International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 10, pp 51-55, October-2019

QR Code Based Secret Sharing Approach in a Distributed Way

Ambadi Vijetha

Assistant Professor, Department of Computer Science And Engineering, Malla Reddy College of Engineering for Women, Hyderabad -500100, Telangana, India

Abstract - QR barcodes are mainly used for its security protection. There are more benefits in using QR code. Users can gain reliability and high speed scanning solution. In our proposed system we implemented secret QR approach to protect the data. The features of this algorithm are splitting the QR tags and pass through distribution method to maintain the secrecy of the data under the code. The other end can retrieve the data shared by grasping this secret tags with authorization. In our experiments implementation, the proposed approach is feasible and provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. The main advantage of the system is the maintain of secret application with a password. The password will be split into 5 parts and stored in a QR code. If someone is in need of data they should be aware of credentials. The password can be getting by scanning those QR codes. The admin will share the QR to the cloud. On the file requirement the user will send a query to the admin the admin will send the file name to the user the user has to use the file name and has to get the five qr codes which contains the key and getting the key he or she has to form the password for the file and can download the details.

INTRODUCTION

Across industries, the barcode labels you use to identify your products and assets are critical to your business. Compliance, brand identity, effective data/asset management require effective (and accurate) labeling. The quality of the labeling and printing effects operational efficiency. Making informed business decisions about which barcode labels – and therefore scanners, readers, printers, and more – all lies in understanding the variations of barcode labels and their unique characteristics.You need to know the type of barcodes not only for determining what works best with your products and assets but also so you can best determine the other supporting technology (integration systems, printers, scanners, readers) that will give you a comprehensive barcode solution for your entire enterprise. QR codes are a special type of barcode created by Denso Wave Incorporated.

A 1D barcode (also known as a linear code) is a visual black and white pattern, using variable-width lines and spaces for encoding information. That information – such as numbers or other keyboard characteristics – is encoded horizontally from left to right. 1D barcodes holds a limited number of characters, typically 20-25 .

A 2D barcode uses patterns, shapes, and dots to encrypt information both horizontally and vertically. 2D barcode can encrypt more characters (around 2000) in the same amount of space as a 1D barcode (which only has 20-25). Types of 2D codes include QR code, PDF417, and Data Matrix. In addition to holding more data, 2D barcodes can encrypt images, website addresses, and other binary data, which means that the codes can work independently of a database. 2D barcodes can be used to mark very small items where a traditional barcode label will not fit – think of surgical instruments or circuit boards inside of a computer. 2D barcode imagers are the best option if you are looking for fast and accurate barcode readings. 2D barcodes used in manufacturing and supply chain applications has increased, as this scanning technology efficiently scans moving items on conveyor belts without worrying about scanner alignment. Additionally, 2D barcodes are ideal for imprinting on the small parts associated with manufacturing, electronics, pharmaceutical and medical equipment industries.

EXISTING SYSTEM

QR code works in such a way that the data mapped to the barcode does not available in direct it is stored in the back end database and the barcode just gives the link to the backend database. Only the authenticate application user can login and get the data using the web link provided. However, the web link posses by the barcode is where the intruders show interest of and it falls into major risk. Chuang et al. proposed a new method of secret sharing scheme with the QR tag as a key which is a failure since the QR tag is meaningless and it is easy to retrieve the data in QR tag without any major authentication. The secret sharing system by QR tag has no control on cheaters in current scenario.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 10, pp 51-55, October-2019

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. By keeping all this into existence we planned of developing an algorithm of distributed secret sharing among owners to control the privacy of QR data to which it links to. 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 treat with 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 activate on the QR tag directly payload of such schemes is equivalent to the QR data. These schemes do not so they are unable of allowing the practice of hiding/reading the secret into/from the QR code directly 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].

DISADVANTAGE:

- The secret sharing scheme lacks privacy in sharing and it does not work against intruders in a certain way.
- The encoded barcode data with its automatic barcode system is easily decoded.
- Data security is a very big concern
- Accuracy of data is a concern for all users.
- Needs lot of paper work to be handled.

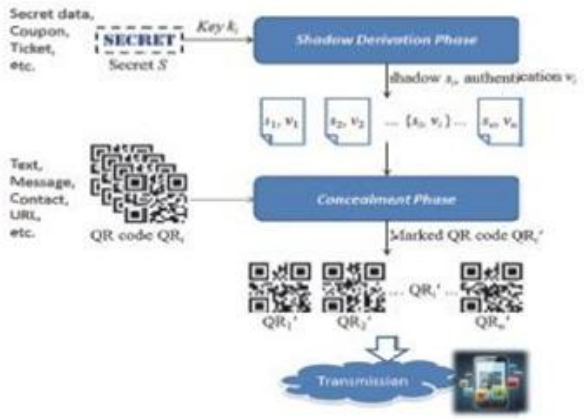
PROPOSED SYSTEM

By keeping all the existing schemes limitations and disadvantages we planned of developing an algorithm of distributed secret sharing among owners to control the privacy of QR data to which it links to. Allowing a secret key to be split into pieces and shared between individual QR-tag owners to ensure the privacy of the QR data [3]. By implementing this method of distributed secret sharing reliability and security becomes significant. This reliability allows the usage of this system in e-commerce. The working of our model is splitting a secret into pieces and shared among individual QR-tag owners to ensure the privacy of the QR data. The data can be retrieved by the users using QR tag only by authentication purpose. 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:

- 1D or Linear codes tend to be used in scenarios where the associated data is prone to changing frequently
- 2D barcodes are used where there may not be database connectivity, where space is limited, and where larger amounts of data are required
- Generated QR data provides more robustness than the related QR schemes.

