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

Stephanie Schuckers, Ph.D. [1, 2]

Lawrence Hornak, Ph.D. [1]

Sujan Parthasaradhi[1]

Reza Derakhshani[1]

[1]Clarkson University

[2]West Virginia University

CITeR

Center for Identification Technology Research

An NSF Industry/University Cooperative Research Center (IUCRC) in the area of Biometrics

West Virginia University
Michigan State University
Clarkson University
St. Lawwrence University
University of Pittsburgh
http://www.csee.wvu.edu/citer

Introduction

- Biometric devices are prone to attacks on the system.
- Attacks are possible through artificially created biometrics, input ports and databases.
- This research focuses on countermeasures to attacks at the sensor level of fingerprint biometric systems or spoofing.
- Spoofing – the process of of defeating a biometric system through an introduction of a fake biometric sample or worst case, a dismembered finger.

Spoof-Attack Protection

- Supervision of verification, in addition to enrollment
- Challenge-response
- Addition of smart card, password, etc.
- Liveness detection based on recognition of physiological activities as signs of life.
  - thermal sensing of finger temperature
  - laser detection of 3d finger and pulse
  - pulse oximetry
  - ECG
  - Impedence electrical conductivity of skin

Introduction

- Two phases to research:
  - Study of spoofing vulnerability in fingerprint scanners.
  - Development and evaluation of a new liveness method based on perspiration changes in the fingerprint image.

Spoofing

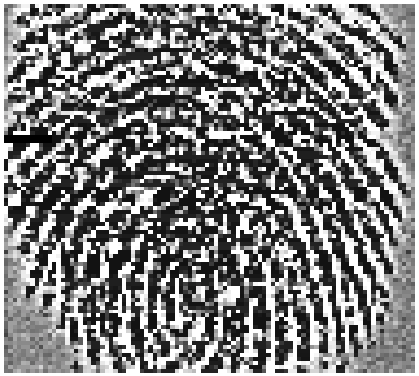
- Techniques used to spoof fingerprint technologies
  - Latent fingerprint on the scanner with pressure
  - Cast made from live fingers, latent fingerprints using wax, silicon, plastic
  - Molds from silicon or gelatin (gummy finger)
- Our laboratory
  - Dental materials for casts
  - Playdoh for molds
  - Cadaver fingers

Capacitive DC (top) & AC (bottom)





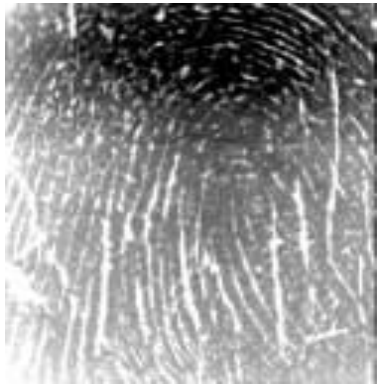





Live Image **Cadaver Image** **Clay Image** **Play-doh Image**

Optical (top) & Optoelectric (bottom)

