Challenges in Biometrics: Security and Permanance

June 2026

Dr. Stephanie Schuckers

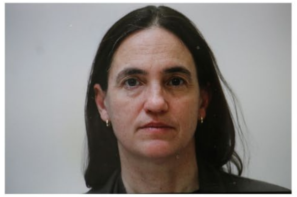
Director, Center for Identification Technology Research (CITeR)

Professor, University of North Carolina - Charlotte

Trust through Liveness

"It Is 'Liveness', Not Secrecy, That Counts."
Denning, Information Security Magazine, 2001

(i.e. a stolen biometric is not useful)


Laptop Display


High-quality photo mask


Low-quality photo paper

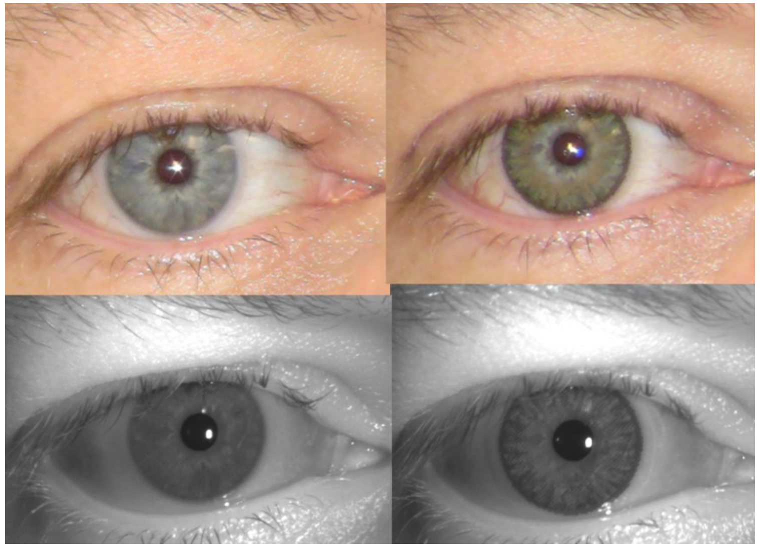

Low-quality 3D mask


Medium-quality 3D mask


High-quality 3D mask

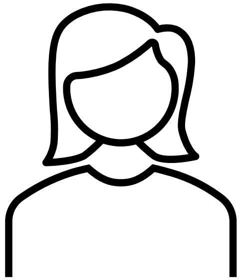
Face Spoofs

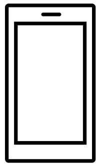
Fingerprint Spoofs



Iris Spoofs

Biometrics - Comparison + Liveness





Biometric Capture

Comparison

Does the sample match the stored reference?

Liveness

Is the sample captured from a live person and NOT a fake?

Decision

Both critical components for effective biometric recognition

Biometric Security—Attack Examples

Presentation Attack Detection
(spoof/liveness detection)

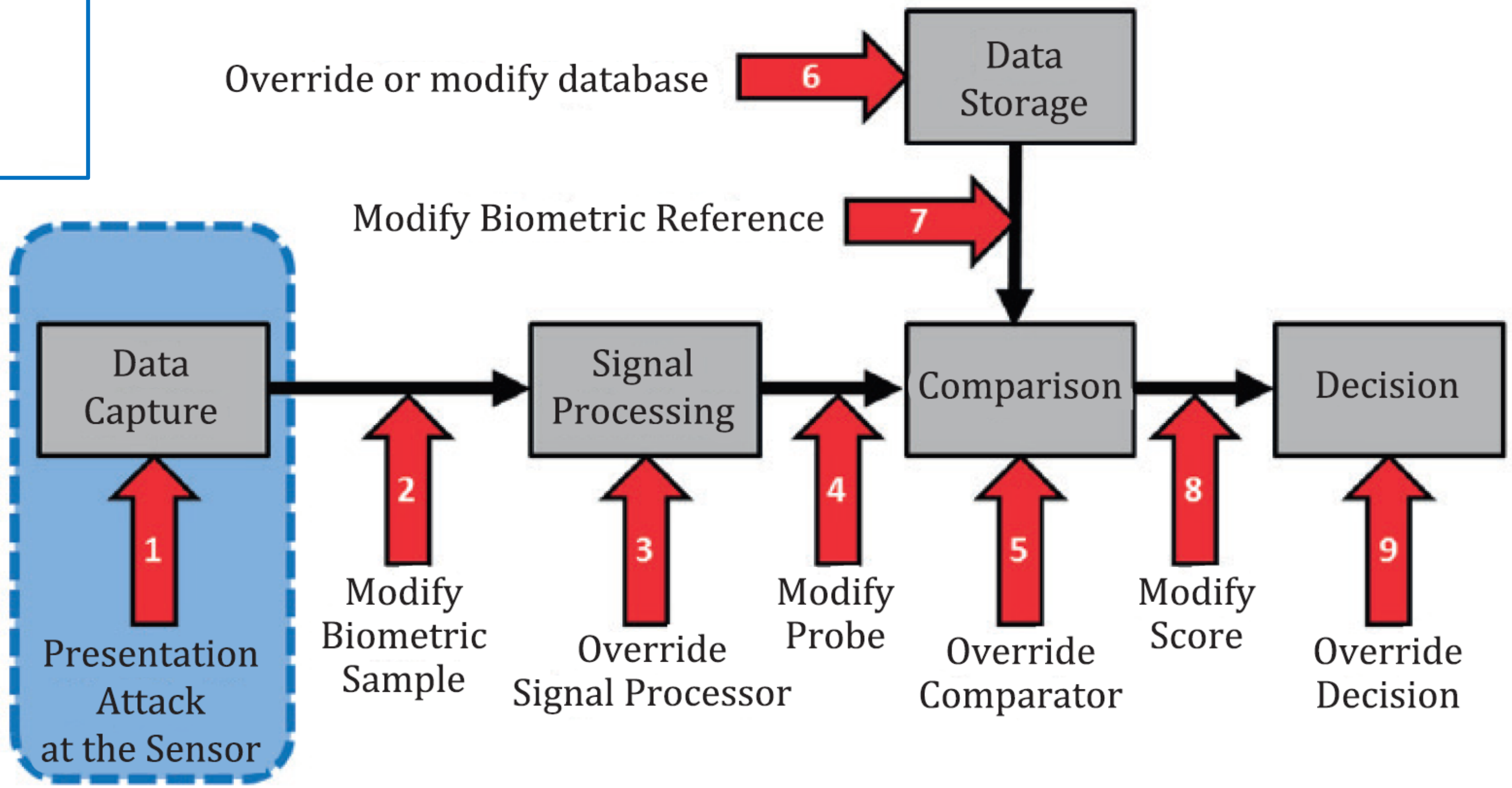


Figure 2 — Examples of points of attack in a biometric system (from ISO/IEC 30107-1)

Best practices in information security should be used throughout the pipeline.

Iphone X - Face

- “To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern.” *

*FaceID Security Guide, 2017, https://www.apple.com/business/site/docs/FaceID_Security_Guide.pdf

PAD Categories defined in ISO 30107

1. Liveness not related to challenge-response (“passive”)*
2. Involuntary Challenge Response

   e.g. random colors of light; change in pupil dilation due to random input
3. Voluntary Challenge Response

   e.g. blinking/smiling at a specific time; saying specific words that are randomly given

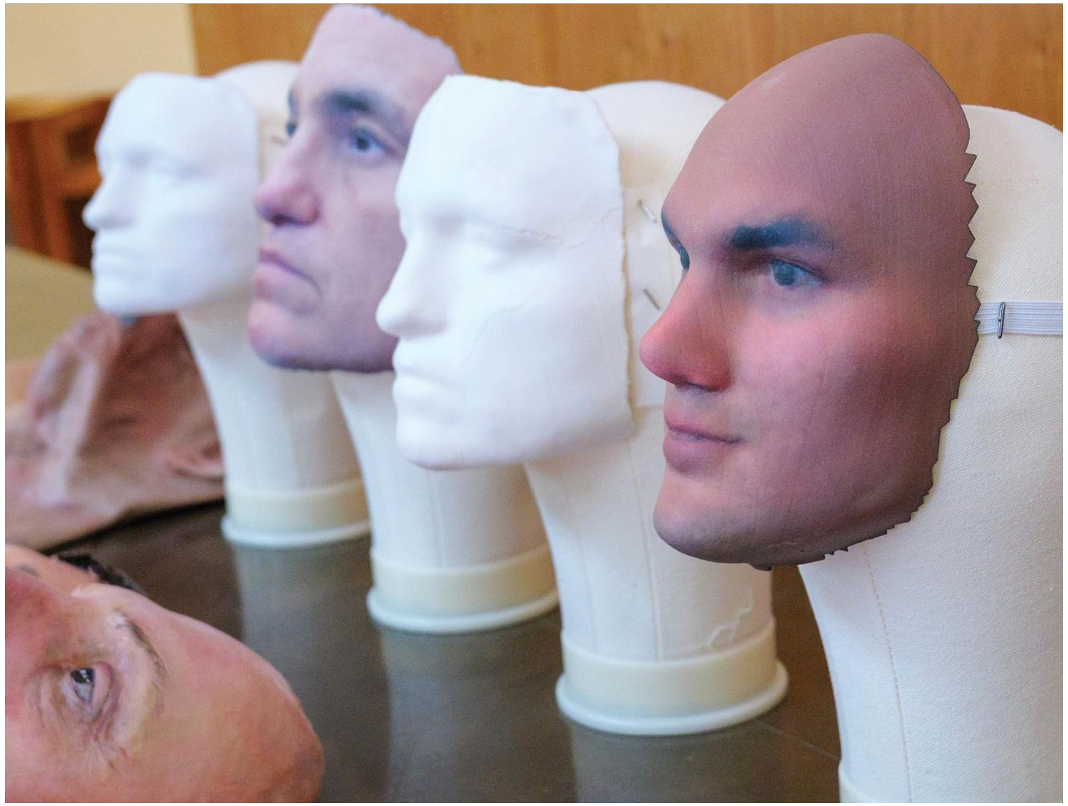
*Active PAD not defined in ISO

From: ISO/IEC 30107-1, Information Technology — Biometrics -- Presentation Attack Detection

Challenge

Evaluation of PAD needed to ensure usable, effective performance in the face of evolving attacks

Lab Controlled Spoofing



CITeR Center for Identification Technology Research

Benchmark Datasets from LivDet

- Over 100,000 spoof and lives images shared
- Over 400 requests from over 40 countries

LivDet 2009

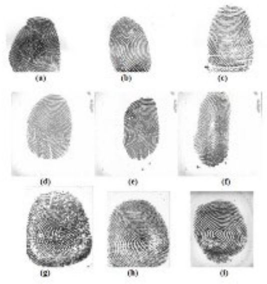
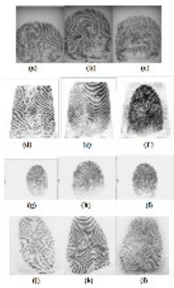


Figure 4: Examples of spoof images of the LivDet 2009 datasets. Crossmatch (top): (a) Play Doh, (b) gelatin, (c) silicone; Identix (middle): (d) Play Doh, (e) gelatin, (f) silicone; Biometrika (top): (g) Play-Doh, (h) gelatin, (i) silicone.

