



FACING-2 project overview



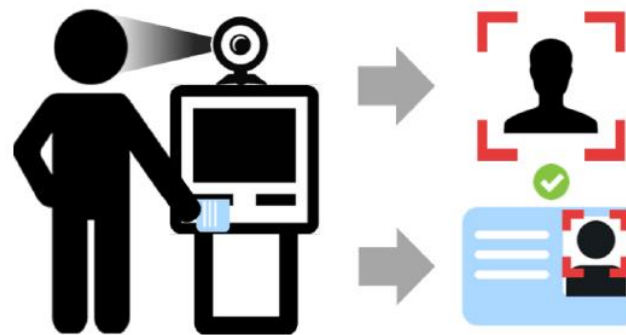
vis team
isr-uc

Coimbra | 2023-05-22

Summary

1. FACING challenges

1. ICAO (International Civil Aviation Organization) compliance
2. Face recognition
3. Morphing attack detection
4. Liveness detection
5. Biometric template protection



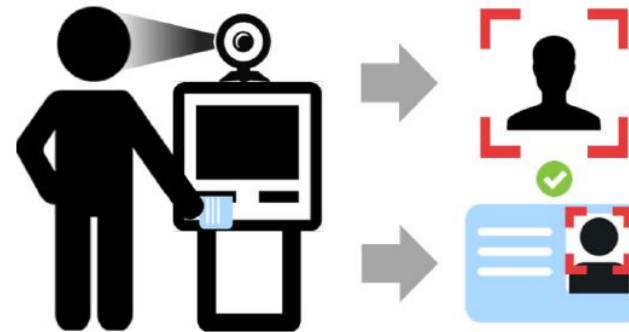
Security processes for biometric (facial) recognition

Summary



1. FACING challenges

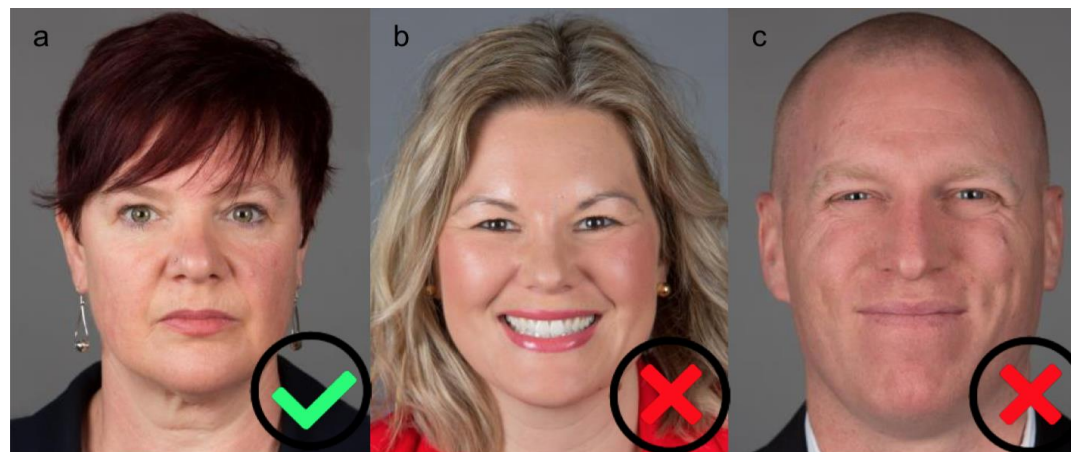
1. ICAO (International Civil Aviation Organization) compliance
2. Face recognition
3. Morphing attack detection
4. Liveness detection
5. Biometric template protection



Security processes for biometric (facial) recognition

ICAO (International Civil Aviation Organization) compliance

- Photographs used in **travel documents** must comply with certain requirements that guarantee standardization and that the individual in the photo is properly identified through that image.
- One of the main institutions to define this type of requirements is the **International Civil Aviation Organization (ICAO)**. It has defined the standards for travel documents [1] [2].
- Examples: neutral facial expression, the contrast with the homogeneous background, the restriction on the use of sunglasses or glasses whose lenses or frames partially or completely hide the eyes, among many others



[1] - [Doc 9303 Machine Readable Travel Documents, 2021](#)

[2] - [Portrait Quality \(Reference Facial Images for MRTD\). Technical Report, 2018](#)

