

# Contents

## Part I    Multimedia Systems

|  |    |
|--|----|
| <b>1    Introduction</b>   | 3  |
| 1.1   Video Coding   | 3  |
| 1.2   Embedded Systems and Reconfigurable Architectures                        | 6  |
| 1.3   Encryption Basics  | 8  |
| <b>2    Advances in Multimedia Encryption</b>                                  | 11 |
| 2.1   Introduction   | 11 |
| 2.2   Multimedia Encryption Problem  | 12 |
| 2.3   Common Approaches to Video Encryption                                    | 13 |
| 2.3.1   Scrambling   | 13 |
| 2.3.2   Post-compression Encryption Algorithm                                  | 17 |
| 2.3.3   Pre-compression Encryption Algorithm                                   | 19 |
| 2.3.4   Selective Encryption   | 19 |
| 2.3.5   Joint Video Compression and Encryption (JVCE)                          |    |
| Approaches   | 21 |
| 2.3.6   Future of JVCE Schemes   | 21 |
| References   | 22 |
| <b>3    Securing Multimedia Content Using Joint Compression and Encryption</b> | 23 |
| 3.1   Introduction   | 23 |
| 3.2   Basics   | 24 |
| 3.3   Our Approach   | 26 |
| References   | 28 |

## Part II   Examples

|   |    |
|---|----|
| <b>4    Polymorphic Wavelet Transform</b> | 33 |
| 4.1   Introduction                        | 33 |
| 4.2   Motivation and Insight              | 37 |

|          |   |           |
|----------|---|-----------|
| 4.2.1    | Daubechies 9/7-Tap Bi-orthogonal Filter . . . . .       | 38        |
| 4.2.2    | Le Gall's 5/3 Filter . . . . .                          | 39        |
| 4.3      | Background and Related Work . . . . .                   | 40        |
| 4.3.1    | Wavelet Transform Background . . . . .                  | 41        |
| 4.3.2    | Hardware Implementation of DWT . . . . .                | 42        |
| 4.4      | Poly-DWT Filter . . . . .                               | 43        |
| 4.4.1    | Parameterized Filter Design . . . . .                   | 43        |
| 4.4.2    | Numerical Study . . . . .                               | 44        |
| 4.4.3    | Candidate Filters . . . . .                             | 45        |
| 4.4.4    | Hardware Architectures . . . . .                        | 47        |
| 4.5      | Fixed Point Implementation . . . . .                    | 51        |
| 4.6      | Hardware (Re)-allocation . . . . .                      | 52        |
| 4.6.1    | 'On-the-Fly' Switching . . . . .                        | 52        |
| 4.6.2    | 'Bit-Width' Switching . . . . .                         | 54        |
| 4.7      | Experiments . . . . .                                   | 55        |
| 4.7.1    | Image Reconstruction Quality . . . . .                  | 55        |
| 4.7.2    | Hardware vs. Software Performance . . . . .             | 56        |
| 4.7.3    | Hardware Comparison . . . . .                           | 57        |
| 4.7.4    | Dynamic Bit Allocation . . . . .                        | 60        |
| 4.7.5    | Real-World Application . . . . .                        | 60        |
| 4.8      | Conclusions and Future Work . . . . .                   | 62        |
|          | References . . . . .                                    | 62        |
| <b>5</b> | <b>The Secure Wavelet Transform . . . . .</b>           | <b>67</b> |
| 5.1      | Introduction . . . . .                                  | 67        |
| 5.2      | Preliminaries . . . . .                                 | 69        |
| 5.2.1    | Parameterized Construction of DWT . . . . .             | 70        |
| 5.2.2    | Subband Re-orientation . . . . .                        | 74        |
| 5.3      | Security . . . . .                                      | 76        |
| 5.4      | Hardware Implementation . . . . .                       | 79        |
| 5.4.1    | Reconfigurable Constant Multiplier (RCM) . . . . .      | 80        |
| 5.4.2    | Implementation Results . . . . .                        | 84        |
| 5.5      | Parameterized Lifting . . . . .                         | 84        |
| 5.6      | Conclusion and Future Work . . . . .                    | 87        |
|          | References . . . . .                                    | 87        |
| <b>6</b> | <b>Chaotic Filter Banks . . . . .</b>                   | <b>91</b> |
| 6.1      | Introduction . . . . .                                  | 91        |
| 6.1.1    | Chaos and Cryptography . . . . .                        | 91        |
| 6.1.2    | Wavelets and Chaotic Filter Banks . . . . .             | 92        |
| 6.1.3    | Scope and Organization . . . . .                        | 93        |
| 6.1.4    | Reconfigurable Hardware Implementation of DWT . . . . . | 93        |
| 6.2      | Chaotic Filter Bank Scheme . . . . .                    | 94        |
| 6.2.1    | Chaotic Maps . . . . .                                  | 95        |
| 6.2.2    | Key Space . . . . .                                     | 95        |
| 6.3      | The MCFB Scheme . . . . .                               | 96        |

