International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
©2021 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Novel Approach for Data Hiding under QR Code using Visual Secret Sharing and Advanced Partitioning based on Specific Relationship

Miss. Neeta Chavan

Department of Computer Engineering Dr.D.Y.Patil Institute of Technology, Pimpri, Pune Savitribai Phule Pune University Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

The QR code was intended for storage data and fast reading applications. Quick Response (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. This paper 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. This operation which can effortlessly be achieved the use of smartphones or different QR scanning gadgets. Contribution work is, working on optimal partitioning method based on specific relationship using clustering and compare original message with shared message using hashing techniques.

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

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 another secret sharing innovation. 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 strategy for visual cryptography gave high security prerequisites of the users and ensures them against different security assaults. It is anything but difficult to create an incentive in business applications.

Review of Literature

The paper [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 $\mathbf{2^{(k-1)}}$ times greater than OVCS. The monotone property of OR operation degrades the visual quality of reconstructed image for OR-based VCS (OVCS). 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.

In paper [2], author proposed that, to accurately recognize the information present in QR code it is necessary to correct the QR code image and do corrections in it if required. So to correct the QR distortion algorithm is proposed based on geometric traditional geometric correction. the process involves following steps, first to find the exact coordinates of four vertices of the QR code image distortion

preprocessing of QR image is done. In second step based on coordinates obtained geometric correction is carried out .In Third step after correction the black and white data blocks of the QR code are recognized and stored, and the QR code binary image is restored accurately.Thats how it increases the application area of QR code.

The two-level QR code (2LQR), has two public and personal storage levels and may be used for document authentication [3]. The general public level is that the same because the standard QR code storage level; therefore it's readable by any classical QR code application. The private level is made by replacing the black modules by specific textured patterns. It consists of data encoded using QR code with a mistake correction capacity. Advantages are: It increases the storage capacity of the QR code. The textured patterns used in 2LQR sensitive to the P&S process. Disadvantages are: Need to improve the pattern identification method. The storage capacity of 2LQR can be increased by replacing the white modules with textured patterns.

This paper [4] propose sharing QR code secrets explodes the error correction mechanism inherent in the structure of the QR code, for circulate and encode data about a mystery message into various activities. Each activity in the plan is developed from a QR cover code, and each offer itself is a legitimate QR code that can be examined and decoded by a QR code reader. Advantages are: The secret message can be recuperated the mystery message can be recouped by consolidating the data contained in the QR code shares. Disadvantages is: secrete sharing depends on code words.

This paper [5] propose Advanced cheating prevention mechanism to QR code. First the sender of the image shares the keys with the participants and after sending the share first participant is authenticated by using validation code and key if any of the participant is dishonest then secret decoding process stops at that point itself. Highest version of the QR code that is version 40 is used in the paper. Advantage is introduced an advanced cheating-prevention visual secretsharing. Presented approach is tolerant to print and scan operation to protect QR data in real world application.

In paper [6] multiple image visual cryptography (MIVC), optimal grayscale reserving visual cryptography (GRVCS) are studied. Embedded extended visual cryptography scheme (Embedded EVCS), simulatedannealing-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 [7] paper, plan a secret QR sharing way to deal with ensure the private QR information with a protected and reliable distributed system. The proposed approach contrasts from related QR code conspires in that it utilizes the QR qualities to accomplish secret sharing and can oppose the print-and-sweep activity. Advantages are: Reduces the security risk of the secret. Approach is practical. 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 scanner tag. QR system requires lessening the alterations.

In this work [8], 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.

In this paper [9], 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 [10], 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.

In this paper [11], 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 k1 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.

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 partioning calculations to group all the kmember 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 :

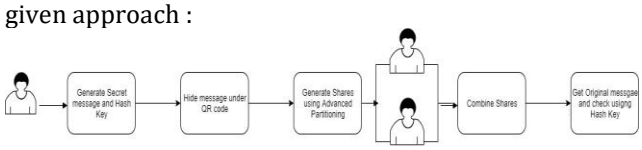


Fig. 1. Proposed System Architecture

C. Algorithms

1. 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 bit key and it is impossible to generate same hash value for two messages, so it gives more secure way for authentication of message.

Steps:

- 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.
- The output of a message digest is considered as a digital signature of the input data.
- MD5 is a message digest algorithm producing 128 bits of data.
- It uses constants derived to trigonometric Sine function.
- 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.
- Most modern programming languages provides MD5 algorithm as built-in functions

2. 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:

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

3. Encoding

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

- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts. Picking of random letters relating to the 4 bit parts.
- Meaningful sentence development by utilizing letters got as the main letters of reasonable words.
- 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.
- Encoding isn't case touchy.

4. Decoding Steps:

- First letter in each word of encoded message is taken and represented by 4 bit number.
- 4 bit binary numbers of merged to obtain 8 bit number.

Finally encoded message is recovered from ASCII codes.

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 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-OR ing 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.

A. Output Results

Input: Meeting on Sunday at JW Mariot Output:

Fig. 2. QR Code

Fig.3 Secret Shares generated of given message

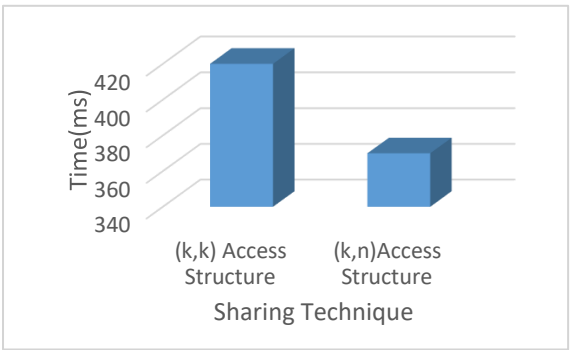
Figure 3 shows the secret shares generated of given message.

Fig.4 Retrieve the original message using selected shares

Message - Meeting on Sunday at JW Mariot

B. Comparison Results

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.



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, Feng Liuping, Zhu Jianle, Huo peijun,"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 onInformation Forensics & Security, vol. 11, no. 13, pp. 571583, 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. 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.

[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. 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.

[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"