IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Progressive Visual Secret Sharing Scheme for QR Code Message

Komal S. Patil[1*], Suhas B. Bhagate[2]

[1,2]Department of Computer Science, D. K. T. E. Society's Textile and Engineering Institute, Ichalkaranji, India

DOI: https://doi.org/10.26438/ijcse/v7i6.882887 | Available online at: www.ijcseonline.org

Accepted: 14/Jun/2019, Published: 30/Jun/2019

Abstract—The quick response (QR) code was designed for storage information and high speed reading applications. With the wide application of QR code, the security problem of QR code is serious, such as information leakage and data tampering. The QR code contains secret message. In order to solve the QR information security problem, this paper proposed progressive visual secret sharing schemes for QR code message. In progressive visual secret sharing scheme the QR code message is divided into several parts called shares, which separately reveals no knowledge about the QR code message. QR code message can be revealed progressively by more and more shares one another. It improves the security of the data transmission and also improves the clarity of a secret image step by step.

Keywords—Visual secret sharing scheme, QR code, Progressive visual cryptography scheme.

I. INTRODUCTION

Visual cryptography is one of the secret sharing techniques. It was originally invented by Moni and Adi Shamir in 1994 [1]. Visual cryptography deals with hiding the information in images, in such a way that it can be decrypted by human vision. The secret image is encrypted into n number of shares, and the secret image can be reconstructed from any k or more shares are stacked together ($k \leq n$).

Quick Response (QR) code is generally used for data storage and high-speed machine reading. QR code is two dimensional (2D) barcode developed by Denso-wave Company in 1994 [2]. The main use of QR code is to store a large amount of data on a small size. In day-to-day life, QR code is used in the variety of scenarios, including information storage, web links, phone number, traceability, identification, and authentication. The 1D barcodes can store a maximum of 20 alpha numeric digits, while the QR codes store around 7089 numeric characters and around 4296 alpha numeric characters. Information stored in the QR code can be accessed by anyone, so it needs to provide security using cryptography or other protection technique.

QR code conveys information through the arrangement of dark modules and light modules. Module refers to the black and white dots that make up QR code. The QR code consists of two main parts, the encrypting region, and the function patterns. Function pattern is the shape that must be placed in the specific area of the QR code to ensure that the QR code scanner correctly recognizes and orients the code for decoding. There are four different types of function patterns i.e. finder pattern, separator, timing patterns and alignment patterns. The encrypting region consists of data that represents version information, format information, data and error correction code words. There are 40 versions (1-40) and 4 error correction levels (L, M, Q, and H) of QR code are defined. Each QR code version has a data capacity, depends on the amount of data, character type, and error correction level. Data is encoded as a bit stream, which is divided into a sequence of codewords. The length of each codewords is 8 bit. The codewords are divided into a number of error correction blocks, based on QR code version and error correction level. The QR code employs error correction mechanism that allows correct decoding of the message even if some part of the symbol is dirty or damaged.

Visual secret sharing mechanism is used to secure the QR code message, so that the data privacy during data transmission can be enhanced. The secret data is divided into number of shares by the secret sharing mechanism and secret data can be recovered when the minimum two or more number of shares is stacked together.

II. RELATED WORK

G.D Moni Naor and Adi Shamir proposed visual cryptography scheme [1]. The main purpose of the visual cryptography scheme is to encrypt a secret image into some shares. Secret information cannot be revealed with few shares. All shares are necessary to combine to reveal the secret image. In (2, 2) Visual Cryptography Scheme, original

image is divided into 2 shares. Both the shares are required to be superimposed to reveal the secret image. Anyone, having only one share will not be able to reveal any secret information. In (k,n) scheme, if any k recipients stack their transparencies together, then a secret message is revealed visually. On the other hand, if only k −1 recipients stack their transparencies, they are not able to obtain any information about the secret message. The main drawback of (k,n) visual cryptography scheme approach is, it require at least k shares to recover the secret message.

Young cheng, Hou and Zen-YuQuan proposed progressive visual cryptography with unexpanded shares [3]. The basic (k,n) threshold visual cryptography scheme is to share a secret image with n participants. The secret image can be recovered while stacking k or more shares obtained; but we will get nothing if there are less than k pieces of shares being overlapped. On the contrary, progressive VC can be utilized to recover the secret message gradually by superimposing more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively. The progressive VC can improve the clarity of a secret image step by step by stacking more and more shares. The pixel unexpanded progressive VC solves the main problem such as leak of secret information, pixel expansion, and bad quality of recovered images.

