A Desktop Application of QR Code for Data Security and Authentication

Partiksha Mittra
Department of Computer Science and Engineering
Amity University Uttar Pradesh
Noida, India
pratikshamittra@gmail.com

Nitin Rakesh
Department of Computer Science and Engineering
Amity University Uttar Pradesh
Noida, India
nitin.rakesh@gmail.com

***Abstract*—Initially the barcodes have been widely used for the unique identification of the products. Quick Response i.e. QR codes are 2D representation of barcodes that can embed text, audio, video, web URL, phone contacts, credentials and much more. This paper primarily deals with the generation of QR codes for Question Paper. We have proposed encryption of Question Paper data using AES Encryption algorithm. The working of the QR codes is based on encrypting it to QR code and scanning to decrypt it. Furthermore, we have reduced the memory storage by redirecting to a webpage through the transmission and online acceptance of data.**

Keywords— QR Codes; AES algorithm; Encryption; Decryption; Scanning

I. INTRODUCTION

"QR" is abbreviated as "quick response," is a reference to the speed at which the huge amount of information it contains, can be decoded with scanners. QR Code shown in figure 1 is a two-dimensional or matrix bar code developed in Japan by Denso Wave. They are sometimes referred to as 2D codes, 2D barcodes, or mobile codes. These are machine readable codes and comprise of black modules on white modules. It holds thousands of alphanumeric characters while the barcode comprises of only 20 characters. This two-dimensional symbol was invented for tracking of automotive parts, but these codes are increasingly found in other fields as well like linking to websites, product labels, advertising campaigns, SMS, contact details, email messages and much more. The information stored in codes varies from tracking information of the products produced in various industries to information of the business on a business card that redirects to the specific website. These small sized codes can also be hidden inside the image.

Fig. 1. QR Code

This document examines the QR codes and realizes the significance of data, information and distributes it in such an obscured or non–obscured way so that authorized people should be able to view it. At the same time, the data should remain publicly accessible but it should either be accessible to the authorized personnel or the ones who have the appropriate tools to view it. In order to improve the security of the information stored in QR code, a 2-D code encryption and decryption method based on cryptic data is proposed in this paper .An interesting use of QR code is to exchange information. Information exchanged can be private information exchange or public information exchange. The public information exchange using QR codes can take place with the help of existing tools and application, wherein no encryption is required. As far as the private information exchange is concerned encryption is required for the secured transactions.

This paper is further divided into five sections. Section first we have introduced QR code and its applications. Second section shows recent application area of QR codes. In third section we have proposed the application of QR code which is a developed application that helps in secure transfer of question papers via websites and interfaced among various universities.

II. CURRENT APPLICATION OF QR CODES

With the increase development in technology, the uses of electronic devices are also increasing and so as the various applications of QR codes. QR Code has been approved as an AIM (Automatic Identification and Mobility) Standard, a JIS (Japanese Industrial Standard) Standard and an ISO standard. So QR Code is being used in a wide variety of applications, such as manufacturing, logistics, and sales applications. QR codes are being used as ticket checker for various transportation systems to avoid manual works and queues. It helps in providing station level security by acting as a ticket and validating the users whether he enters or leaves the station [1].

With constant evolving technologies, there comes new methods for learning and QR codes are one of those being used in present days. As for the university, students can send his/her queries through MMS in form of or codes to the university server, which are further decoded and students are provided with their respective solutions [3]. QR codes are being used in some of the libraries for various purposes. One of the purposes is to find the exact location of the books kept in the library by

scanning the QR codes containing the location of those books stored in the database. QR codes are also being for blind navigation, it provides automatic navigation after scanning of the QR codes and provides the user with the shortest path. If during navigation users deviates from its path then it automatically guides the user back to the right path [2].

QR codes are also giving their best in the field of advertisements. By scanning QR codes it becomes easier for people to get to know about the deals and location of vendors for their preferred products [4]. In addition to, QR Code has many advanced features like QR Code has high capacity encoding of data, its maximum symbol can encode 7089 characters; while PDF417 only encode 2710 characters. QR Code is a matrix two-dimensional barcode; it can be readable from any direction from 360 degree. But the stack two-dimensional barcode, for example PDF417, is very difficult to realize the readable from 360 degree.

