J. Integr. Sci. Technol.2023, 11(4), 568

Article

Journal of Integrated
SCIENCE & TECHNOLOGY

Secured authentication of online documents using visual secret sharing on QR code

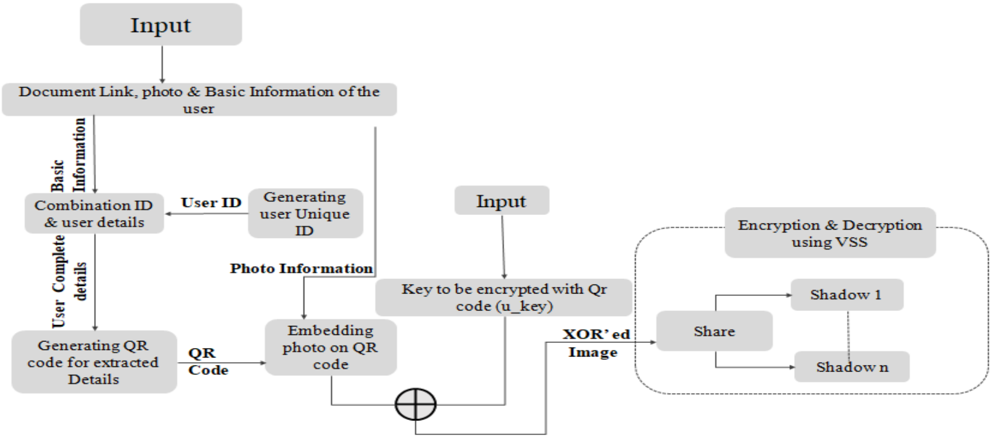
Jalaja Valisireddy[1], Kotte Amaranadha Reddy[2], R. Elumalai[3], L. Narendra Mohan[4], G.S.G.N. Anjaneyulu[3*]

[1]Mathematics, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupathi, India. [2]Mathematics, Kalasalingam Academy of Research and Education, Krishanankoil, Vlrudhunagar(d), Tamilnadu. India [3]Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore, Tamilnadu, India. [4]Mathematics, Sri Venkateswara College of Engineering, Tirupathi, India.

Received on: 22-May-2023, Accepted and Published on: 05-July-2023

ABSTRACT

Privacy of the confidential online documents is one of the major concerns in sharing the information at different platforms. Any methodology of security that has human interference is fully secured as long as the entities involved are ethical, otherwise, it cannot be considered as completely secure. This study is meant to use Visual Secret Sharing (VSS) on QR code. Due to the flexibility of storing complex data in QR code and the ability to split an image into non-readable shares enhance the efficiency of this methodology. The basic notion behind this concept is that the admin will create a QR code of the user and generates a unique id. The QR Code provide the link of the document that has to be secured along with some basic information. Finally, QR code is subjected to VSS where it splits the QR code into equal shares which are distributed among the user and admin. Due to this, admin can't retrieve the document completely until and unless the other shares of the client are merged.


Input
Document Link, photo & Basic Information of the user
Basic Information
Combination ID & user details
User ID
Generating user Unique ID
User Complete details
Photo Information
Input
Key to be encrypted with Qr code (u_key)
Encryption & Decryption using VSS
Shadow 1
Share
Shadow n
XOR'ed Image
Generating QR code for extracted Details
QR Code
Embedding photo on QR code

Keywords: Secure Document Sharing, QR code, Visual Secret Sharing

INTRODUCTION

Secured documents sharing is one of the most ongoing research trend over the years where various methodologies have been proposed with vigorous evolution in each methodology. File Transfer Protocol is the first thing that comes to mind when we talk about file sharing that was proposed in 1979.[1] It is built for both bulk and single file transfers but there lots of security issues raised in FTP. Later in 1990s, file sharing is done by unstructured centralized peer-to-peer file sharing, where the individuals can be shared the files one person at a time. If central point has some failure entire network will be lost. After**,** all these proposals as a milestone,[2] in late 1996 File Transfer Protocol Secure (FTPS) was proposed which is protected by Secure Socket Layer (SSL). It comes with features of Data-in-motion encryption and client server authentication but the firewall issues still persists. Then in 2000s, decentralized file sharing system came into existence, all the connecting software considered as equal, therefore there is no central point of failure.[3] Like this lot more methodologies came into play to secure the document sharing. As a flow for this trend in this paper, a novel secured methodology is proposed with Visual Secret Sharing on QR Code**.**[4]

