Methods Used to Defeat Biometric Security and the Countermeasures Against Them

Teddie Davis
CIS 663 Term Paper
Department of Computer Science
Syracuse University
223 Link Hall, Syracuse, NY 13244
TDavis08@syr.edu

Matthew Brady
CIS 663 Term Paper
Department of Computer Science
Syracuse University
223 Link Hall, Syracuse, NY 13244
MBrady07@syr.edu

Kaiffee Bains
CIS 663 Term Paper
Department of Cyber Security
Syracuse University
223 Link Hall, Syracuse, NY 13244
KBains@syr.edu

Abstract— **With the rise in identity theft, biometric systems based on fingerprints, face, and iris detection are becoming increasingly important in terms of security and access control. By presenting fake attempts, malicious users try to breach these systems. Artificial fingerprints made with gelatin, Play-Doh, and Silicone molds, disguised faces, manipulated facial images, artificial eyes, textured contact lenses, fake images etc. for example could be used by forgers to gain access and commit identity fraud. Spoofing is the term used for these methods. Presentation Attack Detection is the term used for the efforts to stop spoofing attacks. Current methods will be discussed in the following sections as they pertain to Facial Recognition, Fingerprint Recognition and Iris Recognition.**

Keywords—Biometrics, Facial recognition, Fingerprint Recognition, Iris detection, spoofing attacks

I. Introduction

Biometric based authentication systems are being increasingly used in lieu of password based authentication systems. With the rise of biometric-based systems being used to provide security to devices there's also been a rise in the methods used to try to circumvent or thwart those methods.

Use of biometric technology is fast becoming the norm for many of the devices that we use on a daily basis. Being able to unlock your smartphone, your front door or your car with your face, fingerprint or iris is a convenient form of authentication. As with all security devices there will be attempts to break the security that these devices offer.

This paper will focus on the three most popular forms of biometrics, fingerprint recognition, facial recognition, and iris detection. It will provide a brief overview of each of the biometric modalities along with relevant background information. The remainder of the paper will focus on the circumvention aspects for each of the biometrics and the methods employed to counteract those measures.

II. Facial

Biometrics are becoming increasingly more common and starting to be used in our everyday life. Face recognition just happens to be one of those biometrics that is becoming more widely used. "Biometrics based security solutions are widely deployed in various access control applications. In particular, face recognition represents a well-established and widely accepted method, since the reference is easy to capture: a standard camera can be used as a biometric sensor. Further, it can be verified by a human observer in a one to one comparison." [50] One example is being able to unlock your smartphone using your face. One well known example is the Apple iPhone currently has the ability to unlock your phone using your face with a feature Apple calls Face ID. Another example of face recognition used in everyday life is Facebook using face recognition to identify photos that others have posted and asking if you would like to tag yourself [49].

With face recognition being more universally used and available this starts to bring up the concern of just how secure or accurate this type of technology is. This Section will go over Facial recognition, some of the ways that face recognition can circumvent, attacked, or at the very be interfered with and a few of the ways to detect, prevent or lower the risk of circumvention.

"Several distinctive features of the face are utilized in facial recognition technology to perform verification and identification. These features include the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and the eyes ("Face Recognition Technology," 2007)" [11].

Methods to defeat face recognition

"Like many other security systems, biometric systems also have vulnerabilities and face constant circumvention attempts from intruders" [11]. Some of the types of vulnerabilities or attacks on face recognition are presentation attack (a.k.a spoofing) [51], face morphing [50], disguises [56], face swapping, Face image manipulation [52], and expression manipulation [52].

Presentation attack

"Despite the fact that face recognition systems are widely deployed, the vulnerability of these systems with respect to presentation attacks (a.k.a spoofing) greatly impacts the reliability of these systems. Due to the widespread use of social networks, the intruders can easily gain access to high-quality face images of a legitimate user and can exploit those images to get access to face recognition systems. Early studies have indicated the vulnerability of visible spectrum (VIS) face recognition to both low-cost and high-cost Presentation Attack Instruments (PAIs) such as print attacks, display attacks using an electronic screen, photo wrap attacks and 3D masks." [51]

One of the most common vulnerabilities for face recognition is known as presentation attack or more commonly called "spoofing." This type of attack can occur when an attacker presents information to a facial recognition system with the goal of having the system use the presented article to be identified as someone other than the attacker.

Presentation attacks can be in many forms including printing a photo, using an electronic screen, creating 3D masks, and a printed photo wrap attack [51]. "Due to the widespread use of social networks, the intruders can easily gain access to high-quality face images of a legitimate user and can exploit those images to get access to face recognition systems." [51]

Face De-Identification / face swapping

Another potential vulnerability is by attempting to make the face unrecognizable. "Since face technology is both useful and impactful, it also raises many ethical concerns. [48]" Face recognition could lead to the loss of privacy and face replacement may be used by an individual to help prevent this loss of privacy [48]. On the other hand, this same technology may be used by hostile actors, in an attempt to fool face recognition.

"Face swapping, i.e., the replacement of a person's face in an image with another person's face, has been an active research topic for some time [48]". Face swapping isn't limited to only images but is also possible for video as demonstrated by [48].

Face morphing

In [50] face morphing is described as "Morphed face images are artificially generated images, which blend the facial images of two or more different data subjects into one. The resulting morphed image resembles the constituent faces, both in visual and feature representation. If a morphed image is enroled as a probe in a biometric system, the data subjects contributing to the morphed image will be verified against the enroled probe. As a result of this infiltration, which is referred to as morphed face attack, the unambiguous assignment of data subjects is not warranted, i.e. the unique link between subject and probe is annulled." [50] Morphed faces are created by "... landmarks in both faces are detected and moved towards each other. For a morphed face image, representing both faces in equal parts, the landmarks of the morphed face image are typically the mean of the features of both constituent original facial images" [50]

(a) Subject 1 (b) Morph Subj. 1 + 2 (c) Subject 2

At first one might wonder what kind of benefit or scenario an individual would have a need or desire to use face morphing. With the use of biometrics also in place at automatic border crossing that use biometrics passports (ePass) one might start to find scenarios that face morphing could be used. "The key deficiency in the passport issuance process lies in the way the facial picture of an applicant is processed. In many countries, the applicant provides a printed facial image which is scanned and then digitally transferred to the passport production site..." [50]. Since many countries allow individuals to bring printed facial images over having the individual take a new facial image at the time of enrollment this leaves a possible vulnerability that modification of the printed image could occur. This vulnerability allows for bad actors to exploit the vulnerability by using an artificial face image that has been blended with two or more different images into one [50]. "If the newly generated facial image is enroled to a Face Recognition System (FRS), the subjects contributing to the morphed image are positively verified against the morphed face attack reference [1], as the resulting morphed image resembles the constituent faces, both in visual and feature representation. "[50]. In [50] continue to explain that by "Exploiting this fact, a black-listed subject (criminal) is able to obtain a legitimate ePass, by morphing his facial image with that of a non-listed subject (accomplice), which the accomplice utilizes to apply for a passport. Due to the infiltration during the issuance process, the accomplice, as well as the criminal, are able to verify successfully against the reference stored in the ePass [1]. The feasibility of such morphed face attacks has been empirically confirmed in [3] and [1], [2]" [50].

