Advances in Computer Vision and Pattern Recognition

Sébastien Marcel
Julian Fierrez
Nicholas Evans *Editors*

Handbook of Biometric Anti-Spoofing

Presentation Attack Detection and Vulnerability Assessment

Third Edition

Springer

Advances in Computer Vision and Pattern Recognition

Titles in this series now included in the Thomson Reuters Book Citation Index!

Advances in Computer Vision and Pattern Recognition is a series of books which brings together current developments in this multi-disciplinary area. It covers both theoretical and applied aspects of computer vision, and provides texts for students and senior researchers in topics including, but not limited to:

- Deep learning for vision applications
- Computational photography
- Biological vision
- Image and video processing
- Document analysis and character recognition
- Biometrics
- Multimedia
- Virtual and augmented reality
- Vision for graphics
- Vision and language
- Robotics

Sébastien Marcel · Julian Fierrez · Nicholas Evans
Editors

Handbook of Biometric Anti-Spoofing

Presentation Attack Detection and Vulnerability Assessment

Third Edition

Springer

Editors
Sébastien Marcel
Idiap Research Institute
Martigny, Switzerland

Julian Fierrez
Universidad Autonoma de Madrid
Madrid, Spain

Nicholas Evans
EURECOM
Biot Sophia Antipolis, France

ISSN 2191-6586 ISSN 2191-6594 (electronic)
Advances in Computer Vision and Pattern Recognition
ISBN 978-981-19-5287-6 ISBN 978-981-19-5288-3 (eBook)
https://doi.org/10.1007/978-981-19-5288-3

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword

It is a pleasure and an honour both to write the Foreword for a leading and prestigious book. This is the Third Edition of the *Handbook of Biometrics Anti-Spoofing* and I was co-editor for the first two Editions, and now I have been promoted. (More realistically, I have not worked in Anti-Spoofing for some time now.) So I admit bias, and I am taking the opportunity to look at the book from the outside. Essentially, I shall aim to substantiate my claim that the Handbook is indeed leading and prestigious, and I find it not hard to do.

The first evidence I can offer is that the Handbook was the first text to concentrate on anti-spoofing. There appear to be no other books yet which concentrate on this important topic, though it is among the content of some and naturally within those describing the security domain. I have been privileged to be involved in biometrics from its earliest days, in my case in the 1980s before the word biometrics was coined. Even then we knew that if we were working or were ever to work properly, then we needed to countenance the possibility that someone would try and break the system. In modern terminology, we did not consider the possibility that there might be spoofing or presentation attacks. In the First Edition, I, Sébastien, and Stan Li (the Editors then) argued at length over whether the book should be titled "Spoofing" or "Anti-spoofing"—and that is the nature of pioneering work: one does not even know how best to describe it. So the Handbook's uniqueness and initiative strongly underpin a claim that the text is leading and prestigious.

Secondly, the evidence concerns the people involved: those who have edited this Handbook, those who have authored its Chapters, and those who have reviewed them. Sébastien Marcel is well known for his work in multi-modality anti-spoofing, Nicholas Evans is well known for his works on speech and other biometrics, and Julian Fierrez is well known for his prize-winning works on face and signature. All have contributed to the infrastructure this fascinating subject requires and are due many accolades for their other contributions. This is a great team of Editors. Then we find a cohort of authors who are leading lights in this topic area, and like the Editors, they too have contributed to the infrastructure and the building of this topical material. That the contributors derive from many leading institutions around the world further

underpins the suggestion that the pedigree of those involved emphasizes the claim that the text is leading and prestigious.

The third evidence is that the book's coverage is highly appropriate to lead the way in studies of anti-spoofing. The coverage includes major modalities, like Finger, Face, Iris, and Voice (noting that voice/speaker is often—unfortunately—considered within the signal/speech domain rather than within biometrics). There are naturally other biometrics. In previous editions, these have included signature, gait, and vein and two of these maintain in the new Edition. There are also methodological contributions and there is updated material on standards and legal issues. The latter two are of enormous importance as identity verification and recognition continue to pervade society and enable convenient, practicable, and secure access. So the comprehensiveness and the insight afforded by the Handbook's structure reinforce the claim to leadership and prestige.