First Time QR codes are designed for an Automotive Industry of Japan in the year 1994. QR codes are categorized into 40 versions

*Corresponding Author: Prof. G.S.G.N. Anjaneyulu
Tel: +91-9047288639
Email: anjaneyulu.gsgn@vit.ac.in

Cite as: *J. Integr. Sci. Technol., 2023, 11(4), 568.*

based on the data that has to be stored in it ranging from 25 to 1852 alphanumeric characters.[4] Due to this advantage, QR codes are playing a huge role for information exchange even today in all most all sectors like in making payments, marketing, government sectors etc.[5] Generally the version of the QR code is assigned automatically as a part of algorithm based on the size of the data that has to be stored.[6] Along with the version, one more parameter of the QR code is Error correction level which will be one among L(Low), M(Medium), H(High) which instructs the algorithm about amount of data that has to be encrypted.

Principally, all the payment applications are using the QR codes for fast retrieval of their payment information. QR code reduces the effort of sharing the textual information manually. The pattern that has been incorporated in the QR code for storing the data is responsible for the fast retrieval of the data.[7] Another main component in QR code is, the Error Correction Code word which allows efficient retrieval of the data even when some portion of QR code is damaged.

The second component of our mechanism is Visual Secret Sharing and is a concept of sharing of images securely by dividing the original image into shades. Individual shades are non-readable until all the shades are decrypted using the counter process of the same algorithm. The advantage of VSS is that it is easier to recover the secret image by stacking a specific amount of shares without any cryptographic knowledge and computations. However, the characteristics of pixel expansion and codebook (basic matrices) design may be problematic in some situations.

MOTIVATION AND OUTLINE OF THE PAPER

Recently, several attempts have been made to secure the valuable documents either on off-line or online using digital tools. In this protocols security is based on one side, no one is secure in the extent of the confidentiality and integrity of the documents. This kind of mechanism is secure as long as the entities, who are managing this system are ethical. This motivated us to design the methodology that aims the document as dividing into shares among user and admin using VSS on QR Code.

PRINCIPLE COMPONENTS OF THE ALGORITHM

QUICK RESPONSE CODE

QR Code is a machine-readable code consisting of an array of black and white squares, typically for storing URLs or other information for reading by the camera on a smartphone. QR code generation is not as simple as a person can retrieve the information from it. It involves a set of complex steps like Data Encoding, Error Correction coding, Structuring Final Message, Module Placement in Matrix, Data Masking, Format & Version Information. A QR code will be generated after executing each and every step mentioned above and has to be executed in the reverse order, so as to get the stored information which happens in seconds.[8]

Each encoding mode for Data Encoding is designed to create the shortest possible string of bits for the characters that are used in that mode. Data encoding includes the steps like choosing the error correction level, determining the smallest version of the data, adding the mode indicator, adding the character count indicator,[9] encode using the selected mode. Breaking string based on mode and then convert into binary bits, breaking up into 8-bit code words and add pad bytes if necessary, determining the required number of bits for this QR code, add a terminator of 0’s if necessary, if necessary add 0’s to make the length multiple of 8 and add pad bytes if the string is still too short.

Module placement in the matrix is the initial step to place the data onto the QR code.[10] In brief, there will be two kinds of patterns i.e., data present in a QR code named Function pattern and Encoding Region. Components inside each pattern are represented in figure 1. A function pattern is a non-data component of the QR code that is required by the QR code detail specification, such as the three finder patterns in the corners of the QR code matrix whereas Encoding region is the data storage portion of the QR code.[11]

