UNOFFICIAL

Australian Government
Department of Home Affairs

Operational Experiences with Biometric Attack Detection

Jason Prince
Acting Director, Digital Capability Branch, Immigration Operations
Australian Department of Home Affairs.

Operational experiences with mobile devices and remote identity verification

The Australian ETA App is used to submit Electronic Travel Authority (ETA) applications using an applicant's own mobile device.

It is supported on both iOS or Android platforms for this specific visa category.

Image Quality and Liveness Detection using the ETA app

- All imagery is recorded as stills, even if liveness uses video on device:
  – Biometrics - live capture (up to 3 frames) + chip image (if available) + biographical page including passport photograph

- ETA application liveness detection mechanism and human review of riskier applicants are part of our normal workflow, as well as dip sample quality assurance analysis of data not normally reviewed above and below thresholds

- In most cases we suspect the breach of the policy for live capture was done by travel/immigration agents assisting and profiting off facilitating electronic visas.

Key References and Definitions for “non-live” Attacks Seen

ISO/IEC 20059 Methodologies to evaluate the resistance of biometric recognition systems to morphing attacks (currently being drafted)

- Morph – merging two or more facial images to match with all donors

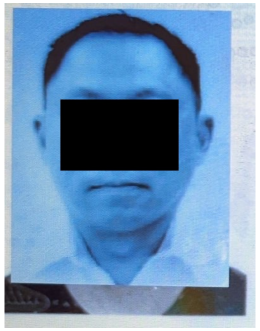
ISO/IEC 30107: Presentation Attack Detection (PAD) series of standards for testing and reporting – 30107-3 Annexure A – Classification of Attack Types

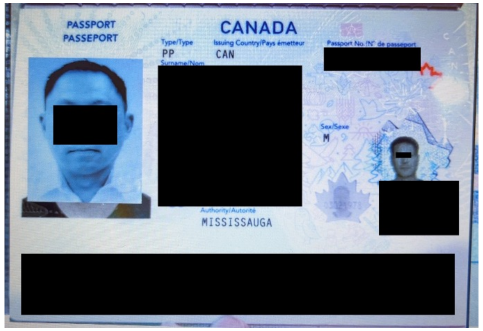
- Artificial – Printed photos, images, videos, or mask of a face
- Partial Artificial – partial prosthetics, make-up
- Lifeless / Altered / Coerced / Conformant
- Static / Dynamic

FIDO (Fast Identity Online) Alliance, Biometric Requirements / Appendix A” Triage of Presentation Attacks by Attack Potential Levels

- Level A – printed photo of face or image
- Level B – paper masks, video, high quality photo
- Level C – Silicon/Theatrical masks, 3D face information (DeepFake?)

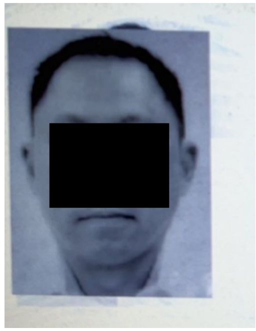
Client Non-Live, Agent Live, using chipless passport biopage image overlay substitute

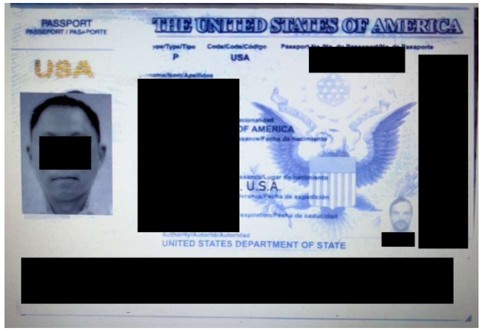

[redacted]


PASSPORT
PASSEPORT

CANADA

Type/Type: PP
Issuing Country/Pays émetteur: CAN
Passport No./N° de passeport: [redacted]
Surname/Nom: [redacted]
Sex/Sexe: M
[redacted]
Authority/Autorité: MISSISSAUGA
[redacted]

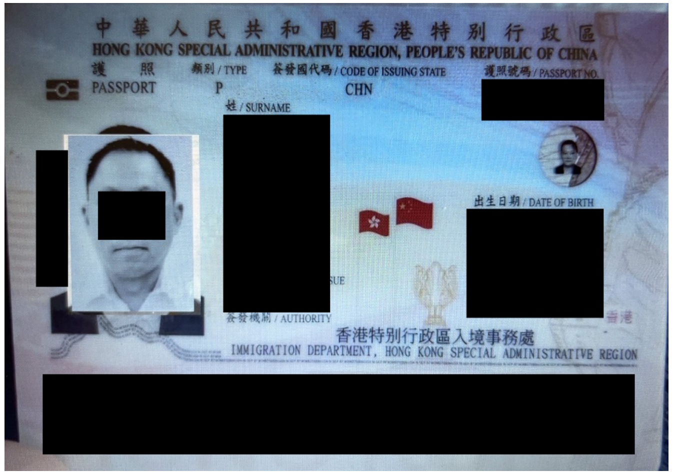

[redacted]


PASSPORT
PASSEPORT / PASAPORTE

THE UNITED STATES OF AMERICA

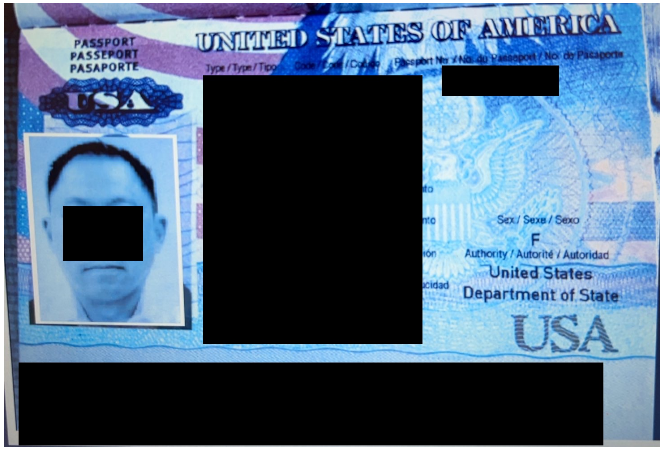
USA

ype/Type/Tipo: P
Code/Code/Código: USA
Passport No./No. du Passeport/No. de Pasaporte: [redacted]
rname/Nom/Apellidos: [redacted]
cionalidad
OF AMERICA
sance/Fecha de nacimiento
ssance/Lugar de nacimiento
. U.S.A.
livrance/Fecha de expedición
expiration/Fecha de caducidad
Authority/Autorité/Autoridad
UNITED STATES DEPARTMENT OF STATE
[redacted]


