Issues for Liveness Detection in Biometrics

Stephanie Schuckers, PhD†
Larry Hornak, PhD†
Tim Norman, PhD‡
Reza Derakhshani†
Sujan Parthasaradhi†

† Lane Department of Computer Science and Electrical Engineering
‡ Musculoskeletal Research Center

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
Marshall University
San Jose State University
http://www.csee.wvu.edu/citer

An individual can be considered as a union of different biological processes such as neural, skeletal, dermal, etc. that uniquely describe that individual.

One or more subsets of these processes with higher specificity are used as biometrics in automatic identification systems.
Since a biometric identifies an individual from one physiological process, the mapping from a biometric feature space to an individual will not be one to one.

Multi-modal biometrics increase precision by considering other highly specific biological traits to limit the number of claimants for an identity.
Concerns

- Is biometrics a reliable, secure solution?
- What are the threats to biometric systems?
- How can we make biometric systems more secure?
Typical Configurations

- Single Biometric System + Smart cards
- Single Biometric System + passwords
- Multiple Biometric systems + password/ tokens
- Multiple Biometric systems
- Multiple Biometric systems + passwords/ tokens

- Liveness enhances the security of a biometric system.
Threats

**BIOMETRIC SYSTEMS**

- Artificially Created biometrics
- Attacking Via input port
- Attacking at Database
Biometrics and Liveness

- Liveness is a major attribute in individuals’ feature space but has very low specificity by itself: it is dichotomy of the feature space into live and non-living.

- Since intruders will introduce a large number of spoofed biometrics into system, liveness detection will enhance performance of a multi modal biometric system (spoof attack).

- Liveness detection reads claimant’s physiological signs of life.
Biometrics and Liveness

- Multimodal biometrics+liveness detection increases specificity.
Threats

- **Spoofing:** "The process of defeating a biometric system through the introduction of fake biometric samples."

- **Artificially created biometrics:** e.g. image of a face or iris, lifted latent fingerprints, artificial fingers, high quality voice recordings, etc.

- **Attacks are also possible through input ports and data-bases.**
Spoof-Attack Protection

- Liveness detection based on recognition of physiological activities as signs of life.
  - From processing the information already captured by biometric reader.
  - From acquisition of life signs by using extra hardware.
- Introducing challenge-response mechanism.
- Putting biometric verification, in addition to enrollment, under supervision.
Liveness Detection Examples: Software Enhancement

- Fingerprint: perspiration.
- Face: head movements.
- Iris: detection of hippus (pupil movement) and saccade (eye movement).
Liveness Detection Examples: Hardware Enhancement

- Fingerprint: temperature sensing, detection of pulsation on fingertip, pulse oximetry, electrical conductivity, ECG, etc.

- Voice: matching the lip movement (video) to the audio.
Liveness Detection Examples: Challenge Response

- Face: expression challenge.
- Voice: repeating randomly generated sequence of digits and phrases.
Spoof Fingers-Example

- Put subject’s finger in impression material and create a mold.
- Molds can also be created from latent fingerprints by photographic etching techniques like those used in making of PCB (gummy fingers).
- Use play-doh, gelatin, or other suitable material to cast a fake finger.
- Worst-case scenario: dead fingers.
Scanners: Capacitive DC-AC

Live Image  Cadaver Image  Clay Image  Play-doh Image
Scanners: Optical-Optoelectric

Live Image  Cadaver Image  Clay Image  Play-doh Image
Anti-Spoofing Research

- Physiologic process of perspiration is used to determine fingerprint vitality.
- Purely software based, needs no additional hardware.
- Patent pending.
How It Works

- Hypothesis: Live fingers, as opposed to cadaver or spoof, demonstrate a specific changing moisture pattern due to perspiration.
- Using a capacitive fingerprint scanner, two fingerprints are captured over a 5-second time frame.
- Features of temporal perspiration pattern of the skin are extracted.
- Using these features, the algorithm makes a final decision about vitality of the fingerprint.

![Fingerprint Images](image-url)
Example: Live Fingerprint

0.5 sec
Example: Cadaver Fingerprint

0.5 sec
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.
Classification and Results

- Derived static and four dynamic features are fed into a back-propagation neural network.
- Training set: 36 cases, test set: 18 cases; from live, cadaver, and spoof fingerprints.
- Achieved 100% precision in distinguishing live fingerprints from spoof and cadaver fingerprints.
Work in Progress

- Testing the algorithm with larger datasets of live, spoof, and cadaver (30 of each).
- Testing the algorithm with a variety of fingerprint scanners with different technologies.
- Testing and enhancing the algorithm for reduced capture time (currently 5 sec).
- Optimizing/enhancing feature extraction and pattern recognition routines.
Conclusion

- Liveness detection in multi-modal biometric devices has the potential to enhance security, reliability and effectiveness.
- Although biometric authentication devices can be susceptible to spoof attacks, different anti-spoofing techniques can be developed and implemented that may significantly raise the level of difficulty of such attacks.