

Contents

1	Information Transmission Systems.....	1
1.1	Terminology	1
1.2	Role of an ITS.....	2
1.3	Model of an ITS.....	3
	References	5
2	Statistical and Informational Model of an ITS	7
2.1	Memoryless Information Sources	7
2.2	Measure of Discrete Information	8
2.3	Information Entropy for a DMS (Shannon Entropy)	11
2.4	Source Redundancy and Efficiency	13
2.5	Entropy of an Extended Discrete Memoryless Source: $H(X_n)$	14
2.6	Moments and Moment Rate.....	14
2.7	Information Rate, Decision Rate.....	15
2.8	Discrete Transmission Channels	16
2.8.1	Probabilities and Entropies in Discrete Channels	16
2.8.2	Mutual Information and Transinformation.....	21
2.8.3	Relationships between Entropies	21
2.8.4	Channel Capacity Using the Noise Matrix.....	23
2.8.5	Shannon Capacity.....	30
2.9	Memory Sources (Markov Sources)	38
2.9.1	Finite and Homogeneous Markov Chains	39
2.9.2	Entropy of m-th Order Markov Source	43
2.9.3	Applications	46
	References	51
3	Source Coding	53
3.1	What Is Coding and Why Is It Necessary?	53
3.2	Aim of Source Coding	55
3.3	Information Representation Codes	55
3.3.1	Short History	55
3.3.2	Natural Systems	56
3.3.3	Binary Codes Used in Data Transmission, Storage or Computing.....	58

3.3.4	Pulse Code Modulation (PCM)	65
3.3.5	Genetic Code	76
3.4	Coding Efficiency: Compression Ratio	80
3.5	Existence Theorem for Instantaneous and Uniquely Decodable Codes (Kraft and McMillan Inequalities)	82
3.6	Shannon First Theorem (1948)	84
3.7	Lossless Compression Algorithms	85
3.7.1	Shannon-Fano Binary Coding	85
3.7.2	Huffman Algorithms	88
3.7.3	Run Length Coding (RLC)	95
3.7.4	Comma Coding	100
3.7.5	Dictionary Techniques [41]	101
3.7.6	Lempel-Ziv Type Algorithms (LZ)	102
3.7.7	Arithmetic Coding	107
3.8	Lossy Compression in Differential Coding	109
3.8.1	Differential Pulse Code Modulation (DPCM)	109
3.8.2	Delta Modulation (DM)	111
3.8.3	Delta-Sigma Modulation	115
3.8.4	Comparison and Applications of Digital Modulations	116
3.9	Conclusions on Compression	116
	References	118
4	Cryptography Basics	121
4.1	Short History of Cryptography	121
4.2	Terminology	123
4.3	Cryptosystems: Role and Classification	123
4.4	Cryptanalytic Attacks and Algorithms Security	125
4.5	Classic Cryptography	127
4.5.1	Definition and Classification	127
4.5.2	Caesar Cipher	128
4.5.3	Polybius Cipher	130
4.5.4	Playfair Cipher	131
4.5.5	Trithemius Cipher	132
4.5.6	Vig��n��re Cipher	134
4.6	Modern Symmetric (Conventional) Cryptography	135
4.6.1	Definitions and Classification	135
4.6.2	Block Ciphers	137
4.6.2.1	Main Features	137
4.6.2.2	DES (Data Encryption Standard)	139
4.6.2.3	Some Other Block Ciphers	147
4.6.2.4	Block Cipher Operation Modes	150
4.6.3	Stream Ciphers	153
4.6.3.1	General Features	153
4.6.3.2	Some Stream Ciphers	157
4.6.4	Authentication with Symmetric Cryptography	158

4.7	Public Key Cryptography	159
4.7.1	Principle of the Public Key Cryptography	159
4.7.2	Public Keys Ciphers	162
4.8	Digital Watermarking	164
4.8.1	Introduction	164
4.8.2	Short History	167
4.8.3	Watermarking Requirements	168
4.8.4	Basic Principles of Watermarking	169
4.8.5	Specific Attacks	177
4.8.5.1	Attack Definition and Classification	177
4.8.5.2	The Inversion Attack / IBM / Confusion / Deadlock / Fake Watermark / Fake Original	178
4.8.5.3	The Collusion Attack	180
4.8.6	Applications	181
4.8.6.1	Broadcast Monitoring	181
4.8.6.2	Owner Identification: Proof of Ownership	182
4.8.6.3	Fingerprinting (Transaction Tracking)	183
4.8.6.4	Content Authentication (Fragile Watermarking)	183
4.8.6.5	Copy Control	184
4.8.7	The Millennium Watermark System [53]	184
4.8.7.1	Introduction	184
4.8.7.2	Basic Principle of the Millennium System	185
4.8.7.3	Millennium Standard Implementation	188
4.8.7.4	Unsolved Problems	188
4.8.7.5	Copy Control [53]	189
4.8.7.6	Media Type Recognition	189
4.8.8	Some Remarks	189
4.9	DNA Cryptography	190
4.9.1	Introduction	190
4.9.2	Backgrounds of Biomolecular Technologies	190
4.9.3	Elements of Biomolecular Computation (BMC)	194
4.9.3.1	DNA OTP Generation	194
4.9.3.2	Conversion of Binary Data to DNA Format and Vice Versa	194
4.9.3.3	DNA Tiles and XOR with DNA Tiles	195
4.9.4	DNA Based Steganography and Cryptographic Algorithms	197
4.9.4.1	Steganography Technique Using DNA Hybridization	197
4.9.4.2	Chromosome DNA Indexing Algorithm	199
4.9.4.3	DNA XOR OTP Using Tiles	202
	References	204
5	Channel Coding	209
5.1	Shannon Second Theorem (Noisy Channels Coding Theorem)	209
5.2	Error Control Strategies	213

