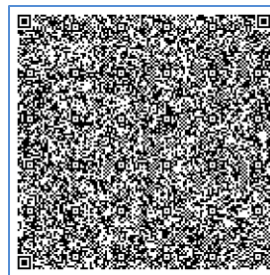
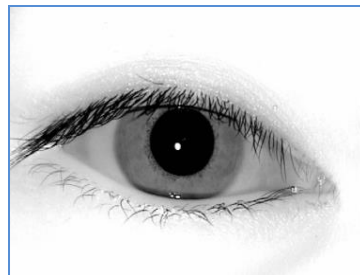
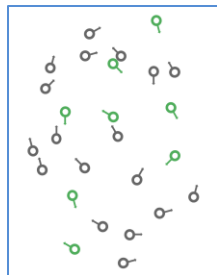


BIOMETRICS FOR DIGITAL IDENTITY

PATRICK GROTHER
U. S. DEPARTMENT OF COMMERCE

ID4AFRICA 2025-05-22



NIST ORGANIZATION

U. S. Department of
Commerce

NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology
Laboratory

Computer Security
Division

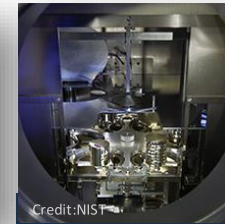
Information Access
Division

Biometrics Group

ENSURING IDENTITY FOR TRUST
IN COMMERCE AND JUSTICE



Material
Measurement
Laboratory



Physical
Measurement
Laboratory



Engineering
Laboratory



Information
Technology
Laboratory

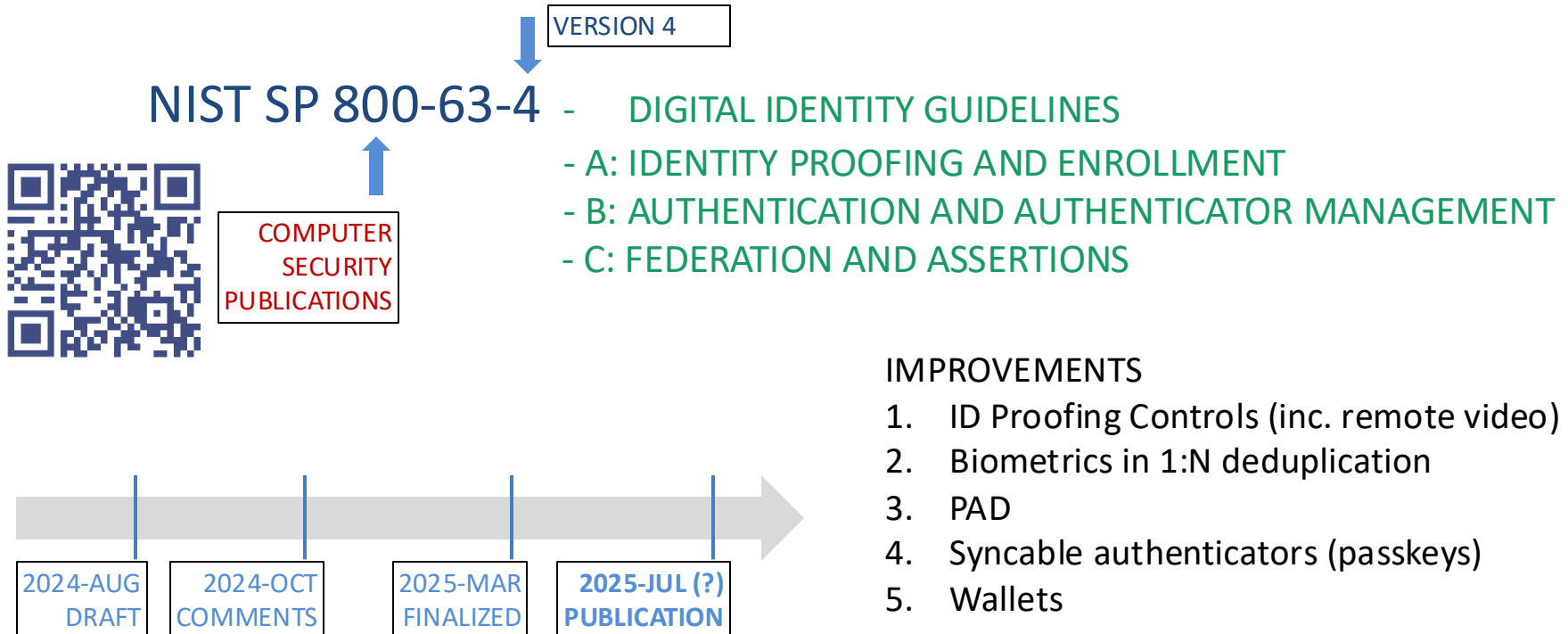


Communication
Technology
Laboratory



NIST Center
for Neutron
Research

NIST Special Publication 800-63



COMPACT BIOMETRIC IMAGES :: HOW SMALL?

FACE



COLLECT: 6MP+
STORE DBASE: 300KB+
STORE PASSPORT: 20KB
ISO/IEC 39794-5:2019

FINGER



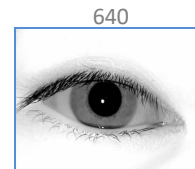
512

COLLECT: 197 pix cm⁻¹
STORE DBASE: 12KB+
STORE PASSPORT: 7KB
ISO/IEC 39794-4:2019

368

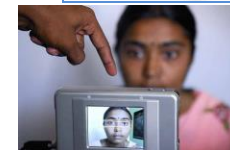
IRIS

COLLECT: 640 x 480 each eye
STORE DBASE: 150KB
STORE PASSPORT: 20KB
ISO/IEC 39794-6:2021



640

480

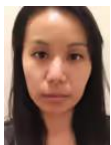


10KB

10KB

4KB

NON-INTEROPERABLE
TEMPLATES

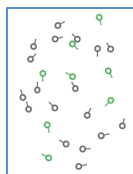


STORE QR: 1KB
ISO/IEC -----:2027

6KB

NON-INTEROPERABLE
TEMPLATES

0.4KB



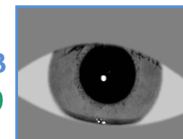
STORE INTEROPERABLE
MINUTIA TEMPLATE: 300B
ISO/IEC 39794-2:2023



NON-INTEROPERABLE
TEMPLATES

1KB

STORE COMPACT: 2KB
ISO/IEC 39794-6:2019



1KB

0.1KB

BIOMETRIC DATA :: STANDARD TEMPLATES

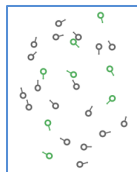
FACE



NO STANDARD
TEMPLATE

- Proposed
- Technically feasible
- Rejected by industry
 - Not needed
 - Impedes innovation

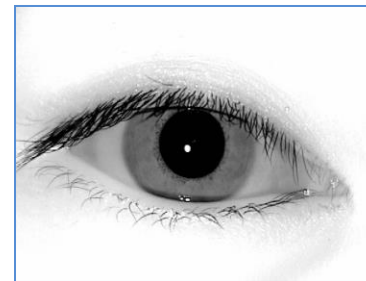
FINGER



STORE INTEROPERABLE
MINUTIA TEMPLATE: ~300B
ISO/IEC 39794-2:2023

- Extensively tested accuracy and cross-developer interoperability
-  **MINEX**

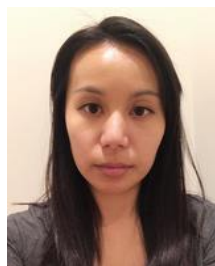
IRIS



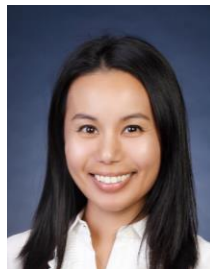
NO STANDARD
TEMPLATE

- Technically feasible using Daugman Iris Code
- Rejected by industry

TEMPLATE → IMAGE ?



