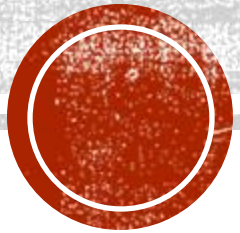
# PRESENTATION ATTACK DETECTION IN FACE RECOGNITION SYSTEMS

Team members:

Dhathri Bathini

Anosh Kudikala



# INTRODUCTION

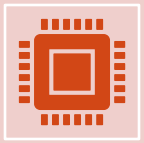
- Face recognition systems are widely used in security-critical applications.
- Presentation attacks exploit vulnerabilities by using artifacts like photos, masks, or videos to deceive the system.
- This presentation explores the challenges, detection techniques, and mitigation strategies.

# DEFINITIONS

- Presentation Attack (PA)
  - An attempt to fool the biometric recognition system by presenting fake biometric data to the sensor and gaining access to the system.
  - These attacks are commonly called as spoofing attacks, and the fake biometric data that is presented to the sensor is called spoof.

- Presentation Attack Detection (PAD)
  - Identifying whether the presented biometric data to the sensor is spoof or not.
  - This is also called as anti-spoofing.

# IMPORTANCE:



Identification of these presentation attacks are very important because they pose a major threat to biometric recognition system.

The attack is done at the sensor level: the sensor is fooled and not replaced nor tampered.

Attackers do not need to have any internal knowledge about the system, it can be done literally by anyone using very basic tools.

# PRESENTATION ATTACKS IN REALITY:

**Bank robbery (2010):**

Conrad Zdzierak used a silicon masks to pass himself off as a black character "SPFX The Player" during bank robberies.

# PRESENTATION ATTACKS IN REALITY:

**Immigration (Jan 2011):**

A passenger boarded a plane in Hong Kong with an old man mask and arrived in Canada!

# PRESENTATION ATTACKS IN REALITY:


**Android 4.0 (Nov 2011):**

Android 4.0 face unlock feature spoofed by photograph.

# PRESENTATION ATTACKS IN REALITY:

**Bank robbery (2013):**

Steven Ray Milam robbed 11 banks in Texas, disguised as "SPFY The Handsome Guy" using a silicon face mask.

# PRESENTATION ATTACKS IN REALITY:

**Robbery (2012):**

Burglars used silicone face masks to disguise themselves as cops while robbing a store in Queens.

# PRESENTATION ATTACKS IN REALITY:

**Jailbreak (2019):**

A Brazilian drug trafficker serving a 73-year prison sentence attempted (and failed ) to escape from jail disguised as his 19-year-old daughter, using a silicon mask of the daughter's face.

# TYPES OF PRESENTATION ATTACK INSTRUMENTS:

They can be divided into 3 main categories:

