Advances in Computer Vision and Pattern Recognition

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

Sébastien Marcel · Mark S. Nixon
Stan Z. Li
Editors

Handbook of Biometric Anti-Spoofing

Trusted Biometrics under Spoofing Attacks

Springer

ISSN 2191-6586 ISSN 2191-6594 (electronic)
ISBN 978-1-4471-6523-1 ISBN 978-1-4471-6524-8 (eBook)
DOI 10.1007/978-1-4471-6524-8

Library of Congress Control Number: 2014942635

Springer London Heidelberg New York Dordrecht

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

Hollywood has long and richly enjoyed depicting biometric spoofing. As early as 1971, in the movie *Diamonds Are Forever*, Sean Connery's James Bond character uses a fake fingerprint attached to his fingertip to convince a woman of his assumed identity. In the movie RED, Bruce Willis' retired CIA agent character uses a custom contact lens to spoof an eye scanner and break into CIA headquarters. In the movie, the scanner is called a retinal scanner, but it clearly images the iris rather than the retina. We should not press Hollywood too much for technical accuracy! In the film *Charlie's Angels: Full Throttle*, Cameron Diaz's character uses a custom contact lens and fake fingerprints to fool a multi-modal biometric scanner and break into the bad-guy corporate headquarters. Anyone working in biometrics can probably supply several more of their favorite such biometric spoofing scenes.

In the most general sense, biometric spoofing can be defined as the deliberate attempt to create an error in a biometric system, either a false match or a false non-match. This typically involves presenting a biometric sample to the system that does not truly correspond to the person presenting it. The person committing the spoof either wants simply to avoid being recognized as their true identity, or wants to be recognized as a some specific chosen identity that is not their own. In the most general sense, then, anti-spoofing is about detecting the presence of biometric samples that are not a true representation of the person presenting the sample. The term "liveness detection" is used to refer to anti-spoofing methods that are based on determining if the sensor is imaging a "live" sample, as opposed to a gummy finger, a textured contact lens, a video of a face, or some other non-live sample.

It is easy to envy what Stan Z. Li, Mark Nixon, and Sébastien Marcel have accomplished with their *Handbook on Biometric Anti-Spoofing*. One reason is that they managed to envision a truly novel theme for their handbook. There are of course many recent books on various themes in biometrics, and more appearing all the time. After all, biometrics is a hot area for both research and application. Some of the books have a chapter devoted to spoofing attacks of one kind or another, but it is not common to have even one chapter devoted to anti-spoofing methods. And while any new spoofing attack tends to attract attention and publicity, it is the

anti-spoofing methods that are more important to the "good guys." Thus, it is significant that Professors Li, Nixon, and Marcel have realized the first book devoted entirely to anti-spoofing methods in biometrics.

A second reason to envy their accomplishment is that I believe Professors Li, Nixon, and Marcel have anticipated an important emerging need. There is now a good amount of solid research on anti-spoofing methods. But it is spread out in the literature of the various biometrics modalities. It is rather difficult for one person to keep abreast of it all. And there is not yet, until this book, and attempt to pull things together and make connections and leverage commonalities between anti-spoofing concepts developed in the context of different modalities. So there is a good opportunity for a whole-is-greater-than-the-sum-of-the-parts effect in this instance.

A third reason is that I judge Professors Li, Nixon, and Marcel to have also timed the wave of need just about right. Large-scale biometric applications are being deployed in many countries around the world. And many of these applications—India's Aadhaar being a prime example—have serious implications for commerce. The old saying about the criminal Willie Sutton was that he robbed banks because that is where the money was. In the same way, as biometrics becomes the means of identity verification for commerce, we can expect the frequency and intensity of spoofing attacks to increase. A news article that appeared just this month ran with the title, "Crime of the Future—Biometric Spoofing?" [1]. Everyone working in the area of biometrics can appreciate that this title may be destined to be more true than we would like. So the biometrics research community needs to increase the amount of attention paid to anti-spoofing methods. This book will serve as the introduction to the topic for biometrics professionals who must come up to speed on the area.

A fourth reason is that the labors of Professors Li, Nixon, and Marcel have resulted in a quality product. They have well covered the breadth of biometric modalities. The depth of the material covered is state of the art, due to Professors Li, Nixon, and Marcel having solicited contributions from accomplished researchers throughout the world. The core technical contributions are placed in the broader context by additional chapters dealing with essential issues such as evaluation methodologies, databases, standards, and legal concerns.

