Visual Cryptography for Image Processing and Security

Feng Liu · Wei Qi Yan

Visual Cryptography for Image Processing and Security

Theory, Methods, and Applications

Springer

Feng Liu
State Key Laboratory of Information Security, Institute of Information Engineering
Chinese Academy of Sciences
Beijing
China

Wei Qi Yan
Auckland University of Technology
Auckland
New Zealand

ISBN 978-3-319-09643-8 ISBN 978-3-319-09644-5 (eBook)
DOI 10.1007/978-3-319-09644-5

Library of Congress Control Number: 2014945954

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Visual cryptography is a secret sharing technique which allows encryption of a secret image among a number of participants. The beauty of the visual cryptography scheme (VCS) is that its decryption of the secret image requires neither knowledge of cryptography nor complex computation. Compared with traditional secret sharing schemes, it can encrypt a large amount of secret information, i.e., an entire image where the content can be versatile. VCS can be applied in secret sharing, information hiding, identification/authentication, copyright protection, etc. This book mainly focuses on fundamental concepts, theories, and practice of visual cryptography, designs, constructions, and analysis of visual cryptography schemes and the related applications.

A construction of general access structure VCS by applying (2, 2)-VCS recursively is presented in this book. Compared with many of the known VCSs, the presented VCS has smaller and average pixel expansion, and larger contrast in most cases. According to the construction, a general access structure VCS can be constructed by only applying (2, 2)-VCS recursively, regardless of whether the underlying operation is OR or XOR. This result is most interesting, because the construction of VCS under the operation XOR for general access structure has never been claimed to be possible before.

For designs and analysis of VCS, an embedded extended visual cryptography scheme (Embedded EVCS) is introduced where its shares are all meaningful images rather than noise. The embedded EVCS applies the embedded technique and halftone technique. Compared with some of the known EVCSs, the scheme has the following advantages: (1) It deals with gray level input images; (2) It has small pixel expansion; (3) It generates a general access structure EVCS and is always unconditionally secure; (4) Each participant only receives one share; (5) It is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares; and between the secret image pixel expansion and the visual quality of the shares.

Various VCS problems are discussed in this book. One of the typical problems is that of alignment. Evidence shows that the original secret image can be recovered visually when one of the transparencies is shifted by at most $m-1$ subpixels, and the average contrast becomes $\bar{\alpha} = \frac{(m-r)\cdot e}{m^2\cdot(m-1)}$. The study is based on a deterministic visual cryptography scheme, and the shifted scheme is a probabilistic visual cryptography scheme with less average contrast but still visible.

Correspondingly, the smallest pixel expansion and the largest contrast of (2, n)-VCS under the XOR operation are analyzed in this book, the values of the smallest pixel expansion, the largest possible contrast, the largest contrast, and the smallest possible pixel expansion, and the concrete constructions are provided as well. The chapter also shows that, construction of the basis matrix of contrast optimal (2, n)-VCS is equivalent to the construction of the maximum capacity binary codes with specific parameters, hence the known constructions of the maximum capacity binary code (constant weight or not constant weight) can be applied to construct contrast optimal (2, n)-VCS optionally. The book shows that (k, n)-VCS presented by Droste in 1996 is a (k, n)-VCS that works both under the OR and XOR operations. This advantage can bring more convenience to the participants. Furthermore, a method to reduce the pixel expansion of (k, n)-VCS is presented. The method can significantly reduce the pixel expansion compared with that of the (k, n)-VCS proposed by Tuyls. A construction of concolorous (k, n)-VCS where the shares are concolorous is introduced in this book. The book proves that the concolorous (k, n)-VCS does not exist with odd k, and proposes a construction of concolorous (k, n)-VCS with even k. The concolorous (k, n)-VCS can be used to protect the shares from being stolen by hidden cameras.

Cheating immune visual cryptography schemes (CIVCS) are presented in this book. The CIVCS in this book are constructed based on the known visual cryptography schemes (VCS), and have been applied to all VCSs for general access structure. Furthermore, the CIVCS detect the cheaters or only detect the existence of cheaters depending on the amount of the authentication information provided.

This book addresses the fundamental problems of visual cryptography from the aspects of theory and practice, which is beneficial for the community to get a better understanding of this media-based security technology. Hence, the book will potentially have a broad impact across a range of areas, including document authentication and cryptography. The book could be used as a reference for potential researchers and students for in-depth study of visual cryptography.

June 2014

Dr. Feng Liu
Dr. Wei Qi Yan

Acknowledgments

We thank the support from our families and we appreciate the work of our colleagues and students who were working with us together in the past few years.

Contents

1 Fundamental Theory of Visual Cryptography 1
1.1 Introduction 1
1.2 Access Structure 2
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 11
1.5.1 Definition of Step Construction and Step Construction of (n, n)-VCS 12
1.5.2 Simplifying the Access Structure Using Equivalent Participants 14
1.5.3 Step Construction of VCS for Access Structure $\Gamma_m = \{A_1, A_2, \cdots, A_r\}$ such that $A_1 \bigcap A_2 \bigcap \cdots \bigcap A_r = \{a_1, a_2, \cdots, a_r\} \neq \emptyset$ 15
1.5.4 Step Construction of VCS for General Access Structure 18
References 19

2 Various Problems in Visual Cryptography 23
2.1 Alignment Problems 23
2.1.1 Precise Alignment of VCS 24
2.1.2 Visual Alignment of VCS 28
2.2 VCS Cheating Prevention 32