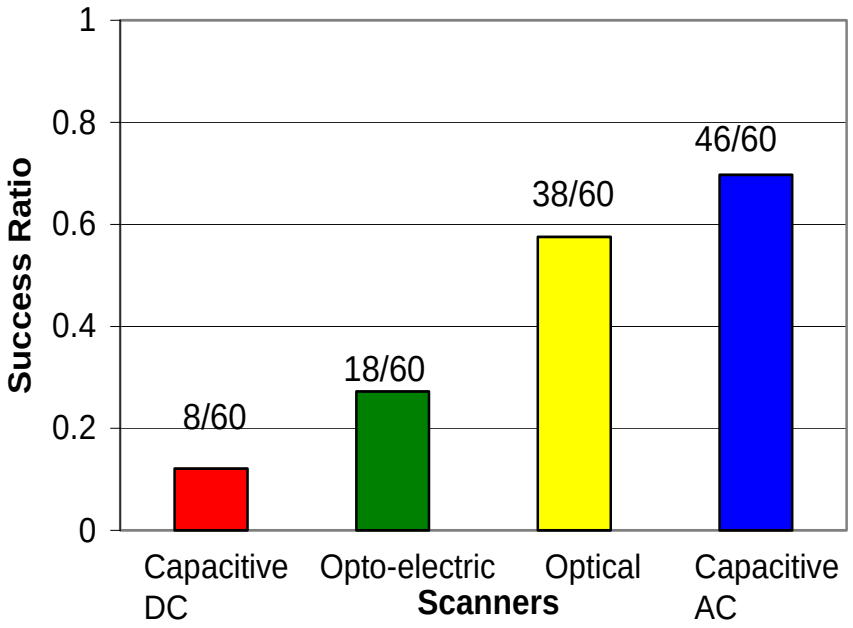




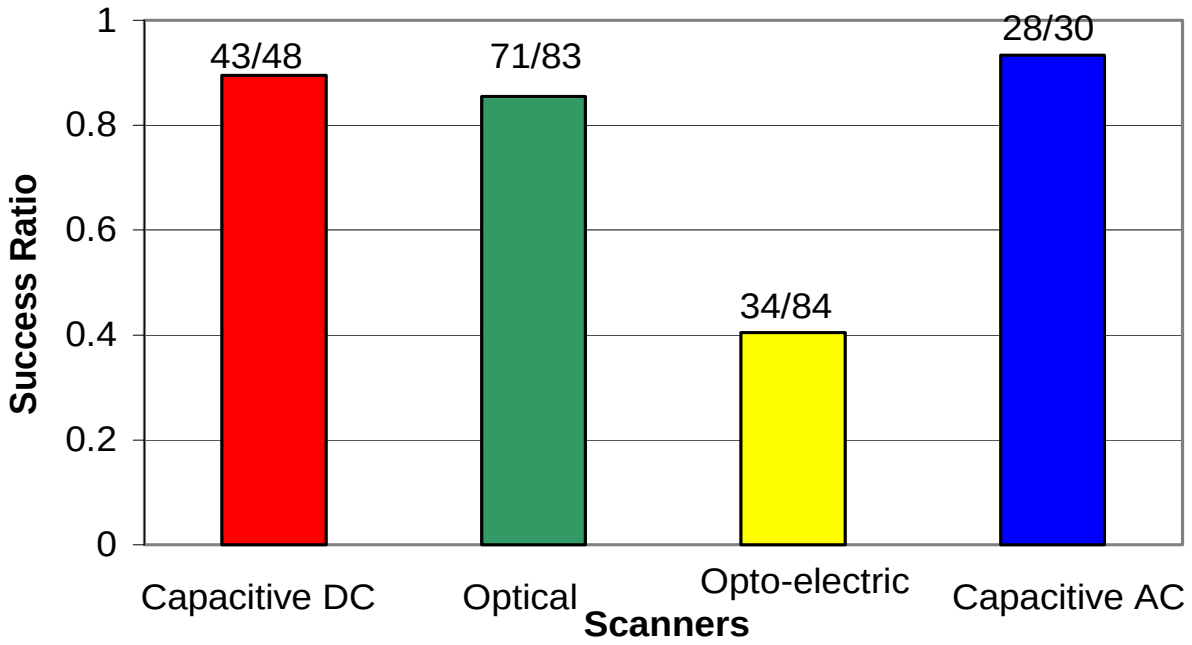

Live Image Cadaver Image Clay Image Play-doh Image

Spoofing Results



- *10 casts from 10 different subjects*
- *Default security level*
- *Enrollment with live finger*
- *Verified six casts for each subject*