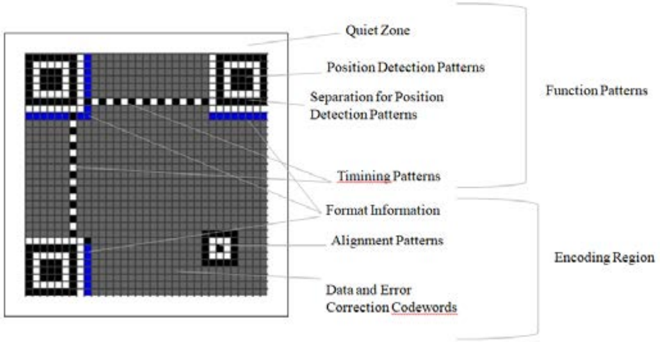

Quiet Zone
Position Detection Patterns
Separation for Position Detection Patterns
Timining Patterns
Format Information
Alignment Patterns
Data and Error Correction Codewords
Function Patterns
Encoding Region

Figure 1. Various Patterns in QR code

VISUAL SECRET SHARING (VSS)

In VSS, a binary image is encoded into n shares by using two matrices i.e one for dark module say V_d and another for white module say V_w.

$$V_d = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}_{\boldsymbol{n \times n}}$$

$$V_w = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}_{\boldsymbol{n \times n}}$$

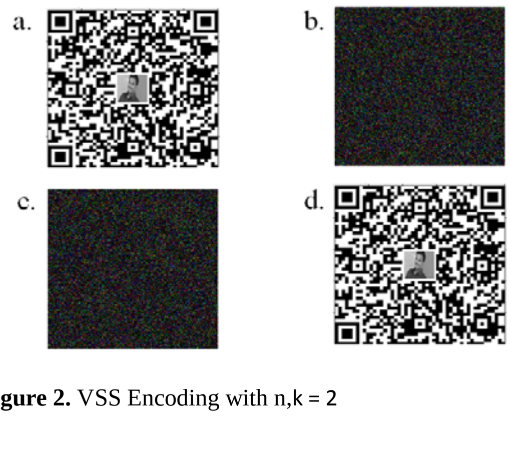


Figure 2. VSS Encoding with n,k = 2

Each pixel *(p)* in the image is fragmented into n sub pixels. If a pixel *p* is white, a row will be selected randomly from the matrix opposite to the white pixel i.e, from V_d. In contrast, if a *p* is black, a row will be selected randomly from the matrix opposite to the black pixel i.e, from V_w.[12] Finally after encoding all the pixels, n shared images will be constructed and transmitted to different participants. In figure 2, a sample binary image '2(a)' is encoded with n,k =2 and results 2 shares 2(b) & 2(c) When these shares are got superimposed, the original binary image is reconstructed very easily as shown in figure 2 (d).

SYSTEM DESIGNED

System Design is a process that identifies input, outputs and explains functions of the system. System design is the high level strategy for solving a problem.

Architecture of current System

Architecture for Encryption using VSS is shown in the figure 3.

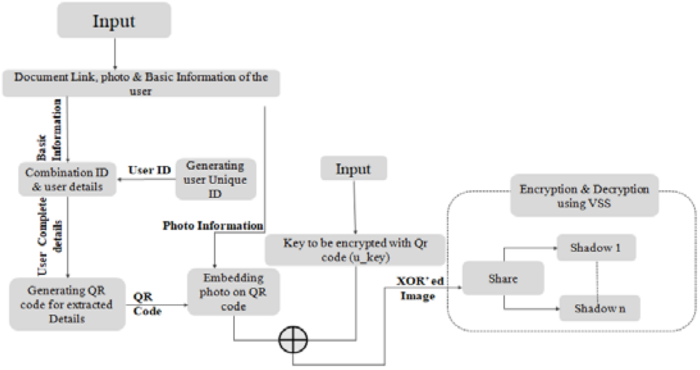

Input
Document Link, photo & Basic Information of the user
Basic Information
Combination ID & user details
User ID
Generating user Unique ID
User Complete details
Photo Information
Input
Key to be encrypted with Qr code (u_key)
Encryption & Decryption using VSS
Shadow 1
Share
Shadow n
XOR' ed Image
Generating QR code for extracted Details
QR Code
Embedding photo on QR code

Figure 3. Architecture of Encryption using VSS

In the above figure, it shows all the inputs and process of how the system works. First, details and photo of the user are taken. Then by using this information, they generate QR code along with a system generated code which will be used as user's unique ID. This QR code is embedded with the photo of the user for ease of identification and is embedded in a way that the QR code is readable and doesn't loss any information. Later, this QR code is encrypted with a key which will be generated randomly and then VSS encryption divides the 'Encrypted Image' into Shares which will be distributed to both the user and Admin as per agreement.

