Evaluation of Liveness or Anti-spoofing in Biometric Systems

Stephanie Schuckers, Andy Adler

Bozhao Tan, Aaron Lewicke, Peter Johnson, Joe Sherry, David Yambay, Rachel Wallace, Greta Collins, Dominic Grimberg

Funding provided by National Science Foundation, Dept. of Homeland Security, and the Center for Identification Technology Research (CITeR)

Spoofing

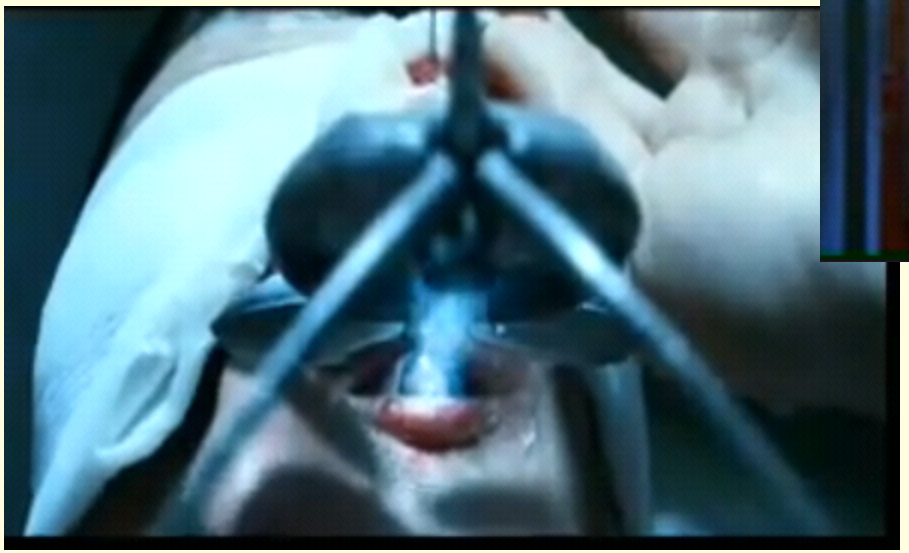
- **Spoofing: "The process of defeating a biometric system through the introduction of fake biometric samples.**
- **Artificially created biometrics:**
  - lifted latent fingerprints
  - artificial fingers
  - image of a face or iris
  - high quality voice recordings
  - worst case—dismembered fingers
- **Famous 'gummy fingers' by Matsumoto 2002**
- **Mythbusters episode in 2007**
- **Spoof attack in early 2009 at Japanese border by a Korean woman**

1 Thalheim, et al, C'T article, 2002.

(a) Live Finger (b) Silicone Finger (c) Gummy Finger

Biometric Spoofing in Popular Media

Cameron Diaz, Charlies Angels

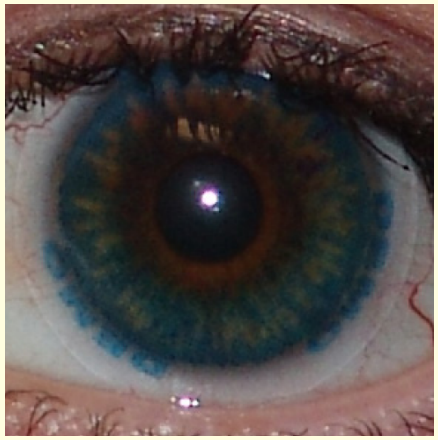


Tom Cruise, Minority Report

Mythbusters, 2007

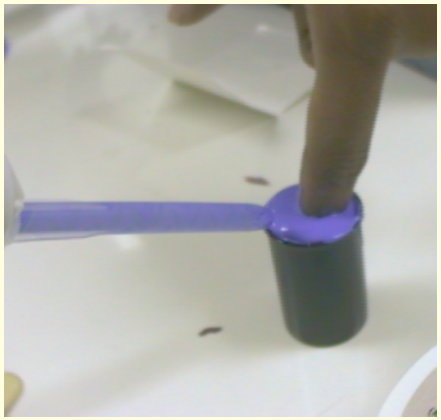
Spoofing versus Obfuscation

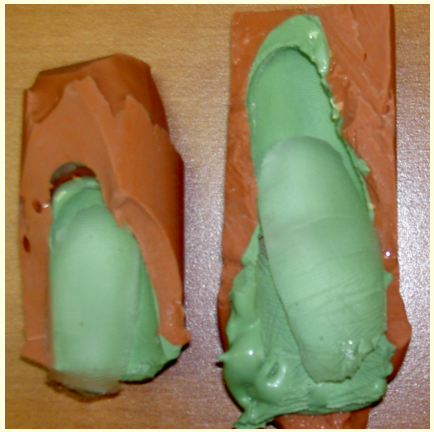
- **Spoofing—posing as another individual**
  - Positive identification applications
- **Obfuscation—hiding your identity**
  - Negative identification applications
  - May form ‘new’ identity for positive identification
  - Mutilation of fingerprint
  - Texture-contact lens to hide iris pattern
  - Theatre makeup/putty to change facial characteristics



Spoofing Techniques in our Lab

- Dental materials for casts
- Cooperative, high quality casts
- Mold made from cast, also termed ‘replica’, ‘spoof’, ‘fake finger’
- Materials for Mold: Play-Doh, gelatin, silicon rubber, paint, caulk, wood glue, paper, latex rubber, paper
- Cadaver fingers



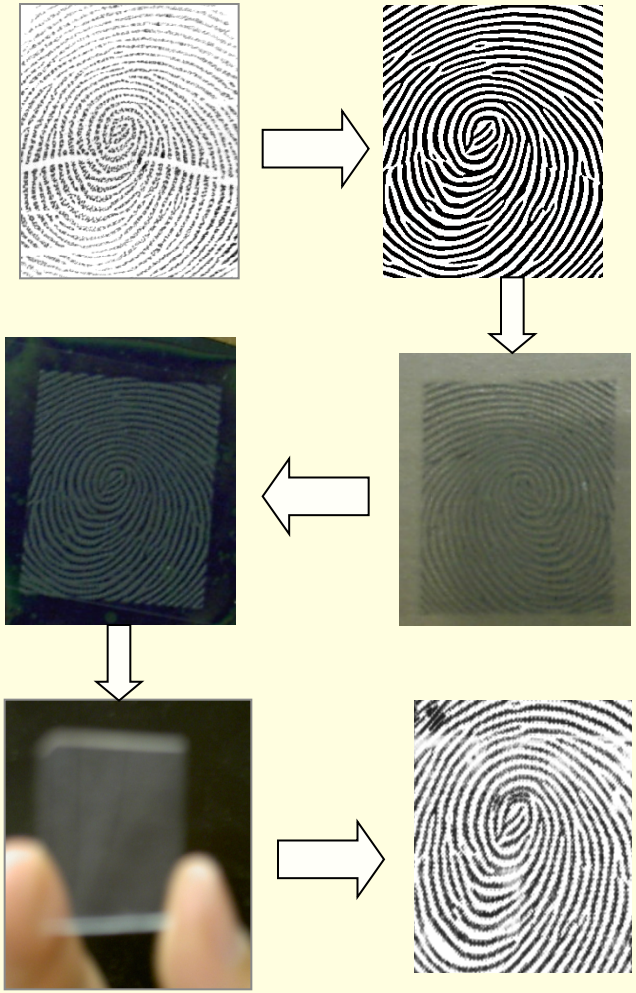


Example Photos of Spoof Fingers and Resulting Images

Caulk Paint Playdoh Silicon

Spoof Techniques in our Lab

- Uncooperative
- Lifted latent print, stolen fingerprint image
- Fingerprint mask generation
- Print on transparent film
- Expose negative photosensitive silicon wafer
- Develop to form cast
- Pour silicone or other liquid material to form mold

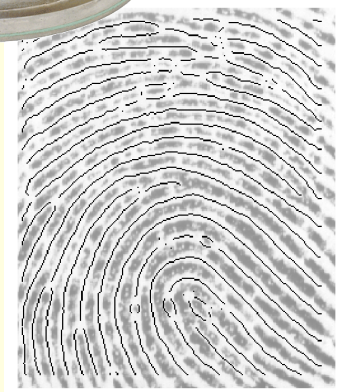


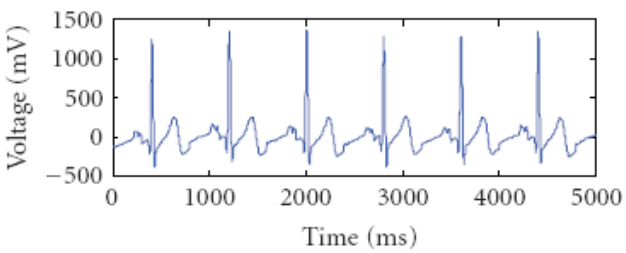
Liveness Detection

- **Also termed**
  - 'Vitality Detection'
  - 'Anti-Spoofing'
- **Definition: to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture**
- **"It is 'liveness', not secrecy, that counts," Dorothy Denning**
  - Your fingerprint is NOT secret.
  - Cannot reasonably expect it to be
  - Therefore, must ensure measurement is of the 'real' biometric and not a replica.
  - True for most other biometrics, with some exceptions to be discussed
- **Typically treated as a two class problem—live or spoof**

