Fingerprint Recognition Biometrics Gov Home

As recognized, adventure as skillfully as experience just about lesson, amusement, as competently as accord can be gotten by just checking out a books **Fingerprint Recognition Biometrics Gov Home** furthermore it is not directly done, you could understand even more almost this life, just about the world.

We meet the expense of you this proper as skillfully as simple habit to acquire those all. We present Fingerprint Recognition Biometrics Gov Home and numerous books collections from fictions to scientific research in any way. among them is this Fingerprint Recognition Biometrics Gov Home that can be your partner.

Fingerprint Recognition Biometrics Gov Home *2021-05-25*

FRIDA KENDAL

Biometrics for Network Security Routledge
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 Axciom 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.
Biometric and Auditing Issues Addressed in a Throughput Model Duke University Press
This book examines the proliferation of surveillance technologies&—such as facial recognition software and digital fingerprinting&—that have come to pervade our everyday lives. Often developed as methods to ensure "national security," these technologies are also routinely employed to regulate our personal information, our work lives, what we buy, and how we live.
Strengthening Forensic Science in the United States The Stationery Office
Scores of talented and dedicated people serve the forensic science community, performing vitally important work. However, they are often constrained by lack of adequate resources, sound policies, and national support. It is clear that change and advancements, both systematic and scientific, are needed in a number of forensic science disciplines to ensure the reliability of work, establish enforceable standards, and promote best practices with consistent application. Strengthening Forensic Science in the United States: A Path Forward provides a detailed plan for addressing these needs and suggests the creation of a new government entity, the National Institute of Forensic Science, to establish and enforce standards within the forensic science community. The benefits of improving and regulating the forensic science disciplines are clear: assisting law enforcement officials, enhancing homeland security, and reducing the risk of wrongful conviction and exoneration. Strengthening Forensic Science in the United States gives a full account of what is needed to advance the forensic science disciplines, including upgrading of systems and organizational structures, better training, widespread adoption of uniform and enforceable best practices, and mandatory certification and accreditation programs. While this book provides an essential call-to-action for congress and policy makers, it also serves as a vital tool for law enforcement agencies, criminal prosecutors and attorneys, and forensic science educators.
Commissioner for the Retention and Use of Biometric Material Annual Report 2015 DIANE Publishing
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 analysing 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.
Routledge Handbook on Information Technology in Government Routledge
Work with common biometrics such as face, fingerprint, and iris recognition for business and personal use to ensure secure identification and authentication for fintech, homes, and computer systems Key FeaturesExplore the next iteration of identity protection and overcome real-world challengesUnderstand different biometric use cases to deploy a large-scale biometric systemCurated by renowned security ambassador and experienced author Lisa BockBook Description Biometric technologies provide a variety of robust and convenient methods to securely identify and authenticate an individual. Unlike a password or smart card, biometrics can identify an attribute that is not only unique to an individual, but also eliminates any possibility of duplication. Identity Management with Biometrics is a solid introduction for anyone who wants to explore biometric techniques, such as fingerprint, iris, voice, palm print, and facial recognition. Starting with an overview of biometrics, you'll learn the various uses and applications of biometrics in fintech, buildings, border control, and many other fields. You'll understand the characteristics of an optimal biometric system and then review different types of errors and discover the benefits of multi-factor authentication. You'll also get to grips with analyzing a biometric system for usability and accuracy and understand the process of implementation, testing, and deployment, along with addressing privacy concerns. The book outlines the importance of protecting biometric data by using encryption and shows you which factors to consider and how to analyze them before investing in biometric technologies. By the end of this book, you'll be well-versed with a variety of recognition processes and be able to make the right decisions when implementing biometric technologies. What you will learnReview the advantages and disadvantages of biometric technologyUnderstand the characteristics of an optimal biometric systemDiscover the uses of biometrics and where they are usedCompare different types of errors and see how to tune your systemUnderstand the benefits of multi-factor authenticationWork with commonly used biometrics such as face, fingerprint, and irisAnalyze a biometric system for usability and accuracyAddress privacy concerns and get a glimpse of the future of biometricsWho this book is for Identity Management with Biometrics is for IT managers, security professionals, students, teachers, and anyone involved in selecting, purchasing, integrating, or securing a biometric system. This book will help you understand how to select the right biometric system for your organization and walk you through the steps for implementing identity management and authentication. A basic understanding of biometric authentication techniques, such as fingerprint and facial recognition, and the importance of providing a secure method of authenticating an individual will help you make the most of the book.
Multimedia Content Representation, Classification and Security Springer Science & Business Media
Since the 1990s, biometric border control has attained key importance throughout Europe. Employing digital images of, for example, fingerprints, DNA, bones, faces or irises, biometric technologies use bodies to identify, categorize and regulate individuals' cross-border movements. Based on innovative collaborative fieldwork, this book examines how biometrics are developed, put to use and negotiated in key European border sites. It analyses the disparate ways in which the technologies are applied, perceived and experienced by border control agents and others managing the cross-border flow of people, by scientists and developers engaged in making the technologies, and by migrants and non-government organizations attempting to manoeuvre in the complicated and often-unpredictable systems of technological control. Biometric technologies are promoted by national and supranational authorities and industry as scientifically exact and neutral methods of identification and verification, and as an infallible solution to security threats. The ethnographic case studies in this volume demonstrate, however, that the technologies are, in fact, characterized by considerable ambiguity and uncertainty and subject to substantial subjective interpretation, translation and brokering with different implications for migrants, border guards, researchers and other actors engaged in the border world.
Biometric Systems Springer Nature
Recent advances in biometrics include new developments in sensors, modalities and algorithms. As new sensors are designed, newer challenges emerge in the algorithms for accurate recognition. 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. It offers coverage of the entire gamut of topics in the field, including sensors, data acquisition, pattern-matching algorithms, and issues that impact at the system level, such as standards, security, networks, and databases
Handbook of Biometrics Packt Publishing Ltd
This book proposes a Throughput Model that draws from computer science, economic and psychology literatures to model perceptual and judgmental processes whereby biometrics might be used to reduce risks to a company's internal control. The book also discusses challenges in employing biometric technology and pinpoints avenues for future research. Biometrics is the examination of measurable biological characteristics. In organizational security, biometrics refers to tools that rely on measurable physical and behavioral characteristics that can be automatically checked. The Throughput Modeling process enables organizations to employ trust systems in assisting transactions that are motivated by ethical considerations. Auditing systems are by far based on trust. Concepts of ethics and trust are aided by the employment of biometrics technology, which enhances the transactions between individuals and organizations in an internal control environment. Issues pertaining to sustainability are also examined with the assistance of the Throughput Model. Finally, this book examines the potential use of an internal control biometrics system to lessen threats to identification and verification procedures. This book proposes an "Throughput Model framework" that considers both exposure and information risks as fundamental factors in classifying applications and organizational processes that might be candidates for the type of internal control biometrics system that biometrics can offer.
An Integrated Approach to Home Security and Safety Systems Penguin
This book describes a range of new biometric technologies, such as high-resolution fingerprint, finger-knuckle-print, multi-spectral backhand, 3D fingerprint, tongueprint, 3D ear, and multi-spectral iris technologies. Further, it introduces readers to efficient feature extraction, matching and fusion algorithms, in addition to developing potential systems of its own. These advanced biometric technologies and methods are divided as follows: 1. High-Resolution Fingerprint Recognition; 2. Finger-Knuckle-Print Verification; 3. Other Hand-Based Biometrics; and 4. New Head-Based Biometrics. Traditional biometric technologies, such as fingerprint, face, iris, and palmprint, have been extensively studied and addressed in many research books. However, all of these technologies have their own advantages and disadvantages, and there is no single type of