中 華 人 民 共 和 國 香 港 特 別 行 政 區
HONG KONG SPECIAL ADMINISTRATIVE REGION, PEOPLE'S REPUBLIC OF CHINA

護照
PASSPORT

類別 / TYPE: P
簽發國代碼 / CODE OF ISSUING STATE: CHN
護照號碼 / PASSPORT NO.: [redacted]
姓 / SURNAME: [redacted]
出生日期 / DATE OF BIRTH: [redacted]
SUE
簽發機關 / AUTHORITY
香港特別行政區入境事務處
IMMIGRATION DEPARTMENT, HONG KONG SPECIAL ADMINISTRATIVE REGION
香港
[redacted]


PASSPORT
PASSEPORT
PASAPORTE

UNITED STATES OF AMERICA

USA

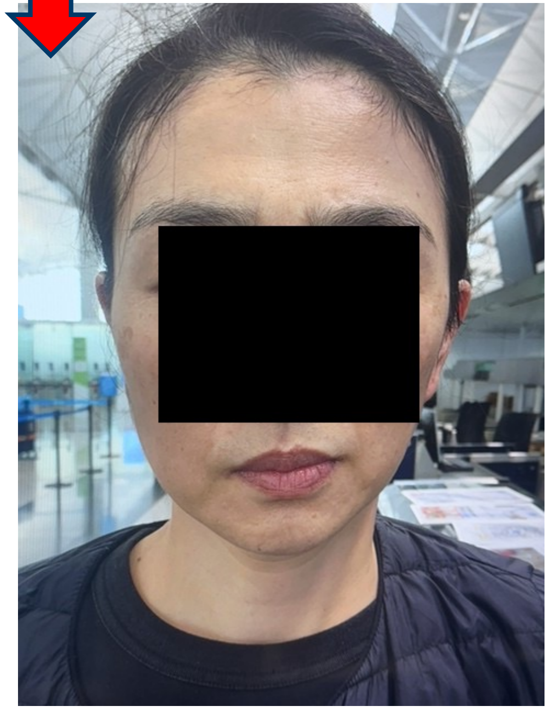
Type / Type / Tipo
Code / Code / Código
Passport No. / No. du Passeport / No. de Pasaporte: [redacted]
[redacted]
Sex / Sexe / Sexo: F
Authority / Autorité / Autoridad: United States Department of State
USA
[redacted]

Attack Artefact – Image on Monitor

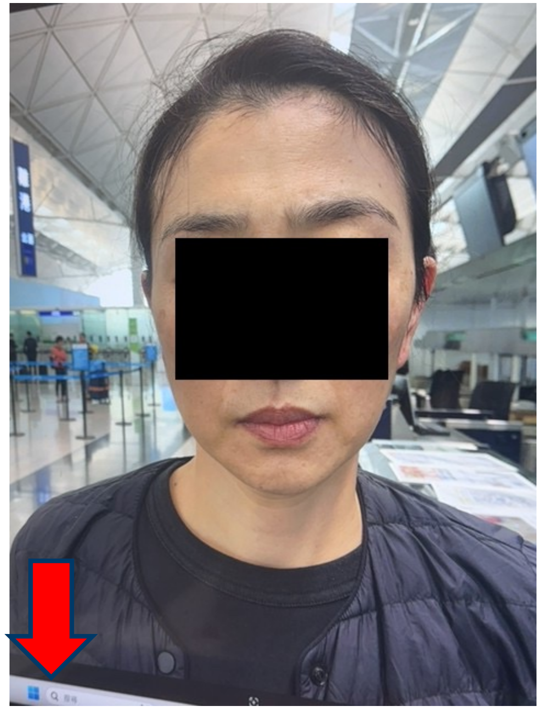
Trivial – Still image on monitor presented to Phone

Hill climbing to defeat liveness / meet image quality, by angling camera to screen

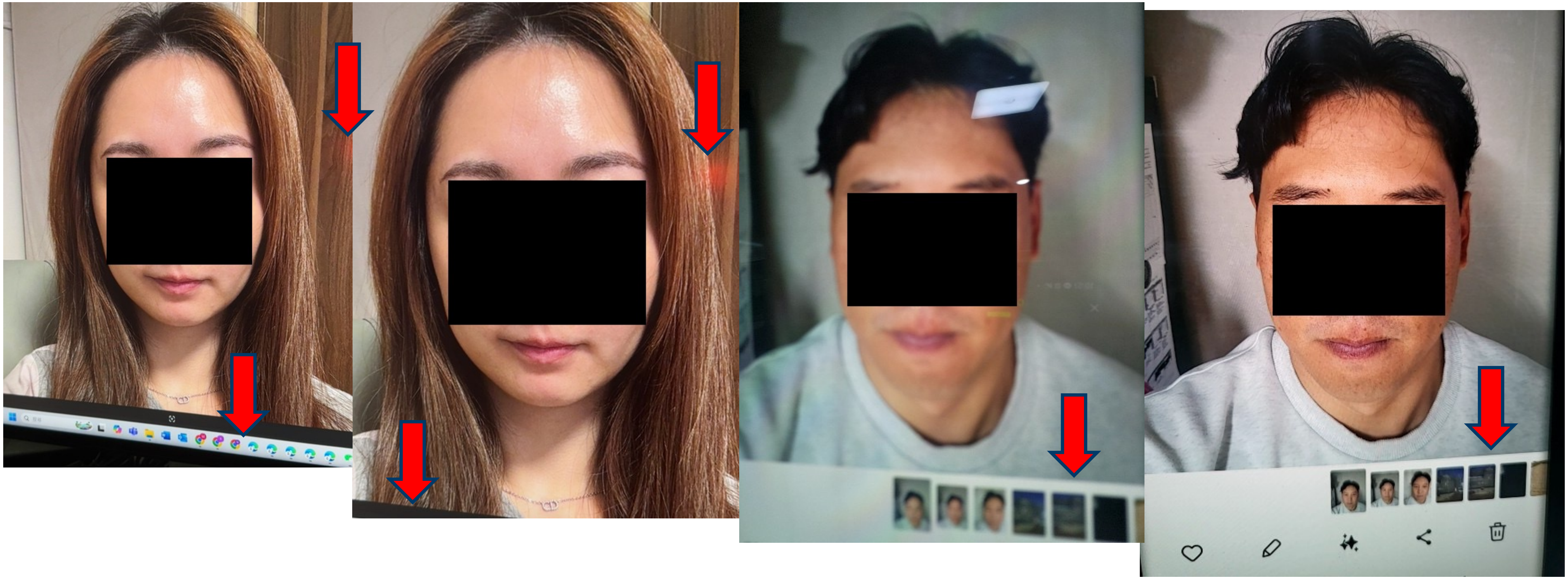
Detection – moiré (lines created from resolution issues of monitor pixels / reflections / computer icons


