Improved Imaginary Hidden Distributed Scheme using QR Code Application

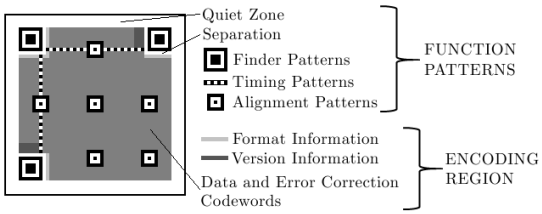
S.Dhivyalakshmi[1], K.P.Sureka Meenatchi[2], P.Sujitha[3] , D.Pavunraj[4]
[1, 2, 3]Dept of CSE
[4] Assistant Professor, Dept of CSE
[1, 2, 3] P.S.R.Rengasamy college of Engineering for women

Abstract- *Quick response (QR) codes have been widely used in applications, such as data storage and high-speed machine reading. Anyone can gain access to the information stored in QR codes; therefore, they are unsuitable for encoding secret information without the addition of cryptography or other protection. In this paper, we propose a visual secret sharing scheme to encode a secret QR code into several shares. In contrast with other techniques, the shares in our scheme are valid QR codes that can be decoded with some specific meaning by a standard QR code reader, thereby avoiding raising suspicion in potential attackers. Moreover, the secret message is recovered by XOR-ing the qualified shares, an operation that can easily be performed using smartphones or other QR scanning devices. In proposed work, the implementation is done using AES Algorithm for encryption and to split the encrypted data into several shares, Division Algorithm is used.*

Keywords- Division algorithm, error correction capacity, high security , (k , n) access structure , Quick Response code , Visual Secret Sharing Scheme .

I. INTRODUCTION

Compared with one-dimensional codes, two dimensional codes, such as Quick Response (QR) codes, allow more-widespread applications because they offer greater data storage. The QR code was originally designed by the Japanese Denso-Wave Company and has since been adopted as a universal standard specification published by ISO. In daily life, QR codes are used in a variety of scenarios that include information storage, web links, traceability, identification and authentication. Moreover, the online-to offline mode of QR codes represents a promising new trend because QR codes provide a contactless information transmission channel. According to a QR code is robust to segmental loss or symbol damage. Any user can access the information in QR codes; therefore, they are unsuitable for storing secret data. During the past few years, many efforts have been made to place and protect secret messages in QR codes. Some scholars have utilized traditional steganography or watermarking techniques. These studies embed a QR code as a secret into a mask image; or treat it as a mask to hide information. Secret extraction in both techniques requires a transformation to one specified domain, such as DCT or DWT. Regarding secret sharing methods, a polynomial algorithm was presented , where shadows were conveyed in the form of QR codes. In this scheme, the QR code was used as an information carrier to transfer shadow information and its message is meaningless.



As a secret image sharing category, the concept of a visual secret sharing scheme (also called a visual cryptography scheme, i.e., VCS) was first proposed by Naor and Shamir. 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. Later, introduced a special type of VCS, termed the XOR-based VCS (XVCS), in which the recovery process was based on an XOR Boolean operation. Irrespective of the specific operation, the most important advantage of a VCS is low computational complexity, which has attracted considerable research attention and resulted in further studies, including investigations of the VCS and QR code combinations. A (k, n)-VCS with QR shares was designed in, where the secret image was not a QR code and had to be decoded by human vision.

However, the access structure discussed in was limited to (n, n). Additionally, its security was influenced when the cover messages were similar. First, an improved (n, n) sharing method is designed to avoid the security weakness . On this basis, we consider the method for (k, n) access structures by utilizing the (k, k) sharing instance on every k-participant subset, respectively. This approach will require a large number of instances as n increases. Therefore, we further

present two division algorithms to classify all the k-participant subsets into several collections, in which instances of multiple subsets can be replaced by only one.

II. PRELIMINARIES IDEA

1) In these mobile devices uses barcode tag to read the content directly.
2) There is a risk of security problem in barcode. For this purpose QR code is designed for secret sharing mechanism. Due to this data privacy during data transmission is enhanced.
3) The secret data is further divided into some shadows and they result into embedded barcode tags.
4) They must be equal or greater than the threshold. The main advantage of this technique improves data security for data transmission. Barcode provides a convenient way for people labeling a tag n product.
5) Barcode is basically of two types : - 1- dimensional and 2-dimensional. 1-dimensional puts emphasis on product identification. 2-dimensional puts emphasis on description. The main disadvantage of barcode is limited storage in 1-d & 2-D.

