Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices

Sujan T. V. Parthasaradhi, B. S., Reza Derakshani, M.S., Lawrence A. Hornak, Ph.D., Stephanie A. C. Schuckers, Ph.D.

Center for Identification Technology Research (CITeR)

Lane Department of Computer Science and Electrical Engineering

West Virginia University

PO Box 6109

Morgantown, WV 26506-6109

Submission to:
IEEE Systems Man, and Cybernetics Society, Part C: Applications and Reviews
Special Issue on Biometric Systems

Contact Information:
Stephanie Schuckers
Clarkson University
PO Box 5720
Potsdam, NY 13699
Phone: 315-268-6536
Fax: 315-268-7600
sschucke@clarkson.edu

Manuscript received March 1, 2003. This work was supported in part by the NSF Center for Identification Technology Research (CITeR).

S. T. V. Parthasaradhi is with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506 USA (email: saradhi21@yahoo.com).

R. Derakhshani is with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506 USA (email: reza@csee.wvu.edu).

L. A. Hornak is with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV, 26506 USA (email: lah@csee.wvu.edu).

S. Schuckers was with West Virginia University, Morgantown, WV, 26506. She is now with the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13699 USA (phone: 315-268-6536, fax: 315-268-7600, email: sschucke@clarkson.edu).

Abstract—**Fingerprint scanners may be susceptible to spoofing using artificial materials, or in the worst case, dismembered fingers. An anti-spoofing method based on liveness detection has been developed for use in fingerprint scanners. This method quantifies a specific temporal perspiration pattern present in fingerprints acquired from live claimants. The enhanced perspiration detection algorithm presented here improves our previous work by including other fingerprint scanner technologies, using a larger, more diverse data set, and a shorter time window. Several classification methods were tested in order to separate live and spoof fingerprint images. The dataset included fingerprint images from 33 live subjects, 30 spoof created with dental material and Play-Doh, and fourteen cadaver fingers. Each method had a different performance with respect to each scanner and time window. However, all the classifiers achieved approximately 90% classification rate for all scanners, using the reduced time window and the more comprehensive training and test sets.**

Index Terms—**biomedical measurements, biomedical image processing, identification of persons, pattern recognition.**

1. Introduction

Biometrics can play a vital role in enhancing security systems and is under consideration for dramatically increased use in order to minimize security threats in military organizations, government centers, and public places like airports. Biometrics systems use physiological or behavioral characteristics to automatically determine or verify the identity of a person. Examples of biometric technologies include fingerprint, facial, iris, hand geometry, voice, and keystroke recognition. As with all security measures, a biometric system is subject to various threats like attacks at the sensor level, replay attacks on the data communication stream and attacks on the database [1]. This paper will focus on countermeasures to attacks at the sensor level of fingerprint biometric systems or spoofing, the process of defeating a biometric system through an introduction of a fake biometric sample or, worst case, a dismembered finger. Liveness detection, i.e. to determine whether the introduced biometric is coming from a live source, has been suggested as a means to circumvent attacks that use spoof fingers.

2. Background

Previous work has shown that it is possible to spoof a variety of fingerprint technologies through relatively simple techniques. These include utilization of latent fingerprints on the scanner with pressure and/or background materials (e.g., a bag of water), molds created from casts of live fingers, and molds from casts made from latent fingerprints lifted from a surface and reproduced with photographing etching techniques [2] - [7]. Casts have been made from wax, silicon and plastic, and molds from silicon or gelatin (gummy finger) [4], [5].

Our laboratory has demonstrated vulnerability to spoofing using dental materials for casts and Play-Doh for molds [6], [7]. Furthermore, we have tested fingerprint scanners with cadaver fingers. In our testing, ten attempts were performed for all available security levels for optical, capacitive AC, capacitive DC, and electro-optical technologies [6]. Results showed that the spoofing rate for cadaver fingers was typically 90% when verified against an enrolled cadaver finger, whereas for Play-Doh and water-based clay, results varied from 45-90% and 10-90%, respectively, when verified against an enrolled live finger. This research demonstrated that water-based casting materials and cadaver fingers are able to be scanned and verified for most fingerprint scanner technologies. Example images from live, cadaver and spoof fingers, obtained using commercially available fingerprint sensor technologies, are shown in Fig. 1.

In order to avoid spoof attacks of fingerprint biometric systems, various liveness countermeasures have been considered including thermal sensing of finger temperature [8], laser detection of the 3-D finger surface and pulse [9], pulse oximetry [8], [10], ECG [8], and impedance and electrical conductivity of the skin (dielectric response) [11]. Other techniques which can make spoofing more difficult include challenge response, use of passwords, tokens, smart cards, and multiple biometrics. Summaries of liveness and anti-spoofing methods are given in [6], [12], [13]. Most methods require additional hardware which is costly and, unless integrated properly, may be spoofed with an unauthorized live person. In addition, most previously developed methods are not available commercially and/or have not been tested rigorously in order to determine their effectiveness.

