Novel Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code

Alakunta Manikanta PG Scholar, M.Tech., (CSE) Department of CSE, K.S.R.M. College of Engg., Kadapa, Y.S.R. Dist., A.P.(INDIA)
V. Lokeswara Reddy Associate Professor, Department of CSE, K.S.R.M. College of Engg., Kadapa, Y.S.R. Dist., A.P.(INDIA)

Abstract: QR barcodes are used extensively due to their valuable properties, including small tag, huge data ability, consistency, and high-speed scanning. However, the confidential data of the QR barcode lacks sufficient security protection. In this paper, we design a secret QR allocation approach to protect the private QR data with a secure and reliable distributed system. The future approach differs from related QR code schemes in which it uses the QR character to get confidential sharing and can oppose the print-and-scan process. The secret can be split and conveyed with QR tags in the sharing application, and the system can retrieve the lossless confidential when authorized participants assist. General browsers can read the original data from the marked QR tag via a barcode reader, and this helps decrease the security risk of the confidential. Based on our experiments, the new approach is possible and provides content readability, cheater identify ability, and flexible confidential payload of the QR barcode.

Keywords: QR barcode, QR data, Distributed Secret Sharing Approach, Quick Response Codes

1. INTRODUCTION

To keep the privacy of the barcode data, the data normally are stored in a back-end database, and the barcode shows the web link for the database. Only a browser with the correct access can log into the database and get the confidential data. However, the web link of the back-end database creates a possible risk in which it may attract the intruder's attention. Chuang et al. proposed a secret sharing scheme for the QR tag to protect the secret barcode data. Unfortunately, the content of the QR tags is meaningless, and the shares can be easily obtained by scanning the QR tags with a barcode reader. The sharing system is also unable of preventing cheaters in its real-world application. A dependable distributed secret storage system with the QR code can be used in important applications, such as offering secret organization and authorization in e-commerce. Based on our observations, our aim was to design a distributed secret sharing scheme based on the QR barcode, thereby allowing a secret to be split into pieces and shared between individual QR-tag owners to ensure the privacy of the QR data. The secret data can be revealed when qualified QR-tag owners help. Recently, most QR-related study has used the conventional image hiding method or the conventional watermarking technique without utilizing the characteristics of the QR barcode. The image hiding schemes treat the QR tag as a secret image and then embed the QR image into the unique domain or the frequency domain of a cover image. Hence, the secret payload of such schemes is equivalent to the QR data. These schemes do not activate on the QR tag directly, so they are unable of allowing the practice of hiding/reading the secret into/from the QR code directly. QR code (abbreviated from Quick Response Code) [1] is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used. The QR code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing. A QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data is then extracted from patterns that are present in both horizontal and vertical components of the image. The proper execution of democratic rights has become linked to the availability and reliable functioning of advanced information and communication technology (ICT) [2]. While modern societies fully rely on ICT for business, work and leisure time activities, the use of ICT for democratic decision making is still in its infancy. In fact, the out date technological concepts for voting have been blamed in part for lost and uncounted votes and could therefore be responsible for biased political decisions making. Countries all over the world are examining e-voting, for it has some striking advantages over traditional paper voting, including security for casting votes, accuracy of counting and analyzing votes options to conduct voting in a centralized and decentralized manner, etc. The reasons why the e-voting technology has not matured to equivalent levels as known for business and leisure time activities lies mostly in an inherent lack of trust and fear of electronic threats. While most countries are still conceptualizing or testing e-voting systems, three cantons in Switzerland have pioneered the development of e-voting to its full technological maturity. The world is always in improvement and growth in technology, that's why we should go parallel with it, to be able as much as we can get benefit from these improvements. To keep the privacy of the barcode data, the data normally are stored in a back-end database, and the barcode shows the web link for the database. Only a browser with the correct access can log into the database and get the confidential data. However, the web link of the back-end database creates a possible risk in which it may attract the intruder's attention. Chuang et al. proposed a secret sharing scheme for the QR tag to protect the secret barcode data. Unfortunately, the content of the QR tags is meaningless, and the shares can be easily obtained by scanning the QR tags with a barcode reader. The sharing system is also unable of preventing cheaters in its real world application. A dependable distributed secret storage system with the QR code can be used in important applications, such as offering secret organization and authorization in ecommerce. Based on our observations, our aim was to design a distributed secret sharing scheme based on the QR barcode, thereby allowing a secret to be split into pieces and shared between individual QR-tag owners to ensure the privacy of the QR data [3]. The secret data can be revealed when qualified QR-tag owners help. Recently, most QR related study has used the conventional image hiding method or the conventional watermarking technique the image hiding schemes treat the QR tag as a secret image and then embed the QR image into the unique domain or the frequency domain of a cover

