Advances in Computer Vision and Pattern Recognition

More information about this series at http://www.springer.com/series/4205

Sébastien Marcel · Mark S. Nixon
Julian Fierrez · Nicholas Evans
Editors

Handbook of Biometric Anti-Spoofing

Presentation Attack Detection

Second Edition

Springer

Editors
Sébastien Marcel
Idiap Research Institute
Martigny, Switzerland

Julian Fierrez
Universidad Autonoma de Madrid
Madrid, Spain

Mark S. Nixon
University of Southampton
Southampton, UK

Nicholas Evans
EURECOM
Biot Sophia Antipolis, France

ISSN 2191-6586 ISSN 2191-6594 (electronic)
Advances in Computer Vision and Pattern Recognition
ISBN 978-3-319-92626-1 ISBN 978-3-319-92627-8 (eBook)
https://doi.org/10.1007/978-3-319-92627-8

Library of Congress Control Number: 2018957636

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

About 5 years ago, I had the privilege to write the Foreword for the first edition of the *Handbook of Biometric Anti-Spoofing*, edited by my good colleagues Sébastien Marcel, Mark S. Nixon, and Stan Z. Li. I was impressed with their work, and wrote that Foreword that there were four reasons that made it easy to envy what they accomplished with their Handbook. I will revisit those reasons below. I now have the privilege to write the Foreword to the second edition of the *Handbook of Biometric Anti-Spoofing*, which I enjoy even more than the first edition. The second edition is edited by good colleagues Sébastien Marcel, Mark S. Nixon, Julian Fierrez, and Nicholas Evans. The editorial team has expanded as the scope and ambition of the Handbook has expanded, and in my assessment, the editors have achieved an impressive final product.

In the Foreword to the first edition of the *Handbook of Biometric Anti-Spoofing*, I wrote that one reason to envy what the editors had accomplished is that they managed to envision a truly novel (at the time) theme for their Handbook. Theirs was the first Handbook that I am aware of to be dedicated to biometric anti-spoofing. As the advertising copy says "the first definitive study of biometric anti-spoofing". This distinction does not go away, but anti-spoofing—or "presentation attack detection" in the current lingo—is a fast-moving area of research and any work in this area can go out-of-date quickly. With the second edition, the coverage of the field has been brought up to date and also expanded to more comprehensive coverage of the field. As the scope and ambition of the field as a whole has grown, so has the scope and ambition of the Handbook.

In the Foreword to the first edition, I wrote that a second reason to envy the editors' accomplishment was that they anticipated an important emerging need. If this was not clear to the entire field 5 years ago, it certainly should be clear now. Biometric technologies continue to become more widely deployed, in consumer products such as the 3D face recognition in Apple's iPhone X, in business processes such as Yombu's fingerprint payment system, and in government applications such as Somaliland's use of iris recognition to create their national voter registration list. With bigger, broader and higher value applications, presentation attacks of more creative varieties are certain to be attempted. The need for an authoritative, broad coverage volume detailing the current state of the art in biometric anti-spoofing has only increased since the first edition, and the second edition fulfills this need.

The third reason that I outlined in the previous Foreword was that the editors had "timed the wave" well; they were on the early leading edge of the wave of popularity of research in anti-spoofing. With the second edition, I believe that they are again on the leading edge of a wave that is still to crest. I can imagine that the CTO of every business integrating biometric identity verification into one of their processes will want to study this Handbook carefully. As well, researchers wanting to begin activity in this area will find this Handbook a great place to start.

The fourth reason that I outlined previously was that the editors' efforts had resulted in a quality product. Now, to these four reasons enumerated in the Foreword to the first edition, I must add a fifth reason specific to the second edition—the editors have evolved and updated the material in a big way, and the result is that they have produced an even better, more comprehensive and more useful second edition of the *Handbook of Biometric Anti-Spoofing*.

Whereas the first edition comprised 13 chapters, the second edition has grown to 22 chapters! And the editors have been bold, and not taken the path of least resistance. They did not automatically keep a chapter corresponding to each chapter in the first edition, but instead both dropped some topics and added new topics. Where the first edition had two chapters dealing with fingerprint, two with face, and one each on iris, gait, speaker, and multimodal biometrics, the second edition has six (!) chapters dealing with face, five with fingerprint, three with iris, three with voice, and one each dealing with vein and signature. There is also coverage of the major presentation attack competitions, and of the major databases available for research. The second edition being very much up to date and globally aware, there is even a discussion of presentation attack detection and how it may be handled under the EU's new General Data Protection Regulation (GDPR). And with every chapter, the contributors are authorities on the topic, having recently published specific state-of-the-art research of their own on the topic. The editorial team has made quite significant and impressive efforts at recruiting contributors to accomplish the expansion and updating of material for the second edition.

The second edition of the *Handbook of Biometric Anti-Spoofing* by Sébastien Marcel, Mark S. Nixon, Julian Fierrez, and Nicholas Evans is the new standard in authoritative and comprehensive coverage of the current state of the art in biometric presentation attack detection. As biometric technology continues to be adapted in new large-scale applications, the wave of research attention to presentation attack detection will continue to grow. We can only hope that the editors will return in a few years with a third edition that continues in the tradition that they have set with the first two.