LivDet 2011



LivDet 2013

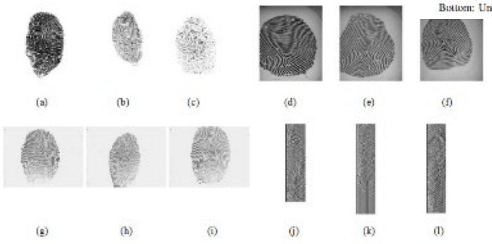
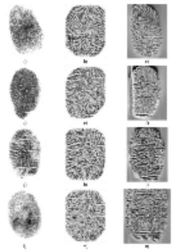


Figure 6: Examples of fake fingerprint images of the LivDet 2013. From Crossmatch (a) body double, (b) latex, (c) wood glue, from Biometrika (d) gelatine, (e) latex, (f) wood glue, from Italdata (g) gelatine, (h) latex, (i) wood glue, from Swipe (j) body double, (k) latex, (l) wood glue.

LivDet 2015

LivDet 2019



LivDet 2021 to 2025

(a) GB CC (b) DL CC (c) GB SS (d) DL SS

LivDet 2025

(a) Printed Finger photo (b) Ecoflex PAI (c) Latex PAI (d) Playdoh PAI (e) Wood Glue PAI (f) Live (g) Synthetic Fingertip PAI

LivDet-Iris 2017

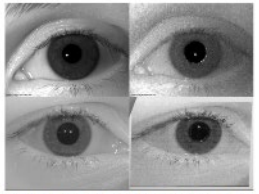


Figure 2. Sample images from Warsaw dataset. Left Top: Known Live, Right Top: Known Print, Left Bottom: Unknown Live, Right Bottom: Unknown Print.

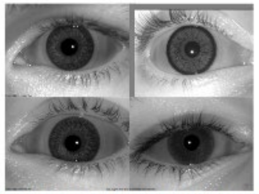


Figure 3. Sample images from Notre Dame dataset. Top: Known Patterned Contact, Bottom: Unknown Patterned Contacts.

LivDet-Iris 2015

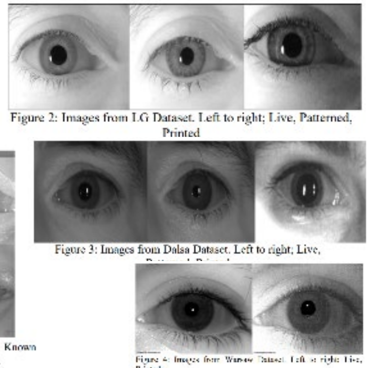
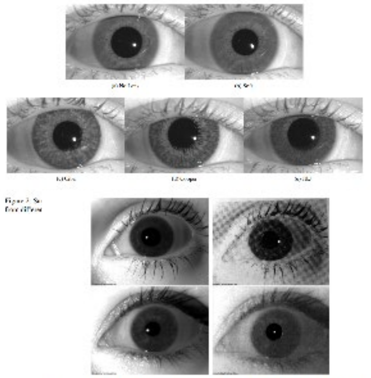


Figure 2: Images from LG Dataset. Left to right; Live, Patterned, Printed

Figure 3: Images from Dalsa Dataset. Left to right; Live,

LivDet-Iris 2013



LivDet-Iris 2020

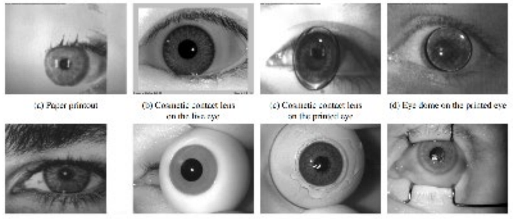
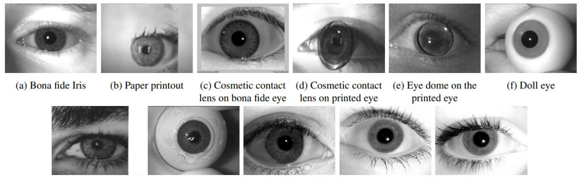


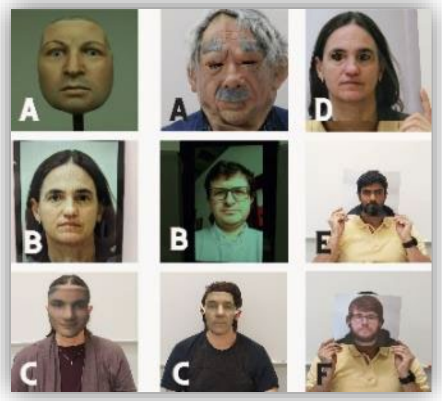
Figure 1: Example images of all presentation attack types present in the LivDet-Iris 2020 test dataset

LivDet-Iris 2023

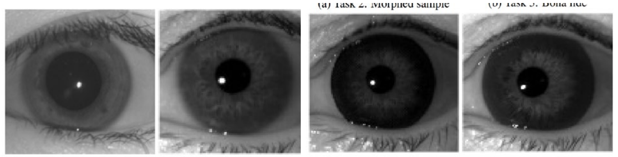


(a) Bona fide Iris (b) Paper printout (c) Cosmetic contact lens on bona fide eye (d) Cosmetic contact lens on printed eye (e) Eye dome on the printed eye (f) Doll eye (g) Electronic display (h) Cosmetic contact lens on the doll eye (i) Synthetic Iris (Low Quality) (j) Synthetic Iris (Medium Quality) (k) Synthetic Iris (High Quality)

LivDet-Face 2021

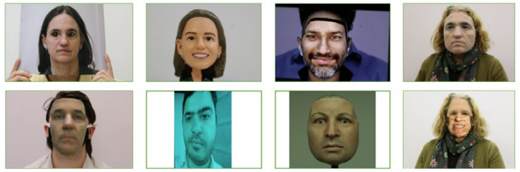


LivDet-Iris 2025



(a) Task 2: Morphed sample (b) Task 3: Bona fide (c) Task 3: Pixelated (d) Task 3: High quality

LivDet-Face 2025



Purnapatra, et al 2023. Liveness Detection Competition-Noncontact-based Fingerprint Algorithms and Systems (LivDet-2023 Noncontact Fingerprint). In 2023 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-10). IEEE.
Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G.L. and Schuckers, S.C., 2022. Review of the Fingerprint Liveness Detection (LivDet) competition series: from 2009 to 2021. arXiv preprint arXiv:2202.07259.
Igene, L. et al, 2024, September. Face Liveness Detection Competition (LivDet-Face)-2024. In 2024 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-9). IEEE.
Tinsley, P., et al, 2023, September. Iris liveness detection competition (livdet-iris)–the 2023 edition. In 2023 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-10). IEEE.
Purnapatra, S, et al., 2023, September. Liveness detection competition-noncontact-based fingerprint algorithms and systems (livdet-2023 noncontact fingerprint). 2023

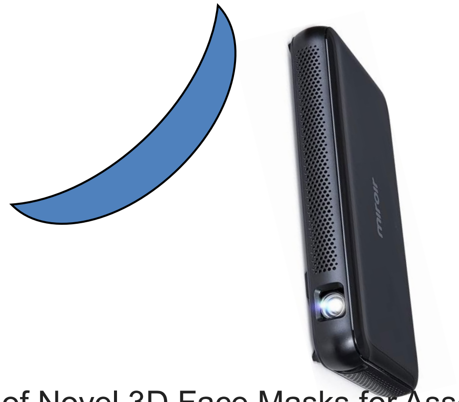
Data collection process for mannequin and white mask face projection

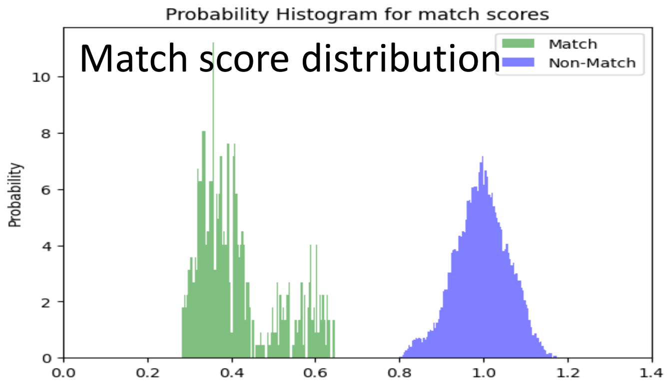
Mannequin head

- Projector display resolution 1920 x 1080.
- Under various lighting conditions.
- Images were collected using a DSLR and an iPhone camera sensor.

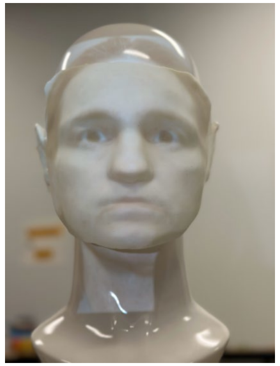
Image projection

Projector



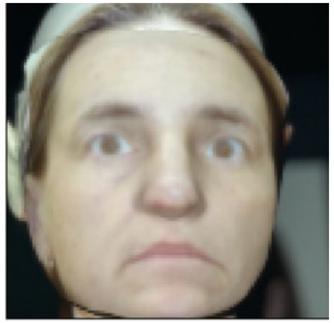


White resin 3D mask

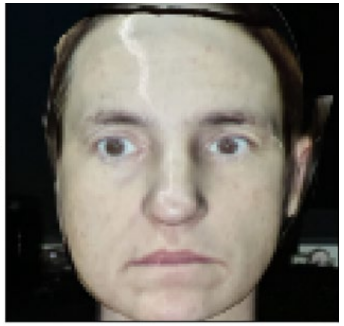


White filament 3D mask

White resin 3D mask with projection



White filament 3D mask with projection



Igene, L, et al 2024, September. Development of Novel 3D Face Masks for Assessment of Face Recognition Systems.

