International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

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]

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***.

Keywords: Partitioning Algorithm, Quick Response code, visual secret sharing scheme, high security, error correction capacity.

I. INTRODUCTION

Quick Response code is still widely utilised. QR codes are utilised on a regular basis in a variety of situations involving data collecting, network connections, traceability, verification, and authentication. To begin with, the QR code makes it simple to detect computer equipment, such as smart phones and scanning guns. Second, QR codes have a large storage capacity and are inexpensive.

The QR code features a geometrical revamp and a framework for quicker disengagement. Three location labels are used for QR code recognition and direction changing. At least one building style must be used in a twisting scheme. The module is intended to handle the business. Furthermore, the corporate data fields have varying degrees of modification and coverage. The code type and error correction bits are employed in the adaption data areas. These attributes are mostly responsible for the popularity of QR codes:

1. QR code-resistant duplication technique

2. Any computer or person can be easily read.

3. Bug fixes have improved its wide encoding capability.

Another milestone in visual cryptography sharing. It improves hidden image sharing to reproduce the secret's complexity using human eye decoding. In contrast to traditional cryptography, it has the advantages of camouflage, secrecy, and simplicity of covert retrieval. The visual encryption solution met the consumers' high security needs and protected them from a variety of security threats. Making a motive for business applications is not difficult.

II. LITERATURE SURVEY

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 2ˆ ((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. that's how it increases the application area of QR code.

In paper [3],The two-level QR code (2LQR), has two public and personal storage levels and may be used for document authentication 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. It increases the storage capacity of the QR code. The textured patterns used in 2LQR sensitive to the PS process. Need to improve the pattern identification method. The storage capacity of 2LQR can be increased by replacing the white modules with textured patterns.

In this paper [4],there is method to improve cost function of JPEG Steganography By exploiting the texture in micro-scale The proposed scheme is designed by using a microscope "to highlight details in an image, so that distortion definition can be more refined. Authors not extend the former work, micro-scale steganography in the spatial domain, into adaptive JPEG steganography.

This paper [5] ,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 [6], 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 secret-sharing. Presented approach is tolerant to print and scan operation to protect QR data in real world application.

In this paper [7],by using RISS algorithm for (k,n) threshold Extended cover pattern to grays scale and color pattern. Also polynomial –based ISS mechanism. using CRT ,Lower computation cost and lossless reconstruction.RISS not applicable for general (k,n) threshold scheme with any n>=k>=2.The recovery method requires more computation.

In paper [8],One solution is to find a proper texture area in the assemblage of candidate patches and replace the mirroring area. Authors propose an attacking method on this steganography, which can not only detect the stego-images but can also extract the hidden messages.

In this paper [9], 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 [10] ,considering the video steganography methods to perform secure steganography communication. Many methods have been proposed for video steganography but they're no more different types of formats, secured, quality, of the results. So here propose secure steganography methods i.e. Secure base LSB method, Neural Networks & Fuzzy logic, and check their using PSNR and MSE data of the methods. That data-set has collected is from video streams. And the result was seen with the more formats**,** more security, quality of outputs, & accuracy values of PSNR & MSE which is better than other proposed methods.

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 portioning 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. Architecture

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

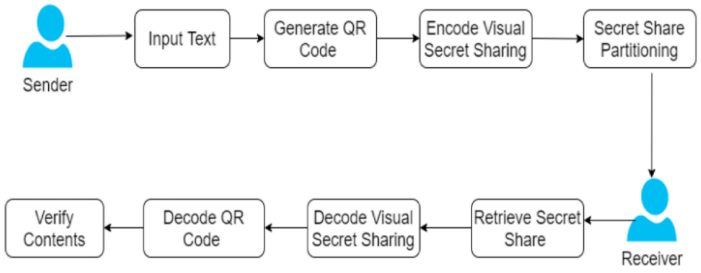

Fig 1-system architecture

B. Algorithms

1. 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.

2. Encoding

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

Steps:

- 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.

3. 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.
- Conversion of 8 bit binary number to equivalent ASCII code.
- Finally encoded message is recovered from ASCII codes.

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 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: I want to meet

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 - I want to meet

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. 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] 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 on Information Forensics Security, vol. 11, no. 13, pp. 571-583, 2016.

[4] Kejiang Chen, Hang Zhou, Wenbo Zhou, Nenghai Yu, " Defining Cost Functions for Adaptive JPEG Steganography at the Microscale", IEEE, 1556-6013 (c) 2018.

[5] 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.

[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] Xuehu Yan, Yuliang Lu, Lintao Liu , Xianhua Song, "Reversible Image Secret Sharing", IEEE,Vol-15,2020.

[8] Hang Zhou, Kejiang Chen, Weiming Zhang, and Nenghai Yu, "Comments on Steganography Using Reversible Texture Synthesis", IEEE, VOL. 26, NO. 4, APRIL 2017.

[9] Deepika M P, A Sreekumar," Secret Sharing Scheme Using Gray Code and XOR Operation" IEEE 2017.

[10] Manohar N, Peetla Vijay Kumar, "Data Encryption and Decryption using Steganography", IEEE -Xplore Part Number: CFP20K74-ART; ISBN: 978-1-7281-4876-2, 2020.