iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.39907

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

A Survey on Secrete Communication through QR Code Steganography for Military Application

Nikita Bhoskar[1], Pradnya Ithape[2], Bhagyashree Gavali[3], Prof. Pradnya Kasture[4]
[1, 2, 3, 4]*Department Of Computer Engineering, RMD Sinhgad School Of Engineering , Warje , Pune.*

Abstract: ***The quick response code (QR) has become most popular barcode because of its larger data capacity and increased damage resistance. Barcode scanners can easily extract information hidden in the QR code when scanning data forms. However, some confidential data stored directly in QR codes are not secure in real world QR apps. To proposed approach to 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. 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. In addition, the secret message is recovered with the aid of XOR-ing the qualified shares. This operation which can effortlessly be achieved the use of smartphones or different QR scanning gadgets. Contribution work is, working on optimal partitioning methods and compare original message with shared message using hashing techniques.***

Keywords: Hashing, partitioning algorithm, error correction capacity, high security, Quick Response code, visual secret sharing scheme.

I. INTRODUCTION

In recent years, the QR code is widely used. In daily life, QR codes are used in a variety of scenarios 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 unique structure for geometrical correction and high speed decoding. Three position tags are used for QR code detection and orientation correction. One or more alignment patterns are used to code deformation arrangement. The module get it together is set by timing patterns. Furthermore, the format information areas contain error correction level and mask pattern. The code version and error correction bits are stored in the version information areas.

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

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

Visual cryptography is a new secret sharing technology. It improves the secret share images to restore the complexity of the secret, relying on human visual decryption. Compared with traditional cryptography, it has the advantages of concealment, security, and the simplicity of secret recovery. The method of visual cryptography provided high security requirements of the users and protects them against various security attacks. It is easy to generate value in business 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.

II. LITERATURE SURVEY

The paper [1] proves that the contrast of XVCS is 2(x-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.

©IJRASET: All Rights are Reserved

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 outline an 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 hare 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. Disadvantgaes 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.Disadvatages 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. PROPOSED SYSTEM

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 partioning 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.

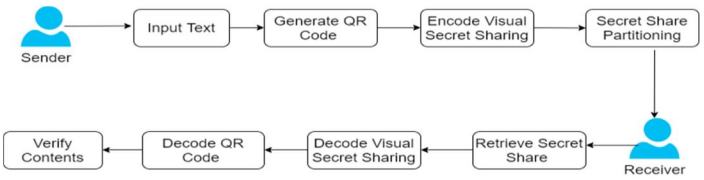


Figure 1 System Architecture

IV. ALGORITHM

A. *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.

B. *Decoding*

Steps:

1) First letter in each word of encoded message is taken and represented by 4 bit number.
2) 4 bit binary numbers of merged to obtain 8 bit number.
3) Conversion of 8 bit binary number to equivalent ASCII code.
4) Finally encoded message is recovered from ASCII codes.

V. CONCLUSIONS

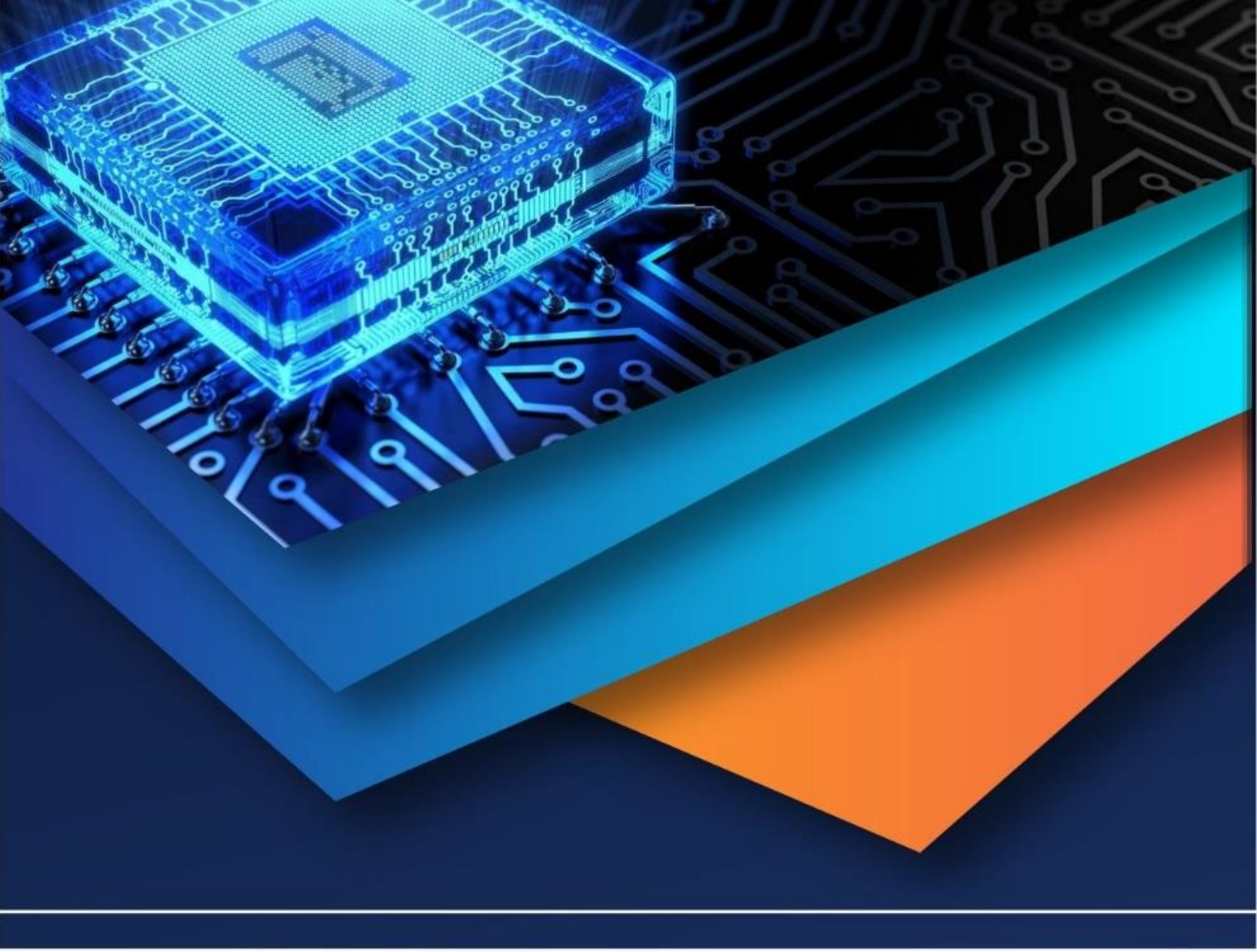
In this paper, a visual secret sharing scheme for QR code applications, which makes improvement mainly on two aspects: higher security and partitioning techniques based on specific relationships. In addition, we extended the access structure from (n, n) to (k, n) by further investigating the error correction 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.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

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, Xuetian Meng," An Improved Digital Watermarking Technology Based 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 XOR operation" 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

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)