Introduction to Presentation Attack Detection in Fingerprint Biometrics

This is the final peer-reviewed author’s accepted manuscript (postprint) of the following publication:

Published Version:

This version is available at: https://hdl.handle.net/11585/929553 since: 2024-01-29

Published:
DOI: http://doi.org/10.1007/978-981-19-5288-3_1

Terms of use:
Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

(Article begins on next page)
Chapter 1

Introduction to Presentation Attack Detection in Fingerprint Biometrics

Javier Galbally, Julian Fierrez, Raffaele Cappelli, and Gian Luca Marcialis

Abstract This chapter provides an introduction to Presentation Attack Detection (PAD) in fingerprint biometrics, also coined as anti-spoofing, describes early developments in this field, and briefly summarizes recent trends and open issues.

1.1 Introduction

“Fingerprints cannot lie, but liars can make fingerprints”. Unfortunately, this paraphrase of an old quote attributed to Mark Twain has been proven right in many occasions now.

As the deployment of fingerprint systems keeps growing year after year in such different environments as airports, laptops, or mobile phones, people are also becoming more familiar to their use in everyday life and, as a result, the security weaknesses of fingerprint sensors are becoming better known to the general public. Nowadays it is not difficult to find websites or even tutorial videos, which give detailed guidance on how to create fake fingerprints which may be used for spoofing biometric systems.

1 Figures do not lie, but liars do figure.

J. Galbally
European Commission, Joint Research Centre, Ispra, Italy
e-mail: javier.galbally@ec.europa.eu

J. Fierrez
Biometrics and Data Pattern Analytics-BiDA Lab, Universidad Autonoma de Madrid, Madrid, Spain
e-mail: julian.fierrez@uam.es

R. Cappelli
Università di Bologna, Cesena, Italy
e-mail: raffaele.cappelli@unibo.it

G. L. Marcialis (Ed)
Università di Cagliari, Cagliari, Italy
e-mail: marcialis@unica.it
As a consequence, the fingerprint stands out as one of the biometric traits which has arisen the most attention not only from researchers and vendors, but also from the media and users, regarding its vulnerabilities to Presentation Attacks (PAs, aka spoofing), as the attempt to impersonate someone else by submitting an artifact or Presentation Attack Instrument. This increasing interest of the biometric community in the security evaluation of fingerprint recognition systems against presentation attacks has led to the creation of numerous and very diverse initiatives in this field: the publication of many research works disclosing and evaluating different fingerprint presentation attack approaches [1–4]; the proposal of new countermeasures to spoofing, namely, novel presentation attack detection methods [5–7]; related book chapters [8, 9]; Ph.D. and MSc Thesis which propose and analyze different fingerprint PA and PAD techniques [10–13]; several patented fingerprint PAD mechanisms both for touch-based and contactless systems [14–18]; the publication of Supporting Documents and Protection Profiles in the framework of the security evaluation standard Common Criteria for the objective assessment of fingerprint-based commercial systems [19, 20]; the organization of competitions focused on vulnerability assessment to fingerprint presentation attacks [21–23]; the acquisition of specific datasets for the evaluation of fingerprint protection methods against direct attacks [24–26], the creation of groups and laboratories which have the evaluation of fingerprint security as one of their major tasks [27–29]; or the acceptance of several European Projects on fingerprint PAD as one of their main research interests [30, 31].

The aforementioned initiatives and other analogue studies have shown the importance given by all parties involved in the development of fingerprint-based biometrics to the improvement of the systems security and the necessity to propose and develop specific protection methods against PAs in order to bring this rapidly emerging technology into practical use. This way, researchers have focused on the design of specific countermeasures that enable fingerprint recognition systems to detect fake samples and reject them, improving this way the robustness of the applications.

In the fingerprint field, besides other PAD approaches such as the use of multibiometrics or challenge-response methods, special attention has been paid by researchers and industry to the so-called liveness detection techniques. These algorithms use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements [32]: (i) non-invasive, the technique should in no case be harmful to the individual or require an excessive contact with the user; (ii) user friendly, people should not be reluctant to use it; (iii) fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; (iv) low cost, a wide use cannot be expected if the cost is excessively high; and (v) performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

Liveness detection methods are usually classified into one of two groups: (i) Hardware-based techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure,
or odor), (ii) Software-based techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).