[redacted]

[redacted]

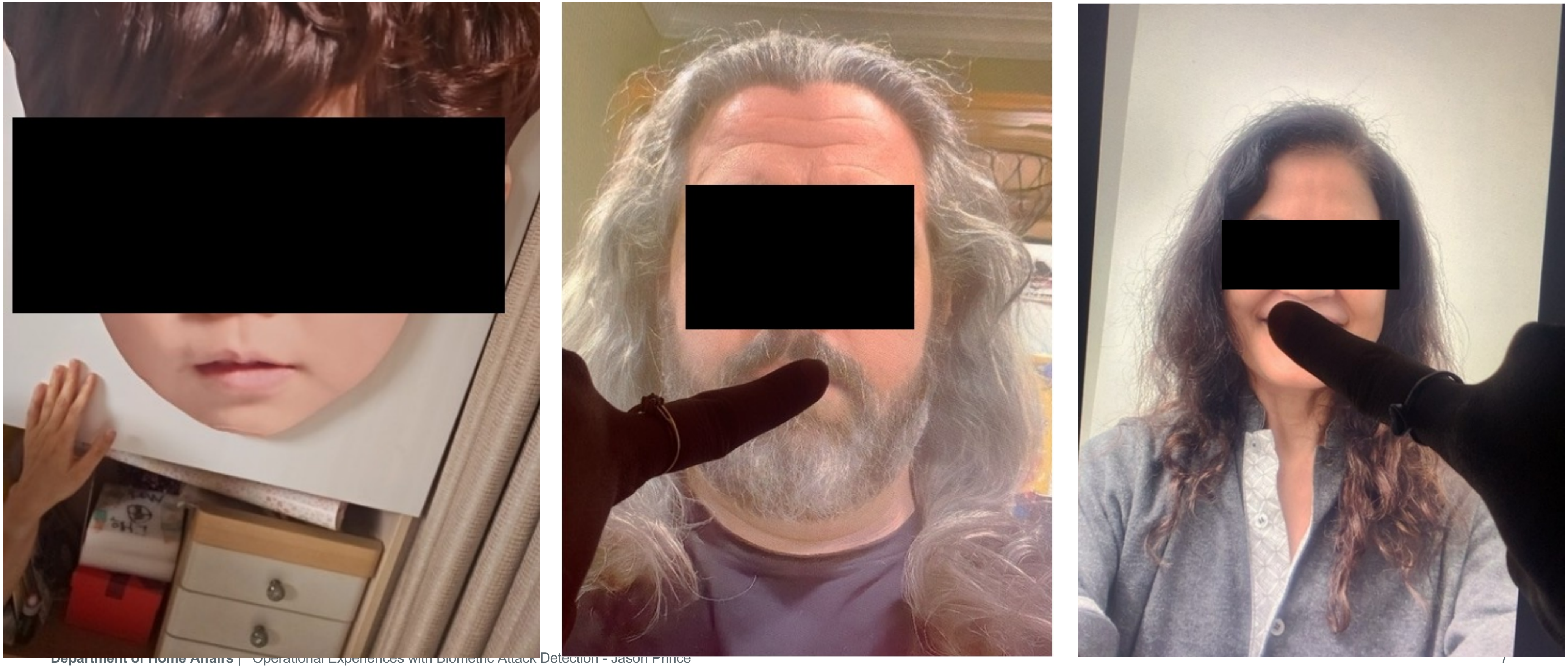

[redacted]

