



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 1, January 2023

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 8.118

9940 572 462

6381 907 438

[ijirset@gmail.com](mailto:ijirset@gmail.com)

[www.ijirset.com](http://www.ijirset.com)

# Novel Approach for Secret Sharing Schema for QR Code Applications: A Review

Mr. Nawale Swapnil k.<sup>1</sup>, Prof. Sapike Nikita S.<sup>2</sup>

Research Scholar, Department of computer Engineering, Vishwabharti Academy's College of Engineering,  
Ahmednagar, India<sup>1</sup>

Associate Professor, Department of computer Engineering, Vishwabharti Academy's College of Engineering,  
Ahmednagar, India<sup>2</sup>

**ABSTRACT:** The most widely used barcode is the quick response code (QR), which has a higher data capacity and improved damage resistance. When scanning data forms, barcode scanners may quickly and simply extract information from the QR code. However, in actual QR apps, certain private information stored directly in QR codes is not safe. To encode a secret QR code into separate shares, a visual secret sharing system is provided. In contrast to other methods, the shares in the proposed scheme are legitimate QR codes that can be read by a current QR code reader using a special method, increasing the number of suspicious attackers. The eligible shares are XORed in order to recover the secret message as well. Using smartphones or other QR scanning devices, this operation can be completed with ease. Contribution work includes developing the best partitioning strategies and utilising hashing methods to compare the original message with the shared message.

**KEYWORDS:** Hashing, partitioning algorithm high security, Quick Response code, visual secret sharing scheme

## I. INTRODUCTION

The QR code has become popular in recent years. The use of QR codes in everyday life can be found in a wide range of applications, such as information storage, web linkages, traceability, identification, and authentication. First, the QR code makes it simple to identify computer hardware, like mobile phones and scanning devices. Second, QR codes are inexpensive, resilient against breakage, and have a lot of storage space.

The structure of the QR code is special and allows for fast decoding and geometrical rectification. For QR code identification and orientation correction, three position tags are utilised. Deformation arrangement is coded using one or more alignment patterns. Timing patterns determine how the module will come together. Error correction level and mask pattern are additionally included in the format information regions. The version information regions contain the code version and error correcting bits.

The popularity of QR codes is primarily due to the following features:

- QR code robust to the copying process,
- It is easy to read by any device and any user,
- It has high encoding capacity enhanced by error correction facilities,
- It is in small size and robust to geometrical distortion.

A recent innovation in secret sharing is visual cryptography. By relying on human visual decryption, it enhances the secret sharing images to restore the complexity of the secret. Its benefits over conventional encryption include concealment, security, and ease of secret recovery. The usage of visual cryptography meets the consumers' high security needs and shields them from a variety of security intrusions. Value creation in business applications is simple. The conventional multi-color QR code with textured patterns that hides data using text steganography and secures data using a visual secret sharing system is proposed in this study.

### Organization of paper

The organization of the paper is as follows section II gives the related work and limitations and last section concludes the paper with future work followed by references.

## II. RELATED WORK

The paper [1] proves that the contrast of XVCS is  $2^{(k-1)}$  times greater than OVCS. The monotone property of OR operation degrades the visual quality of reconstructed image for OR-based VCS (OVCS). Accordingly, XOR-based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast. Advantages are: Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages are: Proposed algorithm is more complicated.

This paper [2] propose sharing QR code secrets explodes the error correction mechanism inherent in the structure of the QR code, for distribute and encode information about a secret message into a number of actions. Each action in the scheme is constructed from a QR cover code, and each share itself is a valid QR code that can be scanned and decoded by a QR code reader. Advantages are: The secret message can be recovered the secret message can be recovered by combining the information contained in the QR code shares. Disadvantages is: secrete sharing depends on code words.

This paper [3] propose Naor and Shamir has numerous applications, including visual authentication and identification, steganography, and image encryption and introduce cryptanalyze the CPVSS scheme and show that it is not cheating immune. They also outlinean improvement that helps to overcome the problem. Advantage is introduce advance cheating-prevention visual secret-sharing. Disadvantages is prevention accuracy is low.

In [4] paper, present a blind, key based watermarking technique, which embeds a transformed binary form of the watermark data into the DWT domain of the cover image and uses a unique image code for the detection of image distortion. The QR code is embedded into the attack resistant HH component of 1stlevel DWT domain of the cover image and to detect malicious interference by an attacker. Advantages are: More information representation per bit change combined with error correction capabilities. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks. Disadvantages are: Limited to a LSB bit in the spatial domain of the image intensity values. Since the spatial domain is more susceptible to attacks this cannot be used.

Visual cryptography [5] i.e. multiple image visual cryptography (MIVC), optimal grayscale reserving visual cryptography (GRVCS) are studied. Embedded extended visual cryptography scheme (Embedded EVCS), simulated-annealing-based algorithm to use the VC construction problem to find the column vectors for the optimal VC construction, natural-image-based VSS scheme (NVSS scheme).

In [6] paper, design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. Advantages are: Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. Disadvantages are: Need to improve the security of the QR barcode. QR technique requires reducing the modifications.

The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication [7]. The public level is the same as the standard QR code storage level; therefore it is readable by any classical QR code application. The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using QR code with an error correction capacity. Advantages are: It increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the P&S process. Disadvantages are: Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.