The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed) and less intrusive since their implementation is transparent to the user. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as presentation attacks. For instance, software-based methods can protect the system against the injection of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor [33, 34].

Although, as shown above, a great amount of work has been done in the field of fingerprint PAD and big advances have been reached over the last two decades, the attacking methodologies have also evolved and become more and more sophisticated. This way, while many commercial fingerprint readers claim to have some degree of PAD embedded, many of them are still vulnerable to presentation attack attempts using different artificial fingerprint samples. Therefore, there are still big challenges to be faced in the detection of fingerprint direct attacks.²

This chapter represents an introduction to the problem of fingerprint PAD [35, 36]. More comprehensive and up-to-date surveys of recent advances can be found elsewhere [37–40]. The rest of the chapter is structured as follows. An overview into early works in the field of fingerprint PAD is given in Sect. 1.2, while Sect. 1.3 provides a summary of recent trends and main open issues. A brief description of large and publicly available fingerprint spoofing databases is presented in Sect. 1.4. Conclusions are finally drawn in Sect. 1.5.

1.2 Early Works in Fingerprint Presentation Attack Detection

The history of fingerprint forgery in the forensic field is probably almost as old as that of fingerprint development and classification itself. In fact, the question of whether or not fingerprints could be forged was positively answered [41] several years before it was officially posed in a research publication [42].

Regarding modern automatic fingerprint recognition systems, although other types of attacks with dead [43] or altered [44] fingers have been reported, almost

all the available vulnerability studies regarding presentations attacks are carried out either by taking advantage of the residual fingerprint left behind on the sensor surface, or by using some type of gummy fingertip (or even complete prosthetic fingers) manufactured with different materials (e.g., silicone, gelatin, plastic, clay, dental molding material, or glycerin). In general, these fake fingerprints may be generated with the cooperation of the user, from a latent fingerprint or even from a fingerprint image reconstructed from the original minutiae template [1–3, 24, 45–49].

These very valuable works and other analogue studies have highlighted the necessity to develop efficient protection methods against presentation attacks. One of the first efforts in fingerprint PAD initiated a research line based on the analysis of the skin perspiration pattern which is very difficult to be faked in an artificial finger [5, 50]. These pioneer studies, which considered the periodicity of sweat and the sweat diffusion pattern, were later extended and improved in two successive works applying a wavelet-based algorithm and adding intensity-based perspiration features [51, 52]. These techniques were finally consolidated and strictly validated on a large database of real, fake, and dead fingerprints acquired under different conditions in [25]. Recently, a novel region-based liveness detection approach also based on perspiration parameters and another technique analyzing the valley noise have been proposed by the same group [53, 54]. Part of these approaches have been implemented in commercial products [55] and have also been combined with other morphological features [56, 57] in order to improve the presentation attack detection rates [58].

A second group of fingerprint liveness detection techniques has appeared as an application of the different fingerprint distortion models described in the literature [59–61]. These models have led to the development of a number of liveness detection techniques based on the flexibility properties of the skin [6, 62–64]. In most of these works, the user is required to move his finger while pressing it against the scanner surface, thus deliberately exaggerating the skin distortion. When a real finger moves on a scanner surface, it produces a significant amount of distortion, which can be observed to be quite different from that produced by fake fingers which are usually more rigid than skin. Even if highly elastic materials are used, it seems very difficult to precisely emulate the specific way a real finger is distorted, because the behavior is related to the way the external skin is anchored to the underlying derma and influenced by the position and shape of the finger bone.

Other liveness detection approaches for fake fingerprint detection include the combination of both perspiration and elasticity-related features in fingerprint image sequences [65]; fingerprint-specific quality-related features [7, 66]; the combination of the local ridge frequency with other multiresolution texture parameters [56]; techniques which, following the perspiration-related trend, analyze the skin sweat pores visible in high-definition images [67, 68]; the use of electric properties of the skin [69]; using several image processing tools for the analysis of the fingerprint surface texture such as wavelets [70], or three very related works using Gabor filters [71], ridgelets [72], and curvelets [73]; and analyzing different characteristics of the Fourier spectrum of real and fake fingerprint images [74–78].

