

Handbook Of Biometrics

This highly anticipated new edition provides a comprehensive account of face recognition research and technology, spanning the full range of topics needed for designing operational face recognition systems. After a thorough introductory chapter, each of the following chapters focus on a specific topic, reviewing background information, up-to-date techniques, and recent results, as well as offering challenges and future directions. Features: Fully updated, revised and expanded, covering the entire spectrum of concepts, methods, and algorithms for automated face detection and recognition systems; provides comprehensive coverage of face detection, tracking, alignment, feature extraction, and recognition technologies, and issues in evaluation, systems, security, and applications; contains numerous step-by-step algorithms; describes a broad range of applications; presents contributions from an international selection of experts; integrates numerous supporting graphs, tables, charts, and performance data. This important text/reference presents the latest secure and privacy-compliant techniques in automatic human recognition. Featuring viewpoints from an international selection of experts in the field, the comprehensive coverage spans both theory and practical implementations, taking into consideration all ethical and legal issues. Topics and features: presents a unique focus on novel approaches and new architectures for unimodal and multimodal template protection; examines signal processing techniques in the encrypted domain, security and privacy leakage assessment, and aspects of standardization; describes real-world applications, from face and fingerprint-based user recognition, to biometrics-based electronic documents, and biometric systems employing smart cards; reviews the ethical implications of the ubiquity of biometrics in everyday life, and its impact on human dignity; provides guidance on best practices for the processing of biometric data within a legal framework.

In the last few years, biometric techniques have proven their ability to provide secure access to shared resources in various domains. Furthermore, software agents and multi-agent systems (MAS) have shown their efficiency in resolving critical network problems. Iris Biometric Model for Secured Network Access proposes a new model, the IrisCryptoOpen

The use of biometric identification systems is rapidly increasing across the world, owing to their potential to combat terrorism, fraud, corruption and other illegal activities. However, critics of the technology complain that the creation of an extensive central register of personal information controlled by the government will increase opportunities for the state to abuse citizens. There is also concern about the extent to which data about an individual is recorded and kept. This book reviews some of the most current and complex legal and ethical issues relating to the use of biometrics. Beginning with an overview of biometric systems, the book goes on to examine some of the theoretical underpinnings of the surveillance state, questioning whether these conceptual approaches are still relevant, particularly the integration of ubiquitous surveillance systems and devices. The book also analyses the implementation of the world's largest biometric database, Aadhaar, in detail. Additionally, the identification of individuals at border checkpoints in the United States, Australia and the EU is explored, as well as the legal and ethical debates surrounding the use of biometrics regarding: the war on terror and the current refugee crisis; violations of international human rights law principles; and mobility and privacy rights. The book concludes by addressing the collection, use and disclosure of personal information by private-sector entities such as Amazon and Facebook, and government use of these tools to profile individuals. By examining the major legal and ethical issues surrounding the debate on this rapidly emerging technology, this book will appeal to students and scholars of law, criminology and surveillance studies, as well as law enforcement and criminal law practitioners.

Handbook of Fingerprint Recognition

Encyclopedia of Biometrics

Biometrics, the Documentary State and Bureaucratic Writings of the Self

Societies of Restricted Access, Discipline and Control

A Privacy-Enhancing Biometric

Computer and Information Security Handbook

As one of the most promising biometric technologies, vein pattern recognition (VPR) is quickly taking root around the world and may soon dominate applications where people focus is key. Among the reasons for VPR's growing acceptance and use: it is more accurate than many other biometric methods, it offers greater resistance to spoofing, it focuses on people and their privacy, and has few negative cultural connotations. Vein Pattern Recognition: A Privacy-Enhancing Biometric provides a comprehensive and practical look at biometrics in general and at vein pattern recognition specifically. It discusses the emergence of this reliable but underutilized technology and evaluates its capabilities and benefits. The author, Chuck Wilson, an industry veteran with more than 25 years of experience in the biometric and electronic security fields, examines current and emerging VPR technology along with the myriad applications of this dynamic technology. Wilson explains the use of VPR and provides an objective comparison of the different biometric methods in use today—including fingerprint, eye, face, voice recognition, and dynamic signature verification.