Previously, we have developed an anti-spoofing method which is based on a time-series of fingerprint images captured from a DC capacitance-based Si CMOS fingerprint scanner [7]. The method

uses the physiological process of perspiration to determine the vitality of a fingerprint. The initial algorithm extracted the grey levels along the ridges to form signals, calculated a set of features, and used a neural network to perform classification. The training and test sets were formed from 18 live, 18 spoof, and 18 cadaver fingerprints. Results gave 100% precision for distinguishing between fingerprints collected from live and spoof/cadaver fingers. While these initial results were encouraging, they also raised a number of issues, which, if adequately addressed would aid in the assessment of the viability of the approach. These include the performance of the techniques across a more diverse population, the contraction of the time series data to achieve user transparency of the technique, and the applicability of the approach to other fingerprint sensor technologies.

In this paper, we present results of the extension of this initial study which addresses these issues. Section 3.1 discusses the collection of a larger, more diverse dataset which includes 33 live, 30 spoof (based on the 30 live individuals), and 14 cadaver fingers for each scanner. Section 3.2 describes the perspiration detection algorithm which was expanded as part of this work to include new features and new classification techniques. The classification techniques used are described in Section 3.3 while Section 4 gives the vitality detection results for optical, electro-optical, and DC capacitive sensor devices for time series of two and five seconds as well as their statistical analysis. These results are discussed in section 5 and the emergence from the data of device dependent feature sets are noted as a potential avenue for further improvement in this vitality based countermeasure to fingerprint system spoofing.

3. Methods

3.1 Data collection

Three types of fingerprint scanner technologies were used in this study: capacitive DC (Precise Biometrics, 100sc), electro-optical (Ethentica, Ethenticator USB 2500), and optical (Secugen, EyeD hamster model #HFDUO1A). These systems were selected based on considerations of technology diversity, availability and flexibility of the software developer kit (SDK), and ability to readily access and construct a time series of sensor raw images. For each device, fingerprint images were collected from live, spoof, and cadaver fingers. Protocols for data collection from the subjects were followed that were approved by the West Virginia University Institutional Review Board (IRB) (HS#14517 and HS#15322).

Thirty-three volunteers were solicited and represented a wide range of ages (20-60 years), ethnicities, and both sexes (17 men and 16 women). Each subject was asked to enroll (up to five times), verify (six times), and create a cast for generation of spoofs (described below). Two live subjects were excluded in two devices and three in another device due to inability to enroll, a technical error or time constraint. Three subjects in the spoof category were excluded because a spoof cast was not created because of subject time constraints or quality of spoof cast. Table 1 summarizes the number of subjects used for each device and category. A time-series of twenty fingerprint images was collected for each subject and device using customized programs developed with manufacturer-provided SDK functions. The images utilized in this paper are the first image and images from approximately two seconds and five seconds after the start of the time-series collection. To generate spoof fingerprint images, finger casts were created from thirty subjects who participated in generation of the time series of live fingerprint images. Dental impression materials of two types were used, (i) name: Aquasil Easy Mix Putty Smart Wetting Impression Material, content: Quadrafunctional Hydrophilic Addition Reaction Silicone (having very high viscosity, high consistency) manufacturer: Dentsply Caulk [14] and (ii) Extrude, content: polyvinylsiloxane impression material (having medium consistency-medium bodied) manufacturer: Kerr [15]. These dental impression materials formed the cast and Play-Doh was used to form the mold. A time-series capture of the Play-Doh spoof fingers was captured similar to the live fingers. Fourteen cadaver fingers (from 4 subjects, of male age 41, female ages 55, 65, and 66) were collected in collaboration with the Musculoskeletal Research Center (MSRC) at the West Virginia University Health Science Center, creating the time-series of cadaver fingerprint images. Only the fingerprint images which were able to enroll were considered for study. Six cadaver fingers were excluded from capacitive DC because of failure to enrollment. One cadaver finger was excluded from the electro-optical device because of technical difficulties with the scanner (Table 1). Examples of the time-series of live, spoof, and cadaver fingerprint images are shown in Fig. 2.

3.2 Perspiration Detection Algorithm

The basis for our original method and details of the algorithm are discussed in detail in [7]. In brief, when in contact with the fingerprint sensor surface, live fingers, as opposed to cadaver or spoof, demonstrate a distinctive spatial moisture pattern which evolves in time due to the physiological

perspiration process. Optical, electro-optical, and solid-state fingerprint sensors are sensitive to the skin's moisture changes on the contacting ridges of the fingertip skin. These sensors can capture the time dependent, spatial pattern (Fig. 2). To quantify the perspiration phenomenon, our algorithm maps a 2-dimensional fingerprint image to a "signal" which represents the gray level values along the ridges (Fig. 3). Variations in gray levels in the signal correspond to variations in moisture both statically (on one image) and dynamically (difference between consecutive images). The static feature measures variability in gray level along the ridges due to the presence of perspiration around the pores. The dynamic features quantify the temporal change of the ridge signal due to propagation of this moisture between pores in the initial image relative to image captures two (or five) seconds later.