III. THE PROPOSED SCHEME

First, we propose an enhanced (*n*, *n*) , (k,n) sharing method that can avoid the security weakness . On this basis, the sharing scheme of a general *k* is recommended.

A. Enhanced (n, n) sharing method

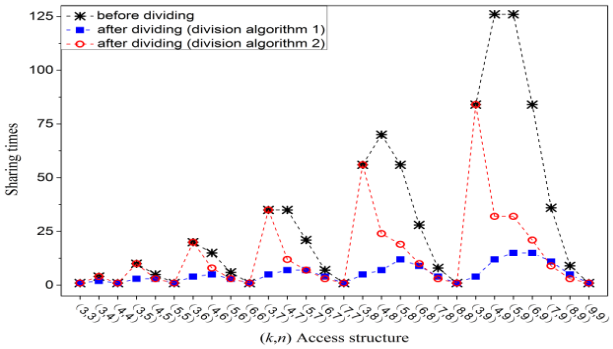
In a (n,n)secret image sharing scheme,a secret image is distributed among n parties in a such a way that cooperation of all the shares is needed fo reconstruction of the original secret image.

B. (k, n) sharing method

Based on the enhanced (*n*, *n*) method, a (*k*, *n*) method can be achieved if apply the (*k*, *k*) instance to every *k*-participant subset of the (*k*, *n*) access structure. However, there will be a huge amount of (*k*, *k*) instances, resulting in *n*! / (*k*! x (*n* - *k*)!). The cost increases significantly as *n* grows.

IV. ALGORITHM USED

Advanced Encryption Standard is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts into cipher text using keys of 128,192 and 256 bits.Based on the key size the number of rounds will vary.Large data can be encrypted using AES and really fast.Strength is the possible key permutations using finite field method internally. It performs computation on bytes rather than bits.



Division algorithm is an algorithm which given two integers N and D, computes their quotient and/or remainder, the result of Euclidean division. Some are applied by hand, while others are employed by digital circuit designs and software. Slow division and Fast division are two categories. Slow division include restoring, non performing restoring, nonrestoring, and SRT division. Fast division methods start with a close approximation on the final quotient on each iteration.

V. CONCLUSION

A visual secret sharing scheme for QR code applications, which makes improvement mainly on two aspects: higher security and more flexible access structures. The security weakness of previous work is solved in our paper. 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. However, our paper introduces only two feasible partitioning algorithms. According to super graph theory, there may be a deeper relation among those k-participant subsets. Finding this specific relationship and designing an optimal partitioning method remains open problems.

REFERENCES

[1] *Information Technology—Automatic Identification and Data Capture Techniques—Barcode Symbology—QR Code*, Standard ISO/IEC 18004:2006, 2006.

[2] P.-Y. Lin, "Distributed secret sharing approach with cheater prevention based on QR code," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 384–392, Feb. 2016.

[3] P. P. Thulasidharan and M. S. Nair, "QR code based blind digital image watermarking with attack detection code," *AEU—Int. J. Electron. Commun.*, vol. 69, no. 7, pp. 1074–1084, 2015.

[4] M. Sun, J. Si, and S. Zhang, "Research on embedding and extracting methods for digital watermarks applied to QR code images," *New Zealand J. Agricult. Res.*, vol. 50, no. 5, pp. 861–867, 2007.

[5] L. Li, R.-L. Wang, and C.-C. Chang, "A digital watermark algorithm for QR code," *IJIIP, Int. J. Intell. Inf. Process.*, vol. 2, no. 2, pp. 29–36, 2011.

[6] J.-C. Chuang, Y.-C. Hu, and H.-J. Ko, "A novel secret sharing technique using QR code," *Int. J. Image Process.*, vol. 4, no. 5, pp. 468–475, 2010.

[7] W.-Y. Chen and J.-W.Wang, "Nested image steganography scheme using QR-barcode technique," *Opt. Eng.*, vol. 48, no. 5, p. 057004, 2009.

[8] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret hiding mechanism using QR barcode," in *Proc. Int. Conf. Signal-Image Technol. Internet Based Syst. (SITIS)*, Dec. 2013, pp. 22–25.

[9] S. Dey, K. Mondal, J. Nath, and A. Nath, "Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA_QR algorithm," *Int. J. Mod. Edu. Comput. Sci.*, vol. 4, no. 6, p. 59, 2012.