With the advancement in technology also brings advancement to the face morphing called deep-morph. In the paper by Pavel Korshunov and Sébastien Marcel states "The main difference from more traditional morphing techniques is that deep-morph can seamlessly mimic facial expression of the target person and, therefore, can also be successfully used to generate convincing fake videos of people talking and moving about" [58]. With the higher quality that deep-morphing can achieve had them question how vulnerable face recognition systems are to this type of attack [58]. They went on to perform tests using a dataset made up of deepfake videos that contained morphed faces created by GAN-based algorithm [58]. The went on to find "... that the state of the art face recognition systems based on VGG and Facenet neural networks are vulnerable to the deep morph videos, with 85.62% and 95.00% false acceptance rates, respectively, which means methods for detecting these videos are necessary." [58]

De-identification in video

A relatively new advancement is the deidentification of faces in live videos. The research in [48] said to be one of the first examples of being able to de-identify in live video with minimally changing the image measured using low- and mid-level features and not pixels themselves. This is accomplished "By concatenating the autoencoder's latent space with the face-classifier representation layer, we achieve a rich latent space, embedding both identity and expression information. The network is trained in a counter-factual way, i.e., the output differs from the input in key aspects, as dictated by the conditioning. The generation task is, therefore, highly semantic, and the loss required to capture its success cannot be a conventional reconstruction loss." [48]

Disguised faces

This type of potential vulnerability is when an individual tries to mask their appearance in the form of a disguise, types of disguises include but not limited to wearing a hat, sunglasses, scarf, and with the unfortunate rise of COVID19 wearing a face mask whether intentional or unintentional can lower accuracy of face recognition [56]. Performance in face recognition is also degraded with a large variety of other physical rations like wearing a wig, changing the hairstyle, hair color, removing or growing a beard [55]

Face image manipulation (FIM)

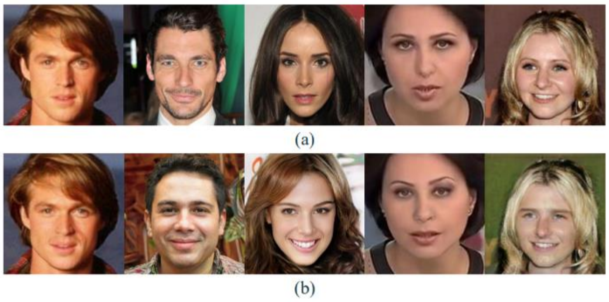
"Face images contain rich and intuitive personal identity information, which make them be commonly used for biometric authentication such as identifying individuals. However, face images also have vulnerability and weak privacy, which makes them easy to be forged. Especially over the last three years, tremendous progresses such as DeepFake, generative models (Goodfellow et al., 2014; Kingma and Dhariwal, 2018; Kingma et al., 2016) and computer graphics (CG) based methods (Thies et al., 2016) have made facial image manipulations (FIM) reach a photo-realistic level. This opens the door to a variety of face image applications such as interactive game, movie industry and photography. Nevertheless, FIM might be intentionally used for malicious purposes" [52].

Face image manipulation are commonly split into three categories identity manipulation, expression manipulation and attribute transfer [52]. "Identity manipulation refers to generating fake face images of entirely imaginary people (Huang et al., 2018), or replacing one face with the other one via FaceSwap (Korshunova et al., 2017) or DeepFake (Korshunov and Marcel, 2018). Expression manipulation refers to generating face images with specific expressions (Kingma and Dhariwal, 2018), or transferring facial expression from the source actor to the target face (Thies et al., 2016)." [52]. Attribute transfer for faces refers to changing attributes about the face some of the attributes are hair color, age gender, facial hair, so on [52].

Face image manipulation is not limited to only expression or attributes, with the advancement from works like PGGAN and StyleGAN that can create hyper realistic fake face images [52].

Example of StyleGAN "Picture: These people are not real – they where produced by our generator that allows control over different aspects of image." From [54]

"Recent expression manipulation techniques also generate fake face images without leaving any perceptible artifacts. Several generative models including GANimation (Pumarola et al., 2018) and Glow (Kingma and Dhariwal, 2018) were proposed for expression manipulation with photo-realistic effects. Face2Face, which is a well-known Computer Graphics (CG)-based method, animates well the facial expression of the target video from a source actor (Thies et al., 2016). For face attribute transfer, there also exist some generative models such as StarGAN (Choi et al., 2018), and CycleGAN (Zhu et al., 2017) which change facial attributes." [52].



"Can you identify which face image is fake? (a) Real face images with different resolutions. (b) From left to right, fake face images generated by Glow, StyleGAN, PGGAN, Face2Face, StarGAN, respectively" [52]

As social media grows the concern for privacy also is growing. "We need tools to protect ourselves from potential misuses of unauthorized facial recognition systems." [59]. As stated in [59], they prosed creating a software tool "Fawkes" with the goal to help protect images against being used in facial recognition systems without being authorized [59]. At the time of publication of this paper it was stated that Fawkes would "work under a wide range of assumptions and provide 100% protection against widely used, state-of-the-art models deployed by Microsoft, Amazon and Face++" [59], but also noted that the current technique used my be overcome by workarounds in the future [59]. The cloaking software is available for download from https://sandlab.cs.uchicago.edu/fawkes/ web site.

Countermeasures

To help mitigate the attacks on face recognition systems several Presentation Attack Detections (PAD) algorithms have been developed, such as Local Binary Patterns (LBP), Binarized Statistical Image Features (BSIF), Difference of Gaussian (DoG), and gray level Co-Occurrence Matrix [51].

Presentation attack detection (PAD) parried with multi-spectral capture devices has shown promising [51]. "Since the PAIs used to attack the face recognition systems are typically made of materials with non-skin texture (plastics, electronic screen, glossy papers, rexine, silicon, rubber or latex), the use of NIR spectrum can provide a clue regarding the presence of a PAI [Presentation Attack Instruments]" [51].

In [57] they evaluated how vulnerable face recognition systems are to 3D silicone face masks on systems using presentation attack detection (PAD) algorithms. largely focused on differentiation texture information. The "experiments indicate that the two commercial FRS are vulnerable to PAs based on custom 3D silicone face masks, especially when operating threshold corresponds to higher values of FAR. When the threshold is set at the lower values of FAR (e.g., FAR = 0.01%), both commercial FRS are not vulnerable to the custom silicone mask PAs." [57]. It was also noted that in the experiments the results indicated that Local Binary Patterns (LBP) support-vector machine (SVM) (LBP-SVM) classifiers had excellent detention accuracy against 3D face masks [57].