The basic steps performed in the algorithm are described as follows. For more information, please refer to [7]. First, two fingerprint images are captured within a 2 (or 5) second interval (referred to as first and last capture). The results are enhanced by having the subjects wipe their fingers immediately before capture. The captured images are binarized and thinned to locate the ridges. Ridges that are not long enough to cover at least 2 pores are discarded. Using the thinned ridge locations as a mask, the gray levels of the original image underneath these ridge paths are recorded. The resulting signals for the first and the last capture are representative of the moisture level along the ridges for a given image in the time series. Fig. 3 illustrates these steps by showing a portion of the ridge signals derived from the first and last captures from a live source along the mentioned mask.

Prior work established and obtained test results from one static and four dynamic measures [7]. The static measure (SM) uses the Fourier transform of the ridge signal from the first image capture and quantifies the existence of active pores through the corresponding spatial frequencies. The four dynamic measures quantify the specific ongoing temporal changes of the ridge signal intensity due to active perspiration. The first dynamic measure (DM1) is the total swing ratio of the first to last fingerprint signal. The second dynamic measure (DM2) is the growth ratio of the minimum to maximum of the first and last fingerprint signal. The third dynamic measure (DM3) is the mean of the differences of the first and last fingerprint signals, and the fourth dynamic measure (DM4) describes the percentage change between the standard deviations of the first and last fingerprint signals.

To increase the robustness of the classification, two additional measures were introduced and are presented here. In the case that the fingerprint signal swings beyond a device's dynamic range (i.e. the device enters cut-off or saturation due to extreme dryness/moisture), the information about the minimums and maximums and their rate of change, utilized in the second dynamic measure, will be lost. These two measures address this by taking advantage of the upper and lower cut off region lengths of the fingerprint signals and converting them into perspiration rates. The equations for the new dynamic measures are given below.

- *Dry saturation percentage change:* This fifth dynamic measure (DM5) indicates how fast the low cut-off region of the ridge signal is disappearing, thus extracting further perspiration rate information from the low-cutoff region:

$$DM5 = \frac{\sum_{i=1}^{m} \delta(C_{1i} - LT) - \delta(C_{2i} - LT)}{0.1 + \sum_{i=1}^{m} \delta(C_{2i} - LT)}$$

  C_{1i} is referring to the i^{th} point (pixel gray level) in the first capture ridge signal. C_{2i} is the same except for that it is for the second capture. i is equal to 1 to the length of the ridge signal (m). m is the same for C_1 and C_2 since the same mask was used for C_1 and C_2. LT is the low-cutoff threshold of the ridge signal ($\min(C_i)$). δ is the discrete delta function. Higher DM5 corresponds to faster disappearance of dry saturation, because the active perspiration raises the baseline of the ridge signal above the low-cutoff region of the sensor. This is an indication of ongoing perspiration. 0.1 is added to the denominator to avoid division by zero.

- *Wet saturation percentage change:* The sixth dynamic measure (DM6) indicates how fast the high cut-off region of the ridge signal is appearing, thus extracting further perspiration rate information from the wet-saturation region:

$$DM6 = \frac{\sum_{i=1}^{m} \delta(C_{2i} - HT) - \delta(C_{1i} - HT)}{0.1 + \sum_{i=1}^{m} \delta(C_{1i} - HT)}$$

C_{1i} and C_{2i} are the same as in DM5. HT is the high-cutoff (saturation) threshold of the ridge signal ($\max(C_i)$). δ is the discrete delta function. Higher DM6 corresponds to faster appearance of moist saturation, because the active perspiration raises the baseline of ridge signal towards the saturation levels of the sensor. This is an indication of ongoing perspiration. 0.1 is added to the denominator to avoid division by zero.

3.3 Classification

One static and six dynamic measures are used as features for classification of images. These measures were obtained from two different time windows of two and five seconds. Classification was performed separately for each time window. Classification of images is divided into live and spoof where spoof fingerprint images include images from Play-Doh spoofs and cadavers. With approximately 75 images for each scanner, 50% of the data was used as a training set and the remaining 50% as the test set for classification. Three classification methods were used: neural networks, discriminant analysis, and One R. One R and neural network classification was performed using the WEKA (Waikato Environment for Knowledge Analysis) software tool [16] that provides different classification techniques for large data sets. Discriminant analysis was performed with R [17] and SAS [18].

For neural network classification, a back propagation algorithm (with momentum 0.2) was used to train the data set with the hidden layer of 4 nodes derived from (attributes + groups)/2) (where there are seven attributes and two groups). Other specifications include a learning rate of 0.3, a nominal to binary filter, and validation threshold of 20.

Discriminant analysis requires that variables represent a normal distribution. Almost all variables were tested for normality with the help of R software tool. Discriminant analysis of two groups was performed using SAS. Discriminant analysis uses pooled variance-covariance matrix of variables for generating a linear combination of variables called discriminant function [19]. The discriminate function separates the two groups. All variables were used as parameters for discriminant analysis.