There are many other metrics that further contribute to this evidence. The Handbook has been highly cited in its previous two Editions, and naturally, the Chapters within it have their own citations too. My own students have enjoyed the book, and many others do. The book is published within Springer's excellent series on biometrics. Then there are sales and library penetration, neither of which I can assess. That a book reaches its third Edition assures one of the market penetration since publishers will not consider furthering texts that have not proved substantially their value. Even in my biased view, I find it easy to find evidence that this book is the leading and prestigious book and a pioneering text in biometric anti-spoofing. By its content, presentation, ethos, and style, the Third Edition of the *Handbook of Biometrics Anti-Spoofing* makes an excellent addition to this compelling series. My congratulations to all who have contributed to this.

March 2022

Mark S. Nixon
Professor Emeritus
School of Electronics and Computer Science
University of Southampton
Southampton, UK

Preface

The study of Presentation Attack Detection (PAD) is now an established field of research across the biometrics community. Increasing awareness of vulnerabilities to presentation attacks has continued to fuel the growing impetus to develop countermeasures to prevent the manipulation and to protect the security and reliability of biometric recognition systems. Progress has been rapid, with PAD nowadays being a key component to almost any deployment of biometric recognition technology and now standardized by the ISO and the IEC.

The tremendous advances since the publication of the second edition in 2019 are the principal reason why we decided to compile a third edition of the *Handbook of Biometric Anti-Spoofing*. As for the second edition, we published an open call for expressions of interest and invited updates to previous chapters in addition to entirely new contributions. The third edition is arranged in seven different parts dedicated to PAD in fingerprint recognition, iris recognition, face recognition, and voice recognition, with two more covering other and multi-biometrics, legal aspects, and standards. Like the second edition, the first four parts all start with an introduction to PAD that is specific to each biometric characteristic. We are delighted that all four also contain a review of PAD competitions (the last being combined with the respective introduction), all updated to provide an overview of progress and the latest results. New chapters feature throughout and complement updates with coverage of new detection approaches and models, multi-spectral/multi-channel techniques, multiple biometric PAD databases and solutions, and legal perspectives. The third edition comprises 21 chapters. We are extremely grateful to the authors and also the reviewers who have helped to ensure quality. Both authors as well as reviewers are listed separately herein.

We wish also to thank the team at Springer for their support and especially *Celine Chang* and *Vinothini Elango* who helped significantly towards the preparation of this third edition. Our thanks also to Prof. Mark Nixon. Mark served as co-editor for both the first and second editions but, following his recent retirement, stepped down from this role for the third edition. We refused to let him off the hook completely, however, and are delighted that he so kindly agreed to provide the foreword. Thank you Mark!

We are confident that the third edition serves as a timely update and defacto reference to biometric presentation attack detection for researchers, students, engineers, and technology consultants alike. Like the second edition, a number of chapters are accompanied by open-source software, scripts, and tools that can be used by others to reproduce some of the results presented in the book. Additional resources can be downloaded from https://gitlab.idiap.ch/biometric-resources. In almost all cases, the experimental work reported was performed using standard or common databases and protocols which we hope will allow and inspire others to join the PAD efforts. PAD will surely remain at the forefront of research in our fields for years to come. While tremendous progress has been made, new threats are emerging and call for greater investments to ensure that biometrics recognition technology remains both reliable and secure.

