

# An Approach for Securing QR code using Cryptography and Visual Cryptography

Cheshtaa Bhardwaj

Department of Computer Engineering  
and Applications  
GLA University  
Mathura, India  
cheshtaa.bhardwaj\_mt.cs20@gla.ac.in

Hitendra Garg

Department of Computer Engineering  
and Applications  
GLA University  
Mathura, India  
hitendra.garg@gla.ac.in

Shashi Shekhar

Department of Computer Engineering  
and Applications  
GLA University  
Mathura, India  
shashi.shekhar@gla.ac.in

**Abstract**—Quick Response code (QR code) is a 2-D matrix barcode which stores data in four different encoding modes (numeric, alphanumeric, kanji, binary). They are widely used nowadays and can be seen almost everywhere whether it is on cosmetics products, general stores, billboards and so on. It has become an important part of day to day activities. As an information sharing medium, it has become so user friendly and mobile-friendly that with just one scan through smart phones you get the information stored in it. The main intent of this work is to secure QR code from unauthorized access by allowing only those who have authorization to access it by using cryptography (by encrypting and decrypting the QR code using a key value). And further security was enhanced by applying ‘k’ out of ‘n’ visual cryptography scheme on the QR code. It creates ‘n’ no. of share of the QR code out of which ‘k’ no. of shares is required to restore it. This work will briefly explain how cryptography and visual cryptography were used to secure the QR code. The experimental results showed that there was no data loss during this process. Also, if at the time of decryption wrong key is entered then the QR code will not be generated. And also it is required to input minimum k number of generated shares of the QR code for the successful retrieval of QR code. Quality of the reconstructed QR code was also measured using PSNR and SSIM which showed that reconstructed QR code was of good quality as well as original QR code and reconstructed QR code were identical.

**Keywords**— Quick Response code (QR code), Cryptography, Visual Cryptography, Peak signal-to-noise ratio (PSNR), Structural Similarity Index (SSIM).

## I. INTRODUCTION

Quick Response code (QR code) is a 2-D matrix barcode invented by Masahiro Hara from “Denso Wave” the Japanese enterprise in 1994. It makes use of four input modes i.e. numeric, alphanumeric, byte/binary, Kanji/Kana to store data efficaciously. It is a square grid consisting of black squares on white background which can be scanned and read by 2-D digital imaging devices like smart phones and also by third party apps. Until the QR code is appropriately interpreted, it is processed by Reed- Solomon error correction. The QR codes stores information in both components of the image, which is horizontal and vertical. After processing, the required data is pull-out from those patterns. “ZXing” which is an open source project maintains a list of QR code data types [1]. QR code is firstly scanned and detected by 2-D digital imaging

devices and then the programmed processor digitally processes and analyzes it. The processor is programmed in such a manner that (using single or multiple smaller squares) it locates three individual squares at the corner of QR code image near the fourth corner to standardize the image for size, orientation and angle of viewing. The tiny black squares throughout QR code are then transformed into binary numbers and authenticated with an error- correcting algorithm.

TABLE I  
Storage Capacity of QR Code with Different Input Modes [1]

Input Mode	Maximum Character	Bits/Character
Numeric only	7089	$3\frac{1}{3}$
Alphanumeric	4296	$5\frac{1}{3}$
Binary/Byte	2953	8
Kanji/Kana	1817	13

There are **eight notable parts** of QR code architecture: Version Information (there are total 40 different versions of QR codes currently being used; these markers specify the version being used in it), Format Information (it consists of information like data mask pattern and error tolerance, thus make it easier to scan the QR code), Data and Error correction keys (it is the primary part of QR code structure where code stores the data and has blank space to store error correction module), Required Patterns, Position Marking (it is located at three corners of every QR code; allowing scanner to accurately recognize and scan the code by indicating the direction of code in which it is printed), Alignment Marking (it helps to straighten out the code drawn on curved surfaces), Timing Pattern (using this pattern scanner determines how large the data matrix is), Quiet Zone (it helps to distinguish the code from its surroundings) [2].