III. FINGERPRINT

Introduction:

One of the main difficulties that biometric systems face is the potential of malicious operations today. To overcome biometric systems, the majority of hostile actors use a common sort of presentation attack known as "spoofing" [2]. The primary purpose of a presentation assault is to impersonate target victims with the appropriate authorization. It occurs when intermediary spoofing forgers purposefully guess the identity of unsuspecting persons by stealing their fingerprints and modifying them with lawful content in order to mislead fingerprint recognition systems [3].

While biometrics may improve security, biometric solutions are not without flaws. Attacks on the biometric sensor level, replay attacks on the data communication stream, and database attacks are only a few of the system vulnerabilities.

As cited in [4], Inability to control personal information from fingerprint spoofing forgeries on devices [5] one could jeopardize video surveillance [6], biometric identification [7], and social media face indexing [8]. Researchers are applying countermeasure techniques and merging them into biometric-based systems to tackle counterfeiting. Figure 1 shows some fingerprints taken from real and fictitious fingers. Visually, the eyes are unable to distinguish between actual and fake objects.

The genuine fingerprints are shown in the first row of Fig. 1. The false ones in the second row were obtained using artificial fingers created from various fabrication materials. There have been numerous spoof fingerprint detection systems developed [9], [10], [11]. As a result, misrepresenting fingerprints and detecting faked fingerprints is still a work in progress [12].

There have been a number of countermeasure strategies proposed [13] that use many elements to secure information. Spoof forgeries [14], [15] are techniques that are used to fool biometric-based systems by providing a counterfeit user identity for authentication. Face recognition, iris features, voice signals, fingerprints, and palm veins [16] are among the behavioral and biological features considered by the authentication system. Finger molds are used by the intermediate spoof forger in fingerprint spoofing forgeries to trick the biometric authentication system. Palm graphics, for example, have been produced and easily defeat the biometric system [17].

Spoofing Background:

Before delving farther into spoofing, it's worth considering how the false accept ratio, a common biometric device assessment parameter, relates to spoofing. When a provided sample is wrongly matched to a template enrolled by another user, it is called a false accept.

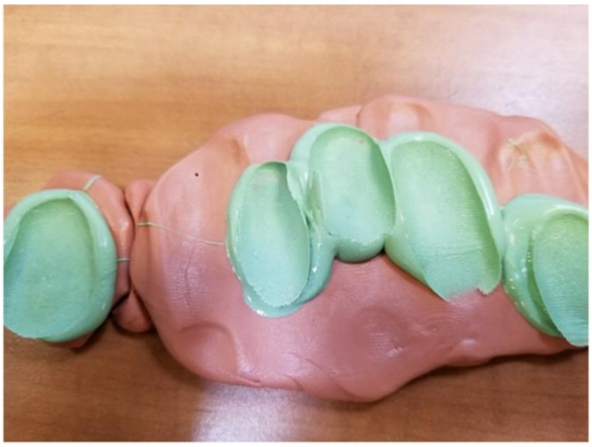


Fig 2: 3D Mould made from Dental Mould

This solely relates to a zero-effort attempt, which is when an illegal user tries to obtain access to a system using their own biometric. If the false accept ratio is kept low, there is a very low chance that a given user with criminal intent will match another template. The false accept ratio does not provide information about a system's vulnerability to spoofing attacks.

As a result, depending on whether or not additional sensors are employed, fingerprint spoofing detection systems are divided into two categories:

1) Hardware-based (experimenting with additional finger readers): modern fingerprint readers can scan input fingerprints at high resolutions adequate for matching. Misrepresentation detection is performed by the fingerprint reader on two sorts of finger images: non-processed and raw fingerprint images [16]. While these raw photos contain clear information that can be used to detect spoofs, they must be processed in order to extract features for matching, such as color conversion, normalization, or filtering. The fundamental goal of hardware-based approaches is to show liveness characteristics such as blood flow [18], [19], skin distortion [20], and odor [14].

2) Software-based approaches classify images into live and fake fingers based on visual information scanned by an intent sensor without requiring additional hardware [21]. The software-based methods have the advantage of being able to be modified in ordinary fingerprint scanners to recognize and analyze if a fingerprint is forged by utilizing bogus materials in the fingerprint image. The software-based strategy is examined in the research to recognize fingerprints under spoof materials.

The two primary groups of software approaches [22] are feature-based [23] and deep learning-based. In its early stages, the feature-based recognition technique primarily extracts , and it has not demonstrated good performance for a variety of false materials. Deep learning approaches are utilized to learn phony fingerprints for many sorts of spoof materials , as can be seen [24].

Research Related:

The spoofing vulnerabilities of biometric devices have been highlighted in two recent high-profile cases. Other spoofing-related articles include and. The first is a team from Japan's Yokohama National University. Matsumoto and his colleagues devised a technique for spoofing fingerprint scanners. To make a mold in this way, two separate procedures were used. The initial experiment employed a subject's finger to make a mold out of free molding plastic.

Making a cast from a latent fingerprint picture was the second step.

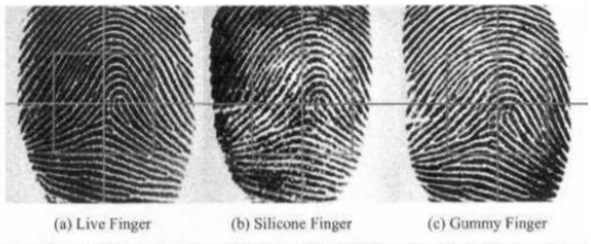

(a) Live Finger (b) Silicone Finger (c) Gummy Finger

Fig 3: Images from spoofing tests performed in Matsumoto’s laboratory

The latent fingerprint was augmented using cyanoacrylate adhesive, photographed with a digital camera, then the image was enhanced and flipped using software.

The image was then printed as a mask onto a transparency sheet using an inkjet printer. The photosensitive-coated PCB was utilized to produce the cast with the mask. Finally, gelatin, a popular confectionary ingredient, was utilized to make fake fingers from the casts. These prosthetic fingers are referred to as "gummy fingers" by the author.

