MANTRA

Innovation that counts

WHITE PAPER

Presentation Attack Detection (PAD) methods for FINGERPRINT AND FACE RECOGNITION

Active, Passive, and deep learning methods

www.mantratec.com

Table of Contents:

Abstract

This paper presents various presentation attacks and their commonly used counter detection methods. We will discuss the anti-spoofing methods used in fingerprint and face recognition systems, as well as future technologies. This article discusses all hardware and software-based spoof detection techniques and the importance of AI-based deep learning.

Introduction

Biometrics has evolved as the most trusted and convenient authentication method for organizations and individuals. Fingerprint scanning is the most widely used biometric modality, followed by facial recognition. Both modalities are employed in everything from simple electronic gadgets to high-security applications, including Civil ID enrollment, airport boarding authentication, and law enforcement. Besides, the most potential application in the future is web applications. Not just the social media accounts and cloud storage spaces, the bank apps, civil registration apps, and travel applications use and will use biometrics to speed up the on boarding and verification processes.

While biometrics is spreading into new fields, hackers are becoming even smarter with the help of AI capabilities. Obviously, biometrics is one of the most secure authentication techniques, but failing to address hacking concerns in an age of rising digital dependency and internet users would result in massive consequences.

There are a couple of common ways to hack biometrics, hacking the database or system to leave the system unanswered on successful authentication, or manipulating the outcome of authentication trails, which can rectify by ensuring robust cyber security. But the most critical issue is spoofing of biometrics. It is the technique of impersonating someone by utilizing fabricated biometric samples, known as a "presentation attack."

Over time, researchers have developed various countermeasures to compact presentation attacks for all biometric modalities. In this research paper, we will discuss the anti-spoofing methods of facial recognition and fingerprint scanning.

Background

Biometric authentication usage has increased recently due to the increased use of the internet and the Covid crisis. The current trend in biometrics, especially contactless biometrics, perfectly suits the changing circumstances in surveillance, work from home, access control, and airport security. Despite the fact that biometric adaptation among companies has reduced cyber attacks, one successful breach into the system may heavily affect the credibility of the company and the biometric system.

Spoofing or presentation attacks are the most dangerous sort of attack since they do not require any programming or coding abilities. Now, biometrics could affect the whole population. Hence, research on spoofing began in the first decade of the century itself. Numerous studies and claims by individuals confirmed the effectiveness of spoofing against biometric authentication. As counter steps, a standard for anti-spoof technology, ISO/IEC 30107, was developed in 2014.

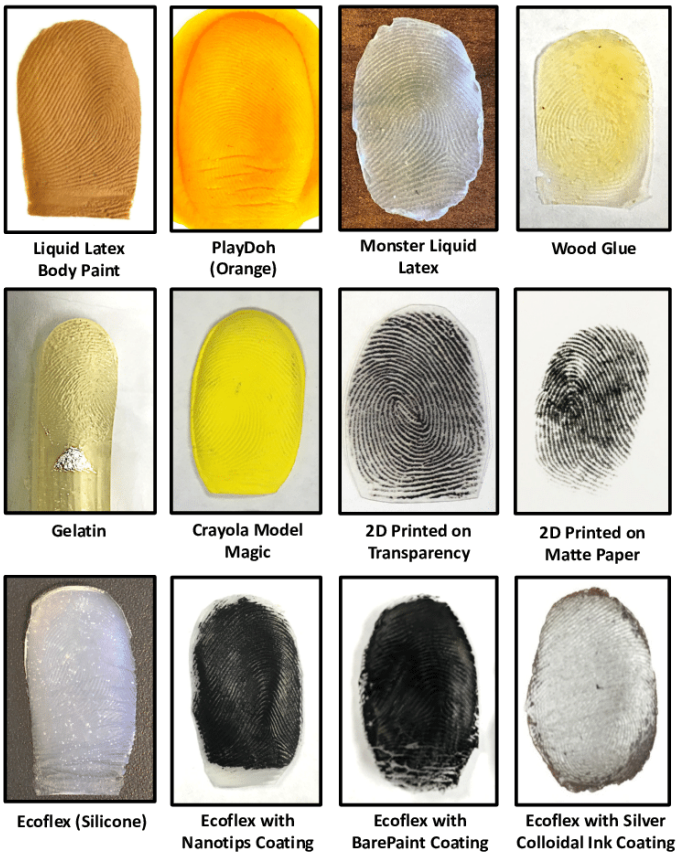
Spoofing techniques and the presentation attack detection (PAD) approaches are categorized in the standard. The standard includes advanced anti-spoofing solutions like AI spoof detection algorithms and data-driven fusion approaches. This paper puts forward the conventional and latest anti-spoofing technologies.