Wen-Yuan Chen et al, proposed image processing and QR code techniques that can be used to construct nested steganography scheme [4]. Steganography technique hide the secret data into the cover image, so any other people cannot discover the secret data. There are two types of data (text and image) is serve as secret data. In the embedding process, the working flow divided into three parts. The upper part can be text data encoding process that converts text into 2D barcode pattern and then embeds into the cover image. Middle part can be face image embedding process. Lower part creates the cover image for secret data embedding. At starting text data taken as input and generate the QR code, then regular area moving (RAM) can be used for moving redundancy. The chaotic mechanism provides hashing of secret data to enhance the security. On cover image, a DCT is used to convert an image from the spatial domain to frequency domain for robustness. The IDCT returns cover image to the spatial domain from the frequency domain, then secret data embedding is complete. In decoding secret data, the extraction algorithm is used that extracts the text and image. The problem of this approach is it requires some other operations such as chaotic inversion or calculation of correlation coefficients which are computationally expensive.

Li Li, Rui-Ling Wang, Chin-Chen Chang proposed digital watermarking algorithm for QR code [5]. Digital watermarking is very interesting topic in current research related to the security field. This technology combines 2D Barcode with a digital watermark. Digital watermarking is an information security and protection technology. The basic idea is to embed the watermark signal in the secret image and detect the watermark signal by certain technology. Watermark signal contains an electronic signature, date, audio, text or digital works. This hidden information can also be extracted from printed or scanned images. The digital watermark method is used for QR Code. The watermark technology is used to embed the invisible watermark into the QR code image. After embedding the watermark, the DCT IF coefficients are compared. To prevent the overflow of the QR Code in the DCT domain of the image, QR image need fuzzy processing and be added noise to. In order to resist image distortion after print and scan operations, the watermark is repeatedly embedded. The watermark is extracted by using the two maximum membership degree of the fuzzy pattern recognition without the original image.

J. C. Chuang, Y. C. Hu, H. J. Ko a proposed method that shares confidential secret data [6]. Secret data is divided into n number of shadows by using the secret sharing technique. The shadows that are generated are embedded in each QR code tag. The secret data can be recovered only when any t out of n shadows ($t \leq n$) are stacked one another. In the decoding process to recover secret data, Lagrange polynomial interpolation technique can be used. A secret sharing mechanism is used to improve the security and data privacy of the QR code and also provides high security during data transmission but it requires high computational complexity for decryption.

Yang-Wai Chow, Willy Susilo, et al, proposed QR code for secret sharing approach exploits the error correction mechanism inherent in the QR code [8]. One of the problems of storing the secret in a single information carrier, which can be easily damaged or lost. The secret sharing mechanism distributes and encodes information about the secret in a number of shares. Each share is constructed from QR code and each share itself a valid QR code. The secret message can be recovered by combining the information contained in the QR code shares. Individually, the shares reveal no information about the secret. The (n,n) secret sharing scheme used to as QR code secret sharing (QRCSS), which exploits the error correction redundancy in the QR code structure. The QR code containing a secret message, it distributes and encodes into n number of shares and secret message is recovered only all n shares are stacked together. The main advantages of this paper are to reducing the attracting the attention of potential attackers and while recovering the secret image, users do not need any computing devices. The secret image is revealed without any loss in visual quality also it requires low computational complexity for decryption.

This approach has low security and it has limited to (n,n) scheme.

Song Wan, Yuliang Lu, Xuehu Yan and Lintao Liu proposed visual secret sharing scheme with (k, n) threshold based on QR codes [11]. In this paper, a novel visual secret sharing (VSS) scheme with using QR codes is investigated. The proposed visual secret sharing scheme based on QR codes(VSSQR) can visually reveal secret image by stacking k or more shares (shadow images)from all the n QR codes 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 that can be scanned and decoded utilizing a QR code reader. The secret image can be recovered by stacking for case (k, n) based on the human visual system without any computation.

