

ISO/IEC 24741:2024-06 (E)

Information technology - Biometrics - Overview and application

Contents

Page

- Foreword v
- Introduction vi
- 1 Scope 1
- 2 Normative references 1
- 3 Terms, definitions and abbreviated terms 1
 - 3.1 Terms and definitions 1
 - 3.2 Abbreviated terms 1
- 4 Fundamentals of biometrics 2
 - 4.1 Biometric characteristics 2
 - 4.2 Biometric systems 3
- 5 History 5
- 6 Overview of biometric technologies 6
 - 6.1 Finger and palm ridge recognition 6
 - 6.1.1 Fingerprint imaging 6
 - 6.1.2 Fingerprint comparison 7
 - 6.1.3 Palm technologies 8
 - 6.2 Face recognition 8
 - 6.3 Iris recognition 9
 - 6.4 Dynamic signature recognition 9
 - 6.5 Vascular recognition 10
 - 6.6 Hand geometry recognition 10
 - 6.7 Voice recognition 10
 - 6.8 DNA recognition 11
 - 6.9 Full body recognition 11
 - 6.10 Gait recognition 11
 - 6.11 Retina recognition 11
 - 6.12 Keystroke recognition 12
 - 6.13 Scent and odour recognition 12
 - 6.14 Cardiogram recognition 12
 - 6.15 Multimodal biometrics 12
- 7 General biometric system 12
 - 7.1 Conceptual representation of general biometric system 12
 - 7.2 Conceptual components of a general biometric system 13
 - 7.2.1 Data capture 13
 - 7.2.2 Transmission 13
 - 7.2.3 Signal processing 13
 - 7.2.4 Data storage 14
 - 7.2.5 Comparison 14
 - 7.2.6 Decision 14
 - 7.2.7 Administration 15
 - 7.2.8 Interface to external application 15
 - 7.3 Functions of general biometric system 15
 - 7.3.1 Enrolment 15
 - 7.3.2 Verification of a positive biometric claim 16
 - 7.3.3 Identification 17
- 8 Example applications 17

8.1	General.....	17
8.2	Physical access control.....	17
8.3	Logical access control.....	18
8.4	Time and attendance.....	18
8.5	Accountability.....	18
8.6	Electronic authorizations.....	18
8.7	Government and citizen services.....	18
8.8	Border protection.....	19
	8.8.1 ePassports and machine-readable travel documents.....	19
	8.8.2 Automated border control (ABC) systems.....	19
	8.8.3 Entry/exit systems.....	19
	8.8.4 Visas.....	19
	8.8.5 EURODAC.....	20
8.9	Law enforcement.....	20
8.10	Civil background checks.....	20
8.11	Clustering.....	20
9	Performance testing.....	20
	9.1 General.....	20
	9.2 Types of technical tests.....	21
10	Biometric technical interfaces.....	22
	10.1 Biometric data blocks (BDBs) and biometric information record (BIRs).....	22
	10.2 Management of information on source of biometric data.....	23
	10.3 Service architectures.....	23
	10.4 The BioAPI application programming interface.....	24
	10.5 The BioAPI interworking protocol (BIP).....	24
11	Biometrics and information security.....	25
	11.1 General.....	25
	11.2 Security of biometric data.....	25
	11.3 Presentation attack (spoofing) detection.....	28
	11.4 Integrity of the enrolment process.....	28
12	Biometrics and privacy.....	29
	12.1 General.....	29
	12.2 Privacy protections for biometric applications.....	30
	12.3 Proportional application of biometrics.....	30
	12.4 Biometric technology acceptability.....	31
	12.5 Confidentiality of biometric data.....	31
	12.6 Integrity of biometric data.....	31
	12.7 Irreversibility of biometric data.....	32
	12.8 Unlinkability of biometric information.....	32
13	Overview of biometric standardisation.....	32
	13.1 Standards development organizations.....	32
	13.2 Types of biometric standards.....	33
	13.2.1 Biometric data interchange format standards.....	33
	13.2.2 Biometric technical interface standards.....	34
	13.2.3 Biometric conformance testing standards.....	34
	13.2.4 Biometric sample quality standards.....	35
	13.2.5 Biometric application profile standards.....	35
	13.2.6 Biometric performance testing and reporting standards.....	36
	13.2.7 Biometric security standards.....	37
	13.2.8 Biometric authentication standards.....	37
	13.2.9 Standards on cross-jurisdictional and societal aspects of biometrics.....	38
	13.2.10 Biometric vocabulary standards.....	39
	13.3 Criteria for selecting a standard.....	39
	Bibliography.....	41