Sheilding Data Usng Ciphered Pictoric Ambiguity

Varsha Panwar
M.TECH Student, Krishna Engineering College,
Ghaziabad, Uttar Pradesh, India

Vinit Kumar
Associate Professor, Krishna Engineering College,
Ghaziabad, Uttar Pradesh, India

Abstract: The identification of objects and places in the real world is very important and 2-D printing code is useful to store identifiers of them. Any camera object or mobile device with capture the function can read content from a barcode tag or 2-Dl barcode directly. When a barcode contains very important data or private information, the risk of security becomes an important problem. Because QR or Quick Response Codes are a type of 2-Dl barcode that can be read using camera and smart phones dedicated QR reading devices that link directly to text, websites, phone numbers, emails and more things. So in this paper we discuss how to secure the QR codes by using some methods. but also it secure by any virus , malware or threats or unauthorized party.

Keywords: URI, URL, AES, DES,

I.   INTRODUCTION

QR code it is also called (Quick Response Code) is the trademark for a type of matrix barcode and it also as 2-dimensional barcode firstly designed in Japan for the automotive industry. A barcode is a readable optical label machine which is contains information about the item or some other things to which it is attached many places. A QR code are used four encoding modes, alphanumeric, numeric, binary, byte also to efficiently store data, extensions may also be used.

It has become very popular outside the automotive industry because its has very fast readability and greater storage capacity as compared to standard 1-D barcode or any other barcode. In this applications are include product tracking , time tracking, general marketing, item identification and documentation much more.

The QR code system was invented by Denso Wave in 1994. Its was purposed to track vehicles during manufacture process it was designed to allow high-speed component for scanning. Initially it is used for tracking parts in vehicle manufacturing products, QR codes now are used in a much broader context, including both convenience-oriented applications and commercial tracking applications aimed at mobile phone users .

A QR code consists of black modules in the form of square dots which are arranged in the form of square grid on a white background in the image of QR code which can be read by any an imaging device such as a camera or any smart phones and its is processed by using Reed–Solomon error correction until the images can be appropriate interpreted data is extracted in the from patterns which is present in both horizontal and vertical components of the images.

QR codes are may be used to display text to the user and to add a vCard or any card contact to the user's device which is used to open a Uniform Resource Identifier (URI), or to compose an e-mail or text messages. Users can generated and can take print their own QR codes for others to scan and its is used by visiting one of several paid or any free QR code generating sites or many apps. It has become one of the most-used types of 2-dimensional barcode.
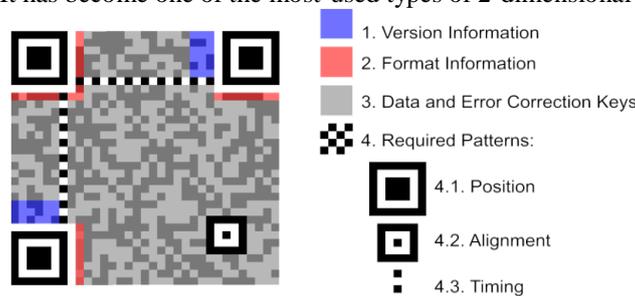

Figure 1. QR Code

Why should care about QR Codes?
With as many as half of us now owning the smartphone , and that number growing on a daily basis, QR Codes have the great potential to have a large impact upon society and particularly in marketing, advertising area and customer service with a wealth of product information just one scan .

How is a QR Code different from a normal 1-D barcode?
Ordinarily a barcode as a collection of vertical lines . QR Codes are store the data in both directions and it differ form 1-D barcode and it can scanned horizontally as well as vertically .Whilst a standard 1-D Barcode (UPC/EAN) are stored up

to 30 numbers, a QR Barcode can store up to a massive 7,089! It has a large amount of data that enables links to such things as Twitter pages or Facebook or a plethora of , videos ,other website pages etc.

How do I scan a QR Code?
If you have a smartphone like Blackberry, Android , iPhone and other phone then there a number of different barcode scanner applications such as Barcode Scanner , Red Laser and QR Scanner that can read it and then decode data from a QR code. The majority free completely all you have to do once you install one is to use your smartphone's camera or any camera to scan these barcode, which will then automatically loaded the encoded data for you.

What can be encoded into a QR Code?
In its simplest way a QR Code is an 'image-based hypertext link'. it can be used offline – any URL can be encoded into the form of QR Code so essentially any webpage can be opened automatically it scanning the barcode and give the results. If you want to encourage someone to be like your facebook page or twitter page – have your facebook or twitter profile page as the URL. Want your video to go viral –so encode the URL in your QR Code form.
In the addition to website URLs in the QR Code can also contain a phone number or other information– so when it is scanned it prompts to the user can call a particular number or other details . Similarly you can encode an SMS text message, V-card data, other details or just plain alphanumeric text. The smartphone or 2-dimensional barcode reading device will automatically know thewhich application to use to open the content to embedded within the QR Code.

