International Journal of Digital Crime and Forensics
Volume 9 • Issue 2 • April-June 2017

On the Pixel Expansion of Visual Cryptography Scheme

Teng Guo, University of International Relations, School of Information Science and Technology, Beijing, China
Jian Jiao, University of International Relations, School of Information Science and Technology, Beijing, China
Feng Liu, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
Wen Wang, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 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.

KEYWORDS

Graph Access Structure, Pixel Expansion, Visual Cryptography

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 □ and black ■ pixels. In a (2, 2)-VCS, every □ is encoded into (□■, □■) or (■□, ■□) with equal probability, while every ■ is encoded into (□■, ■□) or (■□, □■) with equal probability. Observing a single share, we have ■□ and □■ with equal probability, no matter whether the secret pixel is □ or ■. This guarantees that we obtain no information about the secret from a single share. The underling pixel stacking rule is: □+□=□, □+■=■, ■+□=■, ■+■=■. Hence the decoded □ is □■ or ■□, while the decoded ■ is ■■. 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

DOI: 10.4018/IJDCF.2017040104

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 $P = \{1, 2, \cdots, n\}$. $\Gamma = (Q, F)$ is called an access structure if $Q \subseteq 2^P$ and $F \subseteq 2^P$ and $Q \cap F = \varnothing$. 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 $Q \cup F = 2^P$. $Q_0 = \{A \in Q: A' \notin Q$ for all $A' \subsetneqq A\}$ represents the set of all minimal qualified sets. Q_0 is also called the basis. $FM = \{A \in F: A' \in Q,$ 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 by an edge. A clique of a graph G is any complete subgraph of G. The complete multipartite graph $K_{a_1,a_2,\ldots,a_n}$ is a graph on a set of $\sum_{i=1}^{n} a_i$ vertices, which is partitioned into n subsets of sizes a_i $(1 \le i \le n)$ respectively, called partites, such that vertices w and v are joined by an edge iff they are from different partites. The complementary graph of a graph $G = (V(G), E(G))$ is denoted by $\bar{G}$. A graph $G = (V(G), E(G))$ is called a complementary graph of a given graph $G = (V(G), E(G))$ iff $V(G) = V(G)$ and $wv \in E(G)$ iff $wv = \in E(G)$. The complementary graph of a complete multipartite graph is a vertex-disjoint union of cliques. The complete graph K_n can be seen as a complete multipartite graph with n partites of size 1. A path in a graph $G = (V(G), E(G))$ is a sequence of vertices $v_1, v_2, \ldots, v_k$ such that each consecutive pair v_i, v_{i+1} is joined by an edge in G, which is often denoted by P_k, where k is the length of the path. A path is called simple if all its vertices are distinct. Without a special statement, all pathes P_n are simple in this paper. A cycle in a graph $G = (V(G), E(G))$ is a simple path $v_1, v_2, \ldots, v_k$ with v_1 and v_k joined by an edge in G, which is often denoted by C_k. A graph G is connected if for any two vertices $w, v \in V(G)$, there exists a path from w to v.

In the following, we set up our notations. Let S be a $n \times m$ Boolean matrix and X be a subset of $P = \{1, 2, \cdots, n\}$ and Z be a subset of $M = \{1, 2, \cdots, m\}$ and $|X|$ be the cardinality of X. $S[X][Z]$ represents the $|X| \times |Z|$ matrix S constrained to rows in X and columns in Z. $S[X]$ represents the $|X| \times m$ matrix S constrained to rows in X. Let C be a collection of $n \times m$ Boolean matrices. $C[X]$ represents the collection of $|X| \times m$ matrices, which are matrices in C constrained to rows in X. The OR result of rows of $S[X]$ is denoted by S_X and its Hamming weight is denoted by $w(S_X)$.

An SOA-Based Architecture to Share Medical Data with Privacy Preservation: An SOA-Based Architecture to Share Medical Data with Privacy Preservation

Mahmoud Barhamgi, Djamal Benslimane, Chirine Ghedira and Brahim Medjahed (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 310-324).*
www.igi-global.com/chapter/soa-based-architecture-share-medical/60956?camid=4v1a