN looks better than random forest tree.

Fig. 8 shows the comparison of EER values among all three methods for 0 second images. The best classifier for ridge signal method is random forest tree, with a EER of 8.62%. The best classifier for valley noise method is multilayer perceptron network, with a EER of 5.27%. The best classifier when fusing both of these two approaches is multilayer perceptron network, with a EER of 2.55%. From Fig. 7 and Fig. 8, we can see that valley noise analysis is much better than ridge signal analysis, which showed noise pattern along valleys is more suitable for liveness detection than perspiration pattern along ridges in this case. Furthermore, integration of both ridge signal and valley noise methods performs better than both of these two approaches independently. Different to previous time series perspiration pattern detection methods [20], this new approach needs only one image.

As shown in our previous work, fingerprint images change dynamically over time due to perspiration [20] or pressure. Based on our experiments, the time series images become stable after 2 seconds when the perspiration are saturated. To investigate the generality of our methods over time series images, we also consider the images at 1 and 2 seconds. Similar to cross-validation methods for 0 second images, 1 and 2 second images also use features fusing both ridge signal and valley noise analysis. Fig. 9 shows ROC comparison using neural network and classification tree for 0, 1, 2 images, respectively. For 0 second images, EER is 2.55% using the best network. For 1 second images, EER is 3.8% using the best network. For 2 second images, EER is 3.21% using the best network.



(a) ROC comparison using neural network



(b) ROC comparison using random forest tree

Figure 7: ROC curve comparison between ridge signal, valley noise analysis and integration of both for 0 second images

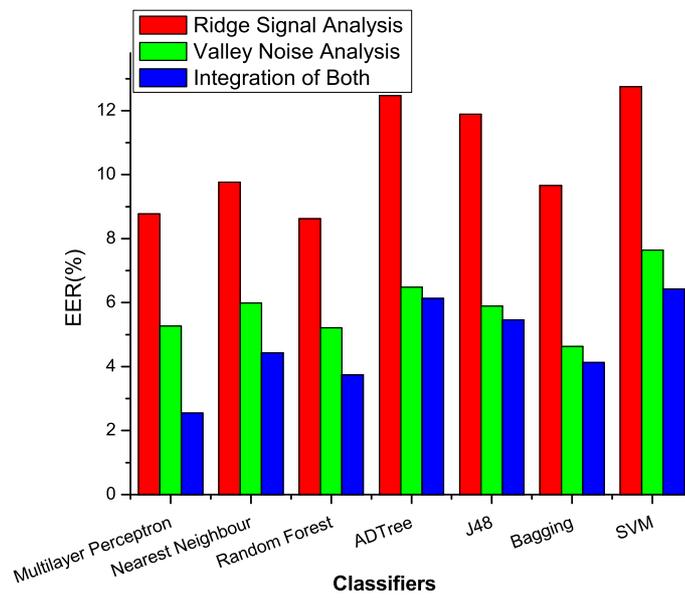
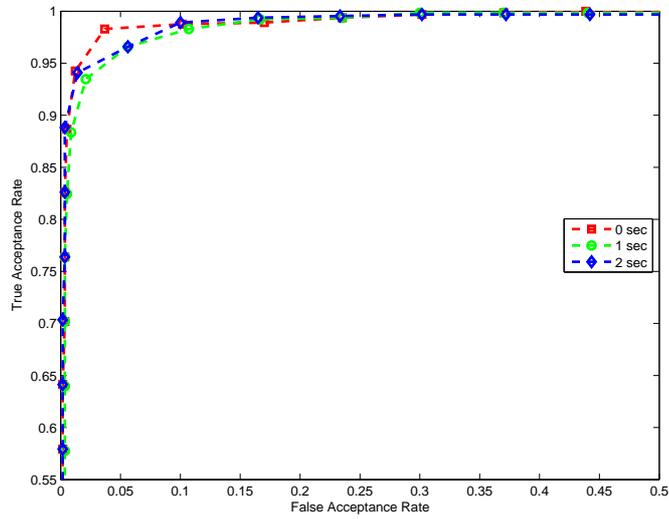
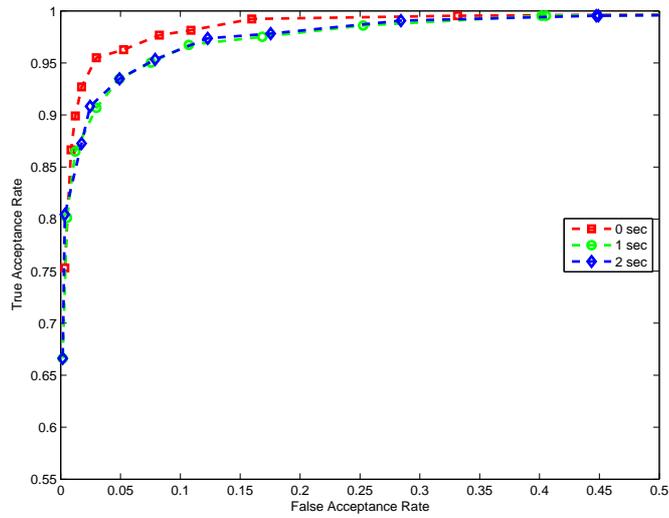