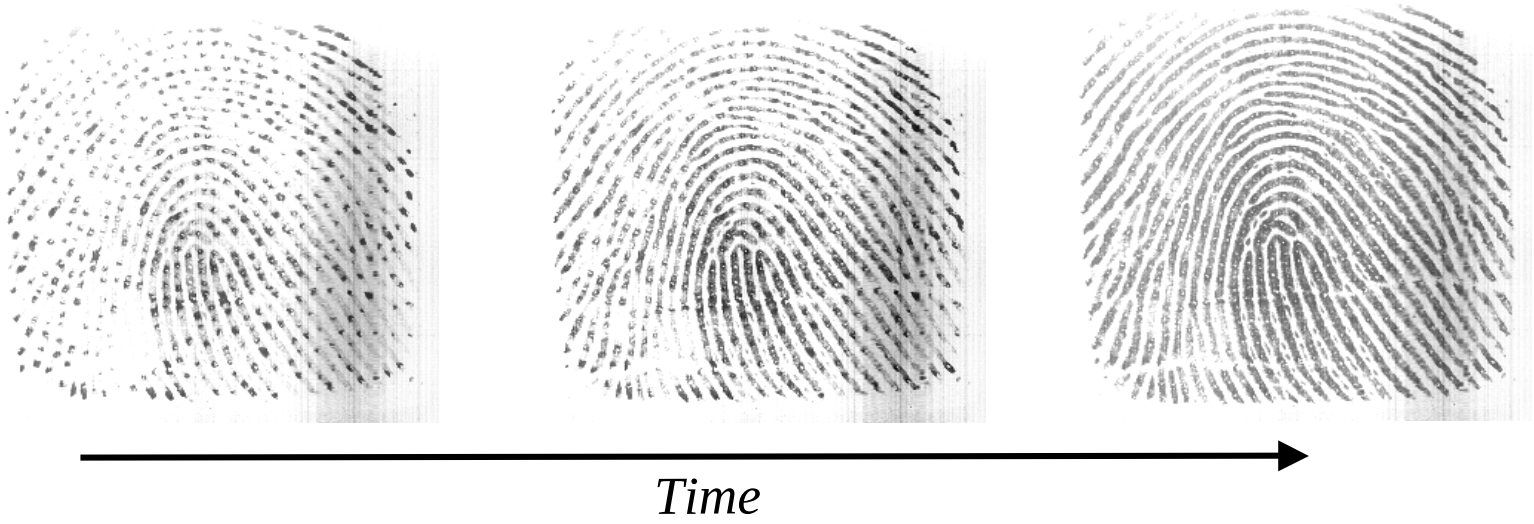
Cadaver Results



- *8 cadaver fingers for Capacitive DC, 14 cadaver fingers for Optical, 13 Cadaver fingers for electro-optical,5 Cadaver fingers for Capacitive AC*
- *Default security level, verification 6 times each*
- *Enrollment and verification with same fingers*

Liveness Detection

- Hypothesis: Live fingers demonstrate a specific changing moisture pattern due to perspiration.
- Cadaver and spoof fingerprint images do not.
- Algorithm uses two fingerprint images over time
- Original algorithm: capacitive DC, 5-second time frame, small dataset



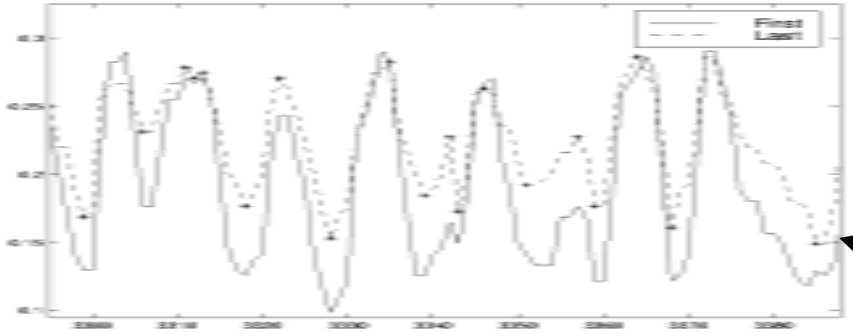
The Algorithm

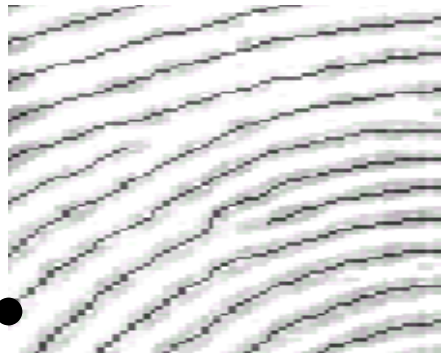
- Process fingerprint images, obtain ridge signals.

- Signal amplitude is proportional to the moisture along the traversed ridges.
- Peaks relate to the moistest and valleys to driest regions.
- In live fingers, perspiration starts around the pores, and spreads along the ridges, creating a distinct signature of the process.

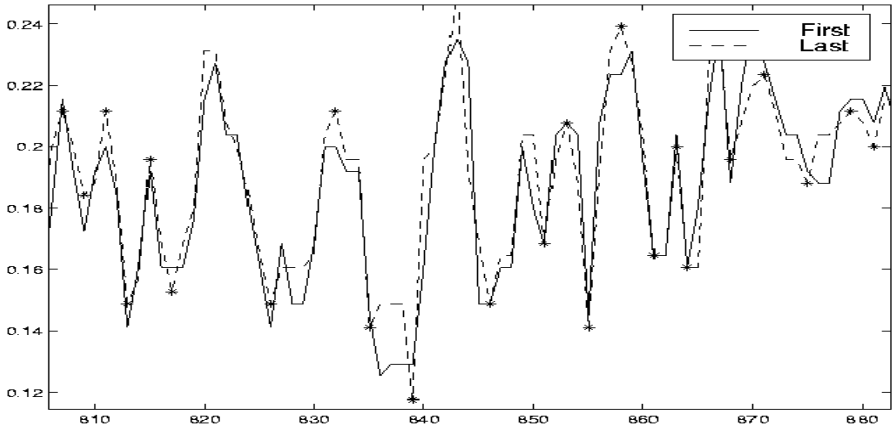
Derived Features

- Fairly constant periodic peaks and rising valleys for live signal.

