

DATA SECURITY THROUGH QR CODE ENCRYPTION AND STEGANOGRAPHY

M. Mary Shanthi Rani¹, K.Rosemary Euphrasia²

¹Dept. of Comp. Sci. and Applications, Gandhigram Rural Institute, Deemed
University Gandhigram, TamilNadu. India.

²Department of computer Sci., Fatima College, Madurai, TamilNadu. India.

Abstract

The art of information hiding has become an important issue in the recent years as security of information has become a big concern in this internet era. Cryptography and Steganography play major role for secured data transfer. Steganography stands for concealed writing; it hides the message inside a cover medium. Cryptography conceals the content of a message by encryption. QR (Quick Response) Codes are 2-dimensional bar codes that encode text strings. They are able to encode information in both vertical and horizontal direction, thus able to encode more information. In this paper a novel approach is proposed for secret communication by combining the concepts of Steganography and QR codes. The suggested method includes two phases: (i) Encrypting the message by a QR code encoder and thus creating a QR code (ii) Hiding the QR code inside a colour image. This hiding process embeds the quantised QR code so that it will not make any visible distortion in the cover image and it introduces very minimum Bit Error Rate (BER). Experimental result shows that the proposed method has high imperceptibility, integrity and security..

Keywords

Steganography, QR code, BER

1. INTRODUCTION

Cryptography, Steganography and Watermarking techniques can be used to obtain security, secrecy, privacy and authenticity of data. Cryptography encrypts the message and makes it unreadable and unintelligent form called cipher. Steganography hides the data in a medium such as text file, image, audio, video etc., and conceals the very existence of the message in the medium. QR code is a two dimensional bar code capable of encoding different types of data like binary, numeric, alphanumeric, Kanji and control code. A piece of long multilingual text, a linked URL, an automated SMS message, a business card or just about any information can be embedded into the QR code.

QR codes (Quick Response codes) were introduced in 1994 by Denso-Wave, a Japanese company subsidiary of Toyota. Initially, these codes were conceived as a quick way to keep track of vehicle parts, being nowadays extremely popular in Asian countries like Japan, South Korea, China or Taiwan and becoming more and more popular in western countries by the day. [1] QR codes are capable of encoding the data both in horizontal and vertical direction, thus able to encode several times more data than the bar codes. The following table shows the maximum number of characters encoded in a QR code (version 40) with and minimum error correcting level L:

Table 1. Capacity of QR codes

| S.No. | Data Type | Characters |
|-------|-------------------|------------|
| 1 | Numeric data | 7,089 |
| 2 | Alphanumeric data | 4,296 |
| 3 | 8-bit byte data | 2,953 |
| 4 | Kanji data | 1,817 |

Fig.1 shows a QR code and Error Correction (EC) levels. [2] The technology of QR codes has proved out to be successful even if the code is partially damaged. This is feasible due to the error correction in QR codes, which is based on the Reed-Salomon Codes. There are four levels of error correction; Low (L) which can tolerate up to 7% damage, Medium (M) can tolerate up to 15% damage, Quartile (Q) can tolerate up to 25% damage and High (H) can tolerate up to 30% damage. The reason why the Low (L) error correction level is preferred is that the High error correction levels raise the percentage of code word used in error correction thereby decreasing the amount of data that can be stored in the code [3]. The black and white modules of the QR codes comprise of the encoded data. This information isn't present in human readable form hence an individual cannot anticipate the information. Any smart phone with built-in camera can capture the image of the encoded QR Code and then decode the data present in it.

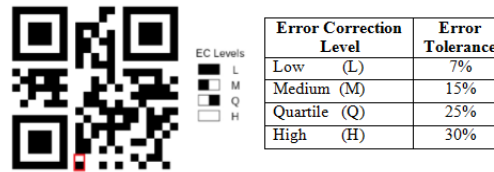


Figure 1: QR code and EC levels

The advantages of steganography and QR codes are taken into consideration for this proposed algorithm to enhance data security.

This paper is organized as follows. Section 2 reviews the works related to applications and security of QR codes, Section 3 presents the proposed scheme and Section 4 reports the experimental results and discussions. Finally, conclusions appear in Section 5.