Liveness Detection

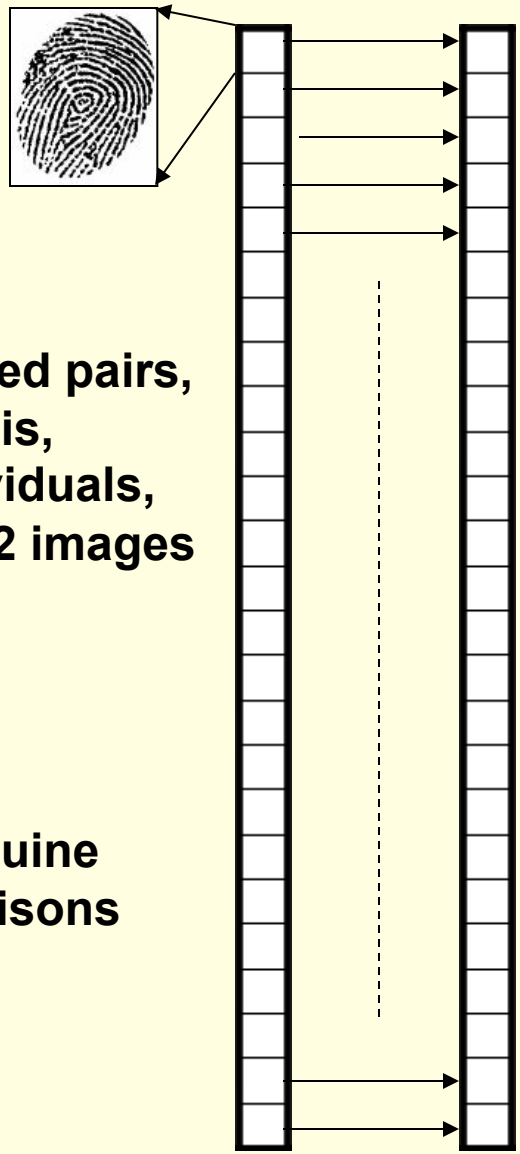
- **Rarely does biometric sensor measure 'liveness', that is, liveness is not necessary to measure the biometric**
- **Hardware-based**
  - Requires specialized hardware design
  - Integrated with biometric sensor
- **Software-based**
  - Uses information already measured from biometric sensor
  - Additional processing needed to make a decision
- **Liveness inherent to biometric**
  - Must be 'live' to measure it, e.g., electrocardiogram





(a) 5 seconds of ECG from subject A

False Reject Rate



100 matched pairs, that is, 100 individuals, each with 2 images

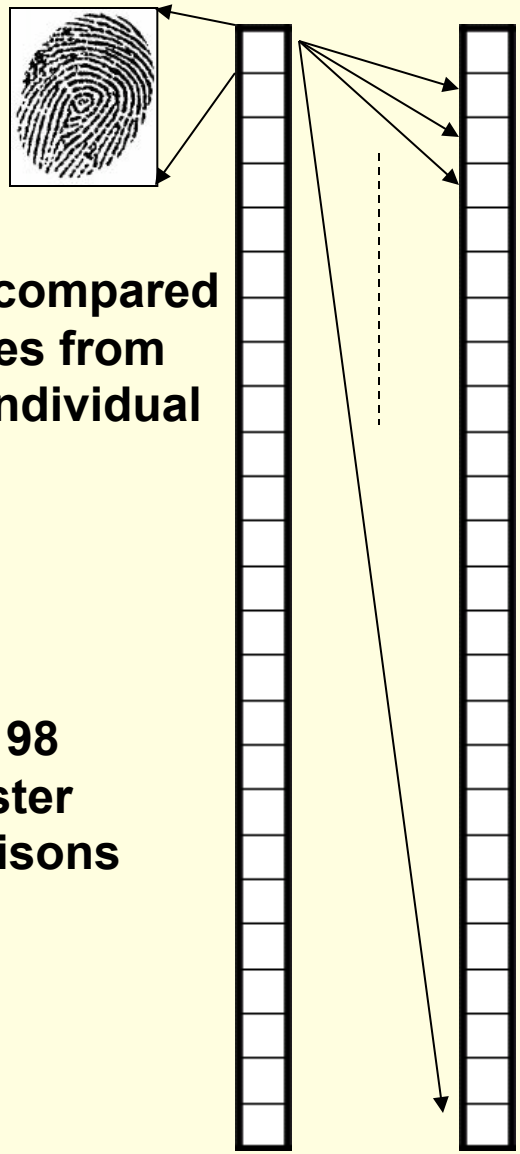
100 genuine comparisons

Matching Algorithm

Truth	Match	Non-Match
Match	99	1
Non Match		

False Reject Rate= $\frac{1}{99+1}$ =0.01

False Accept Rate



Each image compared With images from A different individual

200*198 imposter comparisons

Matching Algorithm

Truth	Match	Non-Match
Match	99	1
Non-Match	10	9990

False Accept Rate= $\frac{10}{10000}$ =0.001

No information regarding false accepts based on deliberate attempts to defeat the system

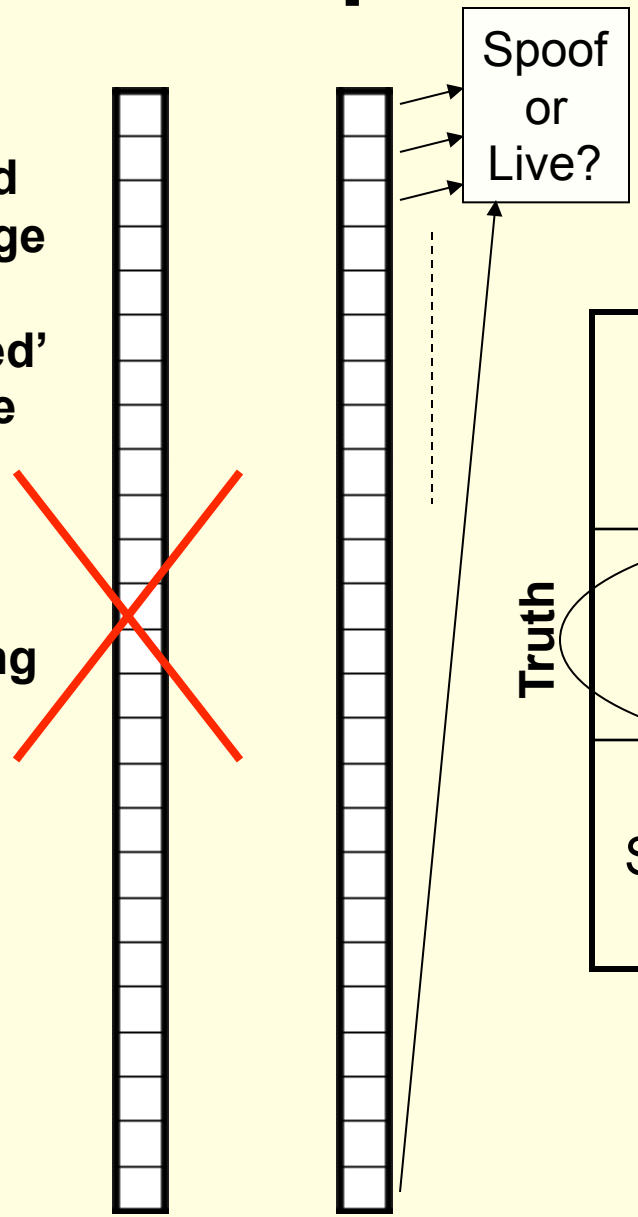
Now Anti-Spoofing--FRR

Typically based On a single image

Assume 'enrolled' fingerprints are live

↓

100 anti-spoofing decisions



Anti-spoofing Algorithm

		Live	Spoof
Truth	Live	90	10
	Spoof		

False Reject Rate= $\frac{10}{90+10}$ =0.1

FRR—Matching and Anti-Spoofing

Matching Algorithm

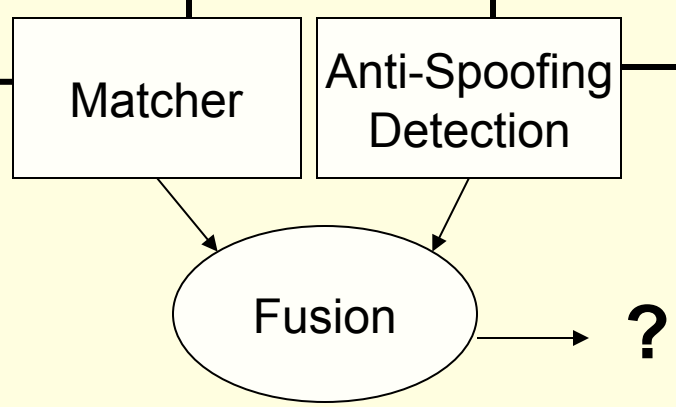
Truth	Match	Non-Match
Match	99	1
Non Match		

