



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 13, Issue 5, May 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com

Secret Sharing Schema for Quick Response Code Applications

Mugale Swati M, Prof. Late R.B

DBAT University, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India

ABSTRACT: QR codes were originally created for quick data storage and reading. They're commonly used for things like storing statistics or quickly reading information from devices. However, since anyone can access the data stored in QR codes, they're not secure for encoding secret information without extra protection like cryptography. The paper suggests a solution: a method to encode secret QR codes into different parts. Unlike other methods, these parts are still valid QR codes that can be read by regular QR code readers. This makes it more challenging for individuals with ill intent to notice any irregular activity. The secret message hidden in the QR codes can be retrieved by combining these parts using a simple operation called XOR, which can be done with smartphones or QR scanning devices. The main contribution of the work is focusing on finding the best way to divide the secret message into parts based on certain relationships, using a technique called clustering. Additionally, it compares the original message with the shared message using hashing techniques to ensure accuracy.

KEYWORDS: Hashing, Partitioning Algorithm, Quick Response code, Visual Secret Sharing Scheme.

I. INTRODUCTION

Now a days, the QR code is broadly utilized. In day by day life, QR codes are utilized in an variety of situations that include information storage, web links, traceability, identification and authentication. First, the QR code is easy to be computer equipment identification, for example, mobile phones, scanning guns. Second, QR code has a large storage capacity, anti-damage strong, cheap and so on.

The QR code has a one of a kind structure for geometrical revision and rapid disentangling. Three position labels are utilized for QR code recognition and direction adjustment. At least one arrangement designs are utilized to code twisting plan. The module take care of business is set by timing designs. Moreover, the organization data zones contain blunder adjustment level and cover design. The code form and error correction bits are put away in the adaptation data regions. The fame of QR codes is essentially because of the following features:

1. QR code is resistant to the duplicating procedure.
2. It is easy to read by any device and any user.
3. It has high encoding capacity enhanced by error correction facilities.

Visual cryptography is Process of hiding or coding information so that only Person a Messages Was intended for can read it.

Bank Card

Computer Password

E-commerce

It is Possible to retrieve any of Hidden Information, if you Only have one of Two Layers.

It Operates By Splitting an Text into Multiple Shares, Such as When Shares are Overlaid (Layer with Other Layer), Original Text becomes Visible.

Advantages of Visual Cryptography

1. No Need for Share the Key.
2. Easy to Implement and Understand.

II. REVIEW OF LITERATURE

C. N. Yang, D. S. Wang, [1] gives complete analysis of OR based and XOR based Visual Cryptography System and proves how XVCS performs better than OVCS. The contrast obtained using XVCS is higher than OVCS. The contrast of XVCS is $2^{(k-1)}$ times greater than OVCS. The OR operation's monotone property reduces the visual quality of reconstructed images in OR-based Visual Cryptography Schemes (OVCS). Advantages are: Easily decode the secret

image by stacking operation. XVCS has better reconstructed image than OVCS. Contrast obtained of the decrypted image is more and so the quality of decrypted image.

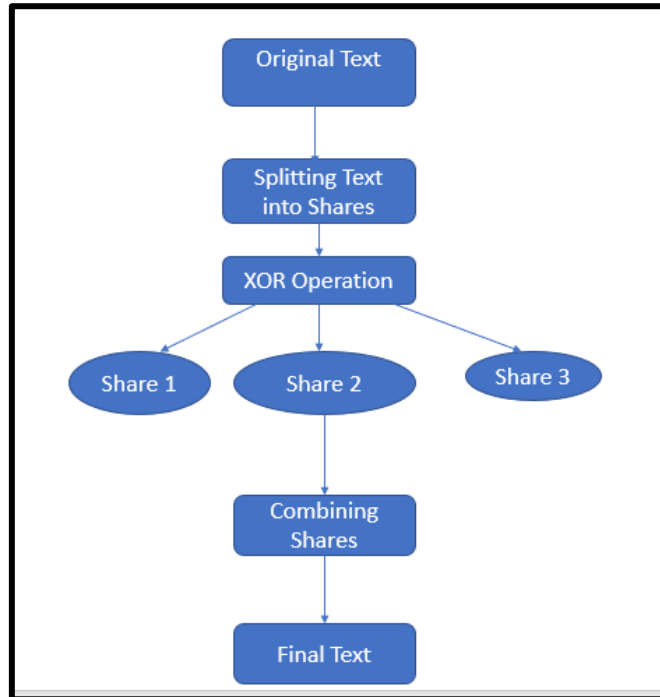


Fig.1.1:XVCS Steps[1]

