

Biometrics at the Crossroads:

From Impact to Responsibilities

A Vision Talk · IEEE Biometrics Council Leadership Award Lecture

Prof. Ajay Kumar

The Hong Kong Polytechnic University, Hong Kong

*“Now that we have built
contactless biometric
systems,
what kind of future
do we owe
the world?”*

This Honor Is Shared

“When I began working on contactless biometrics over two decades ago, we were struggling with lack of datasets, low-cost sensors, unpredictable lighting, and the improbable dream of identifying people from their mobile or contactless hands.

Today, a billion people unlock their lives with a glance, a touch, or a palm.”

With deepest gratitude to:



My Students

Who asked the hard questions —
and then answered them



Collaborators

Across PolyU, IEEE, and partner
institutions worldwide



IEEE BC Community

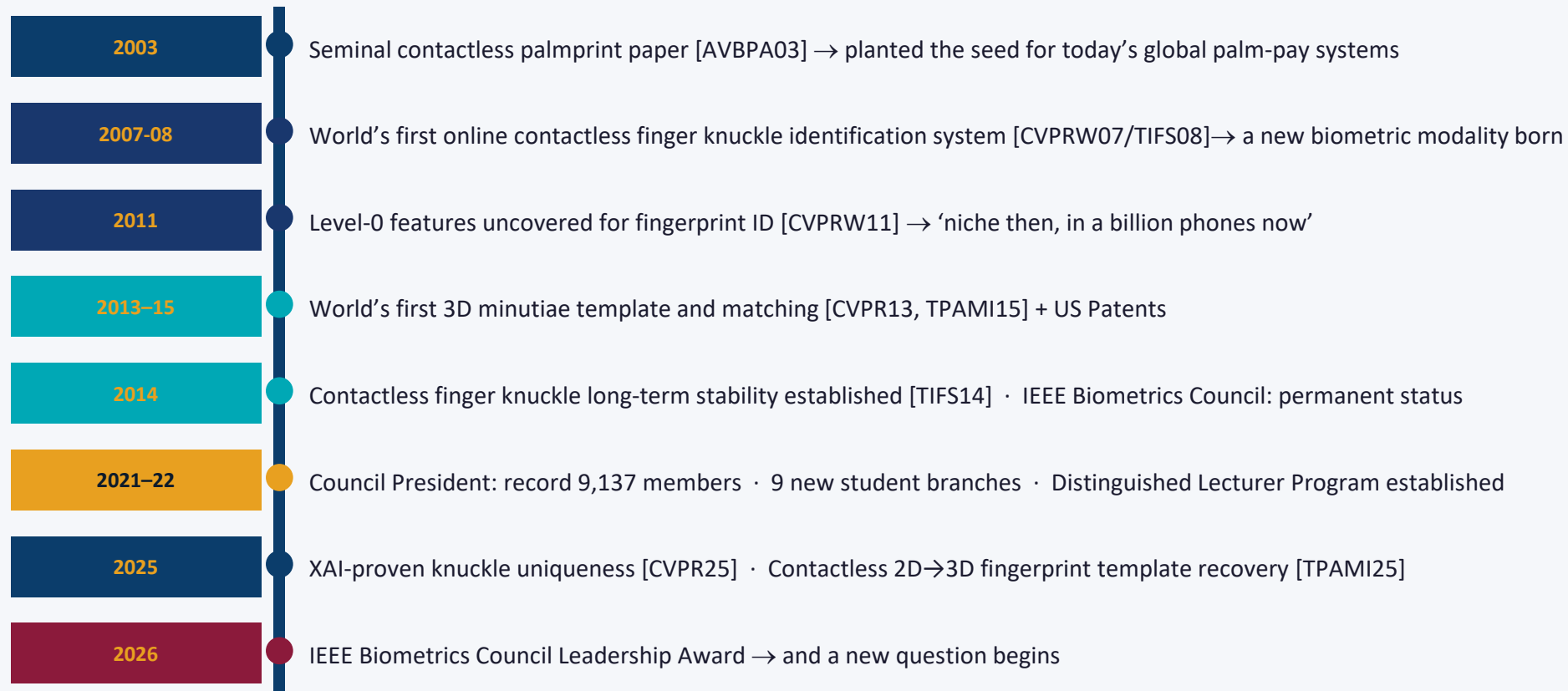
A professional family committed to
advancing responsible biometrics



