The Effect of Environmental Conditions and Novel Spoofing Methods on Fingerprint Anti-Spoofing Algorithms

Bozhao Tan, Aaron Lewicke, David Yambay, Stephanie Schuckers

Department of Electrical and Computer Engineering, Clarkson University
8 Clarkson Ave., Potsdam, NY 13699 USA

{tanb,lewickat,yambayda,sschucke}@clarkson.edu

***Abstract*—Fingerprint recognition systems have been shown to be vulnerable to spoof attacks with artificial fingers made from materials such as Play-Doh, gelatin and silicon. Anti-spoofing or liveness algorithms have been developed which determine at the time of capture whether a finger is live or spoof. Software algorithms rely on characteristics of the image captured by the underlying device and thus may be impacted by environmental conditions at the time of capture. In this study, we collected live fingerprints under various environment weather conditions (high/low/very low temperature, high humidity). Additionally we incorporated more spoofing materials of latex rubber, latex caulk, and latex paint. The algorithms were trained with a baseline dataset for Identix, Crossmatch, and Digital Persona devices with an average spoof/live equal error rate of 3.5%, 5.9% and 5.8%, respectively. Results showed an increase in error to 14.5%, 55.6% and 36.6%, respectively, when data of this type is not included in the training set. Similarly, we found the new spoof approaches developed defeat the liveness algorithm in almost all cases. When the algorithm is retrained to include new environmental and spoof images, the liveness algorithm is able to achieve an average error rate of 4.0%, 9.6%, and 11.4% for Identix, Crossmatch, and Digital Persona scanners, respectively. The impact of temperature, humidity, and novel spoof materials on anti-spoofing algorithm is significant and degrades performance. Performance can be restored when these factors are included in the training of the anti-spoofing model.**

I. INTRODUCTION

While fingerprint recognition is one of the most widely used biometrics [1], it is vulnerable to attacks at the sensor interface with easily made fake finger replicas. Previous studies have shown 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 silicon materials to fool a variety of fingerprint scanners [2-6]. Anti-spoofing methods, also termed liveness detection, are designed to ensure that only the biometric from a live person is submitted for enrollment, verification and identification [7].

Suggested methods to detect liveness for fingerprint can fall into two categories. The first category is a hardware-based measure, which requires additional hardware integrated with the fingerprint scanner to capture live signatures (e.g. temperature, electrocardiogram, pulse oximetry, odor, or a multispectral sensor) [8-14]. The second anti-spoofing method uses software based approaches to exploit the information already captured by traditional fingerprint systems to detect life signs (e.g. skin deformation/elasticity, perspiration pattern, or image characteristics of spoof and live images). The skin deformation technique uses the information regarding how the fingertip's skin deforms when pressed against the scanner surface [15-17]. Methods that rely on the perspiration patterns inherent only to live fingers due to the existence of pores and perspiration use two time series images or a single image [18-21]. Other features include the characteristics of spoof and live fingers, like power spectrum [22], skin coarseness [23], pore detail [15], or valley noise [24]. It is clear that for reliable liveness detection, software-based methods should incorporate live finger characteristics, as well as unique characteristics of individual spoof materials as imaged by the fingerprint scanner.

Although the previous work has demonstrated novel methods for anti-spoofing, no study has systematically determined the effect of environmental factors such as temperature and humidity. Typically the data is collected in a research laboratory with office environment temperatures (70-75 ℉). While the target application for anti-spoofing algorithms may be an office environment, many algorithms are affected by moisture in the finger; thus, impact of temperature and humidity needs to be studied. Similarly, as spoofing techniques evolve, it is necessary to determine the impact of new spoof materials.

In this study we evaluated the performance impact of temperature, humidity, and novel spoof materials on previously developed anti-spoofing algorithms.