Notre Dame, IN, USA
July 2018

Prof. Kevin W. Bowyer
Editor-In-Chief
IEEE Transactions on Biometrics,
Behavior and Identity Science
Schubmehl-Prein Family Professor of
Computer Science and Engineering
University of Notre Dame

Preface

In the 4 years since 2014 when the TABULA RASA[1] project ended,[2] and the first edition of this Handbook was published,[3] the field of biometric anti-spoofing (term now standardized as biometric Presentation Attack Detection—PAD) has advanced significantly with large-scale industrial application. As these applications continue to grow in scale, the number of research challenges and technology requirements are also increasing significantly. The importance of the topic and the related research needs are confirmed by new highly funded research programs like the IARPA ODIN program initiated in 2016 and ongoing, aimed at advancing PAD technologies to identify known and unknown biometric presentation attacks.

The field of biometric PAD has matured significantly since the first edition, with a growing number of research groups working in the topic, various benchmarks and tools now commonly used and shared among researchers, technology competitions, and standardization activities. With the aim of updating our first edition published in 2014, heavily focused then on the research within the TABULA RASA project, we initiated this second edition in 2017 in an Open Call aiming to represent a more up-to-date and comprehensive picture of the current state of the art. We received 25 Expressions of Interest for contributions to the book, which after review resulted in a final set of 22 chapters. We are very grateful both to the authors and to the reviewers, who are listed separately.

We also thank the support provided by Springer, with special thanks to Simon Rees, who similar to the first edition has helped significantly towards this second edition.

As the body of knowledge in biometric PAD is growing in the recent years, the volume and contents in this second edition have increased significantly with respect to the first edition. Additionally, this field is attracting the interest of a growing

[1] Trusted Biometrics under Spoofing Attacks—http://www.tabularasa-euproject.org.

[2] A. Hadid, N. Evans, S. Marcel and J. Fierrez, "Biometrics systems under spoofing attack: an evaluation methodology and lessons learned", IEEE Signal Processing Magazine, September 2015.

[3] S. Marcel, M. S. Nixon and S. Z. Li (Eds.), Handbook of Biometric Anti-Spoofing, Springer, 2014.

number of people: from researchers to practitioners, from students to advanced researchers, and from engineers to technology consultants and marketers. In order to be useful to a wider spectrum of readers, in this second edition, we have included a number of introductory chapters for the most important biometrics. Those introductory chapters can be skipped by readers knowledgeable in the basics of biometric PAD.

With the mindset of helping researchers and practitioners, and speeding up the progress in this field, we asked authors of experimental chapters to comply with two requirements related to Reproducible Research:

- experiments are conducted on publicly available datasets;
- system scores generated with proposed PAD methods are openly available.

Additionally, some chapters and more particularly chapters 2, 4, 7, 11, 12, 13, 16, 17, 18, 19 and 20, also include code for generating performance plots and figures, open source codes for the presented methods, and detailed instructions on how to reproduce the reported results. All this Reproducible Research material is available here: https://gitlab.idiap.ch/biometric-resources.

As researchers in the field for many years, we trust you find this text of use as guidance and as reference in a topic that will continue to inspire and challenge many researchers.

Martigny, Switzerland Sébastien Marcel
Southampton, England Mark S. Nixon
Madrid, Spain Julian Fierrez
Biot Sophia Antipolis, France Nicholas Evans
July 2018

List of Reviewers

Zahid Akhtar, INRS-EMT, University of Quebec, Canada
Jos 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
Adam Czajka, University of Notre Dame, USA
Héctor Delgado, EURECOM, France
Nesli Erdogmus, Izmir Institute of Technology, Turkey
Nicholas Evans, EURECOM, France
Jiangjiang Feng, Tsinghua University, China
Julian Fierrez, Universidad Autonoma de Madrid, Spain
Javier Galbally, European Commission, Joint Research Centre, Italy
Anjith George, Idiap Research Institute, Switzerland
Luca Ghiani, University of Cagliari, Italy
Marta Gomez-Barrero, Hochschule Darmstadt, Germany
Abdenour Hadid, University of Oulu, Finland
Guillaume Heusch, Idiap Research Institute, Switzerland
Ivan Himawan, Queensland University of Technology, Brisbane, Australia
Els J. Kindt, KU Leuven, Belgium
Tomi Kinnunen, University of Eastern Finland, Finland
Jukka Komulainen, University of Oulu, Finland
Stan Z. Li, Chinese Academy of Sciences, China
Sébastien Marcel, Idiap Research Institute, Switzerland
Gian Luca Marcialis, University of Cagliari, Italy
Amir Mohammadi, Idiap Research Institute, Switzerland
Mark S. Nixon, University of Southampton, UK
Jonathan Phillips, NIST, USA
Hugo Proenca, University of Beira Interior, Portugal
Kiran B. Raja, Norwegian University of Science and Technology, Norway
Raghavendra Ramachandra, Norwegian University of Science and Technology, Norway