Whenever the user consults the Admin, they will identify the users with his/her Unique id and collects the user shares. Then all the shares of the user collected from admin and user are given for the decryption to get the original QR code. Before decryption, we have to enter the key that has been generated earlier during encryption. Then using this key and the shares, we get the original QR code. Architecture for Decrypting shares to get QR code is shown in the figure 4. In the figure 4 **u_key** should be same as the key that has been generated earlier while encryption. Otherwise it will generate a false QR code which is not readable. So, like this we get the QR code of the user. This will prevent the user private details from getting forged.

UML- Sequence Diagram

Sequence diagram is the most common kind of interaction diagram, which focuses on the message interchange between a number of lifelines. Sequence Diagram for QR code Generation and VSS encryption is shown in figure 5.

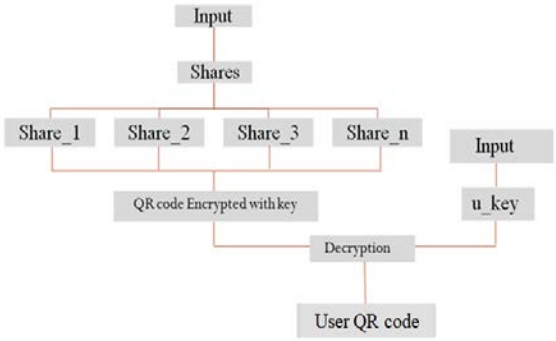


Figure 4. Architecture for Decryption of shares into QR code

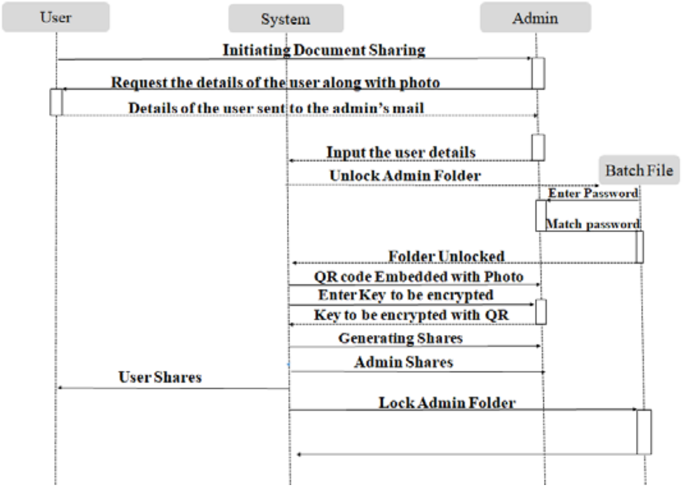

User
System
Admin
Initiating Document Sharing
Request the details of the user along with photo
Details of the user sent to the admin's mail
Input the user details
Batch File
Unlock Admin Folder
Enter Password
Match password
Folder Unlocked
QR code Embedded with Photo
Enter Key to be encrypted
Key to be encrypted with QR
Generating Shares
Admin Shares
User Shares
Lock Admin Folder

