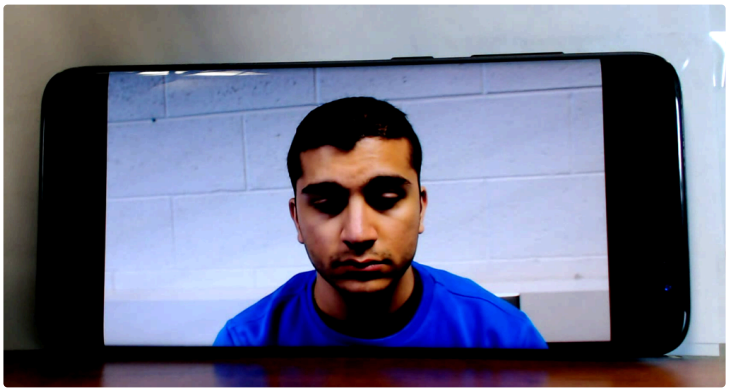
Documentation of Face Presentation Attack Instruments

Presentation Attack Instruments (PAIs) for facial recognition systems are tools or methods used to deceive these systems by presenting false or altered facial data. These attacks aim to gain unauthorized access or impersonate an individual. Here are the different types of face presentation attack instruments:

1. 2D Attacks

- **Printed Photos:**
  - **High-Resolution Images:** Using high-quality printed photographs of a person's face to fool the system.

- **Digital Displays:**
  - **Screens or Tablets:** Displaying a digital image of a face on a screen or tablet to the camera.



2. 3D Attacks

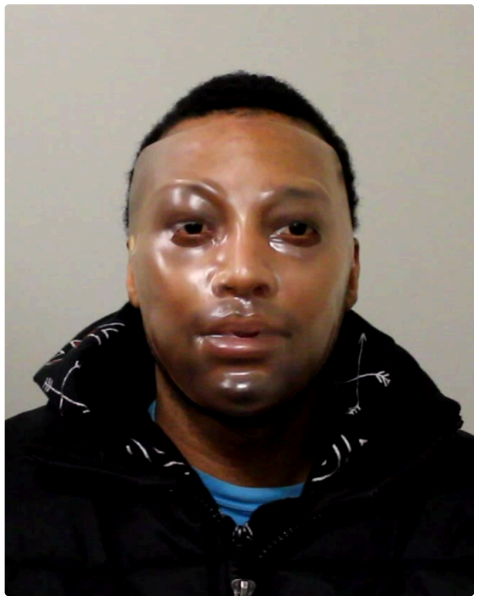
- **Masks:**
  - **Paper Masks:** Simple masks made from printed images on paper.

- **Silicone Masks:** High-quality masks made from silicone to closely resemble a person’s face.

- **Latex Masks:** Flexible masks made from latex.

Latex and silicone masks differ primarily in material properties and realism. Latex masks are made from a natural or synthetic rubber material, making them flexible and lightweight, but they may lack fine detail and realism. Silicone masks, on the other hand, are made from silicone rubber, offering a higher level of detail, durability, and a more lifelike appearance, mimicking skin texture and movement. Latex masks are generally less expensive and easier to produce, while silicone masks are costlier but provide superior realism and comfort for extended wear.

- **3D Printed Masks:**
  - **Plastic or Resin Masks:** Using 3D printing technology to create a detailed replica of a person's face.



Transparent Plastic mask

(a) Transparent Plastic Mask

(b) Opaque Plastic Mask

17 hard resin masks

A resin mask is made from hard, durable synthetic resin, providing a rigid structure that can capture intricate facial details. Its inflexibility can limit realistic facial movements, making it less lifelike compared to silicone or latex masks. Resin masks are often used for high-detail applications where durability is essential.

3. Partial Attacks

- **Eye Cutouts:**
  - **Photos with Eye Holes:** Printed photos with holes cut out for the attacker's eyes to appear more realistic.

- **Partial Masks:**
  - **Glasses with Eyes:** Glasses with printed eyes on the lenses.

- **Nose and Eye Area:** Using a mask that covers only specific parts of the face like the nose and eyes to trick partial recognition systems.