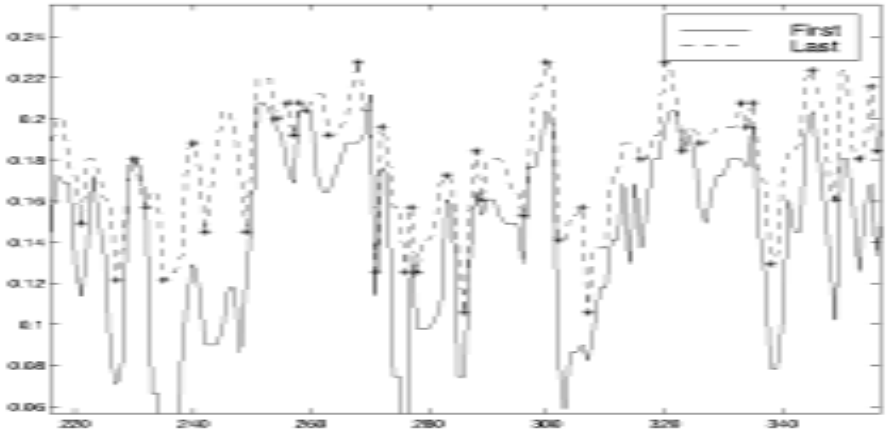




Live Fingerprint Signal



Spoof



Cadaver

Static and Dynamic Measures

Static Measure (SM):

- The energy related to typical pore spacing:

$$SM = \sum_{k=11}^{33} f(k)^2$$

Where n is number of individual strings (Si) in the processed fingerprint mask from last capture

$$f(k) = \frac{\sum_{i=1}^{n} \left| \sum_{j=1}^{256} S_{1i}^{a} \, e^{-j2\Pi(k-1)(i-1)/256} \right|}{n}$$

Dynamic Measures:

- Total swing ratio of first to last fingerprint signal (DM1):

$$DM\ 1 = \frac{\sum_{i=1}^{m} \left| C_{1i} - C_{1\,i-1} \right|}{\sum_{i=1}^{m} \left| C_{2\,i} - C_{2\,i-1} \right|}$$

Dynamic Measures

- Min/Max growth ratio of first to last fingerprint signal (DM2)

$$DM\,2 = \frac{\sum_{j}(C_{2j}^{\min} - C_{1j}^{\min})}{\sum_{k}(C_{2k}^{\max} - C_{1k}^{\max})}$$

- Last-first fingerprint signal difference mean(DM3)

$$DM\,3 = \frac{\sum_{i=1}^{m}(C_{2i} - C_{1i})}{m}$$

- Percentage change of standard deviations of first and last fingerprint signals(DM4)

$$DM\,4 = \frac{SD(C_1) - SD(C_2)}{SD(C_1)}$$

- Dry saturation fraction i.e. how fast the low cut-off region of the ridge signal is disappearing (DM5)

$$DM\,5 = \frac{\sum_{i=1}^{m}\delta(C_{1i} - LT) - \delta(C_{2i} - LT)}{0.1 + \sum_{i=1}^{m}\delta(C_{2i} - LT)}$$