2. RELATED WORK

Apart from Steganography, Cryptography and Visual Cryptography techniques QR codes could also be used for secured data communication. QR codes are generated by the combining visual cryptography and steganography. These QR codes are used for variety of applications like Secret communication, Copyright protection, Marketing, Business, and Education etc. Ching-yin Law & Simon So illustrate the usage of QR codes in education. They carried out some experiments and elucidate the potential of QR codes in education. Since any smart phone with built-in camera can capture the image of the QR Code and decode the information, security and secrecy become an important issue [4]. Shruti Ahuja did a literature survey regarding QR codes and security concerns and suggested few ideas. Since it is easy to modify the content stored in the 2-D code, the author advised the users to verify authenticity of the QR codes [5]. Akshara Gaikwad et al proposed a method to embed QR codes into colour images based on the luminance of the QR codes[6]. In this method the luminance of the colour image is decreased after embedding the QR codes. Dipika Sonawane et. al. suggest a method for authentication by creating OTP using QR codes instead of using conventional methods such as ID/Password[7].

All the above said suggestions and methods are reviewed and a new method is proposed in this paper for secret data communication by integrating the QR code encryption with steganography technique.

3. PROPOSED WORK

A QR code generator encrypts the given message into QR codes which could not be read or understood by human beings. But the message hidden in these QR codes can be easily decoded by any smart phone with built in camera. In order keep the message secret and to protect it from unauthorised access a new method is suggested by merging QR codes with Steganography technique. The proposed method encompasses an encoding process at the sender and a decoding process at the receiver.

3.1 Encoding Process:

The encoding process involves encryption of the secret message into QR codes followed by embedding the QR codes in a colour image as shown in Fig. 2. The steps involved in this process are

1. Select the secret message.
2. Encode it into a QR code using any QR code generator ([8]www.the-qrcode-generator.com)
3. Read a colour image and embed the quantised bits of the QR codes in the pixels of the colour image using LSB substitution method.
4. Save the stego image.

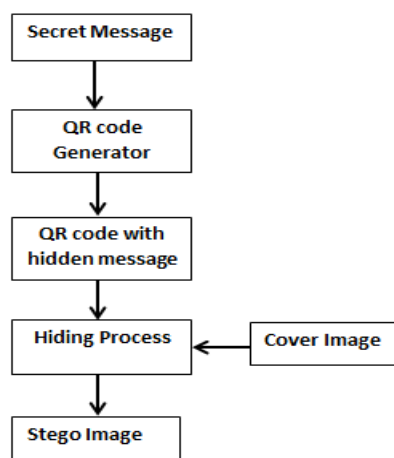


Figure 2 : Encoding Process

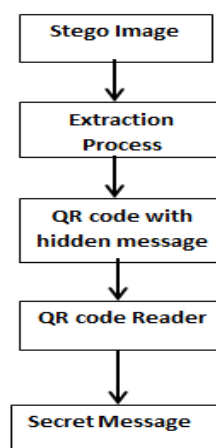


Figure 3: Decoding Process

A steganography technique must give guarantee for visual imperceptibility. In order to obtain this and to minimize the amount of changes in the luminance of the colour image, the QR code is quantised and the quantised QR code is embedded in the colour image. A QR code consists of matrix of black and white patterns. In this proposed method these patterns are represented by single bits 0 and 1 which in turn reduce the number bits to be embedded at large extent. Thus the embedding of a QR code in an image will create very minimum visible distortion which is not visible through naked eye.

3.2 Decoding Process :

The decoding process involves extraction of QR code from the stego image and reading the secret message from the QR code as shown in Fig.3. The steps involved in this process are

1. Select the stego image.
2. Extract the quantised bits of the QR code from the stego image.
3. Dequantise the bits into QR code.
4. Using any QR code scanner scan the secret message from the QR code. ([9] Zxing"online coder/Decoder")

The proposed method has been tested with various QR codes with messages of different sizes. The secret message extracted is exactly same as the original hidden message. The results of these tests are discussed in the following section.

