International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference on "Role of Information Technology in Social Innovations"
26th & 27th February 2019

Visual QR-Code to Authentic Secret Message: Survey

Ms. Aishwarya Chavan[1], Mr. Kundan Mehtre[2], Mr. Ravindra Mali[3],
Mr. Kamalesh Kamatkar[4],Mrs. Vrushali Kolhe[5]
[1,2,3,4,]Student, [5] Project Gauide.
B.E., Department of Computer Engineering,
D.Y.Patil college of Engineering, Akurdi Pune, Maharashtra.

Abstract-QR code used to take a piece of information from a transitory media and put it in to your cell phone, but there is no security in QR code because anyone can scan the QR and got original data. So Visual QR will help to increase security in QR. The QR code is divided into two share images that can be transmitted separately
Keywords: QR-Code, Security, XOR-Based VCS, Shares,Visual QR-Code.

1. INTRODUCTION

***QR code*:-**

A Quick Response code (QR- code) is a two dimensional bar code designed by Denso Wave in 1994 in Japan. A QR code is arranged in rows and columns of black and white, and has been designed to be read by smart phone.
QR code can hide large amount of data, numeric and alphanumeric. Thus, they have become popular all over the world. Moreover, QR codes are widely used in telecommunication due to increased popularity of smart phones, which typically contain software that can read QR-code images.
A QR-code image comprises a functional pattern and an encoding region as can be seen in Fig. 1. The patterns included in a QR-code image are finder, alignment, timing, and separator patterns. Each of these patterns has its own functionalitythe system and using the status of the bins, garbage collection routes can also be planned.

Figure: -QR Code

The QR code was used as an information carrier to transfer shadow information and its message is meaningless. The authors of presented a scheme that can resist print-and-scan operations and detect cheaters.
Additionally, a novel QR code was designed for two-level message sharing and document authentication, in which a hash function is performed when decrypting the secret. Compared with Boolean operations, the computational overhead of all the aforementioned schemes is slightly larger.

Visual QR-Code:

Visual QR code is generated using (K, n) method of cryptography. In a (k, n)-VCS, a secret image is distributed into n shares. Any k shares can obtain the secret by human vision when they are superimposed. However, possession of fewer than k shares meant no information about the secret image could be revealed.
What would work better is to subdivide each block of the QR-code into a finer matrix, e.g. 8x8: each block of the QR-code is turned to either

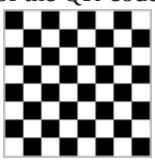
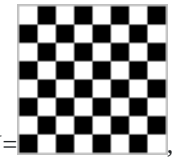
X=  or Y=  ,

Figure:-Subdivision of each QR-Block

Where,
White is actually transparent.

- A black block in the QR-code is, with odds 50%, turned to X in the first transparency and Y in the second transparency, or Y in the first and X in the second; so that the superposition of the transparencies will be essentially black.
- A white block in the QR-code is, with odds 50%, turned to X in both transparencies, or Y in both transparencies; so that the superposition of the transparencies will beessentially grey (50% dithering of black and transparent).

XOR-Based (K, n)VCS:

Extension of VCS, termed the XOR-based VCS, in which the recovery process was based on an XOR Boolean operation. With advances in computing

devices, this method of recovering information is feasible and reasonable.Two matrix consists X-VCS if they satisfies following properties:

1. The first property is contrast, which illustrates that the secret can be recovered by XOR-ing all participant shares.

2. The second property is security, which prevents any k (k, n) participants from gaining any knowledge of the secret.

For any (k, n) access structure, when a subset of k belongs to x, we must consider only any k shares of the subset. Thus, the (k, n) sharing method can be constituted by multiple (k, k) sharing instances in which each k-participant subset corresponds to one.