The direct approach was used to make gummy fingers from five people, while the latent method was used to make gummy fingers from one person. Eleven typical biometric fingerprint devices, including both optical and capacitive methods, were examined. Devices were set to the highest security level when security levels were available. Several tests were carried out, including:

-enrolling a live finger and verifying with a live finger

-enrolling a live finger and verifying with a gummy finger

-enrolling a gummy finger and verifying with a live finger

-enrolling a gummy finger and verifying with a gummy finger

-enrolling a gummy finger and verifying with a gummy finger

-enrolling a gummy finger and verifying with

It is cited in [25]

Impact on Biometric Devices:

Because fingerprints may be easily created using various sorts of equipment, such as wood glue, gelatin, silicone, or printed fingerprints, the duty of observing phony fingerprints has grown increasingly important in recent years. The texture of a real finger may leave a lasting impression on the surface, which is subsequently copied into the material to imitate any biometric authentication method. Because actual and fraudulent fingerprints have the same roughness, this issue can readily fool authentication fingerprints-based systems.

Paper (Presentation attack detection methods for fingerprint recognition systems: a survey by C Sousedik, C Busch - Iet Biometrics, 2014 - ieeexplore.ieee.org) looked at a variety of fingerprint spoofing materials. In reality, the forger attempts to circumvent a fingerprint identification sensor by duplicating a specific fingerprint image. An artifact exists in the cloned fingerprint that is used to perform a presentation attack.

The key research issue is to distinguish real living fingerprints from false ones, which is based on the ISO standard IEC 30107-3. (E). It lays the groundwork for presentation attack detection by offering a uniform framework for defining and detecting presentation assault events. To generate and replicate a fingerprint, two well-known procedures are used:

1) Cooperative methods: the user's finger must be inserted into a stretchy material. These materials, such as silicone, gelatine, or PlayDoh, aid in the creation of a fingerprint mold.

2) Non-cooperative method: it is used when a user leaves a fingerprint trace on a surface by accident, and it is necessary to improve these traces. This can be accomplished by capturing fingerprint traces and saving them as a picture. The fingerprint image is improved, and then silicone, gelatine, or PlayDoh molds are made over the printed image. Researchers at Michigan State University, for example, assisted police in unlocking a fingerprint-secured smart phone with a homicide case1 in July 2016 using a 2D printed fingerprint spoof approach provided by paper (K. Cao, A.K. Jain, Hacking mobile phones using 2D printed fingerprints. Technical Report. MSU-CSE-16-2, 2016).

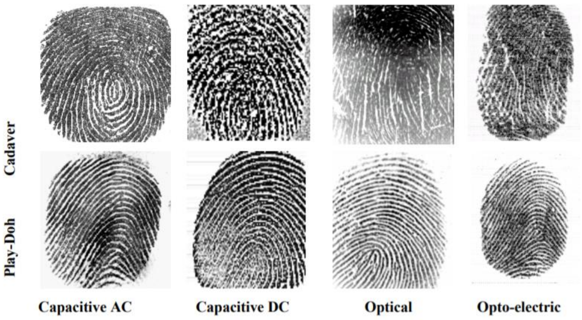


Fig 4: Images of spoof fingerprints made from Play-Doh and of cadaver fingerprints for a variety of fingerprint scanner technologies.

In forged fingerprints, various materials can expose such traits as gradients, ridges, and intensity. As a result, the effectiveness of existing anti-spoof fingerprint identification systems is highly dependent on the sort of synthetic materials employed in the training process to make fake fingerprints. Learning temporal features using LSTM-CNN architecture for face anti-spoofing- Proceedings of the 3rd IAPR Asian Conference on Pattern Recognition (ACPR), IEEE (2015), for example, said that single low-level feature-based approaches struggle to deal with a variety of spoofing fingerprint materials. The core of distinguishing counterfeit fingerprints for various types is based on features in fingerprint photographs.

When the sole of the authentication system does not know what sorts of materials were used for forging, several aspects become a feasible technique to define the attributes of counterfeit fingerprints and actual ones. For example, R.K. Dubey, J. Goh, V.L. Thing-Fingerprint liveness detection from single image using low-level features and shape analysis IEEE Trans. Inf. Forensics Secur., 11 (7) (2016), pp. 1461-1475 has merged several features: Local interest points were discovered by the SURF approach using 1-gradient features from the input image. The Histograms of Oriented Gradient have 2-pyramid multiscale properties. Gabor's texture is three-dimensional. The dynamic score level fusion approach is used to determine if the fingerprint is false or authentic after combining the three elements. Their technique was tested on the LivDet 2011 dataset and found to have a 3.95 percent Average Equal Error Rate and a 2.27 percent Average Classification Error Rate.

For revealing liveness fingerprints, Rattani and Ross [26] suggested a fingerprint spoof detector that combines numerous features: Grey Level Co-occurrence Matrix (GLCM) and Histogram of Oriented Gradients (HOG).

Using intensity variance characteristics and local binary gradient orientation, Xia et al. [27] developed a fingerprint recognition algorithm. The co-occurrence probability approach is used to aggregate these features into a feature vector, which is then categorized by support vector machine (SVM) classifiers.

Two common methods for identifying a spoof fingerprint have been reported in fingerprint spoofing recognition systems: 1) Active liveness aspects of fingerprint detectors, such as examining pulse, perspiration patterns, and blood pressure [28]; 2) Passive pattern analyzer for synthesizing materials [29], such as the absence of details in faked fingerprints compared to real ones, and fingerprint pattern differences The scope of our proposed method detects a threat of employing material and sensor in the last sort of spoofing problem.

[30] provides a number of papers on fingerprint recognition spoofing methods. Statistical feature analysis [31], Ridge based features [32], curvelet transform [33], Power Spectrum Fourier based features [34], Local Phase Quantization patterns [31], and Local Binary Patterns [35] are among the most general approaches for static extracted features.

Recent techniques, on the other hand, have concentrated on merging numerous features, possibly even multiple liveness detectors. For example, for anti-spoofing capabilities, [36] suggests combining a liveness detector with a single modality. To determine the liveness of spoof fingerprints, Galbally et al. [37] used numerous criteria such as orientation confidence level and local clarity score.

One author proposed a deep learning method for recognizing actual fingerprints and detecting spoofs in this paper. The following are the primary contributions of our method:

1) It tries to tell the difference between actual and fraudulent fingerprint photos.

2) It uses scaled and rotated ROIs to assess image consistency. We present a deep discriminative model for training detection based on these ROI features.

Proposed Methods:

As previously mentioned, there are a variety of anti-spoofing strategies that can be utilized to make spoofing a system more difficult. The use of passwords or smart cards, the enrollment of multiple samples, and the supervision of the verification process are all self-explanatory.

The usage of multi-modal biometric systems is another way for anti-spoofing. Multimodal biometrics is the mixing of multiple biometric types into a single biometric system, such as fingerprint and facial recognition. Many studies are being conducted in this field to discover the optimum strategy to merge data from many biometric systems, whether at the feature extraction level or at the decision-making level. Multi-modal biometrics are more difficult to spoof from an anti-spoofing standpoint because they require both a spoof fingerprint and a high-quality facial image or video, for example.