Martigny, Switzerland — Sébastien Marcel
Madrid, Spain — Julian Fierrez
Biot Sophia Antipolis, France — Nicholas Evans
March 2022

List of Reviewers

Zahid Akhtar INRS-EMT, University of Quebec, Canada
José Luis Alba Castro Universidad de Vigo, Spain
André Anjos Idiap Research Institute, Switzerland
Sushil Bhattacharjee Idiap Research Institute, Switzerland
Christophe Champod University of Lausanne, Switzerland
Xingliang Cheng Tsinghua University, China
Adam Czajka Research and Academic Computer Network (NASK), Poland and University of Notre Dame, USA
Héctor Delgado Nuance Communications, Spain
Nesli Erdogmus Izmir Institute of Technology, Turkey
Nicholas Evans EURECOM, Department of Digital Security, France
Jiangjiang Feng Tsinghua University, China
Julian Fierrez Biometrics and Data Pattern Analytics—BiDA Lab, Universidad Autonoma de Madrid, Spain
Javier Galbally European Commission, Joint Research Centre, Italy
Anjith George Idiap Research Institute, Switzerland
Luca Ghiani University of Cagliari, Department of Electrical and Electronic Engineering, Italy
Marta Gomez-Barrero da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany
Abdenour Hadid University of Oulu, Finland
Guillaume Heusch Idiap Research Institute, Switzerland
Ivan Himawan Queensland University of Technology, Brisbane, Australia
Els Kindt KU Leuven, Belgium
Tomi Kinnunen School of Computing, University of Eastern Finland, Finland
Jukka Komulainen Center for Machine Vision and Signal Analysis, University of Oulu, Finland
Ketan Kotwal, Idiap Research Institute, Switzerland
Vedrana Krivokuća Hahn, Idiap Research Institute, Switzerland
Stan Z. Li Chinese Academy of Sciences, China
Sébastien Marcel Idiap Research Institute, Switzerland

Gian Luca Marcialis University of Cagliari, Department of Electrical and Electronic Engineering, Italy
Jeanne Pia Mifsud Bonnici University of Groningen, The Netherlands
Amir Mohammadi Idiap Research Institute, Switzerland
Aythami Morales Biometrics and Data Pattern Analytics—BiDA Lab, Universidad Autonoma de Madrid, Spain
Mark S. Nixon University of Southampton, UK
Jonathan Phillips NIST, USA
Hugo Proenca University of Beira Interior, Instituto de Telecomunica coes, Portugal
Kiran B. Raja Norwegian Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Norway
Raghavendra Ramachandra Norwegian Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Norway
Arun Ross Michigan State University, USA
Md Sahidullah MULTISPEECH, Inria, France
Richa Singh IIIT-Delhi, India
Juan Eduardo Tapia Farias, Hochschule Darmstadt, Germany
Massimiliano Todisco Department of Digital Security, EURECOM, France
Ruben Tolosana Biometrics and Data Pattern Analytics—BiDA Lab, Universidad Autonoma de Madrid, Spain
You Zhang University of Rochester, USA

Contents

Contributors

(Andy) Fang Zhaoyuan University of Notre Dame, Notre Dame, IN, USA

Becker Benedict University of Notre Dame, Notre Dame, USA

Boutros Fadi Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany

Bowyer Kevin Notre Dame University, Notre Dame, IN, USA

Boyd Aidan University of Notre Dame, Notre Dame, IN, USA

Busch Christoph da/sec - Biometrics and Internet-Security Research Group, Hochschule Darmstadt and ATHENE (National Research Center for Applied Cybersecurity), Darmstadt, Germany;
Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

Cappelli Raffaele Università di Bologna, Cesena, Italy

Casula Roberto University of Cagliari, Cagliari, Italy

Chen Xinhui Lehigh University, Bethlehem, USA

Cheng Xingliang Tsinghua University, Beijing, China

Czajka Adam University of Notre Dame, Notre Dame, IN, USA

Damer Naser Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany

Das Priyanka Clarkson University, Clarkson, NY, USA

Delgado Héctor Nuance Communications, Madrid, Spain

Duan Zhiyao University of Rochester, Rochester, USA

Engelsma Joshua J. Michigan State University, East Lansing, USA

Evans Nicholas Department of Digital Security, EURECOM (France), Biot, France

Fang Meiling Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany

Fierrez Julian School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain;
Biometrics and Data Pattern Analytics—BiDA Lab, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Madrid, Spain

Fontanillo López Cesar Augusto KU Leuven – Law Faculty – Citip – iMec, Leuven, Belgium

Galbally Javier eu-LISA / European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, Tallinn, Estonia;
European Commission, Joint Research Centre, Ispra, Italy