Figure 8: EER comparison between ridge signal algorithm, valley noise algorithm and fusion of them for 0 second images only



(a) ROC comparison using neural network for 0, 1, and 2 second images



(b) ROC comparison using random forest tree for 0, 1, and 2 second images

Figure 9: ROC curve comparison for 0, 1, and 2 second images

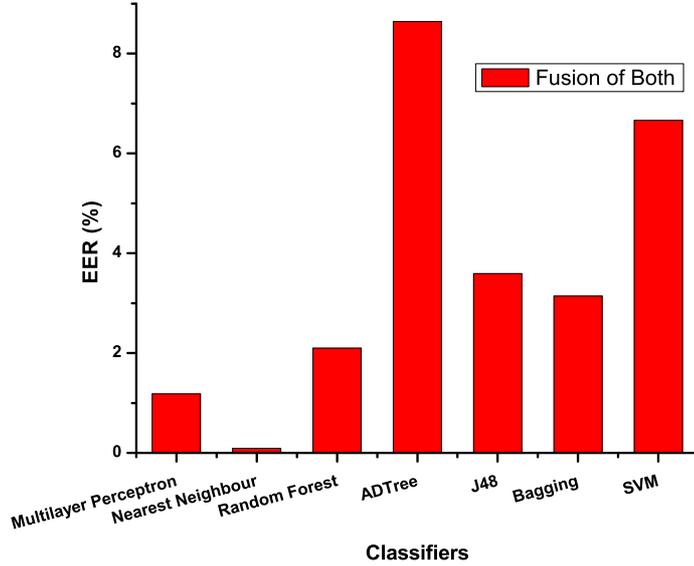


Figure 10: EER comparison by testing all images at 0, 1 and 2 second

In addition, all images at 0, 1 and 2 seconds are mixed and tested using ten-fold cross validation. EER decreases from 2.55% for 0 second images only to 1.18% for all images (0, 1, 2) using neural network. Similarly, EER decreases from 4.43% to 0.9% using nearest neighbour classifier. Therefore, training on images at 0, 1 and 2 second covers more variabilities for both live and spoof fingerprints.

## 5. Discussion

Compared with previous research, the first contribution of this work is the collection of a new live/spoof dataset. Previously, datasets typically contain one sample for each live subject from a single session [20, 21, 24, 25]. In this data, we have repeated samples from multiple live subjects over several sessions (81 subjects with average 4 sessions). Also a large spoof dataset (570) including spoof fingers made from Play-Doh, gelatin and silicone materials in five different sessions are collected. Most of the liveness datasets contain 12-36 fake fingers made of only a single material (gelatin, Play-Doh or silicone,

etc) [20, 21, 14, 19], as summarized in [43]. Even though some researchers collected multiple impressions [14, 15, 44], they did not specify the time interval. We assume they collected the data in a short time interval. Other studies had multiple spoof materials. However, they had smaller dataset, for example, 10 gelatin and 24 plastic clay fake fingers for [16] and 10 casts each of silicone, gelatin, latex and wood glue [15]. This method expands the type of materials and investigates the characteristics of spoof fingers over time. This database includes live and spoof fingerprints with various image quality, as can be seen from Fig. 2. Live and spoof subjects are collected in different sessions, as can be seen from Fig. 11. Time is an important factor affecting the quality of spoof images because as the spoof dries the amount of moisture changes impacting the fingerprint image. From Fig. 11, we can see Play-Doh spoof images change dramatically over time, but silicone images do not change over time. For some live subjects, the fingers are wet or dry depending on the environmental or emotional factors.

