Nicholas Evans, Sébastien Marcel,
Arun Ross, and Andrew Beng Jin Teoh

Biometrics Security and Privacy Protection

Biometrics is the science of recognizing individuals based on their behavioral and biological characteristics such as face, fingerprints, iris, voice, gait, and signature. A typical biometric system may be viewed as a pattern classification system that utilizes 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 organized crime; immigration control and border security systems; national identity programs; identity management systems; and the 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: spoofing, where an adversary presents a falsified biometric trait to the system with the intention of masquerading as another person; evasion, where a person attempts to obfuscate or modify a biometric trait to avoid being detected by the system; database alteration, where the templates stored in a database are modified to undermine system integrity; and 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 toward standardization. A number of signal processing methods have been developed to analyze 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 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 preselection and peer-review process, eight articles were selected.

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 article 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.

The article by Patel, Ratha, and Chellappa 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 noninvertible 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 precursor to many forms of biometric cryptosystems that demand specific input formats such as point-set or binary features.

The final article 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 out 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.

Digital Object Identifier 10.1109/MSP.2015.2443271
Date of publication: 13 August 2015

ACKNOWLEDGMENTS

We wish to express our gratitude to Prof. Fulvio Gini, *IEEE Signal Processing Magazine's* then-area editor of special issues, for the support and advice provided throughout the preparation of this special section. We also thank Rebecca Wollman, IEEE Signal Processing Society publications administrator, for her valuable assistance. Finally, we acknowledge the many anonymous reviewers whose outstanding contributions have ensured and helped to enhance the quality of the articles that follow.

ABOUT THE GUEST EDITORS

Nicholas Evans (evans@eurecom.fr) is with the Department of Multimedia Communications, EURECOM, France.

Sébastien Marcel (marcel@idiap.ch) is with Idiap Research University, Switzerland.

Arun Ross (rossarun@cse.msu.edu) is with Michigan State University, United States.

Andrew Beng Jin Teoh (bjteoh@yonsei.ac.kr) is with Yonsei University, Seoul, South Korea.

[SP]

(continued from page 11)

Using multiple object detection and recognition algorithms, a research team led by K. Vijayan Asari, an electrical and computer engineering professor at the University of Dayton in Ohio, has developed an automated surveillance technique that can be used to protect underground pipeline infrastructures (Figure 4).

The framework consists of three parts. The first part removes imagery that are not considered to be a threat to the pipeline. The method extracts a set of features that precisely represent the shape, structure and texture of various backgrounds, such as trees, buildings, roads and farmland, using a cascade of classifiers to eliminate the insignificant regions. The second part of the framework is a part-based object detection model for searching specific targets that are considered to be threat objects. The third part of the framework assesses the severity of pipeline threats by calculating the location and the temperature information of threat objects, such as construction equipment or drilling gear. "With our approach we can take into account the constraints associated with aerial imagery, such as low resolution, lower frame rate, large variations in illumination, and motion blurs," says Asari, who is also the director of the University of Dayton Vision Lab.

A major challenge to accurate threat detection are objects of interest that are partially occluded by shrubs, trees, buildings and other terrestrial elements. In the part-based model, an object is partitioned into a specific number of parts; the size of each part depends on the size of the object. "We then use local phase information to extract informative attributes for describing the individual parts," Asari says. "The next step is to group the object parts into several clusters. "In this process, we group similar parts into the same cluster and a histogram of oriented phase is used to describe the specific pattern of the parts," Asari continues. "This is to group similar parts of different vehicles, or similar parts in different images of the same vehicle, into the same cluster or category to find the presence of such categories in an occluded image to detect it as a threat object."

[A MAJOR CHALLENGE TO ACCURATE THREAT DETECTION ARE OBJECTS OF INTEREST THAT ARE PARTIALLY OCCLUDED BY SHRUBS, TREES, BUILDINGS AND OTHER TERRESTRIAL ELEMENTS.]

The output of the part-based object detection technique is the pixel location of the threat object in the input image. In real-world applications, however, a system user must also know the exact geographic location of a potentially threatening object. A registration process that links the acquired images to a geographical map provides this capability. Additionally, some detected threats may be far away from a pipeline, or have some other type of low threat probability. "Considering these issues, we have designed an additional framework that can automatically analyze the geolocation and temperature information of a detected object, and can assign a risk level to any given threat—high, medium, or low," Asari says. "A high temperature indicates that the vehicle is active and it may be moving to the pipeline right-of-way; a low temperature indicates that the vehicle is stationary and is of low risk."

"We have reached over 85% accuracy for machinery threat detection in tests," Asari says. "We are confident that our method can be used as a practical approach for wide-area surveillance and to protect pipeline infrastructures."

Asari says that he and his team are currently focusing on hardware-software integration and performance acceleration aspects. "We are looking to enable real-time processing in an onboard flight environment," he remarks.

AUTHOR

John Edwards (jedwards@johnedwardsmedia.com) is a technology writer based in the Phoenix, Arizona, area.

[SP]