# Index

## A

A/V codec 430  
A/V scrambling 430  
access control, dynamic policy management 169  
access control list 90  
access control model 157–180  
adaptive image steganography 454–471  
adaptive steganography 457  
Advanced Encryption Standard (AES) 515  
analogue conversion 76  
Apple 41, 72, 86, 137  
asymmetric multiple description lattice vector quantization (AMDLVQ) 497  
audio and video (A/V) processing software 425  
audio encryption 432  
audio steganography 246  
authentication 67, 94, 305, 315  
authentication, and P2P networks 390  
authentication, basics 317–319  
authentication, message 317  
authentication, multimedia 318  
authorization 159

## B

Bayes classifier 362  
BCAST 62  
benign operation 303  
bit error rate (BER) 258  
Black Wolf’s Picture Encoder 442  
Blindside 356

blokiness 362  
BOBE attacks 95  
BOBE resistance 25, 90  
broadcast streams 65  
Byzantine Agreement protocols 394

## C

capacity 378, 379, 381, 538, 570  
capacity, and detection error rate 267  
certificate authority (CA) 59  
Chameleon 344  
chaotic watermark 287  
Chi-square tests 362  
CITADEL 90  
classification 358  
client-server network architecture 87  
closed circuit teleVision (CCTV) 120  
COiN-video 343  
collusion attack 476  
commercial watermarking 283  
compression 337  
conceptual process model 75  
confidentiality 316  
content creator 74, 77  
content distribution, and P2P networks 387  
content encapsulation 76  
content encryption key (CEK) 57  
content extraction 76  
content protection 45  
content provider 427  
content rendering environment 6
content wrapper 96
copyright balance principle 42
copyright protection, and A/V codec 425–438
copyright protection, and watermarking 282, 474
Coral architecture 80
covered communication. See steganography


D
Data Encryption Standard (DES) 515
data storage 170
desynchronization attack 476
debuggers 25
denial of service (DoS) attack 124, 387
detection error rate 267
DG11 95
Diffie-Hellman Key Exchange Protocol 181–200
digital book 22
digital certificates 391
digital content 500
digital images, and digital watermarking 277
Digital Millenium Copyright Act 40
digital multimedia 257
digital objects 6
digital rights management (DRM) 40, 56, 403, 407
digital rights management (DRM), and P2P networks 88
digital rights management (DRM), and security 71
digital rights management (DRM), for streaming media 22–38
digital rights management (DRM), techniques 23–24
digital signature 317
digital steganography 352–383, 439–453
digital video authentication 298–314
digital video broadcasting 423
digital video recorders (DVRs) 119
digital video watermarking 472
digital watermarking 277–297, 493
digital watermarking, and detection error rate 257–276
digital watermarking scheme 309

DiMaS system 90
direct memory access 33
discrete cosine transformation (DCT) 244, 442
Discrete Fourier Transform (DFT) 244
discrete wavelet transform 361
DRM content format (DCF) 60
DRM systems 6
DRM systems, and the role of RELs 17

E
embedding rate 362
encrypted information 97
encryption 30, 257
endorsement key 408
exception detection 46
exception management 39–54
eXtensible Markup Language (XML) 13
EzStego 364, 442

F
F5 368
FairPlay 89, 137, 140
feature generation 358
fidelity 355
fingerprinting 282, 341
Fisher linear discriminant 359
flexible multimedia stream authentication 315–334
fractal coding 517
fractal mating coding (FMC) 516
frequency-domain steganalytic system (FDSS) 442

G
generic bootstrapping architecture (GBA) 64
genetic algorithm (GA) 443
Gif-It-Up 364
GIF-Shuffle 363

H
H.264/AVC 216
H.264/AVC, and rate control scheme 217
hardware security anchor 404
Hiderman 376
high frequency components spatial (HFIS) image 458
human auditory system 355
human vision system (HVS) 259
human visual system 355
hybrid attack 476
Hydan 357

I

image quality measure (IQM) 442
image steganography 243, 454
information hiding 241–256, 354–356
information hiding capacity analysis 263
integrity 316
invisible secrets 374
iPod 137
iterative coding of multiple description (ICMD) 498
iTunes 72, 86, 137, 142

J

JHymn 143
Jobs, Steve 41
joint source fingerprinting 341
JPEGX 376
JSteg 366

K

Kazaa 86
key exchange protocol 181
key management 63
KL (Karhunen-Loeve) transform 362
kurtosis 361

L

Lessig, Lawrence 39
license creation 76
Linux 32, 140
local angular harmonic decomposition 361
locally most powerful 362

