International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

QR Code Based Data Transmission in Mobile Devices Using AES Encryption

Ajini Asok[1], Arun G.[2]

[1]PG Scholar, Communication Engineering, Dept. of Electronics and Communication,
Sree Buddha College of Engineering for Women , Ayathil, Elavumthitta, Kerala

[2]Assistant Professor, Dept. of Electronics and Communication,
Sree Buddha College of Engineering for Women , Ayathil, Elavumthitta, Kerala

Abstract: ***QR codes have played a significant role in mobile applications due to their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. Any information on a cell phone can be transmitted to a second cell phone as QR code displayed on the LCD which is then captured using camera of second phone and can be decoded there. But motion-blur distortions can be introduced in captured image due to relative movements during capture. This can be solved by using orthogonal frequency division multiplexing (OFDM) modulation along with differential phase shift keying (DPSK). In this technique, large number of closely spaced orthogonal sub-carriers carries data on several parallel data streams (channels). The sub-carriers can be modulated with any of the conventional modulation techniques whereas here DPSK modulation is used. In order to make the sub-carriers orthogonal, Inverse Fast Fourier Transform (IFFT) is applied. This modulated message is encoded into QR code is displayed. The original message can be obtained by applying Fast Fourier Transform (FFT) on QR code captured by receiver, followed by demodulation. Since data is stored in phase difference, adjacent elements are less affected by the motion blur distortions. However, the private data of the QR barcode lacks adequate security protection. Due to the visual nature, 2D barcodes are subject to eavesdropping when they are displayed on the Smartphone screens. In order to add security to this data transmission, AES 128 encryption is used.***

Keywords: QR code, data transfer, encryption, subcarriers, differential phase shift keying.

1. Introduction

Barcode is a simple and cost-effective method for storing machine readable digital data on paper or product packages. Invention of quick response (QR) codes or Two-dimensional (2D) barcodes opened a new front for these cost-effective codes. A 2D barcode is a graphical image that stores information both horizontally (as one-dimensional bar codes do) and vertically. Compared with a one-dimensional (1-D) barcode, the QR code can store a larger data payload and possesses the capability of correcting errors [1]. QR codes have been increasingly used for security-sensitive applications including payments and personal identification. The barcode data easily can be decoded and retrieved via an automatic barcode system.

Transferring a data through near field communication (NFC), like Bluetooth, is subjected to many attacks like man in the middle attack. But, the line of sight visual channel reduces the interference from other applications, and hence can be used in short range communication systems like transferring of data from a cell phone, computer, tablet, or other devices. Data can be encoded into any 2D barcode format and it can be transferred from one phone to another through visual light channel (image capturing). A comparison of different 2D barcode formats that are used in mobile phone applications can be found in [2]. This idea was earlier implemented in [3], where data is transferred through a series of QR code. But the bit rate achieved is less than 10 kbps. Later in [4], data is transmitted between a computer monitor and digital camera. Here a bit rate of 14 Mbps is achieved. Many ideas have been implemented for this type of LCD-camera based communication systems [5]- [8]. The LCD-camera relative movements at the time of image capturing may introduce motion blur distortions. This type of distortions severely affects the performance of Quadrature Phase Shift Keying (QPSK) - Orthogonal Frequency Division Multiplexing (OFDM) modulation. To avoid this, DPSK-OFDM modulation is used [9]. Here data is stored in phase difference of adjacent frequency components. Thus any phase distortions due to motion blur, will affect the adjacent frequency components negligibly.

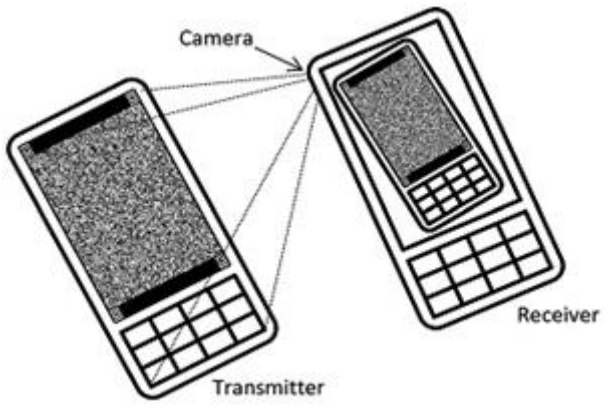

Figure 1: Illustration of data transfer between two phones using QR code.