False Reject Rate= $\frac{1}{99+1}$ =0.01 (1%)

Anti-Spoofing Algorithm

Truth	Live	Spoof
Live	90	10
Spoof		

False Reject Rate= $\frac{10}{90+10}$ =0.1 (10%)

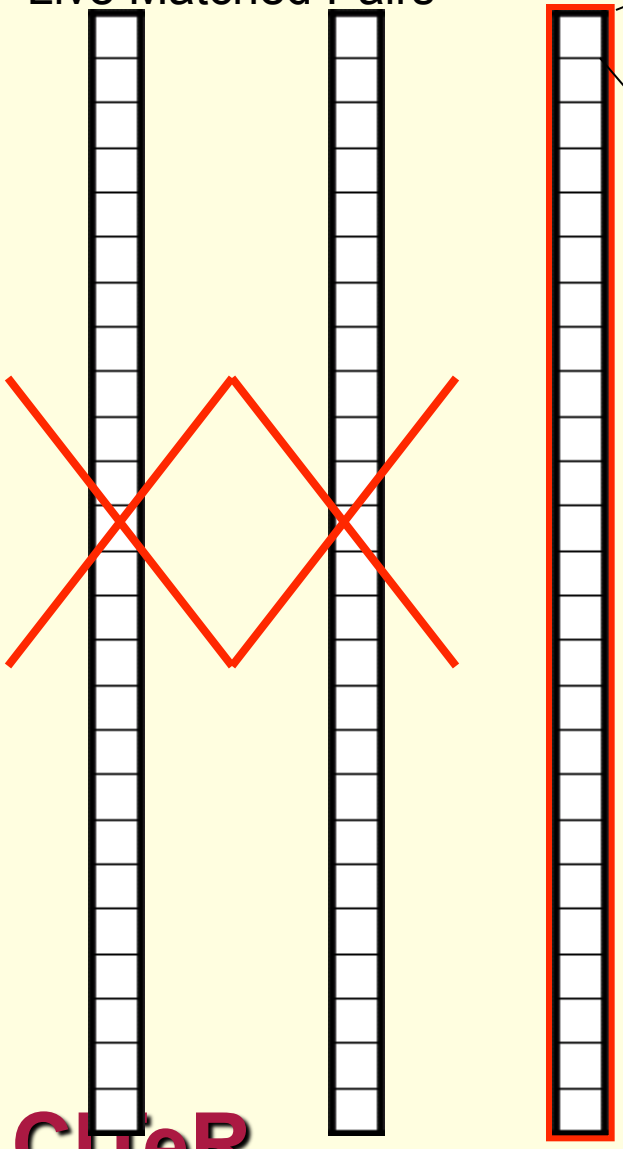


Anti-Spoofing will Impact overall system Performance

? **SystemFRR<=0.11 (11%)**

Now Anti-Spoofing-FAR??

Live Matched Pairs



Spoof images From same individuals

Anti-spoofing Algorithm

		Live	Spoof
Truth	Live	90	10
	Spoof		

How to test? What is performance?
Need spoof dataset.
Need common terminology—
SpoofFAR??

Performance Vocabulary

- **Biometric performance terminology**
  - False reject rate—Error associated with rejecting an ‘genuine’ user
  - False accept rate—Error associated with accepting an un-authorized, ‘imposter’ user
    - Zero-effort attempt—no willful attempt
- **Anti-spoofing terminology**
  - ***Live false reject rate***—similar to above, now anti-spoofing detection algorithm may reject ‘genuine’ authorized user
  - ***Spoof false accept rate***—error associated with accepting the presentation of a spoof
    - Non-zero effort attempt—willful attempt

System Level Performance

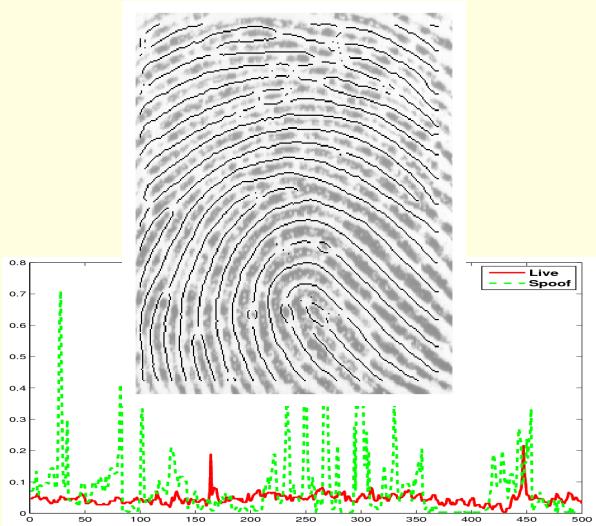
System Performance

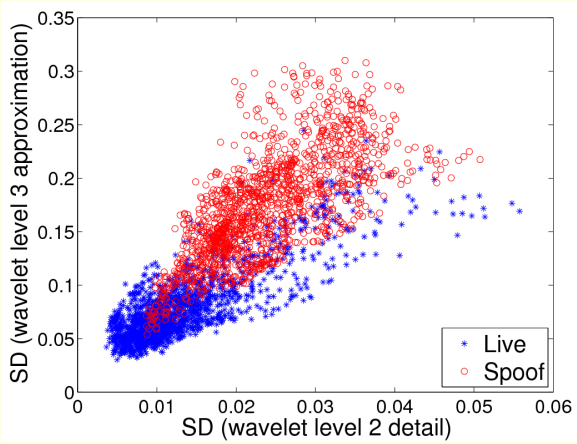
System

Truth	Match Live	Match Spoof	Non-Match Live	Non-Match Spoof
Match Live	Accept	LFRR	FRR	FRR/LFRR
Match Spoof	SFAR	Reject	Poor Quality Spoof---Reject by Matcher	Poor Quality Spoof---Reject by both
Non-match Live	FAR		Reject	
Non-match Spoof	*What do we call the remaining? Do we care?*			Reject

Software-based Fingerprint Liveness Detection

- Live and spoof fingerprint images have distinctive characteristic images.
- Utilizes fingerprint images from device
- Examples
  - Perspiration pattern
  - Ridge/valley characteristics
  - Power spectrum
  - Skin deformation/Elasticity

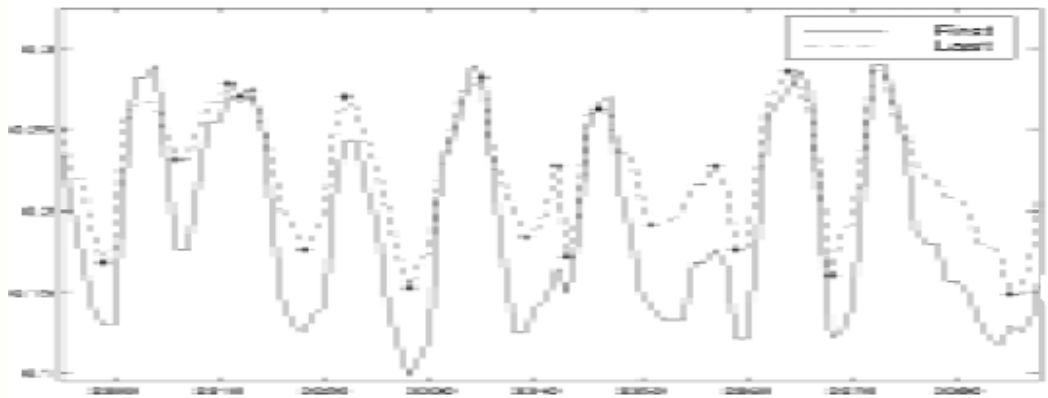




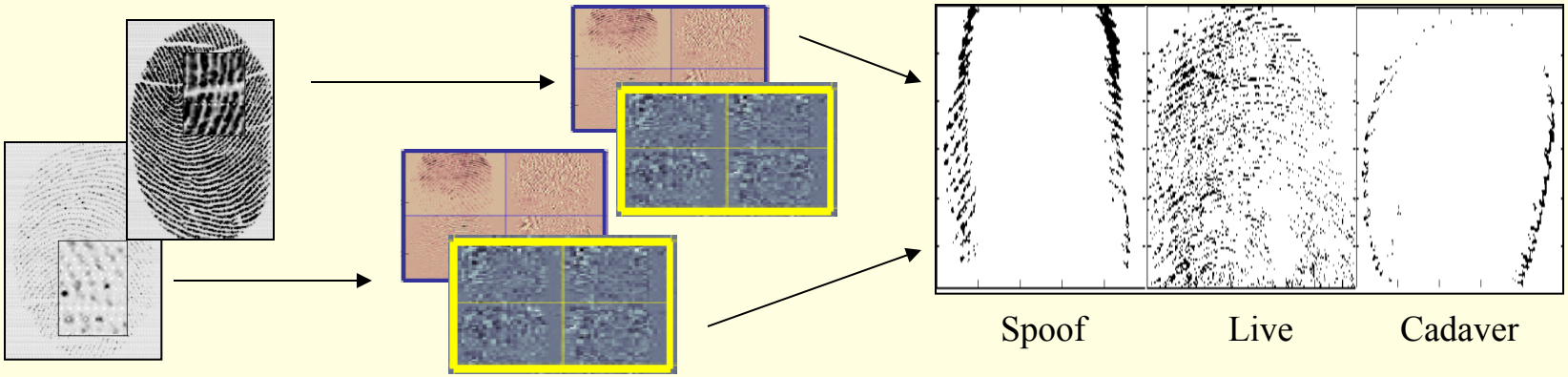
Perspiration Pattern

- Characterizes changes in perspiration pattern
- Two methods: Wavelet Image, Ridge signal changes
- Uses two or more images collected in series
- Published reports use images with minimum time of two seconds