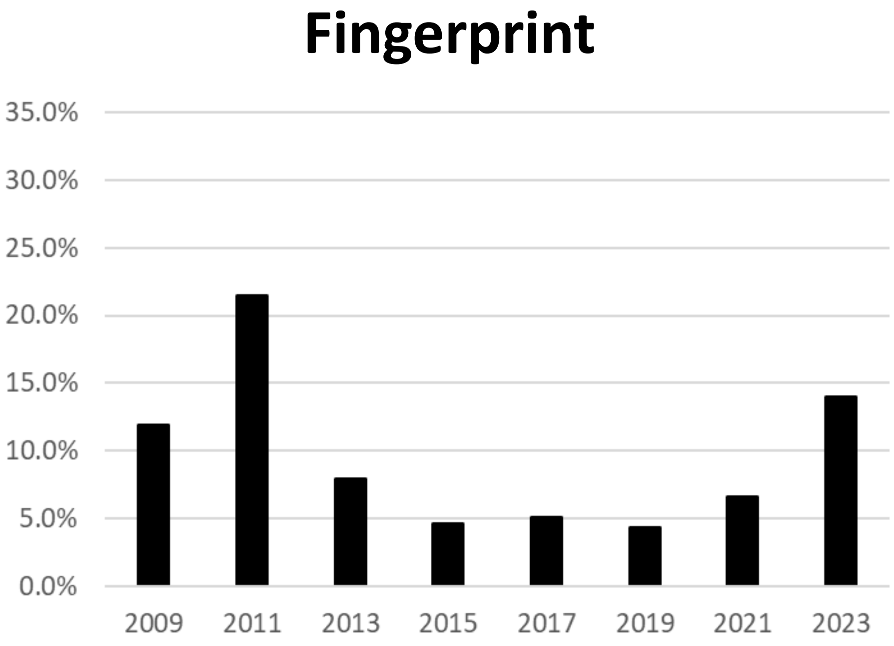
Spoofing/obscuration at a distance

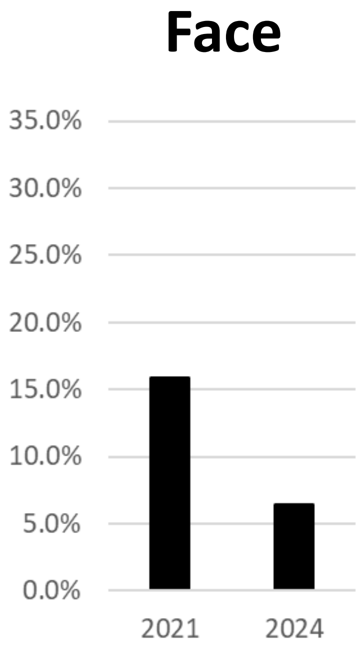
- Multi-distance benchmark: Fixed stand-off distances (1–100 m).
- Multi-session, multi-environment: 283 sessions across indoor and outdoor settings
- Image and video data

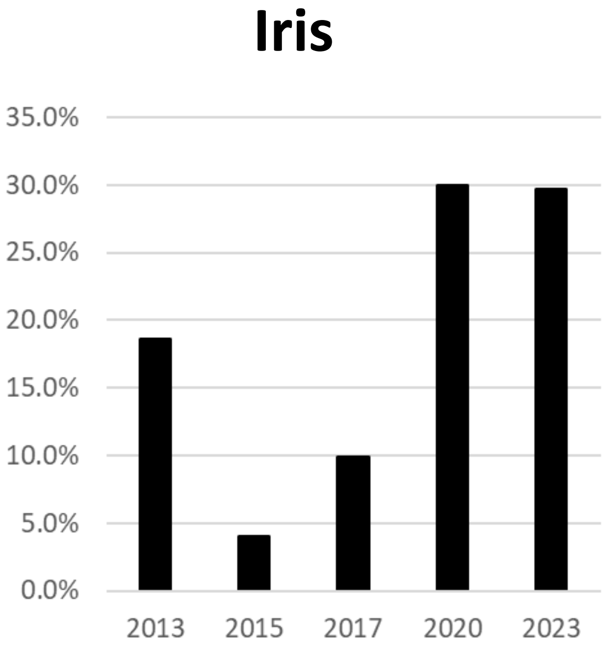
Chowdhury, et al, "MORSE-Face: A Multi-Distance Occlusion-Rich Spoof and Real Face Dataset." IEEE DataPort. DOI: https://dx.doi.org/10.21227/pw2z-ya50.

Chowdhury, et al, MORSE-Face Dataset: A Multi-Distance, Occlusion-Rich, Real and Spoof Evaluation Face Dataset, submitted, 2026

LivDet over the years







Average of APCER and BPCER for top two performers across all databases tested in LivDet competitions

Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G.L. and Schuckers, S.C., 2022. Review of the Fingerprint Liveness Detection (LivDet) competition series: from 2009 to 2021. arXiv preprint arXiv:2202.07259.
Yambay, D., et al, 2023. Review of iris presentation attack detection competitions. In Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment (pp. 149-169). Singapore: Springer Nature Singapore.

*Crossmatch removed

Lesson

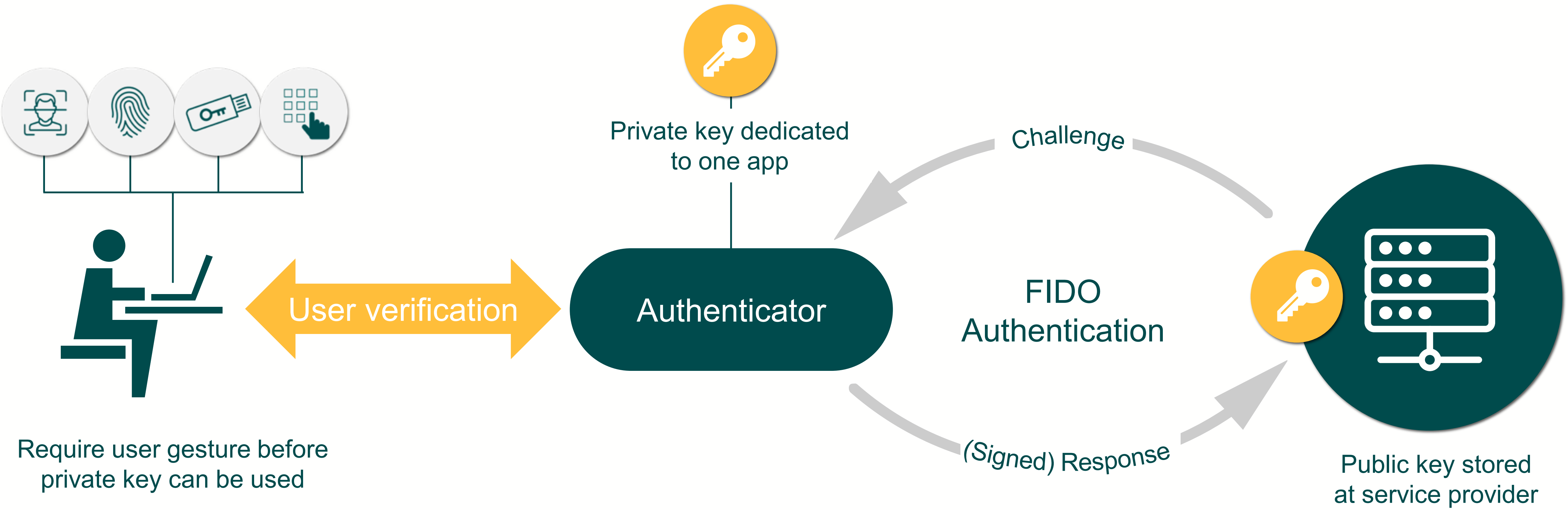
While academic (and commercial) algorithms are improving,
PAD is still not a solved problem.

SHORT DETOUR

Challenge

Replace weak passwords and phishable second factors with strong authentication

FIDO Authentication “Passkey”: How it works



Based on ISO standards

Independent network of laboratories

Challenge

Lack of an ecosystem of
certified biometrics products

Requirements defined by subject matter experts

FIDO IDV and Biometric Certification

Document Authenticity

- Tests for authenticity of government-issued ID documents
- Verifies the authenticity of government-issued documents during initial account set up and account recovery (i.e., employees, citizens)
- Complements the FIDO IDV Face Verification program

Face Verification

- Tests for security, bias, accuracy, and liveness of facial biometrics
- Verifies identities using “selfie-match” technology matched to the user’s government-issued ID (i.e., employee onboarding with I-9 and passport)
- Complements the IDV Document Authenticity program

Biometric Components

- Tests for security, bias, and accuracy of biometric performance during FIDO authentication
- Assures performance, interoperability, and security of biometric components used in FIDO authentication
- Complements the FIDO Certified Authenticator program

Spoof Type Triaged by Attack Potential

		Fingerprint	Face	Iris/Eye	Voice
Level A	***Time***: <1 day ***Expertise***: layman ***Equipment***: standard	paper printout, direct use of latent print on the scanner	paper printout of face image, mobile phone display of face photo	paper printout of iris image, mobile phone display of iris photo	replay of audio recording
	Source of biometric characteristic: easy to obtain	lift of fingerprint off the phone	photo from social media	photo from social media	recording of voice
Level B	***Time***: <7 days ***Expertise***: proficient ***Equipment***: standard, specialized	fingerprints made from artificial materials such as gelatin, silicon.	paper masks, video display of face (with movement and blinking)	video display of an iris (with movement /blinking); paper printout w/ contact lens/doll eye	replay of audio recording of specific passphrase, voice mimicry, voice synthesis (easy)
	Source of biometric characteristic: moderate	Lift of latent print from elsewhere, stolen fingerprint image Cooperative molds - out of scope	video of subject, high quality photo	video of subject, high quality photo	recording of voice of specific phrase
Level C	**Time**: >7days **Expertise**: expert(s) **Equipment**: specialized. bespoke	3D printed spoofs	silicon masks, theatrical masks, deepfake display	contacts lens or prosthetic with a specific pattern	voice synthesizer (sophisticated)
	Source of biometric characteristic: difficult	3D fingerprint information from subject	3D face information from subject	high quality photo in Near IR	multiple recordings of voice to train synthesizer

Schuckers, et al FIDO Biometrics Requirements 4.1, January 06, 2025; https://fidoalliance.org/specs/biometric/requirements/Biometrics-Requirements-v4.1-fd-20250106.html

CITeR
Center for Identification Technology Research

Challenge

Trust in technology—Securing Against the Use of Deepfakes that Interfere with Biometric Recognition

