

Chapter 31

On the Pixel Expansion of Visual Cryptography Scheme

Teng Guo

University of International Relations, China

Jian Jiao

University of International Relations, China

Feng Liu

Chinese Academy of Sciences, China

Wen Wang

Chinese Academy of Sciences, China

ABSTRACT

In this paper, we first follow Ateniese et al.'s work that provides upper bounds of the pixel expansion of visual cryptography schemes (VCSs) for more kinds of graph access structures, in which we require that a subset of parties can determine the secret if they contain an edge of the graph G . The constructive upper bounds are derived by the graph decomposition technique. Then we generalize Ateniese et al.'s method of comparing the optimal pixel expansion of VCSs with two different access structures.

INTRODUCTION

Secret sharing schemes split a secret into several shares that are distributed to several parties (Blakley, 1979), so that certain qualified subsets of parties can determine the secret, while unqualified subsets of parties have no information about the secret (Shamir, 1979). Visual cryptography is a special type of secret sharing in which the secret can be decoded directly by the human visual system without needing any extra calculations (Naor & Shamir, 1995). The best way to understand visual cryptography scheme (VCS) is by an example. Basic VCSs have to deal with binary images that only contain white \square and black \blacksquare pixels. In a (2, 2)-VCS, every \square is encoded into $(\square\blacksquare, \square\blacksquare)$ or $(\blacksquare\square, \blacksquare\square)$ with equal prob-

DOI: 10.4018/978-1-7998-1763-5.ch031

ability, while every \blacksquare is encoded into $(\square\blacksquare, \blacksquare\square)$ or $(\blacksquare\square, \square\blacksquare)$ with equal probability. Observing a single share, we have $\blacksquare\square$ and $\square\blacksquare$ with equal probability, no matter whether the secret pixel is \square or \blacksquare . This guarantees that we obtain no information about the secret from a single share. The underlying pixel stacking rule is: $\square+\square=\square$, $\square+\blacksquare=\blacksquare$, $\blacksquare+\square=\blacksquare$, $\blacksquare+\blacksquare=\blacksquare$. Hence the decoded \square is $\square\blacksquare$ or $\blacksquare\square$, while the decoded \blacksquare is $\blacksquare\blacksquare$. This guarantees that we can perceive the secret by properly aligning the two share images.

In general, a secret pixel has to be encoded into multiple pixels on each share to achieve the above goals. This number is called the pixel expansion and is usually denoted by m . In the above $(2, 2)$ -VCS, the pixel expansion $m = 2$. Since the pixel expansion is directly related to the size of the shares, it is expected to be as small as possible and is extensively studied (Adhikari et al., 2004, Blundo et al., 2001, Blundo et al., 2006, Bose & Mukerjee, 2006, Bose & Mukerjee, 2010, Droste, 1996, Koga, 2002, Shyu & Chen, 2011, Verheul & Tilborg, 1997).

In a graph access structure, a subset of parties can determine the secret iff they contain an edge of the graph. In this paper, we first focus on the pixel expansion of graph access structure VCSs. Similar to the decomposition method in secret sharing, Ateniese et al. propose a method to build larger VCS from smaller schemes. Although the framework is easy to understand, but how to decompose (Blundo et al., 1995, Blundo et al., 1993, Stinson, 1994) and the properties of the decomposition are very tricky (Beimel et al., 2012). In addition to the star and bipartite graph access structures (Ateniese et al., 1996), VCSs based on trees, cycles and multi-partite graph access structures are studied. This paper is organized as follows. Some basic knowledge of VCS is given in Section II. The pixel expansion of some graph access structure VCSs is analyzed in Section III. The comparison of two access structures w.r.t. the optimal pixel expansion is discussed in Section IV. The paper is concluded in Section V.

PRELIMINARIES

This section contains two parts. The first part presents the basic concepts related to VCS. The second part reviews some previous results of graph access structure VCS.

Basic Definitions

We first give some knowledge of access structure. Denote all parties by $P = \{1, 2, \dots, n\}$. $\Gamma = (Q, F)$ is called an access structure if $Q \subseteq 2^P$ and $F \subseteq 2^P$ and $Q \cap F = \emptyset$. The elements of Q are called qualified sets and the elements of F are called forbidden sets. If for any element of Q , all of its supersets are also in Q , then Q is said to be monotone increasing. If for any element of F , all of its subsets are also in F , then F is said to be monotone decreasing. $\Gamma = (Q, F)$ is said to be a strong access structure if Q is monotone increasing and F is monotone decreasing and $Q \cup F = 2^P$. $Q_0 = \{A \in Q: A' \notin Q \text{ for all } A' \subsetneq A\}$ represents the set of all minimal qualified sets. Q_0 is also called the basis. $FM = \{A \in F: A' \in Q, \text{ for any } a \in P \setminus A, A' = A \cup \{a\}\}$ represents the set of all maximal forbidden sets.

Given a graph $G = (V(G), E(G))$, if each vertex is associated with a party in P , and the qualified sets on P are exactly the closure of the edge set of G , then we say G represents a graph access structure. A vertex cover of G is a subset of vertices $A \subseteq V(G)$ such that every edge has at least one endpoint in A . A graph $G' = (V(G'), E(G'))$ is called a subgraph of a given graph $G = (V(G), E(G))$ if $V(G') \subseteq V(G)$ and $E(G') \subseteq E(G)$. The complete graph K_n is a graph on n vertices such that any two vertices are joined

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/on-the-pixel-expansion-of-visual-cryptography-scheme/244936

Related Content

Quantum-Resistant Cryptography

Agung Mulyo Widodo, Princy Pappachan, Binastya Anggara Sekti, Nizirwan Anwar, Riya Widayanti, Mosiur Rahamanand Ritika Bansal (2024). *Innovations in Modern Cryptography* (pp. 100-130).

www.irma-international.org/chapter/quantum-resistant-cryptography/354037

Secure Data Transmission in the WSN Sector Utilizing a Heuristic Multi-Level Clustering Mechanism With Dynamic Trust Computation

Uma R., P. Ramkumar, J. Anitha Ruth, R. Valarmathianand C. Vinola (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security* (pp. 246-254).

www.irma-international.org/chapter/secure-data-transmission-in-the-wsn-sector-utilizing-a-heuristic-multi-level-clustering-mechanism-with-dynamic-trust-computation/348612

Next-Gen Cryptography: The Role of Machine Learning Applications in Privacy Preservation for Sensitive Data

G. Padmapriya, V. Vennila, K. Anitha, N. Manikandanand M. Suresh Anand (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security* (pp. 151-171).

www.irma-international.org/chapter/next-gen-cryptography/348607

Secure Text Extraction From Complex Degraded Images by Applying Steganography and Deep Learning

Binay Kumar Pandey, Deepak Mane, Vinay Kumar Kumar Nassa, Digvijay Pandey, Shawni Dutta, Randy Joy Magno Ventayen, Gaurav Agarwaland Rahul Rastogi (2021). *Multidisciplinary Approach to Modern Digital Steganography* (pp. 146-163).

www.irma-international.org/chapter/secure-text-extraction-from-complex-degraded-images-by-applying-steganography-and-deep-learning/280001

Exploiting the Homomorphic Property of Visual Cryptography

Xuehu Yan, Yuliang Lu, Lintao Liu, Song Wan, Wanmeng Dingand Hanlin Liu (2020). *Cryptography: Breakthroughs in Research and Practice* (pp. 416-427).

www.irma-international.org/chapter/exploiting-the-homomorphic-property-of-visual-cryptography/244929