Feng Liu · Wei Qi Yan

Visual Cryptography for Image Processing and Security

Theory, Methods, and Applications

Springer

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

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

Chapter 1
Fundamental Theory of Visual Cryptography

1.1 Introduction

Visual cryptography (VC), which was originally invented and pioneered by Moni Naor and Adi Shamir in Eurocrypt 1994 [11, 25], decodes concealed images without any cryptographic computations. It works as follows: a secret image is chosen and using VC techniques, it is encrypted into a number of pieces (known as shares). When these shares are printed onto transparencies and stacked together (physically superimposed), our human eyes do the decryption. This allows an average person to use the system without any knowledge of cryptography and without performing any computations whatsoever. This is the advantage of visual cryptography over other popular cryptographic schemes. The image consists of black and white pixels. The original secret image can be recovered by superimposing the two shares. The underlying operation of such scheme is OR. Figure 1.1 is the original secret image to be shared, Fig. 1.2 is the restored secret image with 2×2 expansion.

The secret image is composed of black and white pixels. The original secret image can be recovered by superimposing two share images together. The underlying operation of such a scheme is the logical operation OR. Generally, a (k, n)-VCS takes a secret image as input, and outputs n share images that satisfy two conditions: (1) any k out of n share images can recover the secret image; (2) any less than k share images cannot get any information about the secret image. There are four features of VCS:

- The VCS is for image encryption and decryption;
- Without complicate computation, the decryption is performed using our human vision system, the operation is fast, no information exchanges and communications between VCS shares;
- It is a secret sharing system;
- It is one pad system, satisfies unconditionally secure.

Therefore the VCS is simple, it does not need any decryption devices and computations, several transparencies are enough to get the secret. However, VCS

F. Liu and W.Q. Yan, *Visual Cryptography for Image Processing and Security*,
DOI 10.1007/978-3-319-09644-5_1

Fig. 1.1 Original secret image

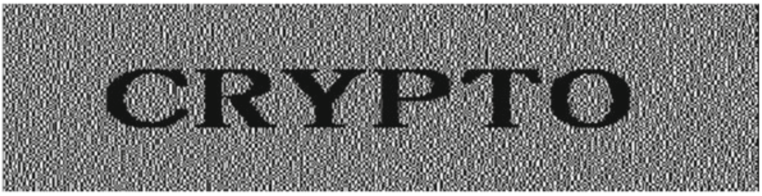

Fig. 1.2 Restored secret image

could deal with a huge volume of picture data compared to the text encryption, because the encrypted object is a picture and the information range is wide.

However, traditional cryptography needs computer participation, since the traditional encryption is based on the limitations of the current timeframe and computing resources. A computer has to be supported by software such as operating system and applications, and hardware such as CPU, memory, etc. This makes computers not a secure computing device, since virus, worms, malware, and backdoors could be used to steal secure information. But VCS can avoid this weakness and guarantee security computations such as encryption and decryption.

VCS can combine with the recent new technologies such as digital watermarking. A watermark is a very small piece of identification, which could be embedded and extracted in real time. VCS shares could be used as watermarks and identify copyright or ownerships in network, Internet, and cloud environment since the size is quite small.

The new recent research directions include optimization of contrast [2–6, 9, 12, 13, 20, 21, 27], pixel expansion [17, 19, 22, 31, 34], constructions of general VCS structure [16, 22, 30, 33, 36], VCS schemes for meaningful images [22, 37], applications of VCS [22], VCS immunity and cheating prevention [10, 14, 18, 22, 23, 26], etc. We organize our book in this order to address each chapter.

1.2 Access Structure

VCS is a secret sharing scheme for images. The scheme is built on access structure, hence we provide the definition of access structure first. In a secret sharing scheme, suppose all the participants of an access structure form a set $V = \{1, 2, \ldots, n\}$.

The specification of all qualified and forbidden subsets of participants constitutes an access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$. Denote it as the set of qualified sets (the participants in a qualified set can collaboratively recover the secret image) and Γ_{Forb} as the set of forbidden sets (the participants in a forbidden set cannot recover the secret image). Obviously, we have $\Gamma_{\text{Qual}} \bigcap \Gamma_{\text{Forb}} \neq \emptyset$. In visual cryptography, we only take the access structure $\Gamma_{\text{Qual}} \bigcup \Gamma_{\text{Forb}} = 2^V$ into consideration, where 2^V is the power set of V, i.e., the set of all the possible subsets of V. The set Γ_{Qual} is monotone because if a part of the participants in a set $B \in \Gamma_{\text{Qual}}$ can recover the secret image, then obviously all the participants in B can recover the secret image as well. We define $\Gamma_m = \{A \in \Gamma_{\text{Qual}} : \forall B \tilde{\subseteq} A \Rightarrow B \tilde{\in} \Gamma_{\text{Qual}}\}$ and $\Gamma_M = \{A \in \Gamma_{\text{Forb}} : \forall B \tilde{\supseteq} A \Rightarrow B \tilde{\in} \Gamma_{\text{Forb}}\}$.

We call Γ_m *the minimal qualified access structure*, and a subset $A \in \Gamma_m$ is called *the minimal qualified set*. We call Γ_M the maximal forbidden access structure, and a subset $B \in \Gamma_M$ is called the maximal forbidden set. For any $C \subseteq 2^V$, define $cl(C) = \{B \subseteq V : \exists A \in C, s.t. B \supseteq A\}$. We call $cl(C)$ the closure of C. Since Γ_{Qual} is monotone, then $cl(\Gamma_m) = \Gamma_{\text{Qual}}$. This means that the qualified access structure Γ_{Qual} and the minimal qualified access structure Γ_m are determined by each other. Similarly, Γ_M and Γ_{Forb} can be determined by each other as well. Furthermore, because $\Gamma_{\text{Forb}} = 2^V \backslash \Gamma_{\text{Qual}}$, we have that Γ_m and Γ_M can be determined by each other.

Particularly, we call a qualified set $B \in \Gamma_M$ that has the largest cardinality *the maximum qualified set* of Γ_m. Formally, the maximum qualified set B satisfies $|B| = \max\{|Q|, Q \in \Gamma_m\}$. Note that, the maximum qualified set of Γ_m may not be V, and there may be several maximum qualified sets in Γ_m.

It should be pointed out that, the threshold access structure is a special case of the general access structure [1], because a threshold (k, n) access structure is a general access structure with the constraints: $\Gamma_m = \{B \subseteq V : |B| = k\}$ and $\Gamma_M = \{B \subseteq V : |B| = k - 1\}$.

In VCS, there is a secret image which is encrypted into some share images. The secret image is called the original secret image for clarity, and the share images are the encrypted images (and are called the transparencies if they are printed out). When a qualified set of share images (transparencies) is stacked together properly, it gives a visual image which is almost the same as the original secret image; we call this the recovered secret image. In the case of black and white images, the original secret image is represented as a pattern of black and white pixels. Each of these pixels is divided into subpixels which themselves are encoded as black and white to produce the share images. The recovered secret image is also a pattern of black and white subpixels which should visually reveal the original secret image if a qualified set of share images is stacked. In this chapter, we focus on the black and white images, where a white pixel is denoted by the number 0 and a black pixel is denoted by the number 1. We notice that the definitions of VCS under OR and XOR operations are quite similar. We give some definitions of visual cryptography under the operation "·", which can either be the OR operation or the XOR operation.