Securing Data for QR Code Recognition using Pallier Cryptosystem

Ms. Sneha S. Hemadre[1],

ME-Student
Department of computer science and engineering
Deogiri Institute of Engineering & Management Studies, Aurangabad

Ms. A. S. Gaikwad[2]

Assistant Professor
Department of computer science and engineering
Deogiri Institute of Engineering & Management Studies, Aurangabad

Abstract- In many existing QR code recognition system, QR code is abstracted or read from motionless objects. Proposed system provides facility to read or fetch QR code from moving object. QR code attached on windshield is read and processed. Video of moving car is divided into frames and pre-processing tasks are carried out on frames as grayscale, CLAHE and binarization. Usually this system use the license plate that is been recognized, but for the more secure and errorless recognition the proposed working is on QR code detection. This QR code is generated from the license plate. QR code is two-dimensional barcode which is developed from the basics of one-dimensional barcode.

Keywords- Barcode, QR Code, Quick Response Code, Binarization, Windshield, CLAHE.

I. INTRODUCTION

All registered vehicles, except two wheelers, must have to mount license plate on such place which is clearly visible for checking purpose at the front and rear of the vehicle. License plate with annual tax payment displays vehicle registration ID, expiration date of tax payment and car brands. Generally, this attributes are checked by policemen in case of human errors. So, there is need of robust system which can be help to curtail some human errors by using QR code instead of an annual tax payment for record information which attached in same position and which possesses same size with annual tax payment.

Figure 1(a): Position of annual tax payment

Figure 1(b): Example of annual tax payment

Barcode can be used in every business around the world. Barcode is a data collection technique for product pricing, information. Barcode gives advantages over traditionally collect information of a product. Barcode is also specified as 'Optical Morse Code' [1]. It is show as lines of black bars and white spaces to uniquely identify items. Two dimensional barcode comes over one dimensional barcode that encrypt data horizontally and vertically like visual pattern so machine can read. 2 dimensional barcode is holds much more information and take less space. It shape as a rectangular and build in a stack or matrix form symbology [2]. Two dimensional barcode offer many advantages as small area, high capacity, high density, error detection, etc. The linear barcode is pile one upon another to obtain the most methodical use of coded area. In the matrix barcode data arrangement is depend upon black spots .Black element present in barcode also with same dimension and location of the item that codes the data. Ordinary matrix barcode is QR Code. The barcode scanner is perceived to read encrypted data.

Bar code is a fast, easy, accurate and automatic data collection method. Barcode facilitates products to be tracked proficiently and precisely at speeds not possible using manual data entry systems. QR Code is a matrix with two-dimensional barcode. The barcode reader only be used to recognize the barcode, and it is expensive. Now day's mobile phones [3] can implement many new kinds of

applications such as taking photos, and movie shooting by using embedded camera devices. So mobile phones with embedded camera devices can be used to recognize the barcode.

II. RELATED WORK

A. Features of QR Code

QR Code (Quick Response Code) is invented by Denso Corporation in 1994, and example of QR code is as shown in Fig. 2. There are total 40 versions in QR Code. It contains four levels of error correction [4]. The highest symbol size in the highest version of QR code is able to encode 7089 numeric data or 4296 alphanumeric data. Error correction with QR code permits error recovery up to 30% [5].

Figure 2. Example of QR Code symbol

QR Code provides many superior characteristics as follows:

1) High capacity for encoding of data:
QR Code possesses high capacity for encoding of data. Its highest symbol can encode 7089 characters; while PDF417 technique can encode only encode 2710 characters.

2) High-speed reading:
As compared with PDF417 technique, QR code requires less time to encode same data. As custom-made with CCD reading, it can recognize more QR Code symbol per second than PDF417 symbol for encoding same data capacity.

3) Chinese encoding capability:
Chinese and Japanese characters are characterized by a two byte permutation of two-dimensional barcode. But in QR Code delivers facility of a precise Chinese mode. This mode can utilize 13 bits encoding a Chinese character. So the effectiveness of Chinese characters enhanced by 20% in QR Code as compared with PDF417.

4) Readable from any direction from 360 degree:
QR Code is a matrix with two-dimensional barcode. Therefore, it can be readable from any direction from 360 degree. But the stack two-dimensional barcode as PDF417 is extremely complicated to recognize for reading purpose from 360 degree.

QR Code has been approved as an, a JIS Standard, ISO standard, AIM Standard. So QR Code is being utilized in extensive diversities of applications, such as manufacturing, logistics, and sales applications.