Family & Mentors

Whose quiet support made the
long hours meaningful

The Journey: 25 Years of Contactless Hand-Based Biometrics



P A R T I

State of the Union:

How Far We've Come

*From lab sensors and academic curiosity to airport e-gates, smartphone unlock,
and global identity infrastructure building for contactless and hand-based biometrics*

Progress with Purpose: Then Vs. Now

THEN (circa 2001)

- X Mostly Ink-and-roll fingerprinting at police stations
- X Heavily controlled illumination & dedicated expensive sensors
- X Laboratory experiments → rarely deployed in practice
- X Datasets: tens and hardly touch hundreds of subjects
- X True Match Accuracy < 90% in challenging conditions
- X Biometrics → criminal identification only

NOW (2026)

- ✓ Contactless fingerprint & palmprint → even from a distance
- ✓ Any smartphone camera, any lighting, any environment
- ✓ Billions deployed: banking, travel, healthcare, retail
- ✓ Datasets: millions → publicly benchmarked globally
- ✓ Near-perfect accuracy on curated benchmarks
- ✓ Identity for inclusion → financial & border access for all

From labs to airports · From 100 subjects to billion-user systems · Contactless biometrics made this possible

What This Community Built: Selected Landmarks in Contactless Hand Biometrics

2003

Contactless Palmprint ID

A paper dismissed as too futuristic became the scientific seed for today's commercial palm-pay and border systems worldwide → Amazon One, Alipay, and beyond

[AVBPA 2003]

2008/11

Contactless Knuckle & Low-Res Fingerprint

World's first contactless finger knuckle system (2007/8) and Level-0 fingerprint features (2011). Called 'niche' at the time → now in a billion smartphones

[CVPRW07/11/TIP2010]

2013–25

3D Fingerprint Minutiae Template and Matching

World's first 3D minutiae templates and matching, 3D Minutiae template from a single contactless 2D image → preserving 3D descriptors without 3D sensors.

[CVPR13, TPAMI15, TPAMI25]

2014+

Contactless Finger Knuckle as a Biometric

Established stability, uniqueness [CVPR25 XAI], and forensic admissibility → empowering courts and law enforcement when contactless knuckle patterns are the only evidence

[T-IFS14, TPAMI20, CVPR25]

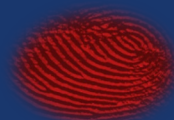
Democratising Research: World-First Open Benchmark Datasets

 WORLD'S FIRST



Contactless 2D/3D
Palmprint DBs

 WORLD'S FIRST



3D Fingerprint
Database

 WORLD'S FIRST



Contactless
Finger Vein DB

 WORLD'S FIRST



3D Finger
Knuckle DB

 MULTIPLE FIRSTS



Contactless Finger
Knuckle DBs

 WORLD'S FIRST



Minor Knuckle
Pattern DB

Used by researchers from THOUSANDS of institutions globally → benchmarking algorithms in academia AND industry

PART II

The Uncomfortable Truths:

What We Have Not Yet Got Right

“As Biometrics Advances, the Challenges Evolve.”

Award winners are expected to critique the status quo → not just celebrate it!

1. Demographic Bias

2. Spoofing and Embodied-fakes

3. Emerging Privacy Risks

Challenge #1: Demographic Bias and Fairness

“If our contactless systems are more accurate for some demographic groups than others, we have not just built recognition, but we have encoded discrimination into infrastructure!”



Performance Disparity

Measurable accuracy gaps across skin tones, agriculture and manual laborers, age groups, and gender, also in commercial contactless systems used at borders and banks today!