Highlighting current VPR implementations, including its widespread acceptance and use for identity verification in the Japanese banking industry, the text provides a complete examination of how VPR can be used to protect sensitive information and secure critical facilities. Complete with best-practice techniques, the book supplies invaluable guidance on selecting the right combination of biometric technologies for specific applications and on properly implementing VPR as part of an overall security system.

An authoritative survey of intelligent fingerprint-recognition concepts, technology, and systems is given. Editors and contributors are the leading researchers and applied R&D developers of this personal identification (biometric security) topic and technology. Biometrics and pattern recognition researchers and professionals will find the book an indispensable resource for current knowledge and technology in the field.

Biometric recognition, or simply biometrics, is the science of establishing the identity of a person based on physical or behavioral attributes. It is a rapidly evolving field with applications ranging from securely accessing one's computer to gaining entry into a country. While the deployment of large-scale biometric systems in both commercial and government applications has increased the public awareness of this technology, "Introduction to Biometrics" is the first textbook to introduce the fundamentals of Biometrics to undergraduate/graduate students. The three commonly used modalities in the biometrics field, namely, fingerprint, face, and iris are covered in detail in this book. Few other modalities like hand geometry, ear, and gait are also discussed briefly along with advanced topics such as multimbiometric systems and security of biometric systems. Exercises for each chapter will be available on the book website to help students gain a better understanding of the topics and obtain practical experience in designing computer programs for biometric applications. These can be found at: <http://www.csee.wvu.edu/~ross/BiometricsTextBook/>. Designed for undergraduate and graduate students in computer science and electrical engineering, "Introduction to Biometrics" is also suitable for researchers and biometric and computer security professionals.

"This book provides an in-depth description of existing and fresh fusion approaches for multimodal biometric systems, covering relevant topics affecting the security and intelligent industries"--Provided by publisher.

Biometric Systems

Handbook of Biometrics

Handbook of Biometrics for Forensic Science

Iris Biometric Model for Secured Network Access

Handbook of Face Recognition

Handbook of Remote Biometrics

Presenting the first definitive study of the subject, this Handbook of Biometric Anti-Spoofing reviews the state of the art in covert attacks against biometric systems and in deriving countermeasures to these attacks. Topics and features: provides a detailed introduction to the field of biometric anti-spoofing and a thorough review of the associated literature; examines spoofing attacks against biometric systems; reviews evaluation methodologies, international standards and legal and ethical issues; describes current challenges and suggests directions for future research; presents the latest work from a global selection of experts in the field, including members of the TABULA RASA project.

With an A-Z format, this encyclopedia provides easy access to relevant information on all aspects of biometrics. It features approximately 2500 overview entries and 800 definitional entries. Each entry includes a definition, key words, list of synonyms, list of related entries, illustration(s), applications, and a bibliography. Most entries include useful literature references providing the reader with a comprehensive list of sources.

A major new professional reference work on fingerprint security systems and technology from leading international researchers in the field. Handbook provides authoritative and comprehensive coverage of all major topics, concepts, and methods for fingerprint security systems. This unique reference work is an absolutely essential resource for all biometric security professionals, researchers, and practitioners.

Handbook of Vascular Biometrics

Vein Pattern Recognition

Security and Privacy in Biometrics

Concepts, Methodologies, Tools, and Applications

Intelligent Systems for Iris Recognition

Advances in Biometrics

Biometrics is a rapidly evolving field with applications ranging from accessing one's computer to gaining entry into a country. The deployment of large-scale biometric systems in both commercial and government applications has increased public awareness of this technology. Recent years have seen significant growth in biometric research resulting in the development of innovative sensors, new algorithms, enhanced test methodologies and novel applications. This book addresses this void by inviting some of the prominent researchers in Biometrics to contribute chapters describing the fundamentals as well as the latest innovations in their respective areas of expertise.