As the mobile phone with camera device is getting more popular, recognition barcode based on embedded system is getting more important and practical. We proposed a new high-speed, high-accuracy automatic recognition method for recognizing QR Code in various illumination conditions. And there is no need the special scanner for barcode recognition in the proposed method. From the experiment, the proposed method produced better results than other method. The recognition test also showed the proposed method is effective for the QR Code image recognition based on embedded system.

III. QR FOR SECURED QUESTION PAPER GENERATION

A. Primer

The application is divided into two modules i.e. QR code generator and QR code reader. Using this application, the user will be able to generate a QR code using 2 options namely, text and image.

Under “Text” option, the user will input some text (in a text-field) that needs to be hidden inside the QR code. Under “Image” option, the user will input web URL of the image location. After that the user will be asked whether to encrypt the QR code or not. 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 inputted, the encrypted QR code shall be generated. If the user selects “No”, the QR code will be generated without a password and displayed on the screen. Once a QR code is generated, it will be displayed on the screen as well as saved as an image file at a specific destination folder/directory within the hard drive of the user PC.

After the QR code is generated, the user will 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. If the QR code is encrypted, it will ask for a password for decryption on the PC screen. Once the correct password is inputted, it will show the text or URL that is hidden inside the QR code. But if the QR code is not encrypted, it won’t ask for a password and upon “Scan”, it will directly show the text or URL hidden inside it.

No another 3rd party QR code scanning application can scan it, if it does, 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. If the URL is displayed after scanning a QR code, there should be an option to visit that URL. There will be “QR Customization” options present in our application namely, Apply Color, Add Logo, Add Label. If the user selects “Apply Color”, he would be able to change the color of the QR code using a multicolor palette. This feature will not make any changes to the data hidden inside the QR code. The user could still scan the QR code perfectly after this customization. If the user selects “Apply Logo”, he would browse an image that needs to be embedded inside the QR code so that it is visible as a tiny image in the QR code. This feature too will not make any changes to the data hidden inside the QR code. The user could still scan the QR code perfectly after this customization. If the user selects “Apply Label”, he would be able to input a text data in a text-field that will become visible below the generated QR code. This text data will be visible below and outside the boundaries of QR code, not inside the QR code. This feature too will not make any changes to the data hidden inside the QR code. The user could still scan the QR code perfectly after this customization.

The encryption process makes use of the AES algorithm and the text gets encrypted with a password which the user uses to decode the text while scanning. In the second module the QR code is scanned which takes the help of the camera of the desktop or laptop. Once it is scanned the data hidden in the QR code is displayed directly if it is not secured by a password and if it is secured by a password then the application asks for the particular password and once the password gets entered the data get displayed.

This application can have many uses but here this application is used to securely transmit the set of question papers prepared in an university to different universities which will be uploaded by various faculties on a website and the URL of that website will be circulated to different faculties of different universities in the form of QR codes so that they can view the question papers by scanning the received QR code.

B. Methodology

The algorithm used for encrypting and decrypting the data stored in QR codes in our paper is Advanced Encryption Standard (AES). There are many algorithms proposed like Data Encryption Standard, Triple Data Encryption Standard (Triple DES), Blowfish etc. but the best suited algorithm for this paper is AES algorithm [8]. Although this paper uses AES algorithm but a modified AES algorithm has been incorporated in this application which makes it a little different from the present AES algorithm. The following steps depict it all:

1) Initially an ASCII matrix of the value inputted for creation of the QR code is built.

2) Then an instance of the AES algorithm is created using Java package.

3) Thirdly a cipher instance involving CBC/PKC5 padding is built.

4) Then the cipher is merged with the created instance of the AES algorithm.

5) Then the ASCII matrix is mixed with the multidimensional-bit matrix of the QR code.

6) Then the (modified) cipher is applied to the resultant matrix in order to generate and output the resultant, encrypted QR code.