Yuqiao Cheng, Zhengxin Fu, Bin Yu proposed an improved visual secret sharing method for QR code [12]. It encodes secret QR code into multiple shares. Each share is valid QR code. The secret message can be recovered by stacking QR code Shares in one another. Secret sharing overcomes the problem of storing a secret in a single information carrier, which can be easily lost or damaged. The security weakness can be solved by extending the access structure from (n,n) to (k,n). In (k,n) secret sharing scheme, the secret message has to be divided into n shares, where n>1 shares should be created and k shares are required to reconstruct the secret QR code message, where $k \leq n$. Even k-1 shares cannot recover the secret message. It provides high security and more flexible access structure. The computational cost is much smaller than other approaches.

III. METHODOLOGY

Figure 1 shows the system architecture of proposed system. It takes secret text message as input and generates the QR code of secret text message using QR code generator. The generated QR code is divided into different shares. The share generation algorithm is used for share generation. The generated shares can be watermarked using a watermarking algorithm. i.e Each share is superimposed with a cover image to generate a meaningful share. Each share is a valid QR code, and it distributes to different participants. The share receiver receives the shares from each participant. Secret text message in the QR code reveal progressively by stacking at least 2 or more and more shares. If there are only a few pieces of shares (more than the 2 shares) then the outline of the secret image can be obtained; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively.

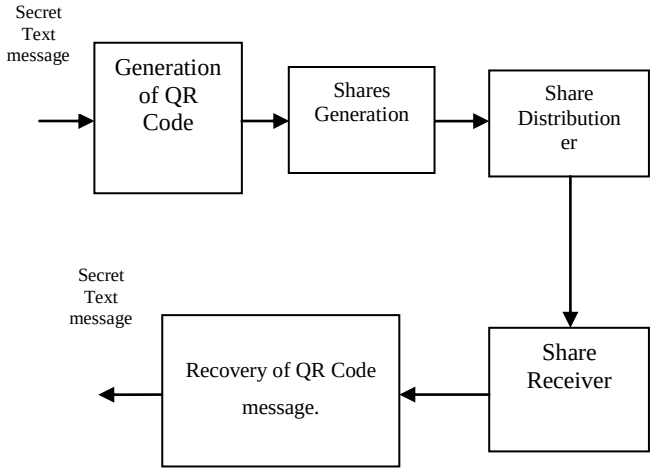

Figure 1: System Architecture

Consists of five modules:

1. Generation of Quick Response (QR) code.
2. Shares generation.
3. Share Distribution.
4. Share Receiver.
5. Recovery of QR code message.

Generation of Quick Response (QR) code:

QR code is a two dimensional barcode that used to secure the document. Data can be text, numeric, URL, email address, or alphanumeric etc. Data is encoded in QR Code as a bit stream, which can be divided into a sequence of codewords. Codewords 8 bit in length will be then divided into a number of error correction blocks based on QR code version and error correction level. It creates the QR code of given secret message by using spire.Barcode. The following steps describes the generation of QR code and save the QR code using spire.Barcode.

Step 1: Instantiate a BarcodeSettings object.
```
BarcodeSettings settings = new BarcodeSettings();
```
Step 2: Set barcode type as QR code.
```
settings.Type = BarCodeType.QRCode;
```
Step 3: Set data and display text for the code.
```
settings.Data = "Hello 123456789";
```
Step 4: Instantiate a BarCodeGenerator object.
```
BarCodeGenerator generator = new
BarCodeGenerator(settings);
```
Step 5: Generate the barcode image.
```
Image image = generator.GenerateImage();
```


Step 6: Save the barcode image.
image.Save("QRCode.png");

Shares generation:
Share generation module generates n shares of secret QR code. The share generation algorithm is used for share generation [3]. The following algorithm describes that design two $n \times n$ matrices denoted by C^0 and C^1 which represents the sharing matrix for white and black pixels of the secret image, respectively. The basis matrices of progressive visual secret sharing scheme are shown in fig2. In matrix C^0, the first row is assigned to 1, and other rows are all 1. On the contrary, matrix C^1 is a diagonal matrix, which means 1 is assigned to the diagonal line and the rest elements are all 0. The random numbers ranging from 1 to n can be needed to create shares. To share a white pixel of the input image, choose a random number l, and distribute the values of the l^{th} row vector of C^0 to every share, which means that first value of row vector $[C^0(l,1)]$ is distributed to share$_1$, and the second value $[C^0(l,2)]$ is distributed to share$_2$, and so on. In the same way, C^1 is applied to share a black pixel with the same sharing steps as sharing white pixel.