image. Hence, the secret payload of such schemes is equivalent to the QR data. These schemes do not activate on the QR tag directly, so they are unable of allowing the practice of hiding/reading the secret into/from the QR code directly.

II. LITERATURE SURVEY

QR Related Data Hiding Scheme :- Advanced Steganography **Algorithm:-**

Due to excessive raise in communication technology, now it is a actual problem / challenge to send some confidential information data through communication network. For this reason, Nath et al. developed some information security systems, combining cryptography and steganography simultaneously, and the present method, Advance Steganography Algorithm QR, is as well individual of them. In the present paper, the authors present a new steganography algorithm to hide any minute encrypted confidential data inside QR Code, which is then assemble in random order and then, finally embed that randomized QR Code inside some ordinary image. Quick Response Codes are a category of two dimensional matrix barcodes used for encoding data. It has become very popular in recent times for its high storage ability. The present technique is Advance Steganography Algorithm QR is a arrangement of strong encryption algorithm and data hiding in two stages to make the whole method very hard to break. Here, the confidential message is encrypted first and hide it in a QR Code and then once more that QR Code is embed in a cover file in random technique, using the standard technique of steganography. In this technique the data, which is secured, can not be retrieved without knowing the cryptography key, steganography password and the accurate unhide technique.

For encrypt in this method to secure a data we use the following algorithms:-

1) Encrypt small secret message using TTJSA method.
2) Formation of QR Code of the encrypted data.
3) Encrypting the QR Code using Randomization.
4) Hide Encrypted QR Code in the cover file using steganography.

Using data The authors used a method developed by Nath et al A. Encrypt Data Using TTJSA Method: The detail description of TTJSA method is discussed in detail by Nath et al. TTJSA is a symmetric key algorithm which is a combination of 3 distinct cryptography met technique namely Generalized modified vernam cipher method with feedback, NJJSAA technique which is essentially bit level encryption method and

MSA algorithm which is actually modified generalized Play fair method. Nath et al developed NJJSAA and MSA method. The modified generalized vernam cipher method developed by Nath et al. B. NJJSAA Algorithm: Nath et al. future a technique which is basically a bit manipulation method to encrypt or to decrypt any file. C.
MSA (Meheboob, Saima, Asoke) Encryption and Decryption Algorithm:- Nath et al. (1) future a symmetric key method where they have used a random key generator for generating the primary key and that key is used for encrypting the given resource file. MSA technique is mostly a replacement method where we take 2 characters from any input file and then search the equivalent characters from the random key matrix and store the encrypted data in a new file. MSA technique provides us several encryptions and several decryptions. The key matrix (16x16) is formed from all characters (ASCII code 0 to 255) in a random order.

Algorithms:-
1. Histogram Modification for Reversible Data Hiding:-
Histogram [4] is famous because it can be implemented easily and little overhead. To hide the information at the encoder the histogram of the original image is modified. At the decoder original image and hidden information is recovered.

Algorithm: 2 for Data Embedding:-

This algorithm is used to hide both location maps and data which are present into the original image and only side information is produced which is 40 bit in size. 3. Algorithm for Extraction of Hidden Data and Recovery of Original Image: -This algorithm is used to extract the data and original information. Using side information of 40 bit which is obtained from the encoder can be used to reproduce the non-location map correctly and then the hidden information and the original image can be recovered with the DEQ [5].

