Camera Base Message Transfer using QR Code

[1]Meghana V Bandiwadekar, [2]Hemant A Tirmare
[1,2]Dept. of Technology, Shivaji University, Kolhapur, India

Abstract
2D barcode system has got a significant penetration rate in mobile applications. This is largely due to the extremely low barrier to adoption for most camera enabled Smartphone by scanning 2D barcode. An alternative to NFC technology 2D barcode have been increasingly used for security sensitive mobile payment and personal identification. Along with such security, file data can also be transferred using barcode system over a short range communication as alternative to radio frequency communication system. The proposed work here provides a novel approach for optical communication using barcode converted data on devices equipped with camera and displays.

Keywords
QR Code, Handshaking Scheme, Near Field Communication (NFC), Barcode

I. Introduction

The 2D colour barcode design that is particularly optimized for real time streaming between small size screens and low speed cameras of smart phones. Colour barcode encode information into specially designed 2D color barcode and use several new techniques to deal with the significant environment and achieves real time barcode stream decoding.

The short range communication techniques including near field communication and 2D barcode have enable many popular smart phone application such as contactless payment confidential data sharing and online payment.

Every camera enabled smart phone can read and process 2D barcode. The 2D barcode have been increasingly used for security sensitive application including online payment and data sharing.

The barcode streaming system run between a sender and receiver. At the beginning of a data transmission the sender divides the data string into sever data chunks single barcode can store before ECC encoding.

Quick Response (QR) codes are two dimensional barcodes that can be used to efficiently store small amount of data. They are increasingly used in all life fields, especially with the wide spread of smart phones which are used as QR code scanners. The purpose secure QR code application more security levels as well as maintains backward compatibility with QR code that do not incorporate security features.

Optical communication between two devices can be established by having display to camera utilization system by means of which two devices can be used for transferring files as far as, short distance communication is concerned.

Based on security analysis develop three secure data exchange protocol that encodes information in barcode stream . Three secure communication schems are:

A. Two Phase Message Transfer Scheme

It is designed for smartphones to opportunistically exchange data such as contracts and photos. It is ultra lightweight and without using any complex cryptographic building blocks.

B. 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.

C. 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 eavesdropper misses at least one barcode frame during the entire communication.

II. Literature Survey

G. Starnberger, L. Froihofer, and K. M. Goeschka [1] proposes an authentication technique called QR-TAN (Quick Response - Transaction Authentication Numbers). QR-TANs use a method based on transaction-signing that has been adapted to fit the capabilities of commonly used Web-based applications. QR-TANs are based on two-dimensional QR barcodes. QR-TANs authenticate transactions by using a trusted device. This device can be a mobile phone with a display and a camera with a modest resolution. QRTANs use QR codes for the transmission of information.

L. Francis, G. Hancke, K. Mayes, and K. Markantonakis [2] propose that the new risks imposed by mobile connectivity and untrusted mobile phone applications. The various APIs for secure element access on different mobile phone platforms and their access control mechanisms are analyzed. The security aspects of mobile phones are explained. Finally, two practical attack scenarios, a method to perform a denial of service (DoS) attack against a secure element and a method to remotely use the applications on a victims secure element without the victim's knowledge, are highlighted.

T. Hao, R. Zhou, and G. Xing [3] propose of a novel VLC communication system called COBRA for off-the-shelf smartphones. COBRA encodes information into specially designed 2D colorbarcodes and streams them between screen and camera of smartphones. They develop a new 2D color barcode that is optimized for streaming between small-size screen and low-speed camera of smartphones.

T. Langlotz and O. Bimber [4] propose that the barcode that they refer to as 4D barcode. It encodes data in four dimensions: width, height, color and time. Consequently, it cannot be printed on paper but is displayed on screens of mobile or spatial devices. Time-multiplexing colored 2D barcodes allows to transmit a larger amount of information robustly to of-the-shelf mobile phones without requiring an explicit synchronization.

N. Saxena, J. erik Ekberg, K. Kostiainen, and N. Asokan [5] propose that several improvements and extensions to the using a visual channel to implement secure pairing. They showed how strong mutual authentication can be achieved using just a unidirectional out-of-band (OOB) channel, which could also improve the usability of the pairing process.