Attack Artefact – Image on Monitor

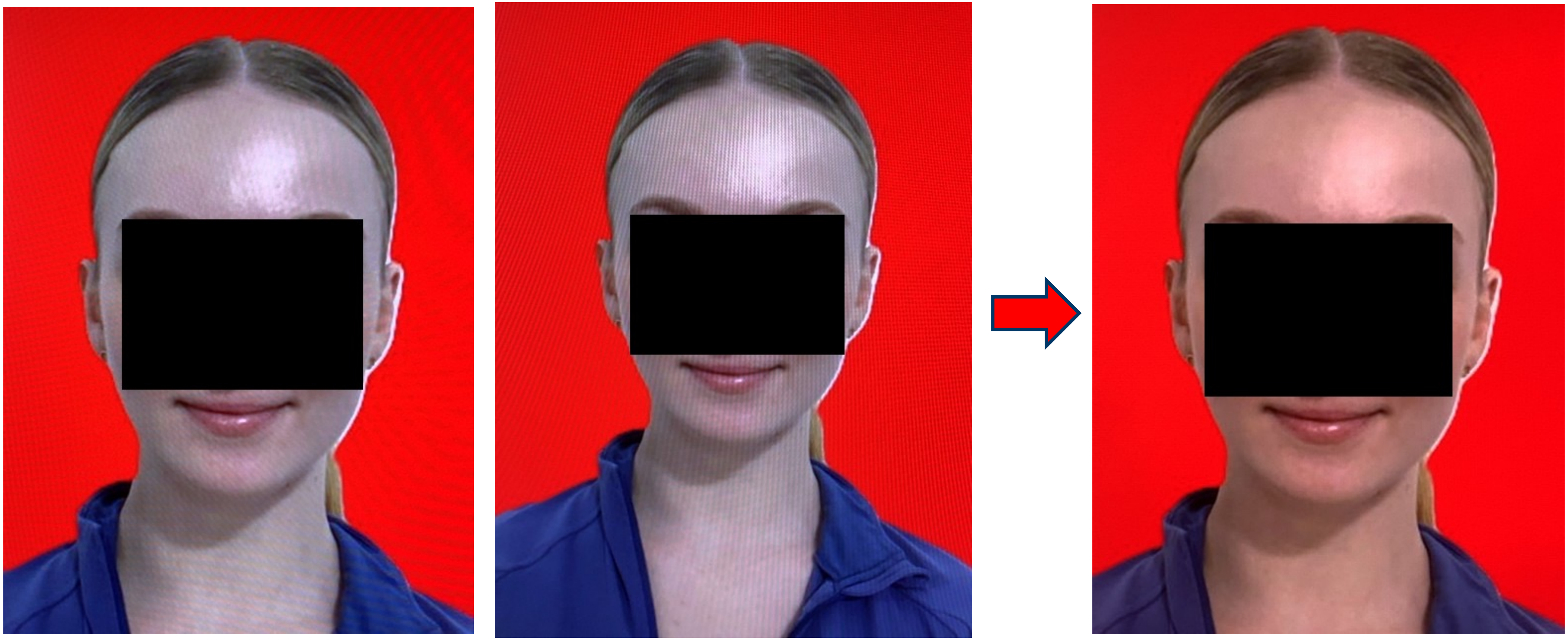


[redacted] [redacted] [redacted] [redacted]

Attack Artefact – Posters and Screen with Lip Region Obscured



Attack Artefact – Modified Image on Monitor

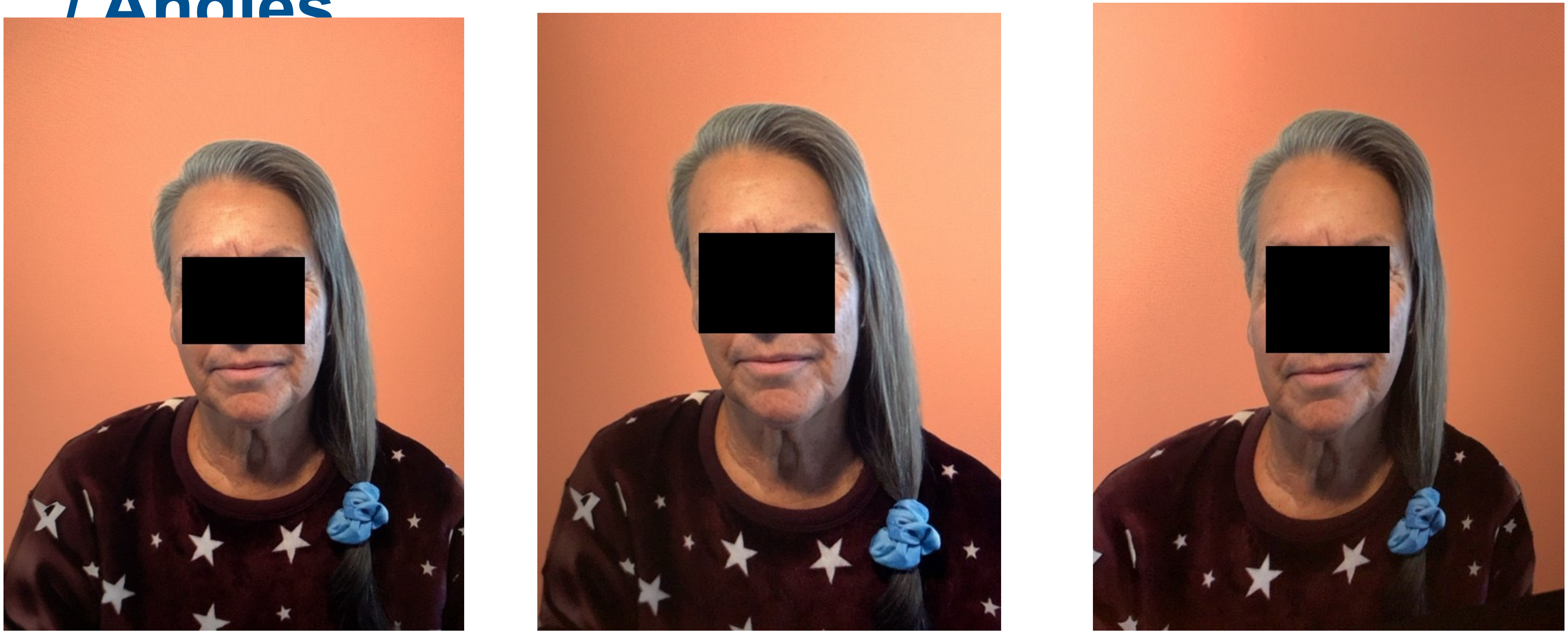


[redacted]