B. Encoding of QR Code

Each QR Code symbol consists of an encoding region and function patterns, as shown in Fig. 3. Finder, separator, timing patterns and alignment patterns comprised function patterns [6]. Function patterns are not utilized for the encoding data. The finder patterns located at three corners of the symbol intended to support in straightforward location of its position, size and inclination.

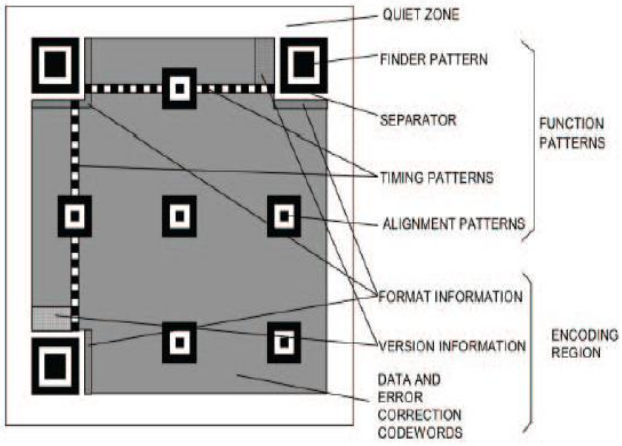

Figure 3. The structure of QR Code

Figure shown above describes the construction of QR code of version 7. Version 1 of QR code contains 12 X 12 numbers of modules and at each version this modules numbers increases in steps of 4 modules, [7]. Version 40 of QR code contains 177 X 177 numbers of modules. Language of QR possesses 4 modes as follows:

1) Numeric Mode
2) Alphanumeric Mode
3) 8-bit Byte Mode
4) Kanji Mode

Languages of QR code are described in following table:

Table1: Language Modes of QR Code

Language Mode	Characters
Numeric Mode	0-9
Alphanumeric Mode	0-9, A-Z (Upper case letters), +,-, *, /, %, $, Space, :
8-bit Byte Mode	Refer to ISO 8859-1
Kanji Mode	Refer to Shift JIS system based on JIS X 0208

QR code delivers facility of error correction automatically. This error correction technique is used to restore data of damaged code. It possesses 4 levels of error correction as L, M, H and Q [8]. These levels of error correction technique allow recovery of codewords. Working of QR code error correction is combined with Reed-Solomon code.

Reed-Solomon code is added to original data to restore data from dirty or damaged QR code.
A Reed-Solomon (RS) code is an error-correcting code invented by Reed and Solomon in 1960. These codes enclose great influence and utility, and hence they found in many applications as CD-ROMs, wireless communications, space communications, DSL, DVD, and digital TV [9].

Reed-Solomon codes considered as non-binary cyclic codes with symbols containing m-bit sequences, where m is any positive integer enclosing a value greater than 2. Reed-Solomon codes achieve the major possible code minimum distance for any linear code with the same encoder input and output block lengths. For non-binary codes, the distance between two code words is defined (analogous to Hamming distance) as the number of symbols in which the sequences differ. For Reed- Solomon codes, the code minimum distance is given by

$$D_{\min} = n - k + 1$$

The Reed-Solomon (R-S) codes are particularly useful for burst-error correction; that is, they are effective for channels that have memory. Also, they can be used efficiently on channels where the set of input symbols is large. An interesting feature of the R-S code is that as many as two information symbols can be added to an R-S code of length *n* without reducing its minimum distance.

RS encoding data is relatively straightforward, but decoding is time-consuming. In the past few years it becomes computationally possible to send high-bandwidth data using RS. RS differs from a Hamming code in that it encodes groups of bits instead of one bit at a time. We will call these groups “digits” (also “symbols” or “coefficients”). A digit is error-free if and only if all of its bits are error-free. For instance, if a digit is an 8-bit character, and three bits of the same single character are in error, we will count that as one corrupted digit.

Table2: Approximate Error Recovery Capacity

Error correction level	Recovery Capacity (approximately)
L	7%
M	15%
H	25%
Q	30%

Table given below describes the approximate recovery capacity of each error correction level.

The encode procedure of QR Code including follows steps.
1) Firstly input data is encoded in according to most efficient mode and formed bit stream. The bit streams are divided into codewords.

2) Then codewords are divided into blocks, and add error correction codewords to each block. All these codewords are put into a matrix and are masked with mask pattern.

3) Finally function patterns are added into the QR symbol. A QR Code symbol is formed.