TEMPLATE
aka EMBEDDING
aka FEATURE VECTORS



- INVERSION? YES!
 - WITH ACCESS TO PAIRS OF IMAGES AND TEMPLATES
 - WITH ML EXPERTISE
- BUT < 20% INVERSIONS FAIL



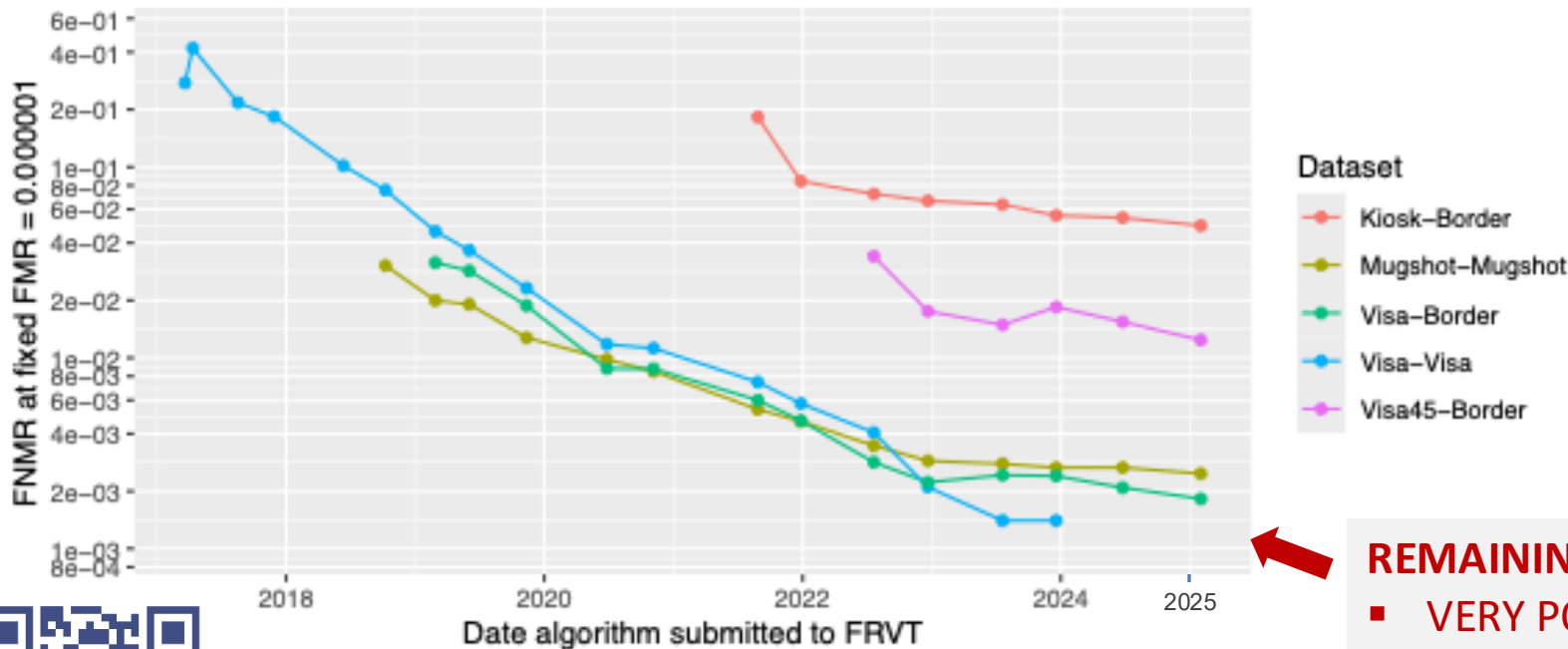
H. Otroshi Shahreza and S. Marcel, *Template Inversion Attack Using Synthetic Face Images Against Real Face Recognition Systems*, in IEEE T-BIOM, July 2024

M. Akasaka, S. Maeda, Y. Sato, M. Nishigaki and T. Ohki, *Model-Free Template Reconstruction Attack with Feature Converter*, BIOSIG 2022



FACE RECOGNITION ACCURACY

roc: Evolution of accuracy on five datasets 2017 – present



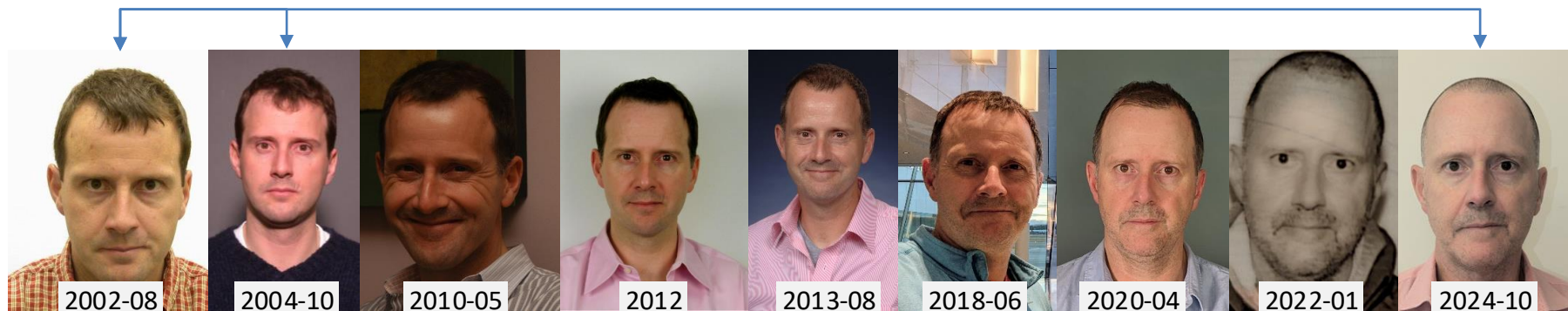
REMAINING ERRORS

- VERY POOL QUALITY
- LONG TERM AGEING
- CHILDREN



Source: NIST FRTE

BIOMETRIC DATA :: PERMANENCE



FACE

- Rapid ageing children, teens
- Steady ageing in adulthood
- Scars, tattoos, surgery, beards, occlusions

FINGER

- From 6 months
- High stability but
- Acute injury
- Scars

IRIS

- From 6 months
- High stability
- Patterned contact lenses

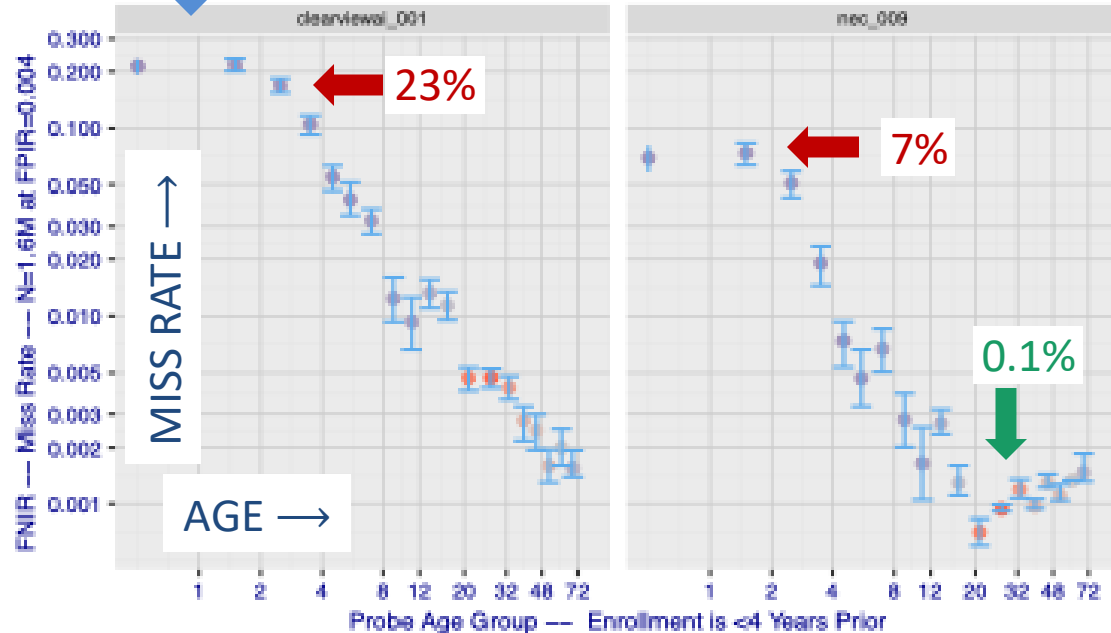
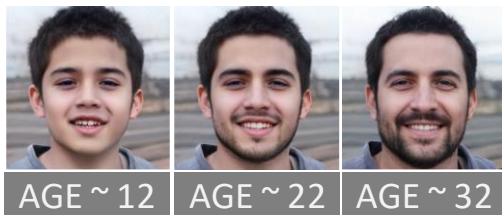
CHILDREN :: FACE RECOGNITION



IN BABIES, SEARCHES FAILURE TIME LAPSE < 120 DAYS

FR Problems:

- Growth
- Eyes closed
- Non-frontal view
- Occlusion



CHILDREN: FINGERPRINT RECOGNITION



https://www.id4africa.com/2019_event/presentations/InF15/3-Elijah-Aronoff-Spencer-USD.pdf

AGEING:

- Stable features after 6 months [JAIN]

PROBLEM:

- Small size, fine ridges, growth →
- High resolution imaging →
- Not interoperable with recognition algorithms expecting 500 ppi

- Industry runs at 500 ppi
- Children need at least 900 ppi. For example:
 - Vaccine-scheduling has driven work in
 - Simprints vero 2 / Secugen at 1700 ppi
 - Integrated biometrics: 5080 ppi interpolated

Best research

- Jain et al. (1900ppi, NEC 1270 ppi)
- Engelsma et al. (2020 open-source sensor.)