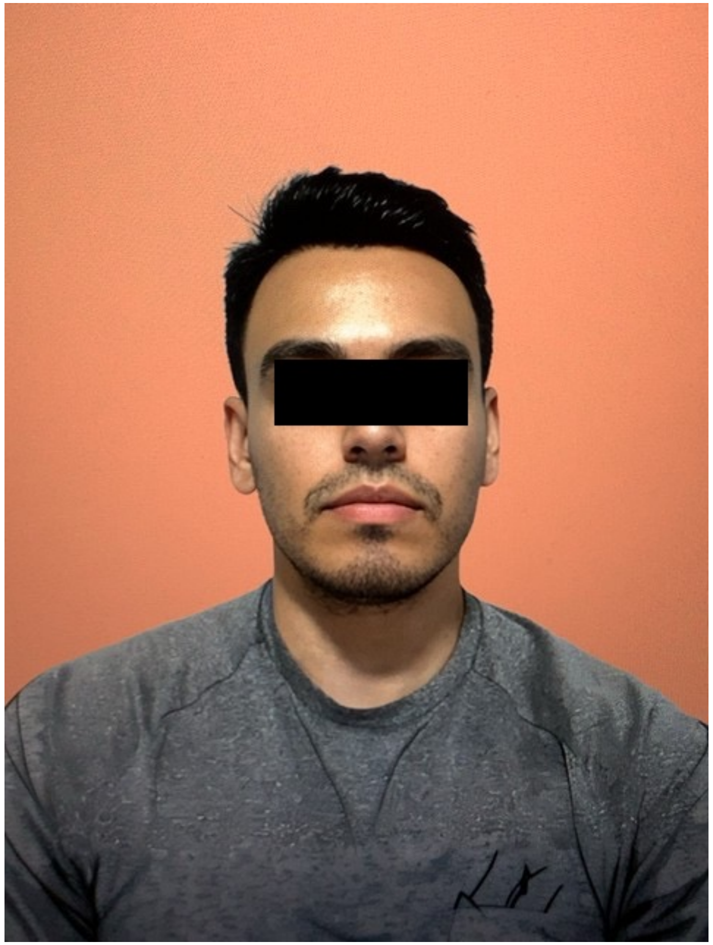
[redacted]

[redacted]

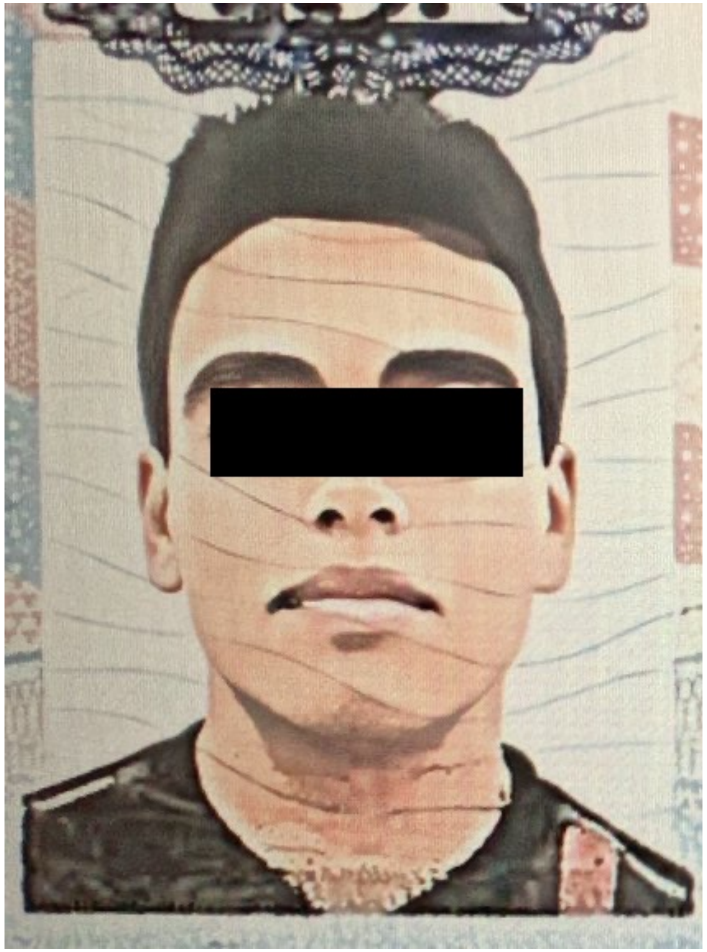
Attack Artefact – Modified Image on Monitor / Angles



Attack Artefact – Modified Image on Monitor



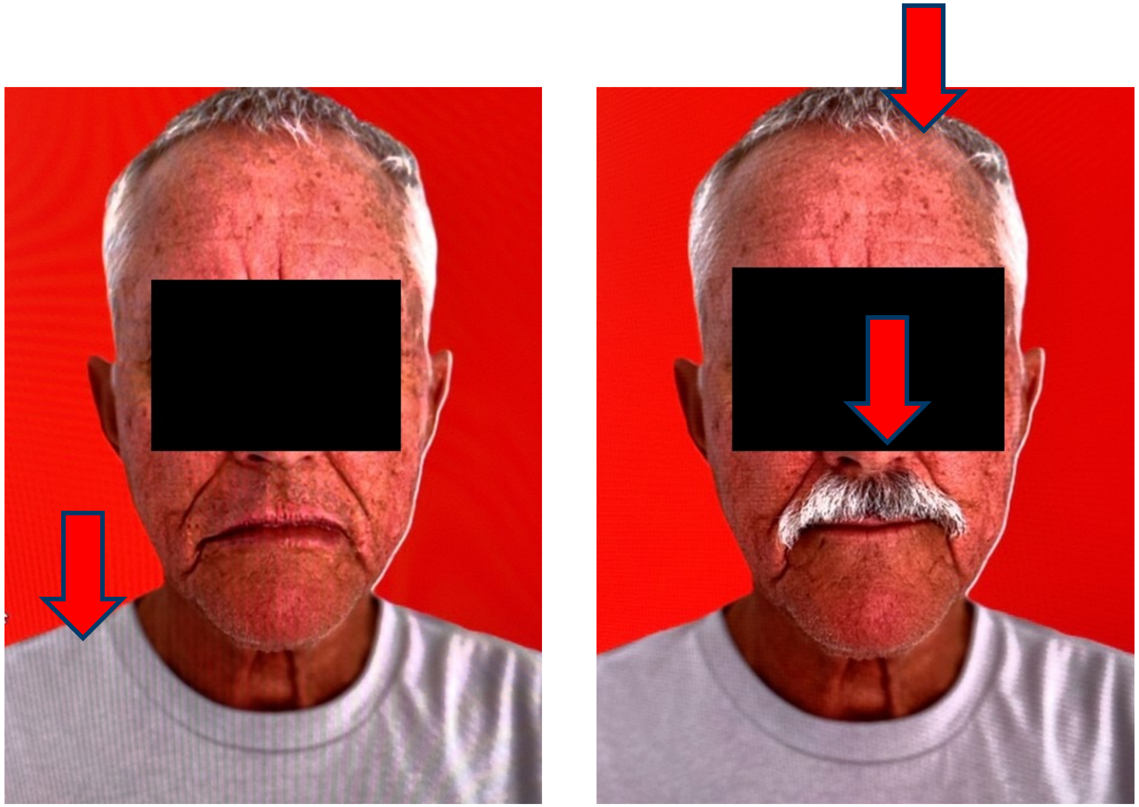
[redacted]