Figure 5 Sequence Diagram for Encryption

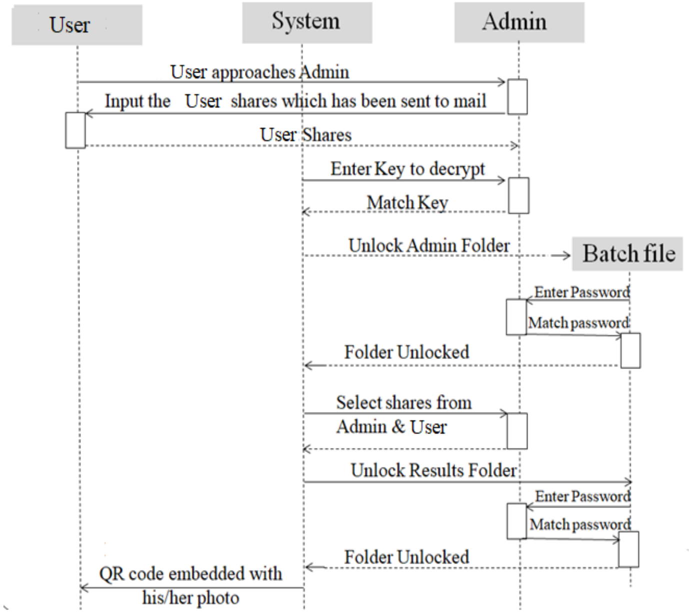


Figure 6. Sequence Diagram for Decryption

Sequence diagram for Decryption of Shares into QR code is shown in figure 6.

Input System

In this system, input is taken using GUI guide of MATlab which is a user-friendly UI to enter the inputs. To provide information, dialog boxes are used which will give a pop up to display the information to the user. Here the inputs are user details, user photo, Folder unlock passwords, Key for decryption. User photo can be taken using file system. Folder unlock passwords can be inputted in command window and finally keys are given in the inputted dialog boxes which pop ups for giving input.

Output Design

In this system outputs are shown in the axes handles, which will display the output image in the form of X and Y – coordinates. Output images are also stored in the file system for further usage. But not all the outputted images are stored in the file system, some images are just outputted to the user reference. The final decrypted QR code image is both outputted in the form of axes and also stored in a secured location of file system.

SYSTEM IMPLEMENTATION

Main Modules

(a) **QR code Generation** : QR code that will be generated for every user can be implemented by following a sequence of steps. Input the user details that have to be embedded into the QR code. Fix the Error correction level to M that has to be applied to the QR code. Fix the version of the QR code to 6. The given input data is then first analyzed, encoded, ECC words are generated and then placed into the matrix along with specifying the format and version information. By completing all the above phases, we will get a QR code for the user.

(b) **Embedding User Photo on QR code:** To identify each QR code of a user uniquely we will embed photo of the user on the QR code by implementing some sequence of steps. Choose the photo of the user and convert it into gray image as it has to be compatible with gray image of QR code. Resize the input image to the size of 250 × 250 and crop the photo if needed. Now resize the cropped image into the size of 50 × 50. Next, place the cropped image on to the QR code according to X and Y co-ordinates. Fix the starting point of embedding image at the coordinate (100, 100). This will be plotted the image onto the QR code from the given coordinate.

(c) **Encryption using VSS:** To provide security to the user's QR code, we implement VSS encryption to generate shares by following the sequence of steps. A key will be generated with which the encryption should be done (In this system we assume that every user should have unique key). XOR is the very element of the image with the key that has been generated to create a new encrypted image. Now this encrypted image is subjected to VSS encryption (4,4) by dividing it into 4 shares. Shares are generated by modifying the pixels of encrypted image to RGB at the specific positions. These shares are distributed equally to both user and admin. So, original QR code can be acquired by gathering all the 4 shares and then those will be subjected for decryption.[13]

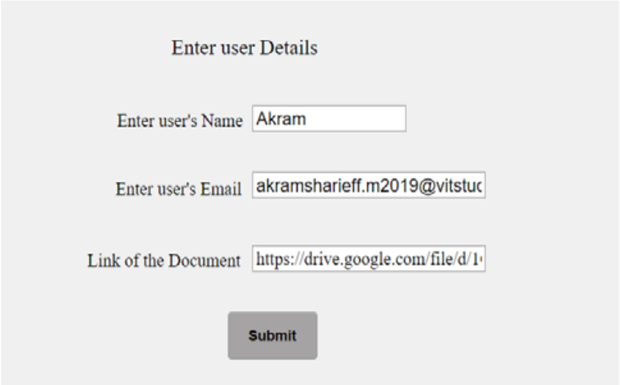
(d) **Decryption using VSS:** When the user approaches the admin with the shares and then decryption can be done by following the sequence of steps. Admin collects the shares from the user and check the availability of the shares with that user's id. After gathering all the shares, they are inputted for VSS decryption. Before decrypting the shares; first, we have to enter the key that has been given during encryption (which was assumed as User's unique key). Then the shares are decrypted by removing those RGB pixels at the specific locations and merge them to get the key encrypted QR code. Now the key encrypted QR code and the key is inputted for decryption to get original QR code. Decryption for getting original QR code can be done by again performing XOR to encrypted image and key. If the entered key is correct then the original user QR code named with user ID is generated. Naming the QR code with user id helps in identifying the QR code easily for issuing it the user. By scanning the QR code we can access the document.