ARCHITECTURE DIAGRAM

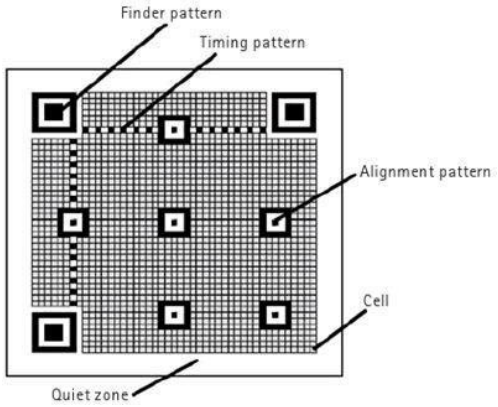


International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 10, pp 51-55, October-2019

ALGORITHM TECHNIQUES



QR code algorithm:

QR code algorithm has been constructed by two different stages.

The first stage is a resemblance transformation where the novel matrix gets transformed real tri diagonal berg form. The first stage passes the input to the second stage.

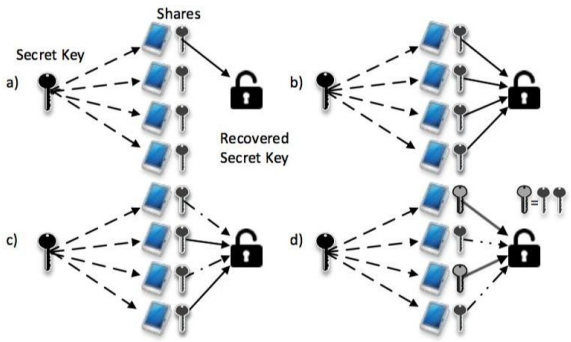
The second stage the exact iterations of QR.

By practicing it in the real the limitation in QR code algorithm is the first stage creates sparse. Therefore excessive memory will be utilized if it works for huge sparse matrix.

Shamir's Secret Sharing:

Shamir's Secret Sharing algorithm is a way to split an arbitrary secret S into N parts, of which at least K are required to reconstruct S. For example, a root password can be split among five people, and if three or more of them combine their parts, they can recover the root password. Splitting a secret works by encoding the secret as the constant in a random polynomial of K degree. For example, if we're splitting the secret number 42 among five people with a threshold of three (N=5,K=3), we might end up with the polynomial:

f(x) = 71x^3 - 87x^2 + 18x + 42



Preparation: If our secret code is 1234, we divide the secret code into 6 parts, subset of 3 parts is more than sufficient. in reconstructing the secret. At random we obtain two numbers: 166 and 94. We execute by constructing 6 points from the polynomialby sharing single point to each. This preparation is in necessity else anyone with this point can know the secret.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 10, pp 51-55, October-2019

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 sufficient to reconstruct the secret. At random we obtain two $(k - 1)$ 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:

$D_0 = (1, 1494); D_1 = (2, 1942); D_2 = (3, 2578); D_3 = (4, 3402); D_4 = (5, 4414); D_5 = (6, 5614)$

We give each participant a different single point (both x and $f(x)$). Because we use D_{x-1} instead of D_x the points start from $(1, f(1))$ and not $(0, f(0))$. This is necessary because if one would have $(0, f(0))$ he would also know the secret $(S = f(0))$

Reconstruction: Reconstruction of secrets is maintained by computing Lagrange basis polynomials:

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

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

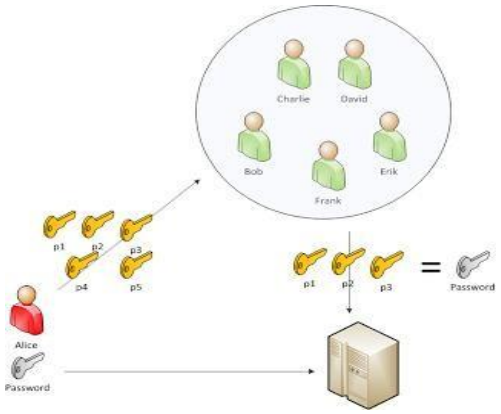
$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5 - 2} \cdot \frac{x - 4}{5 - 4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

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.



CONCLUSION

Once you sent a request to the admin for any information QR code is generated from the cloud and we can get the encrypted pieces of the password now we can scan the QR pieces and set it with the file name for authentication which is sent to you. Now you can see the details using this information. Generated QR is tough to break. QR embedded data is as same as data by payload. This system gets executed also in e-coupons and e- sharing.

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.

ISSN (online): 2581-3048
Volume 3, Issue 10, pp 51-55, October-2019

[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.

****

