Efficient Security of Data By QR Code Encryption & Steganography

Muhamed Jasim TK
Department of Electronics & Communication Engineering
Cochin College of engineering & technology valanchery-676552, India

Pinky Mohan
Department of Electronics & Communication Engineering
Cochin College of engineering & technology valanchery-676552, India

Mitha Raj
Department of Electronics & Communication Engineering
Cochin College of engineering & technology valanchery-676552, India

Janeeba Sherin
Department of Electronics & Communication Engineering
Cochin College of engineering & technology valanchery-676552, India

Mohyiddin
Department of Electronics & Communication Engineering
Cochin College of engineering & technology valanchery-676552, India

Abstract

QR Code (QUICK RESPONCE) are basically embedded with data that can be easily decoded, OR code have substantial role in mobile application like online payment, adhar card etc... In every camera enabled smartphone can scan QR code. The QR code are 2D barcodes that encode text information. In recent year's security of information have become big concern in the internet, so the information hiding has become an important issue. In steganography, Steganography hides the data in a medium suchas text file, image, audio, video etc., and restrain the very existence of the message in the medium from a third party .In this paper ithides the message inside a cover image. The main approaches to steganography must provide two attributes: High security against the dissimilar assaults called steganalysis and second is compression. In this paper a latest approach is proposed for secret communication by combining the concept of steganography and QR codes. In the suggested method include two phase: (1) Encrypting the text message by a QR code encoder and creating a QR code, (2) Hiding the secret image inside the generated QR code. This proposed approach has to be employed in communicating confidential information.

Keywords: QR Codes, Steganography, OFDM

I. 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.

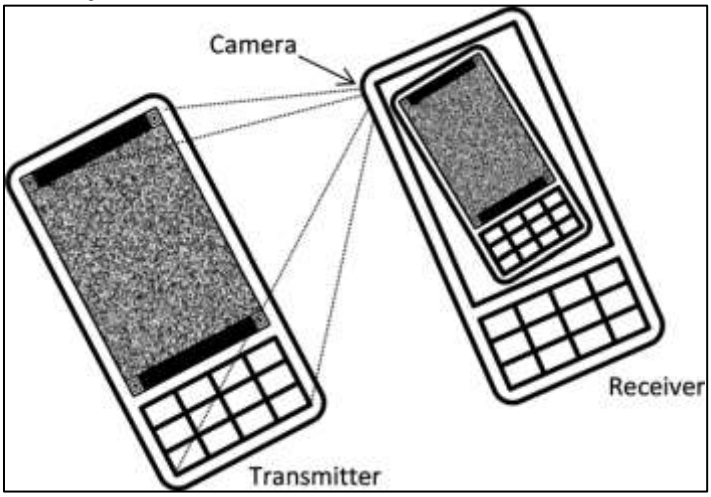

Fig. 1: An illustration of transmission of data between two handheld camera phones using a sequence of 2D barcodes

Barcodes have played a great role in facilitating numerous identification processes since their invention in 1952. In fact barcode is a simple and cost-effective method of storing machine readable digital data on paper or product packages. As pressing needs to transfer even more data faster and with high reliability have emerged, there have been many improvements that were made on the original barcode design. Invention of two dimensional (2D) or matrix barcodes opened a new front for these cost-effective codes and their application in more complex data transfer scenarios like storing contact information, URLs among other things, in which QR codes have become increasingly popular. A comparison of 2D barcode performance in camera phone applications can be found in .Much of the efforts in matrix barcode development have been dedicated to barcodes displayed on a piece of paper as that is the way they are normally used. With the replacement of books with tablets and e-Book readers one could contemplate that replacement of the paper with LCD may open another promising front for broader applications of 2D barcodes as a mean of data transfer. Moreover unlike the static paper, the LCD may display time-varying barcodes for the eventual transfer of streams of data to the receiving electronic device(s) as depicted in Fig. 1.