One R is the most simple classification tree method. It uses ‘one-rule’ to form a single level decision tree [20].The rule tests for each variable and its different values. It enumerates how frequently each class appears for each value of the variable. Then it determines the most frequent class. It creates the

rule and assigns a class for that particular value of variable. Likewise, it forms different rules for different variable values. It computes the error rate for each rule on the training data. Finally it selects the rule with the smallest error rate to classify the groups. In our case, One R classifier with minimum bucket size of 6 was used. It chose the static measure to form a rule for all scanners.

4. Results

Fig. 4 shows the mean of each feature for live and spoof (which includes both cadaver and Play-Doh fingerprint images) for each device. For some features the mean appears graphically different between groups. Further exploratory statistical analysis was performed which showed that the means were statistically different ($p<0.01$) for DM2 and DM5 for capacitive DC, SM, DM2, and DM6 for electro-optical, and SM, DM2 and DM5 for optical (as indicated by a *).

Figs. 5, 6, and 7 present the classification rate for live and spoof fingerprints for each device and time window. The capacitive DC device demonstrates between 80-93.3% classification for live fingers and 80-95% for spoof fingers, depending on the method and time window. There is little difference in the results for two seconds as compared to five seconds. For the electro-optical device, 62.5-93.3% classification is achieved for live and 81-100% for spoof. There is a modest improvement in live classification from two to five seconds (62.5-81.3% to 81.3-93.3%), with a smaller increase in spoof classification (81-94.7% to 95.2-100.0%). For optical, classification ranged from 73.3-100% for live and 85.7-95.4% for spoof with a small change for live classification from two to five seconds (73.3-93.8% to 80-100%).

5. Discussion and Future Work

Detection of liveness has been suggested as a means to make spoofing more difficult. For fingerprint recognition, several liveness methods including temperature, pulse, pulse oximetry, and electrocardiogram have been suggested [6], [8]-[12]. The difficulty with these measurements is that they require hardware in addition to the fingerprint scanner to capture these liveness features. This is expensive, bulky, and the liveness technique may be spoofed with a live finger presented in combination with a spoof. Furthermore, proposed liveness methods have not been rigorously tested and evaluated with relation to

impact on statistical measurements like false reject and false accept ratios, user acceptance, universality, and collectability.

The research presented here suggests a new method which detects the perspiration process through a time-series of fingerprint images measured directly from the scanner itself. Using image processing and pattern recognition, fingerprint images captured from live fingers can be separated from those captured from spoof or dismembered fingers. This method relies solely on the underlying fingerprint scanner with the addition of software-based image processing and pattern recognition to make the liveness decision. This method is more difficult to spoof, since the spoof would have to replicate perspiration emanating from the pores and spreading across the ridges. Through this paper and other published work, this method is being evaluated in terms of statistical performance and other biometric characteristics for its appropriateness to be used widely in combination with fingerprint authentication.

The initial version of the algorithm was performed for a DC capacitance scanner with a five second window for eighteen subjects (ages 20-45) [7]. This study expands this research to consider (1) a variety of technologies, (2) a large, more diverse dataset, and (3) a shorter time window. First, results demonstrate that using standard classification tools, algorithms can be created to separate live and spoof/cadaver fingerprint images for optical and electro-optical technologies, in addition to DC capacitance. Second, in collection of the dataset, a variety of age groups (11 people between ages 20-30 years, 9 people between 30-40, 7 people between 40-50, and 6 people greater than 50), ethnicities (Asian-Indian, Caucasian, Middle Eastern), and approximately equal numbers of men and women were chosen. While in this small dataset, it is impossible to consider these groups separately, the dataset presents a diverse set of fingers and therefore begins to consider potential problems (dry finger, saturated finger, ridge variations, etc.). Even with this diversity, we were able to achieve approximately 90% classification considering standard pattern recognition algorithms and a common set of features. Third, the original algorithm utilized a five-second time window to show feasibility of the concept. The results from this paper demonstrate that a shorter time window of two seconds achieves similar classification results.

The classification performed here used a standard set of seven features and standard classification routines: neural networks, One R (selection of the best single measure and threshold), and discriminant analysis. Training was performed with images from 15 live subjects and 23 spoof samples. Training was

separate for each device and time window. A device-independent algorithm was not developed due to the large differences in the measurements across devices and since the statistical analysis showed different features having relevance for difference devices. Between the statistical analysis and classification results, a device-specific approach would most likely be the most successful for classification. That is, different measures have varying effectiveness for different technologies. The future direction of this research will be to further explore the features and to develop additional features which provide the best classification for each of the device types.