The second contribution of this work is a novel anti-spoofing method by fusing ridge signal and valley noise analysis processing only a single image. From the ridge perspective, live fingers have a distinctive perspiration pattern along the ridges, but the spoof fingers do not have. From the valley perspective, spoof fingers have more noise than live fingers along the valleys because spoof materials are easily transmuted and there are many granules in the valleys due to the property of the spoof materials. Our fusion algorithm achieves 97.45% correct classification on 0 second images and 99.1% on all time-series images. The results show that ridge and valley features evaluating perspiration phenomenon and noise pattern with decision trees, neural network or other pattern classifiers are efficient for liveness classification. The system can reduce spoofing vulnerability just by a simple software update.

We analyzed the error distribution for the live and spoof dataset considering both type of spoof and quality. For example, for Bagging Tree classifier, errors from Play-Doh, gelatin and silicone are 1.05%, 3.16% and 1.05%, respectively. The error ratio is the number of failures over total Play-Doh, gelatin and silicone independently. For the spoofs, gelatin fingerprint are more easily recognized as live compared with Play-Doh and silicone fingerprints. Also for live subjects, typically errors occurred in only one session during many returns for a single individual and did not come from specific subjects. It is hypothesized that in case of failure for live subjects, true live subjects can wipe the finger and try again.