This comprehensive handbook addresses the sophisticated forensic threats and challenges that have arisen in the modern digital age, and reviews the new computing solutions that have been proposed to tackle them. These include identity-related scenarios which cannot be solved with traditional approaches, such as attacks on security systems and the identification of abnormal/dangerous behaviors from remote cameras. Features: provides an in-depth analysis of the state of the art, together with a broad review of the available technologies and their potential applications; discusses potential future developments in the adoption of advanced technologies for the automated or semi-automated analysis of forensic traces; presents a particular focus on the acquisition and processing of data from real-world forensic cases; offers an holistic perspective, integrating work from different research institutions and combining viewpoints from both biometric technologies and forensic science.

"The book gives an introduction to basic biometric image discrimination technologies including theories that are the foundations of those technologies and new algorithms for biometrics authentication"--Provided by publisher.

This authoritative and comprehensive handbook is the definitive work on the current state of the art of Biometric Presentation Attacks (PDA) – also known as Biometric Anti-Spoofing. Building on the success of the previous, pioneering edition, this thoroughly updated second edition has been considerably expanded to provide even greater coverage of PDA methods, spanning biometrics systems based on face, fingerprint, iris, voice, vein, and signature recognition. New material is also included on major PAD competitors, important databases for research, and on the impact of recent international legislation. Valuable insights are supplied by a selection of leading experts in the field, complete with results from reproducible research, supported by source code and further information available at an associated website. Topics and features: reviews the latest developments in PAD for fingerprint biometrics, covering optical coherence tomography (OCT) technology, and issues of interoperability; examines methods for PAD in iris recognition systems, and the application of stimulated pupillary light reflex for this purpose; discusses advancements in PAD methods for face recognition-based biometrics, such as research on 3D facial masks and remote photoplethysmography (rPPG); presents a survey of PAD for automatic speaker recognition (ASV), including the use of convolutional neural networks (CNNs), and an overview of relevant databases; describes the results yielded by key competitions on fingerprint liveness detection, iris liveness detection, and software-based face anti-spoofing; provides analyses of PAD in fingerprint recognition, online handwritten signature verification, and in biometric technologies on mobile devices;includes coverage of international standards, the E.U. PSDII and GDPR directives, and on different perspectives on presentation attack evaluation. This text/reference is essential reading for anyone involved in biometric identity verification, be they students, researchers, practitioners, engineers, or technology consultants. Those new to the field will also benefit from a number of introductory chapters, outlining the basics for the most important biometrics.

From Fiction to Practice

The InfoSec Handbook

The Cambridge Handbook of Surveillance Law

Sensors, Algorithms and Systems

Advanced Pattern Recognition Technologies with Applications to Biometrics

The REGTECH Book

Although the history of computer-aided face recognition stretches back to the 1960s, automatic face recognition remains an unsolved problem and still offers a great challenge to computer-vision and pattern recognition researchers. This handbook is a comprehensive account of face recognition research and technology, written by a group of leading international researchers. Twelve chapters cover all the sub-areas and major components for designing operational face recognition systems. Background, modern techniques, recent results, and challenges and future directions are considered. The book is aimed at practitioners and professionals planning to work in face recognition or wanting to become familiar with the state-of- the-art technology. A comprehensive handbook, by leading research authorities, on the concepts, methods, and algorithms for automated face detection and recognition. Essential reference resource for researchers and professionals in biometric security, computer vision, and video image analysis.

*The Handbook of Loss Prevention and Crime Prevention, 5th Edition, is a trusted foundation for security professionals just entering the field and a reference for seasoned professionals. This book provides a comprehensive overview of current approaches to security and crime prevention, tools and technologies to put these approaches into action, and information on a wide range of specific areas within the field of physical security. These include school and campus security, cargo security, access control, the increasingly violent healthcare security environment, and prevention or mitigation of terrorism and natural disasters. * Covers every important topic in the field, including the latest on wireless security applications, data analysis and visualization, situational crime prevention, and global security standards and compliance issues * Required reading for the professional security professionals * Each chapter is contributed by a top security professional with subject-matter expertise*

Details multimodal biometrics and its exceptional utility for increasingly reliable human recognition systems. Reveals the substantial advantages of multimodal systems over conventional identification methods.

