Increased Throughput SBVLC system using Color Barcodes

Fathima Beevi P. M.[1], Nitha S[2]

[1]M .Tech student, Department of Communication Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Kerala, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Kerala, India

Abstract: ***Color barcodes are used to increase the system throughput of the SBVLC system.2D barcodes have an advantage of significant penetration rate in mobile applications. This is largely due to the extremely low barrier to adoption – almost every camera-enabled smartphone can scan 2D barcodes. As an alternative to NFC technology, 2D barcodes have been increasingly used for security-sensitive mobile applications including mobile payments and personal identification. However, the security of barcode-based communication in mobile applications has not been systematically studied. Due to the visual nature, 2D barcodes are subject to eavesdropping when they are displayed on the smartphone screens. On the other hand, the fundamental design principles of 2D barcodes make it difficult to add security features. SBVLC is a secure system for barcode-based visible light communication (VLC) between smartphones. Three secure data exchange schemes that used to encode information in barcode streams. These schemes are useful in many security-sensitive mobile applications including private information sharing, secure device pairing. Here the system throughput can be increased using color barcodes streaming. In terms of barcode design, by taking advantage of more colors, some new color barcodes are proposed to increase the capacity.***

Keywords: Short-range smartphone communication, key exchange, secure VLC, color barcode streaming, color barcode.

1. Introduction

Barcode is one of the existing system which is very fast in scanning and more accurate when compared to other coding systems.. Barcode enables tracking in an efficient manner. The speed of scanning the barcode system is very high when compared to manual data entry method. 2D barcode is developed from 1D barcode and the information that are encoded will be stored in vertical direction as well as in horizontal direction. The advantages of 2D barcodes includes: less area, high embedding capacity, higher density, higher error error detection level. The advanced level of barcode is the stacked barcode which are stacked one upon another. These barcodes are printed in a rectangular shape which can able to achieve area.

Near Field Communication (NFC) is subject to security vulnerabilities such as eavesdropping and jamming. 2D barcodes have been increasingly used for security-sensitive applications including payments and personal identification. QR Code (Quick Response Code) There four levels of error correction, and the maximum symbol size can encoding 7089 numeric data or 4296 alphanumeric data correction level is upto 30% of code words of the symbol. The advanced features of QR code are:

1) High embedding Capacity.
2) High speed scanning.
3) Represented by two bits of data.
4) It can readable from any direction from 360degree.

Based on our security analysis, we develop three secure data exchange protocols that encode information in barcode streams. Such protocols are useful in many mobile applications including private information sharing, secure device pairing, and contactless mobile payment, etc. Three secure communication schemes are:

1) *Two-phase message transfer scheme*: It is designed for smartphones to opportunistically exchange data such as contacts and photos.
2) *Smartphone handshake scheme*. It is developed for the standard key-exchange-then-encryption paradigm. The scheme serves as an alternative key exchange protocol to the conventional DH key exchange protocol.
3) *All-or-nothing data streaming scheme*. It is tailored forsecure temporary data transfer without the key exchange phase.

2. Proposed System

Color printing uses cyan, yellow. magenta for color reproduction in printing. Color capture devices uses Red, green, blue sensing channels. These are complementary to cyan , yellow , magenta colors. Recently the study of color barcodes provides the information for increase in embedding capacity than monochrome barcodes. All the data are initially extracted from red, green , blue channels. The CMY colorant channel are also extracted from RGB model parameters. The combination of all these colors provides thecolor code with high embedding capacity. The proposed system for Color QR code generation is shown in Figure 1.