George Anjith Idiap Research Institute, Martigny, Switzerland

Gomez-Barrero Marta Hochschule Ansbach, Ansbach, Germany

Gonzalez-Garcia Carlos Biometrics and Data Pattern Analytics—BiDA Lab, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Madrid, Spain

Gonzalez-Soler Lazaro Janier da/sec - Biometrics and Internet-Security Research Group, Hochschule Darmstadt, Darmstadt, Germany

Hernandez-Ortega Javier School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain

Jiang Fei Tencent Technology Co., Ltd., Shenzhen, China

Johnson Alan University of Notre Dame, Notre Dame, USA

Kamble Madhu EURECOM, Biot, France

Kindt Els J. KU Leuven – Law Faculty – Citip – iMec, Leuven, Belgium

Kinnunen Tomi School of Computing, University of Eastern Finland (Finland), Joensuu, Finland

Kohli Naman West Virginia University, Morgantown, WV, USA

Komulainen Jukka University of Oulu, Oulu, Finland;
Visidon Ltd, Oulu, Finland

Lee Kong-Aik Institute for Infocomm Research, A*STAR (Singapore), Singapore, Singapore

Li Lantian Tsinghua University, Beijing, China

Li Xiaobai Center for Machine Vision and Signal Analysis, University of Oulu, Oulu, Finland

Linortner Michael Department of Computer Science, University of Salzburg, Salzburg, Austria

Liu Si-Qi Department of Computer Science, Hong Kong Baptist University, Kowloon, Hong Kong

Maciejewicz Piotr Medical University of Warsaw, Warsaw, Poland

Marcel Sébastien IDIAP Research Institute, Martigny, Switzerland

Marcialis Gian Luca Università di Cagliari, Cagliari, Italy

McGrath Joseph University of Notre Dame, Notre Dame, IN, USA

Micheletto Marco University of Cagliari, Cagliari, Italy

Mohammadi Amir IDIAP Research Institute, Martigny, Switzerland

Morales Aythami School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain

Namboodiri Anoop IIIT Hyderabad, Hyderabad, India

Nautsch Andreas Department of Digital Security, EURECOM (France), Biot, France

Noore Afzel Texas A &M University-Kingsville, Kingsville, TX, USA

Orrù Giulia University of Cagliari, Cagliari, Italy

Ortega-Garcia Javier Biometrics and Data Pattern Analytics—BiDA Lab, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Madrid, Spain

Patino Jose EURECOM, Biot, France

Poiret Eric IDEMIA, Paris, France

Popli Additya IIIT Hyderabad, Hyderabad, India

Raja Kiran Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

Ramachandra Raghavendra Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

Rathgeb Christian da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, Darmstadt, Germany

Sahidullah Md Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

Schuckers Stephanie Clarkson University, Clarkson, NY, USA

Schuiki Johannes Department of Computer Science, University of Salzburg, Salzburg, Austria

Singh Richa Department of CSE, IIT Jodhpur, Jodhpur, RJ, India

Stokkenes Martin Norwegian University of Science and Technology, Gjøvik, Norway

Tandon Saraansh IIIT Hyderabad, Hyderabad, India

Todisco Massimiliano Department of Digital Security, EURECOM (France), Biot, France

Tolosana Ruben Biometrics and Data Pattern Analytics—BiDA Lab, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Madrid, Spain

Trokielewicz Mateusz Warsaw University of Technology, Warsaw, Poland

Uhl Andreas Department of Computer Science, University of Salzburg, Salzburg, Austria

Vatsa Mayank Department of CSE, IIT Jodhpur, Jodhpur, RJ, India

Venkatesh Sushma Norwegian University of Science and Technology, Gjøvik, Norway;
Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Trondheim, Norway;
da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, Darmstadt, Germany;
Hochschule Ansbach, Ansbach, Germany

Vera-Rodriguez Ruben Biometrics and Data Pattern Analytics—BiDA Lab, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Madrid, Spain