4.RESULTS AND ANALYSIS

The proposed system makes use of the advantages of QR codes and Steganography to enhance data security. In this algorithm the secret message is encoded into QR codes using QR code generator (www.the-qrcode-generator.com). An algorithm is written in Java to embed the QR code in a colour image. This algorithm is tested with sample secret message of different sizes (100 bytes to 800 bytes) and the result is shown in Figure 4. The diagram shows that the pattern and the complexity of the QR code differ according to the size of the message encrypted. The complexity of the QR pattern will increase when huge amount of data is encrypted.
















| Size of Secret Message | QR code (200 × 200) | Cover Image (512 × 512) | Stego Image (512 × 512) |
|------------------------|---|---|--|
| 103 Bytes |  |  |  |
| 201 Bytes |  |  |  |
| 530 Bytes |  |  |  |
| 625 Bytes |  |  |  |
| 800 Bytes |  |  |  |

Figure 4: Results of Encoding Process

Some of the salient features of this work is analysed and listed below.

4.1 Imperceptibility

The most important criteria which must be met by any data embedding algorithm is imperceptibility. [9] It is evaluated by MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) values. High value of PSNR indicates high degree of imperceptibility.

Mean Square Error (MSE)

The MSE represents the average of the squares of the "errors" between our actual image and our stego image. The error is the amount by which the values of the original image differ from the degraded image.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|f(i,j) - g(i,j)\|^2$$

Where

f represents the matrix data of our original image

g represents the matrix data of our stego image

m represents the numbers of rows of pixels of the images and **i** represents the index of that row

n represents the number of columns of pixels of the image and **j** represents the index of that column






Peak Signal to Noise Ratio (PSNR)

The PSNR in decibels is computed between the cover image and the stego image. This ratio is often used as a quality measurement between the original and the stego image. The higher the PSNR, lesser is the difference between the cover image and the stego image.

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right)$$

MAX_f is the maximum signal value that exists in the cover image. The PSNR and MSE are calculated for the proposed algorithm after hiding the QR codes generated with secret messages of different sizes in the same image 9baboon) and are tabulated in Table 2. The value of PSNR is almost same and is equal to 52.6 which signposts high degree of imperceptibility. This shows the closeness of original and the stego images.

Table 2. PSNR and BER

| Cover Image (512 × 512) | Message Size | PSNR (dB) | MSE | No. of error bits | Average BER (in %) |
|---|--------------|-----------|------|-------------------|--------------------|
|  | 103 Bytes | 52.585 | .601 | 20061 | .316 |
|  | 201 Bytes | 52.587 | .601 | 20079 | .316 |
|  | 530 Bytes | 52.586 | .601 | 20095 | .316 |
|  | 625 Bytes | 52.587 | .601 | 20089 | .316 |
|  | 801 Bytes | 52.587 | .601 | 20029 | .316 |

4.2 Bit Error Rate

The Bit Error Rate is the ratio of number of bits affected due to hiding of secret message to the total number of bits in the cover image. Table 2 shows the BER calculated after hiding the QR codes with different sized messages in an image (baboon) using the proposed algorithm and one can see that BER is very minimum (.32% only). This minimum value shows that due to embedding of QR codes only a small number of bits have been changed from the original value.

4.3. Bi-level Security

It provides two levels of security to the information being transmitted as shown in Fig. 5.

- The secret message is encrypted using QR code generator. The QR code consists of matrix of Black and White Pixels which is not readable by human beings.
- But the hidden message inside the QR codes can be scanned by any smart phone with built-in camera. In order to prevent this QR code is hidden inside a colour image.

Because of this the intruders cannot easily break the system and read the message. Thus it provides two level of security for the secret message.

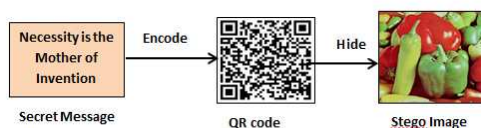


Figure 5: Bi-level Security

4.4 Message Integrity

A security algorithm is considered as an efficient one if the receiver is able to extract the exact message that was hidden and sent. In this suggested algorithm the secret message is encoded using a standard QR code generator (Zxing Encoder) and the QR code is hidden in the spatial domain of the image and no transformations are applied and so the message retrieved in the extraction process is exactly the same as the hidden message. Thus this method assures data integrity.

