Biometric Liveness Detection: Framework and Metrics

Presented at International Biometric Performance Conference (IBPC) March, 2012

Peter Johnson\textsuperscript{1}, Richard Lazarick\textsuperscript{2}, Emanuela Marasco\textsuperscript{4}, Elaine Newton\textsuperscript{3}, Arun Ross\textsuperscript{4}, Stephanie Schuckers\textsuperscript{1}

\textsuperscript{1}Clarkson University
\textsuperscript{2}Computer Sciences Corporation (CSC)
\textsuperscript{3}National Institute of Standards and Technology (NIST)
\textsuperscript{4}West Virginia University

\textit{Funding provided by}
National Institute of Standards and Technology (NIST), National Science Foundation (NSF), Dept. of Homeland Security (DHS), and the Center for Identification Technology Research (CITeR)
This Talk

• Categories of Subversive Presentation Attacks

• Performance Metrics for Suspicious Presentation Detection Systems

• Relationship between Liveness Detection and Challenge-Response
**Subversive Presentation**

**Artefact**
- Live Capture Subject
  - ARTIFICIAL
    - (e.g., fake finger, patterned contact, face photo)
  - HUMAN
    - Cadaver
      - (e.g., dismembered fingers)
    - Altered
      - (e.g., mutilated finger, surgical alteration)
    - Nonconformant
      - (e.g., facial expression changes, side of finger)
    - Conformant
      - (e.g., zero-effort attack)
    - Coerced
      - (e.g., unconscious)

*Some cases may also not be deliberate attacks (e.g., patterned contact for cosmetic reasons, non-conformant due to improper use of system, etc.)*

*A detection system cannot infer intent, therefore, is called Suspicious Presentation Detection System*
Introduction—Definitions

- **Subversive Presentation**
  - Presentation of human or artificial biometric characteristics to the biometric capture subsystem in a fashion that interferes with or undermines the correct or intended policy of the biometric system.

- **Suspicious Presentation**
  - Presentation of a human or artificial characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system.

- **Suspicious Presentation Detection (SPD)**
  - Automated determination of a suspicious presentation.

- **Examples of SPD**
  - Liveness detection failure
  - Artefact detection
  - Altered biometric detection
  - Others terms that have been used: anti-spoofing, biometric fraud, spoof detection, authenticity detection, etc.
Subversive Presentation

 ARTIFICIAL

Artefact
(e.g., fake finger, patterned contact, face photo)

Nonconformant
(e.g., facial expression changes, side of finger)

Conformant
(e.g., zero-effort attack)

Coerced
(e.g., unconscious)

HUMAN
Cadaver
(e.g., dismembered fingers)

Altered
(e.g., mutilated finger, surgical alteration)

Artefact Detection

Live Capture Subject

Non-Subversive Presentation
Subversive Presentation

**Non-Subversive Presentation**

**ARTIFICIAL**
- Artefact
  - (e.g., fake finger, patterned contact, face photo)

**HUMAN**
- Cadaver
  - (e.g., dismembered fingers)
- Altered
  - (e.g., mutilated finger, surgical alteration)
- Nonconformant
  - (e.g., facial expression changes, side of finger)
- Conformant
  - (e.g., zero-effort attack)
- Coerced
  - (e.g., unconscious)

**Liveness Detection**

**Live Capture Subject**
Subversive Presentation

ARTIFICIAL
- Artefact
  - (e.g., fake finger, patterned contact, face photo)
- Altered
  - (e.g., mutilated finger, surgical alteration)
- Nonconformant
  - (e.g., facial expression changes, side of finger)
- Conformant
  - (e.g., zero-effort attack)
- Coerced
  - (e.g., unconscious)

HUMAN
- Cadaver
  - (e.g., dismembered fingers)

Non-Subversive Presentation

Altered Biometric Detection

- Live Capture Subject
  - (e.g., dismembered fingers)
Categories for Subversive Presentation Attacks
Categories for Subversive Presentation Attacks

- First step in development of scientific framework to evaluate suspicious presentation detection security systems
- Classification and brief description of known attack types on biometric authentication at the sensor
- Provide foundation for development of effective countermeasures
  - Basis for performance assessment
  - Empirical testing of countermeasure effectiveness against known attacks
- Not a recipe book for creating artificial biometric traits
- Procedure to create an artificial subversive presentation characteristic:
  - Source of biometric characteristic – Obtain information to describe characteristic
  - Production of artefact – Process for creating artefact to present characteristic to sensor
- Human – no artificial characteristics used
Source of Biometric Characteristics

• **Cooperative**
  - Characteristic captured directly from individual with assistance (e.g. finger mold, hand mold, face mask)

• **Latent**
  - Characteristic captured indirectly through latent sample (e.g. latent fingerprint, latent palmprint, hair, skin, body fluid)