Wang Dong Tsinghua University, Beijing, China

Wang Xin National Institute of Informatics (Japan), Tokyo, Japan

Wasnik Pankaj Norwegian University of Science and Technology, Gjøvik, Norway

Wimmer Georg Department of Computer Science, University of Salzburg, Salzburg, Austria

Xu Mingxing Tsinghua University, Beijing, China

Yadav Daksha West Virginia University, Morgantown, WV, USA

Yamagishi Junichi National Institute of Informatics (Japan), Tokyo, Japan

Yambay David Clarkson University, Clarkson, NY, USA

Yu Zitong Center for Machine Vision and Signal Analysis, University of Oulu, Oulu, Finland

Yuen Pong C. Department of Computer Science, Hong Kong Baptist University, Kowloon, Hong Kong

Zhang You University of Rochester, Rochester, USA

Zhao Guoying Center for Machine Vision and Signal Analysis, University of Oulu, Oulu, Finland

Zheng Thomas Fang Tsinghua University, Beijing, China

Zhu Ge University of Rochester, Rochester, USA

Part I
Fingerprint Biometrics

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[1] 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 (✉)
Università di Cagliari, Cagliari, Italy
e-mail: marcialis@unica.it

S. Marcel et al. (eds.), *Handbook of Biometric Anti-Spoofing*, Advances in Computer Vision and Pattern Recognition, https://doi.org/10.1007/978-981-19-5288-3_1

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 is 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

[2] https://www.iarpa.gov/index.php/research-programs/odin/.

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 fingertip 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

[3] https://www.iarpa.gov/index.php/research-programs/odin/.

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 improvement 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] http://livdet.diee.unica.it.

[5] http://people.clarkson.edu/projects/biosal/fingerprint/index.php.

[6] http://biometrics.eps.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 TRESPASS-ETN. This work was also partially supported by the Spanish project BIBECA (RTI2018-101248-B-I00 MINECO/FEDER).

References

1. van der Putte T, Keuning J (2000) Biometrical fingerprint recognition: don't get your fingers burned. In: Proceedings IFIP conference on smart card research and advanced applications, pp 289–303
2. Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2002) Impact of artificial gummy fingers on fingerprint systems. In: Proceedings of SPIE optical security and counterfeit deterrence techniques IV, vol 4677, pp 275–289
3. Thalheim L, Krissler J (2002) Body check: biometric access protection devices and their programs put to the test. ct magazine, pp 114–121
4. Sousedik C, Busch C (2014) Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biom 3:219–233(14). http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2013.0020
5. Derakhshani R, Schuckers S, Hornak L, O'Gorman L (2003) Determination of vitality from non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognit 36:383–396
6. Antonelli A, Capelli R, Maio D, Maltoni D (2006) Fake finger detection by skin distortion analysis. IEEE Trans. Inf Forensics Secur 1:360–373
7. Galbally J, Alonso-Fernandez F, Fierrez J, Ortega-Garcia J (2012) A high performance fingerprint liveness detection method based on quality related features. Futur Gener Comput Syst 28:311–321
8. Franco A, Maltoni D (2008) Fingerprint synthesis and spoof detection. In: Ratha NK, Govindaraju V (eds) Advances in biometrics: sensors, algorithms and systems. Springer, pp 385–406
9. Li SZ (ed) (2009) Encyclopedia of biometrics. Springer
10. Coli P (2008) Vitality detection in personal authentication systems using fingerprints. PhD thesis, Universita di Cagliari
11. Sandstrom M (2004) Liveness detection in fingerprint recognition systems. Master's thesis, Linkoping University
12. Lane M, Lordan L (2005) Practical techniques for defeating biometric devices. Master's thesis, Dublin City University
13. Blomme J (2003) Evaluation of biometric security systems against artificial fingers. Master's thesis, Linkoping University
14. Lapsley P, Less J, Pare D, Hoffman N (1998) Anti-fraud biometric sensor that accurately detects blood flow 5(737):439
15. Setlak DR (1999) Fingerprint sensor having spoof reduction features and related methods 5(953):441