Arun Ross, Michigan State University, USA
Md Sahidullah, Inria, France
Richa Singh, IIIT-Delhi, India
Massimiliano Todisco, EURECOM, France

Contents

Part III Face Biometrics

Part IV Voice Biometrics

Contributors

Zahid Akhtar INRS-EMT, University of Quebec, Quebec City, Canada

José Luis Alba-Castro Universidade de Vigo, Vigo, Spain

André Anjos Biometrics Security and Privacy Group, Idiap Research Institute, Martigny, Switzerland

Benedict Becker University of Notre Dame, Notre Dame, IN, USA

Sushil Bhattacharjee Biometrics Security and Privacy Group, Idiap Research Institute, Martigny, Switzerland

Zinelabidine Boulkenafet Center for Machine Vision and Signal Analysis, University of Oulu, Oulu, Finland

Kevin Bowyer Notre Dame University, Notre Dame, IN, France

Christoph Busch Hochschule Darmstadt and CRISP (Center for Research in Security and Privacy), Darmstadt, Germany; Norwegian Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

Raffaele Cappelli Università di Bologna, Cesena, Italy

Milos Cernak Logitech, Lausanne, Switzerland

Ivana Chingovska Idiap Research Institute, Martigny, Switzerland

Artur Costa-Pazo GRADIANT, CITEXVI, Vigo, Spain

Adam Czajka Research and Academic Computer Network (NASK), Warsaw, Poland; University of Notre Dame, Notre Dame, IN, USA; Warsaw University of Technology, Warsaw, Poland

Luke Darlow Council for Scientific and Industrial Research, Pretoria, South Africa

Héctor Delgado Department of Digital Security, EURECOM, Biot Sophia Antipolis, France

Nicholas Evans Department of Digital Security, EURECOM, Biot Sophia Antipolis, France

Julian Fierrez Universidad Autonoma de Madrid, Madrid, Spain

Clinton Fookes Queensland University of Technology, Brisbane, Australia

Javier Galbally European Commission - DG Joint Research Centre, Ispra, Italy

Luca Ghiani Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy

Marta Gomez-Barrero da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, Darmstadt, Germany

Daniel González-Jiménez GRADIANT, CITEXVI, Vigo, Spain

Javier Hernandez-Ortega Biometrics and Data Pattern Analytics - BiDA Lab, Universidad Autonoma de Madrid, Madrid, Spain

Guillaume Heusch Idiap Research Institute, Martigny, Switzerland

Ivan Himawan Queensland University of Technology, Brisbane, Australia

Els J. Kindt KU Leuven – Law Faculty – Citip – iMec, Leuven, Belgium; Universiteit Leiden - Law Faculty - eLaw, Leiden, The Netherlands

Tomi Kinnunen School of Computing, University of Eastern Finland, Kuopio, Finland

Naman Kohli West Virginia University, Morgantown, WV, USA

Jukka Komulainen Center for Machine Vision and Signal Analysis, University of Oulu, Oulu, Finland

Pavel Korshunov Idiap Research Institute, Martigny, Switzerland

Kong-Aik Lee Data Science Research Laboratories, NEC Corporation (Japan), Tokyo, Japan

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

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

Srikanth Madikeri Idiap Research Institute, Martigny, Switzerland

Sébastien Marcel Biometrics Security and Privacy Group, Idiap Research Institute, Martigny, Switzerland

Gian Luca Marcialis Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari CA, Italy

Amir Mohammadi Biometrics Security and Privacy Group, Idiap Research Institute, Martigny, Switzerland

Yaseen Moolla Council for Scientific and Industrial Research, Pretoria, South Africa

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

Petr Motlicek Idiap Research Institute, Martigny, Switzerland

V. Mura Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy

Afzel Noore West Virginia University, Morgantown, WV, USA

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

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

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

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

Fabio Roli Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari CA, Italy

Md Sahidullah School of Computing, University of Eastern Finland, Kuopio, Finland

Stephanie Schuckers Clarkson University, Potsdam, NY, USA

Ameeth Sharma Council for Scientific and Industrial Research, Pretoria, South Africa

Ann Singh Council for Scientific and Industrial Research, Pretoria, South Africa

Richa Singh IIIT-Delhi Okhla Industrial Estate, New Delhi, India

Sridha Sridharan Queensland University of Technology, Brisbane, Australia

Massimiliano Todisco Department of Digital Security, EURECOM, Biot Sophia Antipolis, France

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

Pedro Tome Universidad Autonoma de Madrid, Madrid, Spain

Pierliugi Tuveri Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy

Johan van der Merwe Council for Scientific and Industrial Research, Pretoria, South Africa

Mayank Vatsa IIIT-Delhi Okhla Industrial Estate, New Delhi, India

Esteban Vazquez-Fernandez GRADIANT, CITEXVI, Vigo, Spain

Sushma Venkatesh Norwegian Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

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

Daksha Yadav West Virginia University, Morgantown, WV, USA

Junichi Yamagishi National Institute of Informatics, Tokyo, Japan; University of Edinburgh, Edinburgh, Scotland

David Yambay Clarkson University, Potsdam, NY, USA

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

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

Mikel Zurutuza Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy