Liveness Detection in Biometrics

Maximilian Krieg and Nils Rogmann

Hochschule Darmstadt – Fachbereich Informatik
Schöfferstr. 8b, 64295 Darmstadt, Germany
{Maximilian.Krieg; Nils.Rogmann}@stud.h-da.de

Abstract: The use of biometrics as an alternative for PIN and password-based authentication systems becomes increasingly attractive in this day and age. Biometric systems perform an authentication by personal biological or behavioral characteristics. A negative side effect of the increasing use of biometric systems is the progressing development of sophisticated attacks, in particular presentation attacks. Liveness detection has the aim to identify a living and during the biometric authentication process present individual as such and to repel spoofing attacks at the data capture subsystem. In this paper different current attack scenarios are described. Based on these scenarios, several liveness detection techniques are elaborated and investigated as possible countermeasures.

Keywords: Liveness Detection, Presentation Attacks, Spoofing, Presentation Attack Detection

1 Introduction

The use of biometric systems has experienced an enormous growth of interest in recent years. While the recognition of fingerprints has been strongly influenced by the forensic application it becomes more and more accepted in occupational and personal life. The stigmatization as a criminological tool is still present, but is increasingly losing its significance [Ev15], [KS13]. Essential factors for the increasing proliferation are technical advancements which provide convenience and mobility as well as affordable sensors for the user. The increasing digitization has led to a rapid growth of systems that are protected primarily through passwords against unauthorized access. A password-based authentication is flawed with a variety of problems, because passwords can be guessed, forgotten or passed. Biometrics remedies these problems by complementing authentication as a second factor or even substitute passwords completely [Wi15].

The research and advisory company Gartner Inc. predicts that 30 percent of organizations will use biometric authentication for their mobile devices by 2016. This represents a growth of roughly 25 percent within two years [Ga14]. To give an example, the introduction of the electronic passport (ePass) in 2005 is an indicator of the growing importance of biometric systems at national and international level [Ev15], [BI15].

The probability of a successful attack should not be underestimated. Biometric samples such as latent fingerprints are left unconsciously and often unavoidable in many places in everyday life. A latent fingerprint can be collected, for instance, from the surface of a drinking glass or the touch-screen of a smartphone, artificially copied and used for the unauthorized authentication in a biometric system [KS13]. These replicas are referred to

as artifacts. Attacks which rely on the presentation of such artifacts are called presentation attacks and are the main focus of this paper. The unauthorized possession of a high-quality biometric sample poses a risk to the entire system and the user, since the biometric characteristics as opposed to a password cannot be changed. They are persistent and keep their validity typically for a lifetime [Wi15]. Thus, the responsibility lies with the biometric system and its ability to detect presentation attacks.

In addition, the increased use of biometric recognition increases the likelihood of a compromise. A potential risk of inadequately protected data storage subsystems is the theft of stored biometric references. The responsible use and therefore the decision for which system a biometric recognition is required and even suited has to be performed individually [Wi15]. The application of biometric template protection-techniques at this point ensures that a stolen biometric reference does not lead to the uselessness of the complete source. The protection of biometric references is however not part of liveness detection and will therefore not be addressed in this paper.

In this paper current and practice-oriented attack scenarios are investigated and possible countermeasures are worked out. The emphasis is on the assessment of facial, fingerprint and vein recognition. At last, based on the presented knowledge, an overall assessment of recent attack scenarios against biometric systems is conducted.

2 Attack Scenarios for Presentation Attacks

A recent example of the threat posed by these attacks was presented at the 31st Chaos Communication Congress (31C3) in December 2014. Using a digital camera, thumb photo of federal minister of defense Ursula of the Leyen was taken out of a distance of approximately three meters and was processed digitally. A biometric sample can already be generated from a single image (see. Fig. 1). In the next step the biometric features can be extracted from the processed sample [CC14].

Fig. 1: Reconstruction of a fingerprint through photography [CC14].

Furthermore, it was shown how a latent fingerprint can be taken from a smartphone touch-screen to produce an artifact with capacitive properties. For this the touchscreen was scanned with a high-resolution scanner (2400 DPI). The image was preprocessed digitally to print it on a transparent foil. This was used to expose a printed circuit board (PCB), which later serves as a template for the artifact. The PCB was sprayed with graphite spray and coated with wooden glue. An artifact produced in this way can be used to unlock the smartphone. The middle illustration in figure 2 shows how such an artifact may look like [CC14].

