International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Secure Data Transmission using Barcodes in Mobile Devices

Anusree Jayadhar[1], Sajin Salim[2]

[1] *PG Scholar: Dept. of Electronics and Communication.*
TKM Institute of Technology,
Musaliar Hills, Karuvelil P. O., Ezhukone,
Kollam-691505, Kerala, India
[2] *Assistant Professor:Dept. of Electronics and Communication.*
TKM Institute of Technology,
Musaliar Hills, Karuvelil P. O., Ezhukone,
Kollam-691505, Kerala, India

Abstract -*2D barcodes have enjoyed a significant role in mobile applications like online payment, aadhar cards, etc. Almost every camera enabled smartphones can scan barcodes. A barcode can be transferred from one mobile to another by capturing images. But the relative movements during capture can induce motion-blur distortions in the captured image. This problem can be solved by using orthogonal frequency division multiplexing (OFDM) modulation along with differential phase shift keying (DPSK). In this technique, a large number of closely spaced orthogonal sub-carriers carry the data on several parallel data streams or channels. The sub-carriers are modulated with any of the conventional modulation technique. Here DPSK modulation is used to modulate the sub-carriers. The modulation is performed in the message which is encoded as the barcode. Inverse fast Fourier transform (IFFT) is applied to make the N sub-carriers into orthogonal. This modulated message is encoded into barcode and then it is transmitted. The camera acts as the receiver. The barcode is captured and then fast Fourier transform (FFT) is applied onto the decoded message. Then, original message is retrieved by performing demodulation. Since data is stored in phase difference, adjacent elements are less affected by the motion blur distortions. In order to add security to this data transmission, AES 128 encryption is used.*

Key Words: **barcodes; motion-blur distortion; sub-carriers; differential phase shift keying modulation (DPSK); orthogonal frequency division multiplexing modulation(OFDM), encryption.**

1.INTRODUCTION

Transferring a data through near field communication (NFC), say through bluetooth, is subjected to many attacks like man in the middle attack [1]. 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.

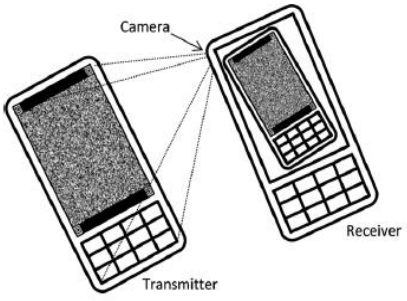

Fig-1: Illustration of data transfer between two phones using barcodes.[Image Courtesy: [9]]

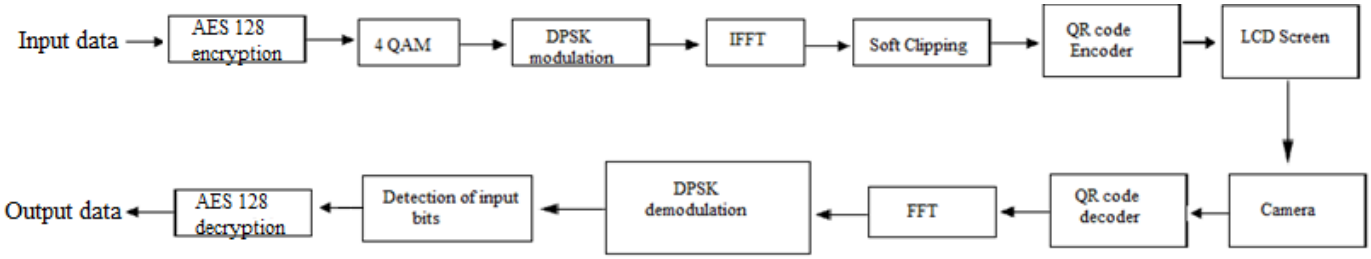

Fig-2: Basic block diagram for data transfer using QR codes from one phone to another

2. METHODOLOGY

Generally data is transferred in mobile phones through bluetooth. But here, a new technique is introduced, in which data is converted into QR code and then is transferred to another phone by capturing the image of the QR code as shown in Fig. 1. The basic block diagram for this data transfer is as shown in Fig.2.