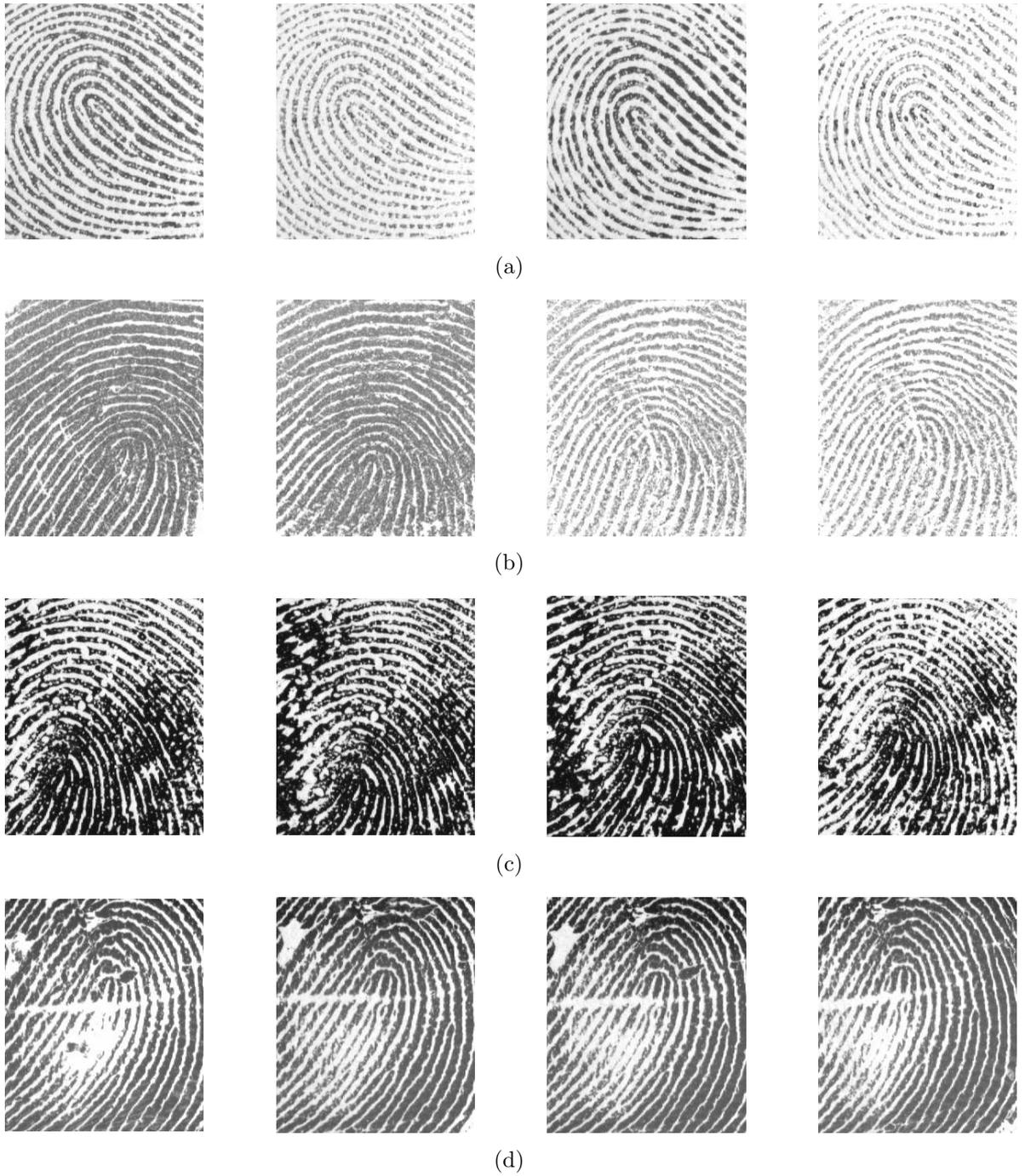


Figure 11: Example of fingerprints on different sessions from same subject: (a) live sample; (b) Play-Doh sample; (c) Gelatin sample; (d) Silicone sample.

Also we analyzed error distribution based on different quality levels, as listed in Table 2. Based on NFIQ standards, scores with 1, 2 and 3 are relatively good quality images; scores with 4 and 5 are relatively poor quality images. From Table 2, we can see live subjects with poor quality are more easily recognized as spoof. Poor quality fingerprint images may be rejected by the matcher stage also, so a slight increase in live/spoof error for live fingers is less of a concern. Spoof images with good quality are more easily recognized as live. This finding is reasonable because good quality spoofs appear more live-like. However, the percentage of best quality spoof images detected as live is still extremely low at 2.97%.

Quality scores	Live % (total #)	Play-Doh % (total #)	Gelatin % (total #)	Silicone % (total #)	Spoof overall % (total #)
1	1.72 (116)	0 (30)	4.76 (42)	3.45 (29)	2.97 (101)
2	2.65 (226)	0 (14)	3.57 (28)	0 (91)	0.75 (133)
3	2.31 (216)	1.33 (75)	2.47 (81)	1.61 (62)	1.83 (218)
4	1.67 (60)	1.79 (56)	0 (36)	0 (8)	1.0 (100)
5	3.85 (26)	0 (15)	0 (3)	0 (0)	0 (18)

Table 2: Error distribution for 0 second images using Bagging Tree

Of course, the fingerprint valley may not be clean if the sensor is very dirty or the finger is very wet. This may cause a false rejection for live subjects. While live subjects can prevent this happening by just cleaning the sensor surface or by wiping their fingers on the clothes to successfully pass the fingerprint liveness system.

This method is tested on the Identix optical scanner. A clear result from our previous research is that the characteristics of live/spoof figures vary across different technologies. We plan to explore this approach for other scanner technologies. While algorithms may vary from technology to technology, we have shown that the general approach does not in previous papers, as described in [20, 21, 22, 23, 24, 25]. The general approach is selection of a set of features and supervised pattern recognition. Variation from technol-

ogy to technology typically is related to the weighting and specific thresholds. We have chosen an optical reader as it represents a large percentage of the market. For the algorithm proposed herein, we expect that other technologies will show similar results because of part of this method has been proved successfully in some other scanners [20, 21, 22, 23, 24, 25]. However due to the difficulty and time consuming nature of creating and collecting the spoofs images, this work is still in progress.

Furthermore, based on our experience, the intensity of spoof fingerprints depends on the materials used. While this algorithm is effective for these materials and methods, it is not guaranteed to be effective for all types of spoof materials. For our research, we have selected the materials and methods which create the most live-like spoof images. In further investigation we would like to further explore the dryness of Play-Doh and thickness of gelatin fingers. In our current database, we use gelatin molds which are thick because the cast is concave, not flat. Therefore, the dryness variability is reduced. Our future plan is to design another type of cast that makes thinner gelatin fingers. Also more variability in quality of live fingers needs to be studied, particularly environmental or climate changes. While it is impossible to conceive of all possible spoof techniques, this work is a significant step forward to reduce spoofing of well known spoof materials - gelatin, Play-Doh and silicone [3, 4, 5].