Secret sharing:- A Novel Secret Sharing Technique Using QR Code:-
In these mobile devices uses barcode tag to read the content directly. 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. The secret data is further divided into some shadows and they result into embedded barcode tags. 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. 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. Design of secret sharing technique using QR code:- Secret sharing technique was first proposed by Shamir in 1979 and was known as “Shamir’s secret sharing scheme”. Its main idea is to divide secret into shadows or shares. QR code is the way forward now. No one can directly read the content from QR codes if the number of received shadows is not achieved the predefined threshold. This shows that our scheme is secure.

Characteristics of QR code:-

1. High data capacity: QR code has the highest capacity which can store 7089 numeric characters and 4296 alphanumeric characters, 1.817 kanji characters.
2. .High speed scanning: QR code has the high speed scanning which utilizes barcode content which can easily be functioned.
3. Small printout size: In QR code the data can carry both horizontal and vertical sequences thus QR codes are better than 1D barcodes in data capacity.
4. Advance error correcting: QR codes have the correctness power that is upto 50% of area of the barcodes even if the barcode are damaged.
5. Freedom direction scanning: QR code have the freedom of

scanning direction.

III. PROPOSED WORK

Compared with a one-dimensional barcode, the two dimensional (2D) QR barcode can store a larger data payload and possesses the capability of correcting errors. The barcode data easily can be decoded and retrieved via an automatic barcode system. However, the lack of security of the barcode with private data creates problems for its real-world application [6].

DISADVANTAGES:

- The sharing scheme also is incapable of preventing cheaters in its real-world application.
- The barcode data easily can be decoded and
- retrieved via an automatic barcode system.
- Challenge on security
- Lack of accuracy. It is very burden to Users.
- Lot of paper works

A reliable distributed secret storage system with the QR code can be used in significant applications, such as offering secret management and authorization in ecommerce. Based on our observations, our aim was to design a distributed secret sharing system based on the QR barcode, thereby allowing a secret to be split into pieces and shared among individual QR-tag owners to ensure the privacy of the QR data. The secret data can be revealed when qualified QR-tag owners cooperate. Recently, most QR-related research has used the traditional image hiding manner or the traditional watermarking technique without utilizing the characteristics of the QR barcode [3]. The image hiding schemes treat the QR tag as a secret image and then embed the QR image into the special domain or the frequency domain of a cover image. Hence, the secret payload of such schemes is equal to the QR data. These schemes do not operate on the QR tag directly, so they are incapable of allowing the practice of hiding/reading the secret into/from the QR code directly.

ADVANTAGES:

- Compared with a one-dimensional barcode, the two dimensional (2D) QR barcode can store a larger data payload and possesses the capability of correcting errors.
- Accuracy, desirable that a query result contains exact the records matching the query.
- Generated QR provides more robustness than the related QR schemes.

IV METHODOLOGY

The cloud acts as php side from where you can get the QR code that is the encrypted pieces of your password you have to scan the QR and get the pieces of password and have to set the password with the file name that the admin sends you. And can see the details of your secret file you have queried about to the admin. Accuracy, desirable that a query result contains exact the records matching the query. Generated qr provides more robustness than the related QR schemes. The image hiding schemes treat the QR tag as a secret image and then embed the QR image into the special domain or the frequency domain of a cover image. Hence, the secret payload of such schemes is equal to the QR data. The secret sharing system is also used in e-coupons and e-sharing.

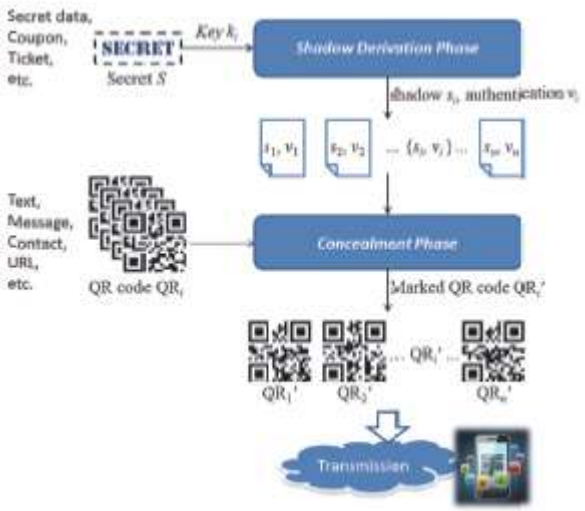


Fig.1. System Architecture

ALGORITHM TECHNIQUES:

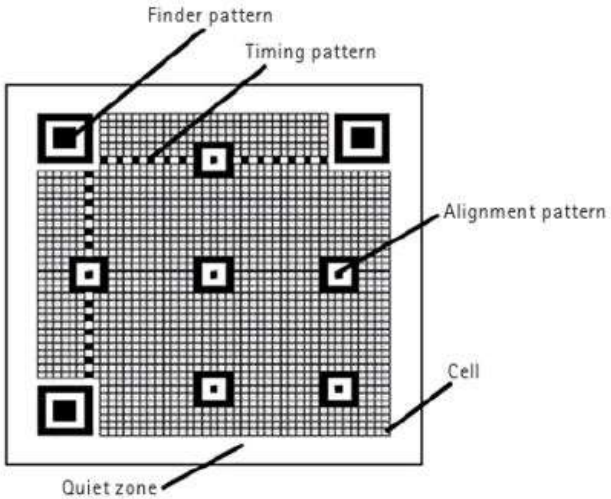


Fig.2. Pattern Finding Process

Quick Response (QR) code is a trademark name given to this 2 dimensional code system. This code was first created by Denso-Waver, a Japanese Toyota subsidiary, back in '94. It was first created as a method of tracking vehicles during assembly of different parts.

QR code algorithm:

QR code algorithm is made up of two different stages. The first one by means of similarity transformation where the novel matrix gets transformed in limited steps to real tri diagonal or Hessen berg form. The first stage of the QR algorithm prepares for the next stage which is the actual iterations of QR which are useful to the tri diagonal or Hessen berg matrix. One of the major limitations faced by the QR code algorithm is the fact that the first stage creates complete 'fill-in' in common sparse matrices (a matrix that is primarily

populated with zeros). This, therefore, hinders it from being used in huge sparse matrices because they require excessive memory.

Shamir's Secret Sharing:

In 1979, Adi Shamir created a secret sharing algorithm which allows a secret to be split into parts, and only when a number of them are added together will the original message be created. Secret can be recovered by combining certain numbers of shares. Imagine a case where you have to encrypt some data. If the key is stolen by attacker, your data will be easily decrypted. However, storing key is always difficult problem. It gets even more difficult if you need to share the key with others. This problem of storing and sharing secret key is cause of headache for administrators. However, if you use Shamir's secret sharing algorithm, you can solve the two problems to greater extent. You can divide your secret key into pieces and distribute them to other administrators. Each administrator still needs to keep a piece of secret key, but knowing a piece is not enough to recover the original secret. Because attacker must compromise multiple administrators' pieces, secret generated by Shamir's secret sharing is very difficult to be compromised.

Preparation: Suppose that our secret is 1234: We wish to divide the secret into 6 parts, where any subset of 3 parts is sufficient to reconstruct the secret. At random we obtain two numbers: 166 and 94.Our polynomial to produce secret shares (points) is therefore, we construct 6 points from the polynomial; we give each participant a different single point. Because we use instead of the points start from and not .This is necessary because if one would have he would also know the secret.

Suppose that our secret is 1234 $(S = 1234)$.

We wish to divide the secret into 6 parts $(n = 6)$, where any subset of 3 parts $(k = 3)$ is

numbers: 166 and 94.

$$(a_0 = 1234; a_1 = 166; a_2 = 94)$$

Our polynomial to produce secret shares (points) is therefore:

$$f(x) = 1234 + 166x + 94x^2$$

We construct 6 points $D_{x-1} = (x, f(x))$ from the polynomial:

$$D_0 = (1, 1494); D_1 = (2, 1942); D_2 = (3, 2578); D_3 = (4, 3402); D_4 = (5, 4414$$

We give each participant a different single point (both x and $f(x)$). Because we use D_x

necessary because if one would have $(0, f(0))$ he would also know the secret ($S = f(0$

Reconstruction: In order to reconstruct the secret any 3 points will be enough. We will compute Lagrange basis polynomials:

$$\ell_0 = \frac{x-x_1}{x_0-x_1}\cdot\frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4}\cdot\frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x-x_0}{x_1-x_0}\cdot\frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2}\cdot\frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x-x_0}{x_2-x_0}\cdot\frac{x-x_1}{x_2-x_1} = \frac{x-2}{5-2}\cdot\frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$= 1234 + 166x + 94x^2$$

Recall that the secret is the free coefficient, which means that $S = 1234$, and we are done.