Questions to ask

- Is it being used? Where, on who
- What reports are available?
- What resolution?

Questions to ask

- Capture performance
 - Failure-to-capture rate
 - Capture duration?
- Which recognition algorithm?
 - Accuracy: FNMR vs FMR?
 - Interoperable with ?

Run tests!

- Interoperability again plain 500 ppi.

NON-CONTACT IMAGING OF FINGERPRINTS



TRADITIONAL
PLAIN IMPRESSION



PIXEL 6: PROPRIETARY
POST CAPTURE PROCESS

1. MOBILE-PHONE CAPTURED PRINTS WITH DEVELOPER-DEFINED POST-PROCESSING
 - 3D GEOMETRY
 - EXPOSURE
 - FILTERING
2. SUCH PRINTS ARE BEING TRANSMITTED IN OPERATIONAL SYSTEMS
3. INTEROPERABILITY – WANT HIGH ACCURACY RECOGNITION vs. PLAIN
 - IS NOT WELL QUANTIFIED
 - CAMERA + SOFTWARE DEPENDENT
 - GOOD DEVELOPER PROGRESS
4. ATTACK POSSIBLE
 - MORPH
 - PRESENTATION
 - INJECTION

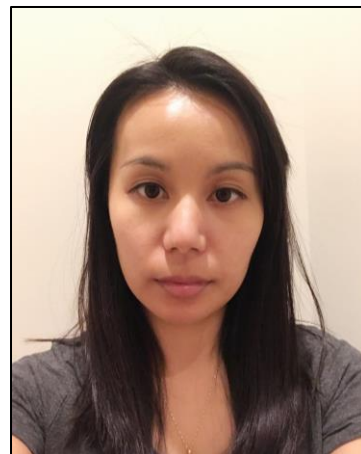
RUN TESTS:

- Interoperability against plain 500 ppi.

AFR mis-matches on twins AND siblings



Source: Notre Dame's Twins Day Collection



Source: Mei Ngan and her sister

Developer	Alg	Score	FMR	Outcome
IDEMIA	011	9397.47	< 5e-07	FALSE MATCH!
PARAVISION	013	0.6268	< 5e-07	FALSE MATCH!

Developer	Alg	Score	FMR	Outcome
IDEMIA	011	4883.2	< 5e-07	FALSE MATCH!
PARAVISION	013	0.2485	< 5e-07	FALSE MATCH!

Twins, triplets etc. are 3% of lives births in the USA in 2022, from 117,000 out of 3.7M births. <https://www.cdc.gov/nchs/data/nvsr/nvsr73/nvsr73-02.pdf>



LOWER SCORES
BUT ABOVE THRESHOLD

ID PROOFING :: DUPLICATE DETECTION



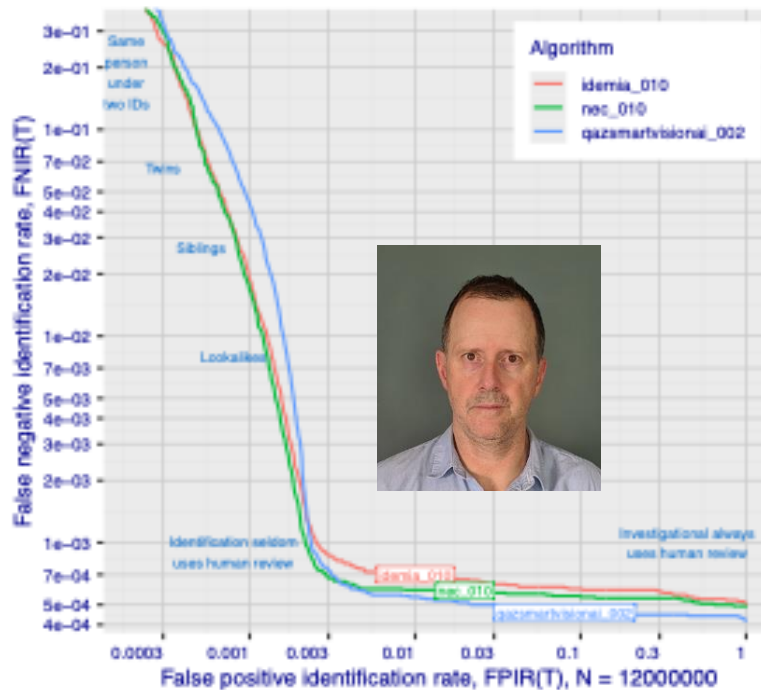
UID Enrolment Proof-of-Concept Report, 2010-12-03.
http://uidai.gov.in/images/FrontPageUpdates/uid_enrolment_poc_report.pdf



http://www.wired.com/magazine/2011/08/ff_indiaid/

FOR FACE RECOGNITION DUPLICATES DETECTION
IMPEDED BY FALSE POSITIVES

- TWINS
- FAMILY MEMBERS





FAMILIAR FACES



UNFAMILIAR FACES



Source: Frøy Løvåsdaal
Team Identity, biometrics and biometric data EUIS-programme
National Police Directorate, Norway froy.lovassdal@politiet.no

HUMAN FACE COMPARISON

- WILL BE NEEDED
- TRAINING AVAILABLE



<https://www.nidsenter.no/face>

ATTACK OVERVIEW

ANALOG



DIGITAL



LEGITIMATE PRESENTATION OR PRESENTATION ATTACK ?



TRUSTED CAMERA OR HACKED INJECTOR ?

Source: <https://www.biometricupdate.com/202406/vote-begins-on-biometric-injection-attack-standard>



BIOMETRIC USERS :: LEGITIMATE? FRAUDSTERS?

1 - x

x

LEGITIMATE, COOPERATIVE
MOTIVATED, HONEST USERS

SUBVERSIVE,
MOTIVATED,
USERS:
ATTACKERS

What is x?

- It's not zero!
 - 0.01% or 0.1% or ...?
- Depends on incentives, opportunity, risk
- Varies with time


[Africa](#)
[Americas](#)
[Asia](#)
[Australia](#)
[China](#)
[Europe](#)
[India](#)
[More](#)

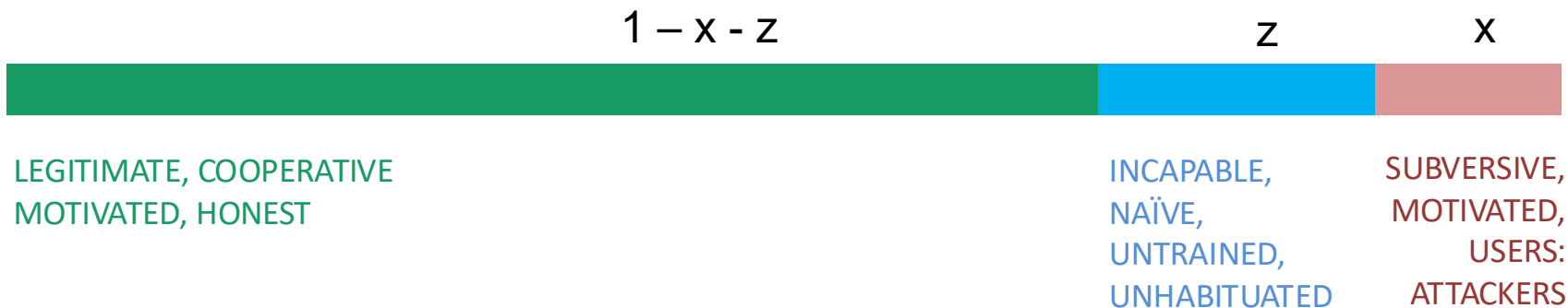
World / Asia

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

BIOMETRIC USERS :: LEGITIMATE? FRAUDSTERS?



Non-adversarial errors from naïve users.

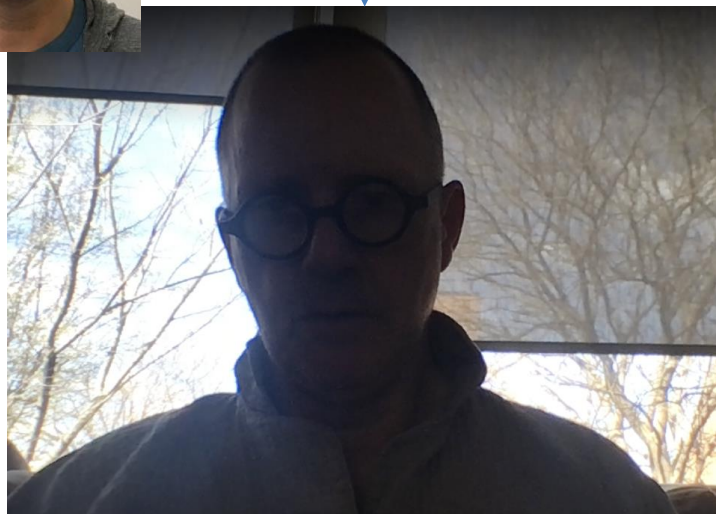
What is z ?

