Infographics

Vulnerability Analysis of Face Recognition Systems to Spoofing Attacks and the Necessity of 4th Generation AI Anti-Spoofing Technology

UBio
Your Bio All the Way

About UNION biometrics

UNION biometrics is a global leader in biometric security, delivering comprehensive, high-performance access control solutions and premium multi-modal recognition devices built on proprietary technologies and patented anti-spoofing methods, protecting critical infrastructure, corporate, and government facilities worldwide through a trusted global partner network.

1. Introduction

A Realized Threat, The Structural Vulnerability of Commercial Face Recognition Systems

The 'realistic face masks' depicted in recent media are no longer a product of imagination. Academic and industrial experiments have proven that high-quality 3D masks and digital synthesis technologies can compromise **Commercial-Off-The-Shelf (COTS)** face recognition systems under specific conditions.

COTS engines are optimized to provide high accuracy in static image-matching environments. However, they fundamentally lack security mechanisms to verify 'liveness,' leading to an inherent vulnerability to **Presentation Attacks (PA)**.

According to literature and empirical studies, when variables such as camera specifications, shooting distance, lighting, and matching thresholds are optimized in favor of an attacker, the **Attack Presentation Classification Error Rate (APCER)** can reach **up to approximately 70%**. This figure is not merely a technical error but should be interpreted as a policy-level warning. It signifies a serious 'Structural Security Debt' that COTS-only strategies can create when an attacker identifies system weaknesses and uses optimized attack media.

2. Background

The Proliferation of High-Risk Infrastructure and the Scope of Threats

- **Deployment of Biometric Infrastructure**
  Biometric technology has become a standard security measure in airports, financial institutions, and critical national facilities.
  As of 2025, the U.S. Transportation Security Administration (TSA) operates **Credential Authentication Technology (CAT)** systems in approximately **84 airports.**
  CAT streamlines the identity verification process by cross-referencing a passenger's scanned ID with their facial biometric data in real time.
  The TSA plans to expand deployment to more than **400 airports** in the coming years.

  This represents a global trend. According to a report by the International Air Transport Association (IATA), **43% of airports** worldwide have already adopted biometric-based boarding systems, and **46% of passengers** have used them.
  As this infrastructure becomes increasingly widespread, the vulnerability of a single system can translate into both national and international security risks.

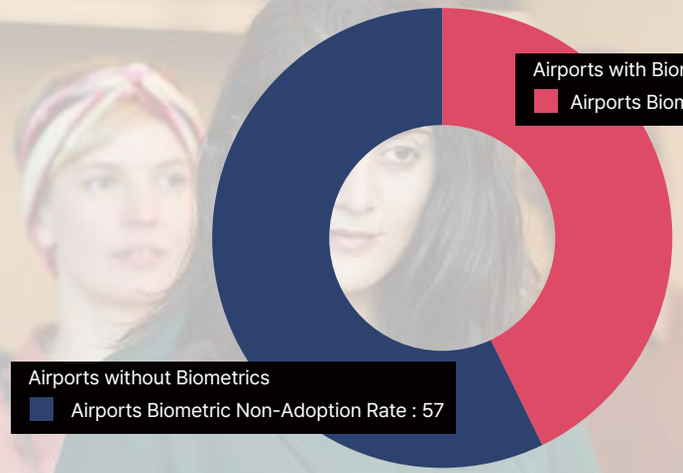
- **Types and Threats of Presentation Attacks**
  Presentation Attacks are broadly classified into three types, each posing a different level of threat:

  - **2D Attacks (Print, Replay):** Attacks using high-resolution photos or video playback. They are the most common due to their low cost and ease of execution.
  - **3D Attacks (Mask):** Attacks using 3D masks made of special materials like silicone. They pose a serious threat to COTS systems lacking depth information by mimicking the three-dimensionality and surface texture of a face.
  - **Digital Synthesis Attacks (Deepfake):** The most sophisticated form of attack, using AI-generated synthetic videos. These attacks attempt to bypass PAD technologies by precisely imitating inter-frame consistency and micro-movements.