Derakhshani, et al, Pattern Recog, 2003
Parthasaradhi, et al, IEEE SMC, 2005
Abhyankar, et al, SPIE, 2004



Live Fingerprint Signal

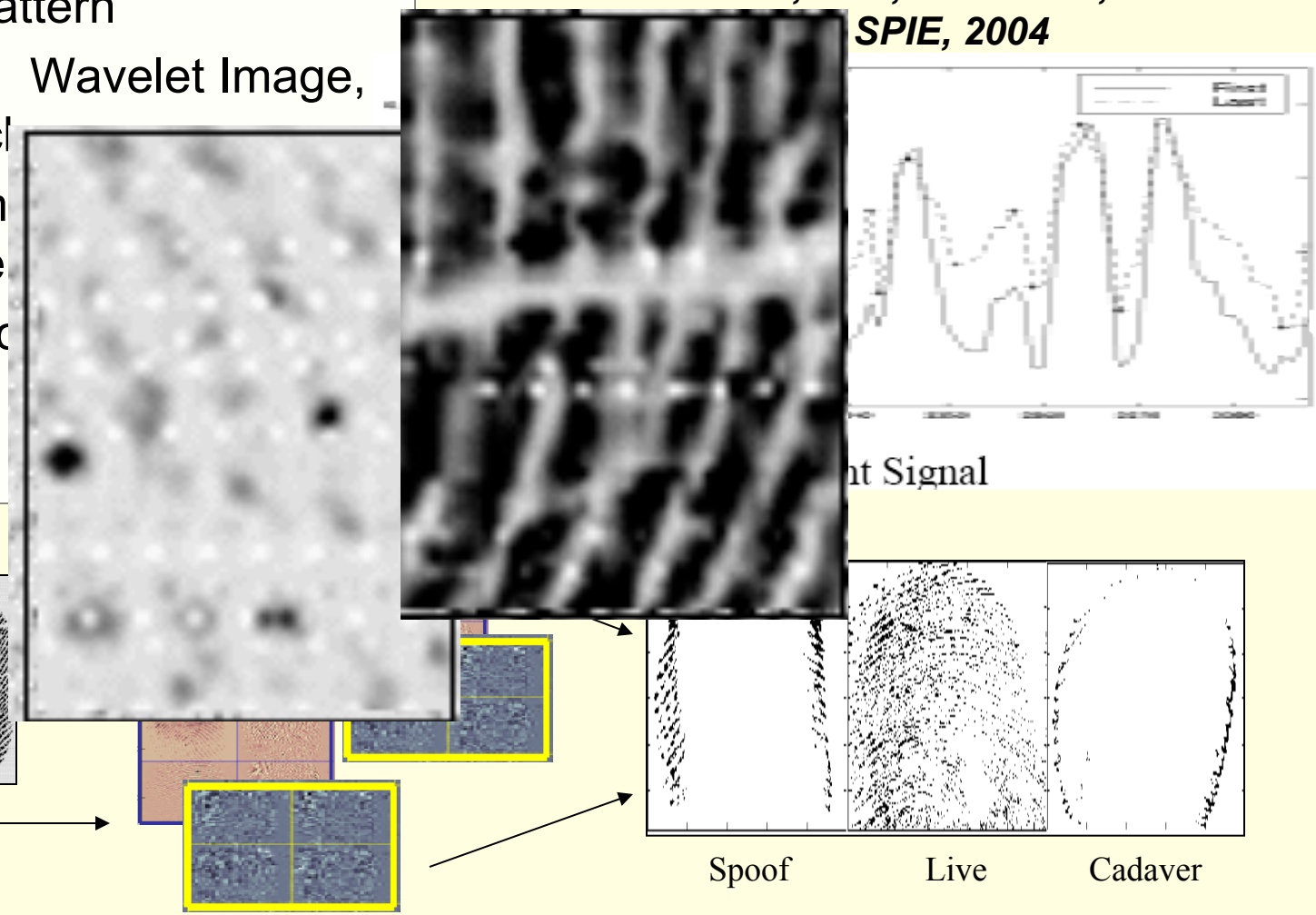


Images *Wavelet analysis* *Perspiration Pattern*

Perspiration Pattern

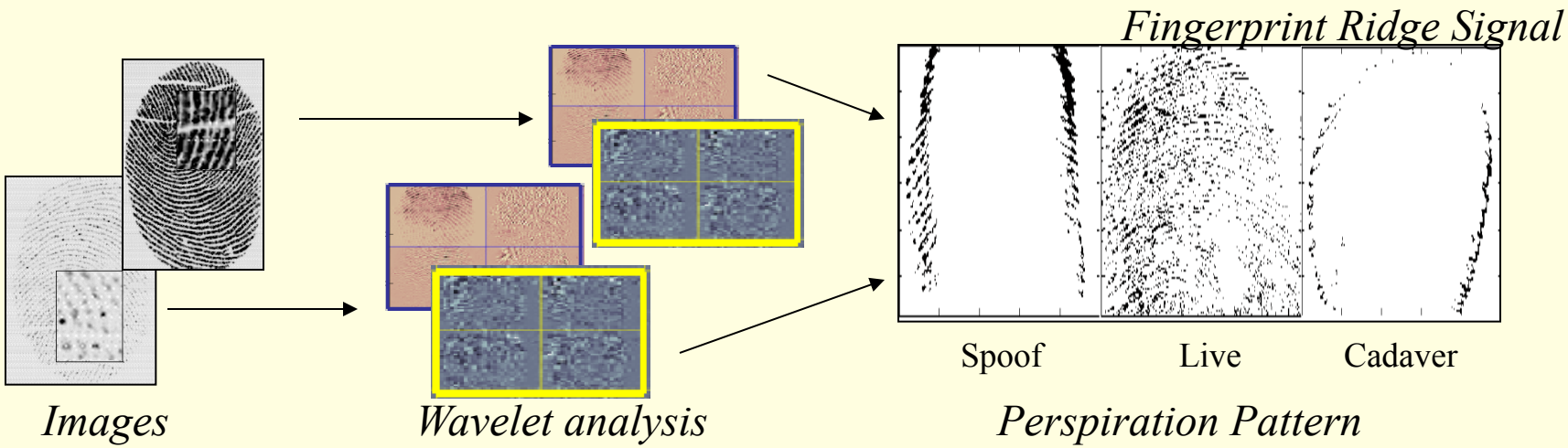
- Characterizes changes in perspiration pattern
- Two methods: Wavelet Image, Ridge signal cl
- Uses two or m collected in se
- Published repo with minimum seconds

Parthasaradhi, et al, IEEE SMC, 2005
SPIE, 2004

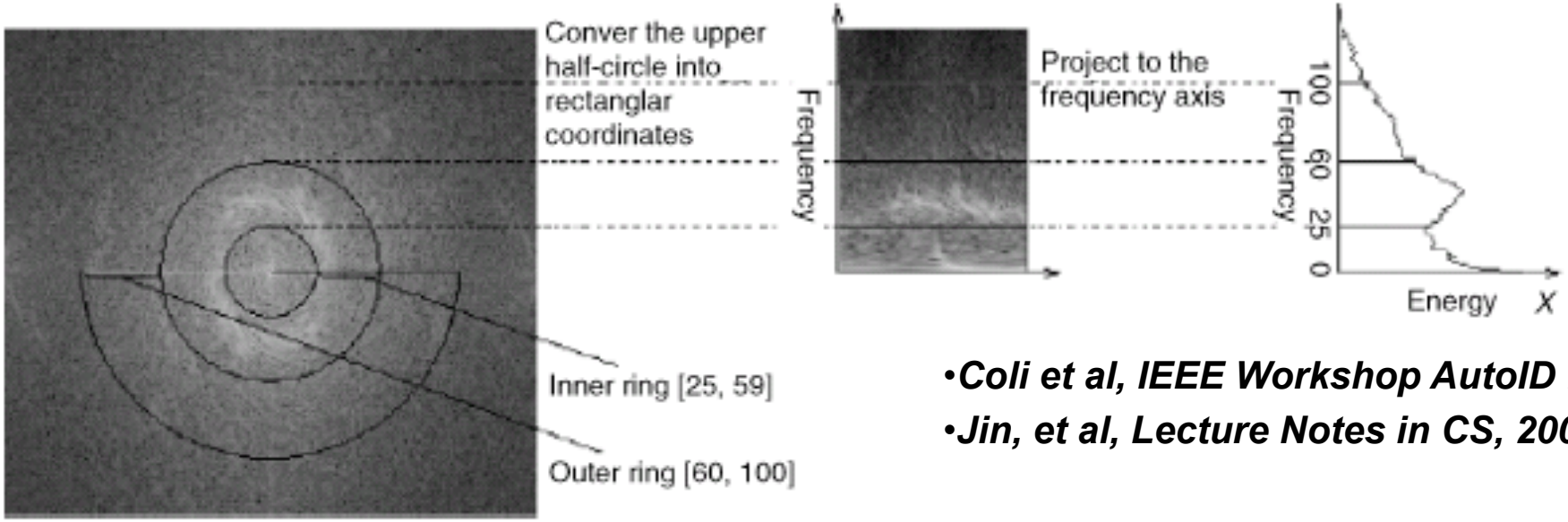


Perspiration Pattern

- Dynamic: Depends on more than one image
- Delay: May need a noticeable time delay
- Variability in live fingers over populations
- Variability due to environmental conditions (hot/cold)
- Variability across to Sensors



