Guest Editorial – Special Issue on Biometric Security and Privacy

Nicholas Evans, Sébastien Marcel, Arun Ross and Andrew Teoh

Biometrics is the science of recognising individuals based on their behavioural and biological characteristics such as face, fingerprints, iris, voice, gait and signature. A typical biometric system may be viewed as a pattern classification system which utilises advanced signal processing schemes to compare and match biometric data.

The past decade has witnessed a rapid increase in biometrics research in addition to the deployment of large-scale biometrics solutions in both civilian and law enforcement applications. Example applications that incorporate biometric recognition include: logical and physical access systems; surveillance operations to fight against fraud and organised crime; immigration control and border security systems; national identity programs; identity management systems, and determination of friend or foe in military installations.

Since an individual's biometric data is personal and sensitive, issues related to biometric security and privacy have been raised. These include (a) spoofing, where an adversary presents a falsified biometric trait to the system with the intention of masquerading as another person; (b) evasion, where a person attempts to obfuscate or modify a biometric trait in order to avoid being detected by the system; (c) database alteration, where the templates stored in a database are modified in order to undermine system integrity; and (d) template compromise, where the stored biometric data is perused or stolen and exploited for illegitimate means. The advent of cloud computing technology and personal mobile devices has broadened the application domain of biometrics; however, at the same time, it has brought to the forefront the need for dedicated security technologies to protect biometric data from being misappropriated and used for purposes beyond those intended. Similarly, the use of surveillance systems in public areas presents new challenges with respect to privacy.

The research community has responded to these concerns with new security and privacy enhancement and protection technologies. There are numerous indicators of the increasing interest, e.g. a number of special sessions in conferences, evaluation campaigns, tutorials, large-scale collaborative projects and ongoing efforts towards standardisation. A number of signal processing methods have been developed to analyse the vulnerability of biometric systems and design solutions to mitigate the impact of these vulnerabilities. At the same time, privacy-preserving constructs have been developed by signal processing researchers in order to ensure that stored and/or transmitted biometric data is adequately protected from misuse.

This special section was conceived to champion recent developments in the rapidly evolving field and also to encourage research in new signal processing solutions to security and privacy protection. After a rigorous pre-selection and peer-review process, eight articles were selected for inclusion in this special section. Brief summaries of each follow.

The first contribution from Hadid, Evans, Marcel and Fierrez focuses on the security side of biometrics, providing a gentle introduction to spoofing and countermeasures and a methodology for their assessment. The paper also provides a case study in face recognition.

The next contribution discusses how adversarial machine learning techniques can be harnessed to protect biometric systems from sophisticated attacks. Biggio, Fumera, Russu, Didaci and Roli argue that security is best delivered with adaptive, security-by-design solutions.

Itkis, Chandar, Fuller, Campbell and Cunningham report the challenges in designing effective cryptosystems for iris recognition systems. Their work also illustrates the shortcoming of the more traditional performance metrics used in biometrics and promotes the use of a new entropy metric.

Patel, Ratha and Chellappa's contribution reviews different approaches to cancelable biometric schemes for template protection. The aim of such techniques is to preserve privacy by preventing the theft of biometric templates through the application of non-invertible transforms.

Barni, Droandi and Lazzeretti describe a different approach to template protection based on cryptographic technology. They illustrate how secure, two-party computation and signal processing in the encrypted domain can be combined to enhance security and protect privacy.

Still on the theme of template protection, Lim, Teoh and Kim describe their work on biometric feature-type transformation. Such transformations are typically used as a pre-cursor to many forms of biometric cryptosystems which demand specific input formats such as point-set or binary features.

The final paper on template protection discusses the practical implications of biometric security and offers a fresh perspective to the problem. Nandakumar and Jain argue that improvements to security and privacy seldom come without degradations to recognition performance and that, consequently, there remains a significant gap between theory and practice.

The special section rounds off with an article by Bustard on the privacy and legal concerns surrounding the collection, storage and use of personal biometric data. In particular, the article discusses recent European legislation on this issue and its potential impact on the adoption of biometrics technology.

Acknowledgments

The guest editors (GEs) wish to express their gratitude to Prof. Fulvio Gini, SPM's Area Editor for Special Issues until the end of 2014, for the support and advice provided throughout the preparation of this special section. They also wish to thank Rebecca Wollman, IEEE Signal Processing Society Publications Administrator, for her valuable assistance. Finally, they acknowledge the many anonymous reviewers whose outstanding contributions have ensured and helped to enhance the quality of the articles which follow.