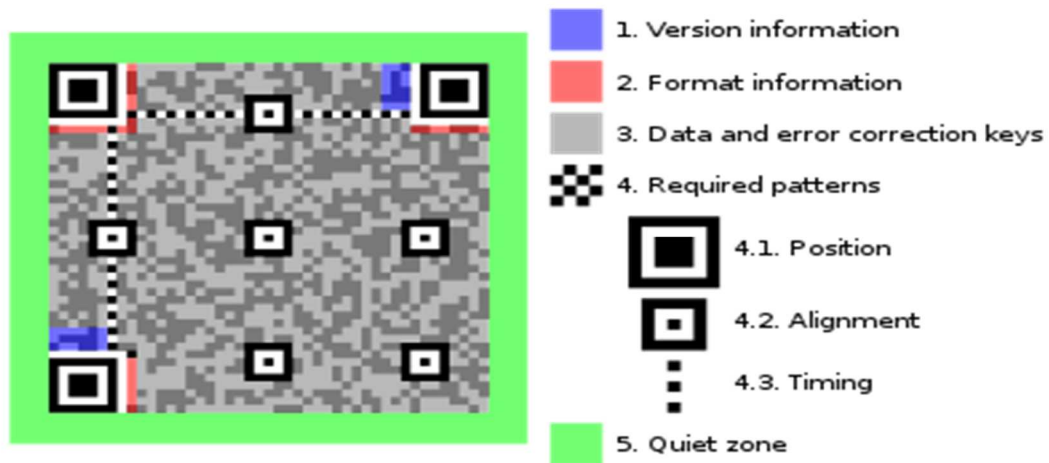


Fig. 1 QR Code Architecture [3]

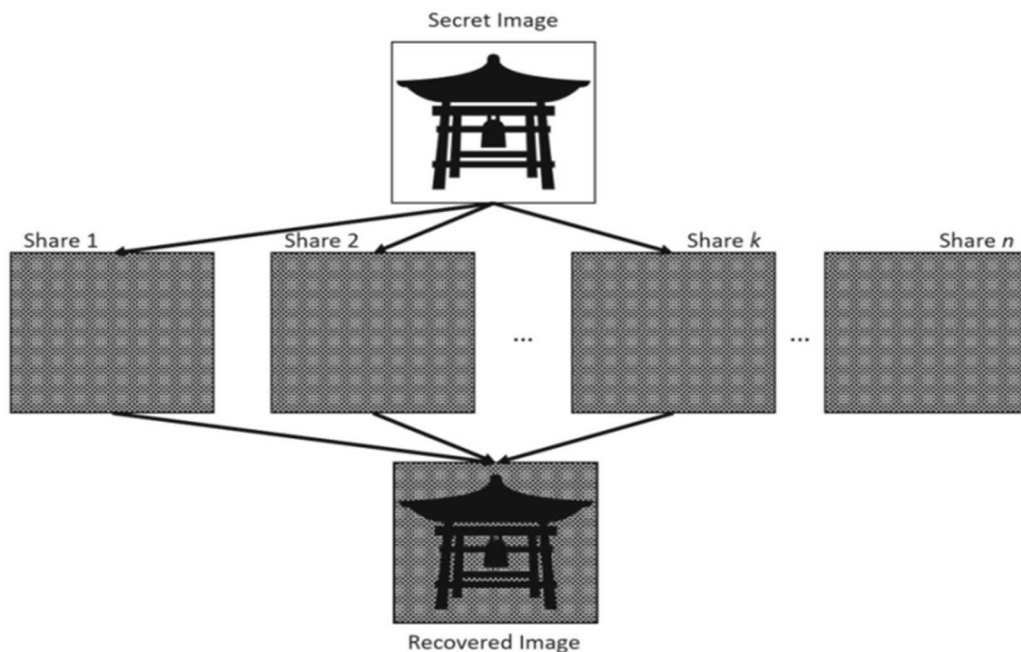


Fig. 2 Visual Cryptography [4]

Visual Cryptography is a method which makes use of sightseeing. It is a cryptographic technique which encrypts the data in such a manner that the decryption can be done just by sight-reading [5]. It uses characteristics of human vision to decrypt the encrypted data. In this cryptographic technique, an image or text is encrypted by making number of shares. These shares are the noisy images of the secret image. Image that is to be encrypted is known as secret image. When the printed shares are superimposed on each other, the image can be decrypted by sightseeing. It removes the requirement for advanced computation during the decryption process.