2.1 AES 128 Encryption Standard

AES 128 encryption is used to securely transfer data from one phone to another. AES stands for Advanced Encryption Standard and is used for encrypting a data using a cypher. It is a symmetric block cypher and it uses a key of 128 bits. This 4 word (128 bit) key is expanded to 44 words key. There are 10 rounds of operations, which include substitution, shift rows, mix columns and add round key. These four steps are executed in different order for encryption and decryption. The following are the steps involved in AES.

1. Different round keys are generated from cipher key.
2. Initialize the state array with block data to be encrypted.
3. Start with initial state array by adding round key.
4. Perform the round operations nine times.
5. The tenth round does not include mix column operation, and after the tenth round the final output is obtained as cipher text.

By following the above process the final encrypted text or cipher text is obtained. The decryption process also includes 10 rounds. The inverse of all the above operations are performed for decryption.

2.2 Transmitter

The modulation is done in the transmitter side. The encrypted message is binarised and is mapped into 2 bits per symbol and is modulated using DPSK modulation. Then it is made orthogonal by taking IFFT. To reduce PAPR, soft clipping is done. Dynamic range adjustment is done in order to transform the PAPR adjusted image pixels into the dynamic range levels of LCD, for efficient utilization of transmission power. The modulated QR code is captured using the mobile phone camera. In the receiver part, FFT is taken and DPSK demodulation is performed. The original constellation mapping is detected and the message is retrieved after decryption. The transmission of modulated QR code is as shown in Figure 2.

Mapping: The constellation mapping used is that of 4QAM. The input data stream is mapped to 2 bits per symbol. The mapping rule is as follows.

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

The real component is modulated by the first bit and the imaginary component is modulated by second bit. These are then placed in a matrix S. These symbols contain the absolute phase elements and are then modulated using DPSK.

Differential matrix: Matrix S is converted into a differential matrix D using the following method:

- $D(0,0) = S(0,0)$;
- $D(0,n) = D(0,n-1) \times S(0,n)$;
- $D(m,n) = D(m-1,n) \times S(m,n)$;

IFFT: An OFDM signal contains N subcarriers. These N subcarriers are then fed to IFFT. If x0, x1, x2 ... are N symbols, then output of the IFFT is

$$X(t) = \frac{1}{\sqrt{N}} \Sigma_{k=0}^{N-1} x_k e^{j\pi 2tk/N}$$

where t = 0, 1, 2 ...N – 1. The IFFT maps the input signal into a set of orthogonal subcarriers. Similarly, at the receiver, FFT performs the reverse mapping of IFFT and the source signal is estimated from the subcarriers.

Soft clipping: The outputs of the IFFT have high PAPR (peak to average power ratio). The probability of having a high PAPR increases with the number of frequency components. Several methods are used to limit the PAPR of OFDM signals, and the most widely used method is soft clipping. Here a threshold level of A_{max} is set. When the amplitude crosses

this threshold, it is clipped to A_{max}. The matrix thus created is Dc.

Amplitude Adjustment: For efficient utilization of transmission power, the PAPR adjusted image pixels are transferred into the dynamic range levels of LCD. Usually, the LCD intensity levels goes from 0 to $I_{\max}$. Let the linearly transformed values of Dc be Da. It can be found using the equation

$$D_a(i,j) = \frac{D_c(i,j) - Min(D_c)}{Max(D_c) - Min(D_c)} I_{max}$$

Adding cyclic prefix: It is a periodic extension of the last part of an OFDM symbol which is added to its front part at the transmitter, and is removed before demodulation at the receiver.
QR code Encoder: The encrypted modulated message is encoded into QR code.
This encrypted modulated QR code is then captured using the camera of a mobile phone and then demodulation and decryption is performed to retrieve the message.

2.3 QR Code Generation

The QR code varies in size from 21x21 pixels to the largest size 177x177. These sizes are called versions. The version 1 is of 21x21 pixel size, version 2 is of 25x25 pixel size, and so on. The largest version is 40, which is of size 177x177. A QR code includes error correction codes. These help a QR reader, to accurately read the code, even if part of it is unreadable. This is done by creating some redundant data that is generated when a QR code is encoded. Error corrections are of four levels. The lowest is L, which allows the code to be read even if 7 percentage of it is unreadable. After that is M, which gives 15 percentage error correction, then Q, which provides 25 percentage, and finally H, which gives 30 percentage. The capacity of a given QR code depends on three factors: the version, error correction level and the type of data that is encoded. A QR code can encode four types of data modes: numeric, alphanumeric, binary, or Kanji. [10]. The algorithm for QR code is as shown.