Wang Xuan, Cao Peng, And Others,[2] suggested that for accurately understanding the information in a QR code, it's important to fix any distortions in the QR code image if they exist. They proposed an algorithm to correct these distortions using traditional geometric correction methods. Here is a Simplified breakdown of Process: 1.First, the algorithm finds the exact positions of the four corners of the distorted QRcodeimage.2.Then, based on these corner coordinates, the algorithm corrects the distortion of the QR code image geometrically.3.After correction, the algorithm identifies and saves the black and white data blocks of the QR code, restoring the QR code's binary image accurately. This method expands the practical uses of QR codes by ensuring accurate decoding even when the QR code image is distorted.

I. Tkachenko, W. Puech, C. Destruel, et al., Suggests The two-level QR code (2LQR) is a type of QR code that has two levels of storage: public and personal. It's useful for verifying documents [3]. The public level works like a regular QR code and can be read by any standard QR code scanner. The personal level is created by replacing black squares with special textured patterns. It holds data encoded with error correction.

Advantages:

- 1.Increases the storage capacity of the QR code.
- 2.The textured designs in 2LQR are affected by how they are printed and scanned.

Disadvantages:

- 1.Requires improvement in pattern identification methods.
- 2.The storage capacity of 2LQR can be further increased by replacing white squares with textured patterns.

Y W. Chow, W Susilo, G Yang, et al,[4] suggests a method called QR code secret sharing, which uses the error correction feature of QR codes to encode and distribute hidden messages across different activities. Each activity involves a QR code cover, which contains part of the hidden message. These covers are valid QR codes that can be scanned and decoded by any QR code reader.

Advantages:

The hidden message can be recovered by combining the information from the shared QR codes.

Disadvantage:

Secret sharing relies on code words, which could potentially limit its effectiveness or security.

P. Y. Lin,[5] indicates a better way to prevent cheating with QR codes. Here's how it works:

- 1.The person sending the QR code shares special keys with everyone involved.
- 2.After sending the code, the first person scans it and checks it using a validation code and key.
- 3.If any person tries to cheat, the process of decoding the secret message stops right there.The paper uses the highest version of QR code, version 40.

Advantage:

- 1.It introduces a more advanced way to prevent cheating with visual secret-sharing.
- 2.This method is designed to work well even with printing and scanning, making it useful in real-world applications.

Dr. R.N. Khobragade,Dr.V.M.ThakareAnd Others,[6] researchers studied different techniques for visual cryptography, such as multiple image visual cryptography (MIVC) and optimal grayscale reserving visual cryptography (GRVCS). They also explored schemes like embedded extended visual cryptography scheme (Embedded EVCS) and a simulated-annealing-based algorithm for finding optimal column vectors in visual cryptography construction problems. Additionally, they looked into a scheme called natural-image-based VSS scheme (NVSS scheme).

Y. C. Chen&Others Develops,[7]a method for sharing secret QR codes is proposed to protect private QR data using a secure distributed system. This approach is different from other QR code methods because it uses QR code properties for secret sharing and can resist printing and scanning.

Advantages:

- 1.Decreases the security risk of the secret information.
- 2.The approach is practical and offers readability of content, detection of cheaters, and customizable secret payload in the QR code.

Disadvantages:

- 1.Requires improvement in the security of the QR code scanner.
- 2.Needs to reduce modifications required for the QR system.

Z. Wang, G. R. Arcerepresents study,[8] methods for creating Hidden Visual Cryptography (HVC) using error diffusion are introduced. This means that while converting the secret image into binary shares, error diffusion is applied to produce halftone versions of these shares. Error diffusion is a simple process that creates high-quality halftone images. When the shares are combined to reconstruct the secret image, there's no interference between the different share images.