ICAO (International Civil Aviation Organization) compliance

Category	Subcategory	Requirement
SCENE	Scene - Background	24 Uniform / Basic
		25 Shadows
		26 Must allow individual segmentation
	Scene - Illumination	27 No directions of light
		28 Evenly distributed
		29 Hot spots / Reflections / Light Artefacts
	Individual - Pose	30 Head Rotation
		31 Centered Face
	Individual - Facial Expression	32 Eyes / Smile / Mouth
	Individual - Shoulder	33 Towards the camera, frontal
	Individual - Eyes	34 Completely visible
		35 Visible Pupils / Iris (eyes looking at the camera)
36 Red eyes		
37 Eye patches		

Subcategory	Requirement
Artefact - Glasses	38 Dark tinted lenses
	39 Transparent
	40 Frame Thickness
Head Covering	41 Generally not allowed, it might be in case of religious coverings (face must be visible)
Assistance	42 Other people not allowed
	43 Object/Toys not allowed

ICAO (International Civil Aviation Organization) compliance

Category	Subcategory	Requirement
DIGITAL	Geometry	1 Pixel aspect ratio
		2 Origin coordinates
	Color Profile	3 Color space
		4 "Video interlacing" not allowed
		5 Infrared cameras not allowed
	Post Processing	6 Rotation
		7 Cropping
		8 Down Sampling

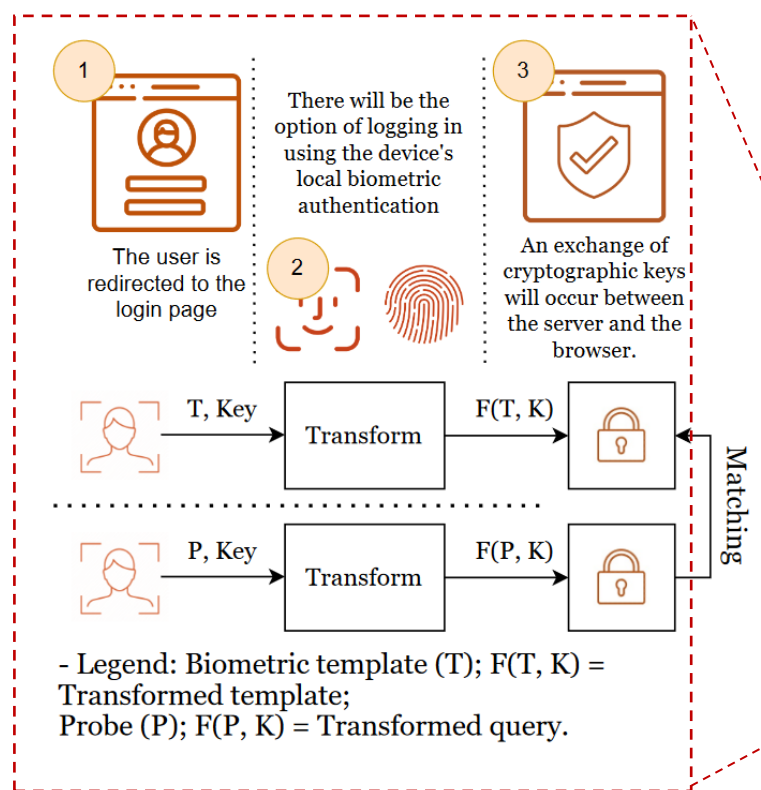
Category	Requirement
PHOTOGRAPH	9 Contrast
	10 Focus and "depth of field"
	11 Unnatural color
	12 Grey scale image correction
	13 Camera Lenses's Radial Distortion below 2.5%
	14 Color Saturation

Category	Subcategory	Requirement
IMAGE	Dimensions - Physical	15 Width,, Height (cm)
	Dimensions - Pixels	16 Width, Height
	Face - Position	17 Horizontal, vertical
	Face - Dimensions	18 Width, Height
		19 Width/Height Ratio
	Eyes - Coordinates	20 Distance between the eyes (inclusive)
		21 Eyes's Coordinate Y
		22 Right eye X coordinate
		23 Left eye X coordinate

Biometric template protection

Obfuscation techniques

“FIDO Biometrics Privacy Schemes protects your keys affected by Data Breaches and Phishing Campaigns”



1st Open Day and Workshop
14th July 2022

ISR INSTITUTO DE SISTEMAS E ROBÓTICA
UNIVERSIDADE DE COIMBRA

FIDO Biometrics Privacy Schemes protects your keys affected by Data Breaches and Phishing Campaigns

Silva, José (openday@silvajose.net)

What's Fast ID Online (FIDO)?