Where can be QR Codes be placed?
The answer to this is almost anywhere place. QR Code printing can be done in newspapers, brochures, magazines, on business cards or leaflets. Further code image they can be put on product packaging or labels or even walls or on billboards. You could even also tattoo a QR Code on your body – now that will be an interesting to take on giving a girl/guy your number in a bar. You can use also QR Codes on a website but they are not generally be used as a substitute for an old-fashioned hyperlinks because the user is already online and doesn't really to want the fiddle around with their phone only to find a website they can have just clicked through to in half the time.

II.   LITERATURE REVIEW
1. A. Sankara Narayanan intoduce"QR Codes and Security Solutions".

In general terms we believe that QR codes have great potential in business media and other filed. Some possibilities are discussed in this paper and there are so many creative ideas waiting for us to explore it. Also, this paper can be served as the first step for the readers to investigate that exciting topic of mobile learning and others .In this paper examine outlined the dangers of possible malicious
2. Peter Kieseberg, Martin Mulazzani , Lindsay Munroe, ,Manuel Leithner Sebastian Schrittwieser, , Edgar Weippl , Mayank Sinha on the topic is "QR Code Security".

In this paper we highlights the dangers of possible attacks utilizing modified QR Codes. Since QR Codes gain increasing popularity through their use for business and marketing purposes, we can expected that this kind of attack will receive more and more attentions by the hacking community in the future .Furthermore, many mobile devices like smartphones which is present are able to decode QR Codes and access the URLs contained in them.
3. Damon Gura , Kevin O'Shea , Arjuna Reddy Micheline (Mich) Sabatté introduce "QR codes"

 The QR codes will be provides to the value of strong firmly in manys different forms. For an investor's point of view, the firms that have a strategic vision and take an innovative approach in using QR code technology will certainly benefit in the long-run. Marketing initiatives that support consumer interaction and the subsequent feedback loop (research and technology) represent a strong value proposition for firms looking to distinguish themselves from competitors. Starbucks is a great example of this approach through their application of QR code technology in overall in-store operations. It will enable them to be a winner in this space.
4 . There are many research papers we have taken many ideas basically work on the security of QR code with the help of AES algorithms. abbreviation

III.   AES ALGORITHM
AES is the short form of Advance Encryption Standard. It is the current standard for secret key encryption. Vincent Rijmen and Joan Daemen was two Belgian cryptographers introduced this application. This application was also known as Rijndael. It replaces the old DES (Data Encryption Algorithm).
The Federal Information Processing Standards Publication 1970 on November 26, 2001 announced this application as the new standard for encryption.It was designed to work in software and hardware both variety of platforms.It is advanced version of DES.AES is a combination of both substitution and permutation. It don't work as Feistal Cipher. It was works as a Block cipher.
AES is the variant of Rijndael algorithm which has a fixed block size of 128 bits, and other a key size of 128, 192, or 256 bits. Its operates on a 4×4 column-major order matrix of bytes. Most of the calculations are done in a special finite field .Initially this algorithm performed on a 2D array for bytes ,called the State.For instance, if you have 16 bytes, $b_0, b_1, ..., b_{15}$, these bytes are represented as this matrix:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

MATRIX

In AES cipher key size specifies the number of repetitions of transformation rounds .The number of repeated cycles are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round(except last one) consists of uniform and parallel composition of 4 steps.

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

Mix Columns stage does not include in tenth round .The description algorithm of nine round consist of the following

1. Inverse Shift rows
2. Inverse Substitute Bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again Inverse Mix Columns stage does not include in tenth round.

3.1Description of an Algorithm
3.1.1. Substitute Byte
It is also known as subByte stage. It uses a lookup table using a 16*16 matrix called an s-box. Its uses Non-linear but invertible Substitution on each byte . S-box is represented by hexadecimal bits. This AES s-box different form DES s-boxes. AES s-box is easy to analyze and based modular arithmetic polynomial .The s-box is generated from multiplicative inverse over GF(2^8).
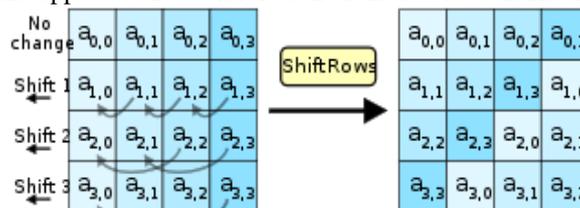 In Inverse SubByte transformation inverse s – box is used.
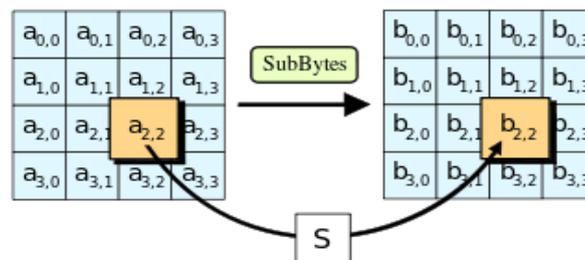
The sub bytes step