S. Mohammad Paknahad&Others,[9] compares two ways of sharing secret information through images. One way uses random grids, while the other is a new idea. The results suggest that the new method is better at controlling image quality and doesn't need a Codebook like the old method. Also, unlike the old method, the new one can use different images as covers and makes it harder for attackers to figure out the secret information.

Deepika M P, A Sreekumar,[10] looks at different ways of sharing secrets, then suggests two new versions of a sharing method. They use Gray code to create the shares and XOR operation to put the secret back together. This new method can be used for cryptography and for sharing secrets, including visual ones.

Javvaji V.K. Ratnam&Others,[11] introduces a method for sharing secret images securely. They use Boolean and shift operations to do this. The method involves encoding the original secret image to create multiple share images. These shares can only be combined to reveal the secret if a certain number of them are used together. Additionally, the original secret is encrypted with a random image and a unique authentication ID for each share to enhance security. The share images are the same size as the original image and don't requires extra space. However, one drawback mentioned is that the paper focuses on grayscale images for constructing two variantsecret sharing schemes.

III. PROPOSED METHODOLOGY

In proposed system, a novel approach is introduced to improve the security of QR codes using advanced partitioning algorithm. An existing sharing technique is subjected to loss of security. On this premise, consider the strategy for (k, n) get to structures by using the (k, k) sharing occurrence on each k-member subset dependent on specific relationship. This methodology will require countless examples as n increments. Therefore, presents partitioning calculations to group all the k-member subsets into a few assortments, in which cases of various subsets can be supplanted by just one. The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of visual sharing schema. Only the authorized user with the private key can additionally uncover the covered mystery effectively.

A. Advantages of proposed system

- 1.Efficient and Secure embedding of text.
- 2.Increases security using advanced partitioning algorithm.
- 3.Increases the sharing efficiency.
- 4.Increasingly adaptable access structures and high security.
- 5.Processing cost is less.
- 6.Message accuracy can be checked with hashing technique.

B. Architecture

Following fig.1 shows the proposed architecture of the given approach:

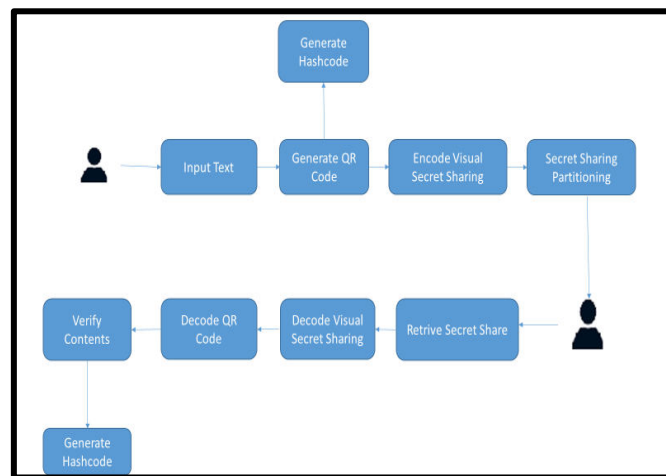


Fig.2: System Architecture

C. Algorithms

1. BlowFish Algorithm:

Blowfish is a symmetric, 64-bit block cipher with changeable length.

1. BlockSize: 64-bits
2. KeySize: 32-bits to 448-bits variable size
3. number of subkeys: 18 [P-array]
4. number of rounds: 16
5. number of substitution boxes: 4 [each having 512 entries of 32-bits each]

Step1: Generation of subkeys:

The resultant P-array holds 18 subkeys.

Step2: initialize Substitution Boxes; 4 Substitution boxes(S-boxes) are needed {S [0] ...S [4]}-256 Entries

2. AES Algorithm for Encryption. AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text.The need for coming with this algorithm is weakness in DES. The 56-bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES was to be used128-bit block with128-bit keys. Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256-bit input (0, 1)

Secret key (128_bit) +plain text (128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256-bit input

XOR state block (i/p)

Final round:10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

cipher text(128 bit)

3. Hashing Algorithm:

The MD algorithm is used for authentication of the message. It is a one-way cryptographic function that takes message of any length as input and generate fixed length hash value as output. The output hash generated is 128 bits key and it is impossible to generate same hash value for two messages, so it gives more secure way for authentication of message.

