

Preface

Visual cryptography is a secret sharing technique which allows the encryption of a secret image among a number of participants. The beauty of visual cryptography scheme (VCS) is its decryption of the secret image requires neither cryptography knowledge nor complex computation. Compared to the traditional secret sharing schemes, it encrypts a large amount of secret information, i.e. an entire image where its content is versatile. The Visual Cryptography Scheme (VCS) has been applied to secret sharing, information hiding, identification/authentication, copyright protection, etc. The second edition of 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 a general access structure VCS by applying (2, 2)-VCS recursively is presented in this book at first. Compared to many of the known VCS, the presented VCS has smaller pixel expansion and average pixel expansion, and larger contrast in most cases. According to the constructions, a general access structure VCS is constructed by only applying (2, 2)-VCS recursively, regardless 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 the 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 to some of the known EVCS's, the scheme has the following advantages: (1) It deals with grey-scale 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; between the secret image pixel expansion and visual quality of the shares.

Various VCS problems will be discussed in this book. One of typical problems is alignment. Evidences shows that the original secret image is able to be recovered

visually when one of the transparencies is shifted by at most $m - 1$ sub-pixels, 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 largest contrast of $(2, n)$ -VCS under XOR operation are analyzed in this book. The values of the smallest pixel expansion, the largest possible contrast, the largest contrast, 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 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) is able to 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 OR and XOR operations. This advantage brings more convenience to the participants. Furthermore, a method to reduce the pixel expansion of (k, n) -VCS is presented. The method significantly reduces the pixel expansion compared to that of the (k, n) -VCS proposed by Tuyls. A construction of concolorous (k, n) -VCS where the shares are concolorous is also 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 is able to be used to protect the shares from being stolen by hidden cameras.

In this edition, we correct the typos and mistakes of the last edition as well as add new contents. We contribute 2D barcode for authentication of VC shares and Braille for authentication of VC shares to this new edition. We combine the content of VC authentication and VC cheating prevention together and put them into a new chapter. We also provide questions and exercises which are put at the rear of each chapter for those interested readers.

In general, 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 the potential researchers and students who have the intention to deeply study visual cryptography.

June 2015

Feng Liu
Wei Qi Yan

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