International Journal of Psychosocial Rehabilitation, Vol. 25, Issue 02, 2021
ISSN: 1475-7192

PRODUCT AUTHENTICATION USING QR CODE WITH THE HELP OF RSA ALGORITHM

Dr.Pankaj Kumar, Kumar Raghav*
Associate Professor, SRM College of Engineering & Management, Lucknow
Associate Professor, BBD University, Lucknow

Abstract

The advent of online shopping has led to a surge in ecommerce websites offering products from well known brands at very competitive prices. However, the cases of fake products and duplicity have also seen an increase in recent years, because of lack of proper mechanism to ensure authenticity of the products, whether purchased online or from a physical shop. In spite of the availability of a number of techniques and technology, there is still no means to check the delicacy occurring due to copying product information and generating fake QR codes, barcodes etc and using on fake or duplicate products. In this paper, we propose a methodology for product authentication by using the RSA algorithm on QR code. RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key...

Keywords: authentication, QR code, RSA algorithm, encryption

1. Introduction

In today's scenario, the authenticity of the product is a very important process because due to this we can buy a genuine product from the organization. Quick Response (QR) code is used for product information contains data in both vertical and horizontal directions, whereas a bar code has only one direction of data, usually the vertical one. QR Code can also correspondingly hold more information and are easily digested by scanning equipment, and because it has potentially twice the amount of data as bar code, it can increase the effectiveness of such scanning. Further QR Code can handle alphanumeric character, symbol, binary, and other kinds of code. QR Code also has an error-correction capability, whereby the data can be brought back to full life even if the symbol has been trashed. All of these features make a QR Code far superior to bar code. Fig.1 shows a QR code and Error Correction (EC) levels. There are four levels of error correction; Low (L) which can tolerate up to 7% damage, Medium (M) can tolerate up to 15% damage, Quartile (Q) can tolerate up to 25% damage and High

(H) can tolerate up to 30% damage. The reason why the Low (L) error correction level is preferred is that the High error correction levels raise the percentage of code word used in error correction thereby decreasing the amount of data that can be stored in the code [1].

Error Correction Level	Error Tolerance
Low (L)	7%
Medium (M)	15%
Quartile (Q)	25%
High (H)	30%

figure1: QR code and Error Correction Level

but main drawback of this QR code is that we can easily design the QR code which is placed in the product because with the help of QR code scanner we can scan the QR code and know the information which is hiding in the QR code. After knowing the information of QR code we can easily generate the same QR code with the help of QR generator. After generating the same QR code we can place this QR code on fake product. To overcome this we can use RSA algorithm on QR code.RSA involve a public key and private key. The public key can be known to everyone it is used to encrypt the messages. Message encrypted using the public key can only be decrypted with the private key.

This paper is organized as follows section 2 is literature review. Section 3 is about the RSA algorithm. Section 4 presents our proposed methodology for product authentication. Section 5 present analysis and experimental result through mat lab. Section 6 proposed our future research proposal and finally conclusions appears in section 7.

2. Literature Review

- Sayantan Majumdar et al. [2] propose a system in which they combine cryptography and mobile computing together. They developed a secured scheme in which digitally sign small file and encode it to a QR code to widely share the information over the network. Here, first the information is digitally signed using RSA algorithm, then encoded into a QR Code. A simple android app is developed in order to obtain the information from the QR Code and to check the authenticity of the decoded information.

- K.Naresh and prathibha N. Pillai [3] proposes a system in which they are using QR code which represents the hidden image and sent the QR code by encryption and decryption. They proposed a novel algorithm, in which the sender has two keys (public and private keys) and the user is provided with only one key (public key) by using RSA algorithm. Thus, the user can only see the data and he can't modify the data.

- Somdip dey [4] presents a new technique of using QR codes in the field of cryptography. The new method is achieved by entering the message along with a password. This password will generate a secret code, which will be added to each digit or alphabet in the numbers or text entered in the message (which is needed to be encrypted) and generate the first phase of encryption. That newly generated encrypted message will again be encrypted using various other methods to generate the final encrypted message.