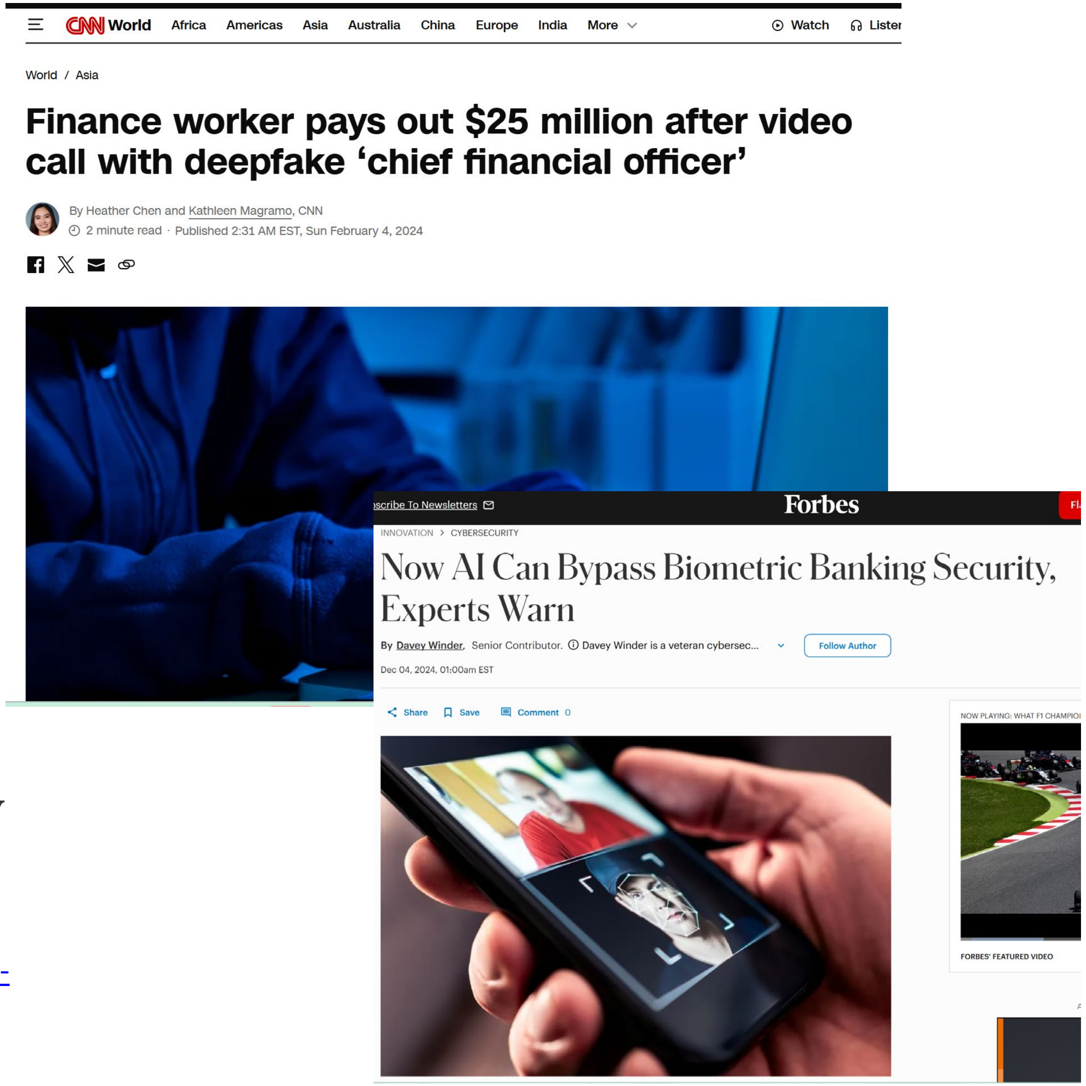
Government of Canada Gouvernement du Canada

U.S. Department of Homeland Security — DHS at 20 — Science and Technology

Challenge: Deepfakes and Biometric Recognition

Problem:

- May interfere with biometric recognition
  - E.g. can impart “liveness” characteristics to a stolen image



World / Asia

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Forbes

INNOVATION > CYBERSECURITY

Now AI Can Bypass Biometric Banking Security, Experts Warn

By Davey Winder, Senior Contributor. Davey Winder is a veteran cybersec...

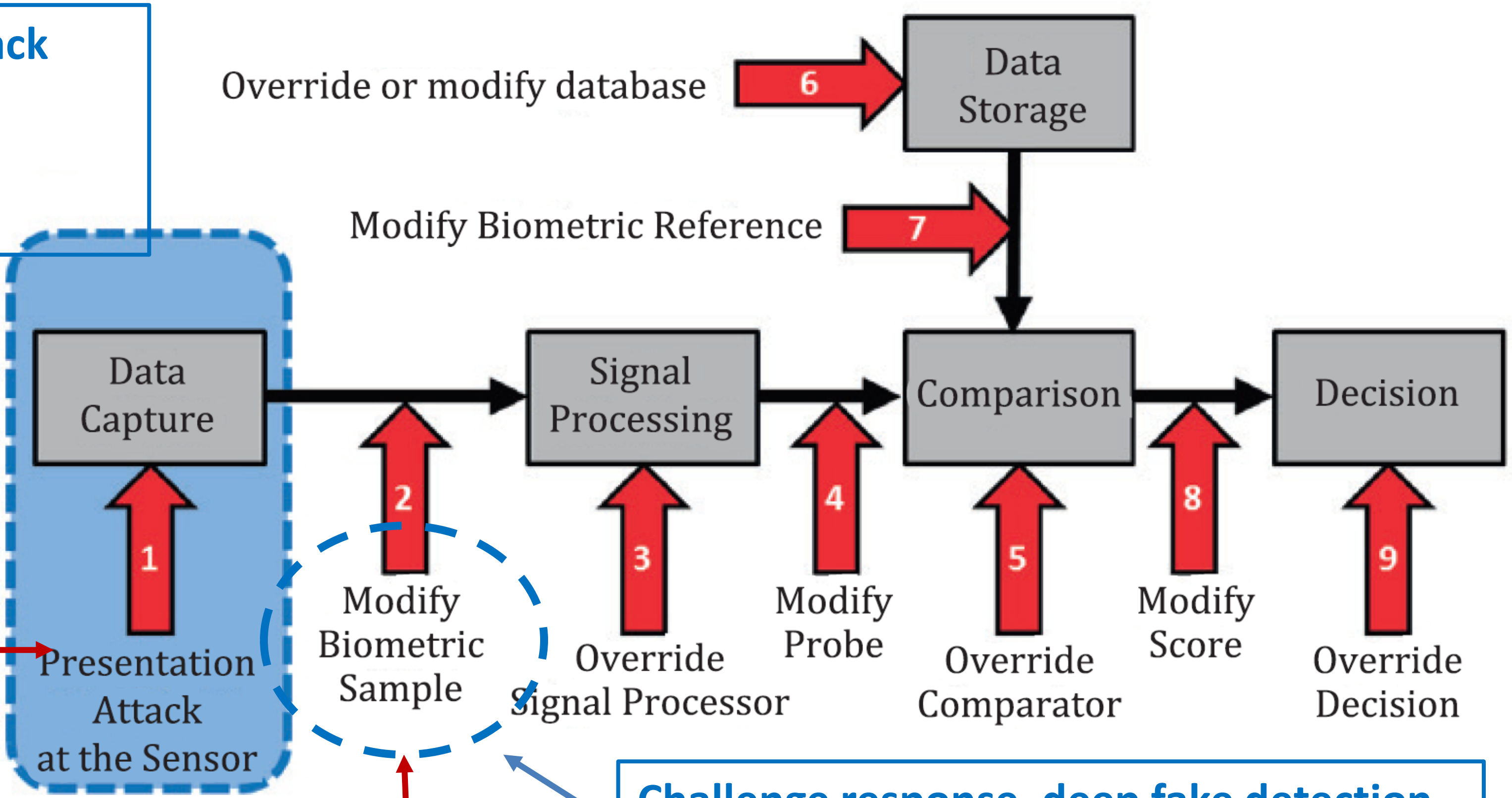
Dec 04, 2024, 01:00am EST

“.....face-swapping technologies enable attackers to replace one person’s face with another’s in real time using just a single photo........[and] deceive facial recognition systems due to their seamless, natural-looking swaps and the ability to convincingly mimic real-time expressions and movements.”

https://www.forbes.com/sites/daveywinder/2024/12/04/ai-bypasses-biometric-security-in-1385-million-financial-fraud-risk/

Biometric Security—Attack Examples

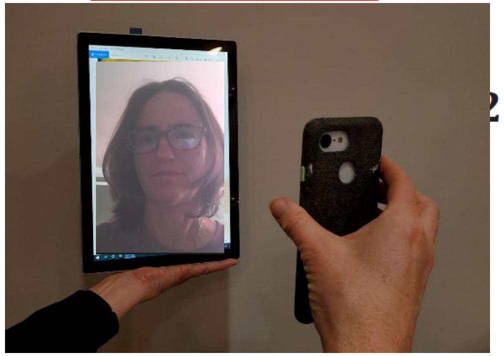
Presentation Attack Detection (spoof/liveness detection)



Present Deep Fake to Biometric Sensor

Challenge response, deep fake detection (e.g., random pattern on face)

2 — Examples of points of attack in a biometric system (from ISO/IEC 30107-1)



"Inject" Deep Fake Bypassing the Sensor

PAD and Injection Attacks

Presentation Attack Detection*

- ISO/IEC 30107
- Categories
  - Liveness not related to challenge-response ("passive")
  - Involuntary Challenge Response
    - e.g. random colors of light; change in pupil dilation due to random input
  - Voluntary Challenge Response
    - e.g. blinking/smiling at a specific time; saying specific words that are randomly given

*Active PAD not defined in ISO

Injection Attack Detection

- ISO/IEC 25456 (under development)
- Possible similar solutions:
  - Deepfake detection not related to challenge-response ("passive")
  - Involuntary Challenge Response
    - e.g. random colors of light; change in pupil dilation due to random input
  - Voluntary Challenge Response
    - e.g. blinking/smiling at a specific time; saying specific words that are randomly given
  - Best practices in IT security

Threats: Challenges in Face Recognition Technology

CITeR
Center for Identification Technology Research

Demo of a real-time deepfake spoofing the keynote speaker @ Authenticate 2025

Matched-unmatched frames example of SimSwap model

*Green frames = Matched; *Red frames = Unmatched

Source Identity


Target Actions


Face Swap

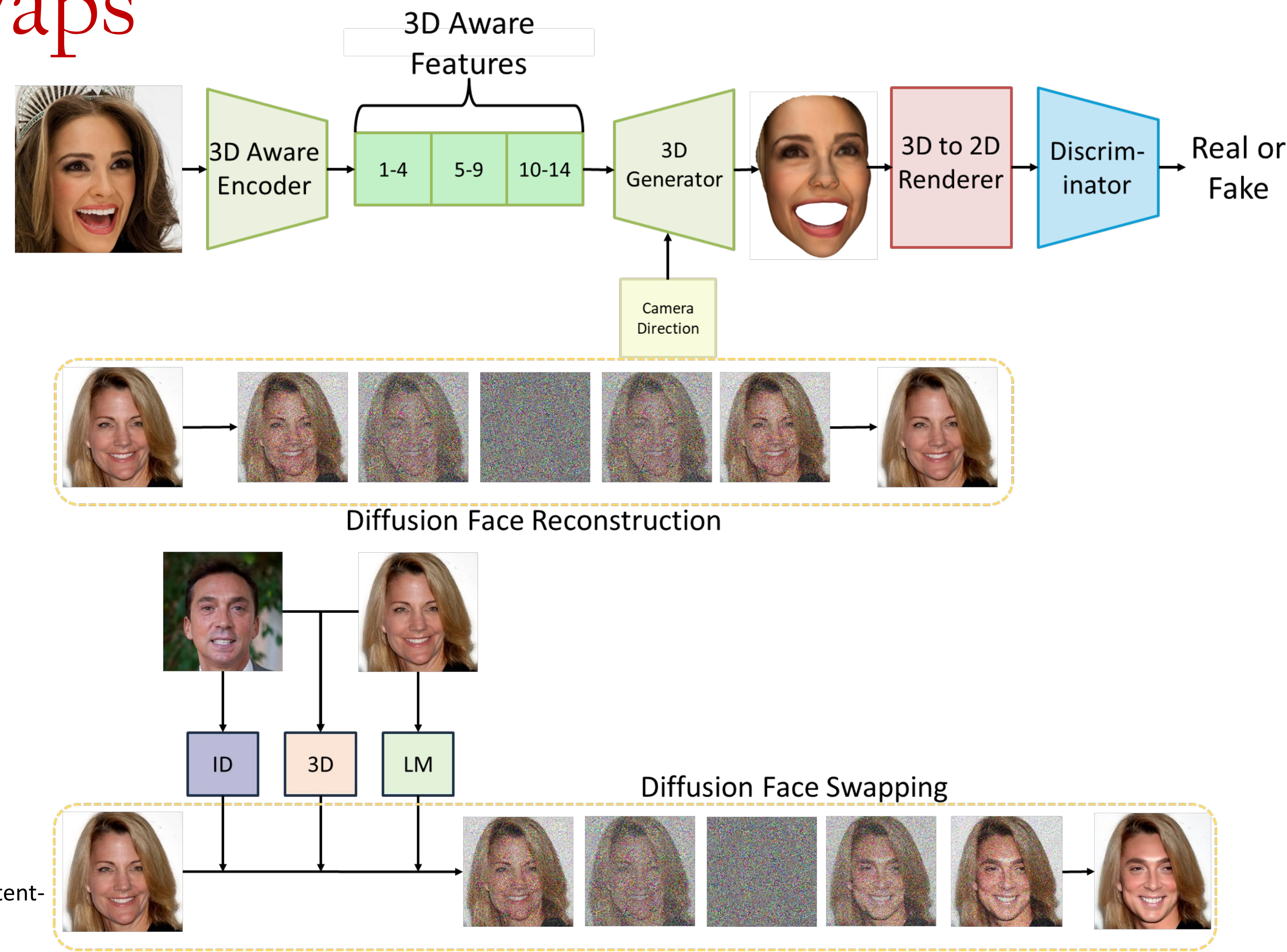
Identity Preservation Results Across Various FaceSwap Models – High Resolution