- Also not zero!
- Depends on age, frequency of use, device usability and affordance, training, exposure, expectations, assistance

BAD PHOTOGRAPHY: CAMERA + ENVIRONMENT



FR comparison
fails: False Negative



Underexposure



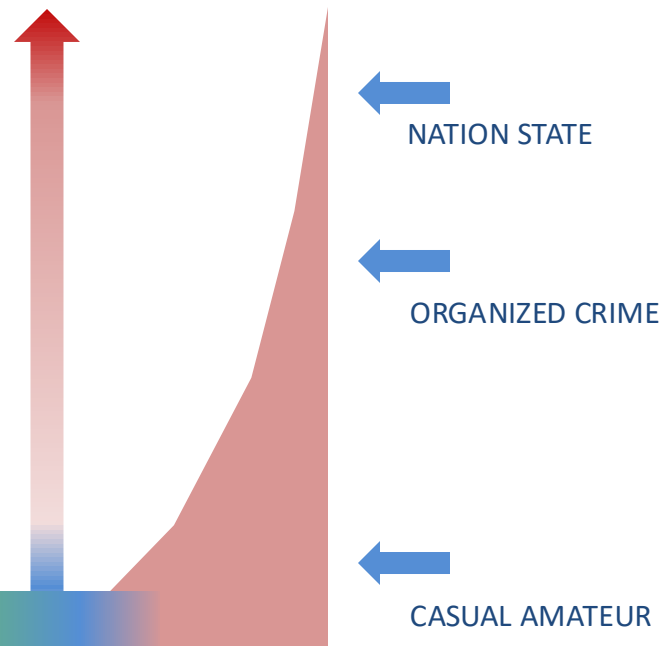
FR comparison
succeeds. True Positive



Better exposure

BIOMETRIC ATTACKERS :: ATTACK POTENTIAL

- Goals
- Resources
- Capability
- Motivation
- Effort
- Persistence
- Recourse



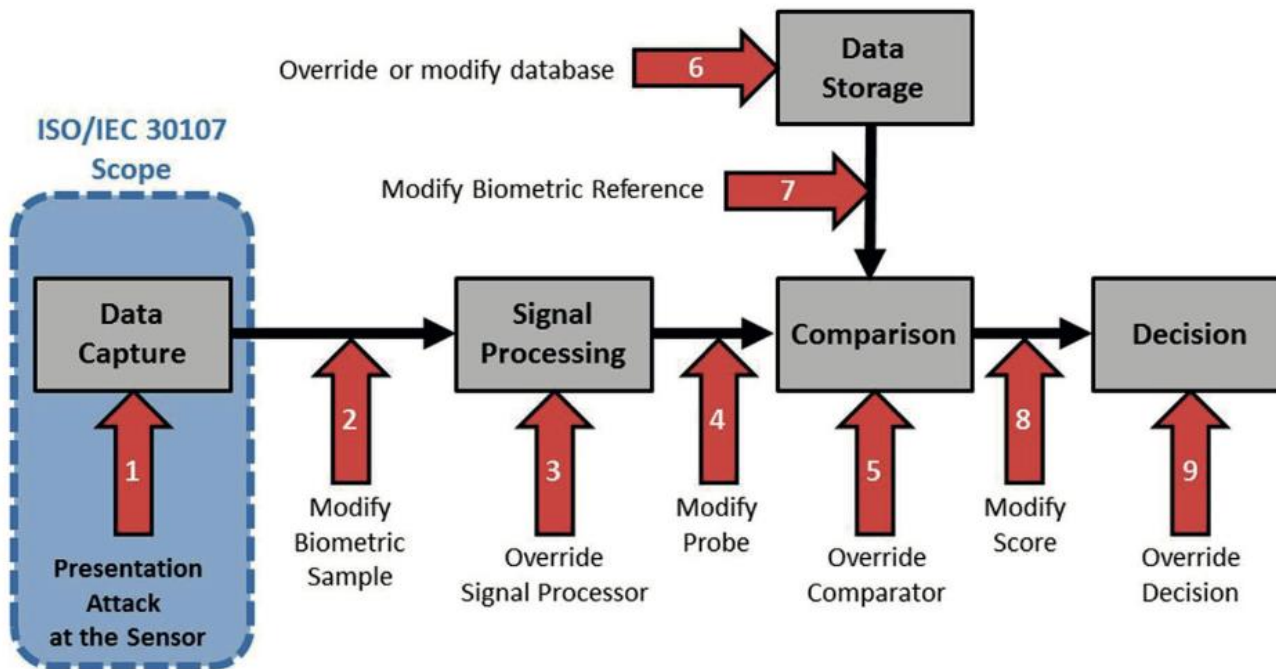
LEGITIMATE, COOPERATIVE
MOTIVATED, HONEST

$1 - x$

x

SUBVERSIVE,
MOTIVATED,
USERS:
ATTACKERS

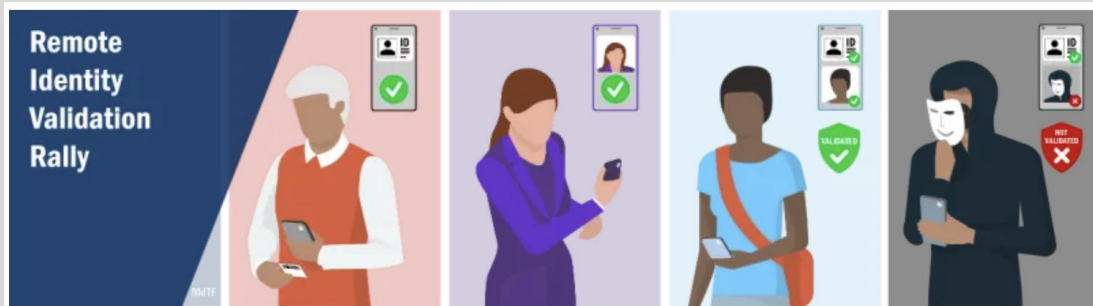
ISO/IEC 30107 – PRESENTATION ATTACK



ISO/IEC 30107-1 Biometric presentation attack detection Part 1: Framework

TWO PARALLEL-AND-TIED EVALUATIONS

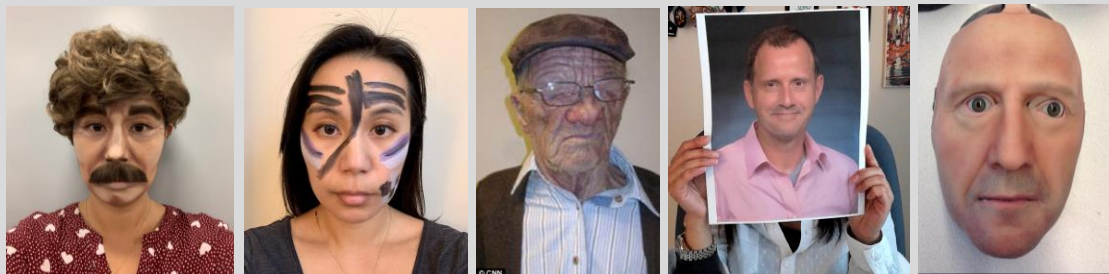
U.S. DHS S&T
RIVR 2025



1. Match-to-document; 2. Document authenticity; 3. Face liveness

JOINT EVALUATION

4. Evaluation of software passive presentation attack detectors



U.S. NIST
FATE-PAD
2025-Q4

STEALING SAMPLES TO ATTEMPT IMPERSONATION

FACE

- **Digital availability: Easy**
 - Social media
 - Weddings
 - Conferences
 - Corporate websites
- **Physical availability: Easy**
 - Take a photo in public
 - From an ID card
- Replay: Easy
- Recognition:

FINGER

- **Digital availability: Difficult**
 - Some immigration and most criminal databases
 - Some ePassports DG3
- **Physical availability: Difficult**
 - Latent mark on surface
 - Close-range high resolution photograph

IRIS

- **Digital availability: Difficult**
 - Some Immigration databases
 - Rarely ePassports DG4
- **Physical availability: Difficult**
 - Photography is optically difficult
 - Reflections, noise, resolution
 - Brown eyes need near infrared



REGISTER FOR FREE!
SEP 3, 2020
14:30-16:30 (CET)

