Implementing Security in QR Codes by using Blowfish Algorithm

Harpreet Sandhu[2], Kamesh Dubey[2]

[1](Dept of Computer Science, CT Institute of Technology & Research, Jalandhar, Punjab, India)
[2](Dept of Computer Science, CT Institute of Technology & Research, Jalandhar, Punjab, India)

Abstract: There is need of QR code to provide a security to the online transaction etc. The upcoming generation will have been developing in technology. Hence, there will be a chance of intruder to intercept the QR code which is difficult. The main purpose of this paper is to give some overview regarding the QR codes, techniques used to develop and pros, cons of QR code. There is need of QR code for many organizations. The research scholars are studying about the QR code and their vast area of usage. The different authors have shared their different views on the QR code. QR codes are useful in sharing the URLs from one user to another user with security feature. This literature review is about the techniques of QR code used for security and output is varied with every different technique used in the code generation and code detection. This review paper is about the QR codes and gives a brief knowledge about the usage, security and techniques used in QR codes.
Keywords: QR codes, PKI, Hash algorithm, RSA, SHA-1, Android studio, Cryptography, Stagnography .

I. INTRODUCTION

In these days, QR codes are seeing the codes on every object like flyers, magazines etc. The user can easily spot these QR codes as there are most of the 2D barcodes. With the help of QR code, the user of a smartphone can interact with security to the websites. The QR code has capabilities to extends the data at disposal to any physical object and create an interactive digital extent to digital marketing. The QR codes are the one through which the user can access the content at the faster as compare to another source.The barcodes support encryption and decryption of the data. The text languages are inserted into the black box with the help of a tool or the specified algorithms. The upcoming generation is technology biased and the user will share more information as compared to current situations. For the generation of QR code, there are major 4 steps. There is the presence of many code generators. The user can select any of the generators. Then enter the design and link the text to the code. The third step is to check whether the QR code is according to the user or not. The last step is to track and analyze the performance. After the completion of all the steps, the user can share the code with the user as they needed. The QR code stands for Quick Response and major they are black in color. But with the development of technology, the user is able to create a bar code on color base also. The first bar code founded was in Japan. The first QR was generated for the automotive industries, marketers and adopted barcode because of their large storage of information within a single box of black. The QR can be viewed with the help of smart phones. The barcodes are easily present at any place like markets, on products etc. The QR codes do not require a special device or gadget to get a scan. A simple smart phone is able to scan the barcode

Fig 1: Samples of QR code

Security in QR codes: Security of QR codes is big matter because they conceal the information in dots so it is hard to give more security to them. But this security is possible in many ways like providing by Steganography and Cryptographic techniques. By applying Encryption/decryption technique we attain more security. There are many malicious QR codes which look like the same but they threaten the security. Similarly there are some legitimate users who are unable to detect these types of attacks. Attacks possible only in case of malicious codes. There are many techniques which gives the security to these codes as like by providing tracing

codes, by authorization methods, by affixing the information, by providing benefits in digital education system, by using AES and DES, security against malwares and by embedding encrypting techniques etc.

II. LIFE CYCLE OF QR CODE

The life cycle of a QR code canbe fragment into five phases: Encoding, Distribution, Code reading, Action and Expiration.
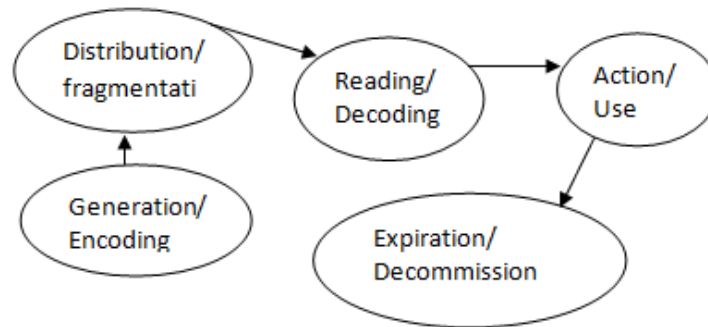

Fig 2: Life cycle of QR Code

III. OBJECTIVES OF PAPER

The objective of the paper is to study and designing of a such a technique which will help to encrypt the image file and the user can send the encrypted file to receiver side without fear. The new technique will help to insert a code into the QR code. This will invalidate the any attack on the mobile phone.

