International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 11 | Nov 2019 www.irjet.net p-ISSN: 2395-0072

# A Survey on Private Messaging based on QR Code using Visual Secret Sharing Scheme

**Pranav Hadawale[1], Sumoli Vaje[2], Dipali Wale[3], Prof. Sachin Dighe[4]**

*[1,2,3]Student, Dept. of Computer Engg. Sahyadri Valley COE & Technology, Pune, Maharashtra, India*
*[4]Assistant Professor, Dept. of Computer Engg. Sahyadri Valley COE & Technology, Pune, Maharashtra, India*

---

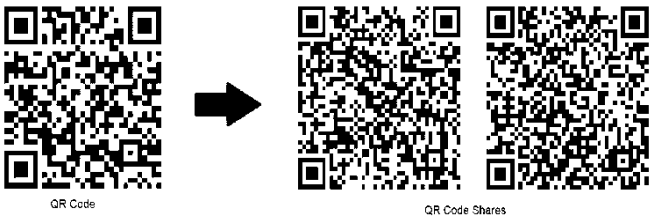
**Abstract -** *The Quick Response (QR) code was frequently implemented for data storage and data catching applications. QR codes were extensively used in fast reading applications such as statistics storage and high-speed device reading. Anyone can gain get right of entry to data saved in QR codes. Hence, they're incompatible for encoding secret statistics without the addition of cryptography or other safety. In this we proposes a visual secret sharing scheme to encode a secret QR code into distinct shares. In assessment with other techniques, the shares in proposed scheme are valid QR codes that may be decoded with some unique that means of a trendy QR code reader, so that escaping increases suspicious attackers. In addition, the secret message is recovered with the aid of XOR-ing the qualified shares. The given scheme is feasible and has low cost is proved experimentally. Two division approaches are provided, which effectively improves the sharing efficiency of (k, n) method. We proposed a standard multi-color QR code using textured patterns on data hiding by text steganography and providing security on data by using visual secret sharing scheme*

***Key Words*: Cryptography, Quick Response code, Visual secret sharing scheme, High security, Blowfish Algorithm, Division algorithm, Error correction capacity.**

## 1. INTRODUCTION

In recent years, the QR code is wide used. In standard of living, QR codes are utilized in a range of situations that embrace data storage, web links, trace ability, identification and authentication. First, the QR code is simple to be PC instrumentality identification, for example, mobile phones, scanning guns. Second, QR code features a giant storage capability, anti-damage strong, cheap and so on. The QR code has a distinct structure for correction and fast cryptography. The tags of position are used for QR code detection and orientation correction. One or many alignment patterns need to use for code deformation arrangement.

After that, the format of information areas contain error correction level and mask pattern. The error correction bits are keep within the data areas of version. The popularity of QR codes is primarily because of the subsequent features like The popularity of QR codes is primarily because of the subsequent features like robust to the copying process, easy reading by any device or any user, High encoding capacity with error correction facilities, small size and robust to geometrical distortion. Visual cryptography is a newest technology for secret message sharing. It improves the key share pictures to revive the quality of the key, relying on human visual decryption. Plus point from traditional cryptography, it has the advantages of information security, information concealment and the ease of secret recovery. The method of visual cryptography provided high security necessities of the users and protects them against varied security attacks. It is useful to implement for business oriented applications. In this paper, proposed a standard multi-color QR code using textured patterns on data hiding by text steganography and providing security on data by using visual secret sharing scheme.




The information is always needed to share between the organizations or person to person. Security of information has an important role in the information communication. The proposed work reduces risk of transmission and extends the security. We will develop a method for encoding a secret image into n share images which will displayed as noise for added security. Protection against frequent security attacks and avoidance to suspicion by attackers is given in this.

## 2. LITRATURE SURVEY

The contrast of XVCS is times greater than OVCS is stated by [1]. The attribute of OR operation reduces the quality of visual of reconstructed image for OR-based VCS (OVCS). XVCS uses XOR operation for decoding. Proposed strategy enhances the characters. Advantages of this includes easily decoding of the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages of this can be viewed as more complicated proposed algorithm.

The [2] present a blind, key based watermarking technique, which embeds a converted binary value of the watermark information into the 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 element of 1st level domain of the cover image associated to find malicious interference by an attacker. Advantages of this are that more information representation per bit change combined with error correction capabilities. This scheme increases the watermark data usability and maintains robustness against visually invariant data removal attacks. Disadvantages includes limited LSB bit in the spatial domain of the image intensity values.