This method minimizes the risk of spoofing. Since this method relies on a single image captured from the fingerprint scanner, fingerprint recognition and anti-spoofing protection can work simultaneously, i.e. at the same time using the same image. If anti-spoofing is detected for a particular application, several factors need to be considered. First, biometric performance will be impacted by the liveness stage. For example, false rejects could come from the matching or liveness stage. Therefore, the false reject from the system is the union (AND) of biometric false rejects and liveness false rejects. If a system has 0.1% biometric and 2% liveness FRR, the total system FRR has a maximum of 2.1% FRR. Clearly driven by the liveness stage, this is the tradeoff for adding a liveness component to the system - increased security may result in decreased performance. It is unknown if repeated attempts will result in an acceptance at liveness stage. More work is needed to evaluate this. Second, it is conceivable if the spoofer is motivated, he/she would repeat efforts until spoofing occurred. With a false acceptance of 2%, approximately 50 times would be needed. In a system where anti-spoofing is critical, many repeated rejections from a single individual due to the liveness stage would

result in a lock-out of the system for that individual.

## 6. Conclusion

A new method based on combining ridge signal and valley noise analysis is proposed for anti-spoofing in fingerprint sensors. Results show that this method is very efficient (EER of 0.9%) for an optical Identix scanner when tested for a large dataset of live subjects with repeated visits and spoofs with varying material and moisture levels. Different to previous methods using two time-series images, the new method needs only one image. The method is purely software based and application of this anti-spoofing method can protect fingerprint scanners from spoofing attacks, like artificial Play-Doh, gelatin and silicone fingers.

## 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] International biometric group white paper, *Liveness Detection in Biometric Systems*, available at <http://www.ibgweb.com/reports/public/reports/liveness.html>,
- [7] M. Sandstrom, *Liveness Detection in Fingerprint Recognition Systems*, Master thesis, <http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf>.

- [8] 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.
- [9] K. Seifried, *Biometrics - What You Need to Know*, Security Portal, 10 January 2001.
- [10] 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.
- [11] 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.
- [12] D. Baldisserra, A. Franco, D. Maio and D. Maltoni, *Fake Fingerprint Detection by Odor Analysis*, Proc. of International Conference on Biometric Authentication (ICBA06), Hong Kong, January 2006.
- [13] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer Verlag, Nu, USA, 2003.
- [14] Y. Chen, A. Jain, and S. Dass, *Fingerprint Deformation for Spoof Detection*, Proc. of Biometrics Symposium (BSYM2005), Arlington, VA, Sept. 19-21 2005 .
- [15] 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.
- [16] 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.
- [17] 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.
- [18] A. Russo, *System for and methods of securing fingerprint biometric systems against fake-finger spoofing*, U.S. Patent No.: US2007/0014443 A1, Jan. 2007.

- [19] P. Coli, G. L. Marcialis, F. Roli, *Power spectrum-based fingerprint vitality detection*, IEEE Workshop on Automatic Identification Advanced Technologies AutoID 2007.
- [20] R. Derakhshani, SAC 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.
- [21] S. Parthasaradhi, R. Derakhshani, L. Hornak, SAC Schuckers, *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.
- [22] SAC Schuckers, A. Abhyankar, *A Wavelet Based Approach to Detecting liveness in Fingerprint Scanners*, Proceedings of Biometric Authentication Workshop, ECCV, Prague, May, 2004.
- [23] 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.
- [24] 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.
- [25] B. Tan, S. Schuckers, *A New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis*, accepted by SPIE Journal of Electronic Imaging (JEI), Special Section on Biometrics: Advances in Security, Usability and Interoperability (ASUI) January-March, 2008.
- [26] M.H. Ross, L.J. Romrell, E.J. Reith, *The integumentary system, Histology: A Text and Atlas*, 2nd Edition, Williams and Wilkins, Baltimore, 1989, pp. 347-349.
- [27] <http://www.dowcorning.com>.
- [28] E. Tabassi, C. Wilson and C. Watson, *Fingerprint image quality*, NIST Research Report NISTR 7151, Aug. 2004.