- Basheer N.Ameen and Sawsan K.Thamer [5] introduced the encryption technique by inverting in two special selected areas to generate one ciphered QR code as in sender side n the present work the authors have introduced the encryption technique by inverting in two special selected areas to generate one ciphered QR code as in sender side In this encryption method authors have used bit-manipulation, byte reshuffling and generalized this method.

- Okfalisa et al [6] propose the system by implementing AES and QR Code algorithm, the information contained in the photo-scan of the certificate can be authenticated. The results of the scan are encrypted by using the legalized code in AES Algorithm. The code will be translated using the QR Code and matched to the data contained in the server system. The system will confirm whether the certificate is original or not.

- Priyanka Gupta et al [7] in this paper, FPGA implementation of 1024 bit RSA encryption and decryption is presented. For encryption, computation of modular exponentiation for 1024 bit size with accuracy and efficiency is needed and it is carried out by repeated modular multiplication technique. For decryption, L-R binary approach is used which deploys modular multiplication module.

- Supyiya chavan et al[8] In this paper, they introduced a new technique, where the resume of a candidate will be encoded in QR [Quick Response] Code in encrypted form, so that if an hacker tries to change the data in the resume then he cannot do that. This is because; the encryption key is unknown to him. They are using TTJSA algorithm method for encryption and decryption purpose.

- Md.Salahuddin Ahamed,Hossen Asiful Mustafa[9] propose in his paper, a novel SQRC system which will allow sharing authentic personal confidential information by means of QR code verification using RSA digital signature algorithm and also allow authorizing the information by means of QR code validation using RSA public key cryptographic algorithm.

- Vitalii Susukailo & Yuriy lakh[10] providing in his paper about secure access control systems using cryptosystem based on RSA algorithm and pseudorandom number generator. The task was to develop an application encrypting information to provide information security for access control systems using encryption techniques in QR-code technology.

- Abhijeet Mendhe, Deepak Kumar Gupta & Krishna Pal Sharma [11] proposed a 3-layered architecture for securing message sharing mechanism by using QR code image in one layer. This architecture utilizes the empirical and strategic use of cryptography and steganography techniques.

3. RSA Algorithm

- Cryptography is one of the reliable techniques for security and secrecy of data.
- RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages.
- RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.
- The keys for the RSA algorithm are generated in the following way:

  a) Choose two different large random prime numbers p and q.

  b) Calculate n=pq

  n is the modulus for the public key and the private keys

  c) Calculate the totient: Ø (n) = (p-1) (q-1)

  d) Choose an integer e such that $1<e<Ø(n)$, and e is co-prime to Ø (n) i.e. e and Ø (n) share no factors other than 1

  e is released as the public key exponent

  e) Compute d to satisfy the congruence relation $de \equiv 1 (\text{mod } Ø(n))$

  d is kept as the private key exponent

  f) Public key is (n, e), Private key is (n, d)