This open access book provides the first comprehensive collection of studies dealing with the hot topic of digital face manipulation such as DeepFakes, Face Morphing, or Reenactment. It combines the research fields of biometrics and media forensics including contributions from academia and industry. Appealing to a broad readership, introductory chapters provide a comprehensive overview of the topic, which address readers wishing to gain a brief overview of the state-of-the-art. Subsequent chapters, which delve deeper into various research challenges, are oriented towards advanced readers. Moreover, the book provides a good starting point for young researchers as well as a reference guide pointing at further literature. Hence, the primary readership is academic institutions and industry currently involved in digital face manipulation and detection. The book could easily be used as a recommended text for courses in image processing, machine learning, media forensics, biometrics, and the general security area.

Automatic Fingerprint Recognition Systems

for Surveillance and Security

Handbook of MultiBiometrics

Biometrics: Concepts, Methodologies, Tools, and Applications

Selfie Biometrics

Handbook of Iris Recognition

Iris recognition is one of the highest accuracy techniques used in biometric systems. The accuracy of the iris recognition system is measured by False Reject Rate (FRR), which measures the authenticity of a user who is incorrectly rejected by the system due to changes in iris features (such as aging and health condition) and external factors that affect iris image, for instance, high noise rate. External factors such as technical fault, occlusion, and source of lighting that causes the image acquisition to produce distorted iris images create error, hence are incorrectly rejected by the biometric system. FRR can be reduced using wavelets and Gabor filters, cascaded classifiers, ordinal measures, multiple biometric modalities, and a selection of unique iris features. Nonetheless, in the long duration of the matching process, existing methods were unable to identify the authenticity of the user since the iris structure itself provides a template changed due to aging. In fact, the iris consists of unique features such as crypts, furrows, collarette, pigment blotches, freckles, and pupils that are distinguishable among humans. Earlier research was done by selecting unique iris features. However, these had low accuracy levels. A new way of identifying and matching the iris template using the nature-inspired algorithm is described in this book. It provides an overview of iris recognition that is based on nature-inspired environment technology. The book is useful for students from universities, polytechnics, community colleges; practitioners; and industry practitioners.

*Handbook of Fingerprint Security for Infrastructure Security Professionals * Each chapter is contributed by a top security professional with subject-matter expertise*

Recognition, speaker recognition evolved from signal processing, the beginnings of face recognition were in computer vision, and privacy concerns arose from the public policy arena. One of the challenges of any new field is to state what the core ideas are that define the field in order to provide a research agenda for the field and identify key research problems. Biometrics has been grappling with this challenge since the late 1990s. With the maturation of biometrics, the separate biometrics areas are coalescing into the new discipline of biometrics. The establishment of biometrics as a recognized field of inquiry allows the research community to identify problems that are common to biometrics in general. It is this identification of common problems that will define biometrics as a field and allow for broad advancement.

"The Biometric Computing, Recognition & Registration" presents introduction of biometrics along with detailed analysis for identification and recognition methods. This book forms the required platform for understanding biometric computing and its implementation for securing target system. It also provides the comprehensive analysis on algorithms, architectures and interdisciplinary connection of biometric computing along with detailed case-studies for newborns and resolution spaces. The strength of this book is its unique approach starting with how biometric computing works to research paradigms and gradually moves towards its advancement. This book is divided into three parts that comprises basic fundamentals and definitions, algorithms and methodologies, and futuristic research and case studies. Features: A clear view to the fundamentals of Biometric Computing Identification and recognition approach for different human characteristics Different methodologies and algorithms for human identification using biometrics traits such as face, iris, fingerprint, palm print, veinprint etc. Interdisciplinary connection of biometric computing with the fields like deep neural network, artificial intelligence, Internet of Biometric Things, low resolution face recognition etc. This book is an edited volume with contributions from researchers and practitioners around the globe in the field of biometrics, describes the fundamental and recent advancement in biometric recognition and registration. This book is a perfect research handbook for young practitioners who are intending to carry out their research in the field of Biometric Computing and will be used by industry professionals, graduate and researcher students in the field of computer science and engineering.