biometric technology that can be used for all applications. Many new biometric technologies have been developed in recent years, especia lly in response to new applications. The contributions gathered here focus on how to develop a new biometric technology based on the requirements of essential applications, and how to design efficient algorithms that yield better performance.

Machine Learning for Biometrics Academic Press

In its broadest sense, biometrics is the measurement and analysis of a biological characteristic (fingerprints, iris patterns, retinas, face or hand geometry) or a behavioural characteristic (voice, gait or signature). Biometric technologies use these characteristics to identify individuals automatically. Unlike identity documents or passwords, biometrics cannot be lost or forgotten since they are a part of the user and are always present at the time of identification. They are also difficult, though not impossible, to forge or share. Three future trends in the application of biometrics were identified during the inquiry: (i) the growth of unsupervised biometric systems, accessed via mobile devices, which verify identity; (ii) the proliferation of "second-generation" biometric technologies that can authenticate individuals covertly; (iii) and the linking of biometric data with other types of 'big data' as part of efforts to profile individuals. Each of these trends introduces risks and benefits to individuals, to the state and to society as a whole. They also raise important ethical and legal questions relating to privacy and autonomy. The Committee are not convinced that the Government has addressed these questions, nor are they satisfied that it has looked ahead and considered how the risks and benefits of biometrics will be managed and communicated to the public.