While this study begins to address some of the limitations of the original work, more data is needed for further verify that this phenomenon is applicable across the population. Potentially, subjects having dry and overly moist fingers may receive a false rejection. Environmental testing will be necessary to demonstrate applicability to a wide variety of settings. Second, while reasonable classification is achieved for a variety of devices using a common set of features, it is necessary to consider each device separately to expand and fine-tune the features and algorithms for each device. This could potentially improve classification performance. Third, features are averaged across the entire fingerprint image. Targeting areas of the image that are changing due to perspiration may improve the separation of live and spoof measurement. Lastly, in this method the fingerprint image is converted to a ridge signal. While effective in pinpointing the parts of the image which are most effected by perspiration, image processing techniques may provide enhanced features, particularly considering the entire area around the pores, and therefore improving classification.

6. Conclusion

This paper describes a unique method to determine liveness through measurement of perspiration process in the finger. Results are presented which improve upon past reports by decreasing the time needed to make the decision and demonstrating its applicability to a variety of fingerprint sensor technologies. A diverse subject population was tested and ~90% classification rate for all scanners was achieved. The method is totally software based and no additional hardware is required. Application of this liveness method can increase the difficulty of spoof attacks for fingerprint scanners.

References

1. N. K. Ratha, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol.40, no. 3, pp. 614-634, 2001.

2. L. Thalheim, and J. Krissler, "Body check: biometric access protection devices and their programs put to the test", *c't magazine*, November 2002.

3. D. Willis, and M. Lee, "Biometrics under our thumb", *Network Computing*, June 1, 1998.

4. T. van der Putte, and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications*, Kluwer Academic Publishers, pp. 289-303, 2000.

5. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems", *Proceedings of SPIE*, vol. 4677, January, 2002

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

7. 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.

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. Kurt Seifried, "Biometrics - What You Need to Know," Security Portal 10 January 2001 (http://www.securityportal.com/closet/closet20010110.html).

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. V. Valencia and C. Horn, "Biometric Liveness Testing," in *Biometrics*, J. D. Woodward, Jr., N. M. Orlans, R. T. Higgins, Ed., Osborne McGraw Hill, New York, to be published.

13. Liveness Detection in Biometric Systems, International Biometric Group white paper, Available at http://www.ibgweb.com/reports/public/reports/liveness.html.

14. DENTSPLY International, York, PA http://ww.dentsply.com.

15. Kerr Dentistry, Orange, CA, http://www.kerrdental.com.

16. WEKA software, The University of Waikato, http://www.cs.waikato.ac.nz/ml/weka/

17. R software, http://www.r-project.org.

18. SAS Insititue Inc., SAS Campus Drive, North Carolina 27513.

19. W. R. Dhillon and M. Goldstein, *Multivariate Analysis Methods and Applications*, Wiley-Interscience, 1984.

20. I. H. Witten and E. Frank, *Data Mining Practical Machine Learning Tools and Techniques with Java Implementations*, Morgan Kaufmann, 1999.

Biographies

1. **Sujan T.V. Parthasaradhi**. was born in Ahmedabad, India. He received his B.S. in Electronics and Communications from Jawaharlal Nehru Technological University, Hyderabad, India. He is currently a graduate student in Lane Department of Computer Science and Electrical Engineering at West Virginia University. His research interests include communications and biometrics.

2. **Reza Derakhshani** was born in Shiraz, Iran. He received his B.S. in Electronics Engineering from Iran University of Science and Technology,Tehran, Iran, and his M.S.E.E. from West Virginia University. He is currently a PhD candidate in Computer Engineering and a Lane Fellow at the Lane Department of Computer Science and Electrical Engineering at WestVirginia University, and an Adjunct Lecturer at Georgetown University. Mr.Derakhshani's research interests include Neural Networks and Biometrics. He is also a member of the IEEE Computer, Neural Network, and EMB societies.

3. **Dr. Lawrence A. Hornak** is a professor in the Lane Department of Computer Science and Electrical Engineering at WVU. He has B.S. in Physics from Binghamton University an M.E. from Stevens Inst. of Technology a Ph.D. in Electrical Engineering from Rutgers. Prior to joining WVU in 1991, he spent nine years at AT&T Bell Laboratories, Holmdel, NJ. At WVU, Dr. Hornak received an NSF National Young Investigator Award in support of his work in mixed technology systems. He currently directs the multiuniversity Center for Identification Technology Research (CITeR), an NSF Industry/University Cooperative Research Center. His primary research explores photonic MEMS, semiconductor and integrated optical devices, and physiological and molecular biometric sensors and systems. Dr. Hornak has completed one edited book, several book chapters, and has over 80 journal and conference papers. He is a member of the IEEE, OSA, and SPIE.

4. **Dr. Stephanie Schuckers (M '95**) was born in Lincoln, Nebrasksa. She received her B.S.E. degree in Electrical Engineering from University of Iowa in 1992, a M.S.E. and the Ph.D. in Electrical Engineering: Systems from University of Michigan in 1994 and 1997, respectively. She was an assistant professor at West Virginia University for five years and is currently at Clarkson University, Potsdam, New York. Her current research interests are signal processing and pattern recognition for a variety of biomedical applications, including biometric devices, implantable defibrillators, sudden cardiac death, and sudden infant death syndrome. She has published over twenty journal papers, conference papers, and book chapters. She was Region 2 representative to the administrative committee for IEEE Engineering Medicine and Biology Society for two years.