(e) ***Folder Lock/Unlock:*** To prevent from intruders we lock the admin, results folder and unlock them whenever needed in program execution. When the program completes its execution, we will lock the folders. We will create a GUI to lock/unlock the results folder if needed by the admin. Admin can unlock folders by entering appropriate passwords. We can implement this locking concept using batch files. These can be implemented by following sequence of steps. Rename the folder to some other name and modify its attributes, so that it is not visible in file system. Restrict to undo the attributes of the folder unless one can enter the password that matches the password we specify in the code. If the password matches, the attributes are restored to default and again rename the folder to the default name. Like this, intruders are restricted from accessing the folders.

EXPERIMENTAL RESULTS

When we run the project, we will get a GUI to input the details of the User.

- In this step we will enter the details of the user along with link of the document.



Enter user Details

Enter user's Name: Akram

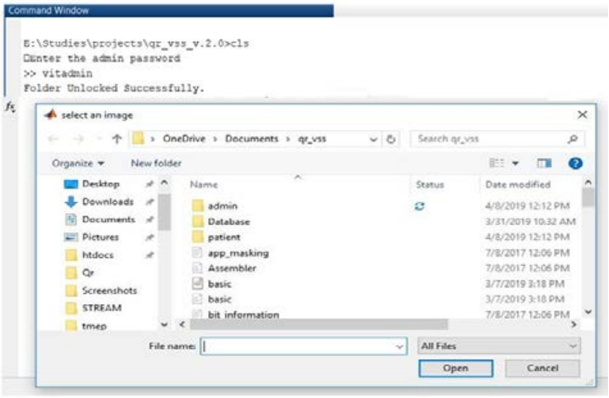
Enter user's Email: akramsharieff.m2019@vitstuc

Link of the Document: https://drive.google.com/file/d/1

Figure 7: Submitting the user details

- When we submit the details, It will prompt to unlock the Admin folder. Admin has to unlock the folder by entering appropriate password to store the admin shares.

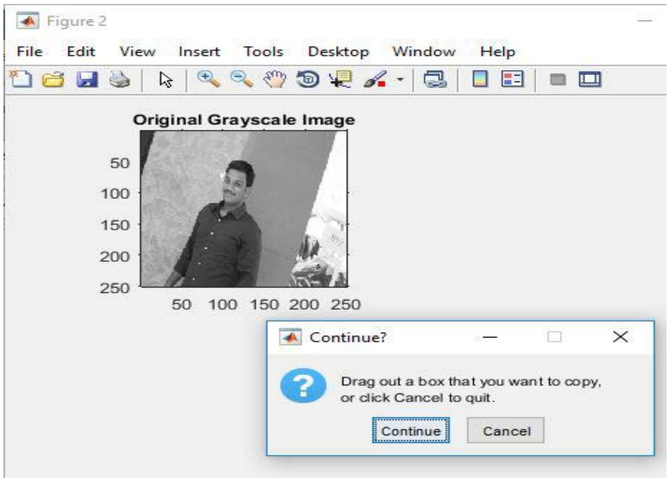
- Then it will prompt to select the photo of the user that has to be embedded on to the QR code.



```
E:\Studies\projects\qr_vss_v.2.0>cls
Enter the admin password
>> vitadmin
Folder Unlocked Successfully.
```

Figure 8: Selecting user photo

- After selecting the user’s photo, we can crop the photo if needed.



Drag out a box that you want to copy, or click Cancel to quit.