Pair	REFace	CanonSwap	VFace	BlendFace	GHOST	DeepFaceLab	E4S	3dSwap	VividFace	Reliable Swap	FaceDancer
Pair1 (000_525)	90.00%	99.33%	84.67%	68.00%	100%	100%	0.00%	0.00%	0.00%	99.33%	26.00%
Pair2 (074_829)	53.33%	73.33%	77.33%	0.00%	100%	100%	76.00%	0.00%	0.00%	44.67%	0.00%
Pair3 (082_132)	56.67%	99.33%	99.33%	0.00%	100%	100%	68.67%	0.00%	0.00%	72.00%	46.67%
Pair4 (117_769)	91.33%	36.67%	80.00%	2.00%	100%	100%	48.67%	0.00%	0.00%	86.67%	51.33%
Pair5 (658_416)	94.00%	60.67%	62.67%	0.00%	100%	99.33%	45.33%	0.00%	0.00%	2.67%	80.67%
Average	**77.07%**	**73.87%**	**80.80%**	**14.00%**	**100%**	**99.87%**	**47.73%**	**0.00%**	**0.00%**	**61.07%**	**40.93%**

Jahangir Khondkar, Weston Bondurant, Srijan Das, S. Schuckers, Unpublished

Example Face Swaps

- Face swapping is primarily evaluated on pose, expression, and identity preservation
- Preserving source face identity makes it more challenging to preserve target face pose and expression
- New method, Diffswap++, estimates 3D features in order to better preserve identity



W. Bondurant, Srijan Das, et al, DiffSwap++: 3D Latent-Controlled Diffusion for Identity-Preserving Face Swapping, 2025

Example Face Swaps

W. Bondurant, Srijan Das, et al, DiffSwap++: 3D Latent-Controlled Diffusion for Identity-Preserving Face Swapping, 2025

Quantitative Results

CelebA (In Domain)

Method	FID↓	ID retrieval ↑ Top-1	ID retrieval ↑ Top-5	Pose↓	Expr.↓
HiFiFace [34]	13.97	86.4%	93.9%	3.01	1.19
FaceDancer [29]	12.25	79.0%	92.9%	2.32	**0.65**
DiffFace [16]	9.49	93.0%	97.2%	3.19	1.01
DiffSwap [38]	8.29	16.9%	34.9%	**2.13**	0.76
SimSwap [5]	10.61	90.3%	93.3%	2.21	0.78
REFace [1]	7.01	92.7%	96.9%	3.30	1.01
DiffSwap++ (w/o 3D)	8.80	86.0%	94.1%	3.48	1.06
DiffSwap++	**6.42**	**94.7%**	**98.2%**	3.29	1.00

FFHQ (Out of Domain)

Method	FID↓	ID retrieval ↑ Top-1	ID retrieval ↑ Top-5	Pose↓	Expr.↓
HiFiFace [34]	11.85	74.0%	86.3%	3.20	1.39
FaceDancer [29]	9.45	75.9%	87.6%	2.43	**0.70**
DiffFace [16]	8.72	86.9%	94.0%	3.67	1.30
DiffSwap [38]	**6.21**	34.9%	55.7%	2.43	1.03
SimSwap [5]	9.48	77.8%	81.7%	**2.39**	0.92
REFace [1]	6.45	91.0%	95.5%	3.69	1.07
DiffSwap++ (w/o 3D)	9.95	84.2%	92.4%	3.56	1.09
DiffSwap++	6.57	**95.1%**	**98.4%**	3.70	1.07

User Study

Method	ID	Expression	Pose
DiffSwap++	**3.46**	3.14	3.65
REFace	3.2	3.22	3.48
HifiFace	2.58	2.72	3.08
DiffSwap	2.46	**3.57**	**4.11**

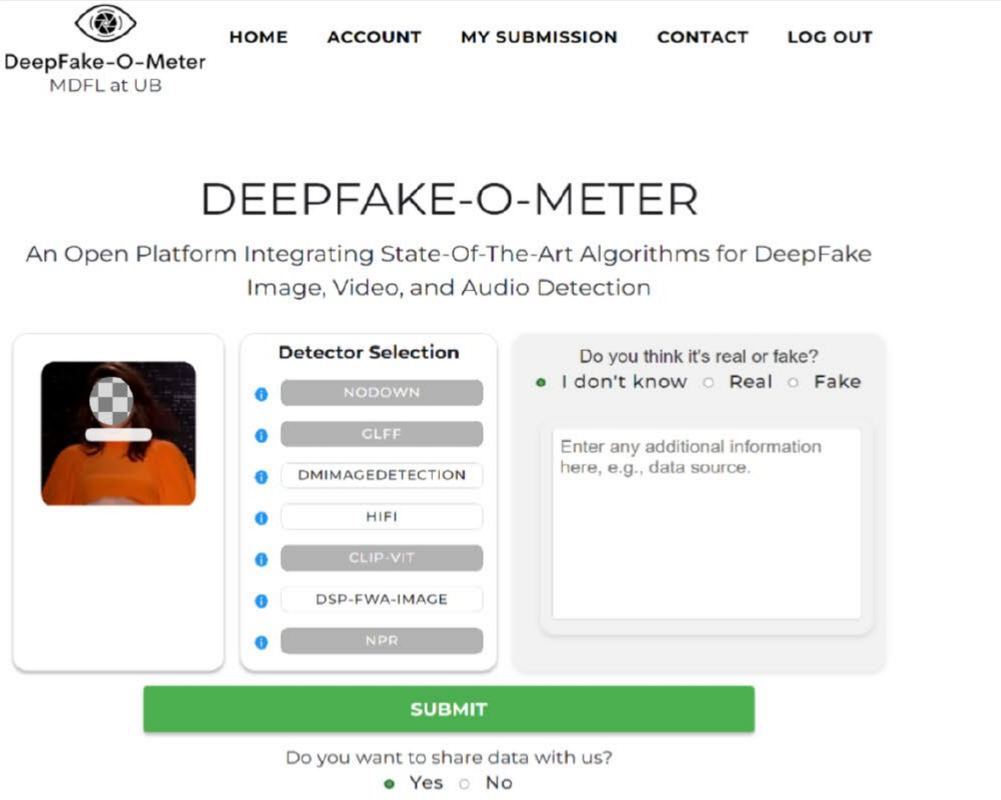
- Performance validated on 2 public datasets.
- User study reveals DiffSwap++ preserves identity

W. Bondurant, Srijan Das, et al, DiffSwap++: 3D Latent-Controlled Diffusion for Identity-Preserving Face Swapping, 2025

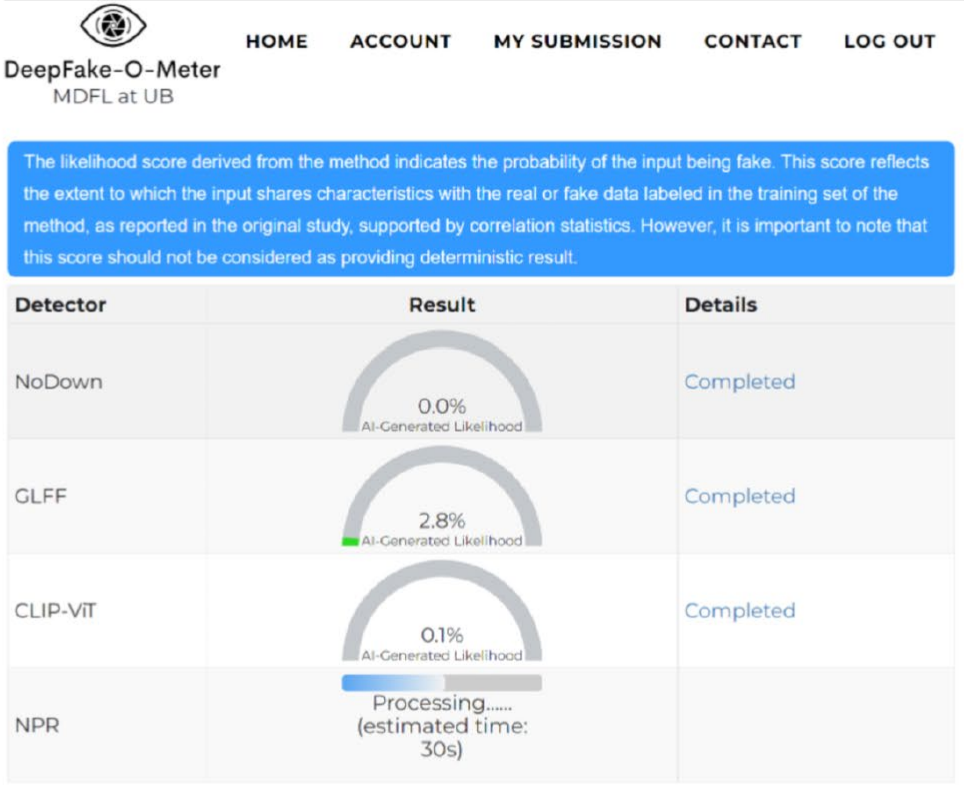
CITeR Center for Identification Technology Research

Deepfake-O-Meter

(a) Homepage



(b) Result Page



Try it!

https://zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/home_login

Ju, Y., et al., 2024, August. DeepFake-O-Meter v2. 0: An open platform for DeepFake detection.

Lesson

Some liveness solutions (e.g. challenge response) may be useful for both PAD and IAD. The difference is how you evaluate – physical attacks versus digital attacks.