C. Contrast Limited Adaptive Histogram Equalization

CLAHE (Contrast Limited Adaptive Histogram Equalization) is an improvised edition of AHE (Adaptive Histogram Equalization). Both this versions of histogram equalization are used to beat the restrictions of standard histogram equalization.
Instead of complete image, CLAHE [10], [11], [12] works on small images regions often called as tiles. Each tile contrast is boosted. Neighboring tiles are then merged into each other with the help of bilinear interpolation to remove artificially stimulated boundaries. Generally in homogenous areas, the contrast is restricted to curtail amplification of any noise which may be lying in the image [13], [14], [15].

III. SYSTEM ARCHITECTURE

The system is developed to recognize the QR code that is placed on the windshield of the car. Usually this system use the license plate that is been recognized, but for the more secure and errorless recognition the proposed working is on QR code detection. This QR code is generated from the license plate. QR code is two-dimensional barcode which is developed from the basics of one-dimensional barcode. It uses bit stream concept. QR code consists of compressed information of the license plate. Fetched QR code is preprocessed and decrypted to get code hidden in the QR code.

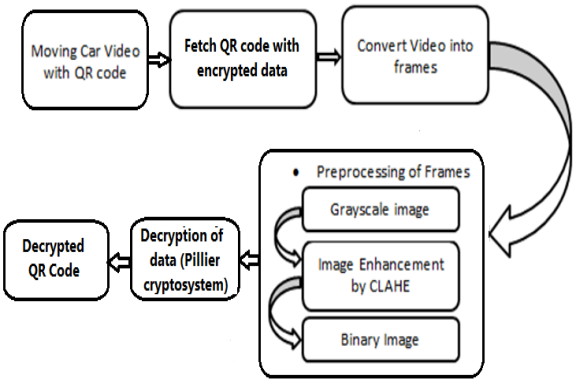

Fig.4: System Procedure for QR Code Detection

The system procedure first gets the input video that consists of the moving car with QR code on its windshield with code which holds important information in encrypted format. Then pre-processing such as enhance image, grayscale, convert to binary image are performed on the video frames as follows:

1) In first step that contains conversion of the video frames into gray scale images. Then the adjustment is performed that provide 1% of saturation of the data at high and low intensities of grayscale images.

2) Then the contrast of the image is enhanced of the grayscale image by applying CLAHE.

3) The obtained enhanced image is converted into binary image based on threshold. The binary image replaces all the pixels into luminance greater with value 1 that is white and lesser with value 0 that is black.

4) After these Pre-processing procedures, QR code is decrypted from binary images using paillier cryptosystem and generated data is given to the user.

If system is not able to decode QR code then it will count next video frame and again replicate preprocessing steps.

Detail information of steps is as given below:

Gray Conversion:

QR Code symbol is detected by embedded system with the help of CCD or CMOS, which is a colorful image. QR Code symbol contains a group of dark and light pixels. It does not require dealing with color information of image and the gray image calculated quickly with little space, so gray conversion is needed as the first step of preprocessing of videos.

Binarization:

Binarization of gray scale is an important step to be performed while pre-processing procedure. Assortment of a suitable binarization method is complex for the performance of barcode detection system. In binarization of an image, a simple and widely used technique is thresholding. There are two types of thresholding methods: global and local thresholding.

Encryption / Decryption of information:

Proposed system provides secure/ encrypted QR code. Encryption is the process which yields encoding of information in such a way that only authorized persons can read the original hidden message. Peoples can store important data in QR code in encrypted format. Proposed system supports this scheme and utilizes paillier cryptosystem for encryption and decryption of QR code.

The Paillier Cryptosystem is public key encryption scheme in which messages is encrypted with the recipient's public key and can only be decrypted with the corresponding private key. It is invented by Pascal Paillier, with possesses numerous attractive properties. To use paillier system, user of system must be familiar with modular arithmetics and the idea of conversion of an alphanumeric message into a numeric message, which further can be divided into m_i blocks in such a way that for each i, $0 < m_i < n$, for a predetermined value, n. The term plaintext is used to refer message which is numeric but not encrypted while the term cipher text is used to denote message which is encrypted but not yet decrypted. The Paillier Cryptosystem's scheme works as follows:

- Select two large primes, p and q.
- Calculate the product n=p x q, such that gcd(n,Φ(n)) = 1.
- Choose a random number g, where g has order multiple of n or gcd(L ($g^{\lambda} \bmod n^2$)n) = 1, where L(t)= (t-1) / n and λ(n)=lcm(p-1, q-1).
- The public key is composed of (g, n), while the private key is composed of (p, q, λ).
- The Encryption of a message m < n is given by:

$$c=g^m r^n \bmod n^2$$

- The Decryption of ciphertext c is given by: $m=(L(g^{\lambda} \bmod n^2)/L(g^{\lambda} \bmod n^2))\bmod n$

