1. Record Nr. UNINA9910448656303321

Autore	Viganò, Francesco
Titolo	Studiare sui casi : materiali integrativi per il corso di diritto penale : parte generale / Francesco Viganò, Melissa Miedico, Tommaso Trinchera
Pubbl/distr/stampa	Torino, : Giappichelli, 2020
ISBN	978-88-921-1384-8
Descrizione fisica	XXI, 204 p. ; 24 cm
Altri autori (Persone)	Miedico, Melissa Trinchera, Tommaso
Locazione	DSPCP
Collocazione	4,1-410
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNINA9910585799903321

Titolo	Multimedia security 2 : biometrics, video surveillance and multimedia encryption / / edited by William Puech
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, , [2022] ©2022
ISBN	1-119-98739-3 1-394-15038-5
Descrizione fisica	1 online resource (320 pages)
Disciplina	006.7
Soggetti	Interactive multimedia Multimedia systems Artificial intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Half-Title Page -- Title Page -- Copyright Page -- Contents -- Foreword by Gildas Avoine -- Foreword by Cédric Richard -- Preface -- Chapter 1. Biometrics and Applications -- 1.1. Introduction -- 1.2. History of biometrics -- 1.3. The foundations of biometrics -- 1.3.1. Uses of biometrics -- 1.3.2. Definitions -- 1.3.3. Biometric modalities -- 1.4. Scientific issues -- 1.4.1. Presentation attacks -- 1.4.2. Acquisition of new biometric data or hidden biometrics -- 1.4.3. Quality of biometric data -- 1.4.4. Efficient representation of biometric data -- 1.4.5. Protecting biometric data -- 1.4.6. Aging biometric data -- 1.5. Conclusion -- 1.6. References -- Chapter 2. Protecting Documents Using Printed Anticopy Elements -- 2.1. Introduction -- 2.2. Document authentication approaches: an overview -- 2.3. Print test shapes -- 2.3.1. Print test signatures -- 2.3.2. Glyphs -- 2.3.3. Guilloches -- 2.4. Copy-sensitive graphical codes -- 2.4.1. Copy detection pattern -- 2.4.2. Two-level barcodes -- 2.4.3. Watermarked barcodes -- 2.4.4. Performance of CSGC authentication -- 2.5. Conclusion -- 2.6. References -- Chapter 3. Verifying Document Integrity -- 3.1. Introduction -- 3.2. Fraudulent manipulation of document images -- 3.2.1. Imitation -- 3.2.2. Copy-and-paste of a

region from the same document -- 3.2.3. Copy-and-paste of a region from another document -- 3.2.4. Deleting information -- 3.3. Degradation in printed and re-scanned documents -- 3.3.1. Degradations linked to the print process -- 3.3.2. Degradations linked to scanning -- 3.3.3. Degradation models -- 3.4. Active approaches: protection by extrinsic fingerprints -- 3.4.1. Watermarking a document -- 3.4.2. Digital signatures -- 3.5. Passive approaches: detecting intrinsic characteristics -- 3.5.1. Printer identification -- 3.5.2. Detecting graphical clues -- 3.5.3. Other approaches.
3.6. Conclusion -- 3.7. References -- Chapter 4. Image Crypto-Compression -- 4.1. Introduction -- 4.2. Preliminary notions -- 4.2.1. The JPEG image format -- 4.2.2. Introduction to cryptography -- 4.3. Image encryption -- 4.3.1. Naive methods -- 4.3.2. Chaos-based methods -- 4.3.3. Encryption-then-compression -- 4.4. Different classes of crypto-compression for images -- 4.4.1. Substitution-based crypto-compression -- 4.4.2. Shuffle-based crypto-compression -- 4.4.3. Hybrid crypto-compression -- 4.5. Recompressing crypto-compressed JPEG images -- 4.5.1. A crypto-compression approach robust to recompression -- 4.5.2. Recompression of a crypto-compressed image -- 4.5.3. Decoding a recompressed version of a crypto-compressed JPEG image -- 4.5.4. Illustration of the method -- 4.6. Conclusion -- 4.7. References -- Chapter 5. Crypto-Compression of Videos -- 5.1. Introduction -- 5.1.1. Background -- 5.1.2. Video compression -- 5.1.3. Video security -- 5.2. State of the art -- 5.2.1. Naive encryption -- 5.2.2. Partial encryption -- 5.2.3. Perceptual encryption -- 5.2.4. Crypto-compression methods -- 5.2.5. Selective encryption methods -- 5.3. Format-compliant selective encryption -- 5.3.1. Properties -- 5.3.2. Constant bitrate format compliant selective encryption -- 5.3.3. Standardized selective encryption -- 5.3.4. Locally applied selective encryption -- 5.3.5. Decrypting selective encryption -- 5.4. Image and video quality -- 5.4.1. Experiments on encryption solutions -- 5.4.2. Video quality: experimental results -- 5.4.3. CSE: a complete real-time solution -- 5.5. Perspectives and directions for future research -- 5.5.1. Versatile Video Coding -- 5.5.2. Immersive and omnidirectinal video -- 5.6. Conclusion -- 5.7. References -- Chapter 6. Processing Encrypted Multimedia Data Using Homomorphic Encryption -- 6.1. Context.
6.2. Different classes of homomorphic encryption systems -- 6.2.1. Partial solutions in classic cryptography -- 6.2.2. Complete solutions in cryptography using Euclidean networks -- 6.3. From theory to practice -- 6.3.1. Algorithmics -- 6.3.2. Implementation and optimization -- 6.3.3. Managing and reducing the size of encrypted elements -- 6.3.4. Security -- 6.4. Proofs of concept and applications -- 6.4.1. Facial recognition -- 6.4.2. Classification -- 6.4.3. RLE and image compression -- 6.5. Conclusion -- 6.6. Acknowledgments -- 6.7. References -- Chapter 7. Data Hiding in the Encrypted Domain -- 7.1. Introduction: processing multimedia data in the encrypted domain -- 7.1.1. Applications: visual secret sharing -- 7.1.2. Applications: searching and indexing in encrypted image databases -- 7.1.3. Applications: data hiding in the encrypted domain -- 7.2. Main aims -- 7.2.1. Digital rights management -- 7.2.2. Cloud storage -- 7.2.3. Preserving patient confidentiality -- 7.2.4. Classified data -- 7.2.5. Journalism -- 7.2.6. Video surveillance -- 7.2.7. Data analysis -- 7.3. Classes and characteristics -- 7.3.1. Properties -- 7.3.2. Classic approaches to encryption -- 7.3.3. Evaluation criteria -- 7.4. Principal methods -- 7.4.1. Image partitioning -- 7.4.2. Histogram shifting -- 7.4.3. Encoding -- 7.4.4. Prediction -- 7.4.5. Public key encryption -- 7.5. Comparison and discussion -- 7.6. A high-capacity data hiding