• **Recording**
  - Characteristic captured directly from individual onto media (e.g. photograph, video recording, audio recording)

Source of Biometric Characteristics

- **Template Regeneration**
  - Regenerate characteristic from template (e.g. fingerprint regeneration, face)

- **Synthetic**
  - Synthetic characteristic, not mapped to real person (e.g. synthetic fingerprint, iris, face, voice, wolf synthesized sample)

- **Impersonation**
  - Conversion of natural characteristic to another individual's with artificial assistance (e.g. computer assisted voice)

Feng and Jain, Advances in Biometrics article, 2009.
Production of Artefact

- **Mold/cast**
  - Create 3D representation of characteristic (negative)
  - Cast is reproduction created from mold (e.g. theatrical face mask, finger artefact of modeling clay, gelatin, silicone, latex, wood glue, glycerin, etc.)
- **Mask – modify or conceal characteristics (partially or completely) with artefact**
Production of Artefact

• **Direct rendering**
  – Printing 2D (e.g. photo of iris or face, fingerprint printed on transparency/paper)
  – Printing 3D (e.g. contact lens printed with pattern, prosthetic hand printed with vein pattern)
  – Etching (e.g. fingerprint etched on metal)
  – Painting – patterns and colors painted on prosthesis

• **Digital Media**
  – Computer screen – laptop or tablet to present image or video
  – Audio – recording of voice


Seelen, “Countermeasures Against Iris Spoofing with Contact Lenses,” Iridian Technologies Inc.
Categories of Human Subversive Presentations (Non-Artefact Methods)

• **Lifeless**
  – Cadaver

• **Altered**
  – Mutilation (e.g. scarring, amputation, acid)
  – Surgical modification (e.g. new fingerprint, nose job, face lift)

• **Non-Conformant**
  – Impersonation (e.g. voice mimicry, forged signature)
  – Presentation (e.g. hand shape control, facial expression/extreme, tip of side of finger)

• **Conformant**
  – Zero effort impostor attempt (e.g. any normal presentation)

• **Coerced**
  – Unconscious or under duress

Performance Metrics for Suspicious Presentation Detection Systems
State of Artefact Detection Performance Metrics

• Performance metrics for biometric systems – adapted unmodified for artefact detection assessment
  – Classification rate (percent correctly classified)
  – FAR/FMR – false accept rate/false match rate
  – FRR/FNMR – false reject rate/false non match rate
  – TAR/GAR – true accept rate/genuine accept rate
  – EER – equal error rate
  – ROC – receiver operating characteristic
  – DET – detection error trade-off

• Need to distinguish “false accepts” in matching from “false accepts” in artefact detection
  – Need common set of vocabulary
Evaluation of suspicious presentation detection systems

• The ability to correctly identify suspicious presentation attacks is quantified by a dedicated set of performance metrics.

• The suspicious presentation detection error rates are defined based on the specific purpose of the suspicious presentation detection module:
  – E.g., live vs non-live, altered vs non-altered, artefact vs non-artefact, etc.
  – Performance metrics are confined to the defined goal.

• Metrics for assessing suspicious presentation detection detection performance differ from those used for assessing matching performance.
General Model for Performance Evaluation

- **Suspicious Presentation Detection**: When the system states that the presentation characteristic is suspicious.

- **Non-Suspicious Presentation Detection**: When the system states that the presentation characteristic is not suspicious.

- **Metrics for error cases**:
  - **False Non-Suspicious Presentation Detection (FNSPD)**: a suspicious presentation is incorrectly classified as being a non-suspicious presentation.
  - **False Suspicious Presentation Detection (FSPD)**: a non-suspicious presentation is incorrectly classified as being a suspicious presentation.
Artefact Detection Case

• **Goal:** Evaluation of module that is designed to distinguish the presentation of an artefact from a non-artefact
  – **Artefact Detection:** When the system states that the presentation characteristic is an artefact
  – **Non-Artefact Detection:** When the system states that the presentation characteristic is not an artefact

• **Metrics for error cases:**
  – **False Artefact Detection Rate (FADR):** proportion of non-artefact presentations incorrectly classified as being artefacts
  – **False Non-Artefact Detection Rate (FNDR):** proportion of artefact presentations incorrectly classified as being non-artefacts
Traditional Metrics for Biometric Evaluation (Live Finger Input)

- **Data Capture Subsystem**: Live Finger Presentation
  - Biometric Characteristics
  - Biometric Capture Sensor
  - Reject
  - Failure To Acquire

- **Suspicious Presentation Detection Subsystem**
  - Artefact Detection Module
  - Signal Processing Subsystem
    - Quality Check
    - Segmentation Feature Extraction
    - Reference Creation
  - Decision Subsystem
    - Match?
    - Decision (Reject/Accept)
    - False Reject
    - False Accept