Generally data is transferred in mobile phones through Bluetooth. But here, a new technique is introduced, in which

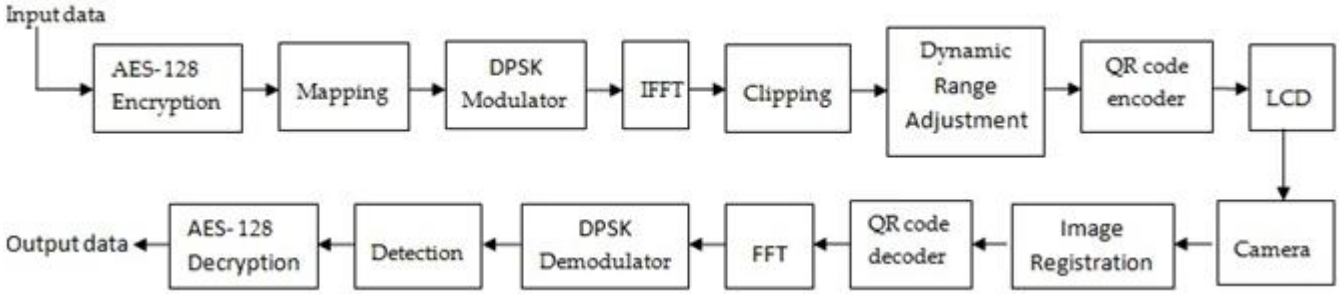

Figure 2: Block diagram of QR code based data transmission in mobile devices using AES encryption

data is converted into QR code and then is transferred to another phone by capturing the image of the QR code as shown in Figure 1. In order to provide additional security for this data transfer AES-128 encryption is used. The basic block diagram for this data transfer is as shown in Figure 2.

The AES algorithm was designed to have resistance against all known attacks, speed and code compactness on a wide range of platforms and design simplicity. AES has three variable key lengths but block length is fixed to 128 bits. The three key sizes of AES are 128, 192 and 256 bits. AES with 128-bit keys has stronger resistance to an exhaustive key search than DES and is designed to be efficient both in hardware and software across a variety of platforms.

2. AES-128 Algorithm

The AES-128 algorithm consists of ten rounds of encryption, as can be seen in Figure 3. First the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. Each round includes a transformation using the corresponding cipher key to ensure the security of the encryption. After an initial round, during which the first round key is XOR ed to the plain text (Add round key operation), nine equally structured rounds follow. Each round consists of the following operations.

- Substitute bytes
- Shift rows
- Mix columns
- Add round key

The tenth round is similar to rounds one to nine, but the Mix columns step is omitted. These four operations are explained in the following sections.

0.1 Substitute Bytes (Sub-bytes Operation)

AES contains 128 bit data block, which means each of the data blocks has 16 bytes. The Sub-bytes operation is a nonlinear substitution. This is a major reason for the security of the AES. In sub-bytes operation, each byte (8-bit) of a data block is transformed into another block using an 8-bit substitution box which is known as Rijndael S box.

0.2 Shift rows (Shiftrows Operation)

It is a simple byte transposition, the bytes in last three rows of the state, depending upon the row location, is cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.

0.3 Mix Columns (Mixcolumns Operation)

The Mixcolumns operation processes columns. A fixed matrix is multiplied to each column vector. In principle, only a matrix multiplication needs to be executed. In AES, Galois field operations are used. In a Galois field, an addition corresponds to an XOR and a multiplication to a more complex equivalent.

3. Add Round Key (Addroundkey Operation)

This operation is simple bitwise XOR between the corresponding bytes of the input data and the 128 bit expanded key.

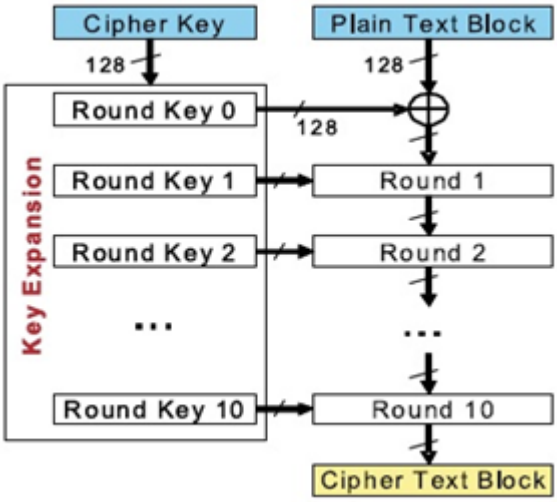

Figure 3: AES-128 algorithm

4. Transmitter

Encryption and modulation is done in the transmitter section. The AES encrypted message is first binarised and is mapped into 2 bits per symbol. It is then modulated using DPSK and made orthogonal by taking IFFT. To reduce PAPR, soft clipping is done. For the efficient utilization of transmission power, the pixel levels in the PAPR adjusted image need to be transformed into LCD dynamic range levels. After that QR coding is done and the image is displayed on LCD. For that, the modulated signal should be real-valued. For that the input to the IFFT algorithm should satisfy Hermitian symmetry. That is,

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

Where $0 \leq m < M$ and $0 \leq n < N$ and * denotes the complex

conjugate operator. Fig. 4 shows the elements relationship in order to have a real-valued IFFT for T matrix. 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. Also, the symmetry requirements for elements that have been deliberately set to zero would be automatically satisfied.

