ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Issue 4, April 2016

SMARTPHONE BASED SECURE COLOR QR CODE USING VISIBLE LIGHT COMMUNICATION

R.SHARMILA[1],M.MOHAMED SITHIK[2]

(Anna Univ Affiliated)M.E Department of Computer Science and Engineering[1]
(Anna Univ Affiliated) Assistant professor Department of Computer Science and Engineering2
Mohamed Sathak Engineering College,Ramanathapuram district,TN.
[1]jeyaramsharmi@gmail.com.
[2]sithikbe@gmail.com

***Abstract*— Short range communication technologies are the emerging technology in mobile phone based applications. One of the technologies used in short range communication is Near Field Communication (NFC). These short range communication technologies are used in mobile advertisement, data sharing and contactless payments. For this purposes 2D barcodes are being introduced in mobile applications. Since every front camera enabled mobile phones can able to scan 2D barcodes. In this paper we are going to implement 2D barcodes in mobile phone applications which are very helpful for mobile payments and personal identification. With the help of visual light communication 2D barcodes are displayed on the smart phone screens when we use barcodes. In this paper we designed a color 2D barcode for providing better security features with the help of visible light communication (VLC) between smart phones. In this paper we are going to develop a secure 2D color barcode which secure private information during private data sharing process. Finally our experimental result shows that our proposed system provides better security when compared to normal 2D barcode schemes.**

***Keywords*— Visible Light Communication(VLC), Near Field Communication(NFC), Barcode, QuickResponse (QR) code.**

I.INTRODUCTION

A 2D (two-dimensional) barcode is a graphical image that stores information both horizontally as one-dimensional bar codes do and vertically. As a result of that construction, 2D codes can store up to 7,089 characters, significantly greater storage than is possible with the 20-character capacity of a uni-dimensional barcode. 2D barcodes are also known as quick response codes because they enable fast data access. 2D barcodes are often used in conjunction with smart phones. The user simply photographs a 2D barcode with the camera on a phone equipped with a barcode reader. The reader interprets the encoded URL, which directs the browser to the relevant information on a Web site. This capability has made 2D barcodes useful for mobile marketing. Some 2D barcode systems also deliver information in a message for users without Web access.

Barcodes became commercially successful when they were used to automate supermarket checkout systems, a task for which they have become almost universal. Their use has spread to many other tasks. 2-D bar codes (sometimes called matrix codes) carry information in two directions: vertically and horizontally. Accordingly, 2-D bar codes are capable of holding tens and even hundreds of times as much information as 1-D bar codes. Still, 2-D codes aren't perfect for every application. Because they're more complex than 1-D codes, they require more powerful scanners to decode. What's more, many people are simply unfamiliar with the technology, which hinders widespread adoption. But thanks to the smartphone in your pocket, that may all be about to change.

You might have already noticed odd black-and-white squares appearing on your parcels, letters, utility bills, T-shirts, product packaging, and in all kinds of other places— a bit like mini crossword puzzles without any letters. They're called two-dimensional (2D) barcodes and, just like ordinary barcodes, they're machine-readable so they can quickly pass on information about a product in the blink of an electronic eye. Where a barcode presents a string of information as a one-dimensional line of black and white bars, a 2D barcode packs a lot more information into a grid of black and white, square-shaped dots.

II.RELATED WORK

1) 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.

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 protocol1. The established key can be used later for many security applications.

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

A. *QR code*

The Quick Response (QR) Code was the earliest 2D barcode. It was designed to be a bump up from its predecessor, the 1D barcode, because it can contain more information. While not technically open source, the inventor of the QR Code and owner of the QR Code trademark, DENSO, has allowed the patents for the code to be freely available to the public. QR Codes have a variety of disparate formats and reader apps, and can be black-and-white or basic colors. Because of these constraints, QR Codes are best suited for simple designs that don't require integration with your branding. QR code abbreviated from Quick Response Code is the trademark for a type of matrix barcode or two-dimensional barcode first designed for the automotive industry in Japan.

A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes numeric, alphanumeric, byte / binary, and kanji to efficiently store data; extensions may also be used. The QR Code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device such as a camera, scanner, etc. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image.