Two $n \times n$ secret sharing matrices:

$$C^0 = \begin{bmatrix} 1 & 1 & \dots & \dots & 1 \\ 0 & 0 & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 0 \end{bmatrix}_{n \times n}$$

$$C^1 = \begin{bmatrix} 1 & 0 & \dots & \dots & 1 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \dots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \end{bmatrix}_{n \times n}$$

Figure2. Basis matrices of progressive visual secret sharing scheme.

Algorithm: Share generation algorithm:
Input: A $W \times H$ halftone secret image P
where $p(i,j) \in P$
Output: n shares $S^m, m = 1,2, \dots, n$.
1) Generate sharing matrices C^0 and C^1.
2) For each pixel
$p(i,j),\ 1 \le i \le W,\ 1 \le j \le H.$
Randomly choose a value of l, range from $1\ to\ n$.
3) For $m = 1,2, \dots, n.$
if the pixel $p(i,j) = 0$ (White), the pixel value $S^m(i,j) = C^0(l,m)$
if the pixel $p(i,j) = 1$ (Black), the pixel value $S^m(i,j) = C^1(l,m)$

The generated shares can be watermarked using a watermarking algorithm [7]. i.e Each share is superimposed with a cover image to generate a meaningful share. It takes cover image of same size as that of secret image for watermarking the secret image. Each secret image shares is watermarked with a cover image and all are transmitted.

Algorithm: Watermarking embedding algorithm:
Input: n secret image shares, cover image.
Output: n watermarked shares.
1) Do for each secret image share
2) Read respective cover image share
3) Do for each pixel
If share pixel is black
Set LSB of cover image pixel to 1
If share pixel is white
Set LSB of cover image pixel to 0

Share Distribution:
Share Distribution module takes input as shares of QR code, each share is valid QR code. The shares are distributed to a group of n participants $T1, T2, \dots Tn$, each participant can gets a piece of secret information. Individually, the participants reveal no information about the secret. The secret can be reconstructed step by step when 2 or more number of shares is stacked together.

Share Receiver:
At the time of recovery process, the share receiver module receives the available QR code shares from each participant and it sends to recovery module for recovering the original secret QR code message.

Recovery of QR code message:
In the Recovery phase, it receives the meaningful shares from share receiver module and extracts the original shares. In Extraction of shares process, for each of the watermarked shares, extract the height and width values of secret image from the watermarked share. In each watermarked share pixel if LSB of pixel is 0, set secret share pixel as 0; else as 1.likewise we get the entire secret

QR code shares. The extracted shares can stack one another and perform XOR operations to get the original secret QR code message [10]. Secret QR code message recover gradually, by superimposing more and more shares. If there are only a few pieces of shares then the outline of the secret image can be obtained; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively.

Algorithm: Decryption algorithm:
Input: n watermarked shares.
Output: secret QR code message.
1) for each of the watermarked shares, extract the secret QR code shares.
2) Perform logical XOR operation by stacking received shares one on another.
3) The secret QR code message can be recovered.

IV. RESULT AND DISCUSSION

A. Exprimental Result

Module 1: Generation of QR code
The secret text message is the input of this module and generate the QR code of the given secret text message. The open source library, spire.Barcode is used to generate the QR code. The spire.Barcode framework provides different syntax for select error correction level, type, etc. There are four versions of QR code. The smallest is version 1-L (version 1: Error correction level L) and the largest is version 40-H (version 40. Error correction level H). Error correction level allows correct decoding of the QR code message even if some part of the symbol is dirty or damaged. This module generate QR code according to given input text message, size of QR code, error correction level and margin value.

Module 2: Shares Generation
The generated QR code is the input of this module and generates the shares of the QR code of the given QR code. Share generation algorithm is used to generate the shares. First generate the sharing matrices C^0 and C^1. C^0 matrices for white pixel and C^1 matrices for black pixel. For each pixel $p(i,j),\ 1 \le i \le W,\ 1 \le j \le H.$ randomly choose a value of l, range from $1\ to\ n$. The shares are generated using white and black pixels; the white pixel is representing by 0 and the black pixel representing by 1. if the pixel $p(i,j) = 0$ (White), the pixel value $S^m(i,j) = C^0(l,m)$ and if the pixel $p(i,j) = 1$ (Black), the pixel value $S^m(i,j) = C^1(l,m)$.