II. METHODS

A. Environmental Data Collection

A temperature and humidity controlled room, which allowed the data collection administrator to dial specific ranges for the temperature and humidity profiles, was used in addition to outdoor data collection. Table 1 details the temperature and humidity profiles used for the data collection process. In our study, most of the subjects for environmental data collection are students at Clarkson (18-26 years old).

WIFS'2010, December, 12-15, 2010, Seattle, WA, USA.
978-1-4244-9080-6/10/*$26.00 ©2010 IEEE.*

For each of the fingerprint scanners, multiple images (3) of both the thumb (R1) and 1st finger of the right hand (R2) were collected. As some of the data collection software applications were being developed during data collection, not all devices were used at each session. Table 2 details the breakdown of the number of subjects from each scanner for all weather conditions.

TABLE 1
ENVIRONMENTAL DATA DESCRIPTION

Weather Condition	Temperature Range	Humidity Range	No. of Subjects
High Temperature / High Humidity	85°-90 ° [F]	>80%	22
High Temperature / Normal Humidity	85°-90 ° [F]	30-60%	31
Low Temperature / Normal Humidity	50°-60 ° [F]	30-60%	23
Very Low Temperature /Normal humidity	<30 ° [F]	30-60%	12

Three fingerprint scanners, Crossmatch Technologies, L-1 (Identix), and Digital Persona were used for this analysis. At each collection event, Crossmatch and Identix device captured multiple time-series images, while Digital Persona captured only a single image because this device was not implemented to collect time-series images. This was repeated three times for each device/condition.

TABLE 2. NUMBER OF SUBJECT COLLECTED FOR THE ENVIRONMENTAL DATA PER SCANNER

Weather Condition	Crossmatch	Identix	Digital Persona	Total Images
High Temperature / High Humidity	20	21	17	252
High Temperature / Normal Humidity	30	30	7	372
Low Temperature / Normal Humidity	23	23	11	276
Very Low Temperature /Normal humidity	12	12	4	132

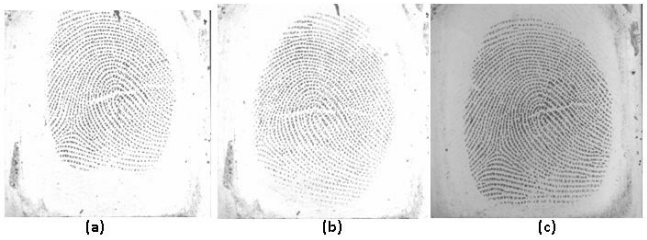


Fig. 1. Typical new environmental Identix images collected from a) High Temperature / High Humidity, b) High Temperature / Normal Humidity, c) Low Temperature / Normal Humidity

B. Spoof Materials

The spoof fingerprint data collection was performed using three scanners: Identix, Crossmatch, and Digital Persona. The software for the Identix scanner is set up to scan each finger 3 times. Crossmatch and Digital Persona are set to scan each finger five times.

Fifty molds were created from casts of 25 live subjects where each subject contributed 2 molds. Each mold was inspected to ensure the highest quality spoof images (e.g. no nicks or gouges, etc.). Not all of the molds were able to be used for each material and not every sample created from a mold was high enough quality to scan (see Table 3). Our goal was to achieve high quality spoofs that are likely to be matched by a fingerprint matcher. Poor quality spoof images will naturally be rejected by the fingerprint system. Thus, we discarded and rescanned based on visual inspection at the time of capture.

When creating a new spoofing approach a reliable technique must be developed to produce quality spoof samples. After investigating many different new materials and techniques, the data collection effort settled on latex rubber, latex caulk, and latex paint. Additionally, spoof fingers from Play-Doh, gelatin, and silicon were also created as in previous studies [19-22, 24-25]. Spoof fingers of the new materials are shown in Fig. 2. Fig. 3 illustrates the prints obtained from the new materials using the Identix scanner.