  g) Encrypting Message

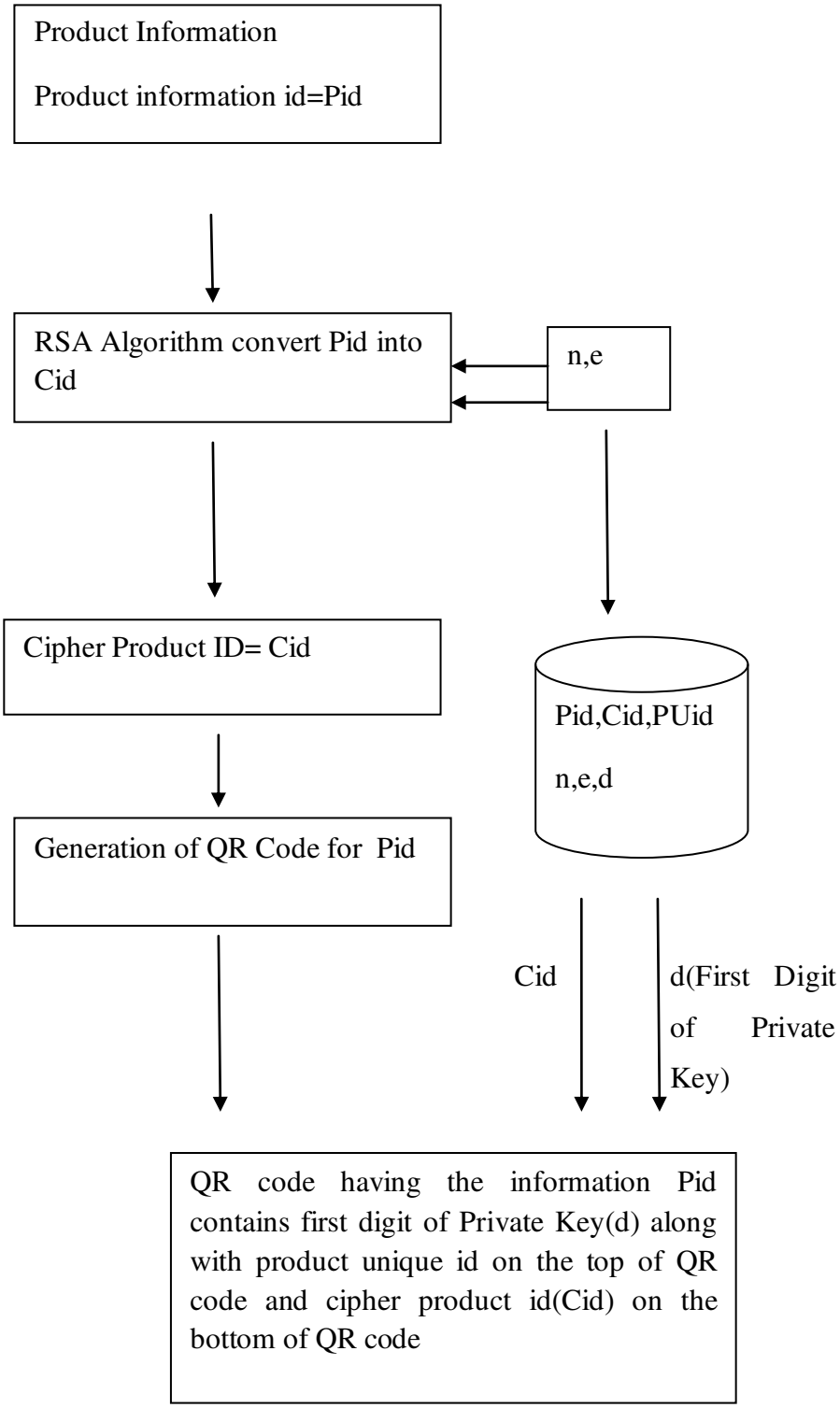
  $C=M^e \text{ mod } n$

  Where M is the message which is to be send and C is the cipertext

  h) Decrypting Message

$M=C^d \bmod n$

4. Proposed Methodology



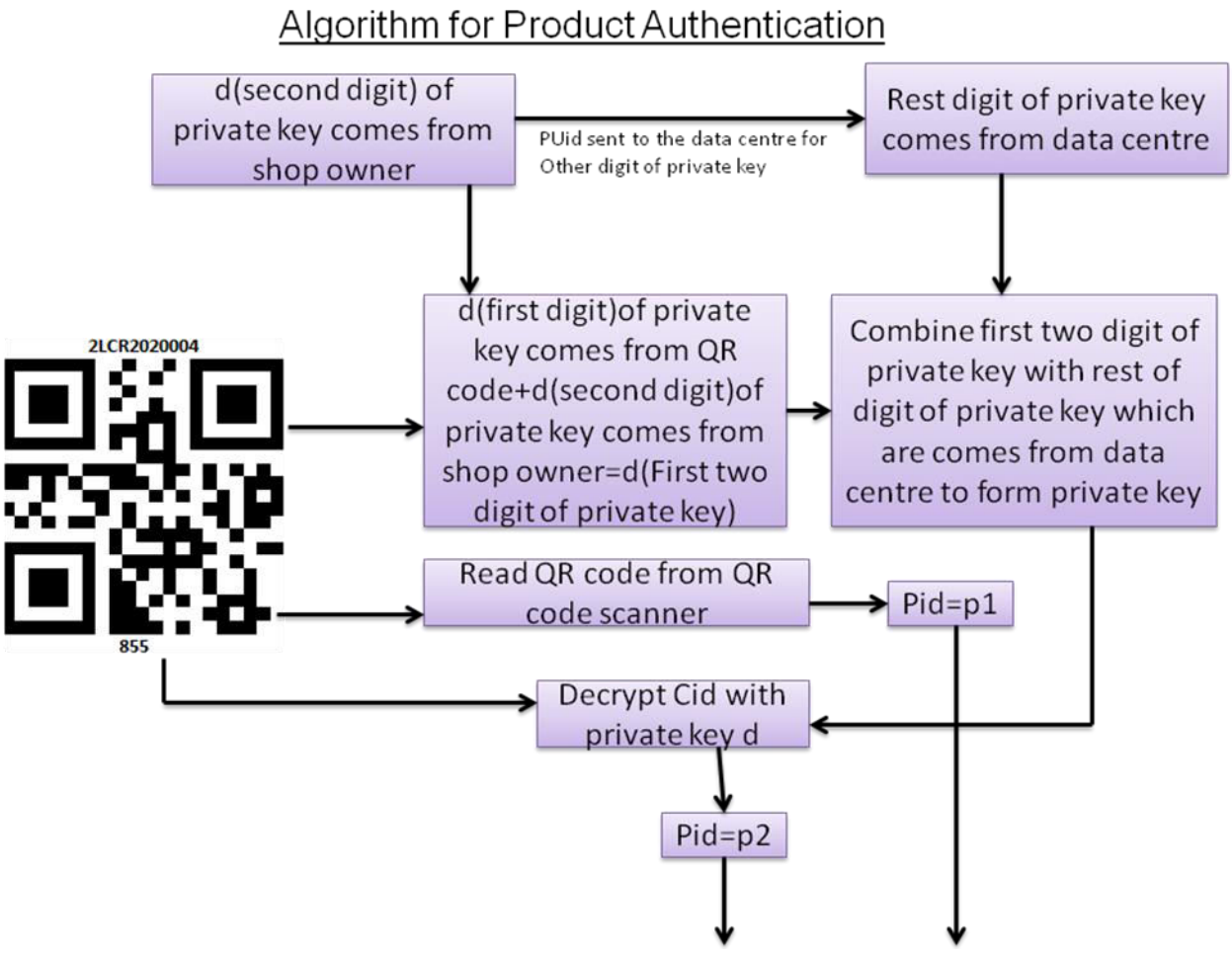
- Product Information Id(Pid) is a numeric digit. This Pid is store in the data base of data centre. Regarding this unique Pid all the product related information is stored in data base.
- We have to applied RSA algorithm with the help of MAT Lab on this Pid to generate cipher product id(Cid).
- Database which is maintain in the data centre contain Product information id(Pid). Regarding this Pid all the product related information is stored in the database. Database also contain cipher product id(Cid), Product Unique id(Puid), and the RSA related information like n,e,d(private key).
- Generate QR code of Pid with the help of QR code generator.
- On the top of QR code we have to place first digit of private key along with product unique id(PUid).
- On the bottom of QR code we have to place cipher product id (Cid)
- This whole QR code is placed on the product so that we have to authenticate it.