Module 3: Shares Distribution
This module distributes the generated shares among the participants. Each participant can get a piece of secret information. Individually, the participants reveal no information about the secret.

Module 4: Shares Receiver
This module receives the available QR code shares from each participant and it sends to recovery module.

Module 5: Recovery of QR code message
This module recovers the QR code message by stacking the two or more shares one another. Secret QR code message recover gradually, by superimposing more and more shares. If there are only a few pieces of shares then the outline of the secret image can be obtained; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively.

The evaluation of this approach, In Figure3, the generate QR code of message komalpatil. The figure4 generates the 4 shares of generated QR code. Figure5 generates the meaningful shares using watermarking algorithm. At the recovery process, remove the watermarking image from meaningful shares. The 2 or more shares can stack together to recover the QR code message progressively.

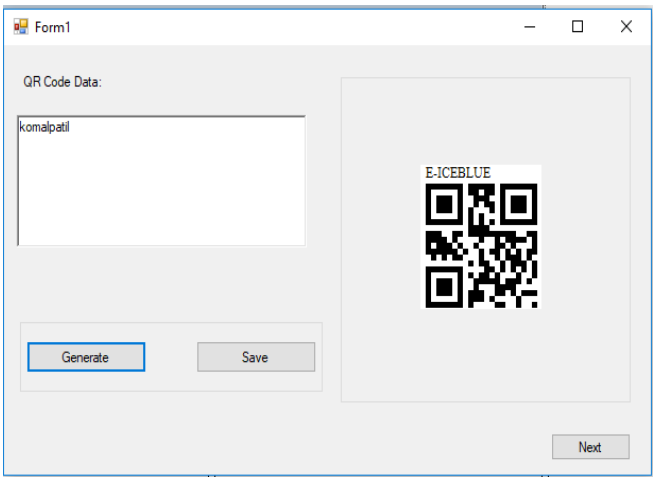

Figure 3. Generation of QR Code

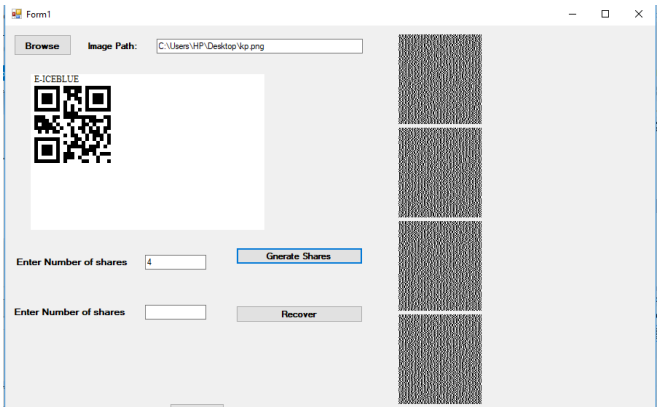

Figure 4: Shares Generation

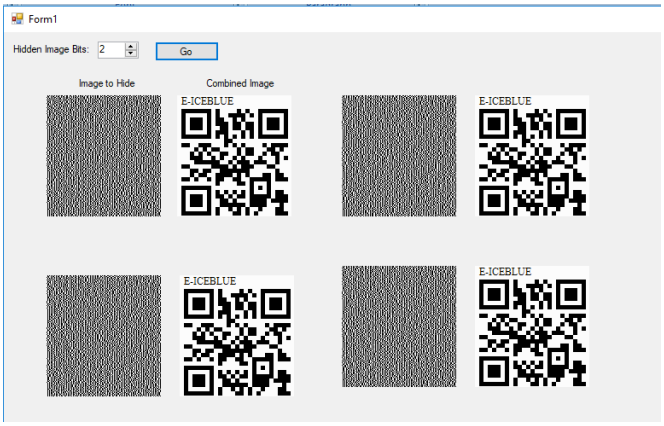

Figure 5: Generate Valid QR Code

B. Metrics:

- **Pixel Expansion:**

Generally, One pixel of original secret image is represented by more than one (like 2 or 4) pixels in each share image. This is called pixel expansion. Using pixel expansion, pixels in generated shares is greater than pixels in original image. Some limitations of pixel expansion are extra space for storage, extra bandwidth for sharing, and more processing time is required. In proposed system there will be no pixel expansion, which saves space and network bandwidth.