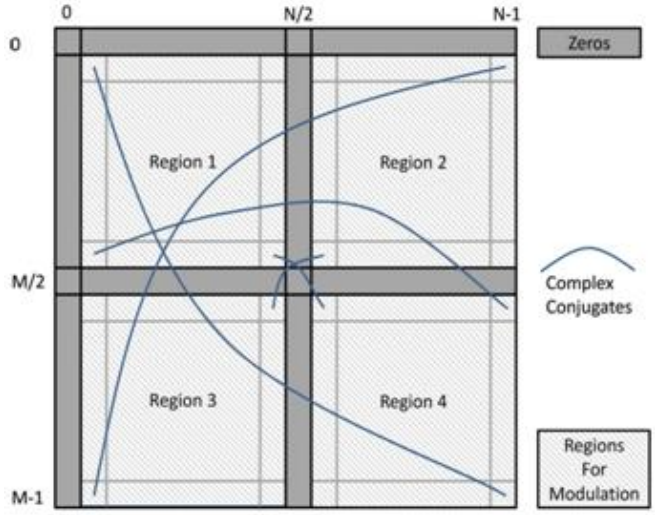

Figure 4: Hermitian symmetric matrix used for DPSK-OFDM modulation.

After encrypting the required data using AES algorithm, the transmitter section consists of constellation mapping, DPSK, IFFT, PAPR adjustment, amplitude adjustment, adding cyclic prefix and QR coding.

4.1 Constellation Mapping

The constellation mapping used in here is 4QAM. The input data is mapped into 2-bits per symbol. Each of the symbols is converted to a complex phase using the following rules:

$$11 \rightarrow e^{j\pi/4},\ 01 \rightarrow e^{j3\pi/4},\ 00 \rightarrow e^{j5\pi/4},\ 10 \rightarrow e^{j7\pi/4}$$

For each data symbol, the first bit modulates the real component and the second bit modulates the imaginary component of the phase. These symbols are then placed in an $\frac{M-2}{2}$ x $\frac{N-2}{1}$ matrix **S.** These symbols contain the absolute phase elements which are then modulated using differential phase shift keying (DPSK).

4.2 Differential Phase Shift Keying

After performing constellation mapping, the matrix **S** is converted into a differential matrix ***P*** using the following method:

- $\boldsymbol{P}(0, 0) = \boldsymbol{S}(0, 0)$;
- $\boldsymbol{P}(0, n) = \boldsymbol{P}(0, n\text{-}1) \times \boldsymbol{S}(0, n) \quad 1 \leq n < N\text{-}2$
- $\boldsymbol{P}(m, n) = \boldsymbol{P}(m\text{-}1, n) \times \boldsymbol{S}(m, n)\ 1 \leq m < \frac{M}{2} - 1$ $0 \leq n < N\text{-}2$

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

- $\boldsymbol{P}^1(m, n) = \boldsymbol{P}(m, n)$
- $\boldsymbol{P}^2(m, n) = \boldsymbol{P}\left(m, n + \frac{N-2}{2}\right)$

where $0 \leq m < \frac{M}{2} - 1$, $0 \leq n < \frac{N}{2} - 1$. Regions 1 and 2 of the matrix **T** are filled by these two matrices. Regions 3 and 4 of matrix **T** are obtained according to the Hermitian symmetry requirements. All the remaining strips on **T** are set to zero.

4.3 Inverse Fast Fourier Transform

Matrix **T** is the frequency domain representation of the signal. IFFT is applied on this signal to obtain time domain signal referred to as $\boldsymbol{P}_i$.