Fig.3.Screen Home Screen Showing View Secret Sharing Details.

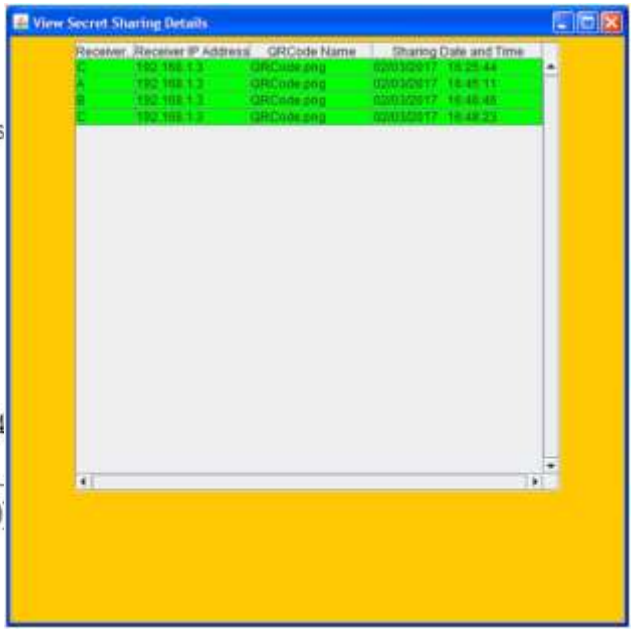
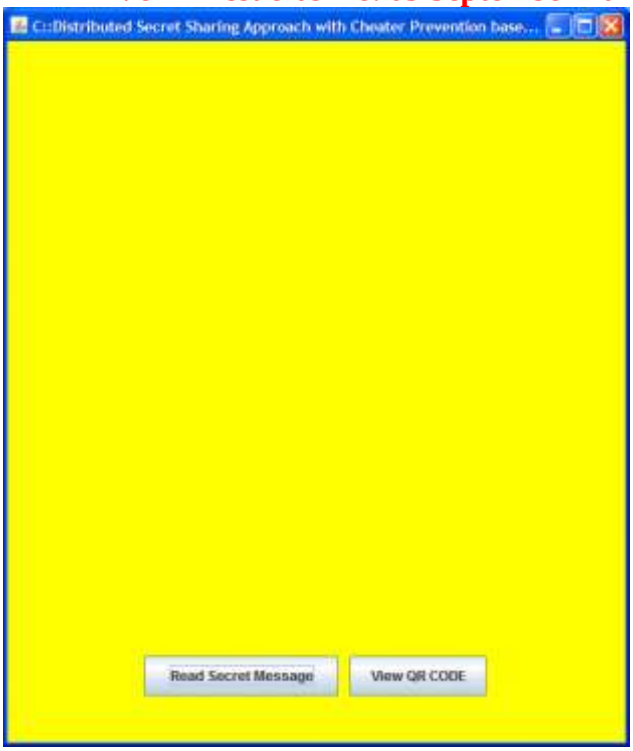
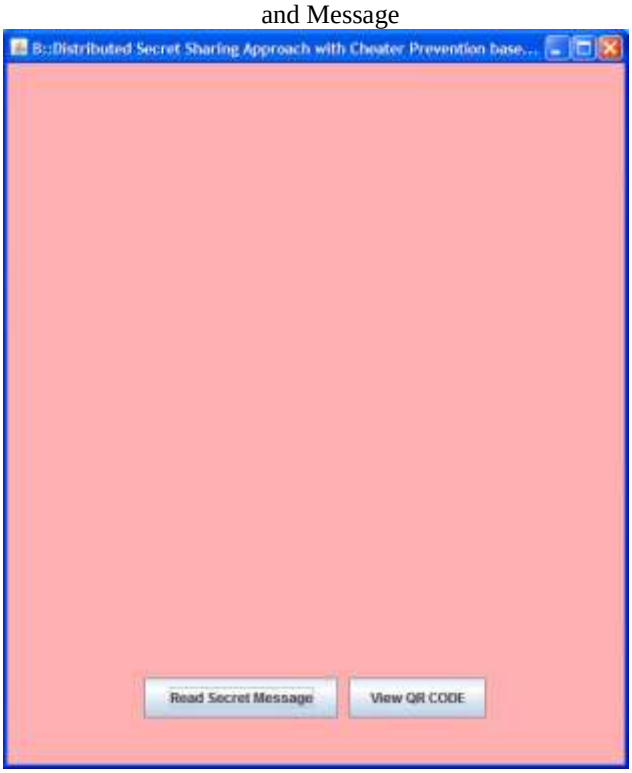


