

# Table des matières

<b>Préface de Gildas Avoine</b> . . . . .	1
Gildas AVOINE	
<b>Préface de Cédric Richard</b> . . . . .	3
Cédric RICHARD	
<b>Avant-propos</b> . . . . .	5
William PUECH	
<b>Chapitre 1. Biométrie et applications</b> . . . . .	9
Christophe CHARRIER, Christophe ROSENBERGER et Amine NAIT-ALI	
1.1. Introduction . . . . .	9
1.2. Histoire de la biométrie . . . . .	11
1.3. Les bases de la biométrie . . . . .	15
1.3.1. Les usages de la biométrie . . . . .	15
1.3.2. Définitions . . . . .	16
1.3.3. Les modalités biométriques . . . . .	16
1.4. Les enjeux scientifiques . . . . .	18
1.4.1. Attaques par présentation . . . . .	18
1.4.2. Acquisition de nouvelles données biométriques ou biométrie cachée . . . . .	21
1.4.3. Qualité des données biométriques . . . . .	23
1.4.4. Représentation efficace des données biométriques . . . . .	29
1.4.5. Protection des données biométriques . . . . .	31
1.4.6. Vieillessement des données biométriques . . . . .	34
1.5. Conclusion . . . . .	36
1.6. Bibliographie . . . . .	36

<b>Chapitre 2. Protection de documents par impression d'éléments anticopies</b> . . . . .	41
Iuliia TKACHENKO, Alain TREMEAU et Thierry FURNEL	
2.1. Introduction . . . . .	41
2.2. Panorama des approches en authentification de documents . . . . .	43
2.3. Formes-tests d'impression . . . . .	45
2.3.1. Figures-tests d'impression . . . . .	47
2.3.2. Glyphes . . . . .	49
2.3.3. Guilloches . . . . .	51
2.4. Codes graphiques sensibles à la copie . . . . .	52
2.4.1. Codes de détection de copie . . . . .	53
2.4.2. Codes à barres à deux niveaux . . . . .	56
2.4.3. Codes à barres tatoués . . . . .	58
2.4.4. Performance d'une authentification par CSGC . . . . .	59
2.5. Conclusion . . . . .	63
2.6. Bibliographie . . . . .	64
<b>Chapitre 3. Vérification de l'intégrité des documents</b> . . . . .	71
Petra GOMEZ-KRÄMER	
3.1. Introduction . . . . .	71
3.2. Manipulations frauduleuses des images de documents . . . . .	74
3.2.1. Imitation . . . . .	74
3.2.2. Copier-coller d'une région provenant du même document . . . . .	74
3.2.3. Copier-coller d'une région provenant d'un autre document . . . . .	75
3.2.4. Suppression d'information . . . . .	76
3.3. Dégradations des documents imprimés et renumérisés . . . . .	76
3.3.1. Dégradations liées au processus d'impression . . . . .	77
3.3.2. Dégradations liées au processus de numérisation par scanner . . . . .	78
3.3.3. Modèles de dégradation . . . . .	79
3.4. Approches actives : protection par empreintes extrinsèques . . . . .	81
3.4.1. Tatouage de document . . . . .	81
3.4.2. Signatures numériques . . . . .	86
3.5. Approches passives : détection de caractéristiques intrinsèques . . . . .	90
3.5.1. Identification de l'imprimante . . . . .	90
3.5.2. Détection des indices graphiques . . . . .	94
3.5.3. Autres approches . . . . .	95
3.6. Conclusion . . . . .	96
3.7. Bibliographie . . . . .	96

**Chapitre 4. Crypto-compression d'images** . . . . . 105

Vincent ITIER, Pauline PUTEAUX et William PUECH

4.1. Introduction	105
4.2. Notions préliminaires	107
4.2.1. Le format d'image JPEG	107
4.2.2. Fondements en cryptographie	111
4.3. Chiffrement d'images	115
4.3.1. Méthodes naïves	117
4.3.2. Méthodes basées chaos	119
4.3.3. Chiffrement-puis-compression	120
4.4. Différentes classes de crypto-compression d'images	121
4.4.1. Crypto-compression par substitution	122
4.4.2. Crypto-compression par mélange	124
4.4.3. Crypto-compression hybride	126
4.5. Recompression d'images JPEG crypto-compressées	129
4.5.1. Une approche de crypto-compression robuste à la recompression	130
4.5.2. Comment recompresser une image crypto-compressée ?	133
4.5.3. Décodage de l'image JPEG crypto-compressée recompressée	135
4.5.4. Illustration de la méthode	137
4.6. Conclusion	138
4.7. Bibliographie	140

**Chapitre 5. Crypto-compression de vidéos** . . . . . 145

Cyril BERGERON, Wassim HAMIDOUCHE et Olivier DÉFORGES

5.1. Introduction	145
5.1.1. Historique	145
5.1.2. La compression vidéo	146
5.1.3. La sécurité dans le domaine de la vidéo	147
5.2. État de l'art	148
5.2.1. Chiffrement dit naïf	149
5.2.2. Chiffrement partiel	150
5.2.3. Chiffrement perceptuel	150
5.2.4. Méthodes de crypto-compression	151
5.2.5. Méthodes de chiffrement sélectif	152
5.3. Chiffrement sélectif compatible du format	153
5.3.1. Propriétés	153
5.3.2. Chiffrement sélectif compatible du format à débit binaire constant	155
5.3.3. Chiffrement sélectif standardisé	157