A COTS-only strategy can lead to severe security gaps across a wide range of areas, from personal finance and corporate access control to airports, ports, and critical national infrastructure (e.g., power plants, military facilities).

UBio
Your Bio All the Way

- **Biometric Adoption in Global Airports**
  According to an IATA report, a significant number of airports worldwide have already implemented biometric-based systems, meaning a single system's vulnerability can escalate into an international security risk.



U.S TSA
400+
Airports in planned expansion

Global Passengers
46%
Have used biometric systems

- **Types of Presentation Attacks**


2D Attacks (Print, Replay)


3D Attacks (Mask)


Digital Synthesis (Deepfake)

Technical Response:
The 4-Stage Evolution of PAD

- **Gen 1: Rule-Based**
  Relied on simple rules like blinking, only effective against low-quality spoofing attempts.
- **Gen 2: Sensor Fusion**
  Used Depth (ToF) and Infrared (IR) sensors, improving 2D attack defense but still vulnerable to high-quality 3D masks.
- **Gen 3: Deep Learning**
  Learned complex features with CNN models but failed against new, 'unseen' attack types it wasn't trained on.
- **Gen 4: Intrinsic Liveness Verification**
  A paradigm shift to verifying 'vital signs,' not just appearance. Uses rPPG to detect the unforgeable 'pulse' from micro-blood flow changes and fuses it with Depth/IR data for the ultimate defense.

3. Technical Response

The 4-Stage Evolution of Anti-Spoofing (PAD) Technology

In response to the evolution of spoofing attacks, Presentation Attack Detection (PAD) technology has also advanced rapidly, now transitioning to 4th generation integrated AI models.

- **1st & 2nd Generation PAD:** Initial Responses and Clear Limitations
  - **1st Gen (Rule-Based):** Relied on simple rules like blinking and head movements, effective only against low-quality print attacks.
  - **2nd Gen (Sensor Fusion):** Introduced depth sensors (ToF) and infrared sensors (IR/NIR) to enhance performance against 2D attacks but had issues with hardware costs and could be bypassed by high-quality 3D masks.
- **3rd Generation PAD:** Used Deep Learning (DL) to learn complex features, but lacked generalization and was vulnerable to new, unseen attacks.
- **4th Generation PAD:** The latest generation uses multimodal fusion AI to simultaneously learn spatial, temporal, and spectral information. This paradigm shifts verification from superficial patterns to 'intrinsic liveness.'

This evolution has established PAD as a core security component for real-world operational environments, moving it beyond a laboratory-level technology.

- **Comparison of PAD Technology Generations**

PAD Generation	Core Technology /Sensor	Key Detection Features	Defeatable Attack Types	Major Limitations
1st Gen (Rule-Based)	2D Camera, Algorithms	Blinking, head movements	Low-quality prints	Replay, 3D masks, high-quality prints
2nd Gen (Sensor Fusion)	ToF/3D, IR/NIR Sensors	Depth info (3D), spectral characteristics	Prints, simple replays	Hardware costs, depth deception by 3D masks
3rd Gen (ML/DL-Based)	CNN, 2D Video Analysis	Texture, micro-reflections, motion patterns	Dataset-based PAs	Poor generalization, vulnerable to unseen attacks /high-quality 3D masks
4th Gen (Integrated AI)	**Multi-spectrum Sensor, AI Fusion**	**rPPG (pulse signal), Depth, IR/NIR, Temporal Features**	**High-quality 3D masks, deepfake videos**	**High data and computing requirements**

4. Technology Reliability Verification

UNION biometrics' Objective Achievements

UNION biometrics has objectively validated the reliability of its **4th-generation integrated AI technology** through nationally accredited testing institutions.