Challenge

Effective biometric recognition for children

CertaScan Technologies

ST LAWRENCE HEALTH
An Affiliate of Rochester Regional Health

Potsdam Central School District

CITeR
Center for Identification Technology Research

Synolo™ Biometrics, Inc.

Real-World Uses of Biometrics in Children

Brazil's Bebê ID project: Neonatal biometric birth registration from birth [1]

- Ensures civil identity from birth → reduces risk of false identity claims later in life
- Strengthens public safety → combats baby swapping (~500 cases/year) & kidnapping.

Bangladesh: Infant biometrics for vaccination tracking [2]

- Partnership between Gavi, Simprints, Ministry of Health.
- Piloted in 50 clinics with 5,000+ children enrolled.
- Fingerprints captured at first measles vaccine, then verified on return visits to ensure correct follow-up doses.

Biometrics in schools [3]

- **Europe (UK, France, Belgium)**: Used for meals, library, attendance under strict privacy laws.
- **India**: Aadhaar supports student ID & welfare access.
- **China:** Used for attendance & behavior monitoring, feeding into the social credit system
- **United States**: Some schools piloted facial recognition for security (e.g., shooting prevention)

1. https://www.biometricupdate.com/202505/bebe-id-project-records-infant-biometrics-with-infant-id-tech
2. https://integratedbiometrics.com/articles/no-child-left-behind-how-digital-identity-ensures-lifelong-immunization?utm_source=chatgpt.com
3. https://recfaces.com/articles/collecting-biometrics-of-minors?utm_source=chatgpt.com

Data Collection Overview : Child Dataset

Subjects : 364 (4-18 years old)

Modalities (7) : Iris, face, fingerprint, palmprint, footprint, voice, and ear.

Time Span: 9.5 years

Sessions : 19 biannual sessions (4 sessions missed due to covid-19).

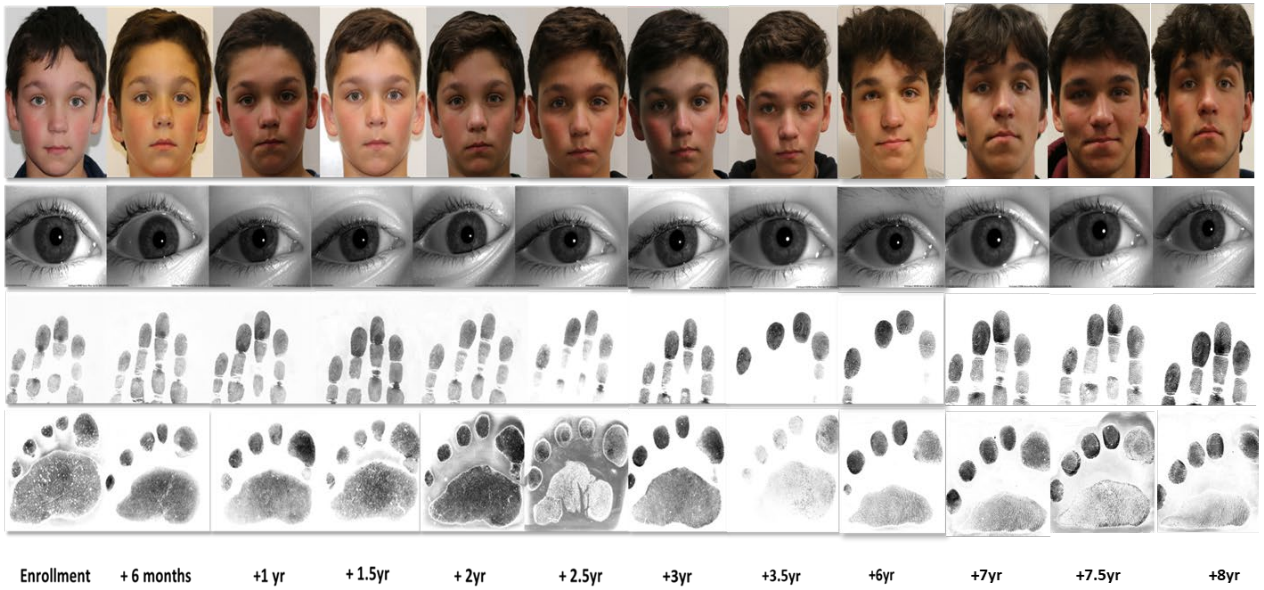


Figure : Sample data from multimodal longitudinal child dataset

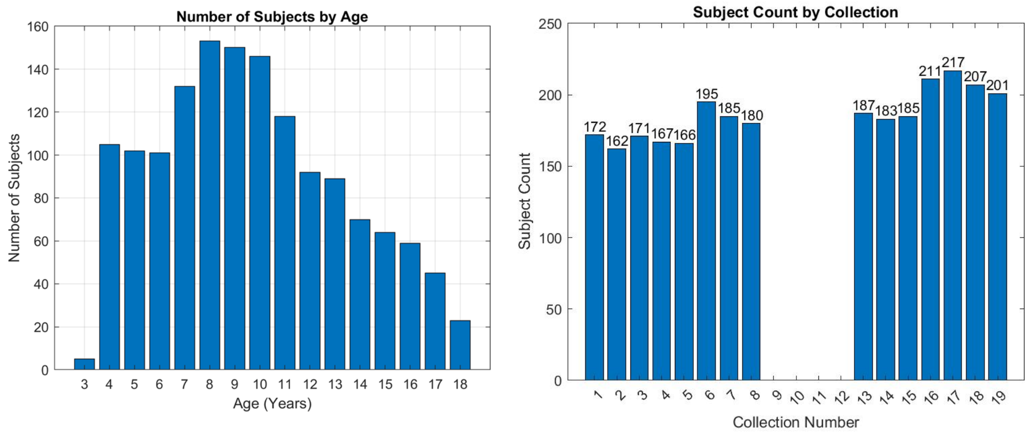


Figure: Age and subject count statistics of all the completed child data collections (1st - 19th). Collection 9-12 not performed due to COVID-19.

Data Collection Overview : Infant and Toddler Dataset

Subjects : 32 (0-3 years old)

Modalities (6) : Iris, face, fingerprint, palmprint, footprint, and ears.

Time Span: 2 years

Sessions : 8 sessions.

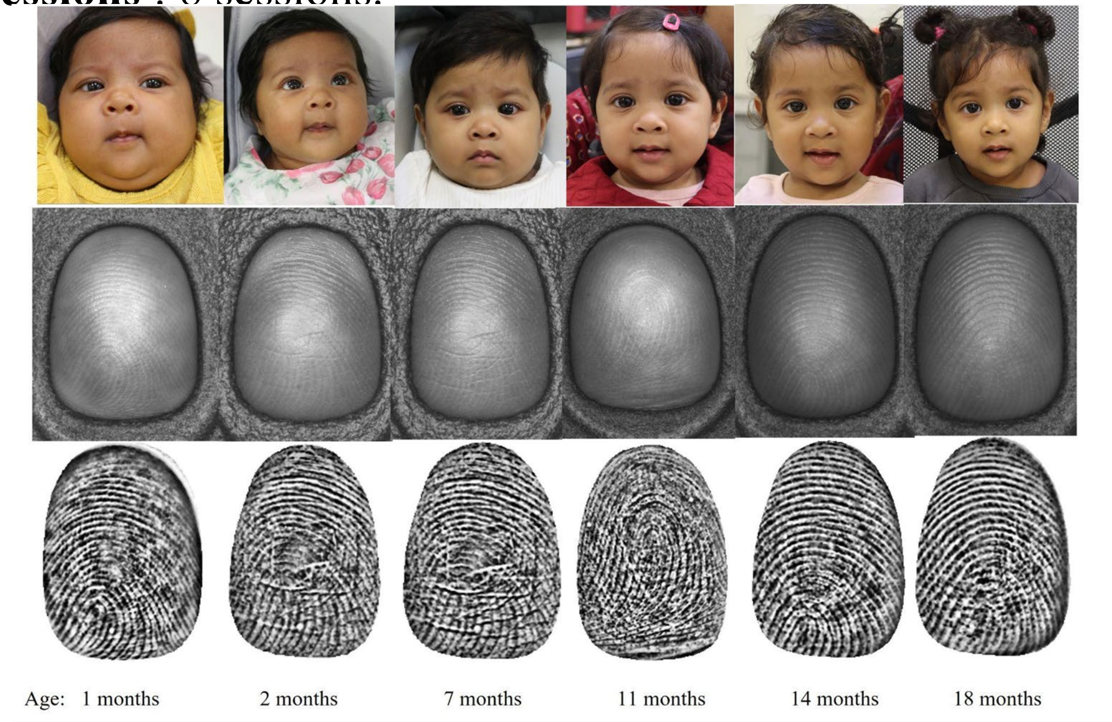
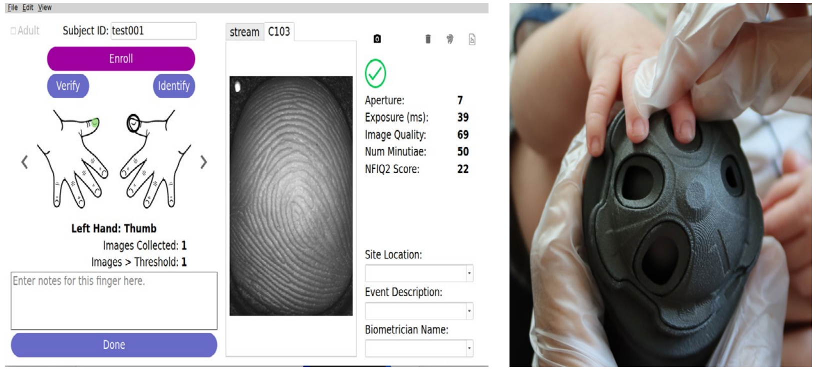