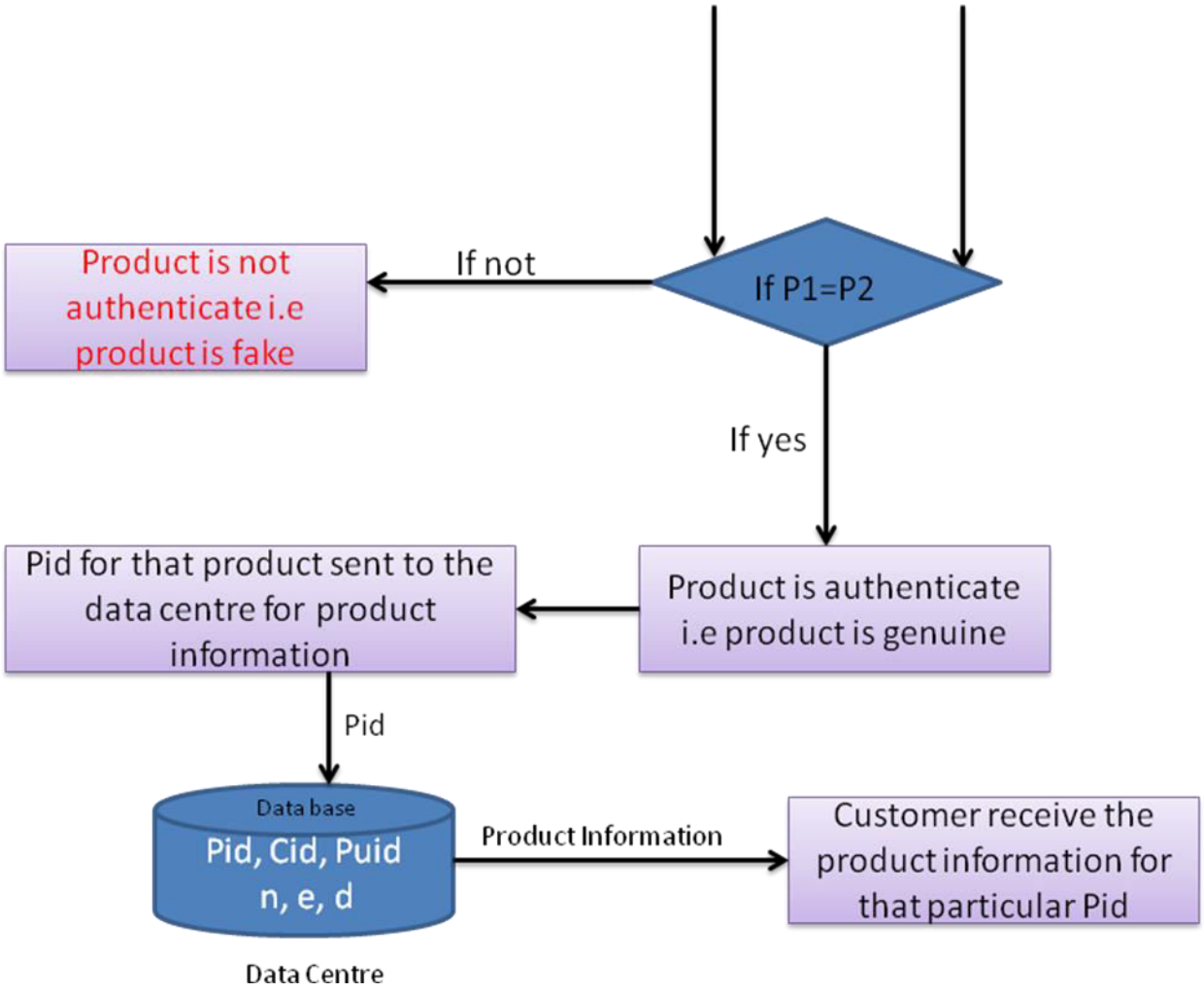
5. Analysis and Experimental result from mat lab

Figure 1(a)

Figure 1(b)

- In the fig 1(a) above a QR code is generated with the help of QR code generator having Pid=123 are stored in it.
- Product Information id (Pid) is stored in the database of data centre contains all the product related information i.e. Pid is serving as a primary key.
- With the help of RSA algorithm we can find Cid.
- Upon applying the formula for encryption, $C=M^e \bmod n$. we have to calculate Cid. For Pid=123,n=3233,e=17 Cid is calculated which is equal to 855.
- With the help of RSA algorithm we have to calculate private key(d).For p=61,q=53 and e=17 the value of private key comes to be 2753.
- In the fig 1(b) first digit of private key which is 2 along with product unique id(PUid)(LCR2020004) is placed on the top of QR code and ciper product id(Cid) is placed on the bottom of QR code.





- Take a first digit of private key from the top of QR code. This QR code is placed on the product. This time it is 2 from 2LCR2020004.This key is placed along with product unique id (PUid) which is LCR2020004.
- Take a second digit of private key from shop owner .This digit of private key is stored in shop owner's database. With the help of PUid shop owner can easily find the second digit of private key which is stored in the database. From the above data this time it is 7.
- Combine first digit and second digit of private key. From the above it is 27.2 is coming from first point and 7 is coming from second point.
- Rest digit of private key come from database of data centre which is easily accessible with the help of PUid.This time it is 53.