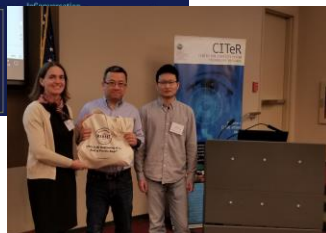
SPOTLIGHT ON FACE RECOGNITION TECHNOLOGY

Simultaneous English-French Translation Provided

KEYNOTE

Dr. Joseph ATICK (IDAFRICA)

Patrick GRÖTHER (NIST)

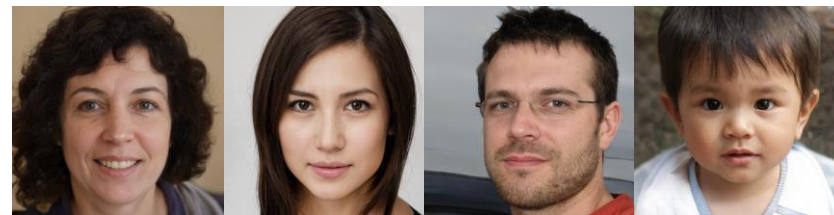
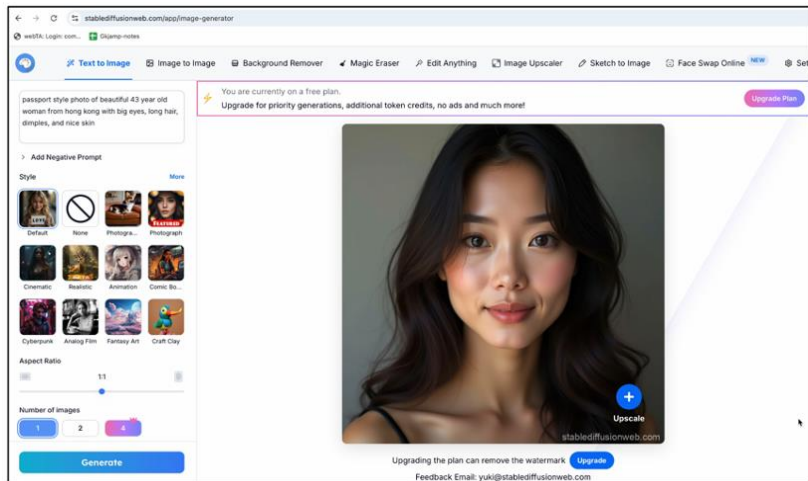


KIM ZETTER SECURITY 03.31.08 07:48 PM

HACKERS PUBLISH GERMAN MINISTER'S FINGERPRINT

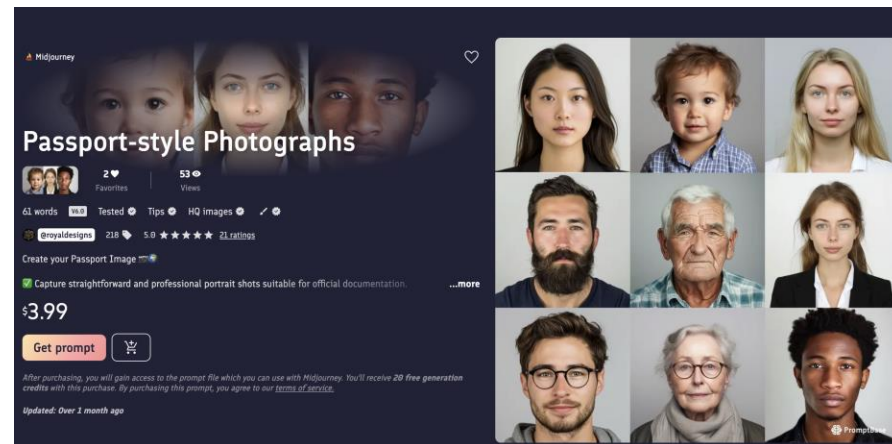


SYNTHETIC IMAGERY A.K.A. “DEEPAKES”



<https://thispersondoesnotexist.com/>

- Deepfakes → generation of fake identities
 - Many public fake generators
 - High quality



<https://promptbase.com/prompt/passportstyle-photography>

ENROLLMENT ATTACK: FAKE IDENTITY

Enrollment Risk

- Acceptance of a fully synthetic face of a non-existent person as a new identity.

Why

- Attacker makes entirely **new identities**
- Defeat **one-to-many** checks
 - “is this person already enrolled”

How

- Many tools

Scalability

- Attack scales massively
- Marginal cost is very small.

Diffusion-based intra-class variations



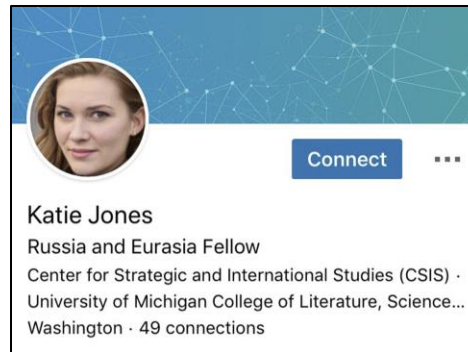
GANDiffFace: Controllable Generation of Synthetic Datasets for Face Recognition with Realistic Variations.
 Pietro Melzi, Christian Rathgeb, Ruben Tolosana, Ruben Vera-Rodriguez, Dominik Lawatsch, Florian Domin, Maxim Schaubert. <https://arxiv.org/pdf/2305.19962>

DEEPAKES: A FAKE IDENTITY RISK

Checklist for determining if an image or video is fake:

- Blurring evident in the face but not elsewhere (or vice-versa)
- Change of skin tone near the edge
- Double chins, double eyebrows, or double edges to the face
- Face is blurry when it is partially obscured by a hand
- Lower-quality sections in one video
- Box-like shapes, cropped effects near mouth, eyes, and neck
- Un-natural blinking (or lack thereof), movements
- Changes in the background and/or lighting
- Contextual clues – Background inconsistent with foreground and subject?

Source: U.S. Department of Homeland Security Report [“Increasing Threat of Deepfake Identities”](#)



Source: MIT Tech Review



Indistinct background, close crop

Other potential artifacts

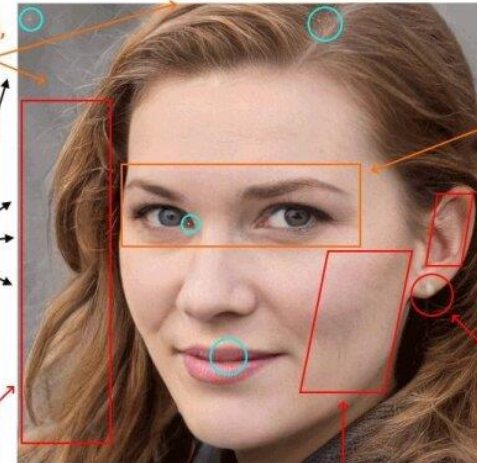
Halo effect or painterly quality around hair

Smudges/striations/drip marks on cheek

Cockeyed, heterochromatic eyes

Strange scale-like effect on upper earlobe

Earring is blurry or melted




Source: AP

ONE MITIGATION TRAINING OFFERED BY NORWAY (BORDER) POLICE

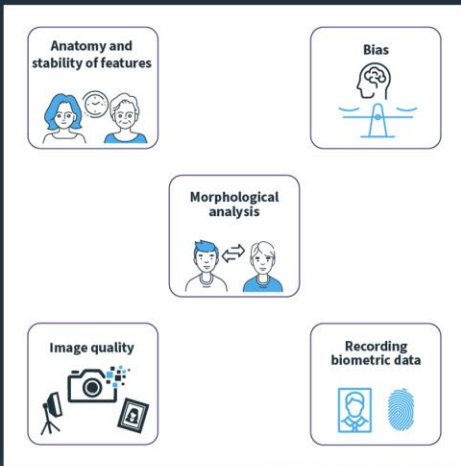
THREE ONLINE TRAINING PROGRAMS

1. Face Comparison
2. MAD
3. PAD (future)

 Norwegian ID Centre

The subjects

- Morphological analysis
- Anatomy and stability of facial features
- Bias
- Image quality
- Recording biometric data



The diagram illustrates five key subjects of training, each represented by an icon and a text box:

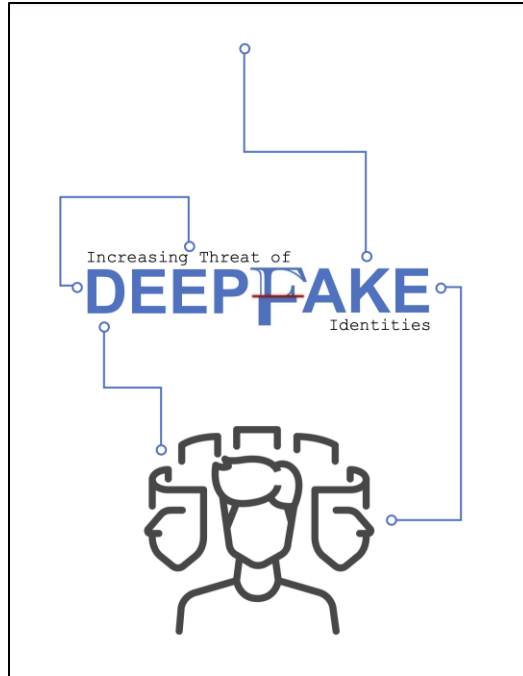
- Anatomy and stability of features:** Shows three stylized human faces with different features.
- Bias:** Shows a hand holding a scale, symbolizing balance or bias.
- Morphological analysis:** Shows two stylized human faces with a double-headed arrow between them, indicating comparison or analysis.
- Image quality:** Shows a camera, a smartphone, and a document, representing different image sources and quality.
- Recording biometric data:** Shows a stylized human face and a fingerprint, representing different biometric data types.