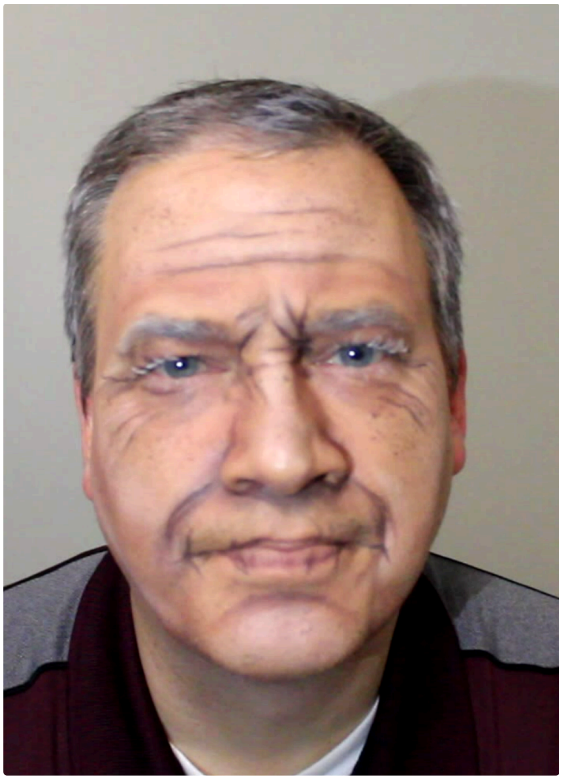
4. Hybrid Attacks

- **Combination of 2D and 3D:**
  - **2D Mask with 3D Features:** Using a 2D printed photo combined with 3D features like a nose or ears to create a more convincing appearance.

- **Enhanced Masks:**
  - **Animated Masks:** Masks with mechanical parts that mimic facial movements, such as blinking eyes or moving lips.

5. Makeup and Prosthetics

- **Makeup:**
  - **Heavy Makeup:** Using makeup to alter facial features to resemble another person.



- **Prosthetics:**
  - **Fake Noses or Chins:** Using prosthetic devices to change the shape of the face.

7. 3D printing attack

Combining 3D scanning and 3D printing involves first using a 3D scanner to capture a highly detailed digital model of a person's face. This digital model includes precise measurements and textures, creating a lifelike representation. The scanned data is then processed and sent to a 3D printer, which prints the face model using materials like plastic or resin. The resulting 3D printed mask or model can be highly accurate and realistic, capable of deceiving facial recognition systems. This method exploits the detailed replication capabilities of both 3D scanning and 3D printing technologies.

8. **Tshirt printing attack**

A T-shirt presentation attack instrument (PAI) is a novel method designed to circumvent remote identity proofing systems. By using a specially designed T-shirt that mimics the visual characteristics of a real person, attackers can deceive biometric systems that rely on facial recognition or similar technologies. This approach highlights vulnerabilities in current identity verification methods, particularly in scenarios where video or live monitoring is minimal. The use of a PAI like this raises significant concerns regarding the effectiveness of remote identity proofing, necessitating the development of more robust detection mechanisms. Addressing these vulnerabilities is crucial for enhancing security and trust in remote identity verification processes.

9. **Wax Face attack**

A wax attack utilizes materials such as high-quality wax, silicone, or 3D-printed substances to create highly detailed masks that mimic the facial features of a legitimate user. These materials are chosen for their ability to replicate human skin texture and tone, making it challenging for biometric systems to differentiate between the mask and a real face. Wax, in particular, offers a malleability that allows for fine detail work, while silicone provides durability and flexibility, enhancing the mask's realism. The incorporation of synthetic hair and pigmentation techniques further improves the mask's authenticity, creating a convincing likeness that can deceive even sophisticated biometric systems. This highlights the importance of integrating advanced detection mechanisms that can identify the subtle differences between genuine human features and artificial materials, thus bolstering security in biometric authentication.

10. Bubblehead Attack:

A bubblehead attack is a sophisticated presentation attack that involves the use of a life-sized, realistic mannequin or model designed to spoof biometric systems, particularly facial recognition. The "bubblehead" refers to the oversized, lifelike head of the mannequin, which is often made from materials like silicone or rubber to closely mimic human skin texture and features. This attack can be particularly effective in situations where biometric systems rely on video feeds or photographs, as the bubblehead can be positioned to appear as though it is interacting with the system. Advanced techniques, such as adding realistic hair and makeup, can enhance the illusion, making it difficult for biometric systems to detect that the entity is not a real person. This underscores the necessity for biometric technologies to incorporate robust liveness detection mechanisms that can differentiate between genuine users and sophisticated impersonation attempts like the bubblehead attack.

11. 3D Mannequin:

A 3D mannequin attack is a presentation attack where an attacker uses a highly realistic 3D-printed mannequin or bust to deceive biometric authentication systems, particularly those relying on facial recognition. The mannequin is created to closely resemble a legitimate user, replicating their facial structure, skin tone, and features using advanced 3D printing technology. Materials such as resin or silicone can be used to give the mannequin a lifelike appearance, with some even incorporating hair and fine details to enhance realism.