http://dx.doi.org/10.21275/v5i6.NOV164759

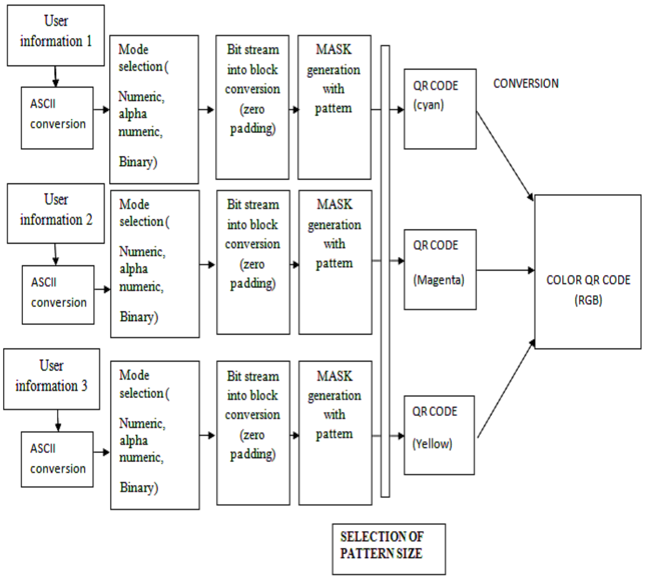

User information 1
ASCII conversion
Mode selection(Numeric, alpha numeric, Binary)
Bit stream into block conversion (zero padding)
MASK generation with pattern
QR CODE (cyan)
CONVERSION
User information 2
ASCII conversion
Mode selection(Numeric, alpha numeric, Binary)
Bit stream into block conversion (zero padding)
MASK generation with pattern
QR CODE (Magenta)
COLOR QR CODE (RGB)
User information 3
ASCII conversion
Mode selection(Numeric, alpha numeric, Binary)
Bit stream into block conversion (zero padding)
MASK generation with pattern
QR CODE (Yellow)
SELECTION OF PATTERN SIZE

Figure 1: Proposed system for color QR code generation

Consider the input as an alpha numeric value. Initially the data is given as an input. The information encoded by a QR code may be made up of four standardized types "modes" of data such as numeric, alphanumeric, byte / binary or through some automatic extensions, virtually is can be any type of data.

All these datas are collected and converted into ASCII values. Then the data is divided into groups of two elements. Each ASCII value is added with next data's ASCII values. All the data's values are added accordingly and grouped into 11 bits. These bits of data are segmented into blocks.

Mask pattern generation is carried out using MATLAB such that the data is highly secured. All the above steps are repeated and entire bit is converted into square blocks. Each and every bit is allocated with the pixel values. Finally the colors such as cyan, yellow and magenta are assigned to all the bits and pixel values. By combining all the colors the final QR code is obtained in color.

3. Secure Communication Schemes

3.1 Two-phase message transfer scheme.

It is designed for smartphones to opportunistically exchange data such as contacts and photos. It is ultra lightweight and without using any complex cryptographic building blocks. After building a high-throughput real-time VLC channel, we are ready to focus on the security aspects. In particular, we are going to show that the communication system can achieve much higher security level once it has a duplex VLC channel. Consider the following scenario: Bob wants to share dozens of his contacts with his friend Alice. VLC seems to be an adequate tool to accomplish this task, because it is extremely simple to setup. However, an eavesdropper can shoulder sniff all the information if he/she can 'see' Bob's smartphone screen. To overcome this security issue, we propose the first scheme of SBVLC: two-phase message transfer scheme is shown in the Figure 2. Color barcodes are used for shorter encoding/decoding time and higher storage capacity. It uses multiple colors for each information block, so it can encode more information than the a mono-color QR code does.

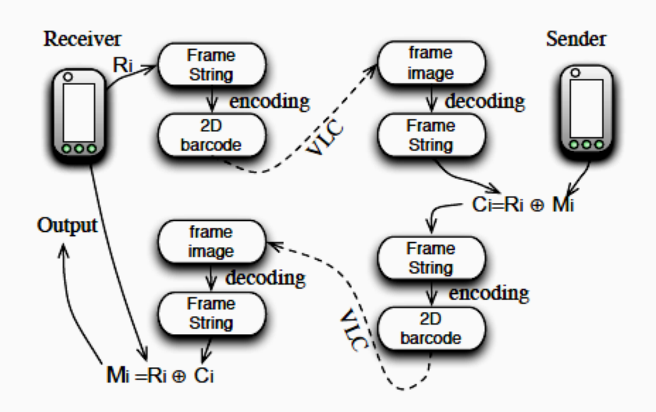


Figure 2: Two-phase message transfer scheme.

3.2 Smartphone handshake scheme

It is developed for the standard key-exchange-then-encryption paradigm. The scheme serves as an alternative key exchange protocol to the conventional DH key exchange protocol. The established key can be used later for many security applications.