Beside fingerprint sensors, other systems are also affected by spoofing attacks. For instance, facial recognition systems can be deceived by printed facial images. This kind

of presentation attack, however, can be identified by many systems today. Mask and video attacks are considered more modern and effective approaches. A video attack can relatively easily be manufactured. For this purpose, a high-resolution video of a person is recorded and presented to the sensor in the next step using a tablet computer. Other sources for such recordings already exist through the internet and television, if it concerns a person of the public life. Corresponding videos can be obtained from sites like YouTube. The generation of 3D masks (see. Fig. 2) is considered more complex. To begin with, at least two images of the head are required, one in frontal and one in profile view. The masks must be shaped and modeled in the next step. The peculiarity of these attacks lies in the ability to collect biometric characteristics at a distance and without direct interaction [EM13], [An14].

Another technique is vein recognition which is considered comparatively reliable. This paper focuses only on finger vein recognition. An essential advantage of this technique is that the biometric characteristic cannot be collected from objects, like with fingerprints, and requires an additional illumination in near infrared area to make the veins visible for a sensor. If an attacker obtains the vein image of a biometric sample, the possibility for the production of an artifact exists. The image is preprocessed using histogram equalization for contrast enhancement and a Gaussian filter for noise reduction. In addition, it is scaled on a size corresponding to the finger, is bordered with black pixels and mirrored to reverse the internal reflection of the sensor. The resulting image is printed on high-quality paper, contoured with a marker if necessary and finally presented to the sensor. This attack achieved a false acceptance rate between 76 and 86 percent. Figure 2 shows on the right side how the sensor “sees” the printed artifact [To14].

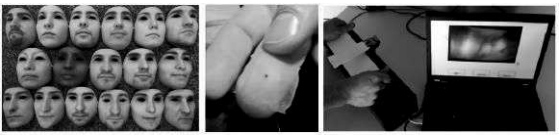

Fig. 2: Examples of Presentation Attack Instruments according to [EM13], [To14], [CC14].

3 Liveness Detection

The detection of presentation attacks can be accomplished by many different *presentation attack detection* (PAD) methods and techniques. Basically, capturing these attacks either takes place through a whole system-monitoring approach or through additional features being implemented into the data capture subsystem that is integrated into a biometric system [Am15]. One of the most frequently used PAD techniques is called *liveness detection*. The relevant aspects of this technique will be preliminarily elaborated and explained within this chapter. Subsequently, the obtained knowledge will be used to acquire and compare several different liveness detection techniques to recognize the previously described attack scenarios against biometric systems.

The general task of liveness detection is to detect whether a biometric probe (e.g. a fingerprint) belongs to a living subject that is present at the point of biometric capture [Am15]. Using liveness detection techniques, a reliable recognition of dead fingers or

photographed faces can be established, for example. Consequently, the risk of successful presentation attacks is significantly reduced. Thus, in addition to the regular biometric recognition, liveness detection is an important procedure aiming at an increased reliability of biometric systems.

In the global market, several different methods verifying the liveness of biometric features are already established. Among others these methods include an evaluation of anatomical characteristics, physiological processes of the human body and involuntary reactions to stimuli as well as various predictable human behaviors [Am15].

3.1 Hardware and Software-based Approaches

Typically, liveness detection methods are divided into hardware and software-based approaches. Giving an example, special medical hardware can be used to perform an electrocardiogram or pulse oximetry to detect living subjects. For this purpose, the acquisition of additional sensors such as devices for measuring body temperature or pulse rate ([LJ09b], pp.924-925) that needs to be combined with the regular biometric test system is required. As a consequence, account should be taken of additional costs for acquisition as well as for routine maintenance.

Software-based techniques, by contrast, make use of biometric data already being captured for biometric recognition of individuals. In general, these solutions are implemented as supplementary algorithms being integrated into a consisting biometric system. To give an example, these algorithms are then applied to the extracted biometric fingerprint probe in order to detect the deformation of a living finger that is pressed on the sensor ([LJ09b], p. 925).

3.2 Passive and active Techniques

Besides the distinction of hardware and software-based techniques another common attempt consists of a separation between passive (non-stimulating) and active (stimulating) automated liveness detection methods [Am15]. In general, passive detection techniques make use of biometric probes which were recorded through a biometric sensor. According to this, further interactions with the data subject are not necessary. For this, a typical example would be a temperature or pulse measurement taking place while the biometric probe is collected [MA14].

Active detection techniques normally require additional interaction of the biometric data subject with the biometric system. These further interactions should be requested using challenge response procedures. The different challenge response approaches can be read in *ISO/IEC DIS 30107*-1 as they cannot be discussed in this paper [Am15].