- **Accredited Institution Verification:**
  - **TTA (Telecommunications Technology Association):** Conducted Verification & Validation tests for the UBio-X Face Pro v1.0 solution, with official results documented in a formal report.
  - **KTL (Korea Testing Laboratory):** Received K-Mark certification for compliance with the KTL C 750-2025 standard, marking it as the first in Korea to be officially certified for face spoofing detection performance. *Access Control System with Spoofed Face Detaction

- **Large-Scale Demonstration Tests:** The system's anti-spoofing performance was validated through a large-scale, repetitive test of **17,500 trials**, utilizing various 2D and 3D spoofed face samples. These tests were conducted under **standard face recognition distance conditions (80cm, 100cm, and 120cm)** by applying performance test scenarios A, B, and C. The system successfully passed all test items, demonstrating excellent defense capabilities against spoofed faces.

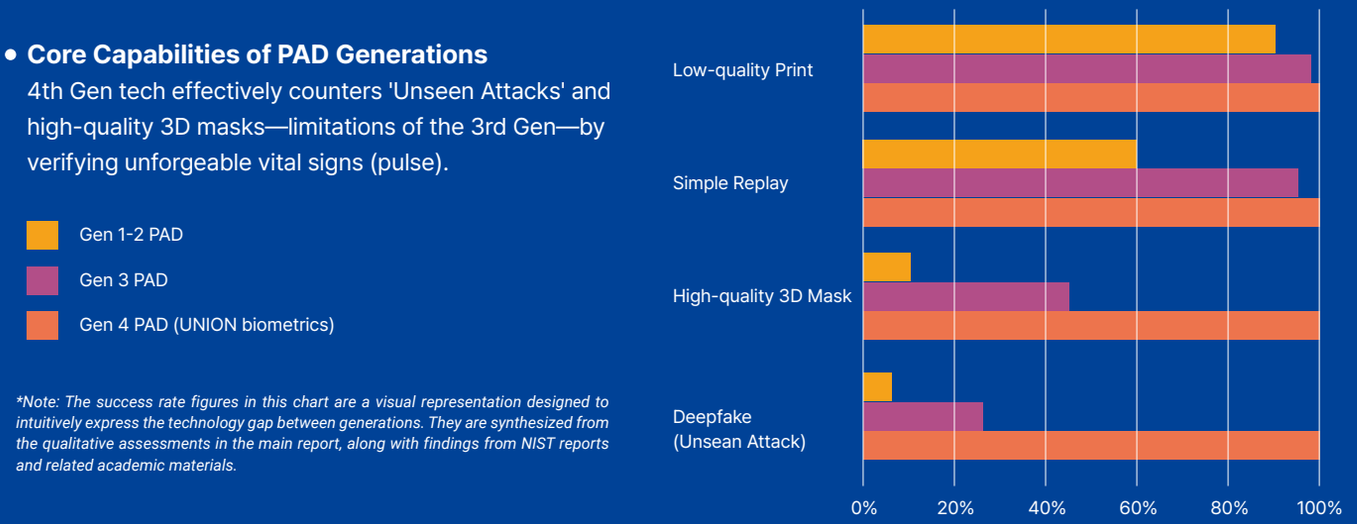
- **AI-Based Adaptive Update Mechanism: Ensuring Long-Term Reliability**

  Faces change over time due to aging and expressions, causing a long-term decline in accuracy. To solve this, UNION biometrics secured a patent for an AI-based **'Method and Apparatus for Updating Face Information' (Acquired Aug. 2025).**

  This technology enables an AI to continuously learn the trend of a user's matching score changes, automatically calculating the most efficient time to update the registered information. This ensures not only immediate threat prevention (Liveness Assurance) but also decades of operational persistence (Long-term Authentication Accuracy).

- **Core Capabilities of PAD Generations**

  4th Gen tech effectively counters 'Unseen Attacks' and high-quality 3D masks—limitations of the 3rd Gen—by verifying unforgeable vital signs (pulse).