To protect the sensitive data, [8] paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones. For a normal scanner, a browser can only reveal the formal information from the marked QR code. Advantages are: The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography. Only the authorized user with the private key can further reveal the concealed secret successfully. Disadvantages are: Need to increase the security.

In this work [9], HVC construction methods based on error diffusion are proposed. The secret image is concurrently embedded into binary valued shares while these shares are half toned by error diffusion—the workhorse standard of half toning algorithms. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images.

This paper [10] author implement an improved algorithm. To start with, the carrier image uses contourlet change to separate the low-frequency part of the image. And it is partitioned into blocks. In addition to the position patterns and



separator symbol image, the QR code as watermark information is scrambled transformation. At that point every one of the QR code data to measure the watermark is inserted into each block low-frequency image. Disadvantages are: This system basically worked on scrambling transformation and only focus on copy write protection.

In this paper [11], the schemes of user-friendly visual secret sharing dependent on random grids are compared to a proposed scheme. The outcomes show that the proposed schema other than not requiring the Codebook, is more adaptable in the quality control than some different schemas and proposed strategy is that separated from the utilization of complementary cover images, different cover images can be utilized and shares do not contain any follow from one another, which it expands the security and more confusion against attackers.

In this paper [12], as first part, many types of secret sharing schemes are examined and author proposed two Variant of a secret sharing scheme using Gray code and XOR operation. The Gray code is used to construct the shares and the XOR operation is used to reconstruct the secret. The proposed method can be used as a cryptographic algorithm and also for secret sharing as well as visual secret sharing. Disadvantages are: in this paper worked on cryptographic algorithm for data security. Security is less.

In this paper [13], author proposed visual secret sharing scheme using Boolean and shift operations that provides high security to the secret image is designed. An algorithm is proposed to encode the original secret image to generate  $n$  share images using simple Boolean XOR and circular shift operations. The secret data cannot be revealed with any  $k-1$  or less number of share images. The security is provided to the original secret by encrypting this secret with a random image and distinct authentication id used for each share during generation of shares. The size of generated share images is same as that of original image and requires no pixel expansion. Disadvantage is: This paper used construct two variant secret sharing schemes depend on gray scale images.

In this paper [14], author proposed visual secret sharing scheme share two color images on rectangular shares with no pixel expansion. The originality of secret is verified by watermark which is embedded into the secret image followed by the sharing process. The secret is reconstructed and watermarks are retrieved from the original secret to perform authenticity. Disadvantage is: In this paper worked on DWT and DCT techniques. Security is less in watermarking.

### III. CONCLUSION

In this paper, a visual secret sharing scheme for QR code applications, which makes improvement mainly on two aspects: higher security and partitioning techniques based on specific relationships. In addition, we extended the access structure from  $(n, n)$  to  $(k, n)$  by further investigating the error correction mechanism of QR codes. Two division approaches are provided, effectively improving the sharing efficiency of  $(k, n)$  method. Therefore, the computational cost of our work is much smaller than that of the previous studies which can also achieve  $(k, n)$  sharing method and compare shared message with original message using hashing techniques.

### REFERENCES

- [1] C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.
- [2] Y. W. Chow, W. Susilo, G. Yang, et al., "Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing," Information Security and Privacy, pp.409-425, 2016.
- [3] Y. C. Chen, G. Horng, D. S. Tsai, "Comment on cheating prevention in visual cryptography," IEEE Transactions on Image-Processing A Publication of the IEEE Signal Processing Society, vol. 21, no. 7, pp. 3319-3323, 2012.
- [4] P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code," AEU - International Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074-1084, 2015.
- [5] Miss A.A.Naphade Dr.R.N.khobaragade Dr.V.M.Thakare, "Improved nvss scheme for diverse image media". International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA, May 24-26, 2016.
- [6] P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.
- [7] I. Tkachenko, W. Puech, C. Destruel, et al., "Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.



- [8] P. Y. Lin, Y. H. Chen, "High payload secret hiding technology for QR codes," Eurasip Journal on Image & Video Processing, vol. 2017, no. 1, pp. 14, 2017.
- [9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009.
- [10] Weijun Zhang, XuettianMeng," An Improved Digital Watermarking TechnologyBased on QR Code" ICCSNT 2015.
- [11] S. Mohammad Paknahad, S. Abolfazl Hosseini, Mahdi R. Alagheband," User-friendly Visual Secret Sharing for color images Based on Random Grids" International Symposium on Communication Systems, Networks and Digital Signal Processing 2016.
- [12] Deepika M P, A Sreekumar," Secret sharing scheme using Gray code and XORoperation" IEEE 2017
- [13] Javvaji V.K. Ratnam,1 P. Ramana Reddy,2 and T. Sreenivasulu Reddy3," Design of High Secure Visual Secret Sharing Scheme for Gray Scale Images" IEEE WiSPNET 2017.
- [14] Modigari Narendra1, Dhanya Ben2 C.P. Jetlin3 , Dr. L. Jani Anbarasi" An Efficient Retrieval of Watermarked Multiple Color Images using Secret Sharing" ICSCN -2017



**INNO SPACE**  
SJIF Scientific Journal Impact Factor  
**Impact Factor: 8.118**



**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details