A critical review of some of these solutions for fingerprint liveness detection was presented in [79]. In a subsequent work [80], the same authors gave a comparative
analysis of the PAD methods efficiency. In this last work, we can find an estimation of some of the best performing static (i.e., measured on one image) and dynamic (i.e., measured on a sequence of images) features for liveness detection, that were later used together with some fake-finger specific features in [78] with very good results. Different static features are also combined in [81], significantly improving the results of the individual parameters. Other comparative results of different fingerprint PAD techniques are available in the results of the 2009 and 2011 Fingerprint Liveness Detection Competitions (LivDet 2009 and LivDet 2011) [82, 83].

In addition, some very interesting hardware-based solutions have been proposed in the literature applying multispectral imaging [84, 85], an electrotactile sensor [86], pulse oximetry [87], detection of the blood flow [14], odor detection using a chemical sensor [88], or a currently very active research trend based on Near Infrared (NIR) illumination and Optical Coherence Tomography (OCT) [89–94].

More recently, the third type of protection methods which fall out of the traditional two-type classification software- and hardware-based approaches have been started to be analyzed in the field of fingerprint PAD. These protection techniques focus on the study of biometric systems under direct attacks at the score level, in order to propose and build more robust matchers and fusion strategies that increase the resistance of the systems against presentation attack attempts [95–99].

Outside the research community, some companies have also proposed different methods for fingerprint liveness detection such as the ones based on ultrasounds [100, 101], light measurements [102], or a patented combination of different unimodal experts [103]. A comparative study of the PAD capabilities of different commercial fingerprint sensors may be found in [104].

Although the vast majority of the efforts dedicated by the biometric community in the field of fingerprint presentation attacks and PAD are focused on touch-based systems, some works have also been conducted to study the vulnerabilities of contactless fingerprint systems against direct attacks, and some protection methods to enhance their security level have been proposed [17, 50, 105].

The approaches mentioned above represent the main historical developments in fingerprint PAD until ca. 2012–2013. For a survey of more recent and advanced methods in the last 10 years, we refer the reader to [37–40] and the ODIN program.³

1.3 A Brief View on Where We Are

In the next chapters of the book, the reader will be able to find information about the most recent advances in fingerprint presentation attack detection. This section merely summarizes some ongoing trends in the development of PADs and some of the main open issues.

As stated in the previous Section, independent and general-purpose descriptors were proposed for feature extraction since from 2013 [38]. In general, these features

looked for minute details of the fake image which are added or deleted, impossible
to catch by the human eye. This was typically done by appropriate banks of filters
aimed at deriving a set of possible patterns. The related feature sets can be adopted
to distinguish live from fake fingerprints by machine learning methods.

“Textural features” above looked as the most promising until the advent of deep
learning approaches [39, 40]. These, thanks to the increased availability of datasets,
allowed the design of a novel generation of fingerprint PAD [26, 106, 107] which
exploited the concept of “patch”, a very small portion of the fingerprint image to
be processed instead of taking the image as a whole input to the network. However,
textural features have not yet been left behind because of their expressive power and
the fact that they explicitly rely on the patch definition [108, 109].

Among the main challenges to be faced with in the near future, it is important to
mention the following[110]:

• assessing the robustness of anti-spoofing methods against novel presentation
  attacks in terms of fabrication strategy, adopted materials, and sensor technology:
  for instance, in [111], it has been shown that the PAD error rates of software-based
  approaches can show a three-fold increase when tested on PA materials not seen
during training;
• designing effective methods to embed PAD in fingerprint verification systems
  [112], including the need for computationally efficient PAD techniques, to be used
  on low-resources systems such as embedded devices and low-cost smartphones;
• improving explainability of PAD systems; the use of CNNs is providing great
  benefits to fingerprint PAD performance, but such solutions are usually considered
  as “black boxes” shedding little light on how and why they actually work. It
  is important to gain insights into the features that CNNs learn, so that system
  designers and maintainers can understand why a decision is made and tune the
  system parameters if needed.

1.4 Fingerprint Spoofing Databases

The availability of public datasets comprising real and fake fingerprint samples and of
associated common evaluation protocols is basic for the development and improve-
ment of fingerprint PAD methods.