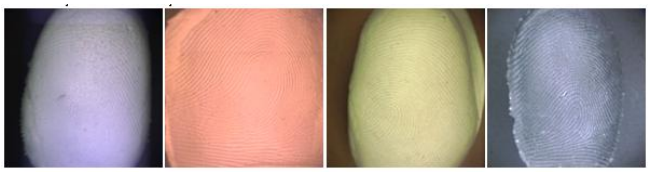


Fig. 2. Photos of spoof fingers made from various materials (left to right: latex caulk, latex paint, Play-Doh, and silicon).

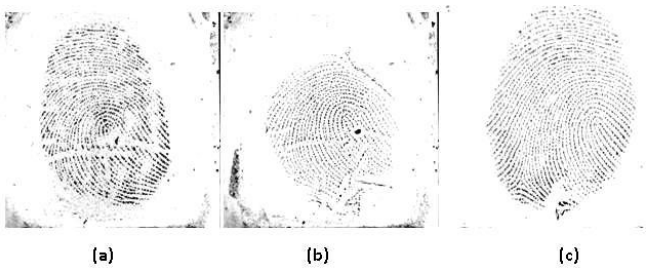


Fig. 3. Representative spoof images made from a) caulk, b) paint, and c) rubber captured using an Identix scanner.

To make the latex rubber finger, latex rubber was applied to the finger molds in three thin coats over the course of an hour and allowed to dry overnight. Next, excess rubber was trimmed with scissors to prevent rolling and sticking to the spoof. These spoofs are similar to silicon in that they may be scanned indefinitely as long as they are not torn.

Spoofs made from latex painter's caulk could be successfully scanned for about 2 days. A pea-sized amount of latex caulk was applied to the mold and then spread on the surface. It was necessary that the layer be thin and even; if the caulk is too thick the spoof will crack and tear. The spoof was allowed to dry for 14 hours and then scanned three times: immediately, 10 hours, and 24 hours.

Spoofs made from latex paint can be successfully scanned for at least 3-4 days. First, the paint is applied to the mold in 3-4 thin coats over the course of an hour and allowed to dry overnight. Care was taken when removing the paint

from the mold to prevent tearing along finger ridges. The spoof was scanned once a day for three days at 24-hour intervals.

TABLE 3
NUMBER OF SPOOF IMAGES COLLECTED PER SCANNER

Material	No. of Finger Molds	Samples Per Mold	Identix	Crossmatch	Digital Persona
Silicon	40	3	550	620	171
Gelatin	40	3	649	690	120
Play-Doh	40	7-10	801	690	120
Latex Rubber	50	2	300	300	300
Latex Caulk	50	2	300	300	300
Latex Paint	50	2	300	300	300

C. Anti-Spoofing Models

Three existing anti-spoofing models plus the fusion of the two were used to test the impact of the environmental conditions and the new spoof materials. We identify the models by the image feature that they exploit: Ridge Signal [22], Valley Noise [24], Region Labeling [25], and Fusion [26]. A baseline dataset composed of live samples and spoof samples (Play-Doh, gelatin and silicon materials) was used to train the models and is described in Table 4 [26]. For live samples, we collected the data in normal laboratories with air-conditional environment. For spoof samples, we collected the dataset using Play-Doh, gelatin, and silicon materials in different dryness situations. The dataset from Digital Persona device is much less than the other two devices, because it was added to our experiments at the end of our project,

The Ridge Signal algorithm for liveness detection 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. 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 [22].

The Valley Noise algorithm detects the noise pattern along valleys specific to spoof fingers due to material properties and fabrication process. 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 techniques. Based on these features, liveness separation (live/spoof) is performed using classification trees and neural networks [24].