Steps:

- 1.A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
- 2.The output of a message digest is considered as a digital signature of the input data.
- 3.MD5 is a message digest algorithm producing 128 bits of data.
- 4.It uses constants derived to trigonometric Sine function.
- 5.It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
- 6.Most modern programming languages provides MD5 algorithm as built-in functions

4. K-means clustering:

K-Means Clustering is an iterative, unsupervised algorithm that is used to partition data into clusters based on the similarity present among data points. In this work K-means clustering is used in order to partition the secret message into shares so that it can be distributed to participants. In K-means data is partitioned in such a way that each data point belongs to only one group so as reduce intra-class dissimilarity and increase interclass dissimilarity. In this work for division of message into cluster, a word is compared with center of each cluster and it is then moved to the cluster in which the distance is less from the center.

Steps:

- 1.Give the number of cluster value as k.
- 2.Randomly choose the k cluster centers
- 3.Calculate mean or center of the cluster
- 4.Calculate the distance between each word to each cluster center
- 5.If the distance is near to the center then move to that cluster.
- 6.Otherwise move to next cluster.
- 7.Re-estimate
- 8.k- the center.
- 9.Repeat the process until the center doesn't move.

5. Encoding

Representation of each letter in secret message by its equivalent ASCII code.

- 1.Conversion of ASCII code to equivalent 8-bit binary number.
- 2.Division of 8-bit binary number into two 4-bit parts. Picking of random letters relating to the 4-bit parts.
- 3.Meaningful sentence development by utilizing letters got as the main letters of reasonable words.
- 4.Omission of articles, pronoun, relational word, intensifier, was/were,is/am/are, has/have/had, will/will, and would/ought to in coding procedure to give adaptability in sentence development.
- 5.Encoding isn't case touchy.

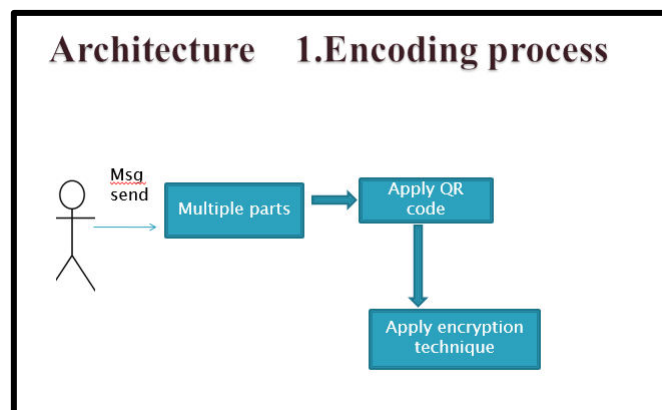


Fig.3: Encoding Process

6. Decoding Steps:

1. First letter in each word of encoded messages is taken and represented by 4-bit number
 2. 4-bit binary numbers are merged to obtain 8-bit number.
- Finally, the encoded message is recovered from ASCII codes.

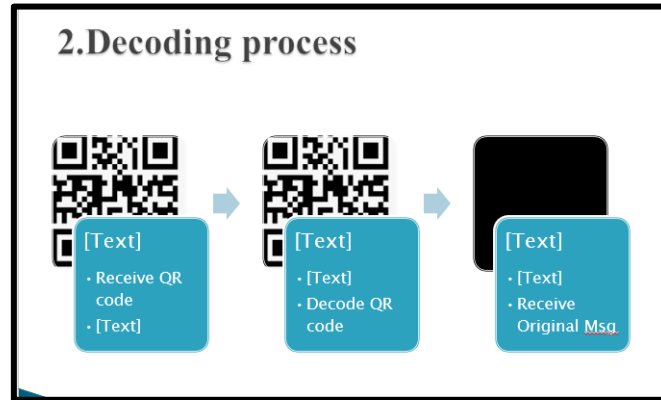


Fig.4: Decoding Process

IV. RESULTS AND DISCUSSION

Experiments can be performed on a personal computer with a configuration: Intel (R) Core (TM) i7-2120 CPU @ 3.30GHz, 8GB memory, Windows, MySQL backend database and Jdk 1.9. The application is a web application used tool for design code in Eclipse and execute on Tomcat server.