It can be particularized as a  $(k,n)$  secret sharing problem where  $n$  is the no. of noisy images or shares of the secret image and  $k$  is the minimum no. of shares which are required to be stacked to recover the secret image. Each share

represents subset of pixels from secret image which are the group of 'p' black and white sub-pixels. There are 2 collection of sub-pixel pattern for the representation of either white or black pixels in the shares. These two components/sets (say  $C_0$  and  $C_1$ ) are for white pixel and black pixel respectively. The kind of shares used in visual cryptographic technique can either be meaningful or meaningless shares. Meaningful shares are the visual image which is used to enclose information from secret image whereas meaningless share resembles the noise. Data security is the prime concern to maintain the confidentiality of the data [6].

To measure the quality of the reconstructed QR code two parameters were being used: Peak signal-to-noise ratio (PSNR) and Structural Similarity Index (SSIM). For a given

reference image (i) and reconstructed image (r), both having size of A×B, the PSNR between both the images is defined by formula shown in figure where MSE is mean square error [7].

$$PSNR(i, r) = 10 \log_{10} \left( 255^2 / MSE(i, r) \right) \quad (1)$$

Where,

$$MSE(i, r) = \frac{1}{AB} \sum_{p=1}^A \sum_{j=1}^B (i_{pj} - r_{pj})^2 \quad (2)$$

Mean square error low means high PSNR. And higher PSNR depicts higher image quality of the reconstructed image. The (SSIM) is another quality assessment metric that measures the similarity between the original and reconstructed image. Its value ranges from -1 to +1. SSIM value +1 depicts that both the images (original and reconstructed images) are identical. It is defined as:

$$SSIM(i, r) = l(i, r) c(i, r) s(i, r) \quad (3)$$

$$\text{where, } \begin{cases} l(i, r) = \frac{2\mu_f \mu_g + c_1}{\mu_f^2 + \mu_g^2 + c_1} \\ c(i, r) = \frac{2\sigma_f \sigma_g + c_2}{\sigma_f^2 + \sigma_g^2 + c_2} \\ s(i, r) = \frac{\sigma_{fg} + c_3}{\sigma_f \sigma_g + c_3} \end{cases}$$

## II. RELATED WORK

Xiaohe Cao et. al. [8] proposed a secured mechanism for QR code to maintain the data integrity. It was achieved using visual cryptography. Compared to other cryptographic techniques, visual cryptography is less complex as decryption of the text/image can be done using human visual system. Concealment, the simplicity of secret recovery and security are the few advantages of visual cryptography over traditional cryptographic methods. The proposed scheme makes two shares of the base image (QR code) using visual cryptography. These two share images are transmitted separately. To retrieve the base image (QR code), it is required to stack both the share images. Once both the share images are stacked over each other, the secret/base image can be visualized using human visual system. Here, the two share images are based in pseudo-random matrix, that is, the pixel value in the share image are identified with the help of the corresponding value of the pseudo-random matrix. Experimental result showed that they have constructed 2 out of 2 visual cryptographic scheme using MATLAB platform and the original image taken was 120×120 binary QR code. And after superimposing the two share images they were able to decrypt the original binary QR code. The only weakness of this proposed system was less number of share images of the original image. Less share image means less secured. Number of share image could be increased as to make it more secured. Zhengxin Fu et. al. [9] used a way which uses the number of noisy images out of which minimum number of noisy images is needed to be stacked to recover the image. Each share represents subset of pixels from secret image. The kind of shares used in visual cryptographic technique can either be meaningful or

meaningless shares. Meaningful shares are the visual image which is used to enclose information from secret image whereas meaningless share resembles the noise. In the proposed system, they have used meaningful share, along with probabilistic sharing model to increase the maximum allowable size of secret image. Here, the error correction capacities of the share were preserved. The experimental result showed that the recovered secret has more image features and looks best. Also, it was able to determine some of the QR codes from unauthorized sources. Here, limitation was that the size of the secret image is limited, even after using probabilistic method to implement no pixel expansion. Also, improvement of secret payload of QR code remains a problem to be resolved. R. G. Sharma et. al. [10] focuses on the various visual cryptographic techniques and analysed their performance on various aspects like pixel expansion, encryption method, type of share, number of secret image etc. Yen–Wu Tiet. al. [11] proposed visual cryptographic scheme based on QR code as an application in medication administration, so that no patient gets wrong medicines or less dosage then the prescribed one. Pan, J. S. et. al. [12] proposed a secret color image mechanism with color QR code using visual cryptography. They used (n,n) visual cryptographic scheme, where they generated (n-1) meaningful shares and a one meaningless share. These schemes were pixel non-expandable.