The Region Labeling algorithm is based on a computer vision technique to identify areas of foreground from the background which quantifies observable differences between live and spoof images. Regarding the capture of a single image, there exist more identifiable regions along both ridge and valley segments than contained in spoof images. This would be expected because ridge segments in live images tend to have consistent intervals of high and low intensity, corresponding to pore locations, a trait not common in spoof images. In the valleys, spoof images are often prone to pressure deformation, causing ridge segments to bleed into the valley. Live images remain relatively clean, though due to the effects of noise, several small areas of intensity should be present. Difference images, a type of image where two captures are subtracted from one another can also expose traits which can be exploited by region labeling. In this format, the element of control an imposter has over a fingerprint scanner is exposed. Here, the slight variance of pressure and rotation distorts ridge segments which would otherwise remain intact, resulting in more identifiable regions in spoof images than live images. Additionally, tracking region size of ridge and valley segmentscan also be taken into account to compare the difference of live and spoof images. This method is advantageous in that it looks at the perspiration pattern in a different sense, as well as isolating traits of spoof images. Another advantage is simplicity where the required computations are presently available and well known. Results from testing are presented which show that the addition of this algorithm leads to improved performance when fused with ridge and valley features [25]. For this algorithm, we considers the images collected at 0 second and 2 second.

To improve performance, fusion was implemented at feature level by integrating the Ridge Signal, Valley Noise, and Region Labeling for Identix and Crossmatch algorithms [26]. The Digital Persona device did not provide a time-series image and fusion was only of the Ridge Signal and Valley Noise algorithms.

10-fold cross-validation is used to evaluate the performance of the proposed algorithms objectively, in which the total dataset was divided into 10 equal subsets for which the classifier was trained on 9 partitions and 1 partition was used for test. This procedure was repeated 10 times and an average accuracy was obtained to represent the average performance for our algorithms. The Equal Error Rate (EER) is used to evaluate the classification performance, in the threshold when spoof false acceptance rate (SFAR) and live false rejection rate (LFRR) are equal.

TABLE 4. BASELINE DATASET

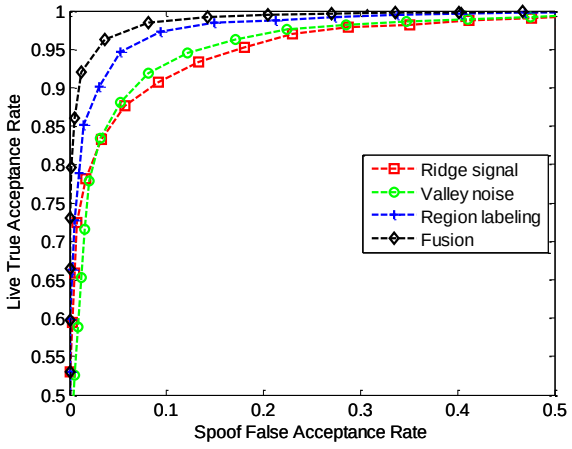
Scanner	Model No.	Resolution	Image Size	Live Samples	Spoof Samples
Identix	DFR2100	686 dpi	720x720	3000	3000
Crossmatch	Verifier 300LC	500 dpi	480x640	4000	4000
Digital Persona	U.are.U 4000B	512 dpi	355x391	172	411

III. RESULTS

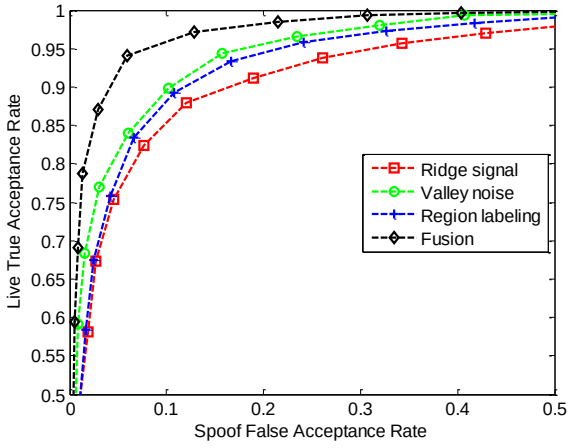
A. Baseline Algorithms

The algorithms are first implemented on the baseline dataset for Identix, Crossmatch, and Digital Persona scanners. Fig. 4 shows the ROC comparison of different algorithms: Ridge Signal, Valley Noise, Region Labeling and Fusion.