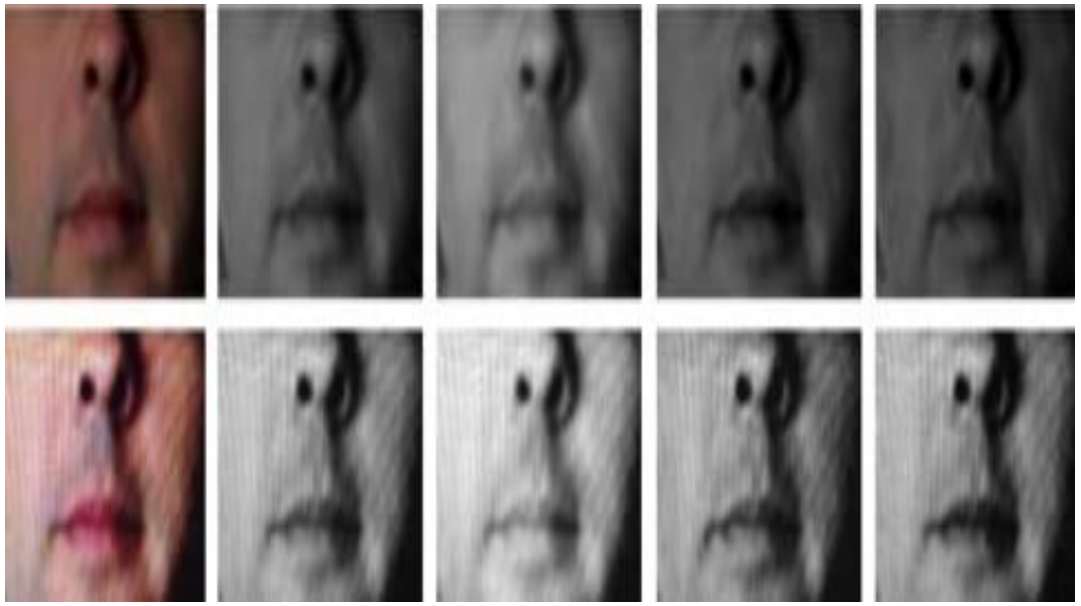
1. Photograph or recording

2. Synthetic biometric characteristic: the attacker generates a synthetic model of either the target's biometric characteristic or generic feature set (ThatsMyFace.com)

3. Self modification: The attacker alters physically or digitally their own biometric characteristic to mimic the target's biometric characteristic. Example: Makeup, Morphed images

# PRESENTATION ATTACK DETECTION FOR PRINTED PHOTO:

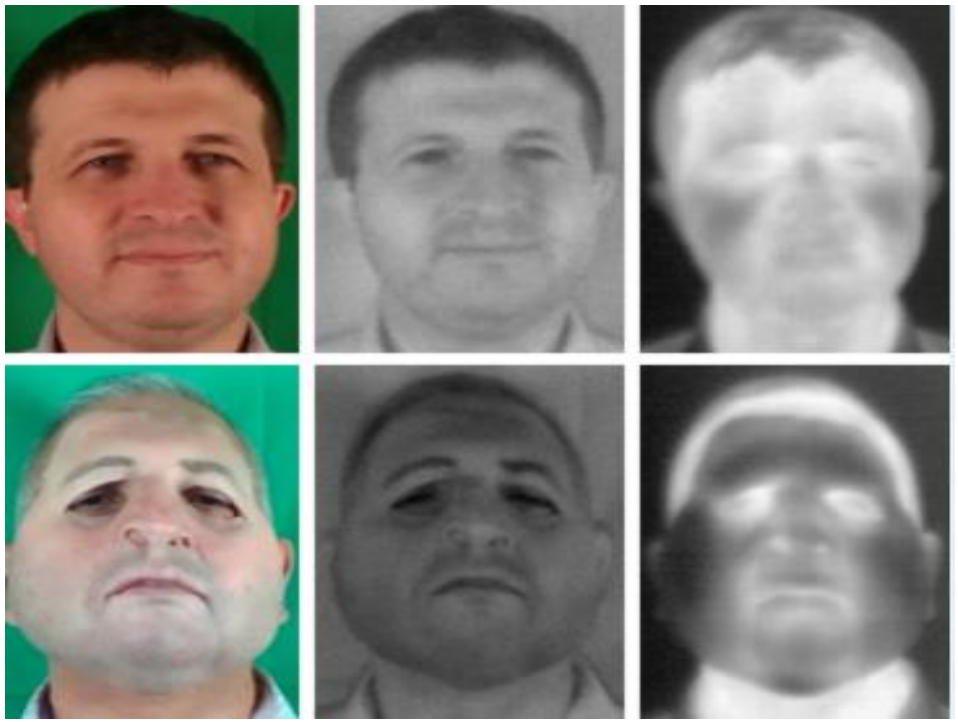
- The main characteristic shared by all printed photo is their static nature, so the method can exploit this by searching for dynamic features.
- An effective PAD method could also look for Moire patterns which are formed when an image is replayed to the sensor
- Can also use 3D cameras to detect flat surfaces.



# PRESENTATION ATTACK DETECTION FOR FACE MASKS:

- Blinking can be used to detect the mask with no eye holes
- Whether or not the mask has eye holes, asking the user to smile or speak could be simple ways of detecting the presence of the mask due to the mask's inflexibility.
- 3D masks can be detected using thermal imaging.