QR codes have become common in consumer advertising. Typically, a smartphone is used as a QR code scanner, displaying the code and converting it to some useful form. The QR code has become a focus of advertising strategy, since it provides a way to access a brand's website more quickly than by manually entering a URL. QR codes storing addresses and URLs may appear in magazines, on signs, on buses, on business cards, or on almost any object about which users might want information. Users with a camera phone equipped with the correct reader application can scan the image of the QR code to display text, contact information, connect to a wireless network, or open a web page in the telephone's browser.

These acts of linking from physical world objects are termed hard linking or object hyper linking. QR codes also may be linked to a location to track where a code has been scanned. Either the application that scans the QR code retrieves the geo information by using GPS and cell tower triangulation (aGPS) or the URL encoded in the QR code itself is associated with a location. QR codes can be used on various mobile device operating systems. These devices support URL redirection, which allows QR codes to send metadata to existing applications on the device. Many paid or free apps are available with the ability to scan the codes and hard-link to an external URL.

The format information records two things: the error correction level and the mask pattern used for the symbol. Masking is used to break up patterns in the data area that might confuse a scanner, such as large blank areas or misleading features that look like the locator marks. The mask patterns are defined on a grid that is repeated as necessary to cover the whole symbol. Modules corresponding to the dark areas of the mask are inverted. The format information is protected from errors with a BCH code, and two complete copies are included in each QR symbol. The message dataset is placed from right to left in a zigzag pattern, as shown below. In larger symbols, this is complicated by the presence of the alignment patterns and the use of multiple interleaved error-correction blocks.

The amount of data that can be stored in the QR code symbol depends on the data type (mode, or input character set), version indicating the overall dimensions of the symbol), and error correction level.

B.Key Exchange

It is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

The key exchange problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy. Historically, this required trusted couriers, diplomatic bags, or some other secure channel. With the advent of public key / private key cipher algorithms, the encrypting key could be made public, since no one without the decrypting key could decrypt the message. Public key infrastructures (PKIs) have been proposed as a way around this problem of identity authentication. In their most usual implementation, each user applies to a 'certificate authority' for a digital certificate which serves for other users as a non-tamperable authentication of identity, at the risk of compromising every user in case the CA itself is compromised. Several countries and other jurisdictions have passed legislation or issued regulations encouraging PKIs by giving (more or less) legal effect to these digital certificates.

This does nothing to solve the problem though, as the trustworthiness of the CA itself is still not guaranteed from an individual's standpoint. It is a form of argument from authority fallacy. For actual trustworthiness, personal verification that the certificate belongs to the CA and establishment of trust in the CA are required. This is usually not possible. For those new to such things, these arrangements are best thought of as electronic notary endorsements that "this public key belongs to this user". As with notary endorsements, there can be mistakes or misunderstandings in such vouchings. Additionally, the notary itself can be untrusted. There have been several high profile public failures by assorted certificate authorities.

C. *Mobile Computing*

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The main concept involves:

- Mobile communication
- Mobile hardware
- Mobile software

Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal information now stored on the smartphone. More and more users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps. All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, wifi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

D. *Domain Justification*

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The main concept involves: Mobile communication, Mobile hardware, and Mobile software. Wireless data connections used in mobile computing take three general forms so. Cellular data service uses technologies such as GSM, CDMA or GPRS, 3G networks such as W-CDMA, EDGE or CDMA2000 and more recently 4G networks such as LTE, LTE-Advanced. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the principle of mobile computing.

Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution to the biggest problem of business people on the move mobility. Mobility implemented in data communications has a significant difference compared to voice communications. Mobile phones allow the user to move around and talk at the same time; the loss of the connection for 400ms during the hand over is undetectable by the user. When it comes to data, 400ms is not only detectable but causes huge distortion to the message. Therefore data can be transmitted from a mobile station under the assumption that it remains stable or within the same cell.