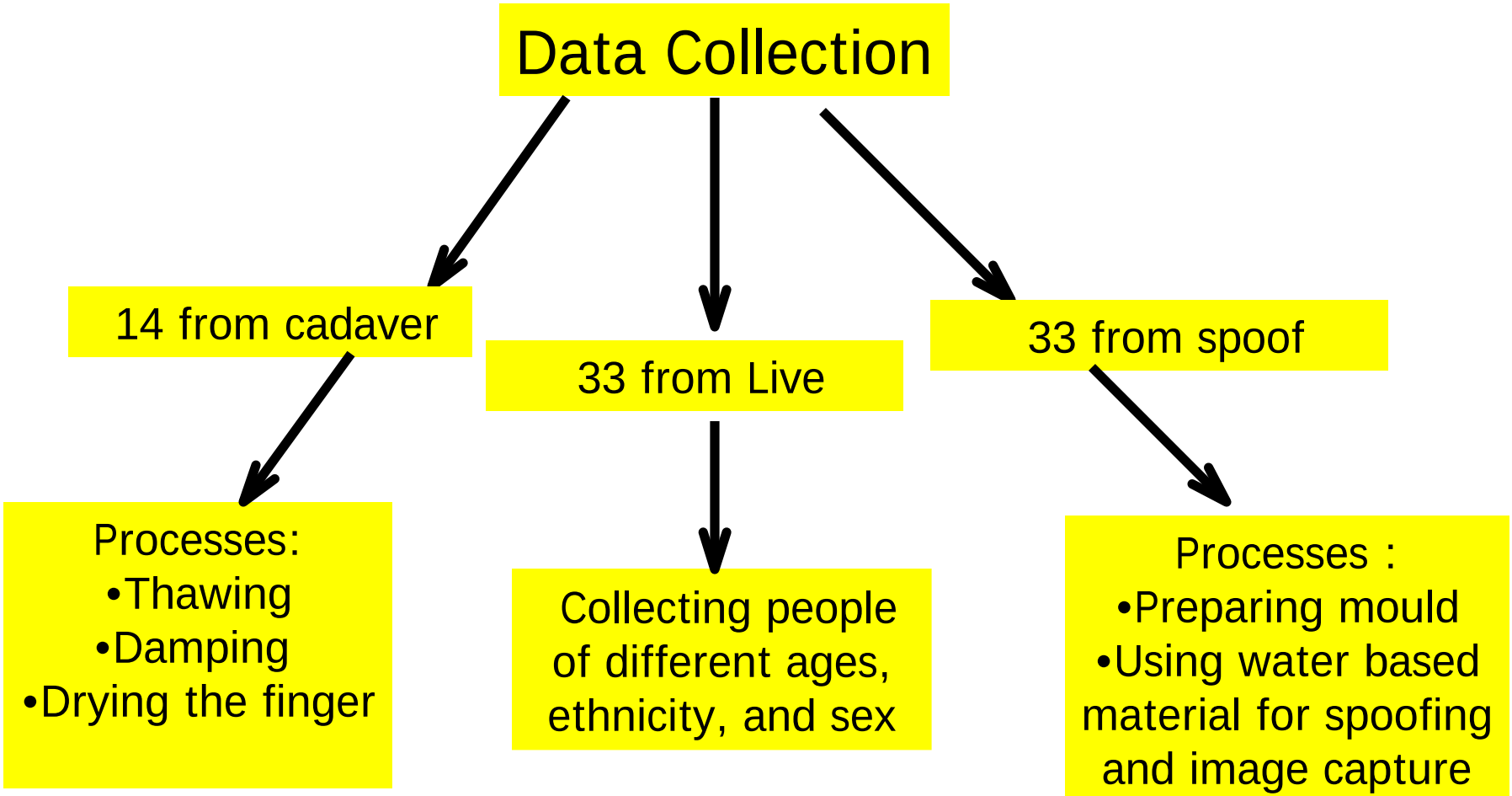
- Wet saturation fraction i.e. how fast the high cut-off region of the ridge signal is appearing (DM6)

$$DM\,6 = \frac{\sum_{i=1}^{m}\delta(C_{2i} - HT) - \delta(C_{1i} - HT)}{0.1 + \sum_{i=1}^{m}\delta(C_{1i} - HT)}$$