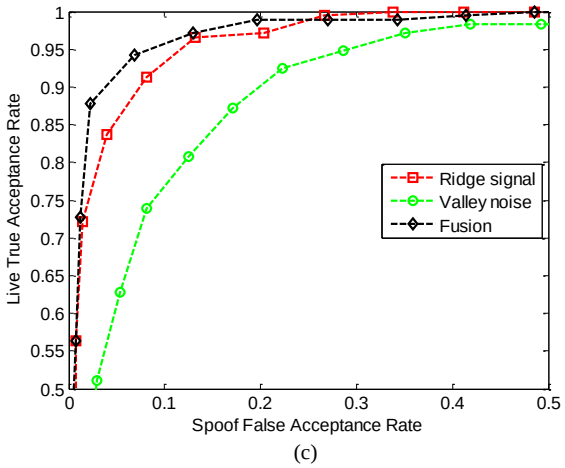
From this figure, we can see the anti-spoofing algorithms are sensor dependent. To improve the performance, we fuse the above algorithms in the feature level [27]. For Identix scanner, the EER is 8.7%, 8.0%, and 5.1% for Ridge Signal, Valley Noise and Region Labeling algorithms, respectively. After



(a)



(b)



(c)

Fig. 4. ROC comparison of three algorithms and their fusion. a). Identix, b). Crossmatch, c) Digital Persona

system fusion, the EER drops to 3.5%. For the Crossmatch scanner, EER is 11.6%, 10.1%, 10.6% for the three algorithms respectively. After system fusion, the EER drops to 5.9%. For Digital Persona scanner, the best EER is 5.8% after fusing Ridge Signal and Valley Noise algorithms. Since this scanner was not implemented to collect time-series images, we cannot apply the region labeling approach on this scanner and apply the methods of fusing the first two algorithms.

B. Environmental Data

After the liveness detection classifier was trained based on baseline dataset (collected indoors with normal temperature and humidity), we tested the classifier on the new environmental live data. Table 5 lists the error rates of the trained classifier on new environmental data. The average error rate for classification is 14.5%, 55.6%, and 36.6% for Crossmatch, Identix and Digital Persona, respectively.

TABLE 5. ERROR RATES OF OUR PROPOSED LIVENESS DETECTION ALGORITHMS ON NEW ENVIRONMENTAL DATA

Weather Condition	Images	Crossmatch (%)	Identix (%)	Digital Persona (%)
High Temperature / High Humidity	252	18.1	42.1	41.2
High Temperature / Normal Humidity	372	12.8	62.5	37.9
Low Temperature / Normal Humidity	276	13.9	57.5	41.7
Very Low Temperature /Normal Humidity	132	14.4	54.5	28.0
Average		**14.5**	**55.6**	**36.6**

C. Novel Spoofing Methods

Similar to testing of the environmental dataset, we tested the trained classifier on the new spoof data made from latex caulk, latex paint and latex rubber. Table 6 lists the error rates of the trained classifier on new spoof data. The average error rate is about 99.1%, 88.8%, and 64.4% for Crossmatch, Identix and Digital Persona, respectively.

TABLE 6. ERROR RATES OF OUR PROPOSED LIVENESS DETECTION ALGORITHMS ON NEW SPOOF DATA

New Spoof Materials	Data Collection	Crossmatch (%)	Identix (%)	Digital Persona (%)
Caulk	300	97.0	85.2	37.0
Paint	300	100	84.8	98.3
Rubber	300	97.32	96.0	58.0
Average		99.1	88.7	64.4

D. Evaluation of Environmental and Spoof Data Combined

From the above experiments, we found images collected by varying environments and with new spoof materials significantly decrease the performance of existing algorithms when representative images are not included in the training set. To make our algorithm more robust, we considered the new data in our training set. Similar to the above evaluation criteria, we test our algorithms using 10-fold cross-validation after training with the new data. As shown in Fig. 5, using

fusion techniques, we achieve an average EER is 4.0%, 9.6%, and 11.4% for Identix, Crossmatch and Digital Persona scanners, respectively. The results are much improved over errors of 14.5%, 55.6%, and 36.6%, respectively, using original algorithm for environmental data and 99.1%, 88.8% and 64.4%, respectively, for spoof data.