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

	Capacitive DC	**Electro-Optical**	**Optical**
Live	31	30	31
Spoof	30	30	30
Cadaver	8	13	14

LIVE IMAGE **CADAVER IMAGE** **SPOOF IMAGE**

Fig. 1. Images captured with commercial fingerprint sensors from live, cadaver and spoof fingers.

Live:

0 sec **2 sec** **5 sec**

Spoof:

0 sec **2 sec** **5 sec**

Cadaver:

0 sec **2 sec** **5 sec**

Fig. 2. Example fingerprint images from live (top), spoof (middle), and cadaver (bottom) fingers captured at 0, 2 and 5 seconds (left to right) after placement on the scanner.

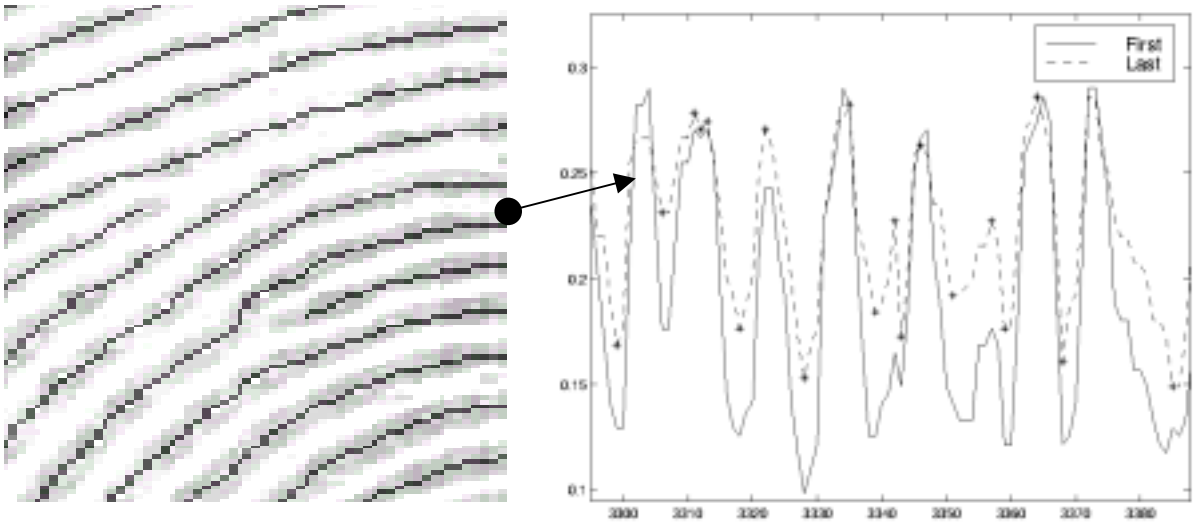

Fig. 3. Ridge mask superimposed over the original grayscale fingerprint image (left) and resulting ridge signal for two image captures, 0 (solid) and 5 (dashed) seconds (right).