The QR code security with texture patterns by applying the X-ORing based Visual Cryptography Scheme on QR code for sharing secrets to the receiver. The figure shows the QR code example. The experiment includes two processes: encryption process and decryption process.

Sender:

Enter message, number of parts to create, enter the number of parts required to reconstruct the secret and specific user participants.



Select Post Type Public Private

Post your private message

visual secret sharing schema



Enter the number of parts to create:

4

(Integer at least 1.)

Enter the number of parts required to reconstruct the secret:

3

(Integer at least 1, no more than number of total parts.)

neha mehra

Message – visual secret sharing schema

Generated Hash code of message - 3750f73ed81827d4e6934c09231cbc2c.

Generate number of Parts using advanced partitioning technique i.e. k-means clustering

List of Secrets




Send








Receiver:

View Message:

Private Friend Messages

Profile Pic	Name	Date	Required Parts	Show
	neeta gavande	2020-07-06 08:52:15.0	3	View

Select required parts:

Profile Pic	Name	Date	Required Parts
	neeta gavande	2020-07-06 08:52:15.0	3
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>		<input type="checkbox"/>	

Decode

Decode Message:

```

gckj1r3z-r//g9ksze-80y27r-
4wrrqc-4z38tp-cdxv4k-ndfh1v-skpnxn-hd7msm-5wqb6-cvtsy3-
f25ssp-hgfh9d-w1m8aa-et9569-3ayn56-bdfs18-70
gckj1r3z-r//g96sxe-80n95k-
ttmg0k-6ri2t1-vc20ce-f8vo1s-7fbk6o-7vxiab-5mevoz-en36ac-
visual secret sharing schema
    
```

Generate Hashcode



Generated hash code:

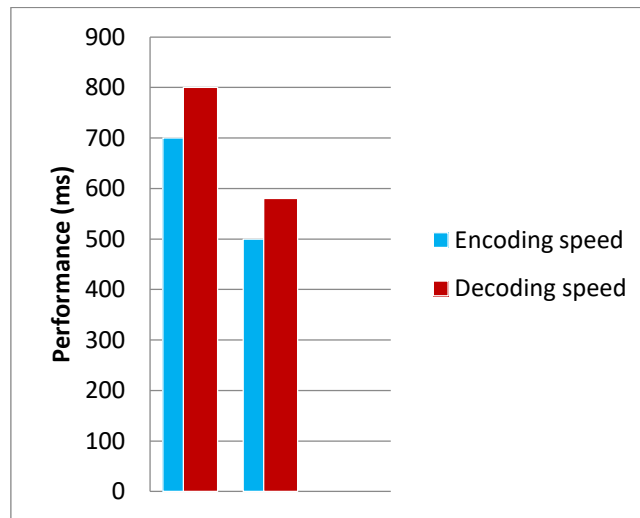
Message:

visual secret sharing schema

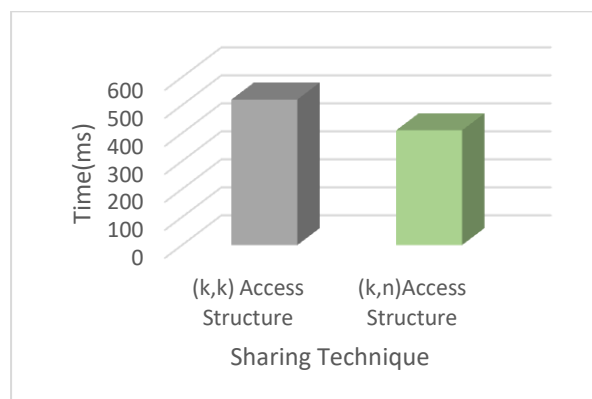
3750f73ed81827d4e6934c09231cbc2c

Comparison Table:

Algorithm	Encoding Speed	Decoding Speed	Security
Division, Sharing	low	low	low
K-means, MD5	High	high	High



Time complexity of a sharing schema algorithm quantifies the amount of time taken by an algorithm to run as a function of the length of the input.