|          |   |            |
|----------|---|------------|
| 6.4      | Improved Chaotic Oscillator . . . . .   | 98         |
| 6.4.1    | The Modified Logistic Map (MLM) . . . . .                                       | 98         |
| 6.5      | Wavelet Parameterization . . . . .  | 100        |
| 6.6      | Resistance of Chaotic Generator Against Cryptanalysis . . . . .                 | 100        |
| 6.6.1    | Randomness Tests . . . . .  | 101        |
| 6.6.2    | Bifurcation Map . . . . .   | 103        |
| 6.6.3    | Lyapunov Exponent . . . . .   | 103        |
| 6.7      | Security Enhancement . . . . .  | 105        |
| 6.8      | Hardware Implementation . . . . .   | 106        |
| 6.8.1    | Hardware Optimizations for ICO . . . . .  | 108        |
| 6.9      | Conclusions . . . . .   | 109        |
|          | References . . . . .  | 109        |
| <b>7</b> | <b>Chaotic Arithmetic Coding . . . . .</b>                                      | <b>113</b> |
| 7.1      | Introduction . . . . .  | 113        |
| 7.1.1    | Weakness of SAC Coder . . . . .   | 114        |
| 7.2      | Arithmetic Coding with Piece-wise Linear Chaotic Maps . . . . .                 | 115        |
| 7.2.1    | Compression Efficiency . . . . .  | 117        |
| 7.2.2    | Binary Chaotic Arithmetic Coding (BCAC) . . . . .                               | 118        |
| 7.2.3    | Implementation Efficiency . . . . .   | 121        |
| 7.3      | Security . . . . .  | 121        |
| 7.3.1    | Application to Multimedia/Data Encryption . . . . .                             | 121        |
| 7.3.2    | Threat Model . . . . .  | 122        |
| 7.3.3    | Security Enhancements (SE) . . . . .  | 122        |
| 7.3.4    | Resistance to Known Attacks . . . . .   | 125        |
| 7.3.5    | Comparison with BAC+AES . . . . .   | 127        |
| 7.3.6    | Key and Plaintext Sensitivity . . . . .   | 127        |
| 7.3.7    | Selective Encryption Using BCAC . . . . .                                       | 129        |
| 7.4      | Compression . . . . .   | 129        |
| 7.5      | Hardware Implementation . . . . .   | 130        |
| 7.5.1    | Literature Review . . . . .   | 131        |
| 7.5.2    | Implementation Details . . . . .  | 132        |
| 7.5.3    | Binary Arithmetic Coder (BAC) Architecture . . . . .                            | 133        |
| 7.5.4    | Binary Chaotic Arithmetic Coder and Encryption (BCAC)<br>Architecture . . . . . | 133        |
| 7.5.5    | Cost of Encryption . . . . .  | 134        |
| 7.5.6    | $N$ -ary Chaotic Arithmetic Coder and Encryption (NCAC)<br>Coding . . . . .     | 134        |
| 7.5.7    | Multiple Symbol per Cycle Arithmetic Coding . . . . .                           | 136        |
| 7.6      | Related Work . . . . .  | 137        |
| 7.6.1    | Multiple Huffman Tables . . . . .   | 137        |
| 7.6.2    | Randomized Arithmetic Coding . . . . .  | 138        |
| 7.6.3    | Secure Arithmetic Coding . . . . .  | 139        |
| 7.7      | Conclusion . . . . .  | 140        |
|          | References . . . . .  | 140        |

|                     |     |
|---------------------|-----|
| <b>8 Conclusion</b> | 143 |
| <b>Index</b>        | 145 |



<http://www.springer.com/978-1-4471-4458-8>

Embedded Multimedia Security Systems  
Algorithms and Architectures

Pande, A.; Zambreno, J.

2013, XVIII, 146 p., Hardcover

ISBN: 978-1-4471-4458-8