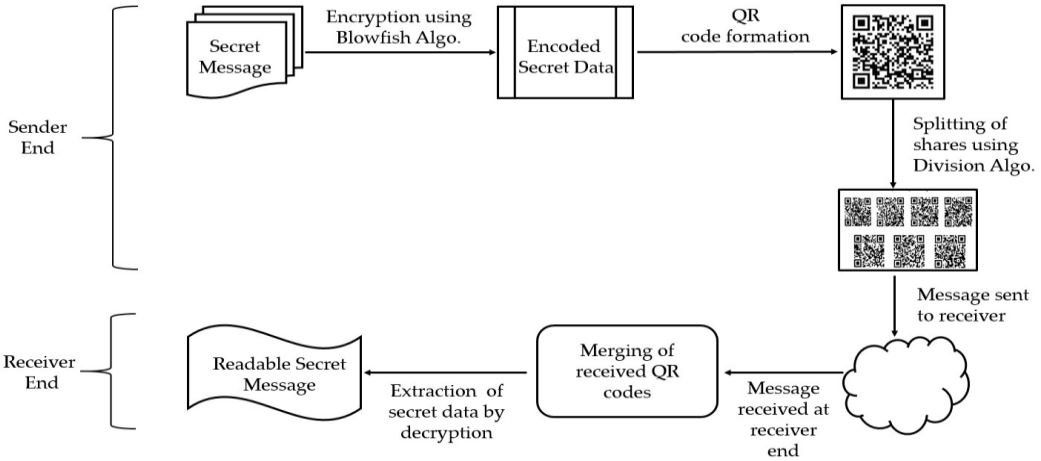
As the spatial domain is very well suspicious to attacks, it is not useful. Designing a private sharing strategy which will protect the secret QR data with reliable system is given by [3]. This approach differs from connected QR code schemes in this it uses the QR characteristics to attain secret sharing and might resist the print and scan operation. Advantages of this can be viewed as decrease in the security related issues of the secret information. Approach is feasible. It gives the readability to content, detectability for attacks and secret payload of the QR barcode. Disadvantages is that there is 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 is stated by [4]. The public level is that the same because the normal QR code storage level; so it's readable by any classical QR code application. The private level is made by exchange the black modules by specific unsmooth patterns. It consists of data encoded using q-array code with a mistake correction capability. Advantages includes that it increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the PS process. Disadvantages of this are includes need to improve the pattern recognition method. By replacing the white modules with textured patterns, we can efficient the data storage limit of 2LQR.

For securing secret information, [5] gives 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 traditional scanner, a browser can only reveal the formal information from the marked QR code. Advantages from this includes that designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography. Only the approved user with the personal key will more reveal the concealed secret with success. Disadvantages of can be viewed as the need for increasing the security.

## 3. PROPOSED APPROACH

Security for QR codes can be improved by proposed work. The important characteristics of QR code in the error correction capability is that the QR code readers can correctly decode data, even when parts of the QR image are damaged or demolished. The secret message data is encrypted into different form by using the Blowfish algorithm. Then the encrypted message data is splited into n no. of partitions called as shares and stored in different QR code share images. Then it will send to the user that is receiver. The security of the communication can be maintained by the Division Algorithm. At the receiver end, it has to merge all the QR code shares to retrieve the original secret message. The retrieving of the original message data is done by merging the QR codes shares using the generated secret key. In the proposed system the message is transmitted with the additional security by implementing the division algorithm. The system includes two users, a sender and a receiver. The sender have login by using his registered username and password and have select the receiver from the bunch of another registered users. Then he will send him the message. The receiver must connected to the internet to get the related key for unlocking the secret message. The secret message data from the sender is received in the form of shares of QR code. The receiver should merge the QR codes by using the respective algorithm and by using his key he can decrypt the message with protection and security. As using this proposed scheme, the third party malicious user unable to detect the original message data.



The sender sends the secret data or information and that private message will be encrypted with cryptographic algorithm, the encrypted cipher is then partitioned in shares of QR code for additional security and to avoid the common time whole access of the secret message.