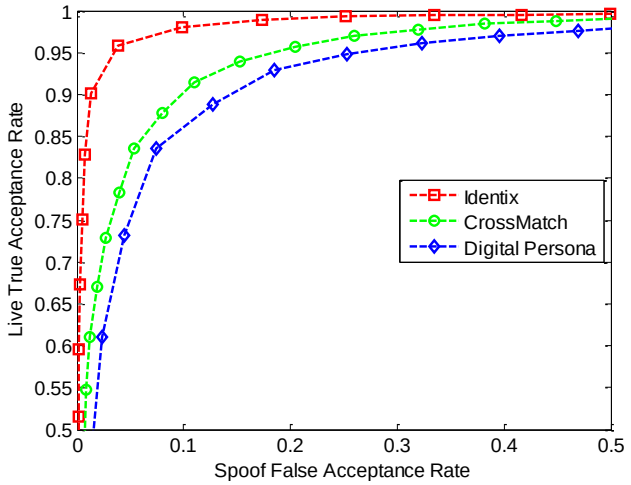


Fig. 5. ROC curve of three scanners based on new training

IV. Discussions

The impact of various environmental conditions on algorithm performance was investigated by varying temperature and humidity. Results showed an increase in error to 14.5%, 55.6%, and 36.6% for Identix, Crossmatch and Digital Persona scanners respectively, when data of this type is not included in the training set. We think the improvement is due to including samples from different environmental conditions and not due to just having more training samples. More experiments will be done in the future to verify this point.

The results show that live images collected by Identix scanner are more sensitive to environmental changes than Crossmatch and Digital Persona scanners. This demonstrates how critical the need is for this type of data be collected. By including environmental data when training the classifier, this will improve the robustness of our liveness detection algorithm, as will be shown.

Similarly, the performance impact of new spoof materials and techniques on our existing algorithms showed an increase in error to 99.1%, 88.8%, and 64.6% for Identix, Crossmatch and Digital Persona scanners respectively, when not included in the training set. In other words, the new spoof approaches developed defeat the liveness algorithm in almost all cases.

The results show that new methods to create spoof fingers defeat our current algorithms. In other words, the current algorithms work well on the spoof attacks from fake Play-Doh, gelatin and silicon fingers used in the training set, but are vulnerable to new spoofing techniques. To improve robustness of our liveness detection algorithm to spoofing attacks, the new spoof data must be used in the training set for the classifier as will be shown.

The results also show that our anti-spoofing algorithms are completely data-driven. They are dependent on the texture feature difference by comparing live and spoof fingerprints. We can guarantee that our algorithms work well on some spoof categories which have samples included in the training dataset. But we still need to tune the threshold or classifier when new spoof materials are introduced, even though the principles behind the algorithms are same which are based on the ridge perspiration pattern or valley noise pattern, etc,

When the algorithm is retrained to include new environmental and spoof images, the liveness algorithm is able to achieve an average error rate of 4.0%, 9.6%, and 11.4% for Identix, Crossmatch and Digital Persona scanners, respectively. This study affirms our need to create a large dataset which represents individual and environmental variability as well as continually improve our spoofing techniques with variable methods and types of materials represented.

To mitigate any risks posed by the variability in the environment or different spoof materials, it is necessary to continue to evolve anti-spoofing algorithms for a more robust model. Future efforts should include both additional data collection for variety of scanners, environmental conditions, spoof techniques, as well as continuous improvement of the algorithms both for training, as well as development of new features which will increase overall performance.