2D Fourier transform



- ***Coli et al, IEEE Workshop AutoID 2007***
- ***Jin, et al, Lecture Notes in CS, 2007***

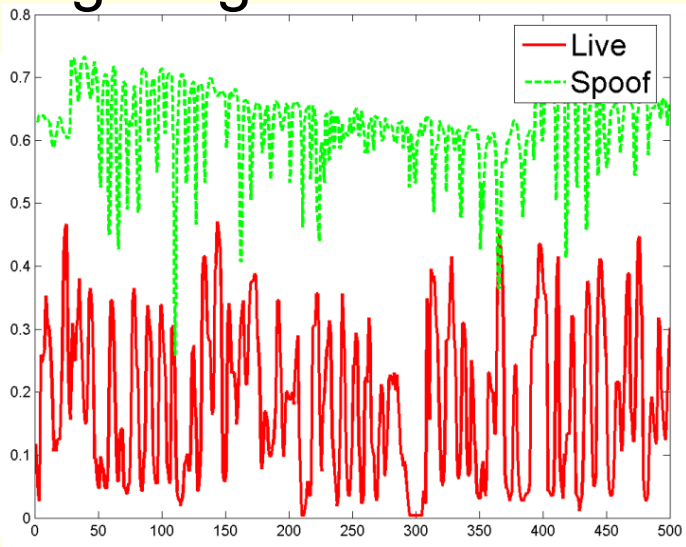
- Band-selective Fourier spectrum approach analyses the difference in spectral energies
- Two similar methods
- Relies on differences in ridge valley structure between live and spoofs
- Sensitive to the sensor being used

Ridge/Valley Characteristics

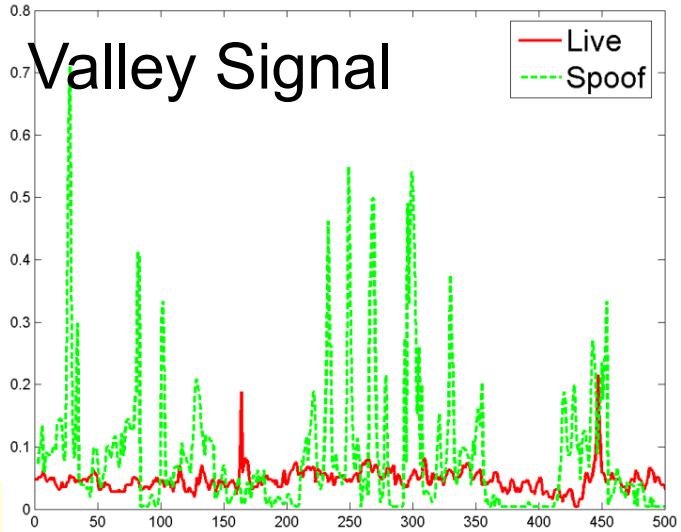
- Relies on differences in ridge/valley structure between live and spoofs
- Uses features measured from ridges and valleys separately
- Sensitive to the sensor being used
- Impacted by environmental conditions
- Must represent large diversity in both spoof and live images

Tan, et al, CVPR, 2006
Ulchida, et al, LN in CS, 2004

Ridge Signal

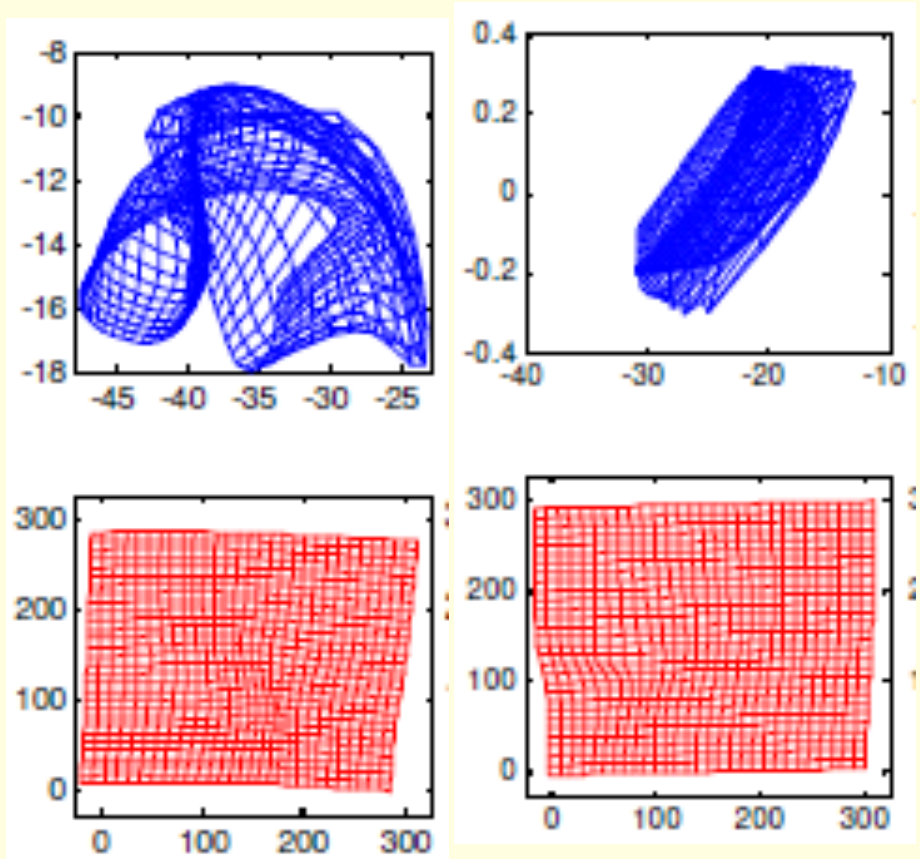


Valley Signal



Skin Distortion or Deformation

- **Two methods**
- **Chen et al:**
  - Examines deformation pattern of a live finger on a scanner surface compared to that of a spoof image based on thin-plate splines
  - Single image
- **Antonelli et al:**
  - Requires specific movement of finger on scanner with a minimum rotational speed for about 1 second
  - Multiple images

