Signals and Communication Technology

Bin Yan
Yong Xiang
Guang Hua

Improving Image Quality in Visual Cryptography

Springer

Signals and Communication Technology

Series Editors

Emre Celebi, Department of Computer Science, University of Central Arkansas, Conway, AR, USA
Jingdong Chen, Northwestern Polytechnical University, Xi'an, China
E. S. Gopi, Department of Electronics and Communication Engineering, National Institute of Technology, Tiruchirappalli, Tamil Nadu, India
Amy Neustein, Linguistic Technology Systems, Fort Lee, NJ, USA
H. Vincent Poor, Department of Electrical Engineering, Princeton University, Princeton, NJ, USA

This series is devoted to fundamentals and applications of modern methods of signal processing and cutting-edge communication technologies. The main topics are information and signal theory, acoustical signal processing, image processing and multimedia systems, mobile and wireless communications, and computer and communication networks. Volumes in the series address researchers in academia and industrial R&D departments. The series is application-oriented. The level of presentation of each individual volume, however, depends on the subject and can range from practical to scientific.

"Signals and Communication Technology" is indexed by Scopus.

More information about this series at http://www.springer.com/series/4748

Bin Yan · Yong Xiang ·
Guang Hua

Improving Image Quality in Visual Cryptography

Springer

Bin Yan
College of Electronics, Communication and Physics
Shandong University of Science and Technology
Qingdao, Shandong, China

Yong Xiang
School of Information Technology
Deakin University
Melbourne, VIC, Australia

Guang Hua
School of Electronic Information
Wuhan University
Wuhan, Hubei, China

ISSN 1860-4862 ISSN 1860-4870 (electronic)
Signals and Communication Technology
ISBN 978-981-13-8288-8 ISBN 978-981-13-8289-5 (eBook)
https://doi.org/10.1007/978-981-13-8289-5

© Springer Nature Singapore Pte Ltd. 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

To my beloved family.
—Bin Yan

To my beloved Shan, Angie, and Daniel.
—Yong Xiang

To my beloved ones.
—Guang Hua

Preface

Visual cryptography (VC) is a new form of secret sharing technique, where no computation is needed for decryption. The decryption can be done by stacking the shares or simple OR/XOR operations. This type of crypto-system is especially attractive for computation-limited environment, such as mobile devices or authentication without computation. It has found many applications including but not limited to privacy protection for biometric identification, bar code security, online evaluation and electronic voting, anti-counterfeiting and commodity tracing, etc. This book comprehensively covers the important efforts in improving the visual quality of images in visual cryptography, with a focus on the cases with grayscale images. We not only cover schemes in traditional VC and extended VC for binary secret image, but also cover topics for grayscale secret image and latest development in analysis-by-synthesis approach.

This book distinguishes itself from the existing literature in three ways. First, it not only reviews traditional VC for binary secret image, but also covers recent efforts in improving visual quality for grayscale secret image. Second, not only traditional quality measures are reviewed, but also measures that were not used for measuring perceptual quality of decrypted secret image, such as Radially Averaged Power Spectrum Density (RAPSD) and residual variance, are employed for evaluating and guiding the design of VC algorithms. Third, unlike most visual cryptography books following a mathematical formal style, this book tries to make a balance between engineering intuition and mathematical reasoning. All the targeted problems and corresponding solutions are fully motivated by practical applications and evaluated by experimental tests, while important security issues are presented as mathematical proof. Furthermore, important algorithms are summarized as pseudo-codes, thus enables the readers to reproduce the results in the book. Therefore, this book serves as a tutorial for readers with engineering background as well as for experts in related areas to understand the basics and research frontiers in visual cryptography.

An open source project was built on GitHub to accompany this book, which includes implementation of most algorithms covered in this book in MATLAB and related images and data. Please visit the following URL: https://github.com/yanbinhit/GrayscaleVisualCryptography.

The key features of this book include:

1. First book focusing on the topic of perceptual quality in VC.
2. First book comprehensively reviewing and discussing perceptual quality improvement of decrypted grayscale secret images.
3. First book employing perceptual quality measures, such as RAPSD for halftone image, to guide the design and evaluation of grayscale VC.
4. Good balance between engineering intuition and mathematical reasoning.
5. Suitable for both engineers targeting at fast implementation and researchers targeting at catching up the latest development in VC.
6. Matlab code for almost all major algorithms.