16. Kallo I, Kiss A, Podmaniczky JT (2001) Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus 6(175):64
17. Diaz-Santana E, Parziale G (2008) Liveness detection method. EP1872719
18. Kim, J., Choi, H., Lee, W.: Spoof detection method for touchless fingerprint acquisition apparatus (2011). 1054314
19. Centro Criptologico Nacional (CCN) (2011) Characterizing attacks to fingerprint verification mechanisms CAFVM v3.0. Common Criteria Portal
20. Bundesamt fur Sicherheit in der Informationstechnik (BSI) (2008) Fingerprint spoof detection protection profile FSDPP v1.8. Common Criteria Portal
21. Ghiani L, Yambay DA, Mura V, GLM, Roli F, Schuckers S (2017) Review of the fingerprint liveness detection (livdet) competition series: 2009 to 2015. Image Vis Comput 58:110–128. https://doi.org/10.1016/j.imavis.2016.07.002
22. Casula R, Micheletto M, Orrù G, Delussu R, Concas S, Panzino A, Marcialis G (2021) Livdet 2021 fingerprint liveness detection competition – into the unknown. In: Proceedings of international joint conference on biometrics (IJCB 2021). https://doi.org/10.1109/IJCB52358.2021.9484399
23. Orrù G, Tuveri P, Casula R, Bazzoni C, Dessalvi G, Micheletto M, Ghiani L, Marcialis G (2019) Livdet 2019 – fingerprint liveness detection competition in action 2019. In: Proceedings of IEEE/IAPR international conference on biometrics (ICB 2019). https://doi.org/10.1109/ICB45273.2019.8987281
24. Galbally J, Fierrez J, Alonso-Fernandez F, Martinez-Diaz M (2011) Evaluation of direct attacks to fingerprint verification systems. J Telecommun Syst, Special Issue of Biom Syst Appl 47:243–254
25. Abhyankar A, Schuckers S (2009) Integrating a wavelet based perspiration liveness check with fingerprint recognition. Pattern Recognit 42:452–464
26. Spinoulas L, Mirzaalian H, Hussein ME, AbdAlmageed W (2021) Multi-modal fingerprint presentation attack detection: evaluation on a new dataset. IEEE Trans Biom Behav Identity Sci 3:347–364. https://doi.org/10.1109/TBIOM.2021.3072325
27. Biometrics Institute (2011) Biometric Vulnerability Assessment Expert Group. http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expert-group-bvaeg.html
28. NPL (2010) National Physical Laboratory: Biometrics. http://www.npl.co.uk/biometrics
29. CESG (2001) Communications-Electronics Security Group - Biometric Working Group (BWG). https://www.cesg.gov.uk/policyguidance/biometrics/Pages/index.aspx
30. BEAT (2012) BEAT: Biometrices evaluation and testing. http://www.beat-eu.org/
31. Tabula Rasa (2010) Trusted biometrics under spoofing attacks (tabula rasa). http://www.tabularasa-euproject.org/
32. Maltoni D, Maio D, Jain A, Prabhakar S (2009) Handbook of fingerprint recognition. Springer
33. Cappelli R, Maio D, Lumini A, Maltoni D (2007) Fingerprint image reconstruction from standard templates. IEEE Trans Pattern Anal Mach Intell 29:1489–1503
34. Cappelli R (2009) Synthetic fingerprint generation. In: Handbook of fingerprint recognition. Springer, pp 270–302
35. Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition. IEEE Trans. Image Process 23(2):710–724. https://doi.org/10.1109/TIP.2013.2292332
36. Hadid A, Evans N, Marcel S, Fierrez J (2015) Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process Mag 32(5):20–30. https://doi.org/10.1109/MSP.2015.2437652
37. Marasco E, Ross A (2014) A survey on antispoofing schemes for fingerprint recognition systems. ACM Comput Surv 47(2). https://doi.org/10.1145/2617756
38. Sousedik C, Busch C (2014) Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biom 3(4):219–233. https://doi.org/10.1049/iet-bmt.2013.0020
39. Karampidis K, Rousouliotis M, Linardos E, Kavallieratou E (2021) A comprehensive survey of fingerprint presentation attack detection. J Surveill Secur Saf 2:117–61