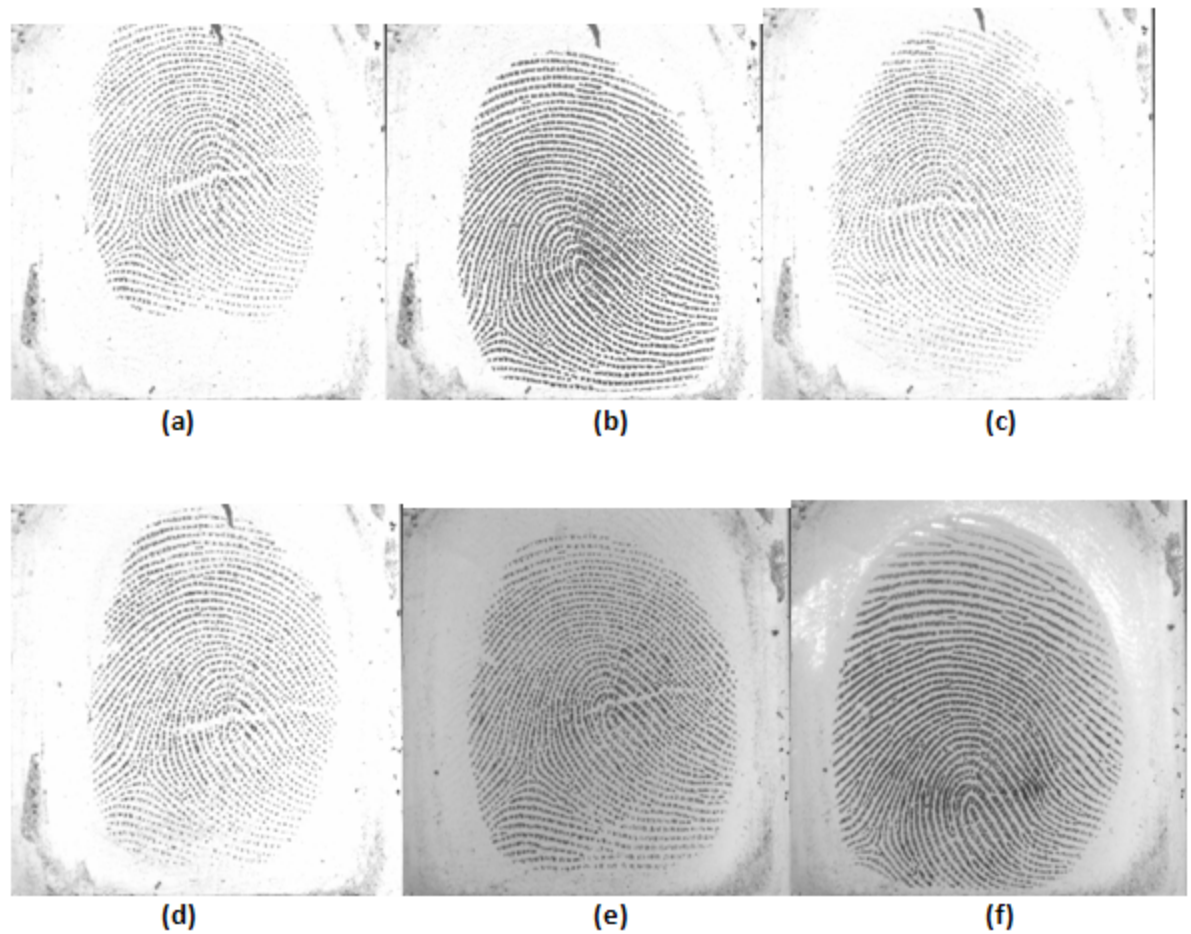


The non-linear def. model *G (1st row) and the linear +non-linear def. model F (2nd row) over the grid P using live and fake queries.*

•**Yi Chen, Anil Jain, and Sarat Dass, et. al**
•**A. Antonelli, et al, *IEEE TIFTS,* 2006**

Environmental Impact

- **Varying temperature/ humidity situations**
  - Indoor and outdoor collection
  - Multiple visits
- **Anti-Spoofing must be robust to varying fingerprints within an individual**

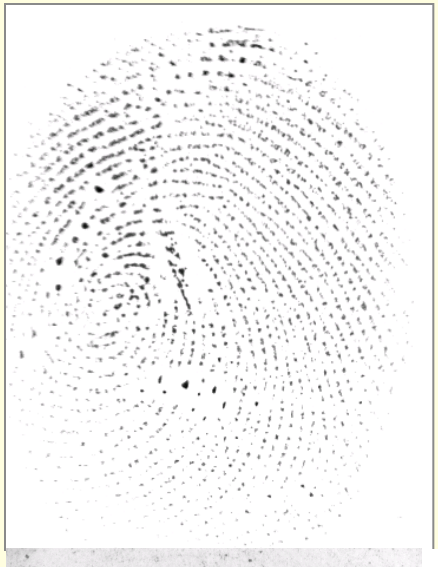


Same Individual

With varying temperature and humidity

Same spoof material
Different scanners

Optical 1



Capacitive 1

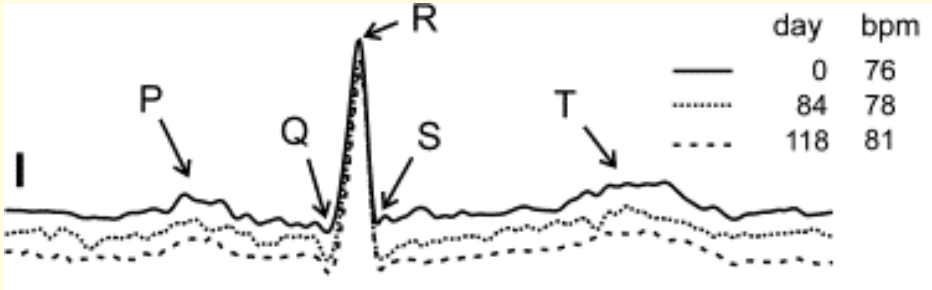
Optical 2

Capacitive 2

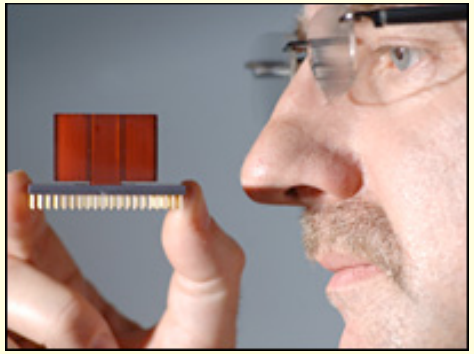
Hardware-based Fingerprint Liveness Detection

- **Hardware-based**
  - Temperature
  - Pulse
  - Blood pressure
  - Odor
  - Electrocardiogram
  - Multispectral imaging, spectroscopy

- The Lumidigm J110 Anti-Spoof scanner
- MultiSpectral imaging

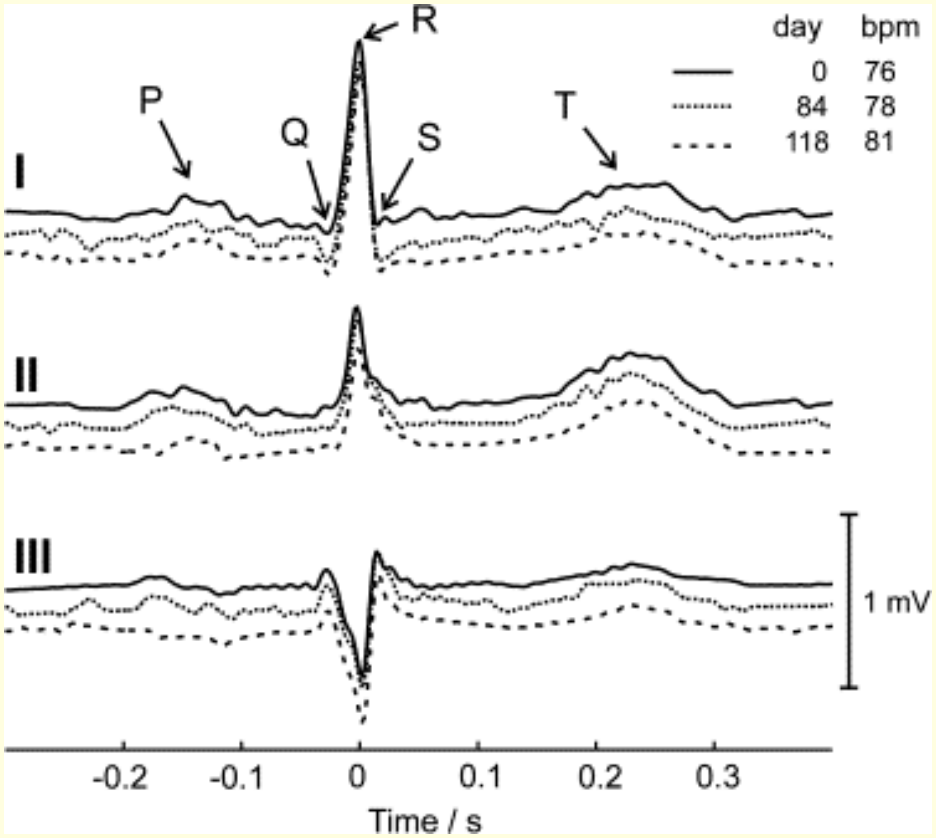


Electrocardiogram



Odor

Electrocardiogram as a Biometric



Single heart beats from three ECG recordings of one subject performed during 4 months

- Electrical measurement of the heart from the surface of the body
- E.g. two hands touching
- Requires two points of contact on opposite side of the heart
- Delay of at least one cycle of heart (>1s)
- Privacy concerns—contains medical information

Wubbeler, Gerd. "Verification of Humans using the Electrocardiogram." 26 June 2009.