- **Comparison Subsystem**
  - Comparison
  - Comparison Score
  - Enrollment Database
  - Reference
  - Biometric Claim

- **Failure To Enroll**
Additional Metrics (Artefact Input)

- Artefact detection methods treated as two class problem
- Evaluation in literature focuses specifically on artefact detection module only

Data Capture Subsystem

- Biometric Capture Sensor

Segmentation

- Feature Extraction

Biometric Characteristics

Suspicious Presentation Detection Subsystem

- Artefact Detection Module

Signal Processing Subsystem

- Quality Check
- Segmentation Feature Extraction
- Reference Creation

Accept/Reject

Artefact Detection Rate
Non-Artefact Detection Rate

Artefact

Live Finger

Reject
Additional Metrics (Artefact Input)

- Artefact detection module will contribute to decision to reject
- Other modules (e.g. quality) may contribute
- During testing specific reason for rejection may not be known
- Need clarification in terminology for system testing (this slide) and artefact detection module testing (last slide)

Failure To Acquire
Artefact Detection Rate

Failure to Enroll
(Live, Non-Artefact)
Artefact Detection Rate
What about matching? (Artefact Input)

- Artefact finger may not be rejected by earlier modules
- If artefact matches stored reference, a successful artefact attack has occurred.

**Data Capture Subsystem**
- Live Finger
- Artefact
  - Biometric Characteristics
  - Biometric Capture Sensor

**Suspicious Presentation Detection Subsystem**
- Artefact Detection Module
  - Signal Processing Subsystem
    - Quality Check
    - Segmentation Feature Extraction
    - Reference Creation

**Comparison Subsystem**
- Comparison
  - Comparison Score
  - Decision Subsystem
    - Match?
      - Decision (Reject/Accept)

**Data Storage Subsystem**
- Enrollment Database
- Reference

**Artefact False Accept**
- False Reject (Non-artefact)
- False Accept (Non-artefact)
On the Relationship between Liveness Detection and Challenge-Response
Motivation

Ways to strengthen Authentication Methods

• Increase to multi-factors
  – Biometrics
  – Knowledge
  – Possession (not addressed further, too application specific)

• Add strength to biometrics with “liveness” (L)
• Add strength to Authentication with Challenge-Response (CR) schemes
Relationship between L and CR

- Some techniques combine L and CR

See illustration in the following table
## L and CR relationship (overall)

### LIVENESS
(BIOMETRIC CAPTURE SUBSYSTEM BASED)

**Primary Examples “L & CR”**
- Controlled change illumination $\rightarrow$ Pupil size
- Multispectral illumination $\rightarrow$ Absorption characteristics

**Concepts:**
- Challenge $\rightarrow$ Response (based on Liveness)
- Stimulated intentionally

**Primary Examples “L”**
- Finger perspiration (over time)
- Hippus (iris) motion/freq
- Pulse

**Concepts:**
- No stimulation (no “challenge”)
- Passive (receive only)

### CR-BIOMETRIC SYSTEM LEVEL
(INVOLVES SOME ASPECTS EXTERNAL TO THE BIOMETRIC CAPTURE SUBSYSTEM)

**Primary Examples “CR”**
- Finger order (random changes by system) $\rightarrow$ Correct presentation & matching
- Digit order $\rightarrow$ Correct pronunciation & matching
- Security question* $\rightarrow$ Correct answer (content) & matching
  * Combination of Knowledge and Biometrics

**Concepts:**
- Challenge logic in System (server/back-end)
- Enrollment of all designed variations (multiple fingers, all digits 0-9)

### CR-SYSTEM LEVEL
(DOES NOT INVOLVE BIOMETRIC CAPTURE)

**Primary Examples (non-BIO)**
- Smart ID card (with authentication) + PIN
- Login name + password + randomized security question
- ID card + scramble pad PIN code*
  * this example has an added cognitive/human/alive aspect

**Concepts:**
- Involves authentication factors other than Biometrics
- Challenge can take the form of device/card authentication (confirm digital cert)
Summary

• Some Liveness approaches do not involve Challenge-Response (L)
• Liveness and Challenge-Response can be used together (L&CR)
• Some Challenge-Response approaches involve biometrics but not Liveness (CR)
• Some Challenge-Response approaches do not involve biometrics (non-BIO)
Overall Summary

• Categories of Subversive Presentation
  – Artificial (Source and Production Methods)
  – Human (altered, coerced, non-conformant, conformant, cadaver)

• Suspicious Presentation Detection
  – Liveness Detection, Artefact Detection, Altered Finger Detection

• Metrics for measuring performance
  – False Suspicious Presentation Detection (FSPD)
    • e.g., False Artefact Detection (FAD)
  – False Non-Suspicious Presentation Detection (FNSPD)
    • e.g., False Non-Artefact Detection (FND)

• Liveness and Challenge Response