Julian Ashbourn

Practical Biometrics

From Aspiration to Implementation

Second Edition

Springer

Practical Biometrics

Julian Ashbourn

Practical Biometrics

From Aspiration to Implementation

Second Edition

Springer

Julian Ashbourn
Biometrics Research
Berkhamsted, Hertfordshire, UK

ISBN 978-1-4471-6716-7 ISBN 978-1-4471-6717-4 (eBook)
DOI 10.1007/978-1-4471-6717-4

Library of Congress Control Number: 2015937622

Springer London Heidelberg New York Dordrecht

Printed on acid-free paper

Springer-Verlag London Ltd. is part of Springer Science+Business Media (www.springer.com)

This book is dedicated to all those who have struggled to find practical and socially acceptable ways of implementing biometric identity verification techniques upon a large scale. It is further dedicated to all the users who will be exposed to the many variations of biometric identity verification in the coming years and their inevitable curiosity as to what is actually happening behind the scenes and why.

"Julian Ashbourn has done a masterful job of presenting a holistic approach for incorporating biometrics technologies into new or existing systems in "Practical Biometrics." A renowned authority within the global biometric community, Julian's perspectives inspire us to realize what "should be done" versus what "could be done." He brings foresight and ethics to the table of mathematicians, scientists, engineers, and application owners to challenge us to ensure positive societal impacts of the use of artificially intelligent technologies – in particular, biometrics. Using the "BANTAM" methodology, Julian informs how biometrics might be deployed in everyday situations. In accordance with the guidance given in "Practical Biometrics," application developers and product designers/developers will optimize successful biometrics integration. I encourage readers to consider Julian's guidance and look forward to his future insights and recommendations."

Cynthia Musselman, Musselman's Authentication SMEs.

Foreword

It is an honour and a pleasure to comment on this second edition of *Practical Biometrics*. Julian Ashbourn provided us in 2006 with a very helpful book, but after nearly a decade, a second edition is badly needed. This is partly due to changing technology, but also because of changing user needs and behaviour and evolving social factors and conditions. Although much has changed since the appearance of the first edition, the gap between what biometrics should contribute towards a safer society and its actual contribution has only been getting wider and deeper.

What hasn't changed, though, is the fact that biometrics is our one and only means of recognising people making use of a person's individual physical characteristics. Most current admission and security systems are based on the use of administrative data that are not physically linked to the person involved. Even in the security business, many people do not realise on a daily basis that we have no defence against what I call *the wrong person*: we only tend to check whether the data provided corresponds with a token, a user name and any other code or password in our system. We then unthinkingly assume the person to be the right one. Thus, biometrics are indispensable for a safe society.

But the concept of biometrics also confronts us with some confusing concepts that are difficult to change:

Firstly, in the context of biometrics we often use the concept of identity verification without realising that this precisely is what biometrics cannot do! Recognising people is not more than a precondition for establishing someone's identity based on other data and documents. In addition, between recognition and attributing an identity, there is spacious room for interpretation errors and manipulation. To be able to monitor interpretation errors and detect manipulation by the person involved, we need more insight into the technology and the practise of biometrics.

Secondly, we tend to forget that repeatedly measuring a specific physical characteristic of the same person inherently produces slightly different measurement results. So, a biometric recognition is based on a statistical evaluation of these differences when assessing the probability that the person is the right one. If we want more certainty, more than one physical characteristic or biometric technique should be used at the same time. This is only effective if these are independent of each other and cannot be manipulated in the same way at the same time. Thus, the practice of biometrics is far from easy to understand or to organise.

Thirdly, we mostly have small-scale models and theories in mind, while application of biometrics is inherently large scale, either by the size or the extent of the process to be secured or by unintended negative spill-over effects in other processes. Generally, this causes overestimating benefits and underestimating problems. In addition, biometrically secured large-scale systems tend to behave differently than we anticipate and might even produce reverse results which, depending on the application's scale, might go unnoticed for a long time. So, biometrics not only provides us with solutions, but causes existing problems to get bigger and new problems to arise, as well.

These considerations may convincingly explain why I am happy with this second edition of *Practical Biometrics*, updated to reflect current trends in technology and the use of biometrics. In the next edition, I would appreciate some attention to the legal restrictions on the use of biometric data, especially in international applications. The requirements and limits differ from one legal culture to another, thus causing big problems for the prevention of identity theft and identity fraud in these vital large-scale applications unless these are taken into account while designing the system.

Biometrics are badly needed in vital parts of our society, and more insight into the technology and practise is essential. But we cannot wait until our insight is up to our security requirements. We have to learn while doing. This is why Julian Ashbourn's book is so very useful, as it is written with this learning process in mind.

Jan Grijpink (1946) is an Emeritus Professor of Information Science at Utrecht University where he part-time lectured in Chain-computerisation from 2004 until his retirement in 2011.

He studied Economics (1969) and Law (1971) at Groningen University and Management Science (1976) in Utrecht (SIOO). In 1997 he obtained his doctorate at Eindhoven Technical University with a thesis about Chain-computerisation. As Principal Adviser at the Dutch Ministry of Justice until his retirement in 2011, he focused on information strategy and identity issues.

From 2006 to 2012 he was Chairman of the Netherlands Biometrics Forum.

He is Senior Adviser of PBLQ, Center of Expertise, IT consultants of the Dutch government, The Hague.

He is Editor-in-Chief of the open-access Journal of Chain-computerisation (http://jcc.library.uu.nl).

Jan Grijpink regularly publishes on identity issues in a complex information society often using his special focus on large-scale information systems and chain-interdependencies to uncover hidden problems or develop better solutions.