5.3.4. Chiffrement sélectif appliqué localement . . . . .	160
5.3.5. Décrypter le chiffrement sélectif . . . . .	166
5.4. Qualité des images et vidéos . . . . .	167
5.4.1. Expérimentations sur les solutions de chiffrement . . . . .	169
5.4.2. Résultats expérimentaux sur la qualité des vidéos . . . . .	171
5.4.3. Système CSE : une solution complète temps-réel . . . . .	179
5.5. Perspectives ouvertes et futures directions de recherche . . . . .	180
5.5.1. <i>Versatile Video Coding (VVC)</i> . . . . .	181
5.5.2. Vidéos immersives et omnidirectionnelles . . . . .	182
5.6. Conclusion . . . . .	183
5.7. Bibliographie . . . . .	183

## **Chapitre 6. Traiter des données multimédia chiffrées grâce au chiffrement homomorphe**

Sébastien CANARD, Sergiu CARPOV, Caroline FONTAINE et Renaud SIRDEY

6.1. Contexte . . . . .	191
6.2. Différentes classes de systèmes de chiffrement homomorphes . . . . .	194
6.2.1. Solutions partielles en cryptographie classique . . . . .	194
6.2.2. Solutions complètes en cryptographie utilisant les réseaux euclidiens . . . . .	196
6.3. Comment passer de la théorie à la pratique ? . . . . .	199
6.3.1. Algorithmique . . . . .	201
6.3.2. Implémentation et optimisation . . . . .	201
6.3.3. Comment gérer et réduire la taille des chiffrés ? . . . . .	207
6.3.4. Sécurité . . . . .	210
6.4. Preuves de concept et applications . . . . .	212
6.4.1. Reconnaissance de visages . . . . .	212
6.4.2. Classification . . . . .	215
6.4.3. RLE et compression d'images . . . . .	221
6.5. Conclusion . . . . .	226
6.6. Remerciements . . . . .	226
6.7. Bibliographie . . . . .	227

## **Chapitre 7. Insertion de données cachées dans le domaine chiffré**

Pauline PUTEAUX et William PUECH

7.1. Introduction : traitement des données multimédia dans le domaine chiffré . . . . .	233
7.1.1. Applications en partage de secret visuel . . . . .	235
7.1.2. Applications en recherche et indexation dans des bases d'images chiffrées . . . . .	235

7.1.3. Applications en insertion de données cachées dans le domaine chiffré . . . . .	236
7.2. Motivations . . . . .	237
7.2.1. Gestion des droits numériques . . . . .	238
7.2.2. Stockage sur le Cloud . . . . .	239
7.2.3. Préservation de la vie privée des patients . . . . .	239
7.2.4. Données classées . . . . .	239
7.2.5. Journalisme . . . . .	239
7.2.6. Vidéosurveillance . . . . .	239
7.2.7. Analyse de données . . . . .	240
7.3. Différentes classes et caractéristiques . . . . .	240
7.3.1. Propriétés . . . . .	240
7.3.2. Approches classiquement utilisées pour le chiffrement . . . . .	242
7.3.3. Critères d'évaluation . . . . .	246
7.4. Principales méthodes . . . . .	250
7.4.1. Partition de l'image . . . . .	250
7.4.2. Décalage d'histogramme . . . . .	251
7.4.3. Codage . . . . .	254
7.4.4. Prédiction . . . . .	255
7.4.5. Chiffrement à clé publique . . . . .	256
7.5. Comparaison et discussion . . . . .	257
7.6. IDCDC haute capacité basée sur la prédiction des MSB . . . . .	258
7.6.1. Description générale de la méthode . . . . .	259
7.6.2. Approche IDCHC-CEP . . . . .	262
7.6.3. Approche IDCHC-SEP . . . . .	265
7.6.4. Résultats expérimentaux sur les deux approches . . . . .	269
7.7. Conclusion . . . . .	273
7.8. Bibliographie . . . . .	273

## **Chapitre 8. Partage d'images et d'objets 3D secrets . . . . . 279**

Sébastien BEUGNON, Pauline PUTEAUX et William PUECH

8.1. Introduction . . . . .	279
8.2. Partage de secret . . . . .	282
8.2.1. Méthodes classiques . . . . .	282
8.2.2. Aspects hiérarchiques . . . . .	284
8.3. Partage d'image secrète . . . . .	292
8.3.1. Principe . . . . .	292
8.3.2. Cryptographie visuelle . . . . .	293
8.3.3. Partage d'image secrète (à base de polynôme) . . . . .	294
8.3.4. Propriétés . . . . .	295
8.4. Partage d'objet 3D . . . . .	296
8.4.1. Principe . . . . .	296

8.4.2. Méthodes sans préservation du format . . . . .	297
8.4.3. Méthodes avec préservation du format . . . . .	298
8.5. Applications aux réseaux sociaux . . . . .	300
8.6. Conclusion . . . . .	308
8.7. Bibliographie . . . . .	309
<b>Liste des auteurs . . . . .</b>	<b>313</b>
<b>Index . . . . .</b>	<b>315</b>
<b>Sommaire de <i>Sécurité multimédia 1</i> . . . . .</b>	<b>319</b>