

Contents

1	Hash-Based Authentication of Digital Images in Noisy Channels	1
	Fawad Ahmed and Amir Anees	
1.1	Introduction	1
1.1.1	Basic Requirements of Data Security	2
1.1.2	Multimedia Security	2
1.1.3	Image Hash	4
1.1.4	Basic Requirements of Image Hashing	5
1.2	Review of Image Hashing Schemes	6
1.2.1	Statistic-Based Schemes	6
1.2.2	Relation-Based Schemes	7
1.2.3	Coarse Representation-Based Schemes	8
1.2.4	Matrix-Based Schemes	9
1.2.5	Low-Level Feature-Based Schemes	10
1.3	Illustration of an Image Hashing Scheme	11
1.3.1	Hash Generation Module	12
1.3.2	Image Verification Module	14
1.4	Reducing Size of Image Hash Using Quantization	15
1.4.1	Hash Generation Using 3-Bit Quantization	15
1.4.2	Image Verification Using 3-Bit Quantization	17
1.4.3	3-Bit Quantization Example	18
1.4.4	A 4-Bit Quantization Scheme	21
1.4.4.1	Hash Generation Using 4-Bit Quantization	21
1.4.4.2	Image Verification Using 4-Bit Quantization	23
1.4.4.3	Reduction in Hash Size Due to 4-Bit Quantization	25
1.4.4.4	Effect on Robustness and Tamper Detection Due to 4-Bit Quantization	25
1.5	Performance Evaluation	26
1.5.1	The Effect of Beta (β) on Hash Collision	27
1.5.2	Robustness to Channel Noise and JPEG Compression	28
1.5.3	Threshold Selection	30
1.5.4	Detection of Tampering	31

1.5.5	The Receiver Operating Characteristic Curve	32
1.5.6	Hash Size	33
1.6	Security Analysis	33
1.6.1	The Impact of Randomized Pixel Modulation on System's Security	34
1.6.2	Statistical Analysis	36
1.6.3	Effect of Secret Key on the Hash	37
1.6.4	Probability of Hash Collision	38
1.6.5	Quantization and System's Security	39
1.7	Conclusion	40
	References	41
2	Watermarking for Image Authentication	43
	Chen Ling and Obaid Ur-Rehman	
2.1	The Basis of Watermarking	44
2.2	Classification	46
2.2.1	Perceptibility	47
2.2.2	Detection Types	48
2.2.3	System Platform	49
2.2.4	Image Compression	49
2.2.5	Embedding Domain	49
2.2.5.1	LSB	50
2.2.5.2	SS	50
2.2.5.3	DCT	53
2.2.5.4	DWT	54
2.2.6	Robustness	54
2.2.7	Lossless	56
2.3	Requirements of Watermarking	57
2.3.1	Fidelity	57
2.3.2	Capacity	58
2.3.3	Robustness	58
2.3.4	Security	58
2.3.4.1	Malicious Attacks	59
2.3.4.2	Incidental Attack	61
2.3.4.3	Secret Key	61
2.3.5	Tamper Detection, Location, and Recovery	62
2.4	A Watermarking Algorithm for Image Authentication	64
2.4.1	Watermark Design	64
2.4.1.1	Feature Extraction	66
2.4.1.2	Watermark Embedding Approach	69
2.4.2	An Example Design Case	69
2.4.2.1	Goals	69
2.4.2.2	Hybrid Feature Watermark Generation	69

2.4.2.3	Watermark Embedding	71
2.4.2.4	Watermark Extraction and Authentication Procedure	71
	References	72
3	Perceptual Image Hashing Technique for Image Authentication in WMSNs	75
	Jinse Shin and Christoph Ruland	
3.1	Introduction	75
3.2	High Level Requirements for Image Authentication in WMSNs . . .	77
3.3	Previous Works on Data Authentication in WMSNs	80
3.4	Perceptual Image Hashing	81
3.4.1	Basic Concept	81
3.4.2	Desirable Properties	82
3.4.2.1	Perceptual Robustness	82
3.4.2.2	Fragility to Visual Distinct Image	83
3.4.2.3	Unpredictability of the Hash	83
3.5	Content Based Image Authentication Using Perceptual Image Hashing Technique	83
3.5.1	Image Statistics Based Approach	85
3.5.2	Relation Based Approach	87
3.5.3	Coarse Image Representation Based Approach	88
3.5.4	Low-level Image Representation Based Approach	89
3.6	Experiment Results	91
3.6.1	Robustness	92
3.6.2	Discriminability	95
3.6.3	Security	97
3.7	Conclusion	98
	References	102
4	A Review of Approximate Message Authentication Codes	105
	S. Amir Hossein Tabatabaei and Nataša Živić	
4.1	Introduction	105
4.1.1	Definitions and Notations	106
4.2	Dedicated AMAC Schemes	107
4.2.1	Majority-Based AMACs	107
4.2.1.1	Shifting Attack	108
4.2.1.2	Security Enhancement	109
4.2.1.3	Analysis of the Majority-Based AMACs	110
4.2.2	Noise Tolerant Message Authentication Codes (NTMACs)	112
4.2.2.1	Analysis of the NTMAC-Based AMACs	115
4.2.3	AMACs Based on Computational Security	117
4.2.3.1	Analysis of the Computational Security Based AMACs	119
4.2.4	Unconditionally Secure AMAC	120