5.3	Classification of Error Control Codes.....	216
5.4	Representation of Binary Code Sequences	216
5.5	Parameters of Detecting and Error Correcting Codes.....	218
5.6	Maximum Likelihood Decoding (MLD)	220
5.7	Linear Block Codes	224
5.7.1	Linear Block Codes: Definition and Matrix Description	224
5.7.2	Error Syndrome.....	227
5.7.3	Dimensioning of Error Correcting Linear Block Codes.....	228
5.7.4	Perfect and almost Perfect Codes.....	228
5.7.5	Detection and Correction Capacity: Decoded BER	229
5.7.6	Relations between the Columns of H Matrix for Error Detection and Correction	230
5.7.7	Standard Array and Syndrome Decoding.....	232
5.7.8	Comparison between Linear Error Detecting and Correcting Block Codes	235
5.7.9	Hamming Group Codes.....	238
5.7.10	Some Other Linear Block Codes.....	253
5.8	Cyclic Codes.....	255
5.8.1	Definition and Representation.....	256
5.8.2	Algebraic Encoding of Cyclic Codes	257
5.8.3	Syndrome Calculation and Error Detection	265
5.8.4	Algebraic Decoding of Cyclic Codes.....	269
5.8.5	Circuits for Cyclic Encoding and Decoding.....	274
5.8.6	Cyclic One Error Correcting Hamming Code	286
5.8.7	Golay Code	290
5.8.8	Fire Codes	292
5.8.9	Reed–Solomon Codes	295
5.9	Convolutional Codes	312
5.9.1	Representation and Properties.....	312
5.9.2	Convolutional Codes Encoding.....	314
5.9.3	Graphic Representation of Convolutional Codes	320
5.9.4	Code Distance and d_{∞}	324
5.9.5	Decoding (Viterbi Algorithm, Threshold Decoding)	326
5.10	Code Interleaving and Concatenation	340
5.10.1	Interleaving	340
5.10.2	Concatenated Codes	342
5.11	Turbo Codes.....	346
5.11.1	Definition and Encoding	346
5.11.2	Decoding	348
5.11.2.1	Basic Principles.....	348
5.11.2.2	Viterbi Algorithm (VA) [46], [48]	349
5.11.2.3	Bidirectional Soft Output Viterbi Algorithm (SOVA) [46].....	357
5.11.2.4	MAP Algorithm	364
5.11.2.5	MAX-LOG-MAP Algorithm	372

5.11.2.6 LOG-MAP Algorithm	373
5.11.2.7 Comparison of Decoding Algorithms	374
5.12 Line (baseband) Codes.....	374
References	385
Appendix A: Algebra Elements.....	389
A1 Composition Laws	389
A1.1 Compositions Law Elements.....	389
A1.2 Stable Part	389
A1.3 Properties.....	389
A2 Modular Arithmetic	391
A3 Algebraic Structures	392
A3.1 Group	392
A3.2 Field	393
A3.3 Galois Field	393
A3.3.1 Field Characteristic.....	394
A3.3.2 Order of an Element	395
A4 Arithmetics of Binary Fields.....	395
A5 Construction of Galois Fields $GF(2^m)$	398
A6 Basic Properties of Galois Fields, $GF(2^m)$	402
A7 Matrices and Linear Equation Systems.....	410
A8 Vector Spaces	412
A8.1 Defining Vector Space	412
A8.2 Linear Dependency and Independency	413
A8.3 Vector Space	414
A9 Table for Primitive Polynomials of Degree k ($k_{max} = 100$).....	417
A10 Representative Tables for Galois Fields $GF(2^k)$	418
A11 Tables of the Generator Polynomials for BCH Codes	420
A12 Table of the Generator Polynomials for RS Codes	421
Appendix B: Tables for Information and Entropy Computing.....	427
B1 Table for Computing Values of $-\log_2(x)$, $0.01 \leq x \leq 0.99$	427
B2 Table for Computing Values of $-x \cdot \log_2(x)$, $0.001 \leq x \leq 0.999$	428
Appendix C: Signal Detection Elements.....	435
C.1 Detection Problem.....	435
C.2 Signal Detection Criteria.....	438
C.2.1 Bayes Criterion.....	438
C.2.2 Minimum Probability of Error Criterion (Kotelnikov- Siegert)	440
C.2.3 Maximum a Posteriori Probability Criterion (MAP).....	441
C.2.4 Maximum Likelihood Criterion (R. Fisher)	441
C.3 Signal Detection in Data Processing ($K = 1$)	442
C.3.1 Discrete Detection of a Unipolar Signal.....	442
C.3.2 Discrete Detection of Polar Signal	446

C.3.3 Continuous Detection of Known Signal448

C.3.4 Continuous Detection of Two Known Signals453

References459

Appendix D: Synthesis Example461

Subject Index.....475

Acronyms.....483