Contents

1 Secret Sharing Schemes 1

1.1 Introduction ............................. 1
1.2 Principle of secret splitting ................. 6
1.3 History of Secret Sharing .................. 8
  1.3.1 Threshold Scheme .................... 10
  1.3.2 The Shamir Secret Sharing Scheme ..... 10
  1.3.3 System Design ....................... 12
  1.3.4 A method of solution ................. 13
1.4 Concluding remarks ....................... 17

2 Evolution of Secret Sharing Schemes 19

2.1 Introduction ............................. 19
2.2 Evolution of the schemes .................. 23
2.3 General Secret Sharing Schemes ............. 32
2.4 Applications ............................. 33
2.5 Ito-Saito-Nishizeki Scheme ................. 34
2.6 Benaloh-Leichter Scheme .................. 36
CONTENTS

2.7 Concluding remarks .......................... 41

3 Visual Cryptography .......................... 42
   3.1 Introduction .............................. 42
   3.2 Division of the pixel ..................... 45
   3.3 Superposition of pixels .................. 46
   3.4 Dealing of a B/W Image .................. 46
      3.4.1 Algorithm to share a pixel into two shares 46
      3.4.2 Shamir’s solutions for small $k$ and $n$ ... 49
   3.5 A general scheme for $(k,k)$ Visual cryptography ...................... 51
   3.6 Concluding remarks ...................... 56

4 Modified Visual Cryptography ................. 57
   4.1 Introduction .............................. 57
   4.2 A Modified scheme for $(k,k)$ Visual Cryptography ...................... 58
      4.2.1 Comparison of the schemes .......... 62
   4.3 A simple Modified scheme for $(k,k)$ ........ 62
   4.4 Generalization of $(3,3)$ scheme .......... 64
   4.5 Concluding remarks ...................... 64

5 Balanced Strings and Uniform Codes .......... 65
   5.1 Introduction .............................. 65
   5.2 An Efficient $(2,n)$- threshold scheme ........ 69
   5.3 An upper bound of the Blowing factor ....... 73
5.4 Concluding remarks 77

6 Scheme for $(n - 1, n)$ threshold 78
  6.1 Introduction 78
  6.2 A new scheme 78
  6.3 sharing one bit 79
  6.4 Concluding remarks 84

7 An Efficient Scheme - Using Balanced Strings 85
  7.1 Introduction 85
  7.2 A $(2, 2)$ Construction 87
  7.3 A $(n, n)$ Construction 91
  7.4 Security Analysis 94
  7.5 Concluding remarks 95

8 Permutation Ordered Binary Number System 96
  8.1 Introduction 96
  8.2 A new number system 96
  8.3 POB-representation is unique 100
  8.4 POB-number and POB-value 103
  8.5 Illustrations 110
  8.6 Concluding remarks 111

9 Improvement Scheme Using POB Numbers 112
  9.1 Introduction 112
  9.2 A $(2, 2)$ Construction 113
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2.1</td>
<td>Algorithm to Share one byte between two shares</td>
<td>113</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Algorithm to Recover the shared byte</td>
<td>115</td>
</tr>
<tr>
<td>9.3</td>
<td>An ((n, n)) Construction</td>
<td>117</td>
</tr>
<tr>
<td>9.3.1</td>
<td>Algorithm to Share one byte between (n) shares</td>
<td>117</td>
</tr>
<tr>
<td>9.4</td>
<td>Security Analysis</td>
<td>121</td>
</tr>
<tr>
<td>9.5</td>
<td>Concluding remarks</td>
<td>122</td>
</tr>
<tr>
<td>10</td>
<td>Conclusions</td>
<td>123</td>
</tr>
<tr>
<td>Appendix 1:</td>
<td>The Distribution of keys</td>
<td>125</td>
</tr>
<tr>
<td>Appendix 2:</td>
<td>The Extended Euclidean Algorithm</td>
<td>134</td>
</tr>
<tr>
<td>Appendix 3:</td>
<td>List of Research Papers</td>
<td>137</td>
</tr>
<tr>
<td>Appendix 4:</td>
<td>Synopsis</td>
<td>138</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>150</td>
</tr>
</tbody>
</table>