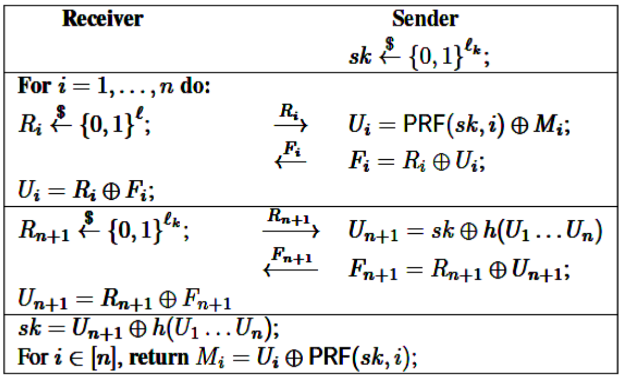
Alice		Bob
$A_0 \xleftarrow{\$} \{0,1\}^\ell;$	$\xrightarrow{A_0\|\|0^\ell}$	$B_0, K_0^b \xleftarrow{\$} \{0,1\}^\ell;$
	$\xleftarrow{C_0\|\|B_0}$	$C_0 = A_0 \oplus K_0^b;$
$K_0^b = A_0 \oplus C_0;$		
For $i = 1, \ldots, n$ **do:**		
$A_i, K_i^a \xleftarrow{\$} \{0,1\}^\ell;$		
$D_i = B_{i-1} \oplus K_i^a;$	$\xrightarrow{A_i\|\|D_i}$	$B_i, K_i^b \xleftarrow{\$} \{0,1\}^\ell;$
	$\xleftarrow{C_i\|\|B_i}$	$C_i = A_i \oplus K_i^b;$
$K_i^b = A_i \oplus C_i;$		$K_i^a = B_{i-1} \oplus D_i;$
$h \xleftarrow{\$} \mathcal{H};$	$\xrightarrow{h}$	
Return $sk = h(K_1^a, \ldots, K_n^a, K_0^b, \ldots, K_n^b);$		

Figure 3: Smartphone handshake scheme.

To preserve data confidentiality against such strong adversaries, we would like to use the standard key-exchange then- encrypt paradigm. Namely, the sender and the receiver first negotiate a common secret key, and then they use the secret key to encrypt the communication channel with some stream cipher, is shown in the Figure 3. Note that the common secret key can be used in many other applications as a substitution of the conventional public-key based key exchange protocol. We now present our key exchange protocol for smart phones, called smartphone handshake scheme that runs between two parties (smartphones) Alice and Bob, and they will establish a common secret key after the execution.

3.3 All-or-nothing data streaming scheme.

It is tailored for secure temporary data transfer without the key exchange phase. The scheme utilizes all-or-nothing transformation to enhance the channel security — it preserves the confidentiality of all the transmitted data, if the eavesdrop permisses at least one barcode frame during the entire communication. In some scenarios where the data string to be transferred is short, so it is not economical to setup a key first. However, one might still want to achieve higher security level. We need a scheme that allows the users to directly transmit the data without key exchange step while still offers high security guarantees. In this section, we propose the all-or-nothing data streaming scheme, is shown in the Figure 4 which is specifically tailored for secure temporary data transfer without key exchange phase.



Receiver		Sender
		$sk \xleftarrow{\$} \{0,1\}^{\ell_k}$;
For $i = 1, \ldots, n$ **do:**		
$R_i \xleftarrow{\$} \{0,1\}^{\ell}$;	$\xrightarrow{R_i}$	$U_i = \mathsf{PRF}(sk, i) \oplus M_i$;
	$\xleftarrow{F_i}$	$F_i = R_i \oplus U_i$;
$U_i = R_i \oplus F_i$;		
$R_{n+1} \xleftarrow{\$} \{0,1\}^{\ell_k}$;	$\xrightarrow{R_{n+1}}$	$U_{n+1} = sk \oplus h(U_1 \ldots U_n)$
	$\xleftarrow{F_{n+1}}$	$F_{n+1} = R_{n+1} \oplus U_{n+1}$;
$U_{n+1} = R_{n+1} \oplus F_{n+1}$		
$sk = U_{n+1} \oplus h(U_1 \ldots U_n)$;		
For $i \in [n]$, **return** $M_i = U_i \oplus \mathsf{PRF}(sk, i)$;		

Figure 4: All-or-nothing data streaming scheme.

The aim of this scheme is to amplify the security such that the confidentiality of the entire transmitted data is guaranteed if the eavesdropper fails to capture at least one data frame. To achieve this goal, the sender first picks a random key and encrypts its data. Then the sender splits the key into many key shares and gradually sends those key shares together with the encrypted data chunks frame by frame. If the adversary miss one frame, then he/she cannot recover the key; subsequently, he/she cannot decrypt the captured data.

4. Simulation Results

MatlabR2013a is used as the platform to perform this task. Developed three secure communication schemes. Here color barcodes are generated instead of QR codes.

4.1 Two-phase message transfer scheme

The word “HELLO” is given as the input. In this scheme, the sender will send the message and this message is converted to color code. This color code is transmitted to the receiver. The receiver receives the message in the form of color code. This scheme is very secure and prevents eavesdropping and jamming. The color code generated is shown in Figure 5.