Finally, a mechanism known as liveness detection can be used to prevent spoofing. Even though biometric technologies use physiologic data for identification and verification, these readings rarely reveal whether or not someone is alive. The purpose of liveness testing is to see if the biometric being taken is from an authorized, live individual who is present at the moment of the collection. Liveness detection is based on the recognition of physiological data as indications of life (1) from the biometrics' inherent liveness information, (2) from extra processing of data already acquired by the biometric reader, and (3) from the acquisition of life signals using additional hardware. Furthermore, the challenge/response might be included in the liveness detection process. In this situation, the user will notice, hear, or feel something and respond accordingly.

Finally, challenge response can be utilized to prevent spoofing. Tactile response to heat or shock, change in expression (smile, frown) (Identix), and repetition of a randomly produced collection of sentences are all instances in this scenario (VeriVoice). Involuntary challenge responses include shock reflexes, pupil changes in reaction to light levels, and muscular responses to electrical stimulation. Obviously, approaches that include shocks are unlikely to be user-friendly. Furthermore, the presence of a person, not necessarily the authorized person, may be indicated by a challenge answer. The biometric data should be carefully linked with the liveness data such that they are inseparable.

Conclusion

Fingerprint security is better than ever, and you can trust it as much as you do passwords, yet we live in a world where even the strongest security measures can fail.

If we were asked for passwords or PINs, we would have given the same answer. Every authentication technique has its own set of benefits and drawbacks. Unfortunately, we have yet to discover something that is both secure and feasible.

In conclusion, while biometric authentication devices are vulnerable to spoof attacks, anti-spoofing solutions may be developed and implemented to considerably increase the difficulty of such attacks. Addition of supervision, password, smart card, enrolment of numerous biometric samples, multi-modal biometrics, and liveness testing are all anti-spoofing measures. Before choosing security methods that will meet the goals, applications must be thoroughly reviewed. While liveness algorithms exist, additional research is needed to determine their effectiveness and impact on the overall biometric system. Finally, no matter what security measures are in place, no one can guarantee that no one will be harmed.

IV. IRIS

The iris is a fascinating and unique organ that is well-suited to the process of biometric identification. In this section we will explore the aspects of the iris that make it suitable for biometric recognition as well as the portions of the eye that are either currently being used as a countermeasure to attacks or have the potential to be used as a countermeasure to an attack.

The Iris as a Biometric

The iris is a small sphincter shaped muscle located in the center of the eye.

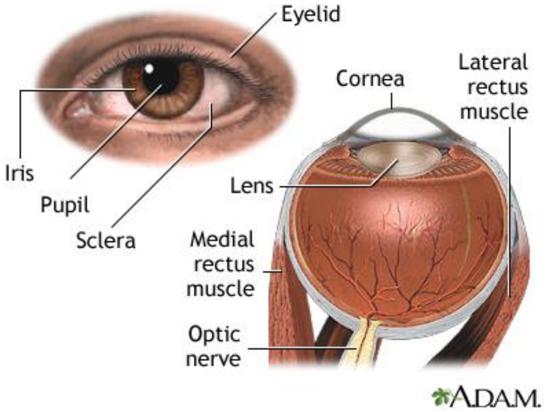


Image from MedlinePlus [64]

The Iris contains the melanin which provides for the color of the eye. The amount of light that enters the eye is controlled by the iris which contracts or expands as needed [69]. The pupil is the colorless section in the center of the iris, it is the opening in which light passes through to the retina. In an environment with bright light, it contracts and in low light situations it expands. The size of the pupil is controlled by the iris [69]. The Cornea is a layer of tissue that covers the iris and pupil, it is transparent and bends light that enters the eye [69].

The iris contains the patterns that make iris recognition possible. “Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles, and a zigzag collarette” [60].

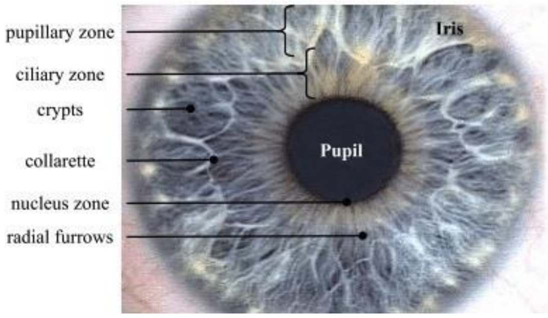


Image from A New Method for Radial Furrow Extraction in Iris Biometric [65].

“Although small (11 mm) and sometimes problem-atic to image, the iris has the great mathematical advantage that its pattern variability among different persons is enormous.” [60] As you can see in the image above the various features of the iris has the potential to create a multitude of different patterns. According to research by Daugman it the variability makes it suitable for a biometric [60]. It has a high degree of potential variability Daugman notes “The combinatorial complexity of this phase information across different persons spans about 249 degrees of freedom and generates a discrimination entropy of about 3.2 b mm2 over the iris” Additionally it forms in the 3rd month of gestation and is its pattern is typically completed in the 8th month, since it is considered to be an internal organ it is well protected but visible, its pattern stays stable over time [60]. Additionally using the iris as a biometric can be done without physical contact with a device since cameras are utilized to obtain the images of the iris [60].

Types of Attacks

Zero Effort Attack

The most basic type of attack is called a Zero Effort Attack. In a zero effort attack the attacker presents their own iris to perform an attack. The attacker has no information about any user in the system nor do they attempt to gain any type of knowledge [61]. The goal of this attack is to match an existing pattern in the database closely enough to take advantage of the false match rate (FMR) inherent in the system. In this type of attack the chances of success are low [61]. “Most iris recognition systems present very low false acceptance rates. The success rate of these attacks can be considered low.” [61]

Photo Attack

With the advent of photo sharing sites and high-definition cameras attackers can often download images from the Internet from places such as Instagram, Facebook etc. they can use images taken directly from news sites, YouTube or anywhere that high-definition images or video are available as well. [61] “Extracting iris is becoming increasingly possible with the advent of digital imaging and social image sharing. Iris patterns can be obtained from high-resolution face images and, the printing of high-quality iris photographs using commercial cameras and ink printers is fairly simple.” [72]

These images are then taken and are printed using a high-quality photo printer or commercial LaserJet printer. “Second, it is relatively easy to print high-quality iris photographs using commercial cameras (up to 12 Megapixels sensors in most of the nowadays smartphones) and ink printers (1200 dpi in most of the commercial ink printers).” [61]