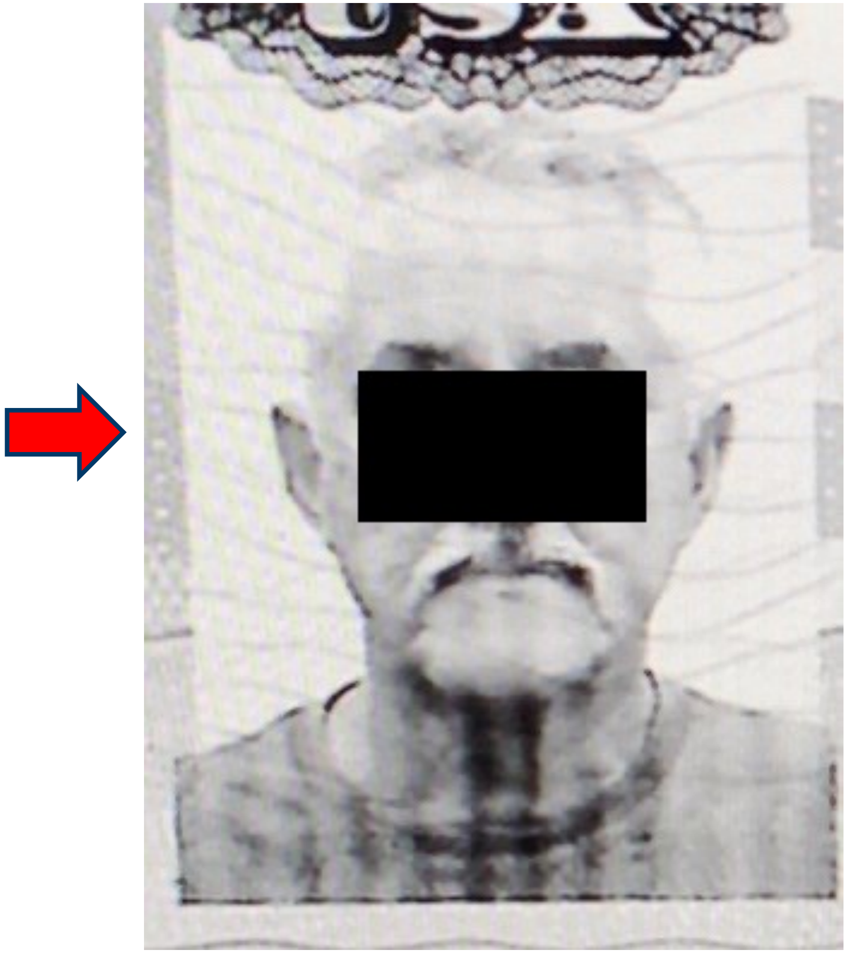


[redacted]

Cartoon Attack?

Red Background / Digital Moustache





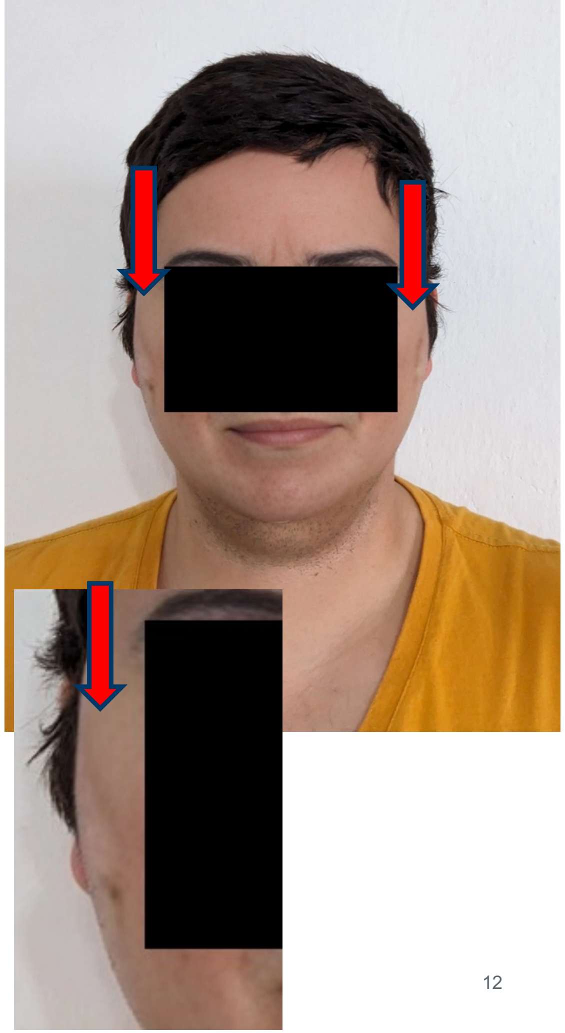
Emulators, Generative Artificial Intelligence (GenAI) and Morphing

A number of more sophisticated attacks originated from phone software emulators (Android) and faces of the traveller appear to be morphed into the centre of a single donors head.

Arguably this is to assist meeting the Image Quality thresholds as well as to match 1:1.

