International Journal of Information Sciences and Application.
ISSN 0974-2255 Volume 8, Number 1 (2017), pp. 7-10

http://www.irphouse.com

Message Sharing and Document Authentication Using QR code: A Survey

Ms. Ashitha. K. S

M.tech Scholar, Department of CSE
M-DIT Ulliyeri, Kozhikode, Kerala, India.

Ms. Rafeeda. K

Assistant Professor, Department of CSE
M-DIT Ulliyeri, Kozhikode, Kerala, India.

Abstract

The QR code designed for storage application and high speed reading application. These QR codes gives large number of applications like information storage, redirection to websites, track and trace application, Identification of products etc. Most of the graphical codes are accessed by anyone by using code readers. But there are some proposed approaches about private message sharing using QR codes. This paper examines different approaches for private message sharing and document authentication using QR codes. They are using technique like embedding secret data in error correction code words. Reed-Solomon codes are used for preventing modification attack, it gives a robust hiding mechanism. Information storage capacity is increased by using contextual awareness system concept. For authentication print and scan process have a larger impact. Textured pattern images, Pattern recognition, pixel value comparison are used for authentication application.

Keywords: QR, CDP, Error correction

INTRODUCTION

Many graphical codes such as Datamatrix code, QR code, Barcode, etc. are used in our daily lives. They have a large number of applications such as storage, Identification of products or persons etc. The popularity of these codes are day by day increasing because they are robust to the copying process, easy to read by any device and any user, they have a high encoding capacity enhanced by error correction facilities, they have a small size and are robust to geometrical distortions. But these

undeniable advantages also make some issues. Information encoded in a QR code is always accessible to everyone. There is a lack of security for the information encoded in a QR. Also it is impossible to distinguish an originally printed QR from its copy due to their insensitive to print and scan process.

For enhancing security of information contained in many approaches are done. Here one approach is using a secret hiding mechanism. Based on the error correction property of QR code, we designed a secret hiding technique for QR barcode. To communicate a QR code with the secret content, the security of QR content raises an important issue. The sender usually stores the secret in a back-end database. Browsers can read the web link from the QR code and then connect to the website of the database. Only the authorized user with password can login and retrieve the secret [8]. However, such manner requests that the QR reader needs to be online and exposes the risk of the database. Like this a lot of security issues are arising in case of QR code. For resolving this many approaches are used. These approaches are based on concealing secret information into error correction code words. These error correction code words are used to recover the damaged information. Like these concepts more powerful techniques are proposed by many authors. For increasing information storage capacity various techniques are used like adding some more levels to a QR or by adding multiple colours.

Another issue is about the authentication of such graphical codes. Because most of these cods are insensitive to print and scan process. Due to this insensitivity towards print and scan process we cannot determine that which one is the original and which one is fake. For resolving this authentication issue here we are using an approach that is digital authentication with copy detection pattern. A copy detection pattern or CDP is a maximum entropy image generated by using a secret key or password. Decision about authentication is taken based on the comparison of pixel values in digital image and scanned CDP. Pattern recognition methods are also used for authentication application.

MESSAGE HIDING MECHANISM

For embedding the information into a QR there are lot of approaches are proposed. Most important issues in message embedding into a QR is about security and storage capacity. Some approaches are discussed here. First approach is a secret hiding mechanism [1]. It is based on the error correction capacity. It can conceal the secret data into the cover QR code without distorting the readability of QR content. That is, general browsers can read the QR content from the marked QR code for the sake of reducing attention. Only the authorized receiver can encrypt and retrieve the secret from the marked QR code. It assures the security of information because secret data is concealed in error correction capacity. Another approach is robust message hiding mechanism [2]. Here Hiding secret information based on bit technique is so fragile to modification attack. If an attacker change any bit of hidden bits, it is impossible to recover the secret information. The scheme based on Reed- Solomon codes [4] and List Decoding to overcome this problem. Here the limitation is also lack of storage

capacity. In first approach there is no security method for preventing attacks like modification attack. But in second approach, they are proposed a scheme based on Reed-Solomon codes to prevent modification attacks. But storage capacity is less in two approaches. For solving this an approach is forwarded. It is Contextual QR [5]. In this approach a particular context represents tremendous data. It contains public level information and private level information. Public level contains an XML message. This message will be send to the web service and it will give the personalized information that is the private message. Contextual QR resolves storage capacity issues.

AUTHENTICATION TECHNIQUES

Most of the graphical codes such as Datamatrix code, QR code etc. are not sensitive to the print and scan process. Print and scan process giving some invisible modifications to an image. If an image is printed or scanned once some in pixel values will be changed. This concept is mainly used to detect if the image or QR is fake or original. It will helps for document authentication and image authentications. Lot of approaches are using the concept of sensitivity towards print and scan process. There is an approach for digital authentication with a copy detection pattern [3]. A copy detection pattern or CDP is a maximum entropy image generated by using a secret key or password. Depends on application combine CDP with an arbitrary digital image that contains some meaningful information(stamp, logo, barcode). Decision about authentication is taken based on the comparison of pixel values in digital image and scanned CDP. The second approach is for fighting against forged documents by using a textured image [6]. It proposed a textured image containing a visual message. It is also useful for detecting the document is legitimate or not. Here textured image will be generated with a number of patterns. Pattern recognition method based on co-relation measure is used for authentication application. Another approach for authentication application is based on geometric distortion and halftone in print and scan process [7]. It consists of pre-processing process of image, Detection of geometric distortion and the correction process. Correction process is based on interpolation points search. It also results a good authentication system.

CONCLUSION

The Quick response codes are widely used in now a days. But they can be accessed by any QR code reader and any one can read the information contained in the QR code. It is also not sensitive to the print and scan process. The main issue faced by QR codes are lack of storage capacity and authentication issue. Many approaches are proposed for resolving these issues. For increasing storage capacity an approach added two levels. Security issues are almost resolves by using the concept of concealing secret data into error correction capacity code words. Reed- Solomon codes are gives strength to QR for preventing modification attacks. For resolving authentication issues pattern recognition based on co-relation measure concept is

used. Other than pattern recognition pixel value comparison are also used to detect which one is original and which one is the fake.

REFERENCES

[1] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen. Secret hiding mechanism using QR barcode. In Signal-Image Technology & Internet- Based Systems (SITIS), 2013 International Conference on, pages 22–25. IEEE, 2013

[2] T. V. Bui, N. K. Vu, T. T.P. Nguyen, I. Echizen, and T. D. Nguyen. Robust message hiding for QR code. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on, pages 520–523. IEEE, 2014.

[3] J. Picard. Digital authentication with copy-detection patterns. In Electronic Imaging 2004, pages 176–183. International Society for Optics and Photonics, 2004.

[4] Geisel, William A. *Tutorial On Reed-Solomon Error-Correction Coding.* (1996).

[5] J. Rouillard. Contextual QR codes. In Computing in the Global Information Technology, 2008. ICCGI'08. The Third International Multi-Conference on, pages 50–55. IEEE, 2008

[6] I. Tkachenko, W. Puech, O. Strauss, J.-M. Gaudin, C. Destruel, and Guichard C. Fighting against forged documents by using textured image. In Signal Processing Conference (EUSIPCO), Proceedings of the 22th European, 2014.

[7] L. Yu, X. Niu, and S. Sun. Print-and-scan model and the watermarking countermeasure. In Image and Vision Computing, volume 23, pages 807–814. Elsevier, 2005.