Qingdao, China — Bin Yan
Melbourne, Australia — Yong Xiang
Wuhan, China — Guang Hua
February 2019

Acknowledgements

This work was supported by the National Natural Science Foundation of China (NSFC) (No. 61272432) and the Shandong Provincial Natural Science Foundation (No. ZR2014JL044). Yong Xiang's work is partially supported the Australian Research Council under Grant LP170100458. Guang Hua's work is partially supported by Hubei Provincial Natural Science Foundation of China (No. 2018CFB225).

Contents

Acronyms and Abbreviations

ABP	Auxiliary Black Pixel
AbS	Analysis-by-Synthesis
AM	Amplitude Modulation
BER	Bit Error Rate
CIP	Cover Information Pixel
DBS	Direct Binary Search
DC	Direct Current
DDF	Directional Distribution Function
FRGVSS	Friendly Random Grid Visual Secret Sharing
HPSNR	Human Peak Signal-to-Noise Ratio
HVS	Human Vision System
IID	Independent and Identically Distributed
MSE	Mean Squared Error
MSSIM	Mean Structure Similarity
NTF	Noise Transfer Function
PDF	Probability Density Function
PSD	Power Spectral Density
PSF	Point Spread Function
PSNR	Peak Signal-to-Noise Ratio
QR	Quick Response
RAPSD	Radially Averaged Power Spectrum Density
RG	Random Grid
RNBED	Random Noise Balanced Error Diffusion
SIP	Secret Information Pixel
SNR	Signal-to-Noise Ratio
STF	Signal Transfer Function
VC	Visual Cryptography
VSS	Visual Secret Sharing

Notations

Matrices/Vectors

$\alpha, \beta, \ldots$	Coefficients or scalar parameters
$a, b, \ldots$	Scalars
A, B	General sets
$\mathbb{N}$	Set of nonnegative integer numbers, i.e., natural numbers $\{0, 1, 2, \ldots\}$
$\mathbb{Z}_n$	Set $\{0, 1, \ldots, n-1\}$
$\mathbb{C}$	Complex number
$\mathbb{R}$	Real number
i, j, k, l, m, n	General index to vector/matrix, limits of index
M, N, L, K	Dimension and length variables, $M, N \in \mathbb{Z}_+$
$\mathbf{a}, \mathbf{b}$	Boldface lowercase letters, vectors, e.g., $\mathbf{a} = (a_1, \ldots, a_N)^T$
$\mathbf{A}, \mathbf{B}$	Boldface uppercase letters, Matrices, digital images
$\mathbf{a}_k$	The k-th column of a matrix
$\mathbf{A}_{k,l}$	The (k, l)-th sub-matrix of matrix $\mathbf{A}$, the (k, l)-th block of image $\mathbf{A}$
$\{\cdot\}^T$	Transpose operator
$\{\cdot\}^*$	Complex conjugate operator
$\langle \cdot, \cdot \rangle$	Inner product operator
$\| \cdot \|_p$	ℓ_p-norm

Probability

$\Pr(\mathrm{A})$	Probability of event A that is a subset of sample space
$\mathcal{U}(\mathrm{A})$	Uniform distribution over the set A
$\mathcal{N}(\mu, \sigma^2)$	Gaussian distribution, mean μ and variance σ^2

Operators

Script letters $\mathcal{F}(\cdot)$, $\mathcal{G}(\cdot)$	General operators or functions
$\otimes$	Convolution operator
round$\{\cdot\}$	Rounding to the nearest integer
$\lfloor \cdot \rfloor$	Rounding to the nearest integer towards $-\infty$
$\mathbf{1}$	An all-one vector with an appropriate length
$\odot$	Stacking operation
$\triangleq$	Equal by definition

Signal Processing

$a[i]$	The i-th components of a signal vector $\mathbf{a}$ having finite or infinite length
$a\,[i,j]$	The (i,j) component of a two-dimensional signal or image $\mathbf{A}$
$a\,[\mathbf{n}]$	A sample at position $\mathbf{n}$, where $[\mathbf{n}] = [i,j]$

Boolean Operation

$a \vee b$	Boolean OR operation between two Boolean variables a and b
$\bar{a}$	Boolean NOT operation on a Boolean variable a