In many fields of work, the ability to keep on the move is vital in order to utilise time efficiently. Efficient utilization of resources (i.e.: staff) can mean substantial savings in transportation costs and other non quantifiable costs such as increased customer attention, impact of onsite maintenance and improved intercommunication within the business. The importance of Mobile Computers has been highlighted in many fields of which a few are described below:

- For Estate Agents
- Emergency Services
- In courts
- In companies
- Stock Information Collation/Control
- Credit Card Verification
- Taxi/Truck Dispatch
- Electronic Mail/Paging

With the rapid technological advancements in Artificial Intelligence, Integrated Circuitry and increases in Computer Processor speeds, the future of mobile computing looks increasingly exciting. With the emphasis increasingly on compact, small mobile computers, it may also be possible to have all the practicality of a mobile computer in the size of a hand held organizer or even smaller. Use of Artificial Intelligence may allow mobile units to be the ultimate in personal secretaries, which can receive emails and paging messages, understand what they are about, and change the individual's personal schedule according to the message.

III.ARCHIETECTURE

1) QR Code generation

QR code generation is the first module of our proposed approach. In that we are going to generate a QR code with added encoding techniques which coverts our original private data into different QR codes. Commonly QR code is an improved encoding technique which means it encrypts a given data as well as compresses the encrypted into reduced size. The size of a given data will be reduced when using an encoding technique. QR code is also performs like an encoding mechanism. QR codes are now used over a much wider range of mobile applications and commercial applications.

2) *Sender*

Sender is the second module of our proposed color QR scheme concept. In that a user (sender) holds en encoded message that is a QR code. The sender of one mobile phone stores QR code in their mobile storage and an opposite mobile (receiver) is kept in front of the sender mobile we can get our private information. This process is performed in the sender side only receiver is not involved in the second stage.

3) Receiver

Receivers are plays an important role in our proposed system since receivers are receive their private information through and with the help of an air interface. The sender can show their QR code in their mobile phone the receiver of one mobile displays private information which one is encoded with help of our visible light communication technology. The distance factor between two mobile phones is not taken into account in our notion of visibility. Since in near field communication, nearby devices are only communicated with each other. In our proposed concept two independent devices are communicate through visible light communication in near field communication mechanism.

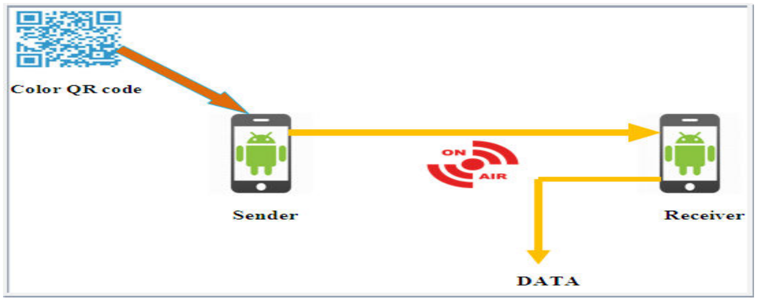

Fig.1. Architecture

4) Performance evaluation

In our proposed work performance evaluation is the final module in that performance against various technologies is measured. The performance evaluation of our proposed system outperforms the state-of-the-art, although the comparison has its limitations. In the proposed system we have examined and compared with several features for each technique to obtain a better performance. Finally our proposed colored 2D QR codes performs well when compared to our existing 2D QR code techniques by means of accuracy.

5) Algorithm Explanation

A QR code is a two dimensional barcode that stores information in black and white dots called data pixels or QR code modules. Besides the black and white version, you can also create a colored QR code. For these codes to work without problems, make sure the contrast is sufficient and the result is not a negative. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera, scanner, etc.) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image.

Users can generate and print their own QR codes for others to scan and use by visiting one of several paid and free

QR code generating sites or apps. The technology has since become one of the most-used types of two-dimensional barcode. QR codes have become common in consumer advertising. Typically, a smart phone is used as a QR code scanner, displaying the code and converting it to some useful form. The QR code has become a focus of advertising strategy, since it provides a way to access a brand's website more quickly than by manually entering a URL. Encrypted QR codes, which are not very common, have a few implementations. An Android app, for example, manages encryption and decryption of QR codes using the DES algorithm (56 bits).