However, in spite of the large amount of works addressing the challenging problem
of fingerprint protection against direct attacks (as shown in Sect. 1.2), in the great
majority of them, experiments are carried out on proprietary databases which are not
distributed to the research community.

Currently, the two largest fingerprint spoofing databases publicly available for
researchers to test their PAD algorithms are as follows:

• LivDet DBs (LivDet 2009–2021 DBs) [21–23]: These datasets, which share the
  acquisition protocols and part of the samples, are available from 2009 to 2021
Fingerprint Liveness Detection Competitions websites\(^4\)\(^-\)\(^5\) and are divided into the same train and test sets used in the official evaluations. Over seven editions, LivDet shared with the research community over 20,000 fake fingerprint images made up of a large set of materials (play doh, silicone, gelatine, latex...) on a wide brands of optical and solid-state sensors. Over years, LivDet competitions also proposed challenges as the evaluation of embedding fingerprint PAD and matching [22, 23] and of a novel approach to provide spoofs called “Screenspoof” directly from the user’s smartphone screen [22]. The LivDet datasets are available for researchers by signing the license agreement.

- ATVS-Fake Fingerprint DB (ATVS-FFp DB) [24]: This database is available from the Biometrics group at UAM.\(^6\) It contains over 3,000 real and fake fingerprint samples coming from 68 different fingers acquired using a flat optical sensor, a flat capacitive sensor, and a thermal sweeping sensor. The gummy fingers were generated with and without the cooperation of the user (i.e., recovered from a latent fingerprint) using modeling silicone.

### 1.5 Conclusions

The study of the vulnerabilities of biometric systems against presentation attacks has been a very active field of research in recent years [113]. This interest has led to big advances in the field of security-enhancing technologies for fingerprint-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known threats (usually based on some type of self-manufactured gummy finger) has proven to be a challenging task.

Simple visual inspection of an image of a real fingerprint and its corresponding fake sample shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space. These differences come from the fact that fingerprints, as 3-D objects, have their own optical qualities (absorption, reflection, scattering, and refraction), which other materials (silicone, gelatin, and glycerin) or synthetically produced samples do not possess. Furthermore, fingerprint acquisition devices are designed to provide good quality samples when they interact, in a normal operation environment, with a real 3-D trait. If this scenario is changed, or if the trait presented to the scanner is an unexpected fake artifact, the characteristics of the captured image may significantly vary.

In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different and therefore image-based

---

\(^4\) \url{http://livdet.dice.unica.it}.

\(^5\) \url{http://people.clarkson.edu/projects/biosal/fingerprint/index.php}.

\(^6\) \url{http://biometrics.ets.uam.es/}. 

presentation attack detection in fingerprint biometrics would be feasible. Key early works in this regard have been summarized in the present chapter.

Overall, the chapter provided a general overview of the progress which was initially made in the field of fingerprint PAD and a brief summary about current achievements, trends, and open issues, which will be further developed in the next chapters.

Acknowledgements This work was mostly done (2nd Edition of the book) in the context of TABULA RASA: Trusted Biometrics under Spoofing Attacks, and BEAT: Biometrics Evaluation and Testing projects funded under the 7th Framework Programme of EU. The 3rd Edition update has been made in the context of EU H2020 Projects PRIMA and TRUSTPASS-ETN. This work was also partially supported by the Spanish project BIBECA (RTI2018-101248-B-I00 MINECO/FEDER).

References

10. Kaiho I, Kiss A, Podmantsky JT (2001) Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus 6(175)r64
41. Weihe A, Beifei JN (1924) Fingerprint can be forged. Terasminn Publish Co
102. PosID (2012). http://www.posid.co.uk/
aliveness-testing fingerprint sensor. In: Proceedings of SPIE novel optical systems design and
optimization XII, vol 7429, p 742915


doi.org/10.1109/TSMC.2018.2874281

https://doi.org/10.1016/j.patrec.2021.03.032


Secur 16:42–55. https://doi.org/10.1109/TIFS.2020.2990789

presentation attacks detection: are we ready? IEEE Trans Inf Forensics Secur 16:3358–3361.
https://doi.org/10.1109/TIFS.2021.3121201