Presentation Attack Detection (PAD) & Liveness detection

PAD is the method of differentiating real live skin from forged biometric samples while the liveness check detects vitals (like blood flow, pulse, skin pores, etc.) to ensure the biometrics scanned is part of live skin. Though the idea behind both the technology is the same; to distinguish fake biometrics. Both technologies accomplish the same objective in different ways. PAD refers to the detection of a fake replica of a real biometric. Liveness detection refers to the identification of human tissue as belonging to a live person.

The techniques have a couple of ways to achieve presentation detection, including additional hardware and software integrations. The system extracts discriminating characteristics from new data from the sample using additional sensors or by further processing the same sensor data.

Fingerprint Spoofing methods



Hackers use different techniques to spoof fingerprints. A typical method for fooling a fingerprint sensor is to create a mold of the fingerprint out of materials such as gelatine, latex, wood glue, silicone, etc. People also use 2D prints of fingerprints to mock the original biometrics. There are other techniques like using graphite and tape to recover fingerprints and recreating their image with the help of software. Or just spread graphite powder or vapourize over the sensors so that it reactivates the previous fingerprint.

PAD in fingerprint scanning

Two categories of PAD techniques are called static and dynamic methods. A forged fingerprint image itself leaves clues in it that can be the absence of patterns, extra perfection, background noise, etc. Sometimes forged artifacts can be extra perfect where usual imperfections are missing, like 2D print spoofing. Reading such parameters turns out to be a static method because it involves analyzing a single frame.

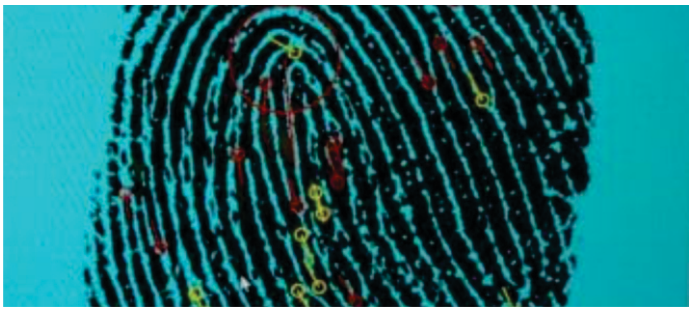
On the other hand, in the dynamic method, sensors read the changing factors, more in-depth analysis of parameters from multiple frames to detect liveness in acquired fingerprints.

Static methods

It is the cheapest PAD approach. The static method mainly reads skin parameters to ensure the liveness of prints that are skin elasticity, perspiration-based features, textural characteristics such as smoothness (aka surface coarseness), and morphology extracted from single fingerprint capture. For example, natural skin is usually smoother than materials such as gelatin and silicone polymers made of agglomerated molecules. A live finger will also have more ridge distortion than a fake.

Other static methods have mentioned below:

A. Pores based



Sweat pores are a unique feature seen only in live skin because molds cannot sweat. Sweat starts from pores and unevenly diffuses along the ridge. In contrast, spoof captures tend to show high uniformity. Since these sweat pores are tiny, it is challenging to incorporate them into the molds.

The method employs two filters: a high-pass filter to extract pores and a correlation filter to determine the location of the pores.

B. Reflection

When illuminated, the spectrum of light reflected from the finger is very distinctive of human skin. In the short-wave infrared spectrum, skin reflection is also independent of the skin tone, making it unique.

Dynamic methods

The process examines consecutive multiple frames of a fingerprint to find a sign of liveness from the finger.

A. Skin distortion analysis:

The skin turns whiter under pressure. This effect becomes visible when a fingertip is pressed against a sensor capturing surface, and the blood flow is held back due to tissue compression. Besides, the user may be asked to move the finger while pressing it against the scanner surface, thus intentionally amplifying the skin deformation. These changes are analyzed using special image sensors to confirm the liveness.

B. Blood flow detection

The anti-spoof detection system employs different sensors to detect the blood flow beneath the finger skin. There are types that use Near-IR, ultrasonic, and optical coherence tomography (OCT) technology to detect blood flow. Laser speckle contrast imaging (LSCI) is an upcoming technology in line.