The format information records two things: the error correction level and the mask pattern used for the symbol. Masking is used to break up patterns in the data area that might confuse a scanner, such as large blank areas or misleading features that look like the locator marks. The mask patterns are defined on a grid that is repeated as necessary to cover the whole symbol. Modules corresponding to the dark areas of the mask are inverted. Four-bit indicators are used to select the encoding mode and convey other information. Encoding modes can be mixed as needed within a QR symbol. Alphanumeric encoding mode stores a message more compactly than the byte mode can, but cannot store lower-case letters and has only a limited selection of punctuation marks, which are sufficient for rudimentary web addresses.

```
Algorithm 1: FrameClassifier({pi}N i=1 ,σ)
    R = 0; B = 0;
    for i ← 1 to N do
        if $\|pi - pr\|1 < \sigma$ then R++;
        if $\|pi - pb\|1 < \sigma$ then B++;
    if $R > 0 \cap B = 0$ then return 'Red';
    else if $B > 0 \cap R = 0$ then return 'Blue';
    else return 'None';
```

IV.PROPOSED SCHEME

1) *Need For New System*

Our proposed system should support colored QR codes. In addition to that it should support secure private data sharing between two mobile phones by means of visible light communication with the help of near field communication. Our proposed system should support better cryptographic technique for generating Quick Response code.

2) *Proposed System*

Nowadays, most of recently developing smart phones can read and display barcodes such as QR codes. To overcome the drawbacks encountered in the existing system we are going to design a new system that can stream QR codes between smart phones with the help of visible light communication technology. Two mobile phones can share their private information in 2D colored QR code format by using near field communication technology. In that two mobile phones should be equipped with a front camera when using recent android platform. Our proposed color 2D QR code approach can able to work with laptops and tablet also. In order to achieve a real-time system, we must ensure that each barcode can be encoded and decoded on time.

First, a 2D barcode only contains a very limited amount of information and hence cannot adopt advanced encryption primitives. Our proposed system uses an 8 bit binary mode for generating QR code. During QR generation we have considered following parameters that are the QR version, error correction level and frame refresh rate. According to our approach compared with the encoding running time, the decoding running time grows slower along with the increase of QR versions. Our proposed system offered high quality QR frame image can be easily decoded with very few errors when compared to our existing concepts.

V.CONCLUSION AND FUTURE WORKS

In this paper we proposed mobile phone based full duplex channel model on 2D barcode for secure our private information during data sharing. This approach is only suitable for android mobile phones and we can securely share our information between two mobiles with the help of visible light communication without need of any external hardware. Our system achieves high level security and NFC provides a comparable throughput when compared to an existing system. The proposed system can be used for secure device pairing, private information sharing, and secure mobile payment, etc. In this paper we propose a two phase scheme for transferring message between two smart phones. Finally we can get our resultant graph by means of frame decoding rate.

VI.REFERENCES

1. L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," ePrint Archive, Report 2011/618, 2011.
2. M. Allah, "Strengths and weaknesses of near field communication (nfc) technology," GJCST, vol. 11, no. 3, 2011.
3. T. Hao, R. Zhou, and G. Xing, "Cobra: color barcode streaming for smartphone systems," in MobiSys, 2012.
4. D. Parikh and G. Jancke, "Localization and segmentation of a 2d high capacity color barcode," in WACV, 2008.
5. S. Perli, N. Ahmed, and D. Katabi, "Pixnet: interference-free wireless links using lcd-camera pairs," in MobiCom, 2010.
6. J. McCune, A. Perrig, and M. Reiter, "Seeing-Is-Believing: using camera phones for human-verifiable authentication," Int. J. Secur. Netw., vol. 4, no. 1/2, pp. 43–56, 2009.

7. N. Saxena, J. erik Ekberg, K. Kostiainen, and N. Asokan, “Secure device pairing based on a visual channel,” in S & P, 2006.
8. R. Kainda, I. Flechais, and A. W. Roscoe, “Usability and security of outof- band channels in secure device pairing protocols,” in Symposium on Usable Privacy and Security (SOUPS ’09). ACM, 2009, pp. 11:1–11:12.
9. G. Starnberger, L. Froihofer, and K. M. Goeschka, “QR-TAN: Secure Mobile Transaction Authentication,” in Availability, Reliability and Security (ARES ’09). IEEE, Mar. 2009, pp. 578–583.
10. J. H°astad, R. Impagliazzo, L. Levin, and M. Luby, “Construction of a pseudo-random generator from any one-way function,” SIAM Journal on Computing, vol. 28, pp. 12–24, 1993.