International Journal of Digital Crime and Forensics
Volume 11 • Issue 1 • January-March 2019

General Construction for Extended Visual Cryptography Scheme Using QR Codes

Yuqiao Cheng, Science and Technology on Information Assurance Laboratory, Beijing, China
Zhengxin Fu, Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Bin Yu, Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Gang Shen, Zhengzhou Information Science and Technology Institute, Zhengzhou, China

ABSTRACT

This article describes how a visual cryptography scheme, with one prominent feature—decrypting simply, has attracted much research attention since it was first proposed. However, meaningless shares remain a continuing challenge in the development of VCS. In this article, an extended visual cryptography scheme (EVCS) based on XOR operation is proposed, in which QR codes are utilized as the cover images of shares. By designation, all the shares generated in the scheme can be decoded by standard QR code readers with specific meaning. In addition, to achieve high sharing efficiency, a method of simultaneously sharing a secret QR code among multiple subsets is presented. Also, sufficient and necessary conditions of the method are analyzed with an integer programming model, providing a general construction approach for EVCS under arbitrary access structures.

KEYWORDS

Error Correction Capacity, Extended Visual Cryptography Scheme (EVCS), General Access Structure, Multiple Subset Sharing (MSS), QR Codes

1. INTRODUCTION

As an important branch of secret sharing, the concept of visual cryptography scheme (VCS) was first proposed by Naor and Shamir (1995). According to the original definition of a (k, n)-VCS, a secret image is distributed into n shares. No secret information will be revealed with possession of fewer than k shares. But when k or more shares are superimposed, the secret can be easily decrypted by human vision. In the past few decades, VCS developed rapidly and has made great progress in many aspects (Liu & Yan, 2014). A scheme for general access structures was given therewith (Ateniese, Blundo, Santis, & Stinson, 1996), getting rid of threshold constraints on the qualified subsets. Optimal pixel expansion (Shyu & Chen, 2015) and contrast (Lin, Chen, & Lin, 2010) were explored later. To further improve the performance of recovery, XOR operation was introduced into the study of VCS (Shen, Liu, Fu, & Yu, 2017; Yang & Wang, 2014; Wu & Sun, 2014). For the sake of flexible sharing strategies, efforts have been made for multiple secrets (Jia, Wang, Nie, & Zhang, 2016), cheat

DOI: 10.4018/IJDCF.2019010101

prevention (Chen, Tsai, & Horng, 2013), region or fully incrementing (Hu, Shen, Fu, Yu, & Wang, 2016; Chen, 2017) and progressive schemes (Hou & Quan, 2012).

All studies mentioned above contribute a lot to the practical applications of VCS. The only downside is that the shares in these schemes are meaningless and easily arouse suspicion of some potential attackers when distributed via a public channel. Therefore, the extended VCS (EVCS) seems more attractive because it generates meaningful shares instead of random images (Naor & Shamir, 1995). By adding some extra columns into the basis matrices, Wang et al. (Wang, Yi, & Li, 2009) designed a (k, n)-EVCS with poor contrast of shares. To improve visual performance, a scheme was proposed on the basis of halftone image technology (Kang, Arce, & Lee, 2011). And other studies have also been attempted with better results (Liu & Wu, 2011; Yang, Sun, & Cai, 2016; Yan, Wang, Niu, & Yang, 2015; Ou, Sun, & Wu, 2015). Nevertheless, the camouflage effect of shares in these schemes was still unsatisfactory since there were many noisy points visible. Later, secret hiding techniques were utilized to generate meaningful shares (Yan, Wang, El-Latif, & Niu, 2015; Amiri & Moghaddam, 2016; Yuan, 2014), but with large computational load.

Quick Response (QR) code is a two-dimensional code developed by the Japanese Denso Wave Company, and now has been adopted as a universal specification performed by ISO (2006). With the popularization of intelligent terminals, QR codes have been widely used in fields such as information storage, mobile payment and electronic tickets. For a given QR code, we can hardly acquire its message by human vision since the dark and light modules are randomly distributed. This meaningless appearance is similar to the image characteristic of VCS shares. As such, QR code can be a good choice for the mask of VCS share. Therefore, investigations of the VCS and QR codes combinations have attracted considerable attention. At first, QR codes were embedded as some parts of shares to authenticate a VCS (Wang, Liu, & Yan, 2014). This method sought the best embedding region of a given share, thus reducing the influence of secret revealing. Later, a continuous-tone VCS (Yang, Liao, Wu, & Yamaguchi, 2016) was developed where the color of a secret module was determined by the grayness of black dots. Subsequently, a class of EVCSs based on QR codes was proposed. In view of machine recognition characteristic, an EVCS was presented for two-level information storage by Liu et al. (Liu, Fu, & Wang, 2016). In this scheme, a proper scanning distance and angle are strictly required to decoding the shares, which significantly increases the inconvenience of practical applications. By exploiting error correction mechanism of QR codes, a (n, n) sharing method was designed (Chow, Susilo, Yang, Phillips, Pranata, & Barmawi, 2016), and then, a (k, n) scheme under the theory of random grids were further implemented (Wan, Lu, Yan, Wang, & Chang, 2017). Sometimes, the secret image may be a QR code, and then Wan et al.'s scheme becomes invalid because the errors contained in the recovered secret are beyond error correction capability. One solution to this problem is that repeatedly performing Chow et al.'s method on each minimal qualified subset. Then, a large number of sharing instances are required.

In this paper, a novel EVCS is presented combining with QR codes. First, to reduce the number of sharing instances, we introduce an idea of MSS and provide its sufficient and necessary conditions with an integer programming model. And based on this model, we divide the initial access structure into several collections, each of which can achieve a MSS instance. Further, detailed sharing algorithm of MSS is presented. Experimental results and comparisons show the validity and advantages of the proposed scheme.

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries concerning our study. The proposed scheme is described in Section 3 while some conditions are theoretically proved in Section 4. Experiments and analysis are presented in Section 5 to illustrate the feasibility of this work and how it improves on previous work.