3.3 Defense against Presentation Attacks

There are several different liveness detection techniques that have already been evaluated on the market and successfully used for presentation attack detection. Various

techniques that behave as possible countermeasures against previously described attack scenarios will be elaborated first. Based on the main results of this paper, an overall evaluation of these scenarios will be carried out in chapter 3.4 subsequently. The table below contains liveness detection techniques that could be used as counter-measures for detecting various presentation attacks:

Biometric Sensor	**Presentation Attack**	**Liveness Detection Technique**	**Remarks**
Fingerprint scanner	2D print, dead finger, artificial finger, capacitive finger	**Passive**: pulse measurement* [Am15], temperature measurement** [MA14], sweat detection [Am15], skin resistance detection ** [KS13] **Active** (challenge response): Request of different fingers in random order [Am15]	* not working against capacitive finger artifacts ** depends on the consistency of the artificial finger
Vein scanner	2D print, dead finger, artificial finger,	**Passive**: pulse measurement, temperature measurement, (sweat detection), skin resistance detection **Active** (challenge response): Request of different fingers in random order	
Face scanner	2D print, 3D face mask, video attack	**Passive**:** natural eye blinking * [Am15], natural muscle movements while speaking [MA14] **Active** (challenge response): eye closing request [Am15], voice usage request** [MA14], head turning request** [Am15]	* Possibly not working against face masks ** No protection against video attacks
Fingerprint, vein & face scanner	2D print, 3D face mask, dead body parts, artificial or digital fingers, veins & faces	**Passive**: Infrared & ultraviolet light, thermal scans* [MA14], medical techniques like ECG, pulse oximetry or blood pressure reading [KS13]	* Possible in combination with all optical sensors

Tab. 1: Liveness detection techniques against presentation attacks.

As shown in table 1, there are several techniques that can be used against different presentation attacks. However, an individual application of one method such as a pulse

or temperature measurement might get tricked with an acceptable effort and without specific knowledge [MA14]. Thus, a combination of multiple liveness detection techniques is reasonable as the security of the whole biometric system will be increased.

3.4 Evaluation of Presentation Attacks

The newly acquired knowledge about liveness detection techniques can be used for a final evaluation of the previously described presentation attack scenarios. For this purpose, first the most important findings will be shown in table 2 and described in detail afterwards. Here it must be considered that the term paper does not focus an assessment of the effectiveness of different PAD techniques. Consequently, this evaluation just gives estimation about the efficiency of these techniques.

Attack scenario	Production cost	Technical complexity	Availability and advantage of counter-measures
High resolution 2D fingerprint image	Low	Low	High
Artificial capacitive finger	Medium	Medium	High
2D face image	Low	Low	High
Video attack	Low	Low	Low
3D face mask	High	High	Medium
2D finger vein image	High	High	Medium to high

Tab. 2: Comparative summary of attack scenarios.

Table 2 contains different attack scenarios and discusses them in terms of production cost as well as technical complexity. Moreover, availabilities and advantages of counter-measures are considered as they provide an important factor in regard to the general risk of a specific presentation attack. Based on these features, each attack scenario will be discussed in detail:

1. The technical capabilities to extract a fingerprint from a high-resolution 2D image have been increased consistently in the past years. Nowadays, digital processing and post-processing no longer present difficult technical challenges while creating a fake print. Finally, several methods reduce the possibility of a successful presentation attack execution, e.g. pulse and temperature measurement or sweat detection as well as several active liveness detection techniques mentioned in table 1.

2. In general, the production of artificial capacitive finger artifacts requires a higher technical knowledge as well as an access to a high-resolution scanner. Furthermore, the usage of optical sensors would reduce the risk of these attacks completely, since only capacitive sensors are vulnerable. However, due to their cost-effective integration into smartphones and tablets, capacitive sensors are widespread. In this case, software-based liveness detection approaches such as sweat detection algorithms can be used to protect the authenticity of these devices [Ne14].

3. In order to create printed 2D face images, no specific technical knowledge or high amount of time is required. Nevertheless, due to their low complexity these attacks

are relatively easy and fast to detect. Giving an example, the detection of natural eye blinking of a living subject provides easy protection against this kind of attacks [MA14]. In addition, challenge response mechanisms such as requests for head rotation or eye closing offer conceivable protection. Taking these circumstances into account, this attack scenario is not dangerous for modern biometric systems.

4. In contrast, the detection of video attacks is more complex. In some cases the turning of a head or the closing of an eye might be recorded and used for a replay attack against biometric systems afterwards. As part of this attack the misuse of voice recordings is also conceivable. As a consequence, biometric face recognition systems should be protected with additional hardware such as infrared, ultraviolet or thermal scanners. The use of medical hardware (e.g. an electrocardiogram) would also be feasible. However, it must be mentioned that due to high costs resulting from these additional systems, some cost-benefit analyses should be done first.