4.4 PAPR Adjustment

The resultant real-valued 2D having high peak to average power ratios (PAPR).The probability of having a high PAPR increases with the number of frequency components. There are several methods to limit the PAPR of OFDM signal. One of the most effective methods to limit the PAPR of OFDM signal is soft clipping of the signal. In this method a threshold level of A_{max} is set based on the signal average power level such that:

$$\text{Clipping Ratio} = \frac{A_{max}}{\sqrt{P_{avg}}}$$

Where $\sqrt{P_{avg}}$ is the average power per element in the OFDM signal before clipping. When the amplitude is greater than this threshold, it is clipped to the level A_{max} and the resulting matrix is referred to as $\boldsymbol{P_c}$

4.5 Amplitude Adjustment

For efficient utilization of transmission power, the pixel levels of PAPR adjusted image needs to be transferred into the dynamic range levels of LCD. The intensity level of LCD goes from 0 to I_{max}. So the $\boldsymbol{P}_c$ values are transformed linearly to this range and the resulting matrix is referred to as $\boldsymbol{P}_a$.i.e.

$$\boldsymbol{P}_a(\text{i, j}) = \frac{\boldsymbol{P}_c(\text{i,j}) - \text{Min}(\boldsymbol{P}_c)}{\text{Max}(\boldsymbol{P}_c) - \text{Min}(\boldsymbol{P}_c)}$$

4.6 Cyclic Prefix

Cyclic extension is required for OFDM systems to prevent inter carrier interference(ICI). Adding cyclic prefix means periodic extension of the last part of an OFDM symbol which is added to its front part at the transmitter, and at the receiver side it is removed before demodulation. For QR code, the periodic extension of the image generated by 2D-IFFT is required to prevent ICI.

4.7 QR Code Encoding

In this step the AES encrypted and modulated message is encoded to QR code. Finder patterns are added in the QR code for proper extraction of modulated data from the captured image.

5. QR Code Generation

The size of QR code varies from 21x21 pixels to 177x177 pixels. The 21x21 pixel size is version 1, 25x25 is version 2, and so on. The 177x177 size is version 40. QR codes include error correction codes, which help a QR reader to accurately read the code, even if part of it is unreadable. The lowest is L, which allows the code to be read even if 7% of it is unreadable. After that is M, which provides 15% error correction, then Q, which provides 25%, and finally H, which provides 30%.The capacity of a given QR code depends on the version and error correction level, as well as on the type of data that is encoded. A QR code can encode four types of data modes: numeric, alphanumeric, binary, or Kanji. [10]. General overview of QR code generation is as shown.

Step 1: Data analysis: Choose proper mode for encoding data. The QR code standard has four modes for encoding text: numeric, alphanumeric, byte and Kanji. Each mode encodes the text as a string of bits.

Step 2: Data encoding: Data is encoded in the desired mode. Each encoding mode is designed to create the shortest possible string of bits for the characters that are used in that mode.

Step 3: Error correction coding: Suitable error correction code words are selected. QR code uses Reed-Solomon error correction.

Step4: Structure final message: The data and error correction code words generated in the previous steps must now be arranged in the proper order. For large QR codes, the data and error correction code words are generated in blocks, and these blocks must be interleaved according to the QR code specification.

Step5: Module placement: After generating the data code words and error correction code words and arranging them in the correct order, place the bits in the QR code matrix Finder patterns are placed in this step.

Step 6: Data masking: Suitable data mask pattern is selected in order for the scanner to correctly read the code.

Step7: Format and version information: The final step is to add format and (if necessary) version information to the QR code by adding pixels in particular areas of the code that were left blank in previous steps. The format pixels identify the error correction level and mask pattern being used in this QR code. The version pixels encode the size of the QR matrix and are only used in larger QR codes.

6. Receiver

The camera of the receiver cell phone captured QR code image displayed on LCD and perform sampling and registering the acquired image so that a fairly acceptable copy of $\boldsymbol{P}_a$ is created at the receiver end. In order to obtain the transmitted data successfully, the following steps should be taken into consideration at the receiver end.

6.1 Image Capture

To ensure capture of at least one acceptable fragment, the sampling rate should be at least twice the display rate. Moreover the relative distance and angle between camera and display is bounded by the Nyquist criteria where each pixel on the display frame should map into a minimum of 2x2 block in the camera.

6.2 Image Registration

In this step using finder patterns, extract the captured image from background. General finder patterns used with QR codes is the 1, 1, 3, 1, 1 pattern.

6.3 QR Code Decoding

The AES encrypted modulated QR code image is decoded to obtain the encrypted modulated message.

6.4 Removal of Cyclic Prefix

The bits that were added in the transmitter side as the cyclic prefix are removed.

6.5 FFT

Fast Fourier Transform is applied on the registered image results in frequency domain data which is comprised of the differential phase modulated elements stored in $\mathbf{R_f}$ matrix**.**

6.6 DPSK Demodulation

By using phase differences between respective elements, the original constellation mapped data can be extracted. The first data corresponding to regions 1 and 2 should be concatenated together to form matrix R corresponding the transmitted matrix **T**.