II. 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, and Marketing, Business, and Education etc.T. Morkel, J.H.P. Eloff , and M.S. Olivier gives a brief idea about image steganography its uses and techniques. It also attempts to identify the requirements of a good stenographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.[1]. 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 cameracan capture the image of the QR Code and decode the information, security and secrecy becomean important issue [2]. Amin Motahariand Malek Adjouadi, it says about a new approach for data modulation in 2-D barcodes is introduced, and its performance is evaluated in comparison to other standard methods of barcode modulation. In this new approach, orthogonal frequency-division multiplexing (OFDM) modulation is used together with differential phase shift keying (DPSK) over adjacent frequency domain elements. A specific aim of this study is to establish a system that is proven tolerant to camera movements, picture blur, and light leakage within neighbouring pixels of an LCD [3]. M. Mary Shanthi Rani, K.Rosemary Euphrasia proposed a method to embed a QRcode image inside a normal image. 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[4].Sinem Coleri, Mustafa Ergen and Anuj Puri give an idea about OFDM ,channel estimation based on comb type pilot arrangement is studied through different algorithms for both estimating channel at pilot frequencies and interpolating the channel .The estimation of channel at pilot frequencies is based on LS and LMS while the channel interpolation is done using linear interpolation, second order interpolation, low-pass interpolation, spline cubic interpolation, and time domain interpolation. Time-domain interpolation is obtained by passing to time domain through IDFT, zero padding and going back to frequency domain through DFT. In addition, the channel estimation based on block type pilot arrangement is performed by sending pilots at every sub-channel and using this estimation for a specific number of following symbols. We have also implemented decision feedback equalizer for all sub-channels followed by periodic block-type pilots. It also compared the performances of all schemes by measuring bit error rate with 16QAM, QPSK, DQPSK and BPSK as modulation schemes, and multipath Rayleigh fading and AR based fading channels as channel models [5].

III. PROPED SYSTEM

We presented QR code image steganography by the secret image is hidden by generated QR code, and the QR code is generated with robustness against pixel light leakage problem and image blur. While LCD technology is improving on pixel to pixel isolation, some of the image capture distortions still remain, causing neighbouring pixels of the barcode mix up in the image and resulting in some kind of Inter Symbol Interference. The main idea in resolving this problem is to interpret the barcode image as a wireless radio signal for which ISI reduction techniques have already been proven successful. One of the best and most feasible modulation methods capable of coping with severe conditions in band limited communication channels is the so-called Orthogonal Frequency Division Multiplexing or OFDM The general idea is that when dealing with band-limited, power-constrained, multipath channels, it is more efficient to transfer a bunch of narrow-band signals in parallel instead of a single high bandwidth signal.

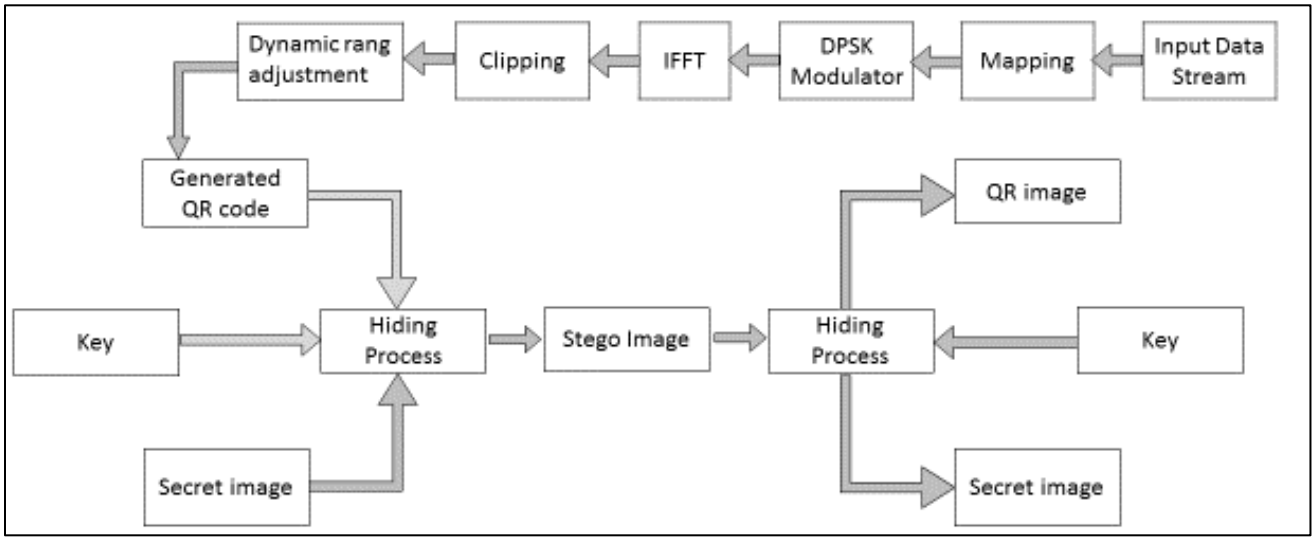

Fig. 2: Block diagram

One of the advantages of using OFDM is its effective computation method which uses the Inverse Fast Fourier Transform`(IFFT) to modulate input data into orthogonal frequencies. The modulated signal should be real-valued in order to be shown on an LCD, so the input to the IFFT algorithm should have Hermitiansymmetry. This requirement is shown in the following question:

$$T(M - m , N – n) = \mathbf{T}(m , n)^*$$

where, $0 \leq m < M$ and $0 \leq n < N$, and * denotes the complex conjugate operator.