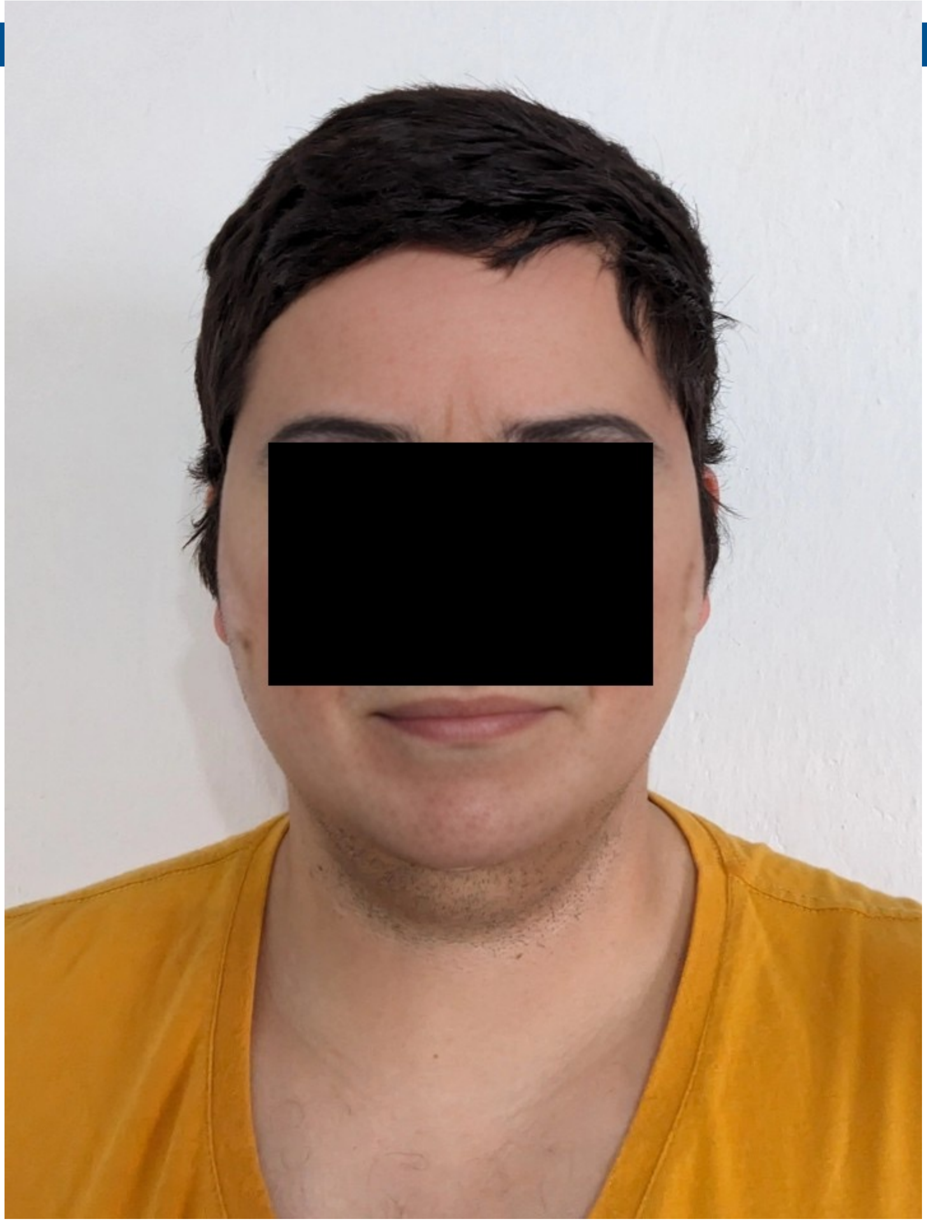
In each case the travellers inner part of the face has been merged/morphed into a male (assumption from facial hair growth) yellow shirt wearing subject.

There are clear indications of morphing technology (we cannot confirm but there are tell tale signs of a tool that’s using Generative AI) with an averaging of facial features but lacking ground truth we cannot be certain.