2. LITERATURE REVIEW:

"Adi Shamir" creates an algorithm known as Shamir's secret sharing .It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part. To reconstruct the original secret, a minimum number of parts is required. In the threshold scheme this number is less than the total number of parts. Otherwise all participants are needed to reconstruct the original secret.Shamir's Secret Sharing is used to secure a secret in a distributed way, most often to secure other encryption keys. The secret is split into multiple parts, called shares. These shares are used to reconstruct the original secret. To unlock the secret via Shamir's secret sharing, you need a minimum amount of shares. This is called the threshold, and is used to denote the minimum amount of shares needed to unlock the secret."Xuehu Yan",et al. demonstrated two PVSS schemes, Houand Quan's PVSS scheme and Chen et al.'s PVSS scheme, are found equal including key ideas, security and visual quality. The presented work will be useful for understanding the relationship between different VSS. They have also concluded their idea about the two means is equal in terms of their ideas, security and visual quality. "Manami Sasaki and Yodai Watanabe", gives idea of a formulation of encryption for multiple secret images, which is a generalization of the existing ones, and also a general method of constructing VSS schemes encrypting multiple secret images. In this paper, they have generalized the formulation of VSS encryption for multiple secret images so that those of the existing schemes, EVCS and VSS-q-PI, may be included as a special case. We then provided a general method of constructing VSS schemes encrypting multiple secret images. We also provided an example of VSS schemes which cannot be formulated as the existing ones. "Yuji Sugasuga", has classified graph-based visual secret sharing schemes, presents several optimal examples, and proposes an ideal graph-based visual secret sharing scheme with real world applications, because the pixel expansion is not greater than 4. This paper also proposes some new methods for the construction of a graph- based visual secret sharing scheme for multiple secrets with practical pixel expansion."Iuliia Tkachenko, William Puech" present a new rich QR code that has two storage levels and can be used for document authentication. This new rich QR code, named two-level QR code, has public and private storage levels. 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 q-ary code with an error correction capacity.This allows us not only to increase the storage capacity of the QR code, but also to distinguish the original document from a copy. This authentication is due to the sensitivity of the used patterns to the print-and-scan process. The pattern recognition method that used to read the second-level information can be used both in a private message sharing and in an authentication scenario. It is based on maximizing thecorrelation values."Nath et al."developed several information security systems, combining cryptography and steganography together, and the present method, ASA-QR, is also one of them. He presents a new steganography algorithm to hide any small encrypted secret message inside QR Code , which is then randomized and then, finally embed that randomized QR Code inside some common image.This QR is a combination of strong encryption algorithm and data hiding in two stages to make the entire process extremely hard to break. Here, the secret message is encrypted first and hide it in a QR Code and then again that QR Code is embed in a cover file (picture file) in random manner, using the standard method of steganography. In this way the data, which is secured, is almost impossible to be retrieved without knowing the cryptography key, steganography password and the exact unhide method."Y.W. Chow et al"introduces a novel approach to secret sharing by distributing and encoding a secret message into a number of QR code shares.This approach exploits QR code error correction redundancy, which is an inherent feature of the QR code structure. The advantage of this approach is that each share is a meaningful QR code, which individually does not reveal the secret message. The secret message can be recovered by combining the information contained in the QR code shares. Since each QR code share can be scanned and decoded by any standard QR code

reader, thismeans that the shares can be distributed via public channels without raising suspicion.In addition, since QR codes are meant to be scanned by a QR code reader, the shares do not have to be stored ortransmitted electronically and can be distributed viaprinted media. Furthermore, the shares can be constructed using any artistic QR code method as long as it can be scanned and read. Therefore, each QR code share can be constructed using a different artistic QR code scheme in order to increase the secret sharing subterfuge by reducing the likelihood of attracting the attention of potential attackers.

3. ALGORITHM USED

***Enhanced (k, n) sharing method (Division Algorithm*):**

In this secret sharing method, a secret is divided into parts, giving each participant its own unique part. To reconstruct the original secret, a minimum number of parts is required.In the threshold scheme, this number is less than the total number of parts. Otherwise, all participants are needed to reconstruct the original secret. Sub-divide each pixel into four smaller sub pixelsand need to shade these four sub pixels to represent the source image, then subjectively divide them between the cypher images are creating.