J. McCune, A. Perrig, and M. Reiter, "Seeing-is-believing [6] propose that current mechanisms for authenticating communication between devices that share no prior context are inconvenient for ordinary users, without the assistance of a trusted authority. Present and analyse Seeing-Is-Believing (SiB), a system that utilises 2D barcodes and camera-phones to implement a visual channel for authentication and demonstrative identification of devices. Then they apply this visual channel to several problems in computer security, including authenticated key exchange between devices that share no prior context, establishment of the identity of a TCG-compliant computing platform, and secure device configuration in the context of a smart home.

Antonio Grillo, Alessandro Lentini, Marco Querini, and Giuseppe F Italiano [7] propose that High Capacity Colored QR codes, a new 2D code which aims at increasing the space available for data, while preserving similar robustness, error correction and without loosing compatibility with the original QR standard.

D. Parikh and G. Jancke [8] propose that A 2D color barcode can hold much more information than a binary barcode. Barcodes are often intended for consumer use where using a cellphone, a consumer can take an image of a barcode on a product, and retrieve relevant information about the product. The barcode must be read using computer vision techniques. While a color barcode can hold more information, it makes this vision task in consumer scenarios unusually challenging.The localization and segmentation of a 2D color barcode in such challenging scenarios, along with its evaluation on a diverse collection of images of Microsoft's recently launched High Capacity Color Barcode (HCCB).

Zhibo Yang, Zhiyi Cheng, Chen Change Loy, Wing Cheong Lau, Chak Man Li [9] propose that a layered framework for high capacity color QR codes, which supports robust and rapid decoding using off-the-shelf smartphones.HiQ enables users and developers to create generalized QR codes with flexible and broader range of choices of data capacity, error correction level and color, etc. Moreover, we have also collected a large-scale color QR code dataset, CUHK-CQRC, which will be made available to the community. Color brings extra data capacity for QR codes, but it also brings tremendous challenges to the decoding because of color interference and illumination variation, especially for high-density QR codes.

III. Proposed system

A. Security

To establish security along communicating devices through proposed method, we use key for encrypting the data. After dividing the whole data in N segments each segment is encrypted using key derived from checksum of the data and DES algorithm can be used to encrypt the data.The data checksum can be calculated for each segment obtained after dividing process. The private key is generated from check sum of the data and public key is used to encrypt this key, after which, its barcode is created to transfer the key. The received first barcode at the receiver side is firstly confirmed by displaying on the screen and receiving the ACK barcode. After this, private key is retrieved by the receiver node using public key and decryption. This private key is used further to retrieve the data by decryption from upcoming encrypted data barcodes.

B. Sender

1. Initialize screen and camera ACK and NACK barcode set.
2. Display start of communication. Barcode and wait for acknowledgment barcode screen by capturing from camera. If different barcode show consider this as negative acknowledgment.
3. When acknowledgment received start showing each barcode on the screen for each data segment.
4. Start sending data with respect to feedback in term of acknowledgment capture from camera.

C. Receiver

1. Initialize screen and camera ACK, NACK barcode sets.
2. Capture barcode and display the same as ACK on screen and extract data length from this.
3. Capture next barcode and compare with existing to check repetition.
4. If new barcode found repeat from step 3 until all data is received.