Biometric Recognition Routledge

Privacy and Technologies of Identity: A Cross-Disciplinary Conversation provides an overview of ways in which technological changes raise privacy concerns. It then addresses four major areas of technology: RFID and location tracking technology; biometric technology, data mining; and issues with anonymity and authentication of identity. Many of the chapters are written with the non-specialist in mind, seeking to educate a diverse audience on the "basics" of the technology and the law and to point out the promise and perils of each technology for privacy. The material in this book provides an interface between legal and policy approaches to privacy and technologies that either threaten or enhance privacy. This book grew out of the Fall 2004 CIPLIT(r) Symposium on Privacy and Identity: The Promise and Perils of a Technological Age, co-sponsored by DePaul University's College of Law and School of Computer Science, Telecommunications and Information Systems. The Symposium brought together leading researchers in advanced technology and leading thinkers from the law and policy arenas, many of whom have contributed chapters to the book. Like the Symposium, the book seeks to contribute to a conversation among technologists, lawyers, and policymakers about how best to handle the challenges to privacy that arise from recent technological advances.

Biometrics in Identity Management NYU Press

A powerful story of war in our time, of love of country, the experience of tragedy, and a platoon at the center of it all. This is a story that starts off close and goes very big. The initial part of the story might sound familiar at first: it is about a platoon of mostly nineteen-year-old boys sent to Afghanistan, and an experience that ends abruptly in catastrophe. Their part of the story folds into the next: inexorably linked to those soldiers and never comprehensively reported before is the U.S. Department of Defense’s quest to build the world’s most powerful biometrics database, with the ability to identify, monitor, catalog, and police people all over the world. First Platoon is an American saga that illuminates a transformation of society made possible by this new technology. Part war story, part legal drama, it is about identity in the age of identification. About humanity—physical bravery, trauma, PTSD, a yearning to do right and good—in the age of biometrics, which reduce people to iris scans, fingerprint scans, voice patterning, detection by odor, gait, and more. And about the power of point of view in a burgeoning surveillance state. Based on hundreds of formerly classified documents, FOIA requests, and exclusive interviews, First Platoon is an investigative exposé by a master chronicler of government secrets. First Platoon reveals a post–9/11 Pentagon whose identification machines have grown more capable than the humans who must make sense of them. A Pentagon so powerful it can cover up its own internal mistakes in pursuit of endless wars. And a people at its mercy, in its last moments before a fundamental change so complete it might be impossible to take back.

The Fingerprint Apress

A credible voter register gives legitimacy to the electoral process and helps prevent electoral fraud. However, voter registration remains a complex and contested task. It is one of the most important activities that an electoral management body needs to conduct, but it is also one of the most costly in terms of both time and resources. Many countries that face challenges in creating an accurate voter register are considering reforming their voter registration systems through the introduction of biometric technologies. The drive towards biometrics has been facilitated by its largely apolitical nature. Investing in high-tech solutions allows stakeholders to demonstrate their commitment to resolving electoral problems. At the same time, expectations on biometric solutions may be exaggerated. This guide provides an overview of key concepts and considerations for all stakeholders involved in discussions about the application of biometrics in elections, both for voter registration before an election and for voter verification at polling stations on election day.

Multimodal Biometric Systems Springer

This book constitutes the refereed proceedings of the 12th Iberoamerican Congress on Pattern Recognition, CIARP 2007, held in Valparaiso, Chile, November 13-16, 2007. The 97 revised full papers presented together with four keynote articles were carefully reviewed and selected from 200 submissions. The papers cover ongoing research and mathematical methods for pattern recognition, image analysis, and applications in areas such as computer vision, robotics, industry and health.

Progress in Pattern Recognition, Image Analysis and Applications Springer Science & Business Media

Face recognition technologies (FRTs) have many practical security-related purposes, but advocacy groups and individuals have expressed apprehensions about their use. This report highlights the high-level privacy and bias implications of FRT systems. The authors propose a heuristic with two dimensions -- consent status and comparison type -- to help determine a proposed FRT's level of privacy and accuracy. They also identify privacy and bias concerns.

