

1. Record Nr.	UNINA9910915784703321
Autore	Chatterjee Amit
Titolo	Biometric Presentation Attack Detection : Towards Securing Biometric Authentication Systems
Pubbl/distr/stampa	Bristol : , : Institute of Physics Publishing, , 2023 ©2023
ISBN	9780750352048 0750352043
Edizione	[1st ed.]
Descrizione fisica	1 online resource (229 pages)
Collana	IOP Ebooks Series
Soggetti	Biometric identification Security systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Acknowledgements -- Author biography -- Amit Chatterjee -- List of acronyms -- Chapter Biometrics -- 1.1 Introduction -- 1.2 Types of biometrics -- 1.2.1 Physiological identifiers -- 1.2.2 Behavioral identifiers -- 1.3 Applications -- 1.3.1 Generic applications -- 1.3.2 Specific applications -- 1.4 Biometrics authentication architecture -- 1.5 ISO standards -- 1.6 Databases -- References -- Chapter Presentation attack detection in biometrics -- 2.1 Introduction -- 2.2 Historical survey -- 2.3 Types of presentation attacks -- 2.4 Preparation of spoofed specimen -- 2.4.1 2D fake -- 2.4.2 3D fake -- 2.5 Existing PA detection technologies -- 2.6 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards -- 2.7 Databases -- References -- Chapter Fringe projection-based secure biometrics -- 3.1 Introduction -- 3.2 Theory -- 3.2.1 Basic configuration -- 3.2.2 Calibration -- 3.3 Processing strategy -- 3.3.1 Phase shifting -- 3.3.2 Fourier transform -- 3.3.3 Unwrapping -- 3.4 Experiments and results -- 3.4.1 Fingerprint -- 3.4.2 Palmprint -- 3.4.3 Face -- 3.4.4 Photo and video attack -- 3.4.5 Ear: a simulation experiment -- 3.5 Discussion -- References -- Chapter Biometric presentation attack detection using speckle metrology -- 4.1 Introduction -- 4.2 Theory -- 4.2.1 Speckle -- 4.2.2 Biospeckle -- 4.2.3 Quality parameters -- 4.3 Processing

strategy -- 4.3.1 Numerical indexing -- 4.3.2 Visual analysis -- 4.3.3 Automated region of interest (ROI) selection -- 4.4 Experimental and results -- 4.4.1 Generalized configuration -- 4.4.2 Fingerprint -- 4.4.3 Retina -- 4.4.4 Palmprint and face -- 4.5 Discussion -- References -- Chapter Presentation attack detection using fringe projection and biospeckle analysis -- 5.1 Introduction -- 5.2 Processing strategies -- 5.2.1 Fringe projection. 5.2.2 Biospeckle analysis -- 5.3 Experimental descriptions and results -- 5.3.1 Fingerprint anti-spoofing -- 5.3.2 Palmprint anti-spoofing -- 5.3.3 Ear anti-spoofing -- 5.4 Discussion -- References -- Chapter Presentation attack detection using optical coherence tomography -- 6.1 Introduction -- 6.2 Theory -- 6.2.1 Skin physiology -- 6.2.2 OCT imaging -- 6.3 Experimental descriptions and results -- 6.3.1 TD-OCT-based PA detection -- 6.3.2 FD-OCT-based PA detection -- 6.3.3 FF-OCT-based PA detection -- 6.4 Discussion -- 6.4.1 Balancing sensitivity and imaging speed -- References -- Chapter Thermography-based presentation attack detection -- 7.1 Introduction -- 7.2 Theory -- 7.3 Experiments and results -- 7.3.1 Thermal-only approach -- 7.3.2 Multispectral approach -- 7.4 Discussion -- References -- Chapter Miscellaneous -- 8.1 Introduction -- 8.2 Topography-based techniques -- 8.2.1 Color texture analysis -- 8.2.2 Motion detection -- 8.2.3 Laser triangulation -- 8.2.4 Stereo vision -- 8.3 Internal property-based techniques -- 8.3.1 Pulse oximetry -- 8.3.2 Ultrasound sensor -- 8.3.3 Impedance-based technique -- 8.4 Hybrid techniques -- 8.4.1 Fringe projection thermography -- 8.4.2 Multimodal biometrics -- References -- Chapter Patents: basics and selected descriptions -- 9.1 Introduction -- 9.2 Patent process flow -- 9.3 Criteria for patent grant -- 9.4 Selected patents for biometric presentation attack detection -- 9.5 Patentability-an example -- References -- Chapter Preliminary experiments and research ideas -- 10.1 Introduction -- 10.2 Fringe projection -- 10.3 Speckle metrology -- 10.4 Speckle projection -- 10.5 Multiwavelength analysis -- 10.6 Extreme attacks -- References.

Sommario/riassunto

This book discusses anti-spoofing techniques in detail. For each anti-spoofing technology, different experimental configurations, processing strategies, scope for generalization, advantages and limitations are detailed. The book also considers applicability of artificial intelligence techniques for automated biometric spoof detection, and future scope of research in this direction.