IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

A Survey Paper on Distributed Secret Sharing Approach on QR Code

Prof. D. H. Patil[1], Rutuja Mhaskar[1], Aishwarya Shirgurkar[1], Priya Surywanshi[1], Aniket Panmalkar[1], Rohit Patil[1]

Information Technology, JSPM's Rajarshi Shahu College of Engineering, Pune, India[1]

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 article, 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.

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.

RELATED WORK

Literature Survey [1]:-

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 algorithm:
1) Encrypt small secret message using TTJSA method.
2) Formation of QR Code of the encrypted data.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

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 (i) Generalized modified vernam cipher method with feedback, (ii) NJJSAA technique which is essentially bit level encryption method and (iii) 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.

Literature Survey [2]:-

Reversible data hiding with histogram based difference expansion for QR code applications:-
In this paper, new algorithm is proposed in reversible data hiding and application associated with the quick response (QR) codes. QR codes are random patterns, which are observed on the corner of web pages. QR codes aims at convenience- oriented applications for mobile phone users. Mobile phone cameras are used for scanning OR code. As they are present at the corners of web pages it may reduce the quality or value of the original image. Main purpose of this paper is to get the original value of image and hiding QR code into original image and increase its embedding capacity. Corresponding hyperlink is accessed first when image with QR code is browsed. Then QR code disappears and original image is shown.

Algorithms:-
1. **Histogram Modification for Reversible Data Hiding**:- Histogram 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.

2. **Algorithm 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.

Literature Survey [3]:-

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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Security Analysis and Performance:-
This section describes mainly about the security performance of the proposed scheme. This concept is based totally on secret sharing scheme. The secret data is divided mainly into shares of shadows by the technique called secret sharing. The generated shadows are embedded into each QR code tag. If someone wants to direct the content from QR codes that is impossible if the numbers of received shadows is not achieved in the predefined threshold.

Literature Survey [4]:-

Watermarking Scheme:-
Nested Image Staganography Scheme Using QR-Barcode Technique:-
In this paper nested steganography scheme is done by using image processing and QR-barcode technique .Basically two types of secret data are covered under barcode that are lossy and lossless data .In this paper median filter is used to avoid the distortion of secret data. So this can also help to protect the data from the JPEG attacks.

Advantages:-
1. Nested scheme provides more security to the hidden data.
2 .Lossless and lossy data can be concealed and more security and be enhanced using this scheme.
3. QR barcode is used as an secret data.

There are basically two types of data security schemes:
1. Stagenography.
2. Watermarking.

Stagenography is basically done on the histogram analysis. This basically helps to obtain several statistical discrepancies. And later on they are passed through the fourier transformation to generate quantitative criterion and determine whether secrete message is embedded or not.
Watermarking is basically done using the 2D-barcode with error correction .In this paper blind digital watermarking is used where text and face both are encoded in 2D barcode . Both text and image serve secret data which is embedded under a cover image.

Embedding Algorithm:-
The proposed algorithm basically consist of three stages.

A. In this the upper path is text data encoding and it transfers text to 2D barcode pattern .And embeds into the cover image.
B. Here the face image embedding is done.
C. Final cover image for secret data embedding is done.

The first stage is barcode encoding (BCE) as QR barcode have regular format it can be eliminated by the by decreasing secret data.

RAM helps to obtain redundancy for providing more security CM is done further DR is used to map 2-D barcodes patterns into 1D data lower nibble byte discarding is done to keep face image & delete unwanted message PRNS generates pseudorandom sequence DCT provides robustness further CS coefficient selection & block selection provides more security SBC is used to secret data image hates IDCT inverse discrete cosine transform cover image to spatial domain and the secret data embedding is done while extracting inverse of the method is done and QR decoder is used to extract the original text. Because the extracted image includes noise the median filter is used that reduces the noise & appropriate face image is occurred.

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.

FUTURE SCOPE

1. The word steganography is well identified to data communication and network for hiding data inside some known image and then send through internet. We embed encrypted confidential message inside QR Code. Then, the embedded QR Code is randomized by the randomization technique used in MSA algorithm. lastly, The randomized embedded code is inserted inside some regular image. To get back the original confidential message, we have to initialy decode the randomized embedded QR Code from the embedded image. Then, we have to apply reverse randomization technique to get back original embedded QR Code. Finally, we extract the confidential message from that second host file and then apply the decryption technique to get back original confidential message. Because of this double encryption and double embedding technique, no one can extract the original confidential message without knowing the exact technique.

2. In this we have discussed about QR code and it can be captured using mobile phones cameras. We proposed new algorithm in reversible data hiding. This algorithm has the capacity of hiding the information and bit side information. But in practical the existence of such code may reduce the value of original image and may also conceals some information contained in original image. User can access the image on web page with QR code and then remove the QR code from corner of the image and original image can be recovered. It can be used in

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

online shopping sites and can also be used in many more applications in future.

3 This technique improves data security during data transmission and also the data privacy. But on the other hand it does not establish a backend database beforehand for content searching. It also saves lot of hardware cost and software maintenance. This technique can also be used in fields such as electronic tickets, air luggage inspection system, medical e-health system and other fields.

4 This paper gives the detail study of steganography & watermarking schemes. Two types of data are served as secret data which are embedded into a cover image. JPEG compression is used or for robustness 25% error correction is designed.

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," Opt. Eng., vol. 48, no. 5, pp. 057004-01– 057004-10, 2009.