V. Conclusion

In this study, we found the impact of temperature, humidity, and novel spoof materials on anti-spoofing algorithms are significant and degrade performance. Performance can be restored when these factors are included in the training of the anti-spoofing model.

Acknowledgment

This work was supported by NexID Biometrics, LLC and the National Science Foundation STTR Grant IIP – 0740601.

References

[1] A. Jain, R. Bolle, and 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, pp. 614-634, 2001.
[3] S. A. C. Schuckers, "Spoofing and anti-spoofing measures," Information Security Technical Report, vol. 7, pp. 56-62, 2002.
[4] T. Matsumoto, "Gummy Finger and Paper Iris: An Update," Workshop on Information Security Research, Fukuoka, Japan October 2004.
[5] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems " Proceedings of SPIE, vol. 4677, 2002.
[6] H. Kang, B. Lee, H. Kim, D. Shin, and J. Kim, "A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules," KES 2003, pp. 1245-1253, 2003.
[7] International Biometric Group, "Liveness Detection in Biometric Systems," 2005.
[8] M. Sandstrom, "Liveness Detection in Fingerprint Recognition Systems ": Linkoping University, 2004.
[9] D. Osten, H. M. Carim, M. R. Arneson, and B. L. Blan, "Biometric, personal authentication system," Minnesota Mining and Manufacturing Company, 1998.

[10] K. Seifried, "Biometrics - What You Need to Know," Security Portal, 2001.
[11] P. D. Lapsley, J. A. Less, D. F. P. Jr., and N. Hoffman, "Anti-fraud biometric sensor that accurately detects blood flow," SmartTouch, LLC, 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., 2001.
[13] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis," in Conference on Biometric Authentication (ICBA06), Hong Kong, 2006.
[14] R. K. Rowe, K. A. Nixon, and S. P. Corcoran, "Multispectral fingerprint biometrics," in Information Assurance Workshop, 2005. IAW '05. Proc. from the Sixth Annual IEEE SMC, 2005, pp. 14-20.
[15] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition: Springer Verlag, Nu, USA, 2003.
[16] Y. Chen, A. Jain, and S. Dass, "Fingerprint Deformation for Spoof Detection," in Biometrics Symposium (BSYM2005), Arlington, VA, 2005.
[17] 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, pp. 360-373, September 2006.
[18] 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, pp. 383-396, 2003.
[19] S. Schuckers and A. Abhyankar, "A Wavelet Based Approach to Detecting liveness in Fingerprint Scanners," in Proceedings of Biometric Authentication Workshop, ECCV, Prague, 2004.
[20] S. Parthasaradhi, R. Derakhshani, L. Hornak, and S. Schuckers, "Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices," Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 35, pp. 335-343, 2005.
[21] B. Tan and S. Schuckers, "Liveness detection using an intensity based approach in fingerprint scanner," in Biometrics Symposium (BSYM2005), Arlington, VA, 2005.
[22] B. Tan and S. Schuckers, "Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing," in 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), 2006.
[23] Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, "Wavelet based fingerprint liveness detection," Electronic Letters, vol. 41, pp. 1112-1113, 2005.
[24] B. Tan and S. Schuckers, "New approach for liveness detection in fingerprint scanners based on valley noise analysis," Journal of Electronic Imaging, vol. 17, pp. 011009-9, 2008.
[25] B. Decann, B. Tan, and S. Schuckers, "A Novel Region Based Liveness Detection Approach for Fingerprint Scanners," in Proceedings of the Third International Conference on Advances in Biometrics Alghero, Italy: Springer-Verlag, 2009.
[26] B. Tan and S. Schuckers, "Spoofing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise," Pattern Recognition, 43(8):2845-2857, 2010.
[27] A. Ross and A.K. Jain, "Information Fusion in Biometrics" Pattern Recognition Letters, 24(13):2115-2125, 2003.