C. Active sweat pores

When the finger presses against the capture area, sweat flows down to the valleys from the pores. Active pores with ionic sweat fluid are only available on live fingers and are tough to replicate. The system reads multiple frames to read this dynamic change.

D. AI-enhanced methods

Today, anti-spoof detection measures are leveraging deep learning convolutional neural networks (CNN), most commonly applied to visual imagery analysis.
CNN models can train to distinguish a live finger from a fake. They can, for instance, identify forged fingerprints with known materials.

Face spoofing methods

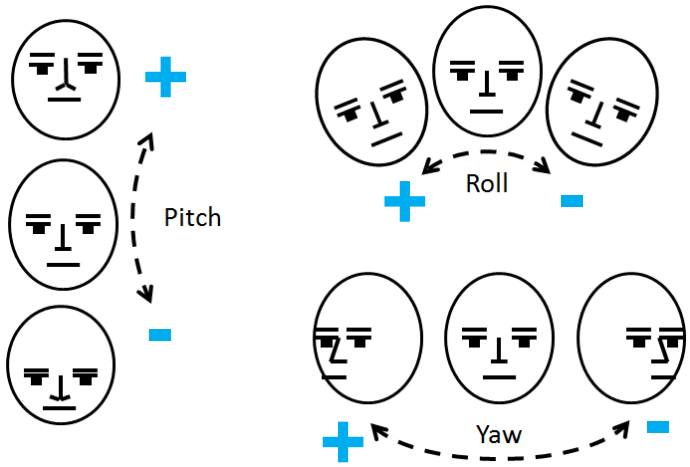
Cheating facial recognition cameras is really difficult these days, especially in the age of AI. However, hackers also have some advanced methods to cheat cameras.

- Showing photographs or videos of legitimate users to the camera that are widely accessible via social media. To counteract this method, early face recognition systems detected eye blinking, which is easily countered by displaying a printed face with the eyes clipped off such that the impostor's eyes flicker below.
- Deep fake: Imposters can take an image or video and create a realistic 3D animation with the help of software. The model can be so realistic that it nodes and blinks in response.
- Hindering the true identity of applying cosmetics to facial landmarks.
- 3D face mask: Such masks created out of 3D images can be made in resin, latex, or silicone with holes for the eyes and other specific areas such as the mouth, lips, and eyes brows. They may also use impersonator's 3D prints, wax heads, or sculptures.

PAD in face recognition

There are several methods for PAD in face recognition: the active and passive methods, plus other hardware methods and AI deep learning.

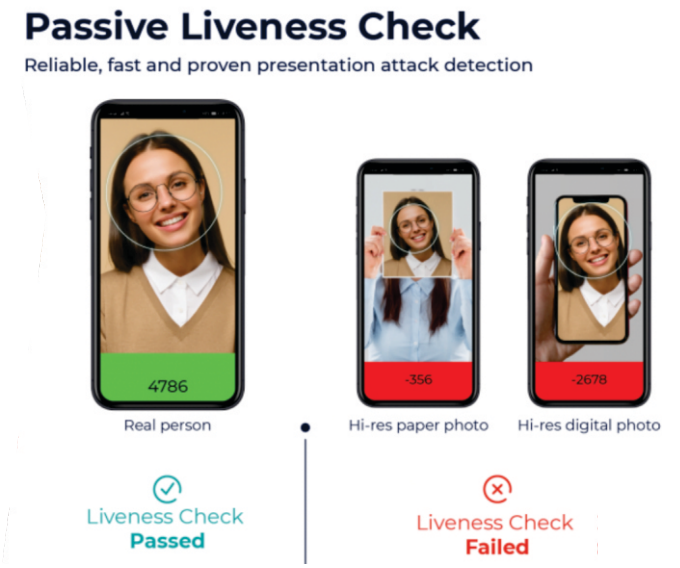
Active Liveness detection:



Active face liveness detection is interactive. The system asks the person in front of the camera to perform a few simple actions. For example, they could be asked to blink, smile, nod, turn their head to the sides, etc. Those actions are randomized for additional security. Only after successfully completing all the steps will the system recognize a person.

Passive Liveness detection method:

Passive liveness detection is non-intrusive. It not only recognizes the individual but also ensures the subject appears in live skin by reading minute characteristics from the face such as tiny motions, temperature, depth, blood flow, etc.