# PRESENTATION ATTACK DETECTION FOR SILICONE FACE MASKS:

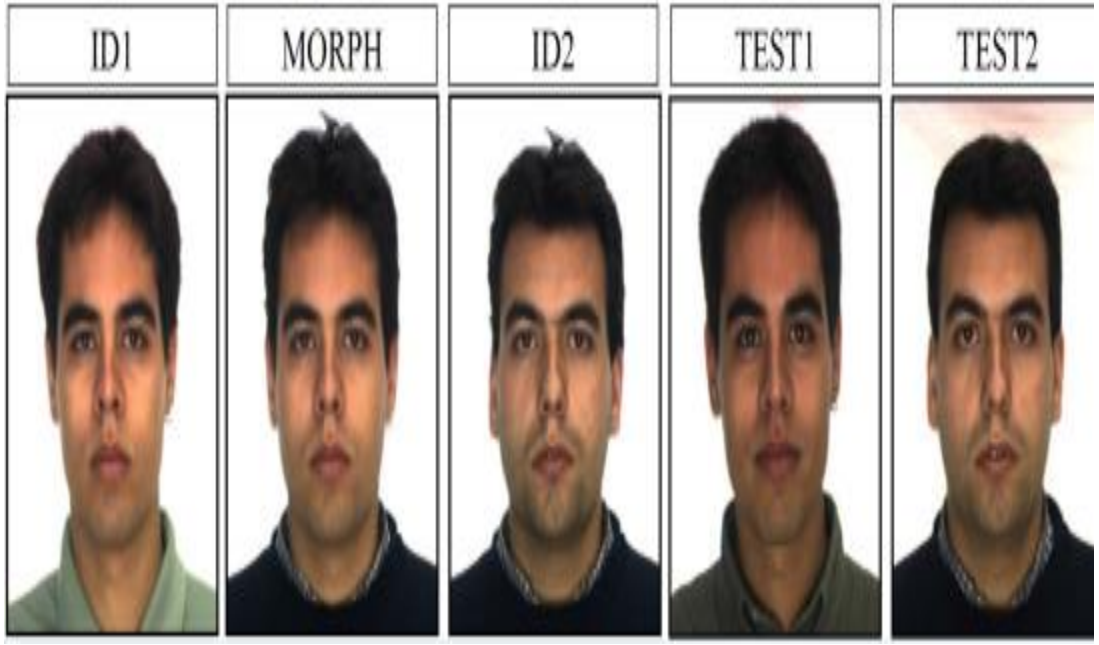


- These masks are flexible. They allow the attacker to blink, talk etc
- Thermal imagery can be quite effective for detecting silicone masks, using a CNN-based PAD method.
- This method is particularly showed effective when using multispectral imaging ( Visible, Near- infrared, and Thermal)

# PRESENTATION ATTACK DETECTION FOR FACE MAKE-UP:

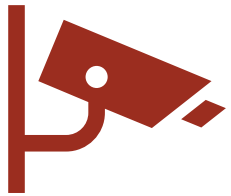
- This is a on-going research topic
- But it can be detected using a CNN to extract both global ( i.e., shape) and local (i.e., texture) face information to detect ageing makeup,

# PRESENTATION ATTACK DETECTION FOR MORPHED FACE IMAGES:



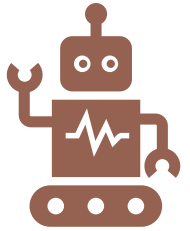

- This involves combining of faces of two people ( attacker and target) to enable both to be identifies as the same identity
- An Effective PAD method could be to example the morphed image for artifacts(anomalies)
- When sophisticated morphing methods are used, well trained CNN could be effective for identifying morphed images

# MITIGATION STRATEGIES



Hardware-based solutions: Employing infrared cameras or depth sensors.

Multi-modal systems: Combining face recognition with voice or fingerprint.



Algorithmic improvements: Robust models trained to detect attacks.

Reference: https://ieee-biometrics.org/event/face-presentation-attack-detection/

# THANK YOU