Liveness Detection based on Fine Movements of the Fingertip Surface

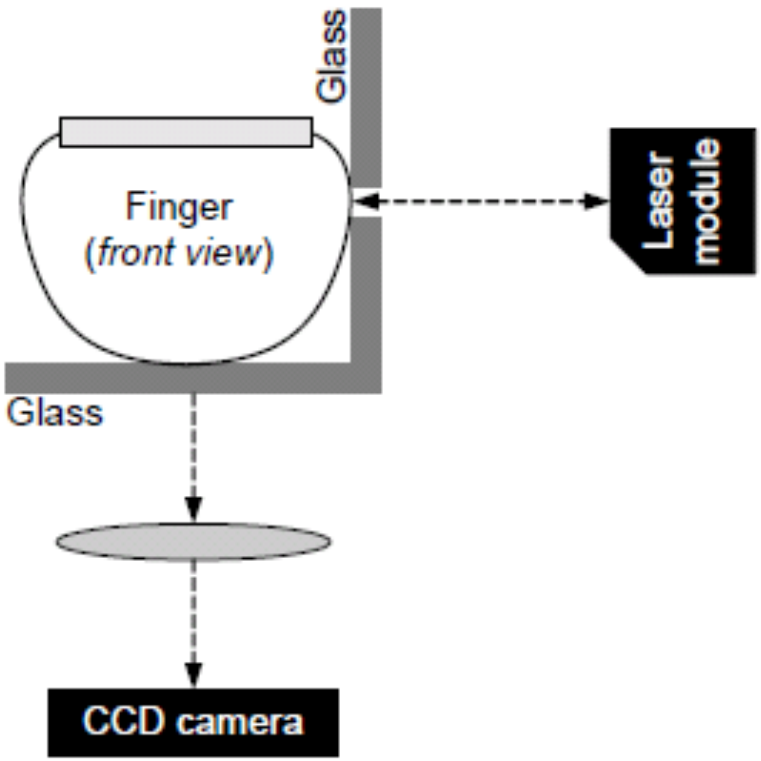
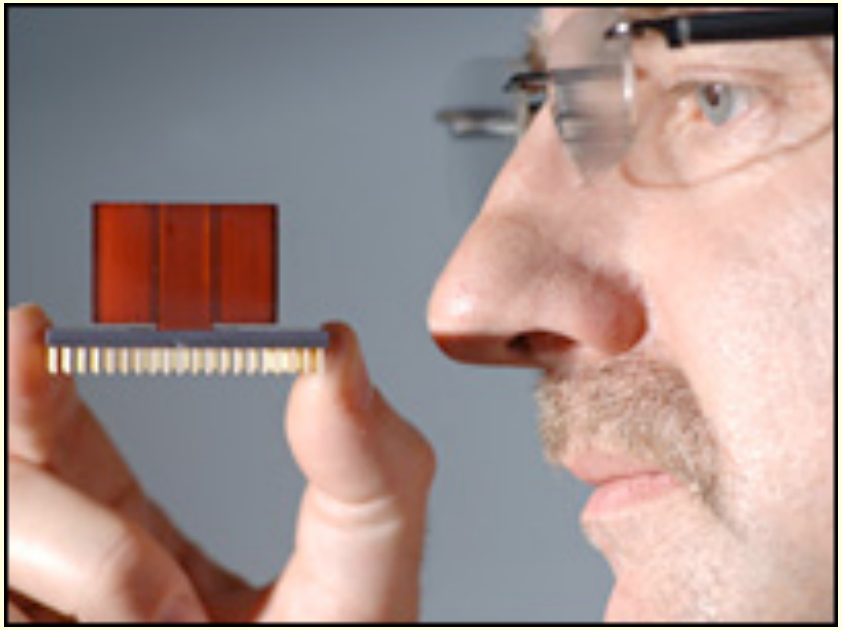


Fig. 8: Possible integration of laser distance measurement for liveness detection. with optical fingerprint sensor (CCD camera).

- Laser measures the small changes in the skin due to the expansion and contraction of papillary lines
- Based on motion from cardiac cycle
- Delay of at least one cycle of heart (>1s)
- Needs to be evaluated when real fingerprint is integrated spoof finger

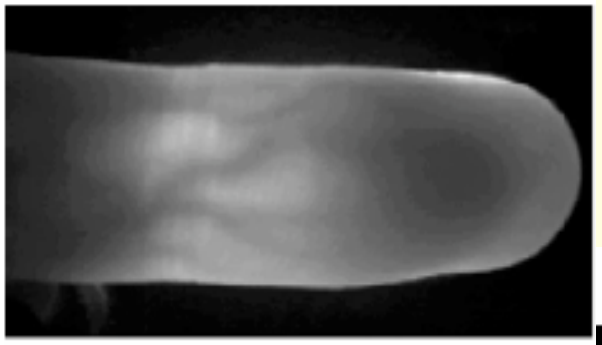
Fake Fingerprint Detection by Odor Analysis



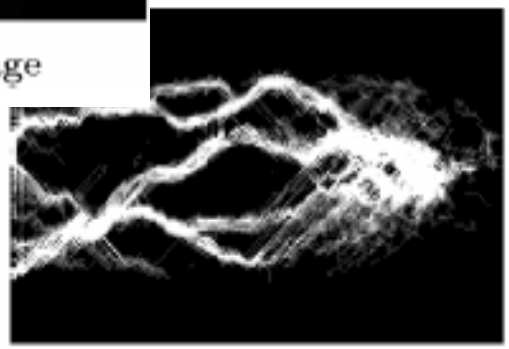
- Odor sensor (electronic nose) to sample the odor signal
- Discriminates spoofing materials
- Integration of hardware may be bulky and expensive
- Relies of knowledge of spoofing material which may be used

Baldisserra et al, Advances in Biometrics, 2005.

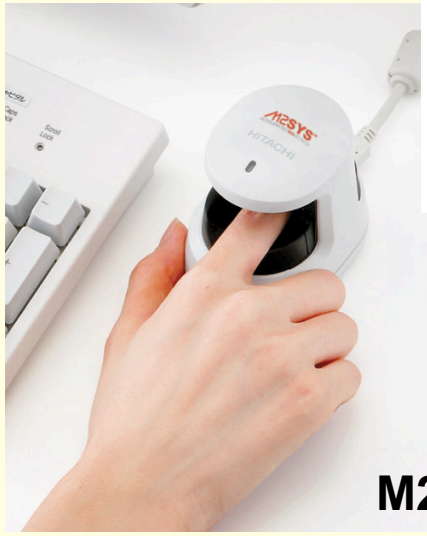
Finger Vein Biometrics



(a) Finger vein image



(b) Score distribution



M2-FV Finger Vein Reader

- Measures finger vein pattern
- Uses vein pattern as biometric
- Liveness is an inherent component of measuring the biometric
- Requires new hardware
- Requires stored template based on vein
- Are there ways to spoof this type of system?

Miura, et al, 2009.

Multispectral

The Lumidigm J110 Anti-Spoof scanner

- MultiSpectral imaging with varying illumination and polarization
- Commercial system which protects from spoofing
- Hardware approach
- Tradeoff—larger and more expensive

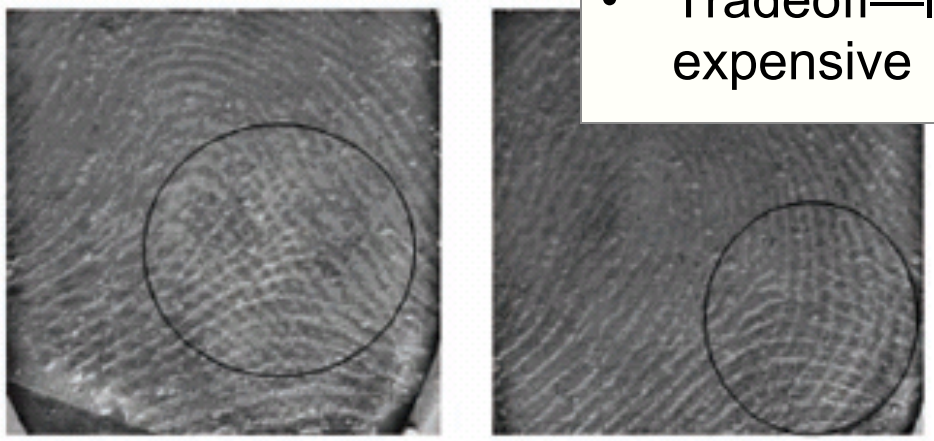


Fig. 9. Example images of various thin, transparent spoofs placed on real fingers. The elliptical marks highlight areas in which unnatural textures are clearly apparent. The automated texture analysis techniques incorporated in the MSI sensor are sensitive to much subtler variations of texture.

Rowe et al. Advances in Biometrics, 2008,

Commercial Products Emerging to Address Anti-Spoofing

- M2SYS-M2-S1 Swipe Reader
- "..will simply not read gummy fingers or other methods used to spoof fingerprint readers."

- Atmel's Thermal Swipe Sensor and Ekey's software,
- Ekey states "near impossible to spoof the scanner."

Factors in Fingerprint Liveness

- **Static or Dynamic**
  - Static: Based on one image
  - Dynamic: Based on two or more images
- **Time delay**
  - May require noticeable time delay
  - Measurements based on heart cycle will lead to delay as wait for one or more cycles >1s
- **User-assisted**
  - Something additional the user must do to assist
  - Electrocardiogram requires two points of contact
- **Device dependence**
  - Features may vary from one sensor to another
  - Hardware methods are difficult to update, each uses own technology
- **Environmental impact**
  - Features may be impacted by environmental changes
  - Hot: more smudgy
  - Cold: dry

Liveness Methods Impact on Standard Biometric Characteristics

- **Ease of Use**
  - ↓ – Dynamic, time delay
  - ↓ – User assisted
- **Collectability**
  - ↓ – User assisted
- **User acceptance**
  - – Measurement which requires medical information may not be acceptable to individuals
- **Universality**
  - – Perspiration differences may not be measurable in some individuals
  - – Some individuals require lotion for fingerprint
- **Permanence**
  - ↓ – Environmental impact

Biometric Characteristics

- **Uniqueness**
  - Typically posed as a two class problem: Live or Spoof
- **Spoof Vulnerability**
  - Need to assess liveness algorithms for their vulnerability
  - Sensitivity to training set
  - May depend on 'live' features present only in live, independent of spoof, e.g. heart beat
  - May depend on differences between live and spoof images
    - unknown what the differences will be for materials that have not been used in training algorithm
  - Reality
    - Algorithms require a comparison
    - Relative to what?