Figure:-Subdivision of each Pixel

If the original pixel in the image is set (black), fill in all four sub pixels then distribute them two per cypher layer. flip a coin to determine which pattern.Place on which layer (so that it is random). It does not matter which pair of pixels goes on which layer, when they are combined, all four pixels will be black.If the source image pixel is white, shade in just two pixels. This time, however, make sure that the same pixels are shaded on both layers.

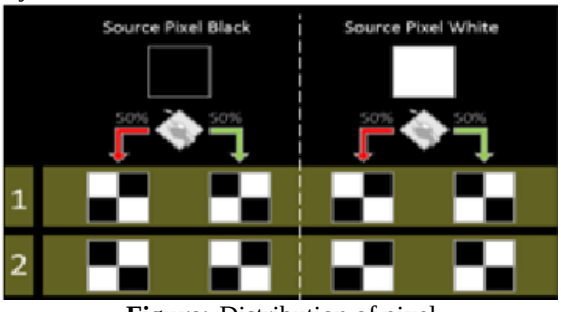


Figure:-Distribution of pixel

Step 1. Take one pixel as one time input P from the secret image.

Step 2. For P, determine whether it is
a. Black b. White

Step 3. If the color of P is

1. Black,

a. Randomly select one block from the four blocks that is peer to the black pixel in the codebook (shown as a table).

b. Randomly select one row from the selected block and assign it to vector V.

2. White,

a. Randomly select one block from the four blocks that is peer to the white pixel in the codebook (shown as a table).

b. Randomly select one row from selected block and assign it to vector V.

Step 4. V= [v1, v2, v3, v4], constructs four shares as: share1= v1, share2= v2, share3= v3, share4= v4.

Step 5. Repeat the steps from 1 to 5 until all pixels of the secret image are shared.

Step 6. To reconstruct the original image, use XOR-ing operation in order to superimpose any order of shares for different construction as follows:

(2, 4): share1 XOR share2 or share1 XOR share3 or share1 XOR share4 or share2 XOR share3 or share2 XOR share4 or share3 XOR share4.

(3, 4): share1 XOR share2 XOR share3 or share1 XOR share2 XOR share4 or share1 XOR share3 XOR share4 orshare2 XOR share3 XOR share4

(4, 4): share1 XOR share2 XOR share3 XOR share4.

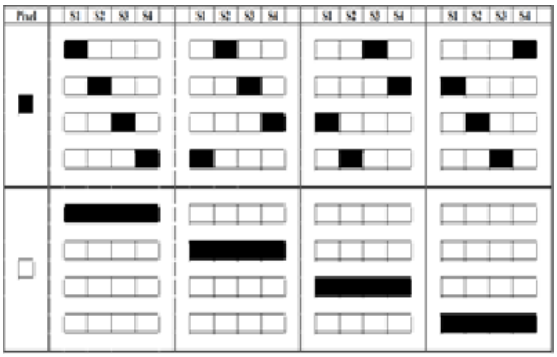


Figure:-Codebook for pixels.

REFERENCES:

[1] Yuqiao Cheng, Zhengxin Fu,BinYu,"Improved visual Secret sharing scheme for QR Code Application",IEEE Transactions on Information Forensics Security,2018.

[2] Manami Sasaki and Yodai Watanabe, "Visual Secret Sharing Schemes Encrypting Multiple Images"IEEE Transactions on Information Forensics and Security, vol. 13, no. 2, February 2018

[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] Song Wan, Yuliang Lu, Xuehu Yan and Lintao Liu"Visual Secret Sharing Scheme With (k, n) Threshold Based on QR Codes,"12th International Conference on Mobile Ad-Hoc and Sensor Networks,2016.

[5] Y. Suga,"New Constructions of (2,n)-Threshold Secret Sharing Schemes Using Exclusive-OR Operations", The 7thInternational Workshop on Advances in Information Security (WAIS2013), 2013.

[6] M. Naor and A. Shamir, "Visual cryptography," Lecture Notes in Computer Science vol.950, 1994, pp.1-12

[7] S. Dey, K. Mondal, J. Nath, et al., "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded with Any Encrypted Secret Message: ASA_QR Algorithm," International Journal of Modern Education & Computer Science, vol. 4, no. 6, pp. 59, 2012.

[8] 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.