Biometric Liveness Detection: Framework and Metrics

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

Peter Johnson¹, Richard Lazarick², Emanuela Marasco⁴, Elaine Newton³, Arun Ross⁴, Stephanie Schuckers¹

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

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)
Subversive Presentation*

Non-Subversive Presentation

Live Capture Subject

Subversive Presentation

ARTIFICIAL

HUMAN

Cadaver
(e.g., dismembered fingers)

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

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)

*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)
- Altered (e.g., mutilated finger, surgical alteration)
- Nonconformant (e.g., facial expression changes, side of finger)

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

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

Coerced (e.g., unconscious)

Non-Subversive Presentation

Artefact Detection

Live Capture Subject
Subversive Presentation*

**Non-Subversive Presentation**

**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)

Liveness Detection

Live Capture Subject

Also helps with this
Subversive Presentation

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

Non-Subversive Presentation

- **Live Capture Subject**
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 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

Suspicious Presentation Detection Subsystem
- Artefact Detection Module
  - Quality Check
  - Segmentation Feature Extraction
    - Reference Creation
      - Reference
  - Signal Processing Subsystem
    - Signal Processing
      - Decision Subsystem
        - Match?
        - Decision (Reject/Accept)
        - False Reject
        - False Accept
      - Data Storage Subsystem
        - Enrollment Database
          - Reference
          - Biometric Claim

Comparison Subsystem
- Comparison
  - Comparison Score
  - Decision Subsystem
    - Reject
    - Fail to Enroll
    - Fail to Acquire

Failure To Acquire
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**
- 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

**Accept/Reject**

**Artefact Detection Rate**

**Non-Artefact Detection Rate**
Artefact Detection Rate

- 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 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.
Performance Metrics for the Combination of Suspicious Presentation Detection System and the Matcher
Artefact Detector and Biometric Matcher

Configuration type 1

Matcher → Artefact Detector

Non-Match

Non-Artefact

Match

Artefact

Non-Artefact

Artefact
Configuration type 1

The combination of Artefact Detection and Matcher should REJECT the artefact

User with an artefact (Genuine)

Matcher

Artefact detector

Artefact

Non-Artefact

TM-TAD

TM-FND

FNM: False Non-Match
TM: True Match

FNM: False Non-Match
TM: True Match

TAD: True Artefact Detection
FAD: False Artefact Detection
TND: True Non-Artefact Detection
FND: False Non-Artefact Detection

System may stop at this point.
Configuration type 1

The combination of Artefact Detection and Matcher should REJECT the artefact

- **FNM**: False Non-Match
- **TM**: True Match

User with an artefact (Genuine)

Matcher → Artefact detector

Artefact detector → Artefact
Artefact detector → Non-Artefact

Artefact → FNM-TAD
Non-Artefact → FNM-FND

Artefact → TM-TAD
Non-Artefact → TM-FND

- **FAD**: False Artefact Detection
- **FND**: False Non-Artefact Detection
- **TAD**: True Artefact Detection
- **TND**: True Non-Artefact Detection
Configuration type 1

The combination of Artefact Detection and Matcher should ACCEPT the live person.

- **FNM**: False Non-Match
- **TM**: True Match
- **TAD**: True Artefact Detection
- **FAD**: False Artefact Detection
- **TND**: True Non-Artefact Detection
- **FND**: False Non-Artefact Detection

User with no artefact (Genuine) → **Matcher**

- **imp**
- **gen** → **TM**

**Artefact detector**

- **Artefact** → **TM-FAD**
- **Non-Artefact** → **TM-TND**

**FNM** System may reject at this point.

- False rejection of the live person
- Correct accept of the live person
Configuration type 1

The combination of Artefact Detection and Matcher should ACCEPT the live person

- FNM: False Non-Match
- TM: True Match
- TAD: True Artefact Detection
- FAD: False Artefact Detection
- TND: True Non-Artefact Detection
- FND: False Non-Artefact Detection

User with no artefact (Genuine)

Matcher

Artefact detector

Artefact
- FNM-FAD
- FNM-TND

Non-Artefact
- TM-FAD
- TM-TND

False rejection of the live person
Correct accept of the live person
Artefact Detector and Biometric Matcher

Configuration type 2

Artefact Detector → Matcher

Artefact
- Match
- Non-match

Non-Artefact
- Match
- Non-match
Configuration type 2

The combination of Artefact Detection and Matcher should REJECT the artefact.

User with an artefact (Genuine)

Artefact detector

Artefact

TAD: True Artefact Detection

Non-Artefact

FND: False Non-Artefact Detection

Matcher

FNM-FND: False Non-Match

TM-FND: True Match

---

FNM: False Non-Match

TM: True Match

TAD: True Artefact Detection

FAD: False Artefact Detection

TND: True Non-Artefact Detection

FND: False Non-Artefact Detection

System may stop at this point.
Configuration type 2

The combination of Artefact Detection and Matcher should REJECT the artefact

- FNM: False Non-Match
- TM: True Match
- FAD: False Artefact Detection
- TND: True Non-Artefact Detection
- FND: False Non-Artefact Detection
- TAD: True Artefact Detection

User with an artefact (Genuine)

Artefact detector → Artefact

Artefact → TAD → Matcher

Non-Artefact → FND → Matcher

FNM-TAD
TM-TAD
FNM-FND
TM-FND

False accept of the artefact
Correct rejection of the artefact
Configuration type 2

The combination of Artefact Detection and Matcher should ACCEPT the live person

User with no artefact (Genuine)

Artefact

Non-Artefact

Matcher

• FNM: False Non-Match
• TM: True Match
• TAD: True Artefact Detection
• FAD: False Artefact Detection
• TND: True Non-Artefact Detection
• FND: False Non-Artefact Detection

FAD: System may stop at this point.

FNM-TND

TM-TND
Configuration type 2

The combination of Artefact Detection and Matcher should ACCEPT the live person

- **FNM**: False Non-Match
- **TM**: True Match
- **TAD**: True Artefact Detection
- **FAD**: False Artefact Detection
- **TND**: True Non-Artefact Detection
- **FND**: False Non-Artefact Detection

User with no artefact (Genuine)

Artefact

Non-Artefact

Matcher

Artefact Detection (FAD)

Non-Artefact Detection (TND)

FNM-FAD

TM-FAD

FNM-TND

TM-TND

False rejection of the live person

Correct accept of the live person
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
Extra Slides
Suspicious Presentation Detection (SPD) Location

- SPD at biometric sensor component level
- Based on hardware’s intrinsic differentiation between real and artificial presentation
- No basis for evaluation of SPD performance

- Independent hardware-based SPD
- State of SPD could be recorded by system
- Upon successful SPD, sample may or may not be transmitted to signal processing subsystem
Suspicious Presentation Detection (SPD) Location

- SPD after sensor component level
- Based only on captured sample
- In case of successful SPD, image may not be transmitted to signal processing subsystem
- State of SPD recorded by system

Figure 1 — Components of a general biometric system
Suspicious Presentation Detection (SPD) Location

- SPD at signal processing component level
- Based on captured sample
- Allows for quality control on sample before SPD
- In case of successful SPD, biometric features may not be transmitted to comparison subsystem
Suspicious Presentation Detection (SPD) Location

- SPD after signal processing component level
- State of SPD transmitted with biometric features to comparison subsystem

Figure 1 — Components of a general biometric system
Suspicious Presentation Detection (SPD) Location

- SPD after comparison subsystem
- State of SPD transmitted with biometric comparison score to decision subsystem
- Allows for fusion of SPD output with comparison score

Figure 1 — Components of a general biometric system