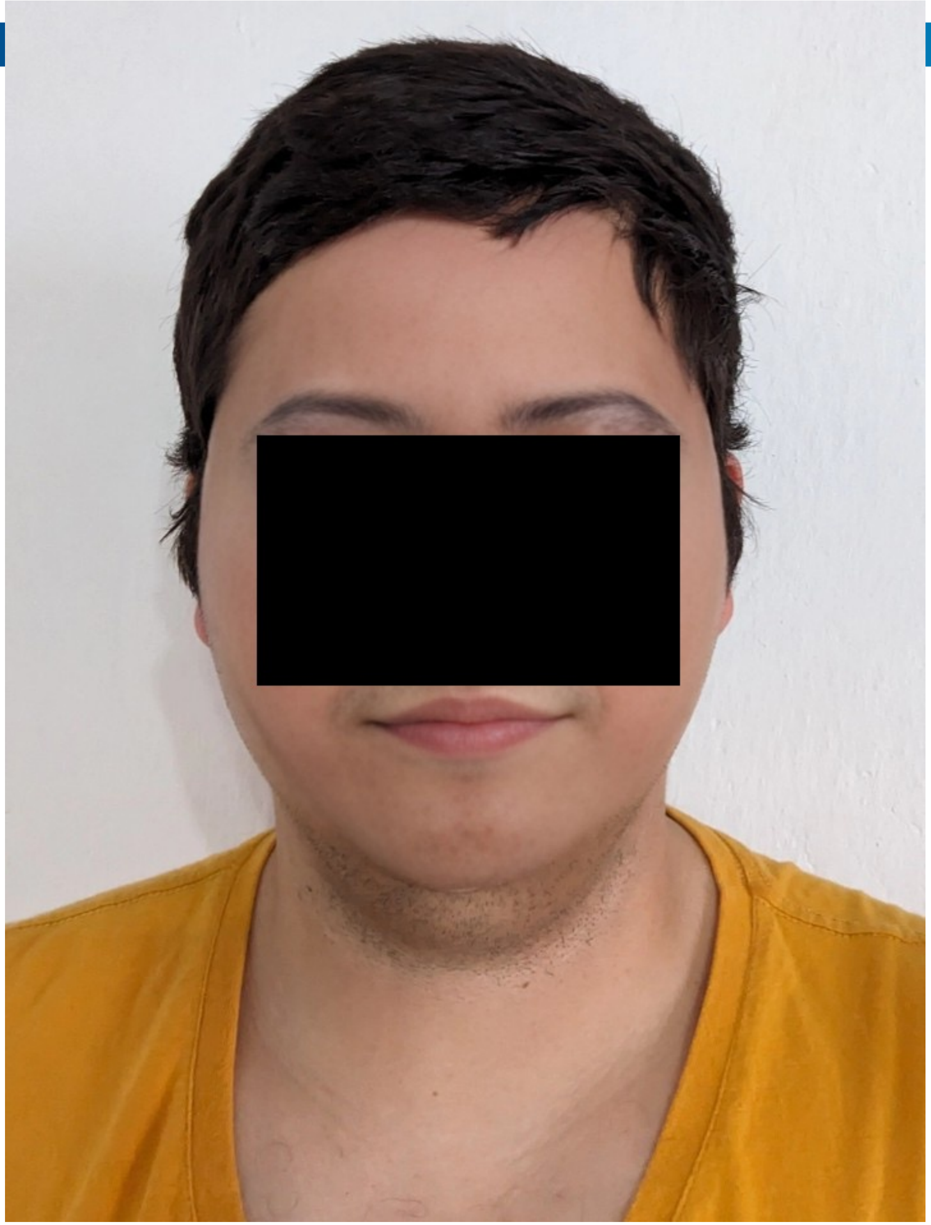


[redacted]

[redacted]



[redacted]



[redacted]

Emulators, Generative Artificial Intelligence (GenAI) and Morphing

[redacted]

[redacted]

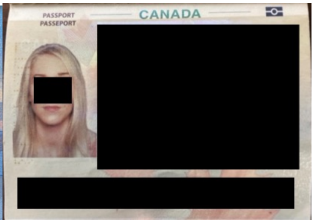
[redacted]

[redacted]

[redacted]
[redacted]
[redacted]

[redacted]
[redacted]
[redacted]

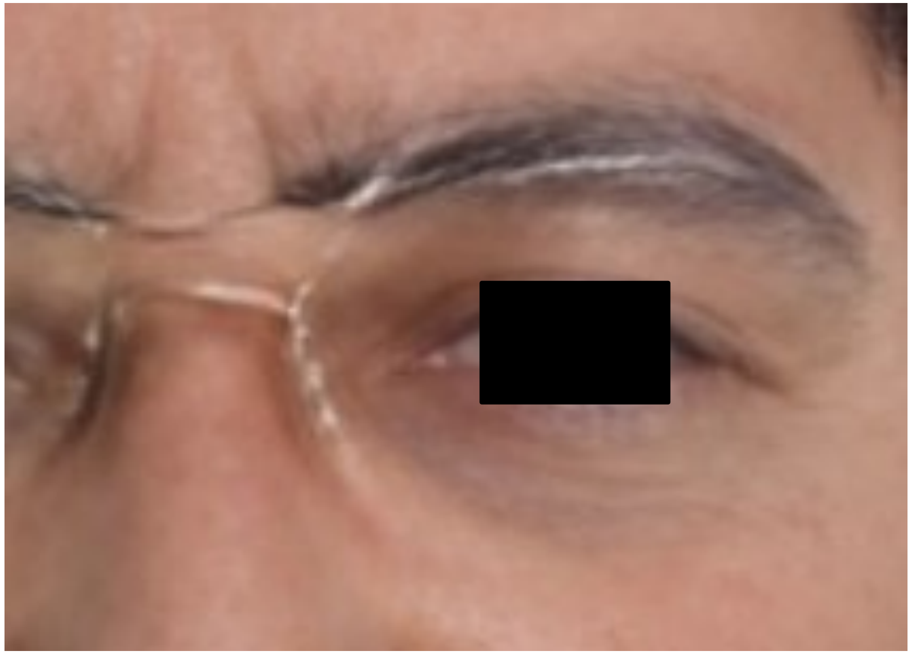
[redacted]
[redacted]
[redacted]
[redacted]

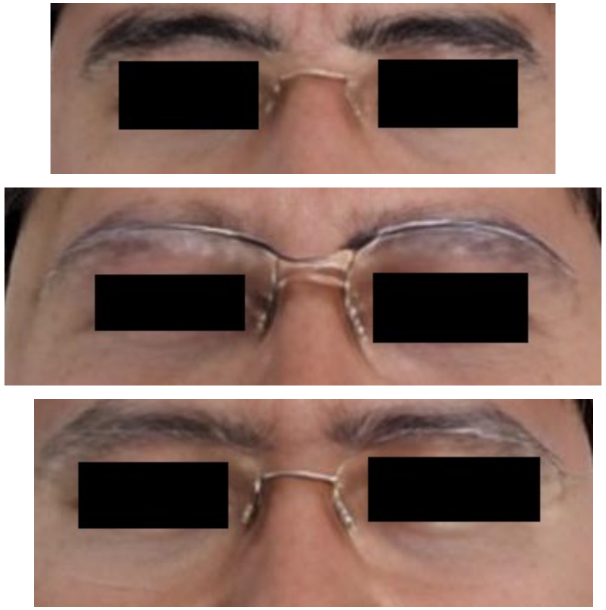


[redacted]
[redacted]
[redacted]

Emulators, Generative Artificial Intelligence (GenAI) and Morphing

If one of the two images has glasses the software being used to Morph them together always uses thin framed gold/silver metallic looking glasses, where the top of the frames, bridge and “feet” are visible, but the lower part of the frames are missing.





Rating Sophistication and Resource Requirements for Attack Types

Skills and tools required – what we have seen and difficulty estimates - to defeat/circumvent quality and liveness

Trivial (simplistic techniques, including hill climbing)

- Taking a photo of a photo or screen image
- Simplistic hill climbing - tilting a physical photo or angling camera to the screen, covering the lips on screen or photo with photographers own finger

Simple (knowledge and everyday tools, includes hill climbing)

- Blanking out/colour change to the image background
- Adding moustache
- Putting own photo over non-chip readable passport image and 1:1 own face (get the facilitator not the traveller)

Sophisticated (knowledge and specialist tools)

- Suspected morphing / image merging
- Using emulators with image modifications

Thankyou

Operational Experiences with Biometric Attack Detection

Jason Prince

Acting Director, Biometric Advisory Section,

Digital Capability Branch, Immigration Operations, Australian Department of Home Affairs

jason.prince@homeaffairs.gov.au

Special thanks: Joshua Abraham, Ph.D.

Biometrics Expert

Identity & Biometrics Engagement & Delivery

Digital Capability Branch