New Research

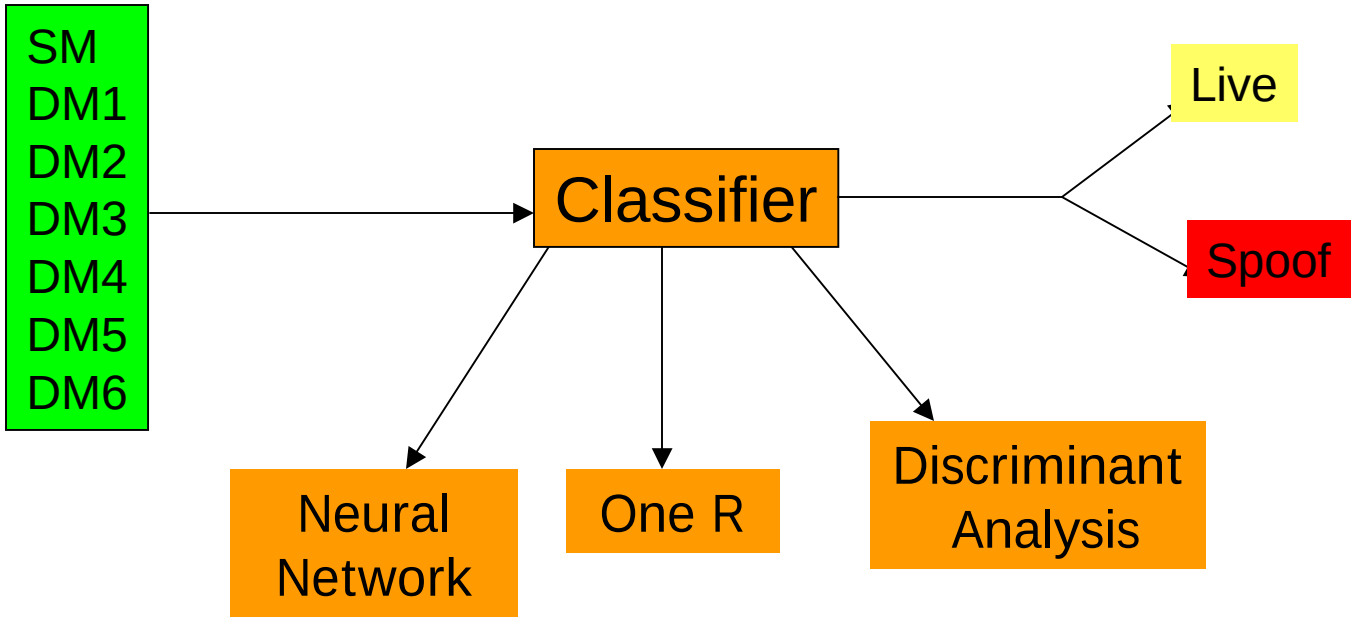
- A diverse data set
  - Approximately equal numbers of men and women
  - Various age groups and ethnicities
- More data
  - Approximately 75 images (30-31 live, 40-44 non-living) for each scanner
- More device technologies
  - Optical (SecuGen)
  - Capacitive DC (Precise)
  - Opto-electric (Ethentica).
- Shorter time window
  - 2 sec
  - 5 sec

Data Collection



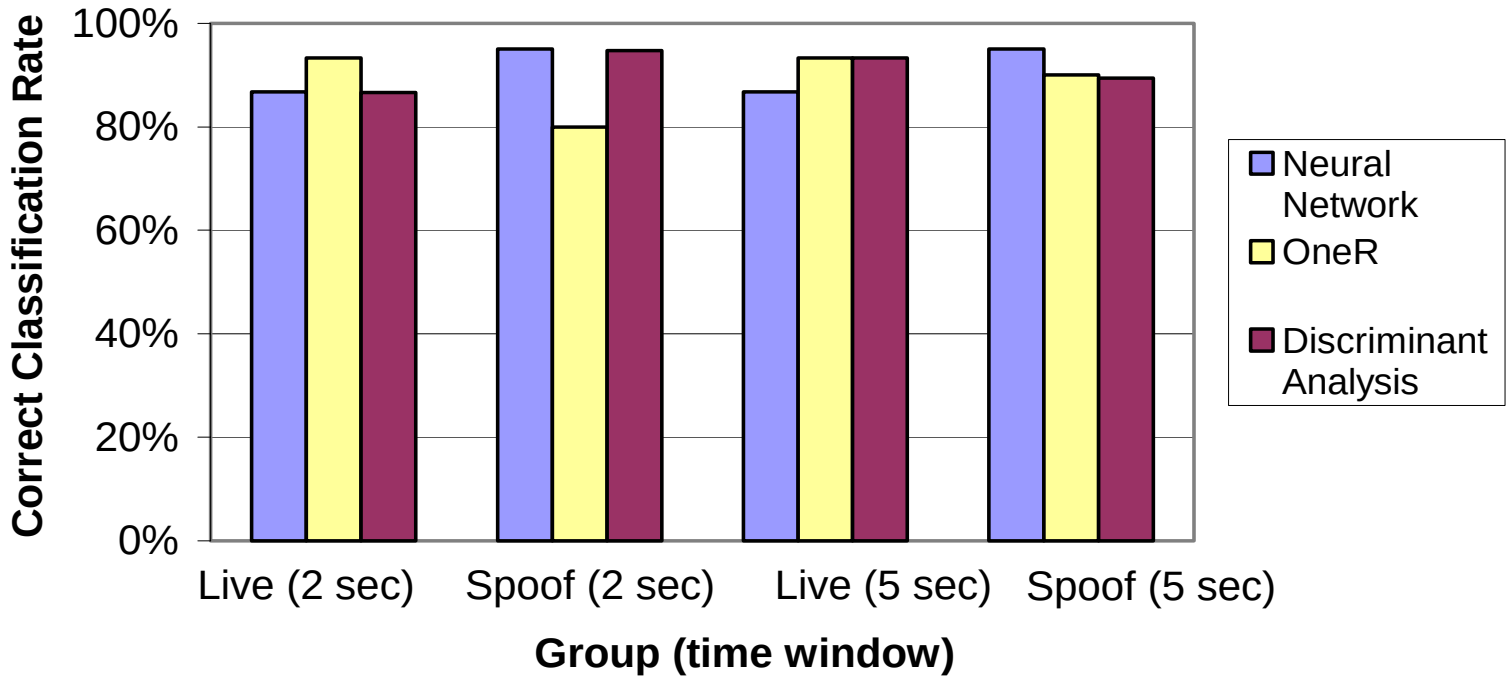
All studies performed at room temperature.