Fig.4. Screen Showing Receivers and Sender Details.

Screen:1. Receiver A with Reading and View of QR Code and Message



Screen:2. Receiver C with Reading and View of QR Code and Message



Screen:3. Receiver B with Reading and View of QR Code and Message

Screen:4. Source Window to open file and generate QR code

Screen :5. A QR Code File is Generated in a path

V. CONCLUSION

The proposed approach utilizes the characteristics of QR modules to satisfy the essentials of steganography, readability, robustness, adjustable secret capacity, blind extraction, cheater detection, and identification for the secret distribution mechanism. The new QR sharing method can achieve suitable performance when compared to related attempts. Also, the designed algorithm is possible and can be applied to the related 2-D barcodes with error correction ability.

REFERENCES

[1]. Distributed Secret Sharing Approach With Cheater Prevention Based on QR Code Pei-Yu Lin, Member, IEEE
[2]. J. C. Chuang, Y. C. Hu, and H. J. Ko, "A novel secret sharing technique using QR code," Int. J. Image Process., vol. 4, pp. 468– 475, 2010.
[3]. H. C. Huang, F. C. Chang, and W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," IEEE Trans. Consum. Electron., vol. 57, no. 2, pp. 779–787, May 2011.
[4]. 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. Educ. Comput. Sci., vol. 6, pp. 59–67, 2012.
[5]. C. H. Chung, W. Y. Chen, and C. M. Tu, "Image hidden technique using QR-Barcode," in Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process., 2009, pp. 522–525.
[6]. W. Y. Chen and J. W. Wang, "Nested image steganography scheme using QR-barcode technique
[7] Marco Carpentieri, "A Perfect Threshold Secret Sharing Scheme to Identify Cheaters", lstituto per la Ricerca sui SistemilnformaticiParalleli, Consiglio Nazionale delleRicerche, Via Pietro Castellino 111, 80123 Napoli (Na), Italy.
[8] Anindya Kumar Biswas, "An Efficient (k/n) Threshold Secret Sharing with Cheating Detection", IJIRCCE DOI: 10.15680/IJIRCCE.2016. 0407083.
[9] Sreela. S. R , G. Santhosh Kumar , Binu. V. P ,"Secret Image Sharing Based Cheque Truncation System with Cheating Detection", arXiv:1502.07993v1 [cs.CR] 26Feb 2015.
[10] L. Harn and C. Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme", Designs, Codes and Cryptography, vol. 52, pp. 15-24, 2009.
[11] Prof. D. H. Patil , Rutuja Mhaskar , Aishwarya Shirgurkar , Priya Surywanshi , Aniket Panmalkar , Rohit Patil, "A Survey Paper on Distributed Secret Sharing Approach on QR Code", IJARCCE Vol. 5, Issue 11, November 2016.
[12] Rupali Kolambe, Megah Kamble, cheaters detection and cheating identification based on Shamir Scheme, IJCA 7-8 April 2012.
[13] Chris Charnes, Josef Pieprzyk and Rei SafaviNaini "Conditionally Secure Secret Sharing Schemes with Disenrollment Capability", Conference Paper • January 1994
[14] T.-C. Wu and T.-S. Wu, Cheating detection and cheater identification in secret sharing schemes,