Utrecht University Jan Grijpink
The Hague, The Netherlands

Netherlands Biometrics Forum
The Hague, The Netherlands
March 22, 2015

Preface

Biometric verification techniques have been available for many years. Although the principle of using a biometric can be traced back to ancient times, the concept of commercially available devices with which to automate biometric identity verification was effectively a product of the late 1960s, with further development through the 1970s and 1980s leading to a step up in interest in the late 1980s. By the early 1990s, there were a raft of biometric device manufacturers offering a range of techniques including hand geometry, retinal scanning, fingerprints, voice verification, signature verification, and facial recognition. These were soon to be complemented by iris recognition, finger geometry, vein recognition, and other techniques, providing an intriguing technology choice for early adopters.

In parallel with technological development, we witnessed a good deal of investment in what was considered to be a technology on the brink of massive adoption across a broad scale of applications. The beginning of each year in the 1990s was marked with optimism that this would be the year for biometrics. The end of each year was marked with confusion and puzzled expressions on the faces of those who confidently predicted an explosion in growth for the industry. It simply never happened in the way the predictions suggested. Instead we saw a steadily but slowly increasing trickle of adoption in specific application areas, often in military or government/public service scenarios. These included applications in prisons, schools and universities, and at airports, primarily for access control purposes. We should be grateful to these early adopters, even with regard to applications which subsequently failed and were withdrawn, because they provided an opportunity to learn about the practical implementation of the technology, together with some of the technical and nontechnical issues highlighted as a result. Whether we have learned all of these lessons is rather debatable as many consultants and practitioners still rely on theoretical device performance metrics as the basis for developing related solutions. Those who have been close to the technology and its potential applications from the beginning know that there is a little more to it than this, especially when we are considering large-scale applications in the public domain.

Against the background depicted above, there have been many tackling the issues which they perceived as hurdles to wider-scale adoption. These included factors such as best practice in testing, API standards for interfacing to devices, and general interoperability. A great deal of good work has been undertaken in these areas,

much of it on a voluntary basis, and this has served to create a more sustainable platform for future development. However, while we have pushed forward the understanding and articulation of many of the technical issues, there still exists a raft of other issues to consider around human factors, environment, and general infrastructure, which are especially pertinent to wider-scale adoption. This book will explore many such issues.

The concept of biometric identity verification may have progressed at a more natural pace had it not been for the tragic events in September 2001 which brought with them a renewed focus on identity verification in general. Ideas which had been simmering in the background were suddenly brought forward. Funding which had hitherto proved elusive was suddenly within reach. It was natural to explore related technologies and ascertain their potential for wider adoption. The concept of biometric identity verification was now in the forefront of such thinking. Since that time, and amid a changing political world background, biometrics have been increasingly used in a military context and, sometimes, for less than obvious applications. More recently, the explosion in the use of mobile devices has brought a new focus to the potential use of biometrics to help secure access both to the device in question and to transactions undertaken via the device. This development will expand the usage of biometrics dramatically and, no doubt, be instrumental in developing a culture change toward biometrics and identity management in general.

If we are to implement the myriad of suggested applications in a workable, sustainable, and socially acceptable manner, then we must understand the real implications of using this technology upon a wide scale, not for tens or hundreds of users, but for tens of millions of users, not only in carefully controlled operational environments where time is of no consequence, but in everyday public situations where timing can be critical. In addition, there are a plethora of background processes which need to be examined, from managing data through to training related personnel. This book, together with companion titles from the same author, published by Springer, will serve as practical hands on guides to make biometric technology work in real-life scenarios.

March 2015 Julian Ashbourn

Acknowledgement

Very special thanks to all at Springer-Verlag London Ltd, for their enduring support throughout the creation of this book and others in the series.

Contents

Introduction

1

This is the second edition of a book about biometrics and the deployment of biometric identity verification techniques in relation to operational systems in both the private and public sector. Such developments often arouse controversy because of the intensely personal nature of biometrics and their alignment with personal identity. Are we moving towards a big brother world to the detriment of all citizens? Can large organisations and governments be trusted to manage such personal data in a competent and ethical manner? Will the introduction of such techniques in relation to wide-scale public applications turn out to be a blessing or a curse? Is the technology really as foolproof as some vendors would have us believe? Such questions and concerns must be properly taken into consideration of course, but some will argue that it is not so much the technology we must beware of but the manner in which it is implemented. In order to design and implement any application properly, we must understand all of the associated issues. This has not been easy in the field of biometrics as there are many variables, some of which have little to do with the technology itself but nevertheless influence operational performance. This book will therefore take a fresh look at what it takes to integrate biometrics into wider applications. It updates the first edition with revised information and two new sections which serve to provide a more complete coverage of the subject and a better understanding of the broader scenario. But first, let us backtrack a little.

In contemporary terms a biometrics is perhaps best described as a physiological or behavioural trait which may be measured, recorded and subsequently compared to another sample in order to confirm an individual's claimed identity. The principle is not new and has been practised since ancient times, although in modern terms we equate biometrics with the automatic measurement and subsequent recognition of such traits via electronic devices. In this context, we may think of modern biometrics as a technology with its roots in the late 1960s, although it took a decade or two to resolve into workable operation. For further information about the history and development of biometrics, the reader may like to refer to *Biometrics: Advanced Identity Verification*, also published by Springer, ISBN 1-85233-243-3.

J. Ashbourn, *Practical Biometrics*, DOI 10.1007/978-1-4471-6717-4_1