The InfoSec Handbook offers the reader an organized layout of information that is easily read and understood. Allowing beginners to enter the field and understand the key concepts and ideas, while still keeping the experienced readers updated on topics and concepts. It is intended mainly for beginners to the field of information security, written in a way that makes it easy for them to understand the detailed content of the book. The book offers a practical and simple view of the security practices while still offering somewhat technical and detailed information relating to security. It helps the reader build a strong foundation of information, allowing them to move forward from the book with a larger knowledge base. Security is a constantly growing concern that everyone must deal with. Whether it's an average computer user or a highly skilled computer user, they are always confronted with different security risks. These risks range in danger and should always be dealt with accordingly. Unfortunately, not everyone is aware of the dangers or how to prevent them and this is where most of the issues arise in information technology (IT). When computer users do not take security into account many issues can arise from that like system compromises or loss of data and information. This is an obvious issue that is present with all computer users. This book is intended to educate the average and experienced user of what kinds of different security practices and standards exist. It will also cover how to manage security software and updates in order to be as protected as possible from all of the threats that they face.

Multimodal Biometrics and Intelligent Image Processing for Security Systems

Handbook of Biometric Anti-Spoofing

Handbook of Digital Face Manipulation and Detection

Identification and Citizenship in Africa

Guide to Biometrics

Biometric Technologies and Verification Systems

This volume helps to fill the gap between data analytics, image processing, and soft computing practices. Soft computing methods are used to focus on data analytics and image processing to develop good intelligent systems. To this end, readers of this volume will find quality research that presents the current trends, advanced methods, and hybridized techniques relating to data analytics and intelligent systems. The book also features case studies related to medical diagnosis with the use of image processing and soft computing algorithms in particular models. Providing extensive coverage of biometric systems, soft computing, image processing, artificial intelligence, and data analytics, the chapter authors discuss the latest research issues, present solutions to research problems, and look at comparative analysis with earlier results. Topics include some of the most important challenges and discoveries in intelligent systems today, such as computer vision concepts and image identification, data analysis and computational paradigms, deep learning techniques, face and speaker recognition systems, and more.

The development of technologies for the identification of individuals has driven the interest and curiosity of many people. Spearheaded and inspired by the Bertillon coding system for the classification of humans based on physical measurements, scientists and engineers have been trying to invent new devices and classification systems to capture the human identity from its body measurements. One of the main limitations of the precursors of today's biometrics, which is still present in the vast majority of the existing biometric systems, has been the need to keep the device in close contact with the subject to capture the biometric measurements. This clearly limits the applicability and convenience of biometric systems. This book presents an important step in addressing this limitation by describing a number of methodologies to capture meaningful biometric information from a distance. Most materials covered in this book have been presented at the International Summer School on Biometrics which is held every year in Alghero, Italy and which has become a flagship activity of the IAPR Technical Committee on Biometrics (IAPR TC-4). The last four chapters of the book are derived from some of the best presentations by the participating students of the school. The educational value of this book is also highlighted by the number of proposed exercises and questions which will help the reader to better understand the proposed topics.

The definitive work on iris recognition technology, this comprehensive handbook presents a broad overview of the state of the art in this exciting and rapidly evolving field. Revised and updated from the highly-successful original, this second edition has also been considerably expanded in scope and content, featuring four completely new chapters. Features: provides authoritative insights from an international selection of preeminent researchers from government, industry, and academia; reviews issues covering the full spectrum of the iris recognition process, from acquisition to encoding; presents surveys of topical areas, and discusses the frontiers of iris research, including cross-wavelength matching, iris template aging, and anti-spoofing; describes open source software for the iris recognition pipeline and datasets of iris images; includes new content on liveness detection, correcting off-angle iris images, subjects with eye conditions, and implementing software systems for iris recognition.

This book introduces readers to the basic concepts, classical approaches, and the newest design, development, and applications of biometrics. It also provides a glimpse of future designs and research directions in biometrics. In addition, it discusses some latest concerns and issues in this area. Suitable for a wide range of readers, the book explains professional terms in plain English. Some concepts and designs discussed are new that commercial systems based on them may not arrive in the market in the next 10 to 20 years.