3.1.2 Shift Rows
This transformation is a simple permutation .Row number is equal to the number of Circular Left Shift.
These Circular Shifts perform in the opposite direction for each of the last rows in Inverse Shift Rows transformation.


The shift Rows

3.1.3. Mix Columns
 This stage use arithmetic of GF(2^8)and it is basically a substitution. Each column interprets as a vector length 4.Each column is individually operated. Each Byte of column of State is replaced by another column by multiplying that column with matrix GF.

The mix columns step
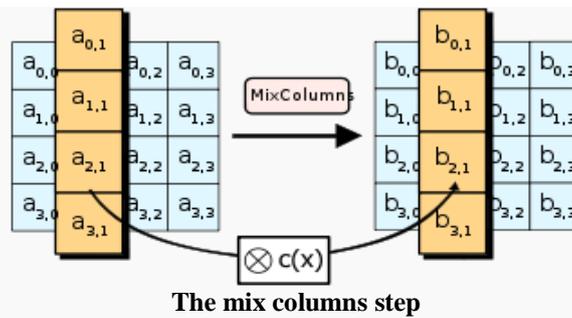
3.1.4. Add Round key

In this transformation Round key is applied to the state are bitwise XOR operation. Round key length is 16 bytes which is equal to block key length .This transformation is very effective but very bit of state is also effected.

The add round key step
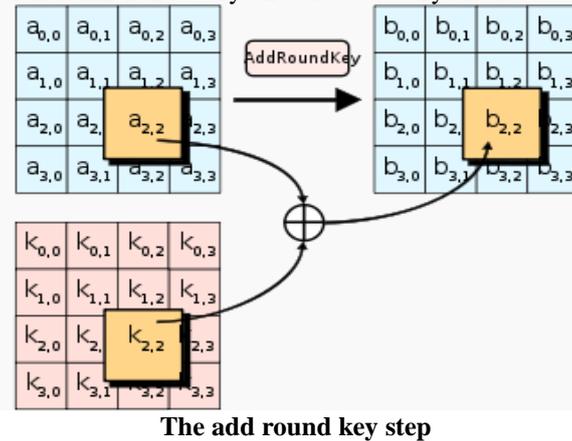
IV. BY USING AES ALGORITHM WE GENERATE THE SECURED QR CODES ON THE BASIS SOME IDEAS

1. The user will be able to generate a QR code using 2 options namely,

- Text
- Image

2. Under "Text" option, the user will input some text (in a text field) that needs to be hidden inside the QR codes

Figure 2. The QR Code is Gentered

3. Under "Image" option, the user will input web URL of the image location.

4 . After that, we will ask the user whether he wants to encrypt the QR code. If the user selects "Yes", we shall ask for a password in a text field in order to encrypt the QR code. Once the password is input, the encrypted QR code will be generated. If the user selects "No", so the QR code will be generated without password and QR code displayed on the screen. Then once a QR code is generated, it will be display on the screen.

6.Then after the QR code is generate in the form image then the user would be able to scan it through the "Scan" option present in our application. Under the "Scan" option, the integrated camera of the laptop shall turn ON. The user will put a printed out image of the stored QR codes before the camera for capturing.

7. If the QR code is encrypted, it will ask for a password for a decryption on the PC screen. Once the correct password is input, it will show the text or URL or other information in the text form that is hidden inside to the QR code. But if the QR code is not encrypted so it won't ask for a password and under "Scan" option, it will directly show the text or URL hidden inside it.