C. Pseudo Code for AES algorithm

The algorithm used for encrypting and decrypting the data stored in QR codes in our paper is Advanced Encryption Standard (AES). There are many algorithms proposed like Data Encryption Standard, Triple Data Encryption Standard (Triple DES), Blowfish etc. but the best suited algorithm for this paper is AES algorithm [8]. Although this paper uses AES algorithm but a modified AES algorithm has been incorporated in this application which makes it a little different from the present AES algorithm. The following steps depict it all:

Step 1: A raw array of the ASCII matrix of the value inputted for creation of the QR code using Charset.forName ("US-ASCII") function is built.

Step 2: An instance of the AES algorithm skeySpec using Java package named SecretKeySpec found in javax.crypto.spec package is created.

Step 3: A cipher instance of AES/CBC/PKCS5Padding using Cipher class located at javax.crypto package is created.

Step 4: Cipher with created instance of the AES algorithm is merged.

Step 5: ASCII matrix with the multidimensional bit–matrix of the QR code which is done using java.awt.Color, java.awt.Graphics2D, com.google.zxing. BarcodeFormat, com.google.zxing. BinaryBitmap packages is mixed.

Step 6: Modified cipher is mixed to the resultant matrix in order to generate and output the resultant, encrypted QR code.

D. Pseudo Code for QR code generation

Step 1: Input data to be stored in QR code.

Step 2: Input the size of the data.

Step 3: Store data in form of bitmatrix (data, size).

Step 4: Encrypt the data stored in matrix using AES algorithm.

Step 5: Generate the encoded QR code using the bitmatrix (data, size) and library function (Zxing) of QR code generation.

Step 6: Display the result.

E. Pseudo Code for Reading of QR code

Step 1: Integrate the webcam using webcam packages provided by java.

Step 2: Create panel using panel.setPreferredSize(size) and set layout for webcam using its resolution.

Step 3: Create text area using textarea.setPreferredSize (size) to display the hidden data after scanning.

Step 4: If webcam is open, get image using webcam.getimage().

Step 5: Read the image using the library function of zxing *i.e.* multiformatreader.

Step 6: If the data is encrypted then decrypt using AES decryption algorithm.

Step 7: Display the hidden data in the text area.

After research, the comparative study of different encryption algorithms on the basis of different parameters is tabulated in Table 1.

IV. Analysis of QR for Secured Question Paper Generation

A. Functional Analysis

This application can be used for various purposes such as secured transmission of question papers that is shown in this paper, crime department investigators can use this application secured communication and transmission of important data such as criminal details, this application can also be used for secured transmission of credentials within an organization. With advancement of technologies this application can also run on mobile phones thus increasing its applications. Several other applications exist to which this QR code may be a revolutionary replacement to existing solutions [12-14].

B. Risk Analysis

Since risk is a part of every paper so there is a need to analyze the risks that can occur in various parameters. Risk has two parts: one is the probability that risk will occur and second is if risk occurs what can be the consequences. Risks are hard to spot so it increases the use of risk analysis so that a person can work properly on his/her plans. For analyzing the risks first it is necessary to identify the possible risks and then think of the possible mitigation strategies. Risk analysis helps in managing the paper very well. Table 2 shows the risk analysis and mitigation strategy of this application.

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.

TABLE I. COMPARATIVE STUDY OF [6, 10 AND 11]

Algorithm	Key Length (bits)	Key Searched (per second)	Block Size (bits)	Cipher Text	Security	Complexity
DES	56	1 billion	64	Symmetric	Low	Complex
Triple DES	168	$1x10^{23}$	64	Symmetric	Low	Complex
AES	128-256	$1x10^{23}$	128	Symmetric	High	Complex
RSA	Variable	Variable	Less than or equal to log2(n)	Asymmetric	High	Simple

TABLE II. RISK ANALYSIS

RISK	RISK LEVEL (L/M/H)	LIKELIHOOD OF EVENT	MITIGATION STRATEGY
Paper Size	Medium	Less	We moderate this risk through keeping the scope of the paper constrained so that we can develop it on schedule.
Complexity	High	More	We mitigate this risk through attaining a clear understanding of the application objectives, its complete functional workflow, the logical framework and final outcome that we aim to achieve.
Technology	High	More	We alleviate this risk by learning the technological fundamentals and concepts thoroughly which are used directly in the implementation of its modules.
Scheduling	Medium	Less	We diminish this risk by formulating milestones clearly indicating the completion of specific executable modules involved within our paper.
Cost / External Dependencies	Low	Less	In order to mitigate this risk and save any hidden costs, we aim to attain a clear technical and functionality visibility so that the actualization of any low level or intensity of risks does not cause maltreatment to the paper and we are able to suppress them conveniently.