- **Two or more shares recover the secret message:**

In the proposed system, two or more shares can recover the secret message gradually without need of all k shares in (k,n) visual secret sharing scheme. There is a restriction in (k,n) visual cryptography scheme, minimum k shares are required to reveal secret information. So as compared to the (k,n) visual cryptography, progressive visual cryptography is lessen strict because in that minimum 2 or more shares can reveal secret information progressively. The progressive VC can improve the clarity of a secret image step by step by stacking more and more shares.

- **Complexity:**

In existing system, compressed secret image at destination side is decompressed to get the actual secret image. The compression and decompression of the secret image are performed using DCT/IDCT. DCT is used to convert an image from the spatial domain to frequency domain. The IDCT returns image in spatial domain from the frequency domain. Some other operations are also used for decompression, such as chaotic inversion or the calculation of correlation coefficients, which are computationally expensive. The proposed system requires only XOR operations for recovery of the secret message, which reduces the computational complexity of decryption.

V. CONCLUSION

In today's world security of data is very important. To protect the confidential data, we need some security techniques. Visual secret sharing schemes provides an effective and efficient way for providing security to QR code message. The proposed system use progressive visual secret sharing schemes for QR code message. The other (2,2) VCS, (2,n) VCS, (n,n) VCS, (k,n) VCS are used to provide security to the QR code. These techniques good to provide security to QR code message but have their own advantages and disadvantages. These schemes require more time and also for recovering the secret message all or at least k shares are needed. The proposed system is compared with the (k,n) VCS, it require at least k shares to recover the secret QR code message. The less than k shares will not recover the secret QR code message in (k,n) VCS. Therefore, Progressive visual secret sharing scheme is used to secure the secret QR code message. It improves the security of the data transmission and also improves the clarity of a secret image. The clarity of the message is increased, by increasing the number of the shares being stacked. The details of the secret QR code message are revealed progressively.

REFERENCES

[1] M. Naor and A. Shamir, "Visual Cryptography," in Proc. Advances in Cryptology: EUROCRYPT 94, vol. 1995, (950) pp. 1–12.

[2] International standard ISO/IEC 18004, "Information technology Automatic identification and data capture techniques Bar code symbology QR Code", Reference number- ISO/IEC 18004:2000(E), First edition 2000-06-15.

[3] Young cheng, Hou and Zen-YuQuan, "Progressive Visual Cryptography with Unexpanded Shares", IEEE Transactions on Circuits and Systems for Video Technology, 2011.

[4] W. Y. Chen, J. W. Wang, "Nested Image Steganography Scheme using QR-barcode Technique", Optical Engineering, vol. 51, no. 5, pp. 057004, 2009.

[5] L. Li, R. L. Wang, C. C. Chang, "*A Digital Watermark Algorithm for QR Code*", International Journal of Intelligent Information Processing vol. 2, no. 2, pp. 29-36, 2011.

[6] J. C. Chuang, Y. C. Hu, H. J. Ko, "A Novel Secret Sharing Technique using QR Code", International Journal of Image-Processing, vol. 4, no. 5, pp. 468-475, 2010.

[7] Jithi P V, Anitha T Nair, "Progressive Visual Cryptography with Watermarking for Meaningful Shares", International Multi-Conference on Automation, Computing, Communication, Control and Compressed Seneing (iMac4s), pp. 394-401, 2013.

[8] Y W. Chow, W Susilo, G Yang, "Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing", Information Security and Privacy, pp.409-425, 2016.

[9] Xiaohe Cao, Liuping Feng, Peng Cao and Jianhua Hu, "Secure QR Code Scheme Based on Visual Cryptography", International Conference on Artificial Intelligence and Industrial Engineering (AIIE), 2016.

[10] Pei-Ling Chiu, Kai-Hui Lee, "An XOR-based Progressive Visual Cryptography with Meaningful Shares", IEEE International Conference on Computer Communication and the Internet, 2016.

[11] Song Wan, Yuliang Lu, Xuehu Yan and Lintao Liu," Visual Secret Sharing Scheme With (k, n) Threshold Based on QR Codes", International Conference on Mobile Ad-Hoc and Sensor Networks,IEEE,2016.

[12] Yuqiao cheng, Zhengxin Fu, Bin Yu, "Improved Visual Secret Sharing Scheme for QR Code Application", IEEE Transactions on Information Forensics and Security,2018.

.