In this attack vector a simple paper printout of an eye is created to be presented to a sensor. While it is a less sophisticated attack methodology there are several studies that have shown this to be an effective method [73]. “Printouts can be produced in many ways. There is no consensus on whether color or black-and-white printing is significantly better, or whether matte or glossy paper is better, to make a successful Presentation Attack instrument.” [73] In this type of attack the attacker obtains a picture of an iris that they would like to present to the sensor. This can be obtained through high resolution images found on photo sharing sites or acquired through high resolution cameras in the open. The vulnerability that is being exploited relies on the fact that the iris is considered a planar surface as indicated in Daugman’s work [60]. During the acquisition process a Near Infrared (NIR) camera is typically used which produces a monochromatic (black and white) image [60]. This image then goes through a process that brings it to single pixel precision in order to determine the lines that will make up the pattern that will be matched [60]. Once a printed image is capture by an iris recognition device it will go through the same thinning process to produce a template to be matched against. Several studies employing this methodology have met with varying success. In one particularly interesting study researchers found that if they cut a hole in the printout where the pupil was located and placed the image over a human eye, they had a very high success rate [73]. “However, it is typically easier to get commercial sensors to generate a sample from such an artifact when a hole is cut in the place where the pupil is printed, in order to produce specular reflections from an authentic cornea hidden behind the printout when taking a picture…" [73] In this study the ability to fool the live iris detection system that was in place was notable in that anyone with the printout could place it over their eye in order to fool the system. Additionally, this would indicate that this methodology could be employed in the enrollment process whereby you could create a false iris pattern that could be enrolled in a system in order to create multiple identities [73]. There could be numerous benefits to a malicious actor who could exploit this vulnerability.

Display screens as an attack vector

In a video or photo attack and attacker can use either a high-definition photo or video from a high-definition display. "The attack is performed displaying a printed photo, digital image or video from the spoofed iris directly to the sensor of the IRS." [61]

There are several studies that have been performed the show video screens can be an effective method used to circumvent iris detection methods. However, these Studies focused mainly on consumer devices. When attempts were made against commercial systems, they more often than not failed. "In particular, iris recogni- tion methods proposed in academic papers for visible-light iris images, if implemented in practice, would have to use visible-light acquisition devices that would photograph iris images displayed on regular LCD screens, as demonstrated in various papers" [73]. "This, however, cannot be generalized to commercial iris sensors, as they use near-infrared light to illuminate the iris as recommended by ISO/IEC 29794-6. The sensors may additionally cut the light outside of the 700–900 nm range by applying near-infrared filters." [73]. By applying near infrared filters the device effectively sees nothing. Since the image is not being displayed in the 700 to 900 mm range the camera cannot detect it. This effectively thwarts the attempt [73].

Textured contact lenses as an attack vector

A textured contact lens is a contact lens that has been manufactured to appear to have a texture printed or etched into their surface. Much like a colored contact lens that can change the appearance of a person eye color a textured contact lens changes the visible texture of an individual iris [61]. This attack requires a high level of sophistication. "In comparison with photo or video attacks, the generation of textured contact lenses requires a more sophisticated method based on optometrist devices and protocols." [61] This is a much more sophisticated attack method where a number of hurdles need to be overcome. "The basic problem is that the texture in the contact lens partially overlays the natural iris texture, and hence the image of an iris wearing a textured contact is a mix of contact lens texture and natural iris texture." [73] Another hurdle is that contact lenses move around on the eye so even if a pattern was created to match another eye the ability to correctly align the contact for subsequent usages makes it nearly impossible to align for future attempts. "Additionally, the contact lens moves on the surface of the eye, so that the exact mixture is different from image to image." [73] While there are some possible applications for the textured contact lens approach, at this point in time, it is most likely a better iris detection avoidance methodology in practice given its ability to mask the underlying iris pattern and not being reproducible in any reliable way. This feature would make it ideal for continued usage for recognition avoidance since the probability of being identifiable at a later date is very low [73].

Prosthetic Eyes as an attack vector

Prosthetic eyes, also known as glass eyes, can be very lifelike in appearance. They have been in use for many years as a method for individuals who have either lost an eye or never developed an eye to have a way to appear to have an eye to blend into society better. They're typically created by Ocularists who spend a considerable amount of time making them as lifelike as possible. With an experienced ocularist a very lifelike replica can be produced [73]. "The resulting product is typically so good that even near-infrared images, acquired by commercial sensors, resemble near-infrared samples of living, healthy eyes." [73] In Laboratory settings this method of attack has been achievable. In a study performed in 2010 researchers were able to fool a system using a glass eye with a contact lens [67]. "Subsequent tests using a glass eye with a contact lens and blacked-out pupil demonstrated that the removal of visible artefacts in the pupil region, due to misalignment or other factors, did lead to successful spoofs." [67]

Avoidance

Avoidance is not an outright attack on an iris recognition system, but it is an attempt at avoiding detect. In this type of scenario an individual does not want the iris detection system to ascertain their identity. In some cases, textured contact lenses can be used [61]. In other cases, drugs can be applied to eyes in order to dial ate the pupil [66]. In a study done by the UAE Border patrol they found cases where individuals used eye drops to dilate their pupils to a size where the iris scanners could no longer read them thereby allowing people to move past border security without being detected. "There were also those cases where some people used eye-drops to bypass the system. The eye-drops were found to cause a temporary dilation of the pupil, meaning that the use of this substance will lead to a false reject; the person is not found in the database when he is supposed to be found. In abnormal cases of dilation using some of the identified eye-drops, the ratio of the pupil radius to the iris radius exceeded 60%" [66] In response to the finding the UAE implemented a countermeasure to ensure that the system would examine the iris size and flag iris's that exceeded a preset threshold. "The system was enhanced to reject any acquisition of irises where the ratio of pupil to iris is greater than 60% and show the ratio percentage on the screen for the operator." [66] This allowed the operator of the scanning device the opportunity to do a manual check of the individual [66].

Presentation Attack Detection

Eye Liveness Detection Challenge Response Approaches

When determining eye liveness challenge responses are often utilized. In the challenge response approaches, there are two different types of responses that can be measured, voluntary and involuntary. "These methods analyze voluntary and involuntary responses of the human eye. The involuntary responses are part of the processes associated to the neuromotor activities of the eye while the voluntary behavior is response to specific challenges." [61]

Voluntary Challenge Response

Voluntary challenge response tests are more straightforward than involuntary response tests. In a voluntary challenge response scenario, a user may be asked to look in a certain direction, blink on command etc. These movements are then measured to determine if an actual person was being observed [61].