- [29] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, *FVC2004: Third Fingerprint Verification Competition*, Proc. International Conference on Biometric Authentication (ICBA), pp. 1-7, Hong Kong, July 2004.
- [30] M. Kawagoe and A. Too, *Fingerprint pattern classification*, Pattern Recognition, 17(3):295-303, 1984.
- [31] 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.
- [32] M. B. Ruskai et. al., *Wavelets and Digital Signal Processing*, Wavelets and Their Applications (pp. 105-121), 1992.
- [33] I. Daubechies, *Orthonormal bases of compactly supported wavelet*, Comm. Pure Appl. Math., 41(1988), pp. 909-996.
- [34] Ian H. Witten and Eibe Frank , *Data Mining: Practical machine learning tools and techniques*, 2nd Edition, Morgan Kaufmann, San Francisco, 2005.
- [35] D. Aha, and D. Kibler, *Instance-based learning algorithms*, Machine Learning, vol.6, 1991, pp. 37-66.
- [36] Y. Freund, L. Mason, *The alternating decision tree learning algorithm*, Proceeding of the Sixteenth International Conference on Machine Learning, Bled, Slovenia, (1999) 124-133.
- [37] R. Quinlan, *C4.5: Programs for Machine Learning*, Morgan Kaufmann Publishers, San Mateo, CA, 1993.
- [38] L. Breiman, *Random Forests*, Machine Learning 45 (1):5-32, October 2001.
- [39] L. Breiman, *Bagging predictors*, Machine Learning, 24(2):123-140, 1996.
- [40] J. Platt, *Fast Training of Support Vector Machines using Sequential Minimal Optimization*, Chap. 12, Advances in Kernel Methods - Support Vector Learning, B. Scholkopf, C. Burges, and A. Smola, eds., pp. 185-208, MIT Press, 1999.

- [41] J. Pearl, and S. Russell, *Bayesian Networks*, in M. A. Arbib (Ed.), Handbook of Brain Theory and Neural Networks, pp. 157C160, Cambridge, MA: MIT Press, 2003.
- [42] R.C. Holte, *Very simple classification rules perform well on most commonly used datasets*, Machine Learning, Vol. 11, pp. 63-91, 1993.
- [43] P. Coli, G. Marcialis, F.Roli, *Vitality detection from fingerprint images: a critical survey*, 2nd International Conference on Biometrics ICB, vol. 4642, pp. 722-731, Seoul (South Korea), 2007 .
- [44] P. Coli, G. L. Marcialis, F. Roli, *Analysis and selection of feature for the fingerprint vitality detection*, SSPR/SPR 2006, pp. 907-915, 2006.
- [45] A. Ross, A. Jain, *Information Fusion in Biometrics*, Pattern Recognition Letters, vol. 24, 13, pp: 2115-2125, September, 2003.
- [46] J. Jia, L. Cai, *Fake Finger Detection Based on Time-series Fingerprint Image Analysis*, Advanced Intelligent Computing Theories and Applications, With Aspects of Theoretical and Methodological Issues, Springer, Volume 4681, pp. 1140-1150, 2007.
- [47] J. Jia, L. Cai, K. Zhang, and D. Chen, *A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis*, Advances in Biometrics, Volume 4642, pp. 309-318, 2007.
- [48] K. Uchida, *Image-Based Approach to Fingerprint Acceptability Assessment*, Biometric Authentication, Springer, Volume 3072, pp. 294-300, 2004.
- [49] Y. Zhang, J. Tian, X. Chen, X. yang, and P. Shi, *Fake Finger Detection Baed on Thin-late Spline Distortion Model*, Advances in Biometrics, Volume4642, pp. 742-749, 2007.
- [50] C. Jin, H. Kim, S. Elliott, *Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum*, Information Security and Cryptology-ICISC 2007, Springer, Volume 4817, pp. 168-179, 2007.
- [51] H. Choi, R. Kang, K. CHoi and J. Kim, *Aliveness Detection of Fingerprints using Multiple Static Features*, Proc. of World Academy of Science, Engineering and Technology, Volume 22, July 2007.

- [52] S.B. Nikam, S. Agarwal, *Fingerprint Liveness Detection Using Curvelet Energy and Co-Occurrence Signatures*, Fifth international conference on CGIV, pp. 217-222, 2008.