- Combine 53 with 27 to form 2753.This is a private key of a product.
- Decrypt Cid, which is placed on the bottom of QR code, with the help of private key (2753) .After decryption the value, comes to be 123.
- $855^{2753} (\text{mod } 3233) = 123$.Assign 123 to p1 i.e.p1=123.
- Scan QR code with the help of QR code scanner. The value comes to be 123 which is assign it to p2 i.e.p2=123.
- If p1=p2 then product is authenticate and if not then product is not authenticate.
- If product is authenticate i.e.p1=p2 then send Pid of this product to the data center. Regarding this Pid data centre send all the product related information to the customer

6. Future Research Proposal

We can also authenticate the product with the help of visual cryptography. We can generate two shares of QR code image. One share is placed on the product and other is in the data centre. Upon taking the photo of first share, which is placed on the product from smart phone, and then send to the data centre. Superimposing both the share in the data centre and gets back the QR code image. After scanning the QR code with the QR code scanner we will get the product information. This product information is send back to the customer for authenticity of the product.

REFERENCES

[1] J. Shieh, J. Zhang, Y. Liao and C. Lin, "Enhancing the Recognition Rate of Two-Dimensional Barcodes Image and Applications," In Proc. Of IEEE 4th International Congress on Image and Signal Processing, Vol. 3, PP. (1567-1571), (2011)

[2] Sayantan Majumdar,Abhisek Maiti,Biswarup Bhattacharyya,Asoke Nath" A new encrypted data hiding algorithm inside a QR code implemented for an android Smartphone system:S_QR system"International journal of Innovative Research in advanced Engineering,volume2,Issue 4, April 2015, Pages 40-46.

[3] K.Naresh and prathibha N.Pillai" QR verification system using RSA algorithm" International journal of innovation and scientific Research, Volume 10, ISSN 2351-8014 No. 2 Oct 2014, Pages 433–437.

[4] Somdip Dey"SD-EQR: A New Technique to use QR Codes in Cryptography"International journal of Information Technology & Computer Science (IJITCS), may 2012.

[5] Basheer N. Ameen and Sawsan K.Thamer " A novel method for Ciphering a Message Based on QR code"International journal of scientific & Engineering Research,Volume 8,Issues 4,April-2017.

[6] Okfalisa,Novi Yanti,Wahyu Aidil Dita Surya Amany Akhyar & Frica A Ambarwati"Implementation of advanced Encryption Standard(AES) and QR code Algorithm on Digital Legalization System" ICENIS E3S web of conferences, 2018,https://doi.org/10.1051/e3sconf/20187313009.

[7] Priyanka Gupta,Sandeep Saini & Kusum Lata" Secure QR codes by RSA on fpga" International Conference on Advances in Computing,Communications and Informatics(ICACCI),Dec 2017, https://ieeexplore.ieee.org/document/8126188.

[8]Supyiya chavan,Sujata Gadakh,GholapKanchan,Sorte Surabhi & D.V Shinkar"QR code Authentication system for confidential Encrypted data hiding and retrieval(Decryption)"International journal of Advanced Research in computer and Communication Engineering, volume 5,Issue 4,April 2016.

[9] Md.Salahuddin Ahamed Hossen Asiful Mustafa "A secure QR code System for sharing personal confidential information"International Conference on Computer,Communication,Chemical,Materials and Electronic Engineering(IC4ME2),march2020,https://ieeexplore.ieee.org/document/9036521.

[10] Vitalii Susukailo & Yuriy lakh"Access control system based on encryption in QR code technology" ieee 4th international Symposium on wireless systems within the international conferences on intelligent data Acquisition and advanced computing system(IDAACS-SWS),November 2018,INSPEC Accession Number:18248813.

[11] Abhijeet Mendhe,Deepak Kumar Gupta & Krishna Pal Sharma"Secure QR code based system using Cryptography and stegamgraphy" First International Conference on Secure Cyber Computing and Commuication(ICSCCC),May 2019,INSPEC Number:18637363.