Advantages of this scheme:

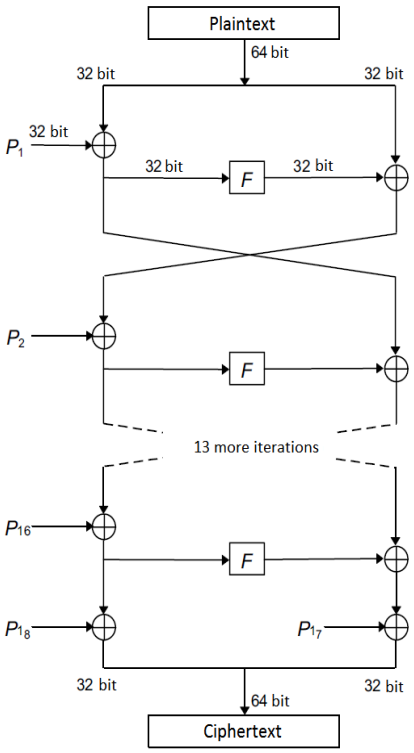
- Secure encoding of document or text secret data by algorithm.
- Higher security and more flexible access structures.
- To integrate a VCS, where the recovery requires only OR or XOR operations.
- No need to use LSB or extra hash function to extract secret data
- VCS has less computational complexity and computation cost.

## 4. STUDY OF BLOWFISH ALGORITHM

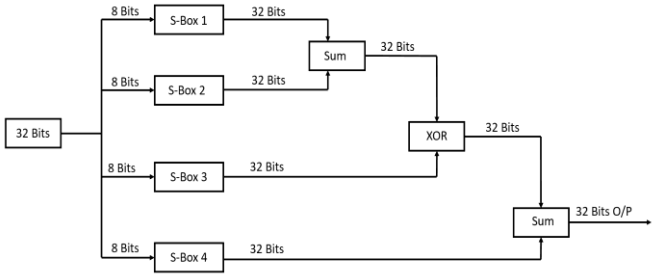
Blowfish algorithm is a replacement of DES or IDEA. It is a symmetric block cipher with a 64-bit block size. It is meant to be significantly faster than DES. The keys are of variable size from 32 bits to 448 bits, but default size is 128 bits. The total no. of rounds to be perform is 16.

Algorithm:

1. Convert input key into 18 sub keys of size 32 bits & store it in P arrays.
2. There are four S-boxes, which are 32-bit arrays with 256 entries in each.
3. XOR first 32 bits of the original key with $P_1$.
4. Similarly, XOR second 32 bits of the original key with $P_2$ and so on up to $P_{18}$.
5. Divide Plaintext into two 32-bit halves:
   XL, XR.
6. For i = 1 to 16.
   {
   XL = XL XOR $P_i$
   XR = F (XL) XOR XR
   Swap XL and XR
   }
7. Swap XL and XR.
8. XR = XR XOR $P_{17}$.
9. XL = XL XOR $P_{18}$.
10. Concatenate XL and XR.




The Function F from algorithm works as follows.




## 3. CONCLUSION

In this paper, we proposed a strategy for QR code applications by visual secret sharing scheme. This makes great improvement mainly on two aspects, higher security and more flexible QR code access structures. So that's why the computation cost of our scheme is much less than that of the previous works.

## 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] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Y. Cheng, Z. Fu and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," *in* IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2393-2403, Sept. 2018.

[7] F. Liu, Guo T: Privacy protection display implementation method based on visual passwords. CN Patent App. CN 201410542752, 2015.

[8] S J Shyu, M C Chen, "Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures," IEEE Transactions on Circuits Systems for Video Technology, vol. 25, no. 9, pp.1-1,2015.

[9] H. D. Yuan, "Secret sharing with multi-cover adaptive steganography," Information Sciences, vol. 254, pp. 197–212, 2014.

[10] J. Weir, W. Q. Yan, "Authenticating Visual Cryptography Shares Using 2 D Barcodes," in Digital Forensics and Watermarking. Berlin, German: Springer Berlin Heidelberg, 2011, pp. 196-210.

## BIOGRAPHIES

Mr. Pranav Vijay Hadawale,
Student, Bachelor of Engineering,
Dept. Of Computer Engineering,
Sahyadri Valley COE & Technology,
Pune.

Miss. Sumoli Lahu Vaje,
Student, Bachelor of Engineering,
Dept. Of Computer Engineering,
Sahyadri Valley COE & Technology,
Pune.

Miss. Dipali Sampat Wale,
Student, Bachelor of Engineering,
Dept. Of Computer Engineering,
Sahyadri Valley COE & Technology,
Pune.

Prof. Sachin Dighe,
Assistant Professor,
Dept. Of Computer Engineering,
Sahyadri Valley COE & Technology,
Pune.