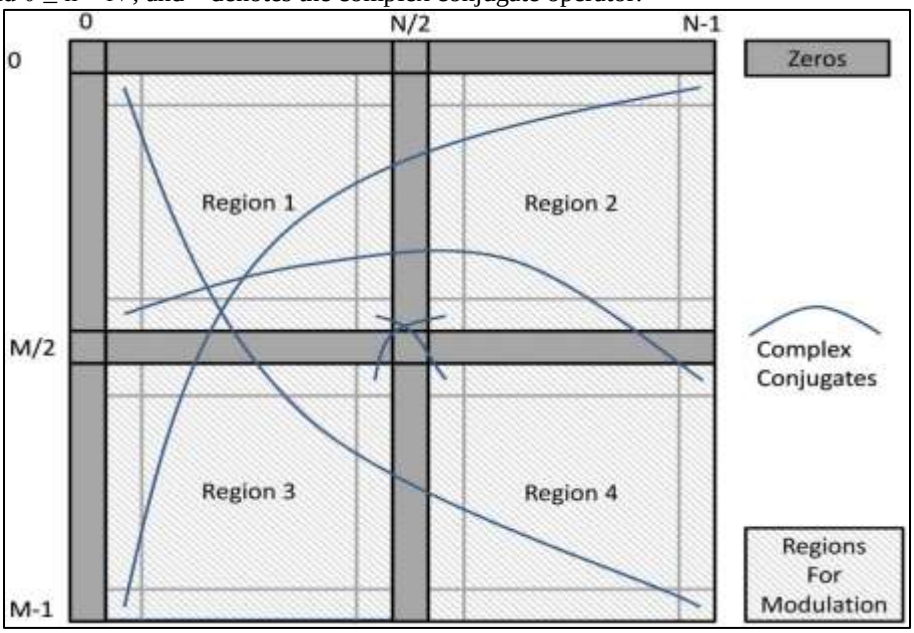

Fig. 3: Hermitian symmetric matrix used for DPSK-OFDM modulation. The IFFT of this matrix would have real-valued output on display. Bended lines show location of complex conjugate pairs

Fig. 5 shows the elements relationship in order to have a real-valued IFFT for T matrix. In this configuration, only regions 1 and 2 are used for data transmission independently, and regions 3 and 4 are calculated accordingly to have a real-valued IFFT. Moreover, the symmetry requirements for elements that have been deliberately set to zero would be automatically satisfied

A. *Constellation Mapping*

The input data is decomposed into2-bit symbols. Each symbol is converted to a complex phase by the following rules

$$11 \rightarrow e^{j\frac{1\pi}{4}} , 10 \rightarrow e^{j\frac{7\pi}{4}} , 01 \rightarrow e^{j\frac{3\pi}{4}} , 00 \rightarrow e^{j\frac{5\pi}{4}}$$

Therefore the first bit modulates the real component and the second bit modulates the imaginary component of the phase for each data symbol. These symbols are placed in a $\frac{M-2}{2} \times \frac{N-2}{1}$ matrix **S** which contains the absolute phase elements that are going to be modulated using DPSK.

B. Differential PSK

Matrix **S** is transferred into a differential Matrix D using the following method:

- D(0 ,0)=S(0,0);
- D(0 ,n)=D(0,n – 1) ×S(0,n)1≤n<N – 2;
- D(m ,n)=D(m – 1,n) ×S(m,n) 1≤m<$\frac{M}{2}$ – 1 , 0≤n<N – 2;

Subsequently, the DPSK modulated D matrix is divided into two matrices:

- D^1(m,n)=D(m,n);
- D^2(m,n)=D(m,n+$\frac{N-2}{2}$);

where 0≤m<$\frac{M}{2}$ – 1, 0≤n<$\frac{N}{2}$ – 1. These twomatrices areused to fill regions 1 and 2 of the matrix T. Regions 3 and 4 of **T**are generated based on the Hermitian symmetry requirement, and all the remaining strips on T are set to zero. These small regions, especially around region 1 (left top corner), may beused for special data transmission such as frame rate or type of error correction coding used.