Step 1: Data analysis: Choose proper mode for encoding data.
Step 2: Data encoding: Data is encoded in the desired mode.
Step 3: Error correction coding: Suitable error correction code words are selected.
Step4: Structure final message: Both data and error correction code words are arranged into final message.
Step5: Module placement: These message bits are arranged in the form of a matrix.
Step 6: Data masking: Suitable data mask pattern is selected.
Step7: Add format and version string
Step8: Add quiet zone.

2.4 Receiver

In the receiver, this QR code is demodulated and decrypted to obtain the actual message. The cyclic prefix is removed before demodulation and FFT is taken. Using the constellation mapping used at the transmitter, the original data bits are retrieved.

Image capturing: The encrypted modulated QR code which is displayed on the LCD of the first phone is captured using the camera of another phone. This QR code can be detected with the help of finder patterns.

QR code decoder: The encrypted modulated QR code is decoded to obtain the encrypted modulated message. Demodulation and decryption is performed in this message.

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

FFT: On taking the FFT, time domain signal is converted to frequency domain signal. The frequency domain data comprises of the differential phase modulated elements. Let this matrix be R.

DPSK demodulation: From the matrix R, the phase difference is extracted as follows.

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

Calculate the input bit: 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.

3. EXPERIMENTAL RESULTS

The proposed technique has been evaluated in MATLAB R2015b. 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. Fig. 3. shows the encrypted modulated QR code. This QR code is displayed on the phone and is transmitted to another phone by capturing the image. Fig. 4.shows the data transfer by capturing the QR code. Fig. 5. shows the captured QR code. On decoding and decrypting this captured QR code, the original data is retrieved.

Fig-3: Encrypted Modulated QR code

Fig- 4: Data transfer using QR code

Fig-5: Captured QR code

4. CONCLUSION AND FUTURE WORK

A data can be securely transferred from one mobile device to another by first encrypting it and then converting the data into barcodes. This is then transferred to another device by capturing the image of the barcode. This data transfer uses visual light communication, thus reducing the possibilities of NFC attacks. In order to avoid motion blur distortions, the data is stored in phase difference of adjacent elements. The data transfer rate can be increased by increasing the bits per symbol from current 2 bits per symbol constellation.

REFERENCES

[1] M. Allah, "Strengths and weaknesses of near field communication (nfc) technology," GJCST, vol. 11, no. 3, 2011.

[2] H. Kato and K. Tan, "Pervasive 2d barcodes for camera phone applications,"*Pervasive Comput.*, vol. 6, no. 4, pp. 76–85, Oct. 2007.

[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*, 2010, pp. 137–148.

[5] J. Memeti, F. Santos, M. Waldburger, and B. Stiller, "Data transfer using a camera and a three-dimensional code," *Praxis der Informationsverarbeitungund Kommunikation*, vol. 36, no. 1, pp. 31–37, 2013.

[6] M.Mondal and J. Armstrong, "Impact of linear misalignment on a spatial OFDM based pixelated system," in *Proc. 18th Asia-Pacific Conf. Commun.*, Oct. 2012, pp. 617–622.

[7] 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.*, Jul. 2012, pp. 1–4.

[8] M. R.H.Mondal and J.Armstrong, "Analysis of the effect of Vignetting on mimo optical wireless systems using spatial OFDM," *J. Lightw. Technol.*, vol. 32, no. 5, pp. 922–929, Mar. 1, 2014.

[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] "Zxing(open source qr library)," 2012, http://code.google.com/p/zxing.

BIOGRAPHIES

Anusree Jayadhar received her B.Tech degree in Electrical and Electronics Engineering from University of Kerala in 2011. She is currently pursuing second year M.Tech in Signal Processing at TKM Institute of Technology.

Sajin Salim received his B.Tech degree in Electronics and Communication Engineering from University of Kerala in 2007 followed by M.E. in Communication Systems from Anna University in 2012. He is currently working as Assistant Professor in Electronics and Communication Engg. Department, TKM Institute of Technology.