The most advanced 3D camera systems can detect subtle changes in a person's face and search for deep information. This, in conjunction with motion detection or a thermal map of the face, will detect 2D attacks. Furthermore, multimodal biometrics, which combines numerous biometric modalities such as the face, iris, and voice recognition, will increase security and make life difficult for attackers.

Binocular camera (RGB + IR)

It can capture and recognize a face, make accurate identification at some key feature points, including eyes, ears, and nose, and calculate length details such as pupil distance, nose height, distance from eyes to mouth to ears, and so on within 1 mm of error.

3D Depth Camera:

Depth sensors are a form of three-dimensional (3D) range finder, which means they acquire multi-point distance information across a wide Field-of-View (FoV).

Standard distance sensing technologies typically measure distance using one or more sensors with comparatively narrow Fields-of-View. For example, Lidar (light detection and ranging) distance sensors emit a laser or infrared signal with Fields-of-View of up to 2°, which offers accurate information regarding a single distance but limited depth data. The depth sensors must be able to output a matrix of multiple distance readings over a Field-of-View, to obtain an accurate picture with full 3D depth perception.

Deep learning and AI

Machine learning is a promising approach for the improvement of facial recognition and liveness detection. It learns from spoof data and artifacts to identify the spoofs. It can learn to detect glare effects on 2D pictures, the artificiality of movement in video analysis, abnormal cosmetic use on the face, mask, occlusions, etc.

To achieve this, AI uses multiple camera sensors and technologies: including standard imaging (measuring combinations of reds, greens, and blues), multi-spectral imaging (reflectivity of skin versus other materials such as latex or paper), thermal imaging (measuring the heat or infrared signatures of objects), and 3D imaging (measuring depths and contours of a live face versus a 2D spoof).

Performance Evaluation of Biometric Systems

The biometric performance evaluation is based on the different measurements listed below:

- ROC: Receiver Operating Characteristic (ROC) curve examines a model's accuracy and ability to differentiate between authentication cases (i.e., acceptance and rejection). It plots the true acceptance rate to the fake rejection rate. All conceivable threshold values might be examined using ROC to determine the system level.

- FAR: False acceptance rate (FAR) refers to the state when a system incorrectly recognizes an unauthorized user. It is the rate of allowing access to an unauthorized user and labeling them as genuine and authorized. It is determined by dividing the number of false acceptances by the total number of log-in attempts.

FAR =∑ Number of False Acceptance / Number of Attempts

- FRR: When the user is real and should be authorized, but the system considers the user as false and denies access. It is calculated by dividing the number of false rejections by the total number of logged-in attempts.

FRR = ∑ Number of False Rejection / Number of Attempts

The future of anti-spoofing

As companies improve PAD or anti-spoofing techniques, hackers are finding new methods to spoof the system. Developers and researchers are now searching for the possible ways hackers may use fake biometrics. Most of the concerns can resolve with the blend of AI deep learning and super sensor capabilities.

Researchers from the University of Southern California have developed a laser image technique to detect blood flow beneath the skin. Reflected laser light from the illuminated face creates a random interference pattern. The pattern changes from frame to frame because of the blood flow. Using the technique known as laser speckle contrast imaging (LSCI), the blood flow can be detected using a series of LSCI image data. Initially designed for fingerprint scanners, the technique is now applicable to all other sorts of biometrics, including face recognition.

Conclusion:

Biometric liveness detection suppliers are constantly updating technology to suit current and future challenges in biometric identification. In fact, whenever a system identifies a spoof presentation, companies save it in order to train the algorithms. The advantage and limitations of current algorithms are the same: they are good at detecting spoofs, but only those spoofs that they are trained to detect. Hence, companies are concentrating more on feature extraction than classifying spoof attacks. The responsibility of biometric vendors is not over with providing software or an algorithm for PAD unless they give proper certifications to ensure data privacy.

Reference:

- Samruddhi S Kulkarni and Hemprasad Y Pati, Survey on Fingerprint Spoofing, Detection Techniques and Databases, - National Conference on Advances in Computing (NCAC 2015)
- Handbook of Biometric Anti-Spoofing, Springer, 2014
- Dr Wael AbdAlmageed, University of Southern California, Anti-spoofing's state-of-the-art: deep learning meets super sensors - Biometric technology today, July/August 2019.
- Ali Hassani and Hafiz Malik, University of Michigan – Dearborn - Securing facial recognition: the new
- spoofs and solutions - Biometric technology today - May 2021.

+91-79-49068001 sales@mantratec.com www.mantratec.com