C. Inverse FFT

Considering T is the frequency domain representation of the signal, the IFFT is applied on it to have the time domain signal referred to as D*i*. This signal would have zero mean because T(0,0) = 0 , so it should be adjusted in order to use the full dynamic range of pixels.

D. PAPR Adjustment

D*i* is a real-valued 2D signal with high peak to average ratios. In fact, the probability of having a high PAPR increases as the number of frequency components increases as can be seen in Fig. 6. There are several methods to limit the PAPR of OFDM signals which might be applied here with slight modifications for 2D signals. One of the most practical methods would be soft clipping of the signal in which a threshold level of **A**max based on signal average power level is set such that:

$$\text{Clipp Ratio} = \frac{\mathbf{A}\max}{\sqrt{Pavg}}$$

Where, Pavg is average power per element in the OFDM signal before clipping. Any components with higher amplitude than are Amax consequently clipped to Amax resulting in a 2D matrix

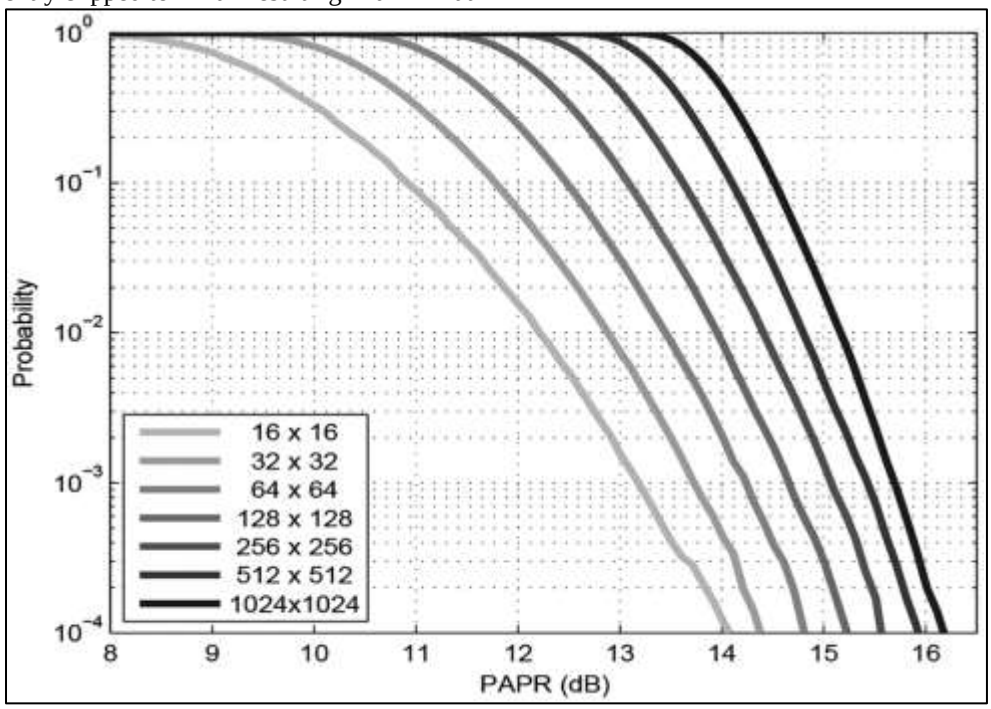

Fig. 4: Probability that the OFDM modulated 2D signal has a PAPR greater than a certain value for different image sizes

E. Amplitude Adjustment

The pixel levels in the PAPR adjusted image need to be transformed into LCD dynamic range levels for efficient utilization of transmission power. Normally the intensity levels on the LCD goes from 0 to Imax . So Dc values are transformed linearly to this range using the following equation:

$$Da(i , j) = \frac{Dc (i ,j) - Min (Dc)}{Max (Dc) - Min (Dc)} Imax$$

Thus the average power of Da is maximized for LCD projection.