Characteristics for Liveness

- **As in biometrics, must consider many factors for liveness when integrating into overall system**

Liveness: Fingerprint. Table 2 Liveness algorithm characteristics[a]

	Ease of use	Collectability	User acceptance	Universality	Uniqueness	Permanence	Spoof-ability
Perspiration	H	H	H	M	L	M	M
Pulse oximetry	L	L	L	H	–	–	H
Multi-spectral	H	H	M	H	–	–	L
Deformation	L	L	H	M	–	–	M
ECG	L	L	L	H	L	H	H

[a] *H* High; *M* Medium; *L* Low; –indicates not applicable

Adler, Schuckers, in Encyclopedia of Biometrics, 2009

Software Based Liveness Algorithm Characteristics

	Ease of use	Collect-ability	User acceptance	Univers-ality	Perman-ence	Unique-ness	Spoof vulner-ability
Perspiration	H	H	H	M	M	L	M
Deformation	L	L	H	M	-	-	M
Power Spectrum	H	H	H	M	H	L	H
Ridge-valley profile	H	H	H	M	H	L	H

H High; M Medium; L Low; - not applicable

Liveness Algorithm Performance Comparison

Algorithm	No. Spoofs	No. Live	No. impressions	No. frames	Live Performance	Spoof Performance
Perspiration with Fourier space	18	18	1	2	88.89%	88.89%
Surface coarseness	10 gelatin 24 plastic clay	23	1	1	100%	100%
Distortion Analysis	40 (10 silicone, 10 gelatin, 10 latex, 10 wood glue)	45 (2 fingers)	10	20	88.76%	88.76%
Perspiration with wavelet space	80	58	1	1	80% - 100%	80% - 100%

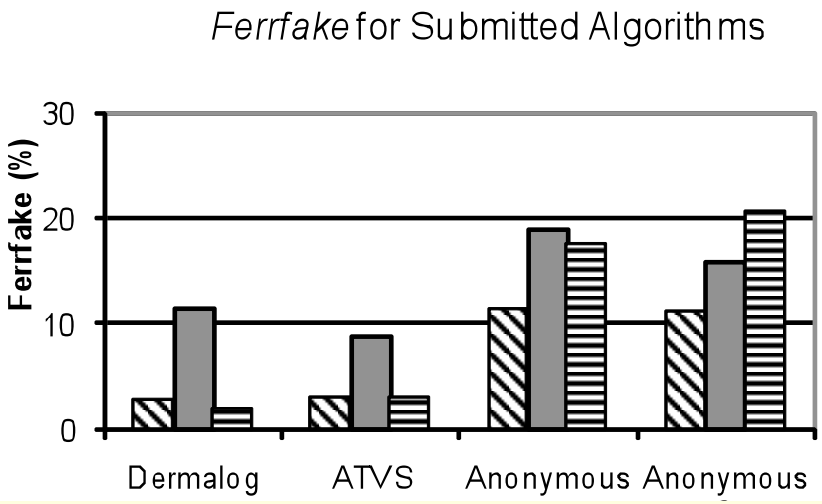
Liveness Detection Competition—LivDet 2009

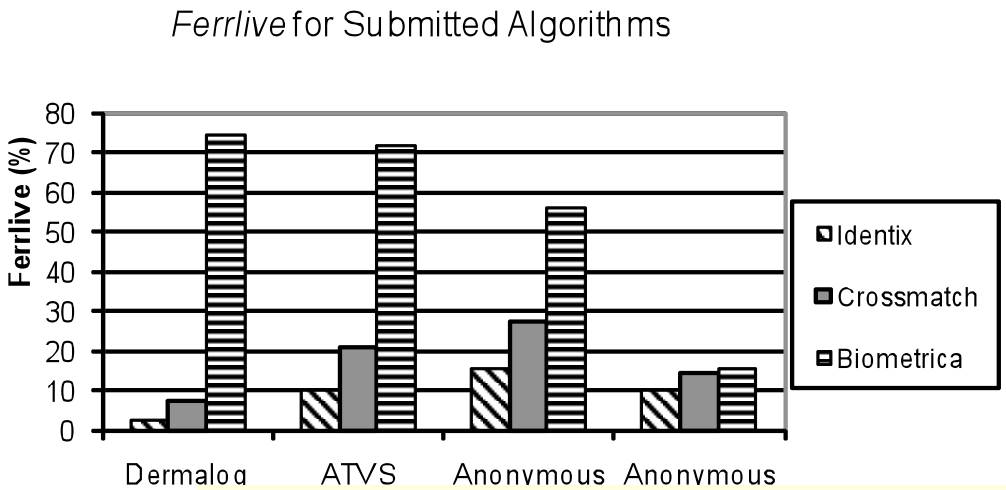
- Detection approaches tested on their home-made live and spoof databases.
- No common dataset
- ***First liveness detection competition at ICIAP 2009 with a public liveness database***
- Collaborating with Univ. of Cagliari
- Focusing on software-based fingerprint liveness

Dataset	Sensors	Model No.	Resolution (dpi)	Image size	Live Samples	Spoof Samples
#1	CrossMatch	Verifier 300LC	500	480x640	1500	1500
#2	Identix	DFR2100	686	720x720	2000	2000
#3	Biometrika	FX2000	569	312x372	2000	2000

The largest public fingerprint liveness dataset

Ferrfake and Ferrlive error rates





Ferrfake ➔ rate of misclassified fake fingerprints (false acceptance)

Ferrlive ➔ rate of misclassified live fingeprints (false rejection)

Importance of modeling individual variability for live subjects

Table 4. Number of unique subjects in training and tests, as well as the average number of images per subject. It should also be noted that Identix and Crossmatch were collected over multiple visits, while Biometrica was collected during a single visit.

Scanners	# of Training Subjects	# of Testing Subjects	Aver Images / subject
Identix	35	125	18.75
Crossmatch	63	191	15.75
Biometrika	13	37	40.0

Next Steps

- Need common terminology for assessing anti-spoofing
- Liveness detection or anti-spoofing will impact overall performance of biometric system
- Must consider many characteristics when choosing liveness (ease of use, collectability, universality, etc.)
- Public datasets can accelerate improvement
- Need for multi-entity approach to testing

Next LivDet in 2011?

- System (hardware/software) testing
- Solutions depend on sensor/finger interaction (even software)
- Anti-spoofing methods depend on strength of data used to design them
- Testing requires collaboration of university/ government/ industry
- Multiple entities attempting to spoof systems

References

- C. Jin, H. Kim, S. Elliot, “Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum,” *Lecture Notes in Computer Sciences,* vol. 4817, pp. 168-179, 2007.
- K. Uchida, “Image-Based Approach to Fingerprint Acceptability Assessment,” *Lecture Notes in Computer Sciences,* pp. 294-300, 2004.
- A. Antonelli, R. Cappelli, D. Maio, D. Maltoni, “Fake Finger Detection by Skin Distortion Analysis,” *IEEE Transactions on Information Forensics and Security,* vol. 1, no. 2, pp. 360-373, September 2006.
- J. Jia, L. Cai, “Fake Finger Detection Based on Time-Series Fingerprint Image Analysis,” *Lecture Notes in Computer Sciences,* vol. 4681, pp. 1140-1150, 2007.
- Parthasaradhi S, Derakhshani R, Hornak L, Schuckers SAC, Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 35, pp. 335- 343, 2005.
- B Tan, S Schuckers, Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing, Computer Vision and Pattern Recognition Workshop, 2006 Conference on, Page(s):26 – 26, 17-22 June 2006.
- Baldisserra, Denis, Annalisa Franco, Dario Maio, and Davide Maltoni. “Fake Fingerprint Detection by Odor Analysis ,.” In Advances in Biometrics, 265-272, 2005.

References--continued

- C. Jin, H. Kim, S. Elliot, “Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum,” *Lecture Notes in Computer Sciences,* vol. 4817, pp. 168-179, 2007.
- Miura, Naoto. “Feature Extraction of Finger Vein Patterns Based on Iterative Line Tracking and Its Application to Personal Identification.” 29 June 2009.
- Wubbeler, Gerd. “Verification of Humans using the Electrocardiogram.” 26 June 2009.
- Rowe, Robert K., Paul W. Butler, and Kristin A. Nixon. "Multispectral Fingerprint Image Acquisition." Advances in Biometrics, 2008.
- Andy Adler, Stephanie Schuckers, Security and Liveness: Overview, in Encyclopedia of Biometrics, editor: Stan Li, Springer Reference, 2009.
- Stephanie Schuckers, Liveness: Fingerprint, in Encyclopedia of Biometrics, editor: Stan Li, Springer Reference, 2009 .