M

Marlin 81
mashup society 39
Masker 376
media distribution 335–351
message authentication 316, 317
message spreading, and information hiding 354–356
Mobile Phone Working Group (MPWG) 424
model based steganalysis 362
modified discrete cosine transform (MDCT) 425
motion estimation 214
Motion Picture Experts Group (MPEG) 3
motion vector 214, 425–438
MP3 compression 428
MP3Stego 372
MPEG-4 standard 139, 429
multimedia authentication 318
multimedia lifecycle 405
multimedia watermarking 493–514
multiple description coding (MDC) 493–514
multiple description quantization (MDQ) 495
multiple description video coding (MDVC) 500
Music2Share system 90
mutual authentication 67
MV scrambling (MVS) 435

N

noise replacement, and information hiding 354

O

objective trees, and security 77
OMA BCAST 63
OMA DRM v2.0 57
OMA Mobile Broadcast Services (BCAST) 62
Open eBook Forum (OeBF) 9
Open Mobile Alliance (OMA) 56
Open Mobile Alliance, digital rights manage-
ment (OMA DRM) 55–70
Open Mobile Alliance DRM 81
OutGuess 371

P

P-SAS 321
P2P file sharing 389
P2P systems, and content replication 386
P2PTunes 137–156
payload capacity 270
peer-to-peer (P2P) network 86–117, 384–402
Index

PicoDBMS 171
PiSAS 322
portability 95
principal component analysis 359
prisoner’s problem 353
proof of ownership 475
Protable Document Format (PDF) 4
pseudorandom watermark 287
public-key infrastructure (PKI) 59, 94, 384
public key exchange protocol 181
pure P2P 384–402

Q
quantization index modulation 357
quantization step-size 362

R
radio channel parameters 219
Read-Write Internet 39
replaying attacks 165
RGB color space 361
rights expression languages (RELs) 1–21
rights expression languages (RELs), an overview 2–3
rights expression languages (RELs), formalization of 9
rights expression languages (RELs), logic-based 14
rights expression languages (RELs), XML-based 13
rights object (RO) 57
rights verification 46
robustness 354
robust video watermarking 477

S
S-Tools 366
satellite distribution 335
scalable distribution 336
scrambling 28
scrambling algorithm 32
secret sharing 201–210, 203
secret sharing schemes 202
secure boot 424
secure chip 163
secure hardware 158, 162
secure multimedia distribution xii, 39
secure software 162
security, and objective trees 77
security, and P2P networks 389
security, and stakeholder analysis 73
security, and value-creation chain 403
security, physical 120
sequential hypothesis 362
sequential steganography 362
shrinkage 369
signal processing 306
skewness 361
snooping attacks 165
software protection 24
software self-defense 24
spatial-domain steganalytic system (SDSS) 442
spatial tampering 299, 303
splicing attacks 165
spoofing attacks 165
spread spectrum 357
spread spectrum watermarking 286
stakeholder, and content creator 74
stakeholder analysis, and security 73
steganalysis 354, 439
steganography 241–256, 278, 352–383, 439, 455
steganography, audio 246
steganography, digital 439–453
steganography, image 243
steganography, in black & white images 249
steganography, in Web pages 250
steganography, text 247
steganography, video 244
Steganos 356
Stegdetect 374
StegoDos 442
Stegotif 356
Stego Watch 377
StegSpy 376
stream authentication 320
streaming media, and DRM 22–38
streaming media system 27
structural similarity metric 458
superdistribution 61
support vector machine 359
surveillance camera systems 299

T

tampering operation 303
technical protection measures 40
temporal tampering 299
text steganography 247
threshold cryptography 393
Trithemius, John 242
trust, and value-creation chain 403–424
trust anchor 407
trust boundary 405
trusted computing 405
trusted computing base (TCB) 404
Trusted Computing Group 407
Trusted Platform Module (TPM) 407
trusted third parties (TTPs) 385

U

universal steganalysis 358
usage control, secure enforcement of access 162

V

variance 361
video authentication 300
video authentication techniques 306
video capturing 120
video coding standards 212
video compression 213
video encoding 120, 125
video encryption 434
video monitoring 120
video recording 120
video steganography 244
video surveillance, case study 129
video surveillance over IP 122–136
video surveillance systems 118–136
video traffic 126
video transmission 120
video watermarking 244, 472–492
video watermarking, capacity 474
video watermarking, robustness 474
video watermarking, transparency 474
video watermarking attacks 476
visual steganalytic system (VSS) 446

W

watercasting 339
watermark 142
watermark, embedded 501
watermark detection 290
watermark embedding 285, 338, 502
watermarking 244, 259, 279, 336, 472, 516
watermarking, and copyright protection 474
watermarking, client based 344
watermarking, commercial 283
watermarking, digital 277–297, 493
watermarking, individual 339
watermarking, multimedia 493–514
watermarking, network based 339
watermarking capacity 261
watermarking process 283
watermark types 284
wavelet coding 337
Wi-Fi 123
Windows Media Player 29
wireless mesh networks 118
wireless video transmission 211–240
worm 26

X

XPath expressions 157
xsteg 376

Y

YouTube 86