Biometrics, Surveillance and the Law Springer Science & Business Media

This book is open access. This book undertakes a multifaceted and integrated examination of biometric identification, including the current state of the technology, how it is being used, the key ethical issues, and the implications for law and regulation. The five chapters examine the main forms of contemporary biometrics–fingerprint recognition, facial recognition and DNA identification– as well the integration of biometric data with other forms of personal data, analyses key ethical concepts in play, including privacy, individual autonomy, collective responsibility, and joint ownership rights, and proposes a raft of principles to guide the regulation of biometrics in liberal democracies. Biometric identification technology is developing rapidly and being implemented more widely, along with other forms of information technology. As products, services and communication moves online, digital identity and security is becoming more important. Biometric identification facilitates this transition. Citizens now use biometrics to access a smartphone or obtain a passport; law enforcement agencies use biometrics in association with CCTV to identify a terrorist in a crowd, or identify a suspect via their fingerprints or DNA; and companies use biometrics to identify their customers and employees. In some cases the use of biometrics is governed by law, in others the technology has developed and been implemented so quickly that, perhaps because it has been viewed as a valuable security enhancement, laws regulating its use have often not been updated to reflect new applications. However, the technology associated with biometrics raises significant ethical problems, including in relation to individual privacy, ownership of biometric data, dual use and, more generally, as is illustrated by the increasing use of biometrics in authoritarian states such as China, the potential for unregulated biometrics to undermine fundamental principles of liberal democracy. Resolving these ethical problems is a vital step towards more effective regulation.

Biometric State Rand Corporation

In todayOCOs digital infrastructure we have to interact with an increasing number of systems, both in the physical and virtual world. Identity management (IdM) -- the process of identifying an individual and controlling access to resources based on their associated privileges -- is becoming progressively complex. This has brought the spotlight on the importance of effective and efficient means of ascertaining an individualOCOs identity. Biometric technologies like fingerprint recognition, face recognition, iris recognition etc. have a long history of use in law enforcement applications and are now transitioning towards commercial applications like password replacements, ATM authentication and others.This unique book provides you with comprehensive coverage of commercially available biometric technologies, their underlying principles, operational challenges and benefits, and deployment considerations. It also offers a look at the future direction these technologies are taking. By focusing on factors that drive the practical implementation of biometric technologies, this book serves to bridge the gap between academic researchers and industry practitioners. This book focuses on design, development, and deployment issues related to biometric technologies, including operational challenges, integration strategies, technical evaluations of biometric systems, standardization and privacy preserving principles, and several open questions which need to be answered for successful deployments."

Biometrics, Crime and Security The Stationery Office

Many governments around the world are calling for the use of biometric systems to provide crucial societal functions, consequently making it an urgent area for action. The current performance of some biometric systems in terms of their error rates, robustness, and system security may prove to be inadequate for large-scale applications to process millions of users at a high rate of throughput. This book focuses on fusion in biometric systems. It discusses the present level, the limitations, and proposed methods to improve performance. It describes the fundamental concepts, current research, and security-related issues. The book will present a computational perspective, identify challenges, and cover new problem-solving strategies, offering solved problems and case studies to help with reader comprehension and deep understanding. This book is written for researchers, practitioners, both undergraduate and post-graduate students, and those working in various engineering fields such as Systems Engineering, Computer Science, Information Technology, Electronics, and Communications.

Advanced Biometrics IAP

The Victorian Protective Data Security Framework (VPDSF) was established under Part 4 of Victoria's Privacy and Data Protection Act 2014 and provides direction to Victorian public sector agencies or bodies on their data security obligations. The VPDSF has been developed to monitor and assure the security of public sector information and information systems across the Victorian public sector (VPS). This document is primarily written to inform executives and designed to support information security practitioners across the VPS.

First Platoon Springer Science & Business Media

This book constitutes the refereed proceedings of the International Workshop on Multimedia Content Representation, Classification and Security, MRCS 2006. The book presents 100 revised papers together with 4 invited lectures. Coverage includes biometric recognition, multimedia content security, steganography, watermarking, authentication, classification for biometric recognition, digital watermarking, content analysis and representation, 3D object retrieval and classification, representation, analysis and retrieval in cultural heritage, content representation, indexing and retrieval, and more.