## III. PROPOSED METHODOLOGY

QR code encodes the information which can be assessed just by scanning it through smart phones. There are cases when information in QR code are confidential and there is the need for an authorized access of QR code only. The proposed method aims to maintain the security of QR code using: encryption, decryption and visual cryptography. The proposed approach works in three stages. The first stage is to generate the QR code after embedding the information in to it. The second stage is to encrypt the QR code by assigning a KEY value to it (key can be alphanumeric, alphabetic or simply numeric) and applying visual cryptography to the QR code. Here, we are using 'k' out of 'n' VC scheme (where 'k' is the minimal number of share required to generate the QR code and 'n' are total number of shares generated of the QR code). So, at this point we assigned the value of 'k' and 'n'. The shares of QR code generated are meaningless shares. Now, at the final decryption stage of the QR code will take place. First we are required to input the value of key and value of k. After this we will input minimum share required to generate the QR code. And if the value of key, k at this stage mismatch with the value inputted at the encryption stage then the QR code will not be generated. Also, the shares used should be 'k' out those 'n' generated shares only for the successful generation of the QR code. For all these stages we developed a user interface (UI) using MATLAB platform. Figure 5 and 6 shows the encryption and decryption process respectively.

The proposed approach has been tested on various QR code with different messages/information embedded in it.

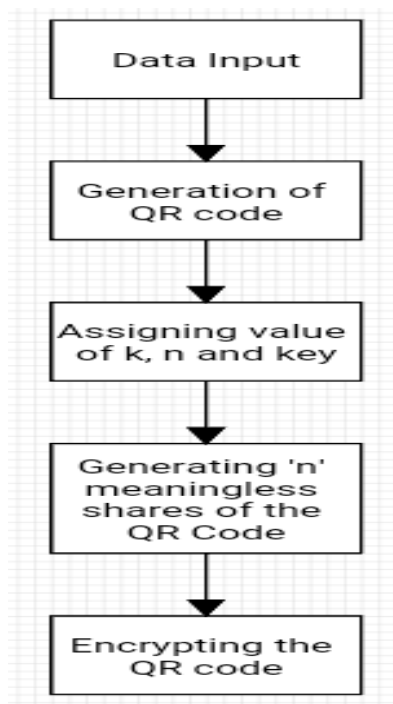


Fig. 3 Encryption process of QR code

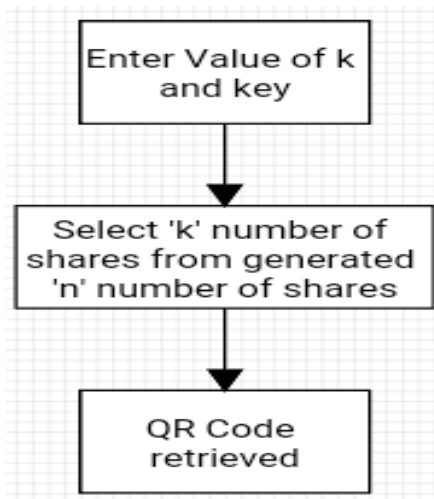












Fig. 4 Decryption process of QR code

#### IV. RESULTS AND DISCUSSIONS

In this research work we have applied security on QR code so that only authorized access can be done. We achieved this by making use of cryptography and visual cryptography. Firstly the message or information was embedded in the QR code and then it was encrypted using a key value and this key value was used to decrypt the QR code, if at that moment wrong key value was entered then no QR code was generated. Then we generated 'n' shares of the QR code out of which 'k' shares will be required to retrieve the QR code at decryption stage along with the key value. The results show that there was no data loss in QR code during this process. The outcome of the proposed approach tested on various QR code with different messages is shown in table 2. The PSNR is high which shows that the quality of the reconstructed QR code is good, that is, less error has been introduced during this process to the QR code. Another parameter used to measure the reconstructed QR code image quality is structural similarity index (SSIM). Its value ranges from -1 to +1 where 1 depicts good quality. And the results show that SSIM of reconstructed QR code is 1 which means reconstructed QR code and QR code are identical. So, the results showed that our approach to secure the QR code from unauthorized access to QR code was successful as without key value and shares of QR code, the QR code cannot be retrieved. Also, the quality of reconstructed QR code was good. This method shows that there was no data loss that is we were able to decrypt the same secret message that was encrypted in the QR code before generating the shares of QR code. Also, if wrong key was entered, QR code was not generated, making it more secure.