Classification

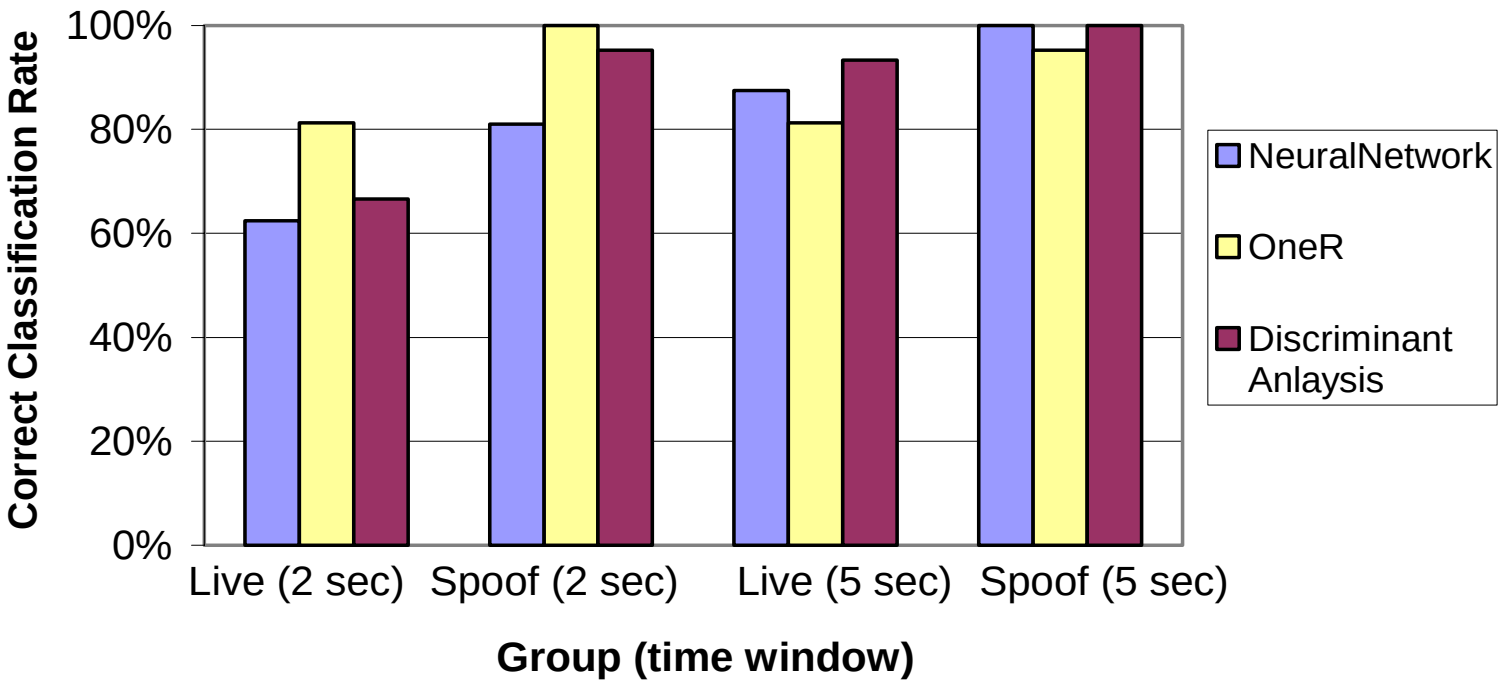


- *50% of the data for training set and 50% for the test set*
- *One R and neural network classification was performed using the WEKA (Waikato Environment for Knowledge Analysis) software tool.*
- *Discriminant analysis was performed with R and SAS tools.*