SLIDE FROM Knut Collett Jørgensen
National Police Directorate, Norway

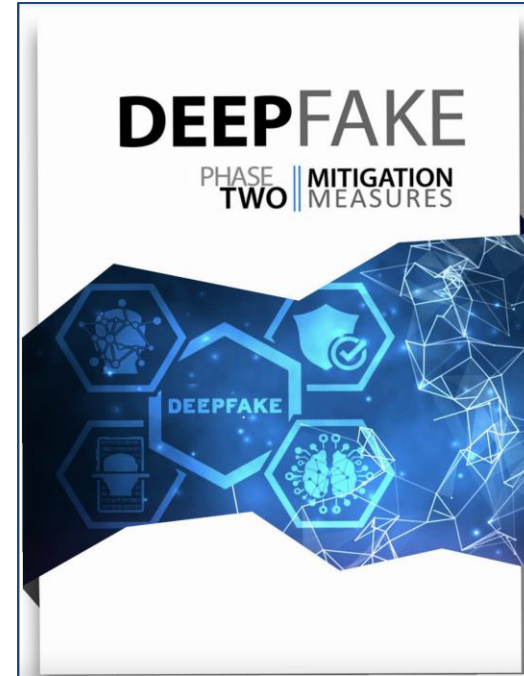


<https://www.nidsenter.no/face>

DHS DEEPFAKE THREATS AND POSSIBLE MITIGATION



U.S. Department of Homeland Security Report
[*Increasing Threat of Deepfake Identities*](#)



U.S. Department of Homeland Security Report
[*Increasing Threat of Deepfake Identities Phase Two: Mitigation Measures*](#)

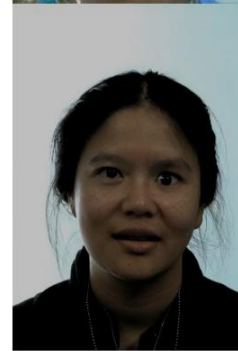


FACE SWAP VIDEO

Genuine user reference photo

High authentication scores of swapped-in face against their reference face.

Credit: DHS S&T, MITRE/HSEDI (and contributors!)



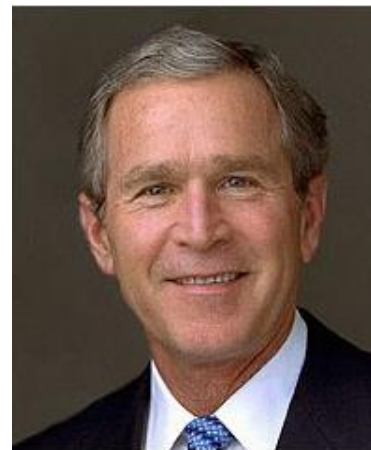
REALTIME FACE SWAP



Credit: DHS S&T, MITRE/HSEDI (and contributors!)

High matching scores of the swapped face in the video frames against the reference photos.

THE MORPHING PROBLEM



George W. Bush
(43rd US president)



Barack Obama
(44th US president)

Biometric morphing resembles both contributing subjects

CAN HUMANS DETECT MORPHS?



A

BONA FIDE



B

MORPH



C

MORPH



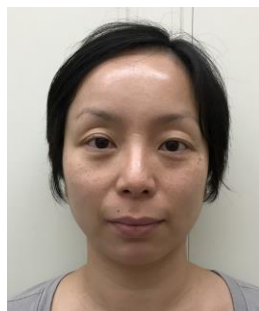
S. R. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Ramachandra and C. Busch, *Analyzing Human Observer Ability in Morphing Attack Detection—Where Do We Stand?* IEEE Transactions on Technology and Society, 2023-06

ONE DOCUMENT, TWO USERS: E. G. PASSPORT



Accomplice
(passport owner)

+



Attacker
(other identity)

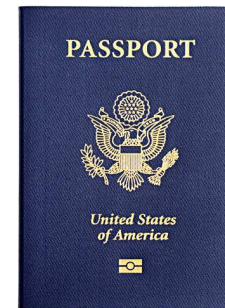


Morph = A + B

Image Source: NIST



Printed on 2in x 2in
photo paper and
mailed to passport office



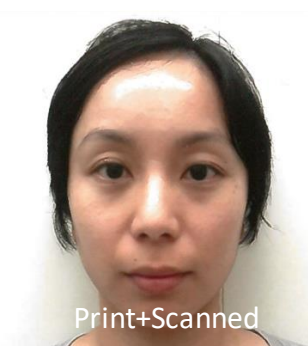
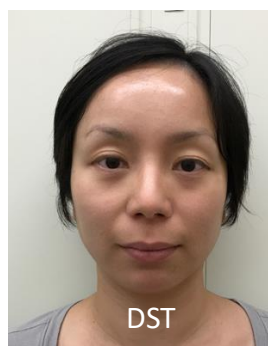
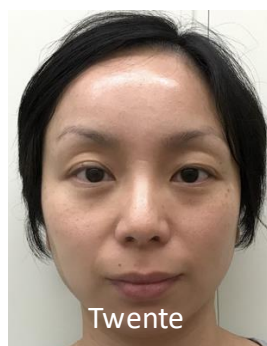
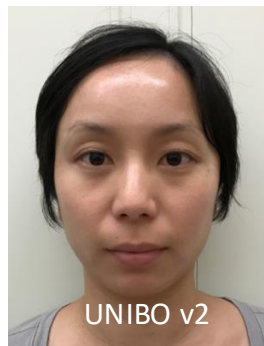
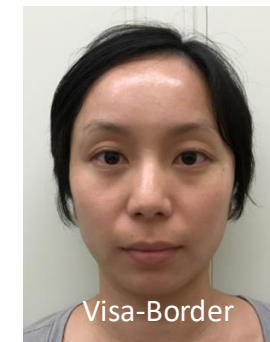
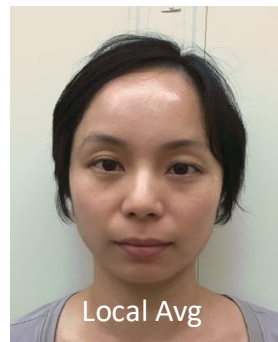
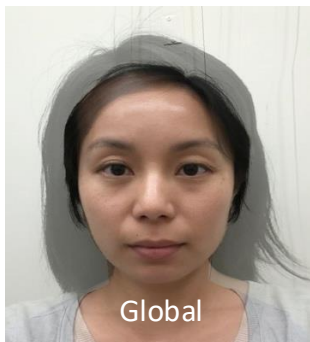
Passport office scans
printed photo, conducts
human examination, ...

Ultimately, passport gets
issued with morphed
photo on it

Matteo Ferrara, Annalisa Franco and Davide Maltoni,
The Magic Passport, 2014-09, IEEE International
Joint Conference on Biometrics



MAKING MORPHS: MANY TOOLS



- GRAPHICAL TOOLS
- NEURAL NETWORKS

- FREE
- NOT

- ONE-SHOT
- PROCESS

- FULLY AUTO
- TOUCH-UP

- DETECTABILITY



PROBLEM:
FACE RECOGNITION
MATCHES BOTH PERSONS



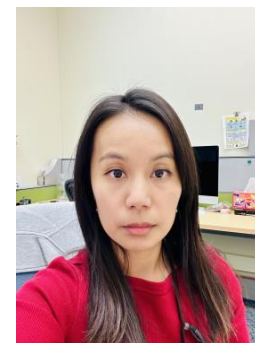
matched
against



Engine: Idemia-011
Score: 4215 → FMR below 5e-07
Outcome: MATCH!



matched
against



Engine: Idemia-011
Score: 6458 → FMR below 5e-07
Outcome: MATCH!

MORPHING: THE SOLUTION !!

TRUSTED CAPTURE!