Figure : Sample data from multimodal longitudinal infant and toddler dataset



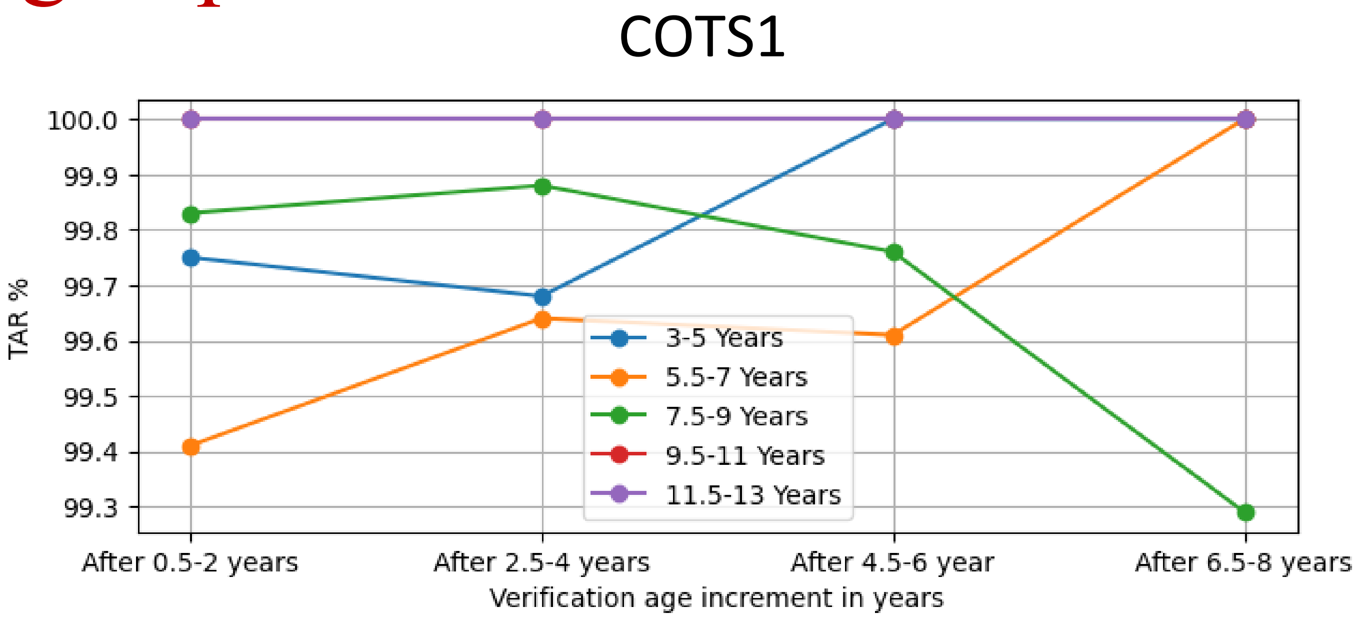
Synolo Fingerprint user interface and scanner (3000 ppi)

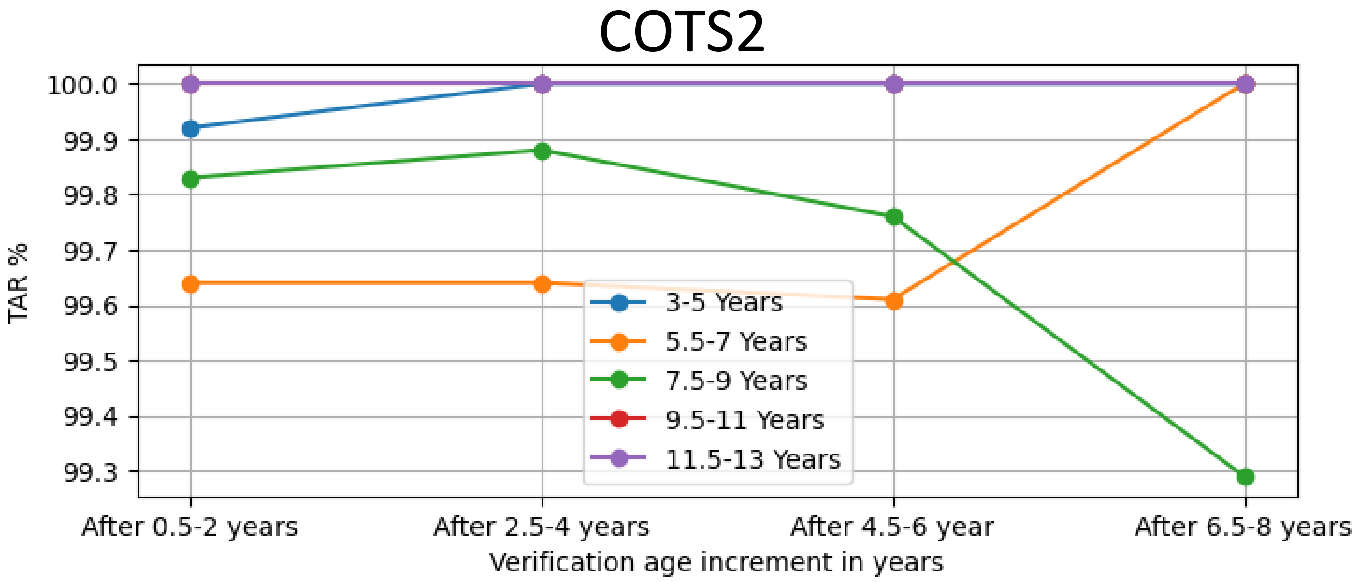
PayEye Infant Iris Scanner

Analysis for age groups

Findings:

Investigation of age-related trends in face recognition performance. Analyzing the impact of enrollment age on True Acceptance Rate (TAR) at 0.1% FAR over time.





Result unpublished

Center for Identification Technology Research

Iris Recognition in Children

Findings:

- Recognition remains stable over time with minimal aging effects.
- False rejections mainly stem from poor-quality captures, not biometric change.
- Capture challenging in small children

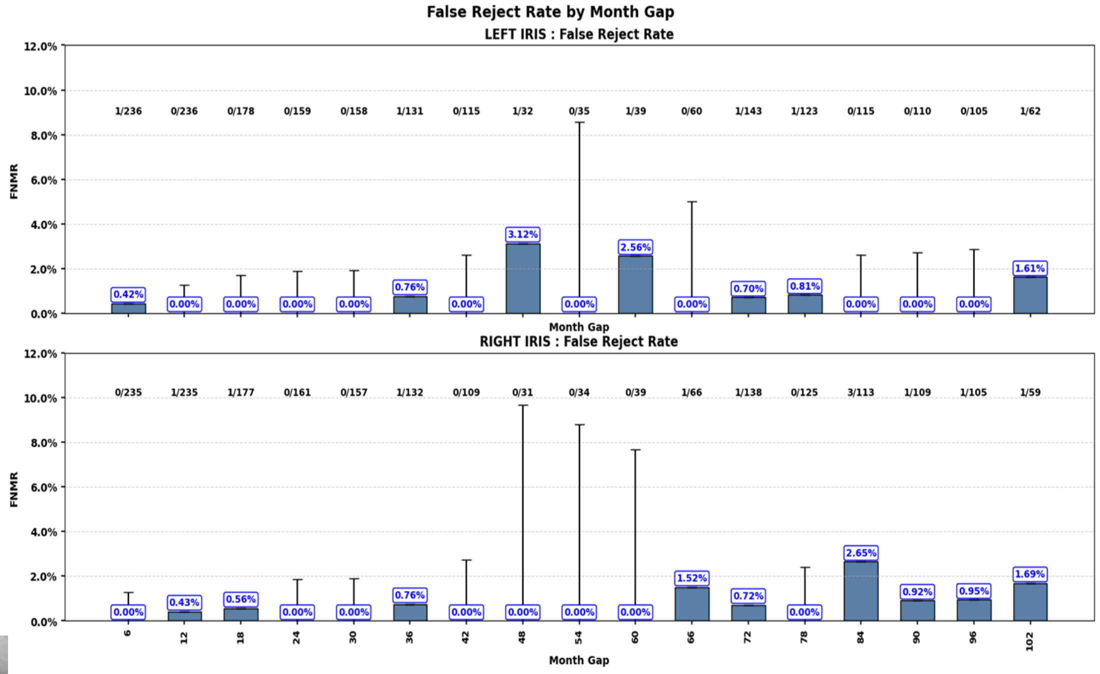
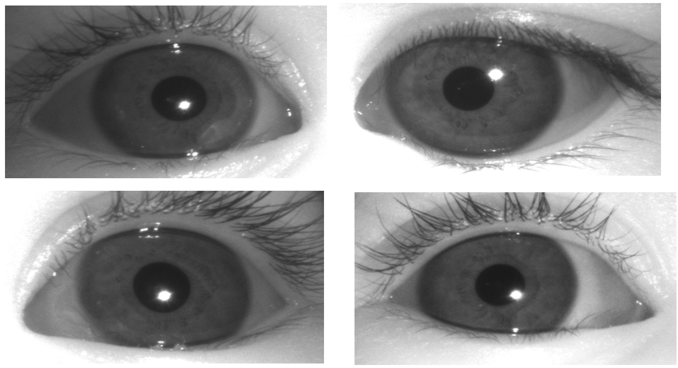


Figure 1: FNMR values for the left (top) and right (bottom) irides across 6-month intervals. Each bar represents the subject-level false non-match rate at a given interval, computed as the proportion of participants with at least one false rejection.

Custom iris scanner for young children



Sample images of 9-month-old infant captured with custom iris scanner.

Das, P, et al 2023. Longitudinal performance of iris recognition in children: Time intervals up to six years.

N. Venkataswamy, et al, Recent results unpublished

Khondkar, M.J.A., Sarker, M.A.B., Imtiaz, M.H. and Schuckers, S., 2024, July. Development of a NIR-based Infant Iris Scanner

Fingerprint Recognition in Children

Limitations of Existing Fingerprint Recognition Systems for Children

- Designed for adults and ineffective for children.
- Lack adaptive models for the rapid growth of children’s fingerprints.
- Standard sensor resolution (500 ppi) is insufficient for young children.

Figure 1: Fingerprint (500ppi) captures at different ages, from infancy to childhood and adulthood.

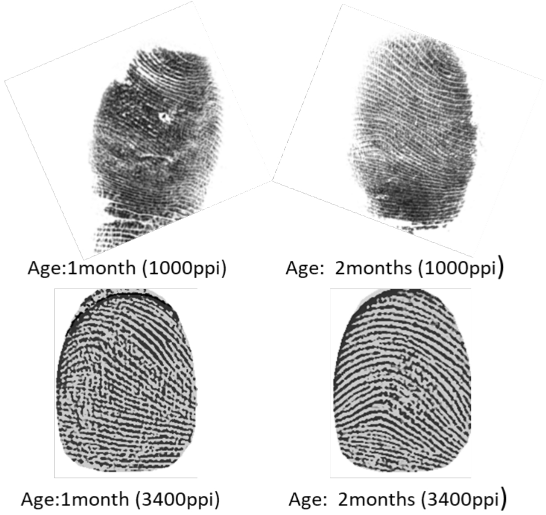
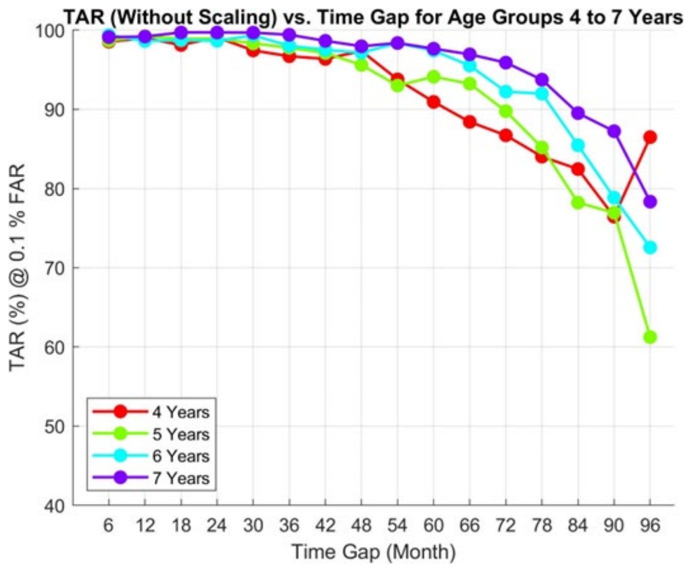


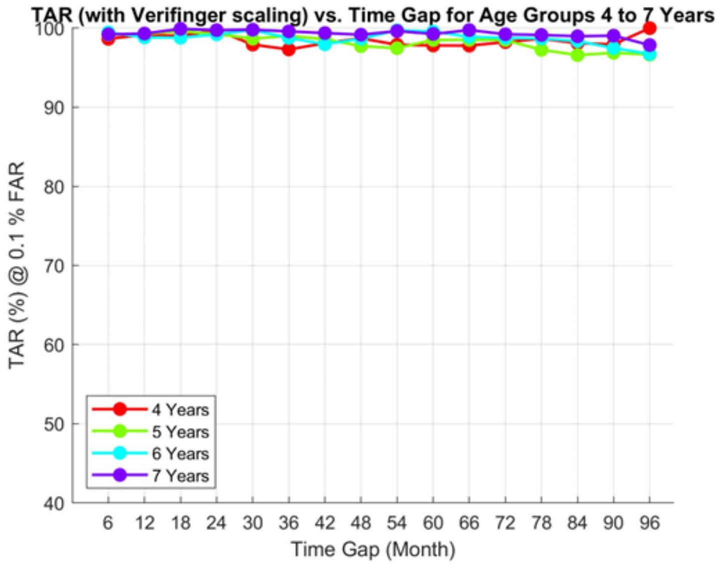
Figure 2: Fingerprint of same subject captured at different ages using low and high resolution.