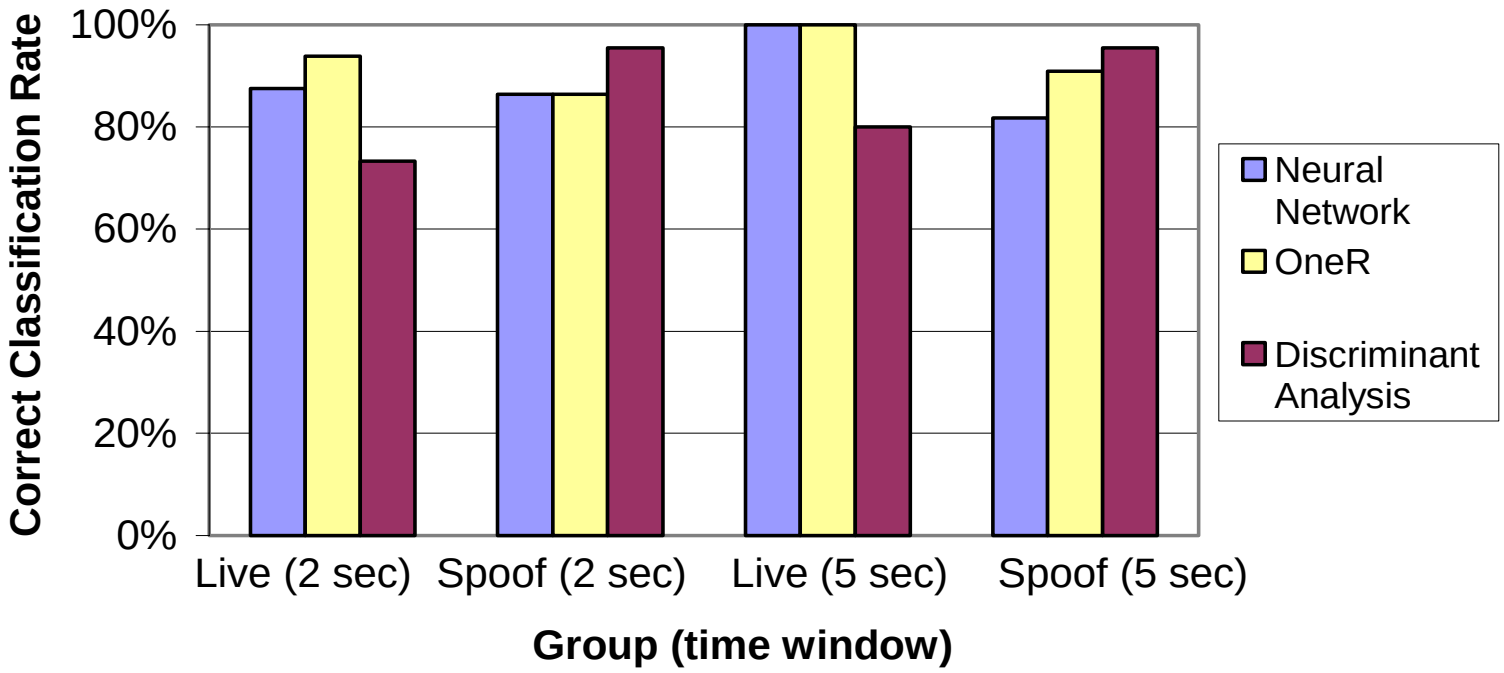
Results for Capacitive DC



Results for Electro-Optical



Results for Optical



Summary Table

Live Classification Table

Device	2 sec	5 sec
Electro-Optical	62.5-81.3%	81.3-93.3%
Optical	73.3-93.8%	80-100%
Capacitive DC	86.7-93.3%	86.7-93.3%

Spoof Classification Table

Device	2 sec	5 sec
Electro-Optical	81-95.2%	95.2-100%
Optical	86.4-95.5%	81.8-95.5%
Capacitive DC	80-95%	89.5-95%

Results

- Perspiration phenomenon seen in capacitive, optical, and opto-electric device technologies.
- Tested on larger, diverse dataset
- Shorter time (2 sec) window possible
- Indications of device specific approach
- Approximately 90% classification achieved for diverse dataset

Conclusion

- This method is totally software based and no additional hardware is required.
- Application of the perspiration based method can provide anti-spoofing protection for fingerprint scanners.