5. The production of a 3D face mask requires multiple high-resolution images of a head as well as the knowledge and capability to create such a mask. Consequently, compared to the video attack scenario the technical and temporal complexity is much higher. However, challenge response mechanisms (e.g. a voice request and comparison) can provide protection against this scenario. Depending on the underlying material of the mask, infrared, ultraviolet or thermal scanners might also detect presentation attacks using 3D masks.

6. The complex procedure for creating spoofing finger vein images from real finger vein samples was already described in detail in the paper “On the Vulnerability of Finger Vein Recognition to Spoofing” [To14]. In general, this scenario represents a promising approach to attack finger vein scanners. However, since the vein pattern that is extracted by the biometric system is embodied inside the finger it cannot be captured or collected like a fingerprint. If an attacker still succeeded to make a high quality copy, liveness detection techniques such as pulse or temperature measurement could be used to protect the biometric system. As the biometric sensor implements a thermal scan to extract vein samples, pulse detection can be realized easily by capturing a video over a short period of time. In this case, no additional hardware would be necessary. Finally, the texture quality of vein images can be compared to fake images using *Fourier Transformation* or an extraction of *Binarized Statistical Image Features*. Since these techniques cannot be discussed in detail within this paper, further information relating this topic can be found in “The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks“ [To15].

4 Conclusion

Since the use of biometric systems for authentication purposes has experienced an enormous growth of interest, the amount and the complexity of attacks has increased dramatically, too. This particularly includes presentation attacks. However, the threat originated from these attacks can be reduced by using liveness detection techniques.

As shown in this paper, there are several different methods and techniques working

against current presentation attack scenarios efficiently. Here it must be mentioned that none of these techniques provide an entire protection to biometric systems. Especially, the detection of video attacks is a particular challenge (see chapter 3.4). As a consequence, a combination of different liveness detection techniques is strongly recommended. Moreover, as already mentioned in chapter 3, there are several other detection techniques that should be used for detecting presentation attacks and protecting against manipulations of biometric systems to increase the overall security [Am15].

Finally, the results of this term paper can be used for future research tasks regarding liveness detection. Here, an evaluation of the techniques performance and reliability would be of peculiar interest.

References

[Am15] American National Standards Institute: ISO/IEC DIS 30107-1 - Part 1: Framework, pp. 2-7, 2015.

[An14] Anjos, André et.al: Handbook of Biometric Anti-Spoofing: Face Anti-spoofing: Visual Approach, pp. 65-82, Springer London, 2014.

[BI15] Federal Ministry of the Interior, http://www.bmi.bund.de/DE/Themen/Moderne-Verwaltung/Ausweise-Paesse/Reisepass/reisepass.html, last visited: 20.05.2015.

[CC14] Chaos Computer Club e.V., https://media.ccc.de/browse/congress/2014/31c3_-_6450_-_de_-_saal_1_-_201412272030_-_ich_sehe_also_bin_ich_du_-_starbug.html#video, last visited: 20.05.2015.

[EM13] Erdogmus, Nesli; Marcel, Sebastien: Spoofing in 2D Face Recognition with 3D Masks and Anti-spoofing with Kinect, Idiap Research Institute, 2013.

[Ev15] Evans, Nicholas et.al.: Guest Editorial Special Issue on Biometric Spoofing and Countermeasures. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 4, APRIL 2015, pp. 699-702, 2015.

[Ga14] Gartner, Inc., http://www.gartner.com/newsroom/id/2661115, last visited: 22.05.2015.

[KS13] Kalla, Christian; Schuch, Patrick: Sicherheit in der Fingerabdruck-Identifikation. Datenschutz und Datensicherheit - DuD Volume 37, Issue 6, 352-357, 2013.

[LJ09b] Li, Stan Z.; Jain, Anil: Encyclopedia of Biometrics, pp. 883-952, Springer US, 2009.

[MA14] Matthew, Peter; Anderson Mark: Novel Approaches to Developing Multimodal Biometric Systems with Autonomic Liveness Detection Characteristics, 2014.

[Ne14] NextID Biometrics: Liveness Detection for the Mobile Biometrics Market, http://nexidbiometrics.com/wp-content/uploads/2014/01/NexID-White-Paper-Mobile-Biometrics.pdf, 2014, last visited: 22.05.2015.

[To14] Tome, Pedro; Vanoni, Matthias; Marcel, Sebastien: On the Vulnerability of Finger Vein Recognition to Spoofing, Idiap Research Institute, 2014.

[To15] Tome, Pedro et.al.: The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks, http://publications.idiap.ch/downloads/papers/2015/Tome_ICB-2015_2015.pdf, last visited: 05.06.2015

[Wi15] Wikibooks: Biometrie, http://de.wikibooks.org/wiki/Biometrie, last visited: 21.05.2015.