**INTRODUCTION**:

COMPARED with one-dimensional codes, twodimensional codes, such as Quick Response (QR) codes, allow more-widespread applications because they offer greater data storage. The QR code was originally designed by the Japanese Denso-Wave Company and has since been adopted as a universal standard specification [1] published by ISO. In daily life, QR codes are used in a variety of scenarios that include information storage, web links, traceability, identification and authentication. Moreover, the online-tooffline mode of QR codes represents a promising new trend because QR codes provide a contactless information transmission channel. According to [1], a QR code is robust to segmental loss or symbol damage. Any user can access the information in QR codes; therefore, they are unsuitable for storing secret data. During the past few years, many efforts have been Manuscript received November 6, 2017; revised February 3, 2018; accepted March 3, 2018. Date of publication March 23, 2018; date of current version May 1, 2018. This work was supported in part by the National Natural Science Foundation of China under Grant 61602513 and in part by the Outstanding Youth Foundation of Zhengzhou Information Science and Technology Institute under Grant 2016611303. made to place and protect secret messages in QR codes. Some scholars have utilized traditional steganography [2]–[5] or watermarking techniques [6]–[8]. These studies embed a QR code as a secret into a mask image; or treat it as a mask to hide information. Secret extraction in both techniques requires a transformation to one specified domain, such as DCT or DWT. Regarding secret sharing methods, a polynomial algorithm was presented in [9], where shadows were conveyed in the form of QR codes. In this scheme, the QR code was used as an information carrier to transfer shadow information and its message is meaningless. The authors of [10] presented a scheme that can resist print-and-scan operations and detect cheaters. Additionally, a novel QR code was designed for two-level message sharing and document authentication [11], in which a hash function is performed when decrypting the secret. Compared with Boolean operations, the computational overhead of all the aforementioned schemes is slightly larger. As a secret image sharing category, the concept of a visual secret sharing scheme [12] (also called a visual cryptography scheme, i.e., VCS) was first proposed by Naor and Shamir. In a (k, n)-VCS, a secret image is distributed into n shares. Any k shares can obtain the secret by human vision when they are superimposed. However, possession of fewer than k shares meant no information about the secret image could be revealed. Later, [13] introduced a special type of VCS, termed the XOR-based VCS (XVCS), in which the recovery process was based on an XOR Boolean operation. With advances in computing devices, this method of recovering information is feasible and reasonable [14], [15]. Irrespective of the specific operation, the most important advantage of a VCS is low computational complexity [16], which has attracted considerable research attention and resulted in further studies [17]–[21], including investigations of the VCS and QR code combinations. Weir and Yan [22] used a QR code to implement share authentication by embedding a QR code as a part of the share. To reduce the influence of secret revelation, a method was proposed in [23] that sought the best embedding region for a given share. In addition, [24] developed a continuous-tone VCS intended for authenticating certain applications on smartphones. Apparently, the shares in these schemes were meaningless and likely to be suspected by potential attackers when distributed via a public channel. A (k, n)-VCS with QR shares was designed in [25], where the secret image was not a QR code and had to be decoded by human vision. However, in most cases, QR codes are used to pursue an intelligent and automatic user experience. After smartphones became popular, this type of scheme [26] became the preferred approach, because its reconstructed secret can be read directly by a machine. However, the access structure discussed in [26] was limited to (n, n). Additionally, its security was influenced when the cover messages were similar. In this paper, an innovative scheme is proposed to improve the security of QR codes using the XVCS theory. First, an improved (n, n) sharing method is designed to avoid the security weakness of [26]. On this basis, we consider the method for (k, n) access structures by utilizing the (k, k) sharing instance on every k-participant subset, respectively. This approach will require a large number of instances as n increases. Therefore, we further present two division algorithms to classify all the k-participant subsets into several collections, in which instances of multiple subsets can be replaced by only one. Experimental results and comparisons show the validity and advantages of the proposed scheme.