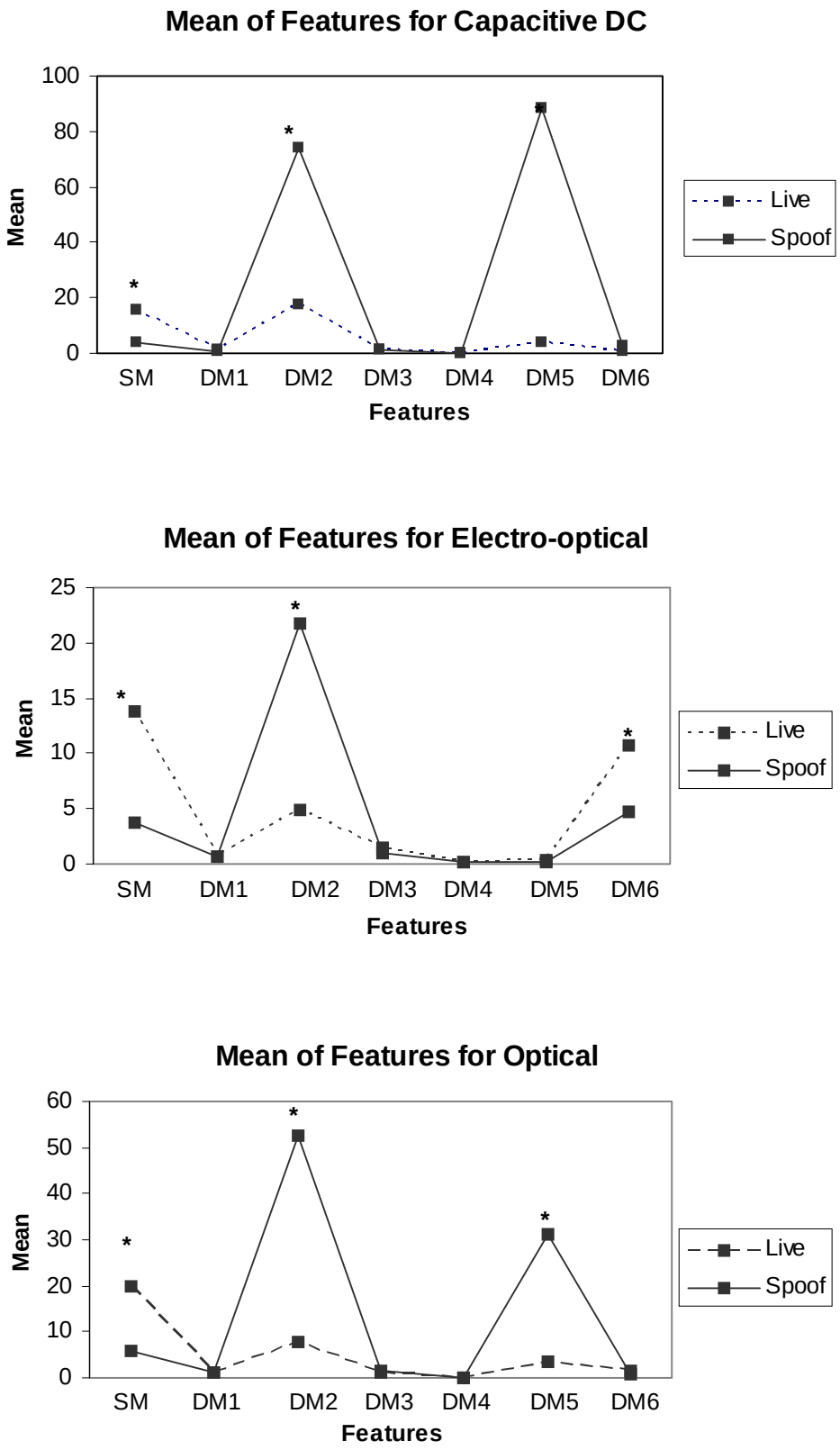

Fig. 4. Mean of each feature for live (dashed) and spoof (solid) for each device, capacitive DC (top), electro-optical (middle), and optical (bottom). * indicates $p<0.01$.

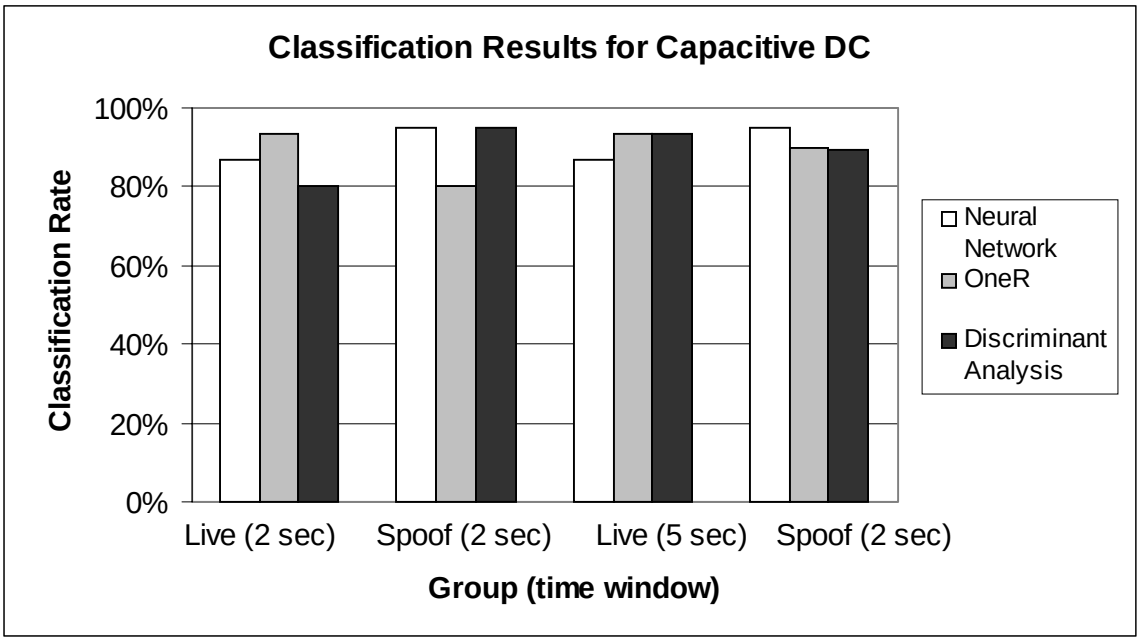

Fig. 5. Classification rates of capacitive DC for live and spoof (2 and 5 second windows) using neural network, One R, and discriminant analysis classification techniques.

