Contents

Zusammenfassung i

Abstract iii

Gratitude v

Contents vi

List of Figures xi

List of Tables xiii

Abbreviations xv

1 Introduction 1
1.1 Background 1
1.2 Motivation 2
1.3 Contributions and Outline of the Thesis 3
1.3.1 Contributions 3
1.3.2 Outline 3

2 Related Work 7
2.1 Cryptology and Authentication Services of Data Origin 7
2.2 Approximate Message Authentication Codes 10
2.3 Image Authentication 12
2.3.1 Classification and Methods 12
2.3.2 Perceptual Image Hashing 14
2.3.3 Design Method of Perceptual Image Hashing 16

3 Fundamental Algorithms of AMACs 19
3.1 Definitions and Notations 19
3.2 Dedicated AMAC Schemes, Analysis and Applications 21
3.2.1 MAJORITY-based AMACs 21
3.2.2 Analysis of the Majority-based AMACs 24

3.2.3 Noise Tolerant Message Authentication Codes (NTMACs) . . . 28
3.2.4 Analysis of the NTMAC-based AMACs 30
3.2.5 AMACs Based on Computational Security 34
3.2.6 Analysis of the Computational Security Based AMACs 36
3.2.7 AMAC Based on Unconditionally Secure Model 37
3.2.8 Analysis of the Unconditionally Secure AMAC 38
3.2.9 Comparison 39
3.3 Application of AMACs in Image Authentication Methods 40
3.3.1 Matrix Transformation and Decomposition Methods in Image Processing 40
3.3.1.1 Discrete Cosine Transform 40
3.3.1.2 Singular Value Decomposition 41
3.3.1.3 Non-Negative Matrix Factorization 42
3.3.2 ROC curve 42
3.3.3 Image Message Authentication Code 43
3.3.4 NTMAC-based Image Authentication Schemes 44
3.3.5 Image Error Correction Row and Column-wise MAC 44
3.3.6 Image Error Correction Weighted Noise Tolerant MAC 45
3.3.7 Analysis of the IEC-WNTMAC 47
3.3.8 Security Consideration 48
3.3.9 Comparison 49

4 Security Models in Perceptual Image Hashing 51
4.1 Methods and Approaches 51
4.2 Information Theoretical Approaches 52
4.2.1 Differential Entropy 52
4.2.2 Unicity Distance 53
4.2.3 Conditional Entropy 53
4.2.4 Computational Complexity Model 54
4.3 Security Consideration of Some Perceptual Image Hashing Schemes . . 55
4.3.1 Security Analysis of a DWT-based Perceptual Image Hash . . . 55
4.3.2 Security Analysis of a Robust Image Hash Based on Dominant DCT Coefficients 59
4.4 Security Enhancement 62
4.4.1 Security Enhancement of the DWT-based Perceptual Image Hash 62
4.4.2 Security Enhancement of the Robust Image Hash Based on Dominant DCT Coefficients 64

5 A New Approximate Message Authentication Code 67
5.1 Motivation 67
5.2 Design Philosophy 68
5.2.1 Number of Bit Runs 68
5.2.2 Boolean Functions and Robustness 68
5.3 Specification of the Proposed Scheme 70
5.3.1 Tag Generation Algorithm 70

5.3.2 Verification Algorithm 70
5.4 Analysis of the Proposed Approach 71
5.4.1 Performance Analysis 71
5.4.2 Comparison Results 73
5.4.3 Security Analysis 74
5.5 Application of BAMAC in Image Authentication 76
5.5.1 Motivation 76
5.5.2 Perceptual Image Hashing Scheme for Binarized Images 76
5.5.3 Implementation and Experimental Results 78
5.5.3.1 Implementation Based on Image Binarization 78
5.5.3.2 Implementation Based on Binary Features 78
5.5.4 Experimental Results 79
5.5.4.1 Perceptual Robustness 79
5.5.4.2 Dependency on the Secret Key 80

6 A New Image Authentication Scheme 85
6.1 Two-phase Image Authentication Scheme 85
6.2 Image Hash Generation Algorithm 86
6.2.1 Preprocessing 86
6.2.2 Feature Extraction 86
6.2.3 Final Image Hash 87
6.3 Verification Algorithm 87
6.4 Variants 88
6.4.1 DCT-RS-based Variant 88
6.4.2 DWT-RS-based Variant 89
6.5 Experimental Results 89
6.5.1 Perceptual Robustness 89
6.5.2 Fragility 90
6.5.3 Comparison Results 91
6.5.3.1 DWT-based Image Hashing 91
6.5.3.2 SVD-based Image Hashing 92
6.5.3.3 Feature Point Based Image Hashing 92
6.5.3.4 Radon-based Image Hashing 92
6.5.3.5 NMF-based Image Hashing 93
6.5.4 Tamper Detection 93
6.6 Analysis 95
6.6.1 Parameters Setting 95
6.6.2 Security Analysis 98
6.6.3 Dependency on the Secret Key 100

7 Conclusion 101
7.1 Summarized Results of the Thesis 101
7.2 Future Works 102

Bibliography **105**