REFERENCES

[1] Karthic.S and Velmurugan.A, "Android Subuurnban Raliway Ticketing with GPS as Ticket Checker", in 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies, Ramanathapuram, 2012, pp. 63-66.

[2] Affan Idrees, Zahid Iqbal and Maria Ishfaq, "An Efficient Indoor Navigation Technique to find Optimal Routes for Blinds Using QR codes", in 2015 IEEE 10th conference on Industrial Electronics and Applications, ICIEA,Auckland, 2015, pp. 690-695.

[3] Vasileios Y fantis, Panagiotis Kalagiakos, Chrysanthi Kouloumperi and Panagiotis Karampelas, "Quick Response Code in E-Learning", in 2012 International Conference on Education and e-learning Innovations, U.S.A, 2012, pp. 1-5.

[4] Pankaj Virulkar and Avinash Bhute, "Application Based Advertisement publishing by using Wi-Fi and QR codes", 2015 International Conference on Green Computing and Internet of Things, ICGCIot, Noida, 2015, pp. 1316-1321.

[5] M.Filipovic Tretinjak, "The Implementation of QR codes in the Educational Process", in 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO, Opatija, 2015, pp. 8333-835.

[6] Somdip Dey and Asoke Nath, "Confedential Encrypted Data hiding and Retrieval Using QR Authentication System", in 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 512-517.

[7] Katharina Krombholz, Peter Friihwirt, Thomas Rieder, Ioannis Kapsalis, Johanna Ullrich and Edgar Weippl, "QR code Security-How Secure and Usable Apps Can Protect Users Against Malicious QR Codes", in 2015 10th international Conference on Availability, Reliability and Security, ARES, Toulouse, 2015, pp.230-237.

[8] Akshay Desai, Krishna Ankalgi, Harish Yamanur and Siddalingesh S. Navalgund, "Parallelization of AES algorithm for Disk Utilization Using CBC and ICBC modes", in 2013 Fourth International Conference on Computing, Communications and Network Technologies, ICCCNT, Tiruchengode, 2013, pp.1-7.

[9] Fei Shao, Zinan Chang and Yi Zhang, "AES Encryption Algorithm based on the High Performance Computing of GPU", in Second International Conference on Communication Software and Networks, ICCSN'10, Singapore, 2010, pp. 588-590.

[10] Mohammed A. Saleh, Nooritawati Md. Tahir, Ezril Hisham & Habibah Hashim, " An Analysis and Comparison for Popular Video Encryption Algorithm", in 2015 IEEE Symposium on Computer Applications and Industrial Electronics, ISCAIE, Langkawi, 2015, pp.90-94.

[11] Sangita A.jaju and Santosh S. Chauhan, "A Modified RSA Algorithm to Enhance Security for Digital Signatures", in 2015 International Conference and Workshop on Computing and Communication, IEMCON, Vancouver, 2015, pp. 1-5.

[12] Praveen K Gupta, Nitin Rakesh, "Different job scheduling methodologies for web application and web server in a cloud computing environment", 2010 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), pp. 569-572, 2010.

[13] Nitin Rakesh, Vipin Tyagi, "Failure recovery in XOR'ed networks", 2012 IEEE International Conference on Signal Processing, Computing and Control (ISPCC), pp. 1-6, 2012.

[14] Kinjal Shah, Gagan Dua, Dharmendar Sharma, Priyanka Mishra, Nitin Rakesh, "Transmission of Successful Route Error Message (RERR) in Routing Aware Multiple Description Video Coding over Mobile Ad-Hoc Network", International Journal of Multimedia & Its Applications (IJMA), Vol.3, No.3, 51-59, August 2011.