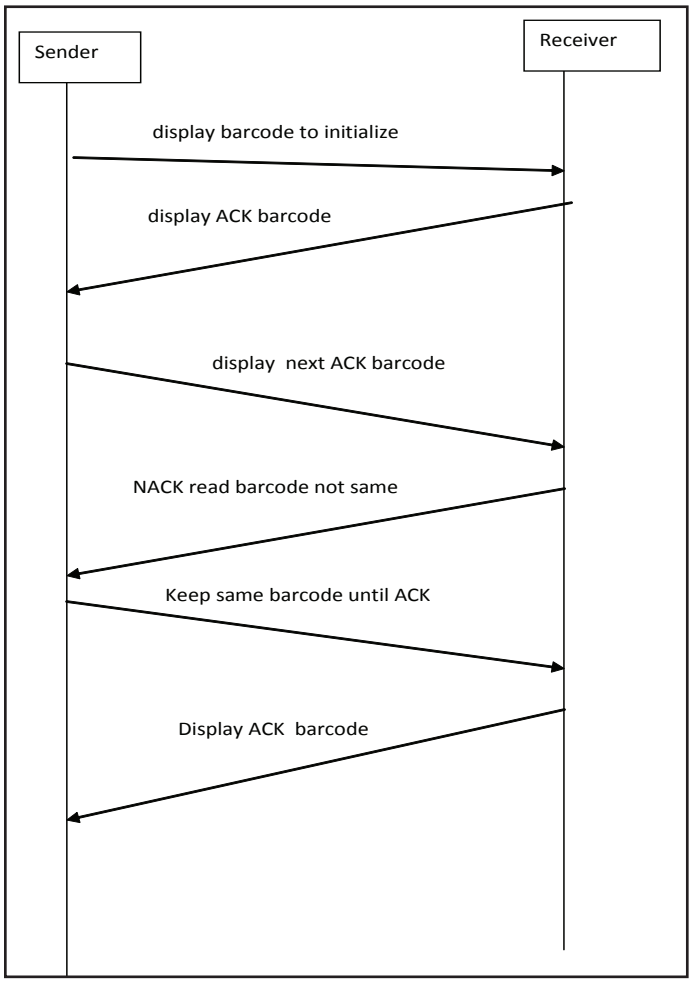

Fig. 1: Handshaking in Devices for Data Transfer

For the sake of synchronized communication for data transfer using proposed optical method handshaking can be established as indicated in fig. 1.

IV. Conclusion

QR barcode are used to increased the system throughput and provides high level security , prevents eavesdropping and jamming. QR barcode for secure private information during data sharing. We can securely share our information between two devices with the help of optical communication. Proposed method achieves high level security.

References

[1] G. Starnberger, L. Froihofer, K. M. Goeschka,"QR-TAN: Secure mobile transaction authentication," In Proc. Availability, Rel. Security, Mar. 2009, pp. 578–583.

[2] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, "Practical relay attack on contactless transactions by using NFC mobile phones," Cryptology ePrint Archive, Tech. Rep. 2011/618, 2011.

[3] T. Hao, R. Zhou, G. Xing,"Cobra: Color barcode streaming for smartphone systems," In Proc. 10th Annu. Int. Conf. Mobile Syst., Appl. Services, 2012, pp. 85–98.

[4] T. Langlotz, O. Bimber,"Unsynchronized 4d barcodes: Coding and decoding time-multiplexed 2d colorcodes," In Proc. 3rd Int. Conf. Adv. Vis. Comput., 2007, pp. 363–374.

[5] N. Saxena, J. Erik Ekberg, K. Kostiainen, N. Asokan, "Secure device pairing based on a visual channel," In Proc. IEEE Symp. Security Privacy, 2006, pp. 306–313.

[6] J. McCune, A. Perrig, M. Reiter,"Seeing-is-believing: Using camera phones for human-verifiable authentication," Int. J. Secur.Netw., Vol. 4, Nos. 1/2, pp. 43–56, 2009.

[7] Antonio Grillo, Alessandro Lentini, Marco Querini, Giuseppe F Italiano,"High capacity colored two dimensional codes," In Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on. IEEE, 2010, pp. 709–716.

[8] D. Parikh, G. Jancke,"Localization and segmentation of a 2d high capacity color barcode," In Proc. Workshop Appl. Comput. Vis.,2008, pp. 1–6.

[9] Zhibo Yang, Zhiyi Cheng, Chen Change Loy, Wing Cheong Lau, Chak Man Li,"TOWARDS ROBUST COLOR RECOVERY FOR HIGH-CAPACITY COLOR QR CODES", In proc. Image Processing (ICIP), 2016 IEEE International Conference on 2016, pp. 2866-2870.

[10] M. Mannan, P. C. Van Oorschot,"Using a personal device to strengthen password authentication from an untrusted computer," In Financial Cryptography, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds., Vol. 4886. Springer, 2007, pp. 88–103.

[11] Prof. Hemant Appa Tirmare, Prof. Sanjay Shamrao Pawar, Prof. Gitanjali Bhimrao Yadav,"Trust Based Micro Payment Authentication System in Mobile data network", Journal of Information, Knowledge and Research Computer Science and Applications, Vol. 01, Issue 02, pp. 26-31, 2011.