

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Introduction	1
1.2	Access Structure	3
1.3	Fundamental $(k, n)$ -VCS	4
1.4	Equivalence of VCS Definitions	7
1.4.1	The Equivalence of Two Definitions of Threshold Basis Matrix VCS	8
1.4.2	The Equivalence of Two Definitions of General Access Structure Basis Matrix VCS	9
1.4.3	The Equivalence of Two Definitions of General Access Structure SIVCS	10
1.4.4	The Inequivalence of Two Definitions of Non-basis Matrix VCS	10
1.5	Step Construction of VCS	12
1.5.1	Definition of Step Construction and Step Construction of $(n, n)$ -VCS	12
1.5.2	Simplifying the Access Structure by Using Equivalent Participants	15
1.5.3	Step Construction of VCS for Access Structure $\Gamma_m = \{A_1, A_2, \dots, A_r\}$ such that $A_1 \cap A_2 \cap \dots \cap A_r = \{a_1, a_2, \dots, a_r\} \neq \emptyset$	16
1.5.4	Step Construction of VCS for General Access Structure	18
1.6	Exercises	20
	References	20
<b>2</b>	<b>Various Problems in Visual Cryptography</b>	<b>23</b>
2.1	Alignment Problems	23
2.1.1	Precise Alignment of VCS	24
2.1.2	Visual Alignment of VCS	27

2.2	Flipping Issues in VCS . . . . .	32
2.2.1	Share Generating . . . . .	35
2.2.2	Share Expansion . . . . .	36
2.3	Distortion Problems . . . . .	40
2.3.1	The Fountain Algorithm . . . . .	42
2.3.2	Improving VC Quality . . . . .	45
2.4	Thin Line Problems (TLP) . . . . .	47
2.5	Exercises . . . . .	50
	References . . . . .	51
<b>3</b>	<b>Cheating Prevention of Visual Cryptography . . . . .</b>	<b>53</b>
3.1	Definitions . . . . .	54
3.2	Attacks . . . . .	55
3.2.1	Attack on Horng's CIVCS . . . . .	55
3.2.2	Detectable Attacks . . . . .	57
3.2.3	Collaborating Cheaters . . . . .	57
3.2.4	Cheater Colluding . . . . .	58
3.2.5	New CIVCS . . . . .	60
3.3	2D Barcode Authentication for Basic VC Shares . . . . .	63
3.3.1	Barcode . . . . .	64
3.3.2	Barcode Embedding for Authentication of VC Shares . . . . .	65
3.3.3	VC Authentication Using 2D Barcodes . . . . .	66
3.3.4	Secret Revealing . . . . .	72
3.4	Braille for Authentication of Basic VC Shares . . . . .	76
3.4.1	Braille . . . . .	77
3.4.2	Braille Embedding in VC Shares . . . . .	77
3.5	Exercises . . . . .	81
	References . . . . .	81
<b>4</b>	<b>Various Visual Cryptography Schemes . . . . .</b>	<b>83</b>
4.1	Embedded Extended VCS . . . . .	83
4.1.1	Introduction . . . . .	83
4.1.2	Embedded EVCS . . . . .	85
4.1.3	Generating the Covering Shares for an Access Structure Using the Dithering Matrices . . . . .	86
4.1.4	Embedding the Shares of the Corresponding VCS into the Covering Shares . . . . .	91
4.1.5	Further Improvements on the Visual Quality of Shares . . . . .	93
4.2	Probabilistic Visual Cryptography Scheme (PVCS) . . . . .	95
4.3	Size-Invariant VCS (SIVCS) . . . . .	96
4.4	A ME-SIVCS that Satisfies ME-SIVCS-2 Security . . . . .	98
4.5	A ME-SIVCS that Satisfies ME-SIVCS-1 Security . . . . .	99

4.6	Threshold VCS (TVCS) . . . . .	101
4.6.1	Definitions of TVCS . . . . .	102
4.6.2	Basis Matrix . . . . .	103
4.7	Construction of $(k, n)$ -TVCS . . . . .	104
4.8	Concolorous TVCS . . . . .	107
4.8.1	The Model of Concolorous TVCS . . . . .	107
4.8.2	The Existence and Construction of Concolorous TVCS . . . . .	108
4.9	Construction of $(k, n)$ -TEVCS . . . . .	109
4.9.1	The Model . . . . .	109
4.9.2	Constructions of $(k, n)$ -TEVCS . . . . .	111
4.10	A Security-Enriched VCS . . . . .	112
4.10.1	PSSS . . . . .	113
4.10.2	ESSVCS . . . . .	114
4.11	Exercises . . . . .	127
	References . . . . .	127
<b>5</b>	<b>Various Color Schemes of Visual Cryptography</b> . . . . .	131
5.1	Introduction . . . . .	131
5.2	Basic Principles of Color Models . . . . .	134
5.3	Color VCS and Color EVCS in the Traditional Visual Cryptography Model . . . . .	136
5.4	Exercises . . . . .	146
	References . . . . .	146
<b>6</b>	<b>Various Applications of Visual Cryptography</b> . . . . .	149
6.1	Watermarking Applications . . . . .	149
6.1.1	Watermarking . . . . .	149
6.1.2	Visual Cryptography . . . . .	151
6.2	Resolution Variant Visual Cryptography . . . . .	159
6.2.1	License Plate Embedding . . . . .	160
6.2.2	Multiresolution VC Scheme . . . . .	161
6.3	Exercises . . . . .	163
	References . . . . .	163
	<b>Glossary</b> . . . . .	165
	<b>Index</b> . . . . .	167

Visual Cryptography for Image Processing and Security  
Theory, Methods, and Applications

Liu, F.; Yan, W.Q.

2015, XVI, 167 p., Hardcover

ISBN: 978-3-319-23472-4