Involuntary Challenge Response

There are several different involuntary challenge response tests that can be employed to determine if the scanner is scanning an actual eye. The first method utilizes the fact that the iris has predictable and measurable involuntary responses such as the contraction and dilation of the pupil in response to varying light conditions. In this type of detection method, a bright light is directed at the iris and the contractions of the iris are measured to determine if there is in fact an actual person being measured rather than an inanimate object [61]. Since a bright light will be presented to a pupil which will cause a nonvoluntary movement within the pupil causing it to shrink when light is present and causing it to expand when the light source is removed there may be a concern that the liveness test will interfere with the iris scan however this test does not typically cause an issue with the pattern matching algorithm, according to Daugman iris dilation has no impact on the ability to map the iris “Since the radial coordinate ranges from the iris inner boundary to its outer boundary as a unit interval, it inherently corrects for the elastic pattern deformation in the iris when the pupil changes in size.” [60]

There are also several types of involuntary eye oscillation movements of the pupil that can be measured called hippus and microsaccades [61] “...hippus are permanent oscillations of the pupil that are visible even with uniform illumination. These oscillations range from 0.3 to 0.7 Hz and decline with age.” [61] Hippus measurements can be difficult to obtain due to lighting and head movement [61]. While hippus movements are oscillations of the pupil Microsaccades are classified as small, measurable, rapid shifts in eye movement [70]. These eye movements are most often horizontal or vertical, horizontal being more common in humans [70]. These movements can be observed by the iris recognition system and utilized to determine if a live iris has been presented [61].

Light Reflection Methodologies

Purkinje reflections are a way to use reflected light to determine if a real iris is being measured [71]. “In a natural eye, four optical surfaces reflect light: the front and back surfaces of the cornea as well as the front and back surfaces of the lens... These reflections are also referred to as Purkinje reflections or images, named after a Czech physiologist.” [71] Purkinje reflections can be measured by changing the direction of a light source to measure the direction of the reflection. By using this method, a determination of whether or not an eye is real or not can be made [71].

Additional Work

Iris detection in real world applications using commercial scanners is a highly secure method for determining an individual’s identity. In instances where speed, accuracy and overall security are required iris recognition is a viable option. In the future additional research around the non-voluntary movements of the eye coupled with additional software approaches that would reduce the cost associated with iris detection would be a worthwhile direction to pursue.

V. Conclusion

Biometric security appears to be very secure, in fact in many cases it provides better security than passwords and PIN numbers. While every authentication technique has its own set of benefits and drawbacks, they can typically be trusted to provide a secure method for identification.

As the world moves to more fully embrace biometrics as a means of authentication the efforts to circumvent those systems will increase. While biometric authentication devices are vulnerable to spoof attacks the ability to maintain a secure environment will leads to an increased effort in the anti-spoofing methodologies that are employed today and that are currently on the horizon.

Going forward additional research is needed to ensure that these methodologies are able to identify and provide countermeasures to current and future attack methodologies.

References

[1] e. a. L. Ghiani, "Livdet 2013 fingerprint liveness detection competition 2013".

[2] A. R. E. Marasco, "A survey on antispoofing schemes for fingerprint recognition systems," ACM Computing SurveysVolume 47Issue 2, January 2015.

[3] R. M. Jomaa, M. S. Islam and H. Mathkour, "Improved sequential fusion of heart-signal and fingerprint for anti-spoofing," 2018.

[4] D. M. A.Jalabb, "Anti-spoofing method for fingerprint recognition using patch based deep learning machine".

[5] ChrisRoberts, "Biometric attack vectors and defences".

[6] K. Bowyer, "Face recognition technology: security versus privacy".

[7] D. a. C. G. a. P. A. a. S. W. R. a. P. H. a. F. A. X. a. R. A. Menotti, "Deep representations for iris, face, and fingerprint spoofing detection".

[8] e. a. M. Sajjad, "CNN-based anti-spoofing two-tier multi-factor authentication system".

[9] e. a. Q. Huang, "An evaluation of fake fingerprint databases utilizing SVM classification".

[10] K. C. A. J. T. Chugh, "Fingerprint spoof detection using minutiae-based local patches".

[11] J. G. V. T. R.K. Dubey, "Fingerprint liveness detection from single image using low-level features and shape analysis".

[12] e. a. C. Wang, "A DCNN based fingerprint liveness detection algorithm with voting strategy".

[13] e. a. Y. Gao, "Intermediate spoofing strategies and countermeasures".

[14] e. a. D. Baldisserra, "Fake fingerprint detection by odor analysis".

[15] e. a. Z. Akhtar, "Evaluation of serial and parallel multibiometric systems under spoofing attacks".

[16] K. C. A. J. J.J. Engelsma, "Raspireader: open source fingerprint reader".

[17] e. a. J.-G. Wang, "Person recognition by fusing palmprint and palm vein images based on “Laplacianpalm” representation".

[18] C. C. P. M. M. Espinoza, "Vulnerabilities of fingerprint reader to fake fingerprints attacks".

[19] W. F. R. N. M. Drahanský, "Liveness detection based on fine movements of the fingertip surface, 2006, IEEE Information Assurance Workshop, 2006.".

[20] e. a. C.J. Lennard, "Fingerprints and Other Ridge Skin Impressions".

[21] e. a. L. Ghiani, "Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015".

[22] D. Yambay, "Review of fingerprint presentation attack detection competitions".

[23] U. J. E. L. Y. Park, "Statistical anti-spoofing method for fingerprint recognition".

[24] e. a. J.B. Kho, "An incremental learning method for spoof fingerprint detection".

[25] P. Stephanie A. C. Schuckers, "Spoofing and Anti-Spoofing Measures".

[26] A. R. a. A. Ross, "Automatic adaptation of fingerprint liveness detector to new spoof materials".

[27] Z. e. a. Xia, "A novel weber local binary descriptor for fingerprint liveness detection, In IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018.".

[28] e. a. P.D. Lapsley, "Anti-fraud biometric scanner that accurately detects blood flow. 1998, Google Patents.".

[29] X. L. Y. Jiang, "Spoof fingerprint detection based on co-occurrence matrix".

[30] e. a. D. Menotti, "Deep representations for iris, face, and fingerprint spoofing detection".

[31] G. M. F. R. L. Ghiani, "Fingerprint liveness detection by local phase quantization".

[32] S. S. A. Abhyankar, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques".

[33] S. A. S.B. Nikam, "Fingerprint liveness detection using curvelet energy and co-occurrence signatures".

[34] G. M. F. R. P. Coli, "Power spectrum-based fingerprint vitality detection, in 2007 IEEE Workshop on Automatic Identification Advanced Technologies, 2007. IEEE.".

[35] e. a. T. de Freitas Pereira, "LBP− TOP based countermeasure against face spoofing attacks".

[36] e. a. Z. Akhtar, "Evaluation of multimodal biometric score fusion rules under spoof attacks".

[37] e. a. J. Galbally, "A high performance fingerprint liveness detection method based on quality related features".

[38] I. S. G. H. A. Krizhevsky, "Imagenet classification with deep convolutional neural networks, in Advances in Neural Information Processing Systems. 2012.".

[39] S. L. W. D. Z. Xu, "Learning temporal features using LSTM-CNN architecture for face anti-spoofing".