1. To study basic life cycle of QR code.
2. To study and analyze the security issues in quick responses.
3. To research and study of working of mobile phone applications.
4. To analyze the malicious QR code attacks along with QR code security issues.

IV. LITERATURE REVIEW

Nishant Goel author briefs us about the QR codes that are used in current generation. This paper provides information about the security issues that are present in scanning of QR code. The different vulnerable attacks mentioned in the paper are phishing, pharming, manipulation and exploitation. The author says that the security flaws present in the QR codes can make a big impact on the average user who uses QR codes daily. The QR codes are 2-D bar codes that decrypt the information from the black square that are placed inside the white box. The QR codes can be 1-D and 2-D. The author discusses the three steps which are using during the decryption of code. In the first step, they read raw bits from picture and perform error correction. In the second step, it interprets the content and placed raw data into formatted objects. Third steps include the action performed on related data. The AES is discussed in the paper and also provides a clear difference between AES and DES. From comparison, author proved that the AES is better than DES. Paper also proposed about the different techniques for code generator. In the end, author proposed about the different ways used to secure a QR codes by using AES. The author also states that if the QR code consist of vulnerable information then it will not have processed by which the user will be prevented from virus Trojans. The user also discussed about the approach by which the response time can be decreased for fast processing.

Rishabh Dudheria the authors evaluate the different features and effectiveness of security in QR codes. There is chance of security threat like phishing and malware attacks. The attacks come while sharing of URLs to other user. The applications are developed by which can scan the QR codes and combat the attacks. The author is discussing about the current status of QR code security. The authors have founded that the applications merely present the URL which are encoded in a QR code rather than validating the URL to database. However, some of the applications does not support basic security features was mentioned by the author in this paper. The author has tested the two different QR codes with different types of attacks like benign, phishing and malware. After the testing, the author founded that the application provides limited protections against the rogue URLs. With the help of paper, the author has discussed proposed about the design recommendations. There is table consist of different application present in Google play.

The author has also discussed about the different techniques used for protection against the malware, phishing etc. The authors also discussed about the design implementation of QR codes. The recommendations are regarding to secure the applications. The different fields like settings, website analysis, URLs have been

discussed by the author in the paper. Hence, the QR code is growing day by day and major use of QR code is sharing of website URLs to avoid malware attacks. The QR codes can be misused by the attacks which will affect the user stated by the author. Hence, the author also discussed about the advantages, disadvantages etc. in the paper.

Xiang Zhang author discussed about the importance of QR codes in current generation. The QR codes encodes the alphanumeric characters which is set of information is encoded with the information. The author also mentioned some of the techniques to detect the QR codes faster. The paper consists of different set of novel approaches used for detection of codes. The author also proposed a new method of detection of QR codes and the design is according to the experimental results that the author founded. The author also discusses some important facts of QR codes with design explanation. The method discussed here is component aggregation method which is divided into three phased. The FIP candidates are detected in first stage and second stage consists of geometrical restrictions which are used to confirm the presence of QR code in the box. The author proposed its own method named as Zbar and Zxingwhich they had upgraded the previous algorithm. The new method is fast and is free open source bar codes and used as detection of QR codes. The paper consists of review of component-based detection approach and proposed a new approach. The first stage in Component based detection is FIP detection and second stage implements restrictions. The author also states that the combining of methods can improve the detection rate. The methods which are complement are used to combine. As the experimental result shown by the author, there can be improve in detection rate.