4.2.4.1	Analysis of Unconditionally Secure AMAC	121
4.2.5	Comparison	121
4.3	Applications of Dedicated AMACs in Image Authentication Techniques	122
4.3.1	Extension of the MAJORITY-Based AMACs and the NTMACs	122
4.3.2	Extension of AMAC ₁ and AMAC ₂	123
4.4	Conclusion	125
	References	126
5	Fuzzy Image Authentication with Error Localization and Correction	129
	Obaid Ur-Rehman and Nataša Živić	
5.1	Introduction	129
5.2	Building Blocks of the Fuzzy Image Authentication Algorithms	131
5.2.1	Content Based Authentication	131
5.2.2	Discrete Cosine Transform	131
5.2.3	Error Correcting Codes	132
5.2.3.1	Error Correcting Codes in Image Authentication	132
5.2.3.2	Reed–Solomon Codes	132
5.2.3.3	Turbo Codes	133
5.3	Applications of Error Correcting Codes in Image Authentication	134
5.4	Fuzzy Image Authentication Codes with Error Localization and Correction	135
5.4.1	Fuzzy Authentication Based on Image Features	135
5.4.2	Image Error Correcting Column-Wise Message Authentication Code (IECC-MAC)	136
5.4.3	Image Error Correction Noise Tolerant Message Authentication Code (IEC-NTMAC)	141
5.5	Performance and Security Analysis of the Proposed Fuzzy Authentication Algorithms	146
5.5.1	Performance Study	146
5.5.2	Security Analysis	147
5.6	Simulation Results	148
5.6.1	Simulation Parameters	148
5.6.2	Data Rate Analysis	149
5.6.3	Simulation Results for IECC-MAC	150
5.6.4	Simulation Results Using IEC-NTMAC	152
5.6.5	Image Error Rate (IER)	152
	References	153
6	Robustness of Biometrics by Image Processing Technology	155
	Robin Fay and Christoph Ruland	
6.1	Introduction	155
6.2	Pattern Recognition and Biometric Authentication	156
6.2.1	Pattern Recognition Systems	156

6.2.2	Affine Invariant Pattern Recognition	157
6.2.2.1	The Problem of Affine Invariant Pattern Recognition	157
6.2.2.2	Alignment-Free Features	158
6.2.3	Biometric Authentication	161
6.2.3.1	Biometric Systems	161
6.2.3.2	Template Protection	163
6.2.3.3	Fingerprint Recognition	164
6.2.3.4	Vein Pattern Recognition	165
6.3	Feature Extraction in Fingerprint Biometrics	167
6.3.1	Global Features	167
6.3.2	Minutiae Based Feature Extraction	168
6.3.2.1	General	168
6.3.2.2	Minutiae Detection	168
6.3.2.3	Minutiae Description	170
6.3.3	Image Based Feature Extraction	171
6.3.3.1	Image Based Feature Detection	171
6.3.3.2	Image-Based Feature Description	173
6.4	A Comparison of Alignment-Free Biometric Systems	173
6.4.1	Global Methods	173
6.4.2	Image Based Methods	174
6.4.3	Minutiae-Based Methods	176
6.4.4	Summary	178
6.5	An Evaluation Strategy for Local Features	178
6.5.1	Evaluation of Local Feature Extractors	178
6.5.2	Repeatability	178
6.5.3	1-Precision-Recall	182
6.6	Conclusion	183
	References	184

Robust Image Authentication in the Presence of Noise

Zivic, N. (Ed.)

2015, XV, 187 p. 79 illus., 33 illus. in color., Hardcover

ISBN: 978-3-319-13155-9