2.2.1 Definitions 33
2.2.2 Attacks 34
2.3 Flipping Issues in VCS. 42
2.3.1 Share Generating. 45
2.3.2 Share Expansion 46
2.4 Distortion Problems 50
2.4.1 The Fountain Algorithm. 52
2.4.2 Improving VC Quality 54
2.5 Thin Line Problems (TLP) 56
References 59

3 Various Visual Cryptography Schemes 63
3.1 Embedded Extended VCS. 63
3.1.1 Introduction 63
3.1.2 Embedded EVCS 64
3.1.3 Generating the Covering Shares for an Access Structure Using the Dithering Matrices. 66
3.1.4 Embedding the Shares of the Corresponding VCS into the Covering Shares 71
3.1.5 Further Improvements on the Visual Quality of Shares 73
3.2 Probabilistic Visual Cryptography Scheme 75
3.3 Size Invariant VCS (SIVCS) 76
3.4 A ME-SIVCS that Satisfies ME-SIVCS-2 Security. 78
3.5 A ME-SIVCS that Satisfies ME-SIVCS-1 Security. 79
3.6 Threshold VCS (TVCS) 81
3.7 Construction of (k, n)-TVCS 83
3.8 Concolorous TVCS 86
3.8.1 The Model of Concolorous TVCS. 86
3.8.2 The Existence and Construction of Concolorous TVCS 87
3.9 Construction of (k, n)-TEVCS 89
3.9.1 The Model 89
3.9.2 Constructions of (k, n)-TEVCS 90
3.10 A Security Enriched VCS 91
3.10.1 PSSS 92
3.10.2 ESSVCS 93
References 106

4 Various Color Schemes of Visual Cryptography 109
4.1 Introduction 109
4.2 Basic Principles of Color Models. 111

4.3 Color VCS and Color EVCS Under the Traditional Visual Cryptography Model 114
References 123

5 Various Applications of Visual Cryptography 127
5.1 Watermarking Applications 127
5.1.1 Watermarking 127
5.1.2 Visual Cryptography 129
5.2 Resolution Variant Visual Cryptography 138
5.2.1 License Plate Embedding 139
5.2.2 Multi-resolution VC Scheme 140
References 142

Index 145

About the Authors

Dr. Feng Liu State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing China.

Dr. Liu received his Bachelor's degree in Computer Science from Shandong University and his Ph.D. in Information Security from Institute of Software (IOS), Chinese Academy of Sciences (CAS). He is currently an Associate Professor with the State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering (IIE), Chinese Academy of Sciences (CAS). Meanwhile, Dr. Liu is serving as the Director of the Executive Office of SKLOIS. His research interests include strategic and economic aspects of information security, visual cryptography, network security, formal analysis of security protocols, etc.

Dr. Wei Qi Yan School of Computer and Mathematical Sciences, Auckland University ofTechnology, Auckland New Zealand.

Dr. Yan received his Ph.D. in Computer Engineering from the Institute of Computing Technology, Chinese Academy of Sciences (CAS), he has worked with renowned universities in the USA, UK, and Singapore. Dr. Yan has contributed to over 120 publications, including four authored monographs and over 50 journal articles with more than 1,200 citations, he has contributed to eight granted research proposals. Dr. Yan has supervised over 100 PG/UG students including a post-doctoral fellow and Ph.D. research students. He is a Fellow of the Higher Education Academy (HEA), UK, the chair of ACM Multimedia New Zealand (NZ) chapter, and Editor-in-Chief (EiC) of the International Journal of Digital Crime and Forensics (IJDCF). Dr. Yan received a research award from SMF Singapore and the best paper award of the ChinaGraph'00 conference. Dr. Yan is a guest professor with Ph.D. supervision of the SKLOIS China.

Acronyms

m, m'	Pixel Expansion
$M_0 \parallel M_1$	Concatenation of Matrix M_0 and Matrix M_1
α	Contrast
$\emptyset$	Empty Set
$cl(C)$	The Closure of the Closed Set C
$max(\cdot)$	Function $max(\cdot)$
$min(\cdot)$	Function $min(\cdot)$
Γ_{Forb}	Set of the Forbidden Set
Γ_{Qual}	Set of the Qualified Set
M	The Maximum Qualified Set
m	The Minimum Qualified Set
$w(v)$	Hamming Weight of the Vector v
OR	OR Operation
XOR	Exclusive Operation
NOT	NOT Operation
$GF(2)$	Galois Field of Order 2
$R(A,P)$	The Dark Ratio of the Subset A in the Full Set P
$R(P)$	The Average Ratio of All the Subset of the Full Set P
$lcm(a,b)$	Least Common Multiple of a and b
$gcd(a,b)$	Greatest Common Divisor between a and b
2^V	Power Set of the Set V
ACM	Advanced Color Model
AP	Authorized Pixel
APE	Average Pixel Expansion
BIBD	Balance Incomplete Design
BSS	Binary Secret Sharing
CEVCS	Color Visual Cryptography Scheme
CIVCS	Cheating Immunity Visual Cryptography
CM	Color Model
CMY	Cyan, Magnet, Yellow
CVCS	Color Visual Cryptography Scheme
DVCS	Determinate Visual Cryptography Scheme
EVCS	Extended Visual Cryptography Scheme

HVS	Human Visual System
OTA	Online Trustable Authorization
PVCS	Probabilistic Visual Cryptography Scheme
RGB	Red, Green, Blue
SCM	Successful Cheating Method
VC	Visual Cryptography
VCM	Visual Cryptography Model
VCS	Visual Cryptography Scheme