TABLE III  
Experimental Result on various QR code with different messages

S.No.	Message	QR code generated	No. of shares created (n)	Value of k	Key	Retrieved image	PSNR (in dB)	SSIM	Data Loss
1.	security check 544434 code #005		5	3	ALERT		Infinite	1	NO

2.	Name- Ansh assembly@ 002		6	5	0076		Infinite	1	NO
3.	Id- 44032 Airline- EmiAir Flight no.- 007		7	4	AD007		Infinite	1	NO
4.	Patient Id- 98546 Room no.- 404		9	6	j0034e		Infinite	1	NO
5.	Platinum Ferry Code*123		10	7	9954ak		Infinite	1	NO

## CONCLUSION

QR codes are widely used nowadays for sharing and covering data. Seeing its incredible rise, still have areas that need to be improved like stockpiling limit, security, fault tolerance and many more. This study works to secure QR code with the help of cryptography and visual cryptography. Cryptography was used to encrypt and decrypt the QR code whereas visual cryptography (k out n scheme) was used to create the shares of the QR code and when k out of these n shares were stacked, the QR code was retrieved. Firstly the message or information was embedded in the QR code and then it was encrypted using a key value and this key value was used to decrypt the QR code. Then we generated 'n' shares of the QR code out of which 'k' shares will be required to retrieve the QR code at decryption stage along with the key value. And as a result we were able to secure the QR code from unauthorized access. This work can be extended to colored QR codes (CQR) as they have larger storage capacity due to their hues and more information can be embedded in CQR which can be encrypted and send secretly for an authorized access.

## REFERENCES

- [1] Moisoiu, M., Negrău, A., Györödi, R., Györödi, C., & Pecherle, G. (2014). QR Code Scanning app for Mobile Devices. *International Journal of Computer Science and Mobile Computing*, 3(6), 334-341.
- [2] Raut, V. R., & Nage, M. A. (2019). Detection and Identification of Plant Leaf Diseases based on Python
- [3] Arora, M., & Verma, A. K. (2018, November). Increase capacity of QR code using compression technique. In *2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)* (pp. 1-5). IEEE.
- [4] Mohan Sai, S., Gopichand, G., Vikas Reddy, C., & Mona Teja, K. (2019). High Accurate Unhealthy Leaf Detection. *arXiv e-prints*, arXiv-1908.
- [5] SABRI, P. N. A. A. B., ABAS, A. B., & DIN, R. B. (2021). Enhancing Data Storage Of Colored QR Code Using C3M Technique. *European Journal of Molecular & Clinical Medicine*, 7(8), 3805-3813.
- [6] Ibrahim, D. R., Teh, J. S., & Abdullah, R. (2021). An overview of visual cryptography techniques. *Multimedia Tools and Applications*, 80(21), 31927-31952.
- [7] S. Kumar, M. S. Gaur, P. Sagar Sharma and D. Munjal, "A Novel Approach of Symmetric Key Cryptography," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 593-598, doi: 10.1109/ICIEM51511.2021.9445343
- [8] Gupta, L. M., Samad, A., & Garg, H. (2020). TBHM: a secure threshold-based encryption combined with homomorphic properties for communicating health records. *International Journal of Information Technology and Web Engineering (IJITWE)*, 15(3), 1-17.
- [9] Sara, U., Akter, M., & Uddin, M. S. (2019). Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. *Journal of Computer and Communications*, 7(3), 8-18.
- [10] Cao, X., Feng, L., Cao, P., & Hu, J. (2016, November). Secure QR code scheme based on visual cryptography. In *Sehiemy RE, Reaz MBI, and Lee CJ, 2016 2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE)*. Beijing, China (pp. 20-21).
- [11] Fu, Z., Cheng, Y., & Yu, B. (2018). Visual cryptography scheme with meaningful shares based on QR codes. *IEEE Access*, 6, 59567-5.
- [12] Sharma, R. G., Dimri, P., & Garg, H. (2018). Visual cryptographic techniques for secret image sharing: a review. *Information Security Journal: A Global Perspective*, 27(5-6), 241-259.
- [13] Ti, Y. W., Chen, S. K., & Wu, W. C. (2020). A New Visual Cryptography-Based QR Code System for Medication Administration. *Mobile Information Systems*, 2020.
- [14] Pan, J. S., Liu, T., Yang, H. M., Yan, B., Chu, S. C., & Zhu, T. (2022). Visual cryptography scheme for secret color images with color QR codes. *Journal of Visual Communication and Image Representation*, 82, 103405.