- FIDO authentication defines a secure authentication mechanism for users to access websites and applications
- FIDO-based authentication with public-key cryptography removes many of the problems that stem from password-based authentication
- With FIDO, websites and applications can request a user to create a passkey to access their account

Biometric schemes

- When using facial recognition, relevant information about the individual is captured, which can compromise the user's privacy
- Biometric schemes should ideally leak no information about the biometric trait that has been captured

Biometric Template Protection Schemes	Feature Transformation Based Schemes	Feature Based Schemes	
	Biometric Cryptosystems	Reversible Transform Based Schemes	Key Binding Schemes
		Key Generation Schemes	Cryptography for Biometric
Neural Network Based Schemes	Feature Level	Image Level	

Passkey Access

- The passkey access method relies on unlocking a device to verify a user's identity
- This may be performed with a biometric scheme, such as facial recognition

Goal

- Evaluate Biometric Schemes to satisfy the most important criteria: recognition accuracy, irreversibility, renewability, and unlinkability
- Performing Testing and Certification for Servers and Devices using the FIDO2 Certified Solutions available
- Performing Biometric Systems Certification according to the Portuguese Law 27/05/2021

- Legend: Biometric template (T); F(T, K) = Transformed template;
Probe (P); F(P, K) = Transformed query.

Department of Electrical and Computer Engineering | FCTUC
web.isr.uc.pt/openday

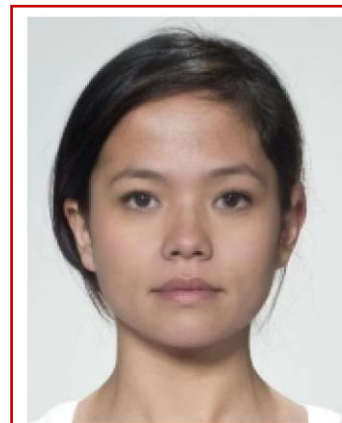
FACING - Morphing

Face Morphing

Image morphing techniques are used to combine information from two (or more) images into one image.



Subject 1



Morphed



Subject 2



Subject 1



Morphed



Subject 2

Morphing attacks:

- Face Morphing oppose significant risks for document security.
- Two scenarios of morphing detection are usually considered:

Differential (border control scenario)

Photo presented as
being from Alice



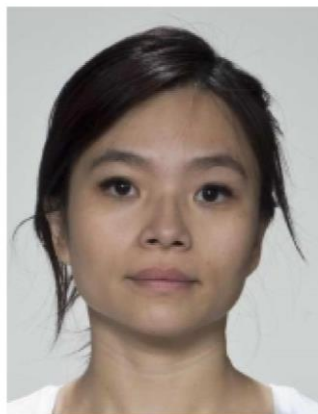
Morphed

Does this photo
correspond to
Alice?



Face verification (1:1)

Database Photo
of Alice



Subject 2

No-reference (enrollment scenario)



Is this face a
morphed face?

FACING – Liveness detection

Liveness detection:

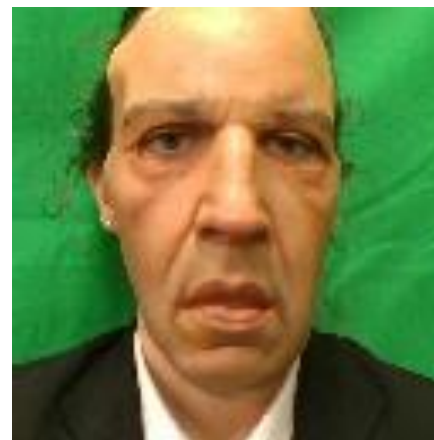
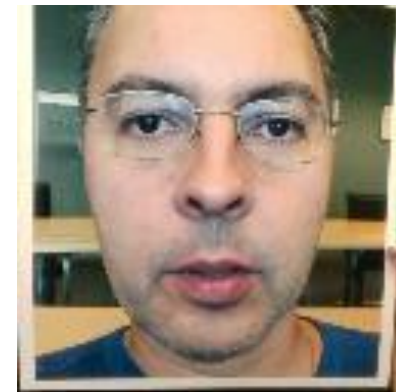
- What is **liveness detection**? Liveness Detection or Face Anti Spoofing is the task of verifying if a face presented to a system is real or an attack (*bonafide* or *spoof*)
- What is meant by “**attack**”? An attack is any attempt to change the identity of the individual who presents himself to the system, either by obfuscating his own identity or by impersonation (em português: representação ou personificação) of another subject.

Types of attacks

Print attack: display a printed image (photo) to an authentication system

Replay attack: display a video recording

Mask attack: covering one's face with a material which may present or not human facial features (impersonating or obfuscating)



Thank you!

Visit us at:

<https://visteam.isr.uc.pt>