8 .The encrypted QR codes will only be scanned by our application. In other words, if some another 3rd party QR code scanning application scans it, junk characters will be displayed. But if scanning is done through our application, the password will be asked first and only upon its correct entry, the hidden text or URL will be displayed.
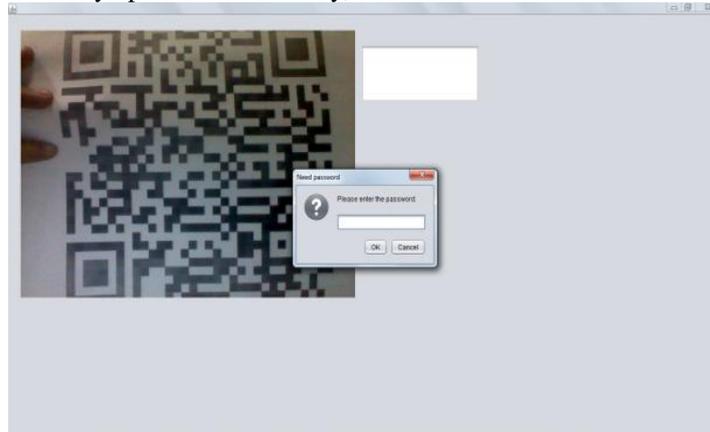

Figure 3. Secured QR Code is Generated

If the URL is displayed after scanning a QR code, there should be an option to visit that URL.

9. There are QR Customization options which are presented in our application namely are:

    a.   Apply Color
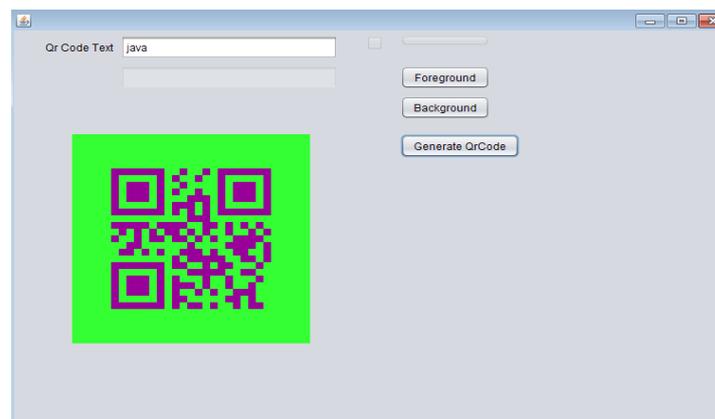
    b.   Add Logo

    c.   Add Label

Figure 4. Coloured QR Codes Generated

9. If the user are select the option for "Apply Color" he/she will be able to change the colours of the QR code by using a multicolor palette . This feature will not be make any changes in the data hidden inside the QR code image. The user can be still scan the QR code perfectly after this customization.

10.If the user are select the option for "Apply Logo" she/he can be easily able to browse the image which are needed to be embedded on the QR code so that it is visible as a tiny image form in the QR code. This additional feature too will not make any changes in the hidden data inside the QR code. The user can be easily scan the QR code perfectly after this customization.

11.If the user select the option for "Apply Label" her/his can be able to input a text data in a text-field that will become visible below the generated QR code.   Please also note that this text data will be visible below and outside the boundaries of QR code, not inside the QR code. This addition feature will not make any changes in the data hidden inside the QR code. The user can be still scan the QR code perfectly after this customization.

12. While developing this application, we will divide the features into different user interface windows. In other words, we shall not include all the features in one single UI.

V. CONCLUSION

We may hereby conclude that with the use of this application:

The organization would be able to save significant costs on paper, printing, labor, etc. through hiding a lot of vital content and information to be communicated with the use of QR code.This application / tool would help the company bring advancement in its processes by the use of latest technology which is considered as superior that its closest substitute .As the QR codes could be customized or formatted as per the company's wish by applying color, embedding logo image or label, it shall help the organization to communicate the information in a more emphasized and differentiating manner than others. The secured QR codes will help the company to securely communicate the information thereby serving the double purpose of secure and obscure data exchange.

The organization will not be able to use it on products but in any objective like posting of jobs, display of images, etc. This will help the company implement a one stop solution for a compressed, cost – effective, secure and hidden information exchange.

REFERENCES
[1]   Law, C. & So, S. (2010). QR codes in education. Journal of Educational Technology Development and Exchange, 3(1), 85-100.
[2]   Designer QR Codes; Ensuring the "beep" Kevin Berisso, OHIO University, Spring 2013
[3]   QR Codes and Security Solutions, International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012]
[4]   QRP: An improved secure authentication method using QR codes, David Pintor Maestre Universitat Oberta de Catalunya, Barcelona, June 8, 2012
[5]   Automatic Recognition Algorithm of Quick Response Code Based on Embedded System   Yue Liu , Mingjun Liu, Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06)
[6]   QR Codes , Damon Gura ,Kevin O'Shea ,Arjuna   Reddy, Micheline Sabatté, March , 2011
[7]   Law, C. & So, S. (2010). QR codes in education. Journal of Educational Technology Development and Exchange, 3(1), 85-100
[8]   QR Codes , Tan Jin Soon Executive Director, EPCglobal Singapore Council, synthesis journal 2008
[9]   .https://en.wikipedia.org/wiki/Advanced_Encryption_Standard