V. 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. Message accuracy is checked using Hashing technique.

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] Wang Xuan, Cao Peng, FengLiuping, Zhu Jianle, Huopeijun, "Research on Correcting Algorithm of QR Code Image's Distortion" 17th IEEE International Conference on Communication Technology 2017.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] Miss.A.A.Naphade, Dr.R.N.Khobaragae,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.
- [7] 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.
- [8] 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.
- [9] S. Mohammad Paknahad, S. AbolfazlHosseini, 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.
- [10] Deepika M P, A Sreekumar, "Secret Sharing Scheme Using Gray Code and XOR Operation" IEEE 2017.
- [11] 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.
- [12] Y. Cheng, Z. Fu, and B. Yu, —Improved visual secret sharing scheme for QUICK RESPONSE code applications, IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2393–2403, Sep. 2018.
- [13] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. Gupta, —Efficient quantum information hiding for remote medical image sharing, IEEE Access, vol. 6, pp. 21075–21083, 2018.
- [14] Y. Li and L. Guo, —Robust image fingerprinting via distortion-resistant sparse coding, IEEE Signal Process. Lett., vol. 25, no. 1, pp. 140–144, Jan. 2018.
- [15] D. Hou, W. Zhang, J. Liu, S. Zhou, D. Chen, and N. Yu, —Emerging applications of reversible data hiding, in Proc. 2nd Int. Conf. Image Graph. Process. (ICIGP), Singapore, Feb. 2019, pp. 105– 109.
- [16] Yuqi He, Yan Hu, "A Proposed Digital Image Watermarking Based on DWT-DCT- SVD" 2018 2nd IEEE Advanced Information Management Communicates Electronic and Automation Control Conference (IMCEC 2018).
- [17] Shaekhhasan Shron "A Digital Watermarking Approach using SMQT, OTSU, DWT and IDWT" IEEE Conference 2018.
- [18] Abhilasha Singh, 2 Malay Kishore Dutta, | Lossless and Robust Digital Watermarking Scheme for Retinal Images | International Conference on "Computational Intelligence and Communication Technology" (CICT 2018). RESPONSE Code, | IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.
- [19] <https://www.slideshare.net/melendra/qr-codes-32615691>
- [20] <https://www.sciencedirect.com/science/article/abs/text/applications>
- [21] Etti Mathur, Manish Mathuria, | Unbreakable Video Processing, vol. 2017, no. 1, pp. 14, 2017. Digital Watermarking using combination of LSB and DCT | International Conference on Electronics, Communication and Aerospace Technology ICECA 2017
- [22] 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.

- [23] P. P. Thulasidharan, M. S. Nair, —QUICK RESPONSE 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.
- [24] P. Y. Lin, —Distributed Secret Sharing Approach with Cheater Prevention Based on QUICK RESPONSE CODE
- [25] Tkachenko, W. Puech, C. Destruel, et al., —Two- Level QUICK RESPONSE Code for Private Message Sharing and Document Authentication, | IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.
- [26] https://en.m.wikipedia.org/wiki/qr_code#:~:interpreted
- [27] <https://www.tutorialspoint.com/how-can-a-qr-code-be-used>
- [28] P. Y. Lin, Y. H. Chen, —High payload secret hiding technology for QUICK RESPONSE codes, | Eurasip Journal on Image &
- [29] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, —Analyzing android encrypted network traffic to identify user actions, | IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 114–125, Jan 2016
- [30] V. F. Taylor, R. Spolaor, M. Conti, and I. Martinovic, —Robust smartphone app identification via encrypted network traffic analysis, | IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp.63–78, Jan 2018.
- [31] Dipesh Vaya "OR based Visual Cryptography: A Review" DOI:10.5120/ijca2017915406
- [32] Dipesh Vaya "OR based Visual Cryptography: A Review" DOI:10.5120/ijca2017915406
- [33] https://www.researchgate.net/publication/323974127_secret_sharing_scheme_for_qr_code+Applications
- [34] Dhanashri Kulkarni "Overview of Visual secret sharing schemas for qr code message", vol 13 2019
- [35] <https://www.geeksforgeeks.org/qr-code-features/working>
- [36] David Harrington, "Data security: Defination, basic concepts And Explanation" vol.12, pp.561-521,2020



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

Scan to save the contact details