- $R_d(0, 0) = R(0, 0)$
- $R_d(0, 0) = R(0, n)\ X\ R^*(0, n-1)$
- $R_d(m, n) = R(m, n)\ X\ R^*(m-1, n)$

6.7 Detection

Each input bit is calculated using the constellation map of the transmitter. Now these input bits are decrypted to obtain the data. Thus the QR code is captured without much motion blur and the message is retrieved.

7. Simulation Results

The proposed technique has been evaluated in MATLAB R2013a. The AES encrypted modulated QR code so obtained was transferred from one phone to another. The captured image was successfully decoded and decrypted to obtain actual data. Fig. 5 shows encrypted and modulated QR code. This QR code is displayed on phone and is transmitted to another phone by capturing the image. Fig. 6 shows data transfer by capturing QR code. Fig. 7 shows the captured QR code. The original data is retrieved by decoding and decrypting this captured QR code.

Figure 5: AES encrypted modulated QR code.

Figure 6: QR code image captured by the camera of the receiver cell phone

Figure 7: Captured QR code

8. Conclusion

Data can be securely transferred between LCD and smart phone as QR codes by first encrypting the information using AES algorithm and then modulated using DPSK-OFDM. The encrypted modulated QR code thus generated displayed on LCD, is captured by the camera of the receiver cell phone. This data transfer uses visual light communication and thus can reduce the possibilities of NFC attacks. Addition of differential phase shift keying avoids motion distortion, since data is stored in phase differences of adjacent elements. Also image blur and light leakage have limited effect on OFDM modulation. AES-128 bit key has stronger resistance to an exhaustive key search than DES. That can be easily implemented in both software and hardware.The data transfer rate can be increased by increasing the bits per symbol from current 2 bits per symbol constellation.

References

[1] H. Kato and K. Tan, "Pervasive 2d barcodes for camera phone applications," Pervasive Comput., vol. 6, no. 4, pp. 76-85, Oct. 2007.
[2] Information Technology-Automatic Identification and Data Capture Techniques-QR Code 2005 Bar Code Symbology Specification, ISO/IEC 18004:2006, 2006.
[3] X. Liu, D. Doermann, and H. Li, "Vcode-pervasive data transfer using video barcode," IEEE Trans. Multimedia., vol. 10, no. 3, pp. 361-371, Apr. 2008.
[4] S. D. Perli, N. Ahmed, and D. Katabi, "Pixnet: Interference- free wireless links using LCD-Camera pairs," in Proc. MobiCom., pp. 137-148, 2010.
[5] M. Allah, "Strengths and weaknesses of near field communication (NFC) technology," GJCST, vol. 11, no. 3, 2011.
[6] M. Mondal and J. Armstrong, "The effect of defocus blur on a spatial OFDM optical wireless communication system," in Proc. 14th Int.Conf. Transparent Opt. Netw, pp. 1-4, Jul. 2012.
[7] S. Kuzdeba, A. M. Wyglinski, and B. Hombs, "Space shift keying modulation for MIMO channels," in Proc.2010 IEEE Globecom Workshops, pp. 184-189, Apr. 2013.
[8] S. Dimitrov, S. Sinanovic, and H. Haas "Clipping noise in OFDM-based optical wireless communication systems," IEEE Trans.Commun., vol.60, no. 4, pp.1072-1081, Apr. 2012.
[9] Amin Motahari and MalekAdjouadi,"Barcode modulation method for data transmission in mobile devices," IEEE Trans. on Multimedia, vol. 17, no. 1, Jan. 2015.
[10] Someshwar Vaidya and Mahesh Sanap,"AES Algorithm using 512 Bit Key Implementation modulation method for data transmission in mobile devices," IEEE Trans. on Multimedia, vol. 17, no. 1, Jan. 2015
[11] Bingsheng Zhang and Kui Ren,"SBVLC: Secure Barcode-Based Visible Light for Smartphones," IEEE Trans.Mobile Comput., vol.15,no. 2,pp.432-446, Feb. 2016.
[12] "Zxing(open source qr library)," 2012, http://code.google.com/p/zxing

Author Profile

Ajini Asok received the B.Tech degree in Electronics and Engineering from University of Kerala in 2012. She is currently pursuing second year M.Tech in Communication Engineering at Sree Buddha College of Engineering for Women.

Arun G. received the B.Tech degree in Electronics and Communication Engineering from University of Kerala in 2011 followed by M.Tech. in Electro Optical Engineering from Anna University in 2014. He is currently working as Assistant Professor in Electronics and Communication Engineering Department, Sree Buddha College of Engineering for Women.