DENY ALL OPPORTUNITIES TO INTRODUCE A MORPH

WHEN

- ISSUANCE + RENEWAL

HOW

- TRUSTED STAFF: LIVE ATTENDED CAPTURE
- TRUSTED HARDWARE:
 - TAMPER-PROOF BOOTH
 - DIRECT UPLINK TO RELYING PARTY
 - LIVENESS DETECTION

EXAMPLE: TRUSTED REMOTE PASSPORT PHOTO CAPTURE

AVOIDS MORPH ATTACKS
AVOIDS INJECTION ATTACKS
BUT ... PRESENTATION ATTACKS ??

Photo-Me
A BRAND BY BE

Need a passport or ID photo now? We send your digital photo direct to the UK Passport Office.

Find your local booth

Get your ID photo

in 2 minutes



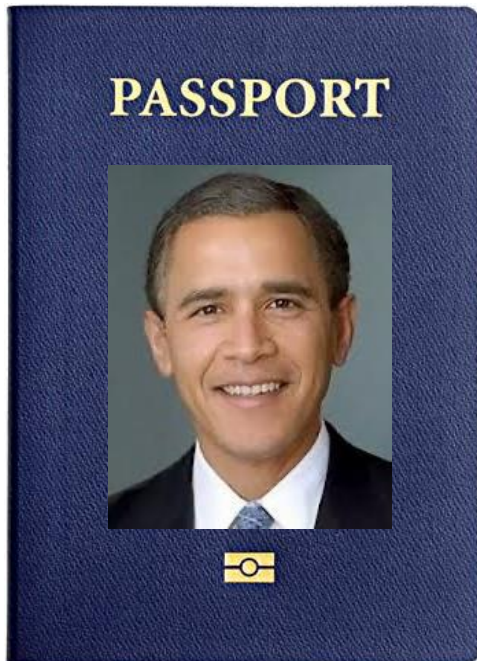
All you need is the **idpass***

*Select Digital Passport Photo inside the booth

MORPH DETECTION: TWO VERY DIFFERENT APPROACHES

- DIFFERENT PHILOSOPHY
- DIFFERENT PHASES OF OPERATION
- DIFFERENT CAPABILITY

TWO DETECTION OPPORTUNITIES



Morph of US Presidents 43+44

A: DOCUMENT ISSUANCE: Analyze suspect image in isolation

S-MAD
SINGLE IMAGE MORPH
ATTACK DETECTION



D-MAD
TWO-IMAGE DIFFERENTIAL
MORPH ATTACK DETECTION



B: BORDER CROSSING: Analyze suspect image + live image

S-MAD
HOW?
LOOK FOR
ARTIFACTS

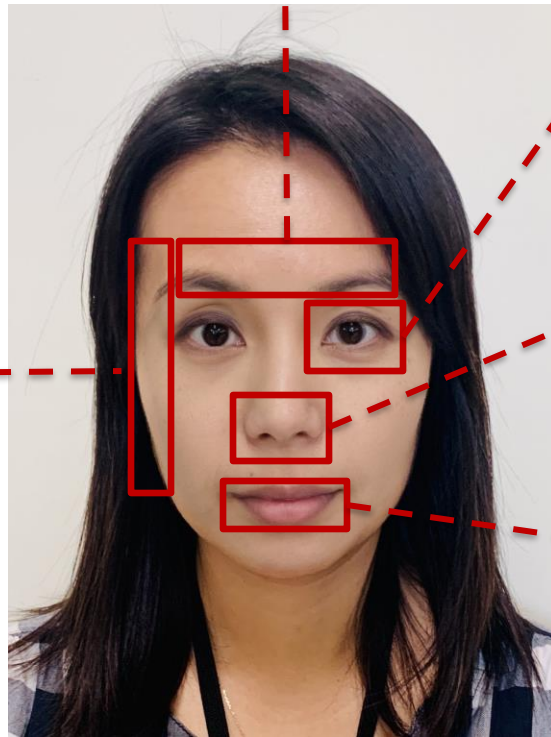
forehead color and
texture
inconsistencies



eyebrow
artifacts



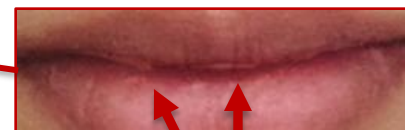
inconsistent
skin texture



iris
artifacts



nostril
artifacts



lip
artifacts

D-MAD HOW? QUANTIFY FACIAL DIFFERENCES

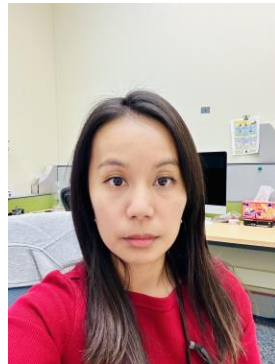


MORPH GENERATION

DIFFERENTIAL MORPH DETECTION (D-MAD)



SUSPECT MORPH
(FROM PASSPORT)



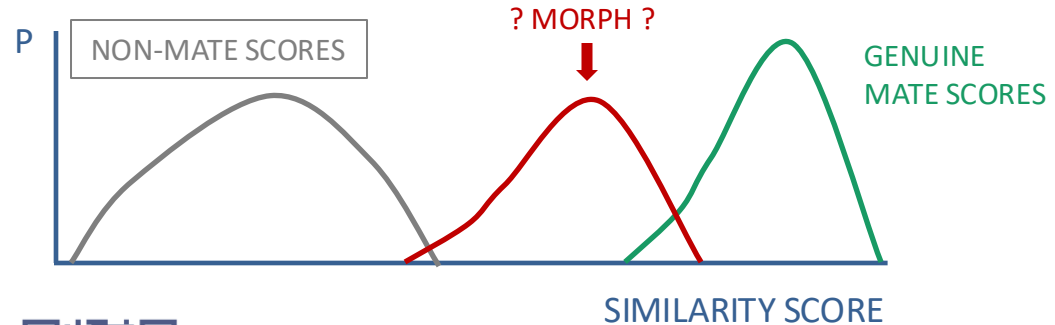
NOT A MORPH
(LIVE)

