

# Preface

Through the recent years, innovative computational intelligence procedures and frameworks have been established as convenient techniques to address the various security issues. Computational intelligence approaches are widely used for modeling, predicting, and recognition tasks in several research domains. One of these is denoted by multimedia that finds enormous applications in security, entertainment, and health. Advancement in sensor technology, signal processing, and digital hardware lead to a variety of signal types including text, audio, animation, and video. Technological advancement in this media production and computer hardware/communications as well make information processing/transmission relatively simple and quick. However, the rate of exposure to various threats increases for multimedia data. Thus, providing security for multimedia data becomes an urgent challenging task.

Recently, various security mechanisms are developed to provide security for multimedia data, such as cryptography, steganography, and digital watermarking. Cryptographic techniques are used to protect digital data during the transmission from the sender to the receiver, but once it gets decrypted at the reception end, there is no control over the data for providing further security. In contrast, steganography is applied for secret communication between trusted parties with the limitation of payload. Moreover, digital watermarking uses the identity of the multimedia data owner. Thus, signal processing provides a major role in providing security for multimedia data.

This book consists of 21 chapters, including a brief discussion about the multimedia content security chapter followed by eight chapters that reported various aspects in the multimedia security domain. These chapters handled the intelligent security techniques for high-definition multimedia data as well as the morphing and steganography security techniques for information hiding, the digital watermarking as a solution for the multimedia authentication in addition to the representation of reversible watermarking with real-time implementation, and the comparison between singular value decomposition and randomized singular value decomposition-based watermarking. Furthermore, the concept and challenges of the biometric-based security systems were carried out followed by the evaluation of

different cryptographic approaches in wireless communication network. In addition, this book contains another set of chapters that deal with the personal authentication and recognition systems in several applications, including personal authentication system based on hand images, surveillance system security using gait recognition, and face recognition under restricted constraints such as dry/wet face conditions, and the three-dimensional face identification using developed approach was also included. Thereafter, a proposed attendance recording system based on partial face recognition algorithm was conducted followed by the recognition of the human emotion that applied in surveillance video applications. Moreover, the concept of the security based on watermarking in the healthcare and medical applications and the pixel repetition-based high-capacity/reversible data hiding method for e-healthcare applications were included. Afterward, two chapters introduced several security issues for different types of multimedia contents, namely secured compressed data transmission over Global System for Mobile Communication (GSM) voice channel using wavelet transform and early tamper detection using joint stego-watermark approach. Finally, since biometrics has a great significant role in the security and authentication, the last chapter proposed a multifingerprint unimodel-based biometric authentication to support the cloud computing.

This book offered a precise concept and proposed approaches for the security in various applications combined with computational intelligence for multimedia security technologies. Based on the efforts done and the included contributions, it is expected very good endorsement from almost all readers of this book—from the graduated to postgraduate students' levels and researchers, professionals, and engineering. We are the editors wishing this book will stimulate further research to develop several intelligent techniques in signal processing for multimedia security applications in the various domains based on algorithmic and computer-based approaches.

Actually, this volume cannot be in this outstanding form without the contributions of the promising group of authors to whom we introduce our appreciation. Moreover, it was impossible to achieve this quality without the impact of the anonymous referees who assisted us during the revision and acceptance process of the submitted chapters. Our thankfulness is extended to them for their diligence in reviewing the chapters as well. Special thanks are directed to our publisher, Springer, for the endless support and guidance.

We hope this book presents promising concepts and outstanding research results supporting further development of security based on intelligent techniques.

Kolkata, India  
Vellore, India

Nilanjan Dey  
V. Santhi

Intelligent Techniques in Signal Processing for  
Multimedia Security

Dey, N.; Santhi, V. (Eds.)

2017, IX, 485 p. 226 illus., 96 illus. in color., Hardcover

ISBN: 978-3-319-44789-6