An Introduction to Information Security

Technology, Design and Performance Evaluation

Presentation Attack Detection

Biometrics

The Biometric Computing

I

The Regulatory Technology Handbook The transformational potential of RegTech has been confirmed in recent years with US\$1.2 billion invested in start-ups (2017) and an expected additional spending of US\$100 billion by 2020. Regulatory technology will not only provide efficiency gains for compliance and reporting functions, it will radically change market structure and supervision. This book, the first of its kind, is providing a comprehensive and invaluable source of information aimed at corporates, regulators, compliance professionals, start-ups and policy makers. The REGTECH Book brings into a single volume the curated industry expertise delivered by subject matter experts. It serves as a single reference point to understand the RegTech eco-system and its impact on the industry. Readers will learn foundational notions such as: • The economic impact of digitization and datification of regulation • How new technologies (Artificial Intelligence, Blockchain) are applied to compliance • Business use cases of RegTech for cost-reduction and new product origination • The future regulatory landscape affecting financial institutions, technology companies and other industries Edited by world-class academics and written by compliance professionals, regulators, entrepreneurs and business leaders, the RegTech Book represents an invaluable resource that paves the way for 21st century regulatory innovation.

Written for researchers, advanced students and practitioners to use as a handbook, this volume captures the very latest state-of-the-art research contributions from leading international researchers in the field.

Biometric Technologies and Verification Systems is organized into nine parts composed of 30 chapters, including an extensive glossary of biometric terms and acronyms. It discusses the current state-of-the-art in biometric verification/authentication, identification and system design principles. It also provides a step-by-step discussion of how biometrics works; how biometric data in human beings can be collected and analyzed in a number of ways; how biometrics are currently being used as a method of personal identification in which people are recognized by their own unique characteristics; and how to create a detailed and secure biometric verification/authentication system. Only biometrics verification/authentication is based on the identification of an intrinsic part of a human being. Tokens, such as smart cards, magnetic stripe cards, and physical keys can be lost, stolen, or duplicated. Passwords can be forgotten, shared, or unintentionally observed by a third party. Forgotten passwords and lost "smart cards" are a nuisance for users and an expensive time-waster for system administrators. Biometric security solutions offer some unique advantages for identifying and verifying/authenticating human beings over more traditional security methods. This book will serve to identify the various security applications biometrics can play a highly secure and specific role in. • Contains elements such as Sidebars, Tips, Notes and URL Links • Heavily illustrated with over 150 illustrations, screen captures, and photographs • Details the various biometric technologies and how they work while providing a discussion of the economics, privacy issues and challenges of implementing biometric security solutions

In the context of a global biometric turn, this book investigates processes of legal identification in Africa 'from below,' asking what this means for the relationship between citizens and the state. Almost half of the population of the African continent is thought to lack a legal identity, and many states see biometric technology as a reliable and efficient solution to the problem. However, this book shows that biometrics, far from securing identities and avoiding fraud or political distrust, can even participate in reinforcing exclusion and polarizing debates on citizenship and national belonging. It highlights the social and political embedding of legal identities and the resilience of the documentary state. Drawing on empirical research conducted across 14 countries, the book documents the processes, practices, and meanings of legal identification in Africa from the 1950s right up to the biometric boom. Beyond the classic opposition between surveillance and recognition, it demonstrates how analyzing the social uses of IDs and tools of identification can give a fresh account of the state at work, the practices of citizenship, and the role of bureaucracy in the writing of the self in African societies. This book will be of an important reference for students and scholars of African studies, politics, human security, and anthropology and the sociology of the state.