4.5 Histogram

Histogram is a display of statistical information to show the frequency of data items in successive numerical intervals of equal size. The following histograms are drawn between pixel value verses number of pixels. The histograms generated before and after hiding the QR codes of size (200×200) 6.13 KB in a 512×512 colour image and are shown in Fig. 6. It reveals that only very few pixel values are changed by hiding the QR codes in the cover image.

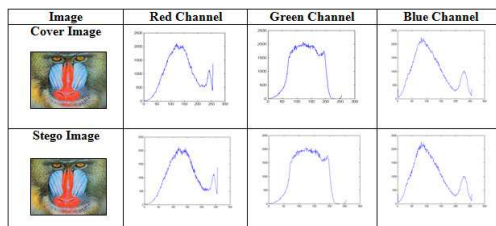


Figure 6: Comparison of histograms of cover and stego images

5.CONCLUSION

QR codes can be used for various applications such as business, marketing, education, data security, authentication etc. In this paper a novel method is suggested for data security using QR codes and steganography. Message encrypted in a QR code can be read easily by any QR code scanner. But since the proposed method incorporates steganography, it enhances the confidentiality and security. Similar work could be done in future using colour QR codes so that more information can be encrypted and sent secretly.

REFERENCES

- [1] Ioannis Kapsalis., 2013. "Security of QR Codes", Master thesis submitted in June 2013, Norwegian University of Science and Technology
- [2] Kinjal H. Pandya and Hiren J. Galiyawala, 2014. "A Survey on QR Codes: in context of Research and Application", International Journal of Emerging Technology and Advanced Engineering, Vol. 4 Issue 3, pp. 258-262
- [3] Ioannis Kapsalis., 2013. "Security of QR Codes", Master thesis submitted in June 2013, Norwegian University of Science and Technology
- [4] QRStuff. QR Code Error Correction, 2011. QRStuff blog: <http://www.qrstuff.Com/blog/2011/12/14/QR-code-error-correction>.
- [5] Law, C. & So, S., 2010. "QR codes in education. Journal of Educational Technology Development and Exchange", Vol. 3 Issue 1, pp. 85-100
- [6] Shruti Ahuja, 2014. "QR Codes and Security Concerns", International Journal of International Journal of Computer Science and Information Technologies, Vol. 5 Issue 3 pp. 3878-3879
- [7] Akshara Gaikwad et al, 2015. "Information Hiding using Image Embedding in QR Codes for Colour Images: A Review", International Journal of Computer Science and Information Technologies, Vol. 6 Issue 1, pp. 278-283
- [8] Dipika Sonawane et al., 2014. "QR based Advanced authentication for all hardware platforms "International Journal of Scientific and Research Publications, Vol. 4(1) pp.1-4
- [9] www. The-qr-code-generator.com
- [10] ZXing, "Decoder Online," 2011, <http://zxing.org/w/decode.jsp>
- [11] M. Mary Shanthi Rani and K. Rosemary Euphrasia, 2015. "Dynamic Hiding of Message in RGB Domain based on Random Channel Indicator", International Journal of Applied Engineering Research, Vol.10 No.76., pp. 478-483

Authors

Dr.M. Mary Shanthi Rani, a NET qualified Assistant Professor in the Department of Computer Science and Applications, Gandhigram Rural Institute (Deemed University), Gandhigram has twelve years of teaching and eight years of research experience as well. She has nearly twenty publications in International Journals and Conferences. Her research areas of interest are Image Compression, Information Security, Ontology, Biometrics and Computational Biology. She has authored a book titled "Novel Image Compression Methods Based on Vector Quantization" and is one of the editors of Conference Proceedings "Recent Advances in Computer Science and Applications". She has served in various academic committees in designing the curriculum for B.Sc. and M.C.A courses as well. She has also served as reviewer of Peer-reviewed International Journals and Conferences and is a Life member of Indian Society for Technical Education. She has the credit of being the Associate Project Director of UGC Indo-US 21st Knowledge Initiative Project.



Ms. K. Rosemary Euphrasia Associate Professor in Computer Science, Fatima College, Madurai. She received B.Sc., and M.Sc., degrees in Physics and M.Phil. degree in Computer science. She has 20 years of teaching experience in computer science. She is now studying towards her Ph.D. degree in Computer science at Gandhigram Rural Institute – Deemed University, Gandhigram, Tamilnadu, India. Her area of research is information security through video steganography.