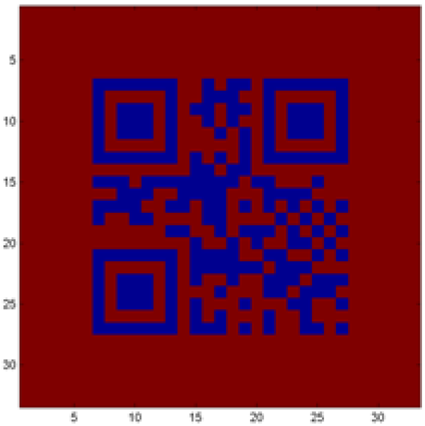


Figure 5: Color barcode generated of message ‘HELLO’.

4.2 Smartphone handshake scheme.

The sender and the receiver first negotiate a common secret key, and then they use the secret key to encrypt the communication channel with some stream cipher. Note that the common secret key can be used in many other applications as a substitution of the conventional public-key based key exchange protocol. After the common *sk* is established, Alice and Bob can use it to encrypt the one-way VLC channel. Alternatively, it can be used to pair two devices, e.g. Bluetooth. Here word “HELLO” is given as the input. The message can be send to the receiver by using a common secret key. If both of the sender and receiver have the common secret key then only the message will be transferred. The result is shown below.

The secret key of sender : 1101011101.

The secret key of receiver :1101011101.

Both of them have common secret key, then the message will be transferred to the receiver.

4.3 All-or-nothing data streaming scheme.

The aim of this scheme is to amplify the security such that the confidentiality of the entire transmitted datais guaranteed if the eavesdropper fails to capture at least one dataframe. To achieve this goal, the sender first picks a random keyand encrypts its data. Then the sender splits the key into many key shares and gradually sends those key shares together with the encrypted data chunks frame by frame. If the adversary miss one frame, then he/she cannot recover the key; subsequently, he/she cannot decrypt the captured data. The word “HELLO” is given as the input. Here color barcodes are generated. If anyone frame misses then the color barcode cannot be generated. In that case, receiver will not get the message from the sender. The color barcode generated is shown in Figure 6.

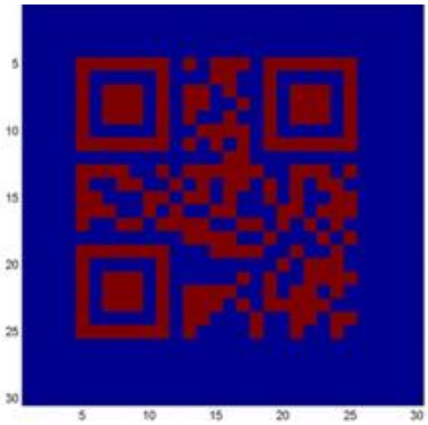


Figure 6: Color barcode generated of message 'HELLO'.

5. Conclusion

Color barcodes are used to increased the system throughput and provides high level security, prevents eavesdropping and jamming. It is also used for private information sharing, secure device pairing. In terms of barcode design, by taking advantage of more colors, some new color barcodes are proposed to increase the capacity for robust data transmission between smartphones. Developed three secure communication schemes.

6. Acknowledgment

I would like to express profound gratitude to our Head of the Department, Prof. Cherian Schariah, for his encouragement and for providing all facilities for my work. I express my highest regard and sincere thanks to my guide, Asst. Prof. Ms. Nitha S., who provided the necessary guidance and serious advice for my work.

References

[1] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: secure barcode-based visible light communication for smartphones," in IEEE Conference INFOCOM 2014, 2014, pp. 2661–2669.
[2] T. Hao, R. Zhou, and G. Xing, "Cobra: color barcode streaming for smartphone systems," in MobiSys, 2012.
[3] M. Allah, "Strengths and weaknesses of near field communication (nfc) technology,"GJCST, vol.11, no. 3, 2011.
[4] M. Querini, A. Grillo, A. LentiniAnd G.F. Italiano, "2D Color Barcodes For Mobile Phones", Vol. 8 No. 1, pp. 136 - 155, 2011.
[5] www.mathworks.in

Author Profile

FathimaBeevi P.M received the B-Tech degrees in Electronics and Communication Engineering from M.G University, Kerala at KMEA Engineering college, Edathala, Ernakulam in 2014. And now she is pursuing her M-Tech degree in Communication Engineering under the same university in Sree Buddha college of Engineering for women.

Nitha Sworking as Assistant Professor in department of Electronics and Communication, Sree Buddha college of Engineering for women, Elavumthitta, Pathanamthitta.