Biometrics, Surveillance and the Law

Advances in Biometric Systems, Soft Computing, Image Processing, and Data Analytics

Introduction to Biometrics

Trusted Biometrics under Spoofing Attacks

From DeepFakes to Morphing Attacks

Handbook of Loss Prevention and Crime Prevention

*Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network design with respect to particular vulnerabilities and threats. It also covers risk assessment and mitigation and auditing and testing of security systems as well as application standards and technologies required to build secure VPNs, configure client software and server operating systems, IPsec-enabled routers, firewalls and SSL clients. This comprehensive book will provide essential knowledge and skills needed to select, design and deploy a public key infrastructure (PKI) to secure existing and future applications. * Chapters contributed by leaders in the field cover theory and practice of computer security technology, allowing the reader to develop a new level of technical expertise * Comprehensive and up-to-date coverage of security issues facilitates learning and allows the reader to remain current and fully informed from multiple viewpoints * Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions*

Biometric Systems provides practitioners with an overview of the principles and methods needed to build reliable biometric systems. It covers three main topics: key biometric technologies, design and management issues, and the performance evaluation of biometric systems for personal verification/identification. The four most widely used technologies are focused on – speech, fingerprint, iris and face recognition. Key features include: in-depth coverage of the technical and practical obstacles which are often neglected by application developers and system integrators and which result in shortfalls between expected and actual performance; and protocols and benchmarks which will allow developers to compare performance and track system improvements.

This book highlights the field of selfie biometrics, providing a clear overview and presenting recent advances and challenges. It also discusses numerous selfie authentication techniques on mobile devices. Biometric authentication using mobile devices is becoming a convenient and important means of verifying identity for secured access and services such as telebanking and electronic transactions. In this context, face and ocular biometrics in the visible spectrum has gained increased attention from the research community. However, device mobility and operation in uncontrolled environments mean that facial and ocular images captured with mobile devices exhibit substantial degradation as a result of adverse lighting conditions, specular reflections and motion and defocus blur. In addition, low spatial resolution and the small sensor of front-facing mobile cameras further degrade the sample quality, reducing the recognition accuracy of face and ocular recognition technology when integrated into smartphones. Presenting the state of the art in mobile biometric research and technology, and offering an overview of the potential problems in real-time integration of biometrics in mobile devices, this book is a valuable resource for final-year undergraduate students, postgraduate students, engineers, researchers and academics in various fields of computer engineering.

Surveillance presents a conundrum: how to ensure safety, stability, and efficiency while respecting privacy and individual liberty. From police officers to corporations to intelligence agencies, surveillance law is tasked with striking this difficult and delicate balance. That challenge is compounded by ever-changing technologies and evolving social norms. Following the revelations of Edward Snowden and a host of private-sector controversies, there is intense interest among policymakers, business leaders, attorneys, academics, students, and the public regarding legal, technological, and policy issues relating to surveillance. This handbook documents and organizes these conversations, bringing together some of the most thoughtful and impactful contributors to contemporary surveillance debates, policies, and practices. Its pages explore surveillance techniques and technologies; their value for law enforcement, national security, and private enterprise; their impacts on citizens and communities; and the many ways societies do – and should – regulate surveillance.

The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation

Biometric Image Discrimination Technologies

Recognition and Registration

Intelligent Systems

Advances and Challenges

Security and authentication issues are surging to the forefront of the research realm in global society. As technology continues to evolve, individuals are finding it easier to infiltrate various forums and facilities where they can illegally obtain information and access. By implementing biometric authentications to these forums, users are able to prevent attacks on their privacy and security. Biometrics: Concepts, Methodologies, Tools, and Applications is a multi-volume publication highlighting critical topics related to access control, user identification, and surveillance technologies. Featuring emergent research on the issues and challenges in security and privacy, various forms of user authentication, biometric applications to image processing and computer vision, and security applications within the field, this publication is an ideal reference source for researchers, engineers, technology developers, students, and security specialists.

This open access handbook provides the first comprehensive overview of biometrics exploiting the shape of human blood vessels for biometric recognition, i.e. vascular biometrics, including finger vein recognition, hand/palm vein recognition, retina recognition, and sclera recognition. After an introductory chapter summarizing the state of the art in and availability of commercial systems and open datasets/open source software, individual chapters focus on specific aspects of one of the biometric modalities, including questions of usability, security, and privacy. The book features contributions from both academia and major industrial manufacturers.