F. Key

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes. For the one-time pad system the key must be at least as long as the message. In encryption systems that use a cipher algorithm, messages can be much longer than the key. The key must, however, be long enough so that an attacker cannot try all possible combinations.A key length of 80 bits is generally considered the minimum for strong security with symmetric encryption algorithms. 128-bit keys are commonly used and considered very strong. See the key size article for a more complete discussion.The keys used in public key cryptography have some mathematical structure. For example, public keys used in the RSA system are the product of two prime numbers. Thus public key systems require longer key lengths than symmetric systems for an equivalent level of security. 3072 bits is the suggested key length for systems based on factoring and integer discrete logarithms which aim to have security equivalent to a 128 bit symmetric cipher. Elliptic curve cryptography may allow smaller-size keys for equivalent security, but these algorithms have only been known for a relatively short time and current estimates of the difficulty of searching for their keys may not survive. As of 2004, a message encrypted using a 109-bit key elliptic curve algorithm had been broken by brute force.[2] The current rule of thumb is to use an ECC key twice as long as the symmetric key security level desired. Except for the random one-time pad, the security of these systems has not (as of 2008) been proven mathematically, so a theoretical breakthrough could make everything one has encrypted an open book. This is another reason to err on the side of choosing longer keys.

IV. RESULTS AND ANALYSIS

The proposed technique has been evaluated in MATLAB R2015b .The system makes use of the advantages of QR codes and Steganography to enhance data security. In this algorithm the normal message is encoded into QR codes using QR code generator (www.the-qrcode-generator.com).The complexity of the QR pattern will increase when huge amount of data is encrypted. The modulated encrypted QR code so obtained was transferred from one phone to another by capturing the image. This captured image was successfully decoded and decrypted to obtain the actual data. This algorithm is tested with sample secret message of different sizes (100 bytes to 800 bytes) and the result is shown in table 1. The diagram shows that the pattern and the complexity of the QR code differs according to the size of the message encrypted. The complexity of the QR pattern will increase when huge amount of data is encrypted.

Our experiment proved to be successful in being able to convert a general purpose carrier QR code into canvas image that used in steganography. The fig 5 showing the secret image is combine with generated QR code. The general message, which was generated with high error correction, gave us an opportunity to hide a secret message or normal message, this allowed the general message to scan successfully at 100% despite the presence of hidden information. The secret message was then created with an overall smaller size but still had the same pixel size. This allowed for the secret message to blend in and become completely undetectable. Unless someone knows of the secret message, there is no possible way to look at the QR code and see any modifications. If and only if the key is aligned correctly, the general message easily becomes disabled allowing only the secret message to be retrieved when scanned. The code cannot be interpreted if the key is one pixel off because of sensitive alignment. To further show the capacity of this communication method,

Table – 1

Size of general message	*Generated QR image (200×200)*	*Secret image (200×200)*	*Stego image (200×200)*
100 bytes			
200 bytes			

500 bytes			
750 bytes			
1000 bytes			

(a) (b) (c)

Fig. 5: a) secret image b) Generated QR code image c) Stego image

V. 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. A general message encrypted in a QR code can be read easily by any QR code scanner. But since the proposed method incorporates steganography, so the secret image is hidden by using the generated QR code and the intruder can read only the information in the QR code and intruder didn't know the existence of the secret message, it enhances the confidentiality and security. In this paper Differential Phase Shift Keying was combined with Orthogonal Frequency Division Multiplexing in order to modulate data stream into visual two dimensional barcodes, the addition of a differential phase modulator before OFDM to modulate the data stream into phase differences of adjacent elements (DPSK-OFDM) causes the motion effect to increasingly weaken because of its gradual change from element to element, contributing to a small deviation from the ideal phase in the received signal.

REFERENCES

[1] T. Morkel , J.H.P. Eloffand M.S. Olivier, "An Overview Of Image Steganography", June/July 2005
[2] Ching-yin Law & Simon "QR codes in Education "jan 2010
[3] Amin Motahari,and MalekAdjouadi"Barcode Modulation Method For Data Transmission In Mobile Devices", JAN 2015
[4] M. Mary Shanthi Rani, K.RosemaryEuphrasia, "Data Security ThroughQrCodeencryption And Steganography", March 2016
[5] SinemColeri, Mustafa Ergen, Anuj Puri, "Channel Estimation Techniques Based On Pilot Arrangement InOfdm Systems,"
[6] Shweta Sharma,"Qr Code Steganography For Multiple Image And Text Hiding Using Improved Rsa-3dwt Algorithm",2016
[7] R. V. Nee and R. Prasad,Norwood"OFDM for Wireless Multimedia Communications",., 2000.
[8] S. Coleri, M. Ergen, A. Puri, and A. Bahai "Channel estimation technique based on pilot arrangement in OFDM systems,",2002.
[9] M. Morelli and U. Mengali "A comparison of pilot-aided channel estimation methods for OFDM systems, Dec. 2001