Critical



Dataset Homogeneity

Our contactless hand biometric benchmark datasets, including datasets this community released, are demographically skewed and largely from white collar individuals. Systems trained on them inherit those biases invisibly

Urgent



Legal & Regulatory Exposure

The EU AI Act and NIST guidelines now mandate bias audits. Systems that fail face regulatory rejection or documented harm to real people at borders and financial access points

Regulatory

“Every contactless hand recognition faces an emerging generation of attacks: Hyper-realistic synthetic fingerprints, palm-vein enabled contactless palms, and embodied 3D-fake hands, all at consumer-level cost!”

⚠ 2D / 3D Fake Finger & Palm Attacks

High-quality gelatin, silicone hands fool many contactless scanners. Cost has dropped to a consumer level →, no longer requiring a state actor

→ Our contactless fingerprint & palmprint systems must assume adversarial acquisition as a design baseline

⚠ GAN & Diffusion-Synthesised Contactless Biometrics

Gen-AI-based synthetic contactless palmprint and fingerprint images can defeat standard matching algorithms → without any real hand present

→ Contactless palmprint [2003 onwards] must co-evolve urgently with liveness detection

⚠ Covert Contactless Capture

Convenient contactless recognition may also enable covert biometric capture of people in motion, without their awareness, participation, or consent

→ Same technology that improves access enables surveillance: the dual-use problem we must address

3 Challenge #3: Biometrics at Scale: Consent, Control, and Privacy

“Fingerprints cannot be reset like passwords, and palms may be captured remotely without consent. At scale, contactless biometric collection creates enduring risks to privacy, autonomy, and personal identity.”



Contactless → Covert

Contactless fingerprint and palmprint can be acquired from a distance without user consent. The privacy threat model has been fundamentally changed by our own innovations!



Surveillance Capitalism

Biometric data collected for ‘access control’ is increasingly monetized → used to profile behavior, target advertising, and enable discriminatory pricing without explicit consent



Centralised Template Risk

When millions of irreplaceable contactless biometric templates sit in centralised databases, a single breach is permanent. There is no privacy-reset button for your contactless palmprint!

“

**Now that we have built
contactless biometric systems,
what kind of future
do we owe the world?**

The answer defines our vision for 2035

P A R T I I I

Vision 2035:

From Contactless to Conscious

Privacy-first · User-sovereign · Multi-modal · Responsibly governed · Adversarially robust

Five research imperatives that must define the next decade

Privacy-Preserving

Self-Sovereign Identity

Multi-Modal Fusion

Explainable & Fair AI

Anti-Deepfake

FROM: Centralized databases storing permanent contactless biometric templates

TO: On-device matching · cancelable templates · homomorphic verification (verify without ever retaining)



On-Device Processing

Contactless palmprint & fingerprint matching runs entirely on the user's smartphone or smart card. Raw biometric data never leaves the device. Research target: sub-10ms accurate matching on edge hardware with full contactless modality support



Cancelable and Revocable Templates

User-specific, renewable transformations applied to contactless hand biometric templates (2D/3D fingerprint, palm, vascular, or knuckle). If a template is breached, regenerate it with a new key like resetting a PIN, but for your contactless biometric identity



Federated Learning + Encrypted Matching

Train contactless recognition models across distributed devices without sharing raw biometric data. Combined with homomorphic encryption: verify 'match/no-match' on encrypted contactless templates, the server never sees your actual palmprint or fingerprint

The future of identity is not managed by governments, banks, or tech companies.

It is owned by the individual, portable, private, and under their exclusive control.

TODAY: Institution-Centric Identity

- ✗ Your contactless fingerprint stored in a government database
- ✗ Your palm pattern at a retailer's data centre
- ✗ You cannot audit, revoke, or move your own biometric
- ✗ One breach = permanent compromise for millions
- ✗ Contactless capture possible without your knowledge



2035: Self-Sovereign Identity (SSI)

- ✓ Your contactless biometric credential on your own device
- ✓ Decentralized Identifiers (DIDs) → W3C standard
- ✓ Contactless palm/finger authenticates the DID wallet
- ✓ Selective disclosure: prove identity without revealing biometric data
- ✓ Revocable, auditable, fully user-controlled

Vision 3: Seamless Multi-Modal Fusion → The Adaptive Identity Ecosystem

No single biometric trait is sufficient for all scenarios. The future is context-aware, seamlessly fused identity.