Following code describes the pseudo code for the QR code detection:

1) Get Input as Video: V=VideoReader('Path');
2) Convert Video into frames: Frame=read(videoObject, frame);

3) Apply Grayscale Function on frames: rgb2gray(Frame);
4) Apply CLAHE on the grayscale frame using components: Cliplimit, Rayleigh
5) Convert Frame into binary image: im2bw(frame);
6) Enhanced Contrast by transforming threshold values using CLAHE.
7) Read QR code from binary image of frames: QR_writer.encode(message, BarcodeFormat.QR_CODE);
8) Display the resultant recognition.

IV. CONCLUSION

Proposed Method used to read and fetch QR code attached to windshields on vehicles. Firstly, video of moving car with its QR code is divided into frames. Further Pre-processing tasks such as grayscale, binary image and CLAHE are carried out on video frames. Binary images are generated for video frame images. System reads binary images containing QR Code. Further, Decryption of QR Code is carried out to recognize it.

REFERENCES

Watsamon Hogpracha, "Recognition System For QR Code on Moving Car", The 10th International conference on Computer Science & Education (ICCSE), July 22-24, PP no. 14-18, 2015

Xiao Yonan, Yang Chao, Luo Chuting, "A new method of QR Code Accumulation Encoding in Mobile Education", International conference on Consumer Electronic, Communication and Networks", 16-18, April, pp. 42-45, 2011

J. K. Stark, "Adaptive Image Contrast Enhancement Using Generalizations of Histogram Equalization", IEEE Transactions of Image Processing, Vol.9, No.5, 2000, pp.889-894.

Chanon Skawattananon, Mahasak Ketcham. Sartid Vongpradhip, "Identifying QR Code", International conference on Computer and Communication Technologies, pp. 132-135, 2012.

Kamon Homkajorn, Mahasak Ketcham, Sartid Vongpradhip,"A Technique to Remove Scratches from QR Code Images", International conference on Computer and Communication Technologies, pp. 127-131, 2012.

Suppat Rungraungsilp, Mahasak Ketcham, Virutt Kosolvijak, Sartid Vongpradhip," Data Hindng Method for QR Code Based on Watermark by Comparing DCT with DFT Domain" Computer and Communication Technologies, pp. 144-148, 2012.

Fadi Masalha, Nael Hirzallah, "A Students Attendance System Using QR Code", International Journal of Computer Science and Technology, Vol.5, No.3, 2014.

Suppat Rungraungsilp, Mahasak Ketcham, Pruch Surakote, Sartid Vongpradhip," Data Hindng Method for QR Code Based on Watermark by Comparing DCT with DFT Domain" Computer and Communication Technologies, pp. 149-154, 2012.

Suppat Rungraungsilp, Mahasak Ketcham, Virutt Kosolvijak, Sartid Vongpradhip," Data Hindng Method for QR Code Based on Watermark by Comparing DCT with DFT Domain" Computer and Communication Technologies, pp. 144-148, 2012.

Zuiderveld, Karel, "Contrast Limited Adaptive Histograph Equalization", Graphic Gems IV. Sans Diego: Academic Press Professional, 1994, 474-485.

E. D. Pisano, S. Zong, B.M. Hemminger, M.DeLuca, R. E. Johnston, K. Muller, M.PBraeuning and S. M. Pizer, "Contrast Limited Limited Adaptive Histogram Equalization Image Processing to Improve the Detection of Stimulated Spiculations in Dense Mammograms", Journal of Digital Imaging, Vol.11, No.4, 1998, pp193-200.

Jiejing Zhou, Yunfie, Liu, Amit Kumar, "Research on Distortion correction of QR Code Images", International Journal of Computer Science and Technology, Vol.3, Issue 1, 2012.

S. K. Shome and S. R. K. Vadali, "Enhancement of Diabetic Retinopathy Imagery Using Contrast Limited Adaptive Histogram Equalization", International Journal of Computer Science and Technology, Vol.2, No.6, 2011, pp no. 2694-2699.

Suppat Rungraungsilp, Mahasak Ketcham, Pruch Surakote, Sartid Vongpradhip," Data Hindng Method for QR Code Based on Watermark by Comparing DCT with DFT Domain" Computer and Communication Technologies, pp. 149-154, 2012.

S. Srinivasan and N. Balram, "Adaptive Contrast Enhancement Using Local Region Stretching", Proceedings of ASID'06, New Delhi , 8-12 October 2006, pp. 152-155.