[40] K. C. A. J. T. Chugh, "Fingerprint spoof buster: use of minutiae-centered patches".

[41] G. H. T. S. D.H. Ackley, "A learning algorithm for Boltzmann machines".

[42] R. S. G.E. Hinton, "Reducing the dimensionality of data with neural networks".

[43] P. Smolensky, "Information processing in dynamical systems: Foundations of harmony theory, 1986, Univ at boulder dept of computer science colorado.".

[44] G. H. V. Nair, "Implicit mixtures of restricted Boltzmann machines, in Advances in Neural Information Processing Systems, 2009.".

[45] S. O. Y.-W. T. G.E. Hinton, "A fast learning algorithm for deep belief nets".

[46] G. H. M. Welling, "A new learning algorithm for mean field Boltzmann machines".

[47] D. L. M. Muja, "Scalable nearest neighbor algorithms for high dimensional data".

[48] [39] Oran Gafni, Lior Wolf, & Yaniv Taigman. (2019). Live Face De-Identification in Video.

[49] [40] Zafeiriou, Stefanos (09/01/2015). "A survey on face detection in the wild: Past, present and future". Computer vision and image understanding (1077-3142), 138 , p. 1.

[50] [41] U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb and C. Busch, "On the vulnerability of face recognition systems towards morphed face attacks," 2017 5th International Workshop on Biometrics and Forensics (IWBF), 2017, pp. 1-6, doi: 10.1109/IWBF.2017.7935088.

[51] [42] R. Raghavendra, K. B. Raja, S. Venkatesh, F. A. Cheikh and C. Busch, "On the vulnerability of extended Multispectral face recognition systems towards presentation attacks," 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), 2017, pp. 1-8, doi: 10.1109/ISBA.2017.7947698.

[52] [50] Guo, Zhiqing (03/01/2021). "Fake face detection via adaptive manipulation traces extraction network". Computer vision and image understanding (1077-3142), 204 , p. 103170.

[53] [51] Hadi Mansourifar, & Weidong Shi. (2020). Vulnerability of Face Recognition Systems Against Composite Face Reconstruction Attack.

[54] StyleGAN Official TensorFlow Implementation https://github.com/NVlabs/stylegan

[55] Amarjot Singh, Devendra Patil, G Meghana Reddy, & SN Omkar. (2017). Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network.

[56] R. Lionnie, C. Apriono and D. Gunawan, "Face Mask Recognition with Realistic Fabric Face Mask Data Set: A Combination Using Surface Curvature and GLCM," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-6, doi: 10.1109/IEMTRONICS52119.2021.9422532.

[57] R. Ramachandra et al., "Custom silicone Face Masks: Vulnerability of Commercial Face Recognition Systems & Presentation Attack Detection," 2019 7th International Workshop on Biometrics and Forensics (IWBF), 2019, pp. 1-6, doi: 10.1109/IWBF.2019.8739236.

[58] Pavel Korshunov, & Sébastien Marcel. (2019). Vulnerability of Face Recognition to Deep Morphing.

[59] Shawn Shan, Emily Wenger, Jiayun Zhang, Huiying Li, Haitao Zheng, & Ben Y. Zhao. (2020). Fawkes: Protecting Privacy against Unauthorized Deep Learning Models.

[60] J. Daugman, "How iris recognition works," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan. 2004, doi: 10.1109/TCSVT.2003.818350.

[61] Morales A., Fierrez J., Galbally J., Gomez-Barrero M. (2019) Introduction to Iris Presentation Attack Detection. In: Marcel S., Nixon M., Fierrez J., Evans N. (eds) Handbook of Biometric Anti-Spoofing. Advances in Computer Vision and Pattern Recognition. Springer, Cham. https://doi-org.libezproxy2.syr.edu/10.1007/978-3-319-92627-8_6

[62] Hájek J., Drahanský M. (2019) Recognition-Based on Eye Biometrics: Iris and Retina. In: Obaidat M., Traore I., Woungang I. (eds) Biometric-Based Physical and Cybersecurity Systems. Springer, Cham. https://doi-org.libezproxy2.syr.edu/10.1007/978-3-319-98734-7_3

[63] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, pp. 1148-1161, Nov. 1993, doi: 10.1109/34.244676.

[64] Wisse, B., & Zieve, D. (n.d.). External and INTERNAL Eye ANATOMY: Medlineplus medical Encyclopedia image. MedlinePlus. https://medlineplus.gov/ency/imagepages/8867.htm.

[65] Zainal Abidin, Zaheera & Manaf, Mazani & Shibghatullah, A.. (2014). ant-CBIR: A New Method for Radial Furrow Extraction in Iris Biometric.

[66] Al-Raisi, Ahmad N., Ahmad N. Al-Raisi, and Ali M. Al-Khouri. "Iris Recognition and the Challenge of Homeland and Border Control Security in UAE." Telematics and Informatics, vol. 25, no. 2, 05/01/2008, pp. 117-132, https://doi.org/10.1016/j.tele.2006.06.005. https://www.sciencedirect.com/science/article/pii/S0736585306000360

[67] Ted Dunstone, Geoff Poulton, Vulnerability assessment, Biometric Technology Today, Volume 2011, Issue 5, 2011, Pages 5-7, ISSN 0969-4765, https://doi.org/10.1016/S0969-4765(11)70093-5. (https://www.sciencedirect.com/science/article/pii/S0969476511700935)

[68] U.S. National Library of Medicine. (n.d.). Eye: Medlineplus medical Encyclopedia image. MedlinePlus. Retrieved September 14, 2021, from https://medlineplus.gov/ency/imagepages/1094.htm.

[69] Vision: Definition, parts of the eye & eye health. Cleveland Clinic. (2020, March 4). Retrieved September 14, 2021, from https://my.clevelandclinic.org/health/articles/21204-vision.

[70] Rolfs M. Microsaccades: small steps on a long way. Vision Res. 2009 Oct;49(20):2415-41. doi: 10.1016/j.visres.2009.08.010. Epub 2009 Aug 13. PMID: 19683016.

[71] Toth A., Galbally J. (2014) Anti-spoofing: Iris. In: Li S., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-3-642-27733-7_179-4

[72] Agarwal, R., Jalal, A.S. Presentation attack detection system for fake Iris: a review.Multimed Tools Appl 80, 15193–15214 (2021). https://doi-org.libezproxy2.syr.edu/10.1007/s11042-020-10378-7

[73] Adam Czajka and Kevin W. Bowyer. 2018. Presentation Attack Detection for Iris Recognition: An Assessment of the State-of-the-Art. ACM Comput. Surv. 51, 4, Article 86 (September 2018), 35 pages. DOI: https://doi-org.libezproxy2.syr.edu/10.1145/3232849