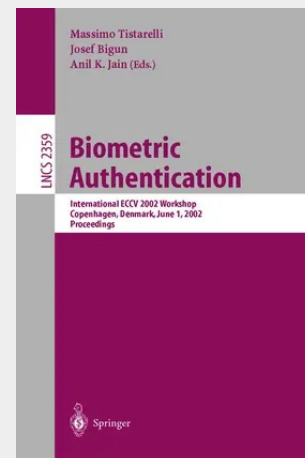


Biometric Authentication

International ECCV 2002 Workshop Copenhagen, Denmark, June 1, 2002 Proceedings

Biometric authentication refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics. It associates an individual with a previously determined identity based on that individual's appearance or behavior. Because many physiological or behavioral characteristics (biometric indicators) are distinctive to each person, biometric identifiers are inherently more reliable and more capable than knowledge-based (e.g., password) and token-based (e.g., a key) techniques in differentiating between an authorized person and a fraudulent impostor. For this reason, more and more organizations are looking to automated identity authentication systems to improve customer satisfaction, security, and operating efficiency as well as to save critical resources. Biometric authentication is a challenging pattern recognition problem; it involves more than just template matching. The intrinsic nature of biometric data must be carefully studied, analyzed, and its properties taken into account in developing suitable representation and matching algorithms. The intrinsic variability of data with time and environmental conditions, the social acceptability and invasiveness of acquisition devices, and the facility with which the data can be counterfeited must be considered in the choice of a biometric indicator for a given application. In order to deploy a biometric authentication system, one must consider its reliability, accuracy, applicability, and efficiency. Eventually, it may be necessary to combine several biometric indicators (multimodal-biometrics) to cope with the drawbacks of the individual biometric indicators.

Biometric authentication refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics. It associates an individual with a previously determined identity based on that individual's appearance or behavior. Because many physiological or behavioral characteristics (biometric indicators) are distinctive to each person, biometric identifiers are inherently more reliable and more capable than knowledge-based (e.g., password) and token-based (e.g., a key) techniques in differentiating between an authorized person and a fraudulent impostor. For this reason, more and more organizations are looking to automated identity authentication systems to improve customer satisfaction, security, and operating efficiency as well as to save critical resources. Biometric authentication is a challenging pattern recognition problem; it involves more than just template matching. The intrinsic nature of biometric data must be carefully studied, analyzed, and its properties taken into account in developing suitable representation and matching algorithms. The intrinsic variability of data with time and environmental conditions, the social acceptability and invasiveness of acquisition devices, and the facility with which the data can be counterfeited must be considered in the choice of a biometric indicator for a given application. In order to deploy a biometric authentication system, one must consider its reliability, accuracy, applicability, and efficiency. Eventually, it may be necessary to combine several biometric indicators (multimodal-biometrics) to cope with the drawbacks of the individual biometric indicators.



53,49 €

49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540437239

Medium: Buch

ISBN: 978-3-540-43723-9

Verlag: Springer Berlin Heidelberg

Erscheinungstermin: 17.05.2002

Sprache(n): Englisch

Auflage: 2002

Serie: Lecture Notes in Computer Science

Produktform: Kartoniert

Gewicht: 330 g

Seiten: 202

Format (B x H): 155 x 235 mm