And so the final result is the *Handbook of Biometric Anti-Spoofing*. It is the only book on this important theme. It arrives at just the time that the need for it should be apparent to all in the biometrics community. And it is a well-executed concept, collecting together chapters of quality material authored by leading experts, and covering all the major topics and issues.

As mentioned, Professors Li, Nixon, and Marcel have solicited chapters that well cover the breadth of different biometric modalities. There are two chapters on fingerprint spoofing, from the forensic viewpoint and the biometric viewpoint, by Christophe Champod and Marcela Espinoza, and by Javier Galbally and coworkers, respectively. There are also two chapters on face anti-spoofing, covering a visual approach and a multi-spectral imaging approach, by André Anjos and coworkers, and by Dong Yi and co-workers, respectively. Iris anti-spoofing is

covered by Zhenan Sun and Tieniu Tan, who have done some of the pioneering work in the area. Voice anti-spoofing is covered by Nick Evans and coworkers, gait anti-spoofing by the John Bustard and coworkers, and multi-modal anti-spoofing by Giorgio Fumera and coworkers. In addition to broad coverage of anti-spoofing techniques for various major biometric modalities, this book also includes chapters on important general topics. Nesli Erdoğmus and Sébastien Marcel set the stage early in the book with a general overview of biometric spoofing attacks. Ivana Chingovska and coworkers cover the important topic of how to evaluate the effectiveness of anti-spoofing methods. Christoph Busch discusses the topic of standards related to anti-spoofing methods. Els Kindt addresses the topic of legal issues related to anti-spoofing. And, finally, Stan Z. Li summarizes the evaluation databases that are currently available.

I take it as a confirmation of the comprehensive and authoritative approach that Professors Li, Nixon, and Marcel have taken that their Handbook includes a chapter covering evaluation methodologies. In our own experience working on iris anti-spoofing methods at the University of Notre Dame, we found that coming to the right view of how to evaluate the accuracy of an anti-spoofing method can be difficult. In our initial work, we happily evaluated the accuracy of algorithms to detect textured contact lenses using a person-disjoint, ten-fold cross-validation. This is, after all, the standard approach for evaluation of biometric algorithms. Using this approach to evaluation, any of a variety of classifiers trained with local-binary-pattern feature vectors could achieve highly accurate detection of textured contact lenses. But when it occurred to us to ask what would happen if the textured lenses in the test partition were from a manufacturer whose lenses were not represented in the training data, the results were much lower on average and highly variable with the specific lens manufacturer represented in the test partition [2]. This illustrates how the area of biometric anti-spoofing is a specialized and difficult subarea of biometrics research.

The *Handbook of Biometric Anti-Spoofing* edited by Professors Li, Nixon, and Marcel is a valuable addition to the biometrics research literature. It brings a needed focus to a theme that is certain to grow in interest and importance. I predict that the *Handbook of Biometric Anti-Spoofing* will prove quite popular, and that it will not be long before several additional books imitating this theme appear.

Notre Dame, Indiana, USA, November 2013 Kevin W. Bowyer

References

1. Crime of the future—biometric spoofing? (2013) http://www.zdnet.com/crime-of-the-future-biometric-spoofing-2039376855/. Accessed 11 Nov 2013
2. Doyle JS, Bowyer KW, Flynn PJ (2013) Variation in accuracy of textured contact lens detection based on iris sensor and contact lens manufacturer. In: IEEE international conference on biometrics: theory, applications and systems (BTAS 13), Sept 30–Oct 2

Preface

In its short history, biometrics has developed very fast and is now used to enrol entire populations. As Kevin Bowyer's Foreword points out, the motivation of spoofing such systems is natural and must be expected. Under the leadership of Sébastien Marcel, the EU-funded seventh Framework Research Programme: Trusted Biometrics under Spoofing Attacks (TABULA RASA) was aimed to be the first concerted research program that addressed this issue. The TABULA RASA team was formed of an international set of researchers from Switzerland, Italy, Finland, France, UK, Spain, and China who addressed the main biometric modalities, many of which feature within the chapters that follow. The program included industrial partners and their demonstration and commercial material is less suited to inclusion with a text, though their contribution to the research program's success was enormous.

The publisher now with the largest coverage of biometrics is Springer. Those attending any of the major conferences that includes biometrics will have met Wayne Wheeler and so our gratitude remains for his early enthusiasm of this project. Of late, Simon Rees has been very patient while we reach the final stages of the book. We regret that delay appears innate to edited texts, though this can lead to greater polish in the result.