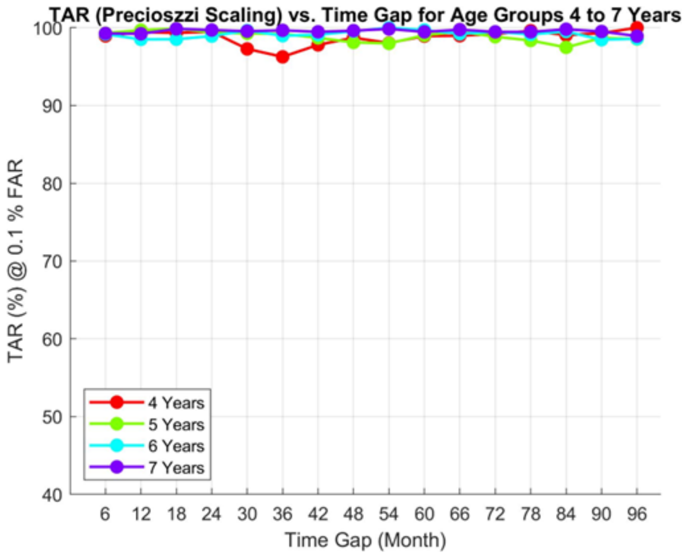
Preciozzi, J., et al., 2020. Fingerprint Biometrics from Newborn to Adult: A Study from a National Identity Database System

Fingerprint Recognition in Children

Verification Performance for Age Group 4 to 7 Years







Findings:

- Without scaling, 4 yr old recognizable up to 48–60 months (TAR: 97.4–90.9%).
- With scaling, 4 yr old recognizable up to 90 months (TAR 99.3%).

Rumana Sumi, Stephanie Schuckers, CITeR Report 2025, unpublished.

Fingerprint

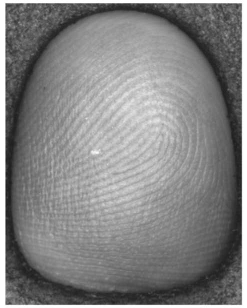
Verification Performance for Children - Ages 5 Days to 2 Years

TABLE IV
VERIFICATION PERFORMANCE OF YOUNG CHILDREN

Sub ID	Enrollment Age	Sub	TAR @ 0.1% FAR (1000ppi)	TAR @ 0.1% FAR (3000ppi)	Time Gap
01-19	0-2yrs.	16	62.26 %	100%	0
10	2 years.	1	50%	100%	1 month
13	2 months	1	50%	100%	2 months
11	1 month	1	50%	100%	2 months
15	1 month	1	n/a	100%	1 month
05	1 month	1	n/a	100%	18 days
06	15days	1	0%	n/a	15 days
09	5 days	1	0%	100%	2 months

Note: Here n/a due to the unavailability of the data for that specific scanner.

Synolo® Neo Fingerprint Scanner (3000 ppi)



Raw

Processed

Findings:

High resolution 3000 ppi scanner significantly outperformed 1000 ppi scanner for children under age 2.

5 days (3000ppi)

1month (3000ppi)

2 months (3000ppi)

4 months (3000ppi)

Sumi, M.R.A., Imtiaz, M.H. and Schuckers, S., 2024, July. A Longitudinal Study on Fingerprint Recognition in Infants, Toddlers, and Children.

Dedicated Device for Children

(Ergonomic and enhance image quality)

High Image Resolution

(Features are small)

Use Platen-Free Imaging

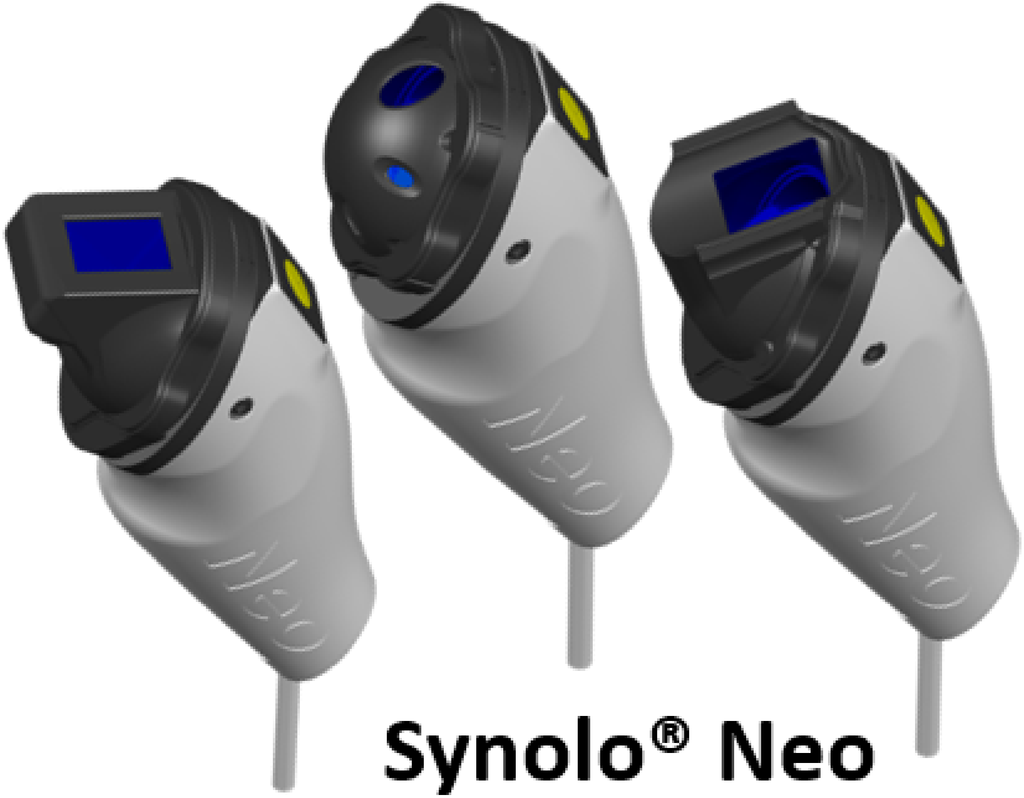
(Reduces fingerprint distortions)

Optimize Image Processing

(Correct for Size/Aging Effects)

Collection Protocols

(Optimized for children)



Synolo® Neo

Swappable Tops for Fast Optimization
for All Ages and Modalities

CITeR Center for Identification Technology Research

Comparative Overview of Child Biometric Modalities

Modality	Longitudinal stability	Scaling / Age-handling	Collectability	Youngest Age of Success / Notes
Fingerprint	**With scaling:** **0–3y old: Moderate** **4–8y : High** **8y+ : High** Quality-dependent.	Scale to adult fingerprint size; periodic template refresh.	**0–3y old: Difficult** (portable, faster scanners required) **4–5y : Moderate** **6y+ : Easy**	Usable from day 4; with scaling and a ≥3000 ppi scanner.
Face	**0-3y: Low** **4y+: Moderate** affected by growth, pose, expression.	Age-invariant embeddings; frequent template updates.	**0-3y: Moderate / Difficult** (Semi Professional/ Professional DSLR camera helpful) **3y+: Easy**	Usable from 3y+; possible below 3y, but lower accuracy and short-term stability.
Iris (NIR)	**4y+: High**, below 4y remain unexplored; sensitive to dilation/occlusion	No adjustment required.	**0-5y: Difficult** **6y+: Easy**	Useable from 4y with cooperation; Infant recognition possible, but capture difficult
Voice	**0-11y: Low**, rapid drift (pitch/formants), noise sensitive	frequent re-enrollment or adaptive models	**0-4y: Difficult** **5yr+: Easy**	Usable from 4y but low accuracy; limited long-term stability.

Lesson

Child biometric recognition is possible, but care needs to be taken to understand the implications of capture and age progression

Good practice for biometrics

Biometric vulnerabilities

Top 10 Vulnerability Questions

A guiding document that provides clarification around some of the frequently asked questions about the spoofing of biometrics.

Biometrics Vulnerability Assessment Checklist

A checklist which complements the Top 10 Vulnerability Questions, prepared to help guide members in addressing vulnerability assessments in biometrics.

Presentation attack detection (PAD) and liveness guiding document

This document explaining what PAD and liveness is and suggests some general considerations and questions users may want to ask when choosing a biometric product.

www.biometricsinstitute.org

Conclusions

- Presentation Attack Detection (PAD)
  - Attacks at the biometric sensor – Physical attacks
  - Biometrics + Liveness/PAD = Success!
- Injection Attack Detection (IAD)
  - Attacks which “bypass” the biometric sensor – Digital attacks
  - IAD can use similar approaches to PAD, but with a different purpose
  - Biometrics + Liveness/PAD/IAD = Success!
- FIDO Biometric Certification
  - Incorporates both live subject testing + PAD testing + fairness evaluation
  - Value Proposition
    - Requirements developed by biometrics experts
    - Independent, international network of laboratories
    - Based on ISO standards
  - Future work – IAD evaluation

Special Thanks to CITeR Current Affiliates—2026

- ACV Auctions
- Athena Sciences
- Aware
- DRDC—Defence Research and Development Canada (DRDC)
- DoD—Defense Forensics and Biometrics Agency (DFBA)
- DoD — U.S. Army Criminal Investigation Laboratory (USACIL)
- DHS—Office of Biometric Identity Management (OBIM)
- DHS—Science & Technology (S&T)
- FBI Criminal Justice Information Services (CJIS)
- FBI Operational Technology Division (OTD)
- Home Team Science and Technology Agency (HTX) – Singapore
- Idemia
- Integrated Biometrics
- Israel National Cyber Directorate (INCD)
- Metalenz
- National Security Agency (NSA)
- Neurotechnology
- Oak Ridge National Labs (ORNL)
- Private Identity
- Public Safety Canada
- Qualcomm
- Synolo
- Thales