Preface

Nobuyuki Nishiuchi*

Department of Management Systems Engineering,
Graduate School of System Design,
Tokyo Metropolitan University,
6-6 Asahigaoka, Hino, Tokyo 191-0065, Japan
E-mail: nnishiuc@cc.tmit.ac.jp
*Corresponding author

Toru Yamaguchi

Department of Information and Communications Systems Engineering,
Graduate School of System Design,
Tokyo Metropolitan University,
6-6 Asahigaoka, Hino, Tokyo 191-0065, Japan
E-mail: yamachan@tmu.ac.jp

Biographical notes: Nobuyuki Nishiuchi is Associate Professor of the Department of Management Systems Engineering, Graduate School of System Design at Tokyo Metropolitan University, Japan. He received his PhD in Mechanical Engineering in 2004 from the Graduate School of Engineering of Yokohama National University, Kanagawa, Japan. His interests include biometrics, human interface, image processing and application of image processing.

Toru Yamaguchi received his BS and ME in Electrical Engineering from Chiba University, Chiba, Japan, in 1979 and 1981, respectively. In 1992, he received his PhD in Computer Science from Chiba University. Since 1993, he has been with System Software Lab. of Toshiba Corp, Tokyo, Japan and has been working in the field of intelligent system using fuzzy and neural network system. He has also been with Lab. for Int. Fuzzy Eng. Research (LIFE) as a Chief Researcher of FAM (fuzzy associative memory) project. Since 2000, he has been Professor at Department of Electronic Systems and Engineering, Tokyo Metropolitan Institute of Technology.

The development of information technology (IT) emphasises the importance of people's identification and recognition. One of the techniques that identifies humans, biometrics has attracted attention. Over the last two decades, biometrics and human biometric characteristics have been studied greatly. Moreover, the biometric authentication has been applied in a variety of ways for different products.

On the other hand, biometric spoofing is a serious growing problem. The vulnerability of the biometric authentication on the spoofing issue has been pointed out by many researchers. Both spoofing and biometric authentication technology are advancing day by day. Recently, spoofing is a major issue in biometrics authentication technology. We can overcome the issue of the spoofing so that everyone can use the biometric authentication technology securely around the world.

Therefore, this special issue focuses on the spoofing issues and the anti-spoofing. The subject coverage of this special issue includes biometric spoofing issues, anti-spoofing techniques' new approach, applications of fundamental and applied research on anti-spoofing and biometrics' new approach.

We are very pleased to present varied and new challenging research in this special issue to the readers. There are six papers that present new methods of biometrics.

In the first paper, Shankar Bhausaheb Nikam et al. demonstrate various ways of spoofing and also propose a new texture analysis based vitality detection method. It is based on the observation that, real and spoof fingerprints exhibit different textural characteristics.

In the second paper, Miki Yamagishi et al. propose a new anti-spoofing method that is a hybrid fingerprint authentication using an artifact-metrics. The authors conduct experiments. Some spoofing attacks are assumed and the security of this proposed method is evaluated. The proposed method is able to prevent all assumed spoofing attack as a security system. Their results show sufficient accuracy for personal identification.

In the third paper, Masakatsu Nishigaki et al. propose a user authentication method that utilises human reflex responses. The expectation is that, even if a person's reflex characteristics are publicly known, it would be difficult for someone else to impersonate that person, since human beings are basically unable to control their own reflexes. It is the first in English literature that reports this sort of biometric authentication.

In the fourth paper, Fahim Sufi et al. propose a novel ECG anonymisation technique based on wavelet packet. It is proven to provide 100% anonymisation, resulting in failure with a replay attack by the spoofer. This particular research is one of the first few attempts to anonymise real-time ECG transmission from anti-spoofing.

In the fifth paper, Takeshi Sano et al. propose a method to authenticate a person based on their buying history receipts applying classification methods when they use a buying system. This is also considered to be available for equipment which accumulates the buying history in them. This particular research is one of the first few attempts to authenticate a person when they purchase products and is useful for anti-spoofing.

In the sixth paper, J. Sheeba Rani et al. propose an efficient face recognition system using wavelet transform and modular autoassociative neural network (AANN). To evaluate their scheme, experiments are conducted using various images in illumination, pose, expression and facial details. Their proposed method produces a very good performance compared to existing methods.

Finally, the editors would like to thank all the people involved in this special issue including all the authors who have submitted their papers and all the reviewers who have done such a good job to ensure the quality of this special issue. In particular, we would like to express special thanks to the Editor in Chief of the *International Journal of Biometrics*, Professor Khalid Saeed, for his encouragement and kind support.