Aayushi Malhotra the author discusses the multilevel security that can be provided to online transaction with different methods. This paper consists of different current securities present to secure the online transaction. As the online services are utilization is more in the current generation, the author have proposed a new method to provide security against the current securities present in the market. The author had also briefed about the internet banking propose along with pros and cons. The paper also consist of different security features that should be present in any protocols. The features like authentication, Encryption, Auditing, Integrity, Non Repudiation is most needed. There is brief introduction to current existing security system like OTP, QRP code, Biometric, SMS Banking. Due to lack of security, the attackers is able to forge this securities system easily. Hence, the author proposed a method which is a combination of two different technologies like digital water marking and QR code. The method generated for the user who generally save their passwords in the browser. With the help of new approach, there will be a use of different security level through which the risks are avoided. This research paper has major focus on internet banking. The author proposed a new method by which the people can easily make transactions online without fear at any time. The authentication method which provides a better security and is convenience to use. The author proved with the help of experimental result that new proposed system is better than old securities system.

Nandhini **S.** the author had discussed about the embedded color QR codes used on LOGOS. There are many organizations which have implemented logo using QR codes. The paper consists details of an embedded technique which are implemented on color logos. A paper is created using a tonal mask and the errors occurred are corrected by RS code. A DWT is performed and embed the technique with the watermark and proper embedded technique is used to create QR codes are converted into equivalent components. The embedded image is created by joining RGB components into it. The author has analyzed and compared the input with image. This paper is about a well-organized technique which is used for embedding the color QR codes on color images. The result is 95% and has a good recognition rate with better accuracy. The author had stated that the colored QR code having a better capability to get recognized then the black and white QR codes. The final QR code is generated by using wavelet transform. It is developed by concatenating of blocks with black-white image.

Sheshang D. Degadwala authors explains about the two-way privacy in QR code and VCS. The author defined QR code as two dimensional barcode which is used by many organizations for security purpose and mentioned that QR code look likes noisy structure. The QR codes are generated by conversion to text form into QR code. This research paper consists of information of a method which explains the appearance of QR codes. This paper also includes information regarding the text information which is hide in QR code. VCS technique is used to share conversion of QR code. The text to share is not an easy task according to author as there is 2-level privacy. This paper also consists of two sharing methods: - single sharing and multiple sharing. The author had examined the different visual cryptography schemes and execution is accessed with respect to 4 criteria according to the author which are mystery images, pixel expansion and picture design. The author has recommended that arrange of QR code should be with the secondary security such as with picture encoding, information embedding and data extraction. The second stage will provide a chance to shares.

V. PROBLEM DEFINATION

This paper resolves about the issue of usage of QR codes. This paper is about the QR code importance in various fields. The QR code is using for the past 40 years. It is important to know about the usage of the security features used in QR code to provide a security to online transactions and there are many advantages of the QR codes. The above are some review of the different papers writer by the different authors. They have researched on QR codes. They shared their knowledge about the QR codes in their respective papers.

VI. PSEUDO CODE FOR DESIGNED ALGORITHM

Code for sender side:
Step 1: Take a simpleimage.
Step 2: Convert above image into blocks of 32 bits.
Step 3:Then blocks aredivided into 8 bits of 4 blocks.
Step 4: Applying Blowfish algorithm on blocks.
Step 5: It collects the pixels of image and send to VHDL for encoding and decoding.
Step5: Generating QR code of above output.
Step 6: Stop.

Code for receiver side:
Step 1: Input of encrypted image.
Step 2: Matching the image pixel with encrypted image.
Step 3: Decryption of image with blowfish algorithm.
Step 4: The image is decrypted and will be shown to the receiver.
Step 6: Stop.

VII. RESULTS

The results are measured in the tool MATLAB. The MATLAB tool is used to analyze the code. The reason to use MATLAB is to run the code easily. The image is taken like as shown in below, the image we have taken is the actress image.

Fig 3: - The Sample Image.