As such, with many thanks to many people: the authors, the reviewers, and the technical staff, here you will find the first consolidated text that addresses biometric anti-spoofing. It has been a great pleasure to work with the TABULA RASA teams during the past 4 years; it has been a great pleasure to work in biometrics for this is a technology that will continue to mature as it offers the solutions to many of the problems faced by modern society. As researchers in the field we trust you find this text of use as guidance and as reference in a field which will continue to inspire and challenge its many researchers.

Switzerland, May 2014 — Sébastien Marcel
England — Mark S. Nixon
China — Stan Z. Li

Acknowledgments

The editors would like to thank the TABULA RASA (www.tabularasa-euproject.org) and BEAT projects (www.beat-eu.org) funded under the seventh Framework Programme of the European Union (EU) (grant agreement numbers 257289 and 284989) for financial support.

Contents

Contributors

Federico Alegre Department of Multimedia Communications, Campus Sophia-Tech, EURECOM, Biot, France

André Anjos Idiap Research Institute, Martigny, Switzerland

Battista Biggio Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy

Christoph Busch Fraunhofer IGD, Darmstadt, Germany

John D. Bustard University of Southampton, Southampton, UK

Raffaele Cappelli Biometric Systems Laboratory (BioLab), Universit‘a di Bologna, Bologna, Italy

John N. Carter University of Southampton, Southampton, UK

Christophe Champod Faculty of Law and Criminal Justice, School of Criminal Justice, Institute of Forensic Science, University of Lausanne, Lausanne, Switzerland

Ivana Chingovska Idiap Research Institute, Martigny, Switzerland

Phillip De Leon Department 3-O, Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM, USA

Nesli Erdoğmuş Idiap Research Institute, Martigny, Switzerland

Marcela Espinoza Faculty of Law and Criminal Justice, School of Criminal Justice, Institute of Forensic Science, University of Lausanne, Lausanne, Switzerland

Nicholas Evans Department of Multimedia Communications, Campus Sophia-Tech, EURECOM, Biot, France

Julian Fierrez Biometric Recognition Group—ATVS, Universidad Autonoma de Madrid, Madrid, Spain

Giorgio Fumera Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy

Javier Galbally Biometric Recognition Group—ATVS, Universidad Autonoma de Madrid, Madrid, Spain

Mohammad Ghahramani Pentti Kaiteran katu 1, Oulu, Finland

Abdenour Hadid Pentti Kaiteran katu 1, Oulu, Finland; Center for Machine Vision Research (CMV), Department of Computer Science and Engineering (CSE), University of Oulu, Oulu, Finland

Els J. Kindt KU Leuven, Leuven, Belgium

Tomi Kinnunen Speech and Image Processing Unit, School of Computing, University of Eastern Finland (UEF), Joensuu, Finland

Jukka Komulainen Center for Machine Vision Research (CMV), Department of Computer Science and Engineering (CSE), University of Oulu, Oulu, Finland

Zhen Lei Chinese Academy of Sciences, Institute of Automation, Beijing, China

Stan Z. Li Chinese Academy of Sciences, Institute of Automation, Beijing, China

Sébastien Marcel Idiap Research Institute, Martigny, Switzerland

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

Mark S. Nixon University of Southampton, Southampton, UK

Javier Ortega-Garcia Biometric Recognition Group—ATVS, Universidad Autonoma de Madrid, Madrid, Spain

Matti Pietikäinen Center for Machine Vision Research (CMV), Department of Computer Science and Engineering (CSE), University of Oulu, Oulu, Finland

Andrew P. Rebera Independent Scholar, 7, Albert Road, Keynsham, UK

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

Stephanie Caswell Schuckers Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA

Zhenan Sun Center for Research on Intelligent Perception and Computing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, P.R. China

Tieniu Tan Center for Research on Intelligent Perception and Computing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, P.R. China

Zhizheng Wu Emerging Research Lab, School of Computer Engineering, Nanyang Technological University (NTU), Singapore, Singapore

Junichi Yamagishi National Institute of Informatics, Chiyoda-ku, Tokyo, Japan; University of Edinburgh, Edinburgh, UK

Dong Yi Chinese Academy of Sciences, Institute of Automation, Beijing, China

Zhiwei Zhang Chinese Academy of Sciences, Institute of Automation, Beijing, China