A Novel Visual Secret Sharing Scheme Based on QR Codes

Song Wan, Hefei Electronic Engineering Institute, Hefei, China
Yuliang Lu, Hefei Electronic Engineering Institute, Hefei, China
Xuehu Yan, Hefei Electronic Engineering Institute, Hefei, China
Lintao Liu, Hefei Electronic Engineering Institute, Hefei, China

ABSTRACT

In this paper, a novel visual secret sharing (VSS) scheme using QR codes is investigated. The proposed visual secret sharing scheme based on QR codes (VSSQR) can visually reveal secret image by stacking sufficient (shadow images) shares as well as scan the QR code by a QR code reader. Our VSSQR exploits the error correction mechanism in the QR code structure, to embed the bits corresponding to shares generated by VSS from a secret bit into the same locations of QR codes in the processing of encoding QR. Each output share is a valid QR code, which may reduce the likelihood of attracting the attention of potential attackers. The secret image can be recovered by stacking sufficient QR code shares based on the human visual system without any computation. In addition, it can assist alignment for VSS recovery. The experiment results show the effectiveness of our scheme.

KEYWORDS

Error Correction, QR Code, Visual Cryptography Application, Visual Secret Sharing

INTRODUCTION

A secret sharing scheme is a method of encoding a secret image into a number of shares where each share reveals no information about the secret image. Only qualified shares can reconstruct the secret message (Beimel, 2011). Visual cryptography (VC), also called Visual Secret Share (VSS), is a kind of secret sharing scheme (Naor & Shamir, 1994; Wang et al., 2007; m Wang, Arce & Crescenzo, 2009; Weir & Yan, 2010; Yang, 2004) where the secret image can be recovered by stacking the qualified number of shares based on the human visual system without any computation. Similarly, as secret sharing, VSS (Feng et al., 2008; Wang et al., 2009; Yang et al., 2014) can overcome the problem of storing a secret in a single information-carrier which would be damaged and lost easily by splitting and encoding a secret into a number of shares. However, as each share in VSS looks like a random pattern of pixels, it will raise suspicion and increase the likelihood of attracting the attention of potential attackers. Furthermore, the alignment is also an important issue for VSS recovery.

QR code (Jtc1/Sc, 2006) is a popularly used two-dimensional barcode recently with the advantages of larger QR content and error correction capability. Also, the appearance of QR code is similar to the share of VSS. Based on the above advantages, the technology of combining QR code and VSS
can be applied in many scenes, such as transferring secret information via public channels (Cimato & Yang, 2012; Tkachenko et al., 2016).

Recently, many researchers have proposed some schemes combining the technologies of QR code and VSS. Jonathan and Yan (2011) presented a scheme that uses a QR code to authenticate the shares. It attempts to embed the verification information inside the recovered secret in the form of a QR code. In their scheme, the QR code can be used as the secret transport mechanism which a long string of alphanumeric characters can be embedded inside the barcode. Wang et. al (2016) proposed a scheme by embedding QR codes into given shares to prevent cheating. They search the best region of a given share where the QR code could be embedded into so as to keep the visual quality of the revealed secret and the embedding will not affect the visual cryptography secret revealing too much. However, the shares are random in the schemes above, which may attract suspicion of encryption, due to embed QR codes into VSS shares.

Chow et. al (2016) proposed a secret sharing scheme for \((n, n) \ (n \geq 3)\) threshold based on XOR operation by distributing and encoding the information of a QR code containing a secret message into a set of QR codes. Each QR code share is a valid QR code that can be recognized by a QR code reader. The secret message can be recovered by first XORing the light and dark modules contained in the encoding region of all the \(n\) QR code shares and adding the function patterns. Nevertheless, the scheme needs a computational device with XOR ability and a QR code reader for secret recovery as well as is only for cases that \(n\) is larger than 3.

In this article, we propose a novel scheme which deeply integrates the error correction mechanism of QR code with the theory of VSS. The proposed scheme embeds the bits corresponding to shares generated by VSS from a secret bit into the same locations of QR codes in the processing of encoding QR. Each share is a valid QR code that can be scanned and decoded by a QR code reader. The secret image can be recovered by stacking sufficient shares including case \(n\) equals to 2 based on the human visual system without any computation. As a result, when recovering the secret image, we do not need any computational devices and QR code readers as well as \(n\) can be equal to 2. Since each QR code can be recognized, it means that the shares may not be suspected if distributed via public channels and will reduce the likelihood of attracting the attention of potential attackers.

The remainder of the paper is organized as follows. The introduction to the QR codes and Visual Cryptography are presented in Section 2. The secret data embedding algorithm is described in Section 3. Section 4 demonstrates the simulation results and analyses. Finally, Section 5 concludes this paper.

**BACKGROUND**

**QR Codes**

QR code (Samretwit & Wakahara, 2011; Smith, 2016) which was invented by the Denso Wave Incorporated in 1994 is defined as a two-dimensional barcode. The standard (Jtc1/Sc, 2006) defines forty sizes of QR code symbol versions which range from version 1 to version 40. A QR code is divided into modules and each QR code symbol version is comprised of a different number of modules. Each version has four modules more than the previous one. For example, Version 1 is made up of 21x21 modules while version 2 is made up of 25x25 modules. The QR code structure consists of function patterns and encoding regions. The encoding region consists of error correction and data codewords, version information and format information while function patterns consist of the alignment patterns, timing, separators patterns and finder patterns. The structure of a QR code version 7 is illustrated in Figure 1. Each QR code has three Finder Patterns which are located in the
Efficient Transparent JPEG2000 Encryption
www.igi-global.com/chapter/efficient-transparent-jpeg2000-encryption/27000?camid=4v1a