The code is written in MATLAB language. The code is run after compiling the code. The below screen shot the 4 different blocks consist of original image, resized image, black and white image and original black-white image.
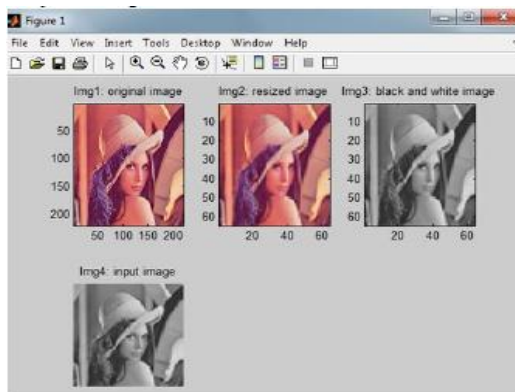

Fig 4: Four different blocks of original image

The below screenshot consist of the encryption of image done by the MATLAB.
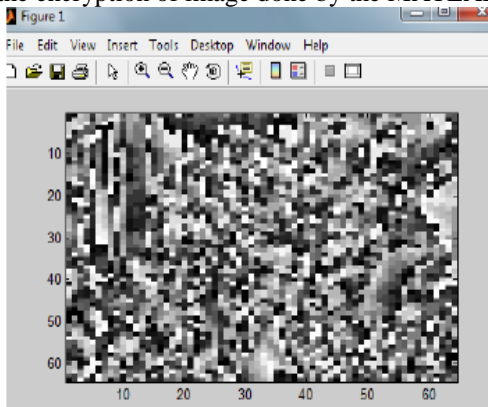

Fig 5: Encrypted Image

The image below is the QR code generated for the image we have used for the encryption of the data. The QR code is sent to the receiver and receiver can scan the image by their phone or QR code based devices.

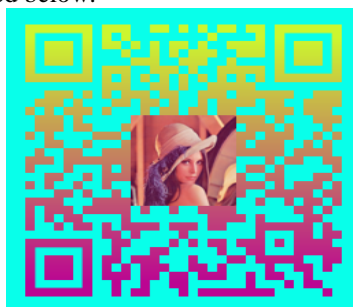Fig 6: QR code

The color image of QR code is generated below.

Fig 7: Colored QR code

VIII. FUTURE DIRECTION

From the review of above paper and the result we have found in this research paper, it is clearly shows that there are many security parameters left which are still needed to add in the encryption and decryption process of image. The increase of security on image will help to make more secure of using QR codes in the public place. The future of QR codes security can be increase with the help of techniques used in Steganography like Blowfish algorithm etc. The storage of image can be also increase to make space for the codes used for the images. The increase space will help the user to store the values of pixel and can use later according to need.

IX. CONCLUSION

The major goal of this review paper is to give a small brief knowledge about the usage of QR code. AS the QR code is one of essential technology to make the security high for the online transactions. There are many different QR code 1-D and 2-D whereas 2-D is considered as the best for the security. There is different

encryptions security which is AES and DES. Due to more advantages of AES over DES, the AES is preferred. The various papers of different authors had been reviewed for a better understanding of the paper. By reading above paper, the user is able to understand about the QR ode, its advantages and disadvantages. The QR codes can become more secure if the QR codes are embedded in colors. The QR code is a future need to make security higher for online transactions and sharing of URLs online.

REFERENCES

[1]   N. Goel, "A Way to Secure a QR Code: SQR", *International Conference on Computing, Communication and Automation*, 2017.

[2]   R. Dudheria, "Evaluating Features and Effectiveness of Secure QR Code Scanners", *2017 International Conference on Cyber-Enabled Distributed Computing and   Knowledge Discovery (CyberC)*, 2017.

[3]   A. Mishra, "Multilevel Security Feature for Online Transaction using QR Code & Digital Watermarking*", International Conference on Electronics, Communication and Aerospace Technology,* 2017.

[4]   N. .S, "Performance Evaluation of Embedded Color qr Codes on Logos", *International Conference On Science Technology Engineering and Management*, 2017.

[5]   S. Degadwala, "Two Way Privacy Preserving System using Combine Approach: QR-code & VCS*", International Conference on Innovations in Power and Advanced Computing Technologies*, 2017.

[6]   X. Zhang, H. Luo, J. Peng, J. Fan and L. Chen, "Fast QR code detection", 2017 *International Conference on the Frontiers and Advances in Data Science (FADS),* 2017.