Note: The success rate figures in this chart are a visual representation designed to intuitively express the technology gap between generations. They are synthesized from the qualitative assessments in the main report, along with findings from NIST reports and related academic materials.

- **Implications for High-Security Facilities and Technology Integration Strategy**

  UNION biometrics' AI-based patent is associated with the research project titled *"Development of Evaluation Methodology for Nuclear Facility Access Authentication Systems against Biometric Spoofing Threats,"* supported by the **Nuclear Safety and Security Commission (NSSC)** and the **Korea Foundation of Nuclear Safety (KoFONS)**.
  This association indicates that the technology has been designed for application in environments requiring the highest level of security, such as national Class A security facilities.

  The integration of fourth-generation PAD technology with an adaptive AI-based update mechanism provides an optimal solution that simultaneously enhances the two key security metrics required in high-risk environments: Liveness Assurance (PAD) and Long-Term Authentication Accuracy (AI Update).

- **Overview of UNION biometrics' Technology Verification**

Verification Item	Institution/Issuer	Period	Key Standard/Document	Scale and Results
Face Spoofing Detection Performance (PAD)	TTA / KTL	04/14/2025 – 07/15/2025	KTL C 750-2025 (K-Mark)	Passed 17,500 repetitive tests under standard face recognition distance conditions (80/100/120 cm), achieving K-Mark certification.
AI Technology Differentiation	Korean Intellectual Property Office	Acquired Aug. 2025	'Method and Apparatus for Updating Face Information' Patent	AI-based learning of matching score trends for optimal auto-updates
Final Application Reliability	Nuclear Safety and Security Commission / Korea Foundation of Nuclear Safety	Research in progress	Linked to Nuclear Facility Access Authentication System Development	Expected to enhance reliability and operational efficiency for 'Class A' national security facilities

UBio
Your Bio All the Way

5. Conclusion and Policy Recommendations

COTS-based face recognition systems have an inherent vulnerability to spoofing attacks, a problem that must be addressed in high-risk environments. 4th generation integrated AI-based PAD technology, through rPPG and sensor fusion, overcomes the limitations of previous generations and provides a practical, security-oriented alternative.

UNION biometrics has demonstrated the effectiveness and unique technological strength of this advancement through its K-Mark certification and multiple AI patents. This achievement reflects a vision that goes beyond meeting current security standards to leading the future security paradigm. The AI-based intelligent adaptive update mechanism is a core technology for maintaining high accuracy and reliability over long-term operation. Based on this groundbreaking technology, UNION biometrics will play a pivotal role in redefining global security infrastructure standards beyond the domestic market, paving the way for a safer and more trustworthy digital future.

- **Policy Recommendations:** Mandating Standards in High-Risk Environments

1

Mandate 4th Gen PAD Tech

Require integration of rPPG and Depth/IR fusion tech in high-risk environments like airports and financial institutions.

2

Strengthen Standard-Based Verification

Mandate large-scale spoofing detection performance tests based on accredited standards before system deployment.

3

Ensure Long-Term Reliability

Incorporate AI-based adaptive update mechanisms from the initial system design phase.

- **Data Sources:**

- U.S. Government Accountability Office. (2022, July). Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues (GAO-22-106154) - U.S. GAO.
- SITA (2023) Passenger IT Insights 2023. - SITA.
- [2507.07795] Robust and Generalizable Heart Rate Estimation via Deep Learning for Remote Photoplethysmography in Complex Scenarios - arXiv
- [2110.11525] Digital and Physical-World Attacks on Remote Pulse Detection - arXiv
- K-Mark Certification Report - UNION Biometrics Co., Ltd.
- TTA_Spoofed Face Detection Performance Test (UBio-X Face Pro V1.0)_Test Report and Results - UNION Biometrics Co., Ltd.

UNION biometrics Co., Ltd.
Sales Inquiry: +82.2.6488.3207 / www.unionbiometrics.com / salesinquiry@unionbiometrics.com

UNION biometrics