40. Singh JM, Madhun A, Li G, Ramachandra R (2021) A survey on unknown presentation attack detection for fingerprint. In: Yildirim Yayilgan S, Bajwa IS, Sanfilippo F (eds) Intelligent technologies and applications. Springer International Publishing, Cham, pp 189–202
41. Wehde A, Beffel JN (1924) Fingerprints can be forged. Tremonia Publish Co
42. de Water MV (1936) Can fingerprints be forged? Sci News-Lett 29:90–92
43. Sengottuvelan P, Wahi A (2007) Analysis of living and dead finger impressions identification for biometric applications. In: Proceedings of international conference on computational intelligence and multimedia applications
44. Yoon S, Feng J, Jain AK (2012) Altered fingerprints: analysis and detection. IEEE Trans Pattern Anal Mach Intell 34:451–464
45. Willis D, Lee M (1998) Biometrics under our thumb. Netw Comput (1998). http://www.networkcomputing.com/
46. Sten A, Kaseva A, Virtanen T (2003) Fooling fingerprint scanners - biometric vulnerabilities of the precise biometrics 100 SC scanner. In: Proceedings of Australian information warfare and IT security conference
47. Wiehe A, Sondrol T, Olsen K, Skarderud F (2004) Attacking fingerprint sensors. NISlab, Gjovik University College, Technical report
48. Galbally J, Cappelli R, Lumini A, de Rivera GG, Maltoni D, Fierrez J, Ortega-Garcia J, Maio D (2010) An evaluation of direct and indirect attacks using fake fingers generated from ISO templates. Pattern Recognit Lett 31:725–732
49. Barral C, Tria A (2009) Fake fingers in fingerprint recognition: glycerin supersedes gelatin. In: Formal to practical security, LNCS 5458, pp 57–69
50. Parthasaradhi S, Derakhshani R, Hornak L, Schuckers S (2005) Time-series detection of perspiration as a liveness test in fingerprint devices. IEEE Trans Syst Man Cybernect - Part C: Appl Rev 35:335–343
51. Schuckers S, Abhyankar A (2004) A wavelet based approach to detecting liveness in fingerprint scanners. In: Proceedings of biometric authentication workshop (BioAW), LNCS-5404. Springer, pp 278–386
52. Tan B, Schuckers S (2006) Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners. In: Proceedings of SPIE biometric technology for human identification III (BTHI III), vol 6202, p 62020A
53. Tan B, Schuckers S (2008) A new approach for liveness detection in fingerprint scanners based on valley noise analysis. J Electron Imaging 17:011,009
54. DeCann B, Tan B, Schuckers S (2009) A novel region based liveness detection approach for fingerprint scanners. In: Proceedings of IAPR/IEEE international conference on biometrics, LNCS-5558. Springer, pp 627–636
55. NexIDBiometrics (2012). http://nexidbiometrics.com/
56. Abhyankar A, Schuckers S (2006) Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques. In: Proceedings of IEEE international conference on image processing (ICIP)
57. Marasco E, Sansone C (2010) An anti-spoofing technique using multiple textural features in fingerprint scanners. In: Proceedings of IEEE workshop on biometric measurements and systems for security and medical applications (BIOMS), pp 8–14
58. Marasco E, Sansone C (2012) Combining perspiration- and morphology-based static features for fingerprint liveness detection. Pattern Recognit Lett 33:1148–1156
59. Cappelli R, Maio D, Maltoni D (2001) Modelling plastic distortion in fingerprint images. In: Proceedings of international conference on advances in pattern recognition (ICAPR), LNCS-2013. Springer, pp 369–376
60. Bazen AM, Gerez SH (2003) Fingerprint matching by thin-plate spline modelling of elastic deformations. Pattern Recognit 36:1859–1867
61. Chen Y, Dass S, Ross A, Jain AK (2005) Fingerprint deformation models using minutiae locations and orientations. In: Proceedings of IEEE workshop on applications of computer vision (WACV), pp 150–156