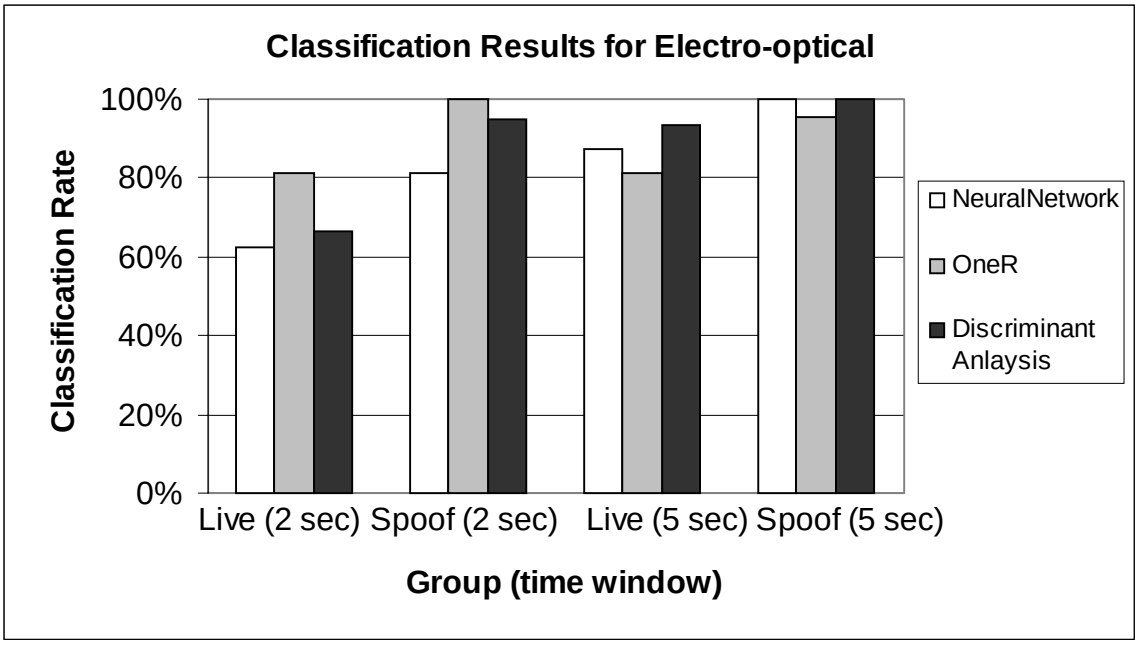

Fig. 6. Classification rates of electro-optical for live and spoof (2 and 5 second windows) using neural network, One R, and discriminant analysis classification techniques.

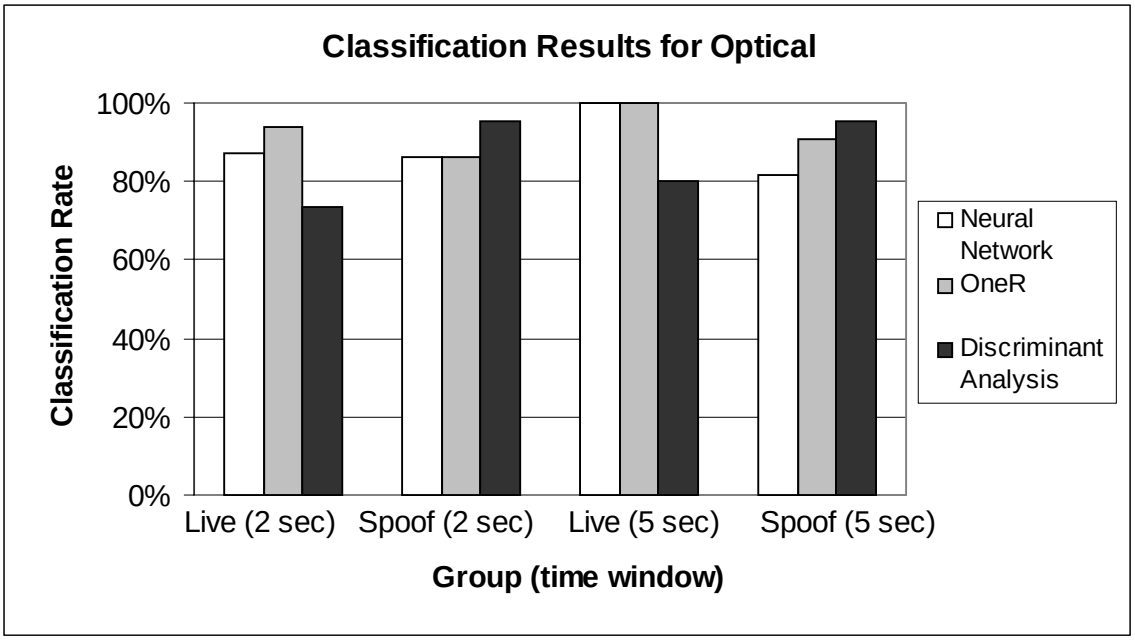

Fig. 7. Classification rates of optical for live and spoof (2 and 5 second windows) using neural network, One R, and discriminant analysis classification techniques.