USE FR TECHNOLOGY



DIFFERENCE SCORE

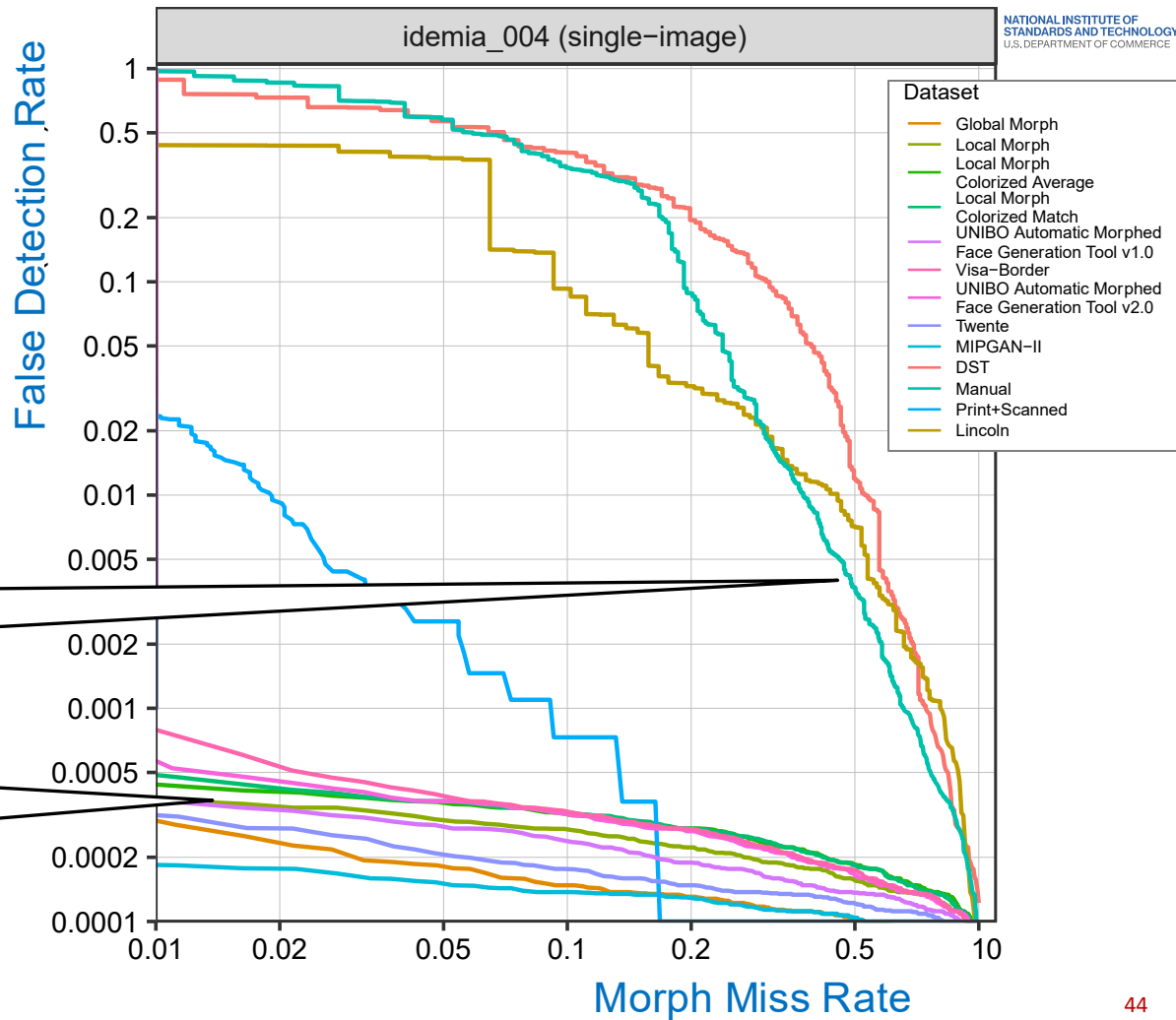
- BIG DIFF → MORPH



STATE OF THE ART IN MORPH DETECTION

- **S-MAD** - DETECTION FROM ONE SUSPECT IMAGE
- **D-MAD** - DETECTION FROM ONE SUSPECT IMAGE AND ONE LEGITIMATE NON-MORPH

S-MAD: ACCURACY



**CHALLENGE: POOR
ACCURACY ON NEVER
SEEN MORPH SPECIES**

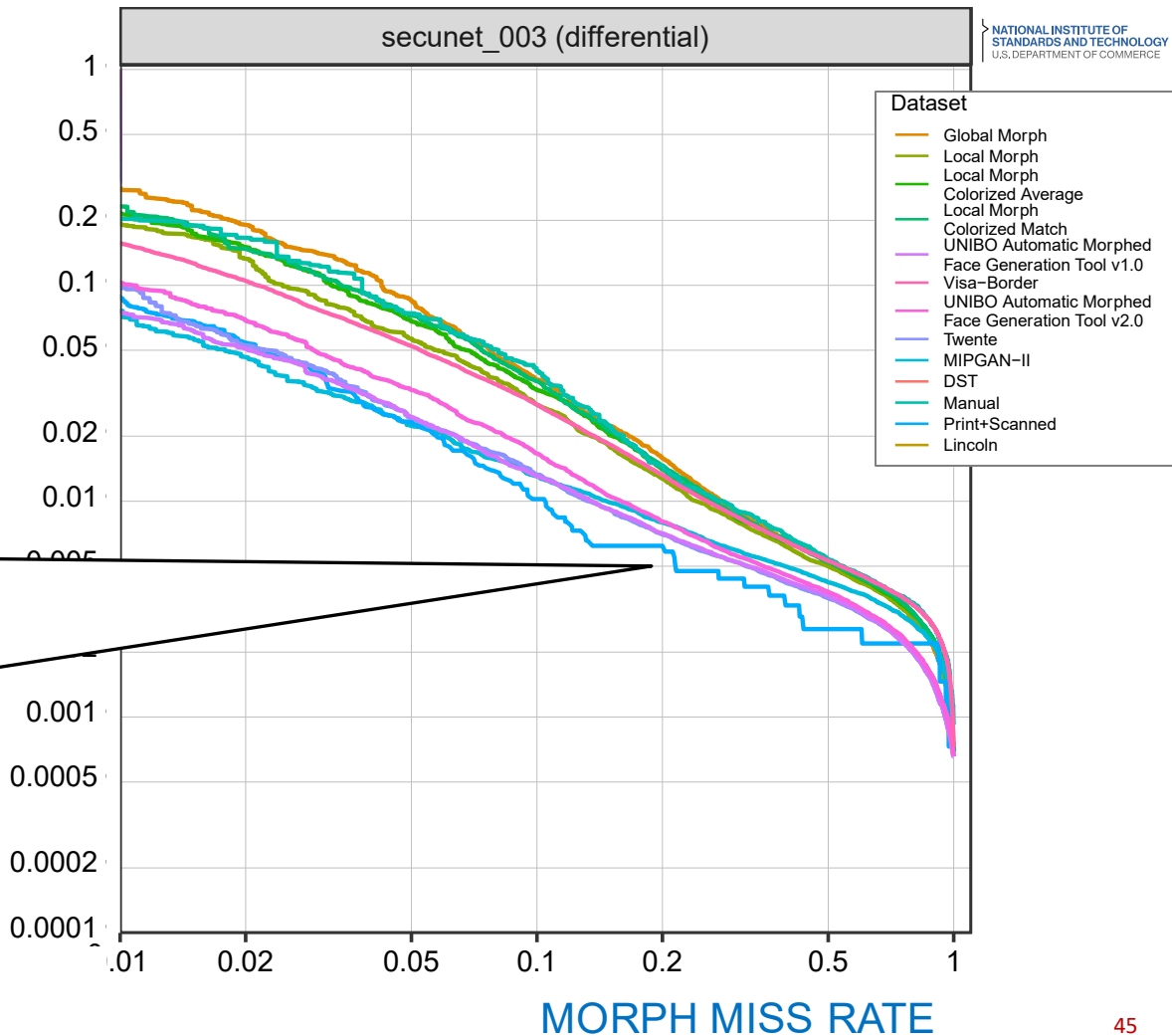
**SUCCESS: KNOWN MORPH
SPECIES DETECTED WITH
VERY LOW ERROR RATE**

D-MAD: ACCURACY

USEFUL ACCURACY:

- AT 1 in 200 FALSE ALARM RATE, 4 OF 5 MORPHS ARE FOUND
- LINES MORE CLUSTERED: GENERALIZATION

FALSE DETECTION RATE



MORPH DETECTION IN OPERATIONS



INFORMED ASSUMPTION: MORPH DETECTION IS READY TO BE PILOTED

TWO ACTIONS:

1. ENGAGE USG ENTITIES ON RUNNING PILOTS
 - DOES MAD GIVE BENEFIT?
 - HOW PREVALENT ARE MORPHS?

2. GUIDANCE DOCUMENT: AUTOMATED MORPH DETECTOR FIRES →
 - DURING DOCUMENT APPLICATION → INVESTIGATE: **HOW?**
 - DURING BORDER CONTROL → INVESTIGATE: **HOW?**

TOOLS:

- S-MAD
- D-MAD

▪ BOTH!

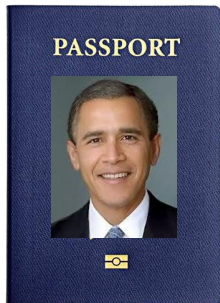
▪ 1:N SEARCH

▪ FINGERPRINTS

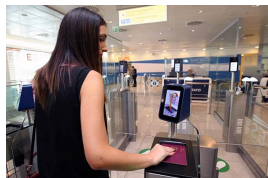
- FORENSIC INSPECTION
- CONTEXT

▪ OTHER USG

SUMMARY



Morph of US Presidents 43+44



- Incentives and opportunity to make morphs
- Two people on one passport!
- **Gold standard solution: Trusted Capture**

- Morphs vary in attack potential
- Morph detection is difficult → impossible when attacker covers tracks.

- S-MAD detectors
 - work on known morph species
 - fail on different / unseen morphing species

- D-MAD detectors quantify lack of similarity
 - work on some morphs
 - generalize
 - fail on when confederates look similar
 - give false alarms with ageing

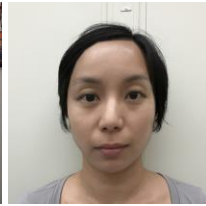
- MAD detectors need to produce low false alarm rates < 1%.

- Human capability is poor

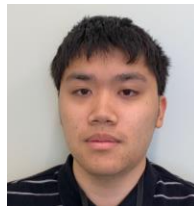
- After a morph is detected: Investigate!
 - D-MAD and S-MAD in combination
 - One-to-many
 - Upcoming NIST document “Morph Detection in Operations”



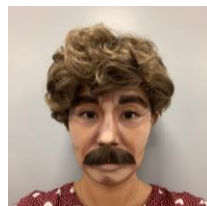
Patrick
Grother



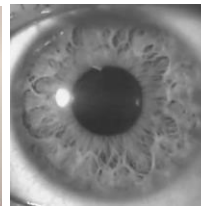
Kayee Hanaoka
(+ Mei Ngan)



Austin
Hom



(not)
Mei Ngan



Jim
Matey



Joyce
Yang

THANK YOU
PATRICK.GROTHER@NIST.GOV