3D Fingerprint & Contactless Finger-vein

Our specialty → now consolidate with 3D depth

Finger Knuckle & Vein Patterns

Established with our research → multi-spectral

Behavioural: Gait, Keystroke, Touch

Passive, continuous → invisible to user

Face, Iris and Document Context

Cross-modal consistency checking



Adaptive Fusion Engine

Context-Aware: High-risk transaction demands stronger multi-modal evidence

Continuous and Passive: Fuse signals invisibly as you interact → not just at login

Liveness Built-In: Anti-spoof layer mandatory across all modalities

Fail-Graceful: One modality unavailable? Fusion adapts seamlessly

Hand Identity Central: Palm + knuckle + vein → powerful combined signal from one appendage

“Scientists who do not engage with regulators will have regulation done to them → usually by people who don’t understand the science. XAI gives us the language to engage on equal terms.”

EU AI Act (2024)

Biometric categorization at scale → prohibited. Real-time remote biometric ID in public spaces → restricted to specific cases. High-risk AI systems require mandatory conformity assessment

Our job: Define technical standards that make compliance implementable → not just enforceable

GDPR & PDPA

Biometric data is a ‘special category’ under GDPR requiring explicit consent. Data minimisation and purpose limitation are legal requirements, not design suggestions

Our job: Build systems where privacy-by-design is the architecture, not the afterthought

NIST Bias Standards

Federal agencies must audit biometric systems for demographic performance disparities and report failures publicly via FRVT. Industry is watching closely

Our job: Produce demographically representative benchmarks and build the bias measurement tools compliance requires

“Contactless biometrics now faces an accelerating contest with Gen-AI, making liveness detection and anti-spoof resilience fundamental requirements, not optional safeguards!”

⚠ Gen-AI Threats to Contactless Biometrics

- GAN/diffusion-synthesised contactless fingerprint images defeating matchers
- AI-generated contactless palmprint patterns bypassing commercial recognition
- 3D-printed & deepfake hand models attacking contactless finger & palm sensors
- Synthetic palm vein & contactless finger vein patterns defeating vein systems
- Masterprint attacks: one AI-synthesised palmprint defeating multiple identities

✓ Our Research Agenda: Liveness, Anti-Deep/Embodied-fake

- ✓ Nailbed microcirculation patterns → biological signal AI cannot synthesize
- ✓ Multi-spectral contactless capture (NIR/SWIR) → sub-surface palm/finger vascular patterns
- ✓ Physics-based liveness: 3D depth & pore structure → synthetic images fail geometry tests
- ✓ Adversarial training on GAN-synthesized contactless biometric images from the start
- ✓ Building liveness into every new contactless palmprint, fingerprint and knuckle system

A Challenge to the Next Generation of Biometrics Scientists

To the PhD students and early-career researchers: You inherit both extraordinary algorithms/datasets and extraordinary responsibility!



Work on the Future, Not the Present

The contactless biometrics leaderboard is crowded. The unsolved problems of 2035 await you. Work on something that looks niche today → because niche becomes essential. That is how contactless palmprint became Amazon One or Tencent PalmAI



Build for the Global Majority

Most contactless biometric systems are designed and tested on a small fraction of humanity. Build systems that work for agricultural workers in rural Asia, elderly populations in Africa, children in South America → equally and accurately



Cross the Disciplinary Boundary

Privacy law, ethics, sociology → these are not distractions from biometrics. XAI methods that make your contactless knuckle matcher court-admissible are as important as the matching algorithm itself!



Open Everything You Can

Release your contactless biometric datasets. The greatest accelerant for our field is open access. Our world-first open databases have been used by researchers at thousands of institutions. Your open dataset may outlast your best paper!

Thank You

IEEE Biometrics Council Leadership Award

*To my students, collaborators, and the biometrics community worldwide →
This recognition belongs to all of you!*