Figure 9: Cropping the user photo (If needed)

- QR code is generated with the user photo embedded on it. Next a key is generated which has to be encrypted with QR code.

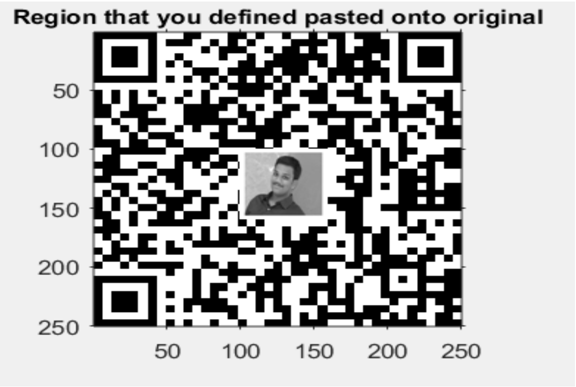


Figure 10: QR code generated

- We will get a key encrypted QR code. This image is now divided into shares.

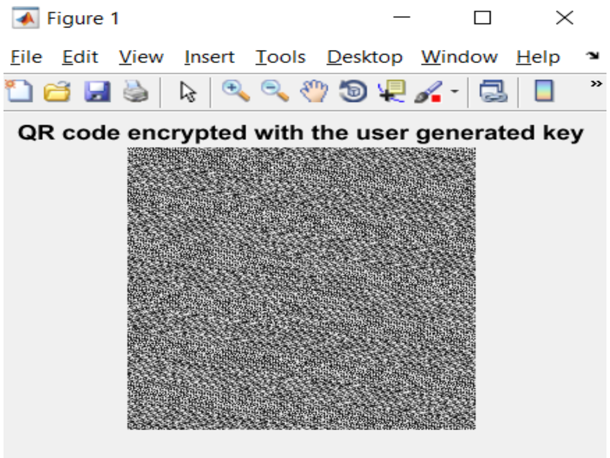
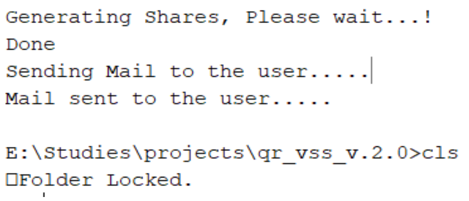


Figure 1
File Edit View Insert Tools Desktop Window Help
QR code encrypted with the user generated key

Figure 11: QR code Encrypted with given key

- Finally shares are generated and user shares are sent to the user’s mail. Four shares are equally distributed to the admin and user and user shares are not stored in admin file system.

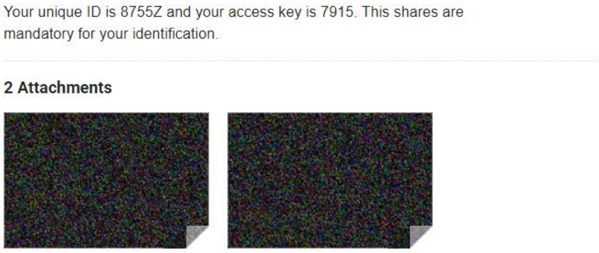


```
Generating Shares, Please wait...!
Done
Sending Mail to the user.....
Mail sent to the user.....

E:\Studies\projects\qr_vss_v.2.0>cls
Folder Locked.
```

Figure 12: Encryption completed and Folder locked

- User Shares send to mail from the admin mail address.



Your unique ID is 8755Z and your access key is 7915. This shares are mandatory for your identification.

Figure 13: Mail to the user sent by the admin

- When user approaches the admin, the user shares has to be received and stored in the admin file system where there will be a empty folder named with the user ID.

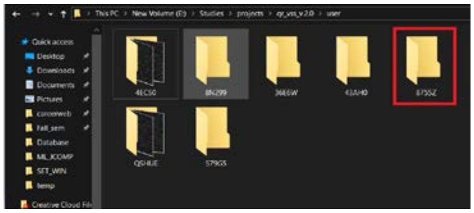


Figure 14: Empty user folder named with User ID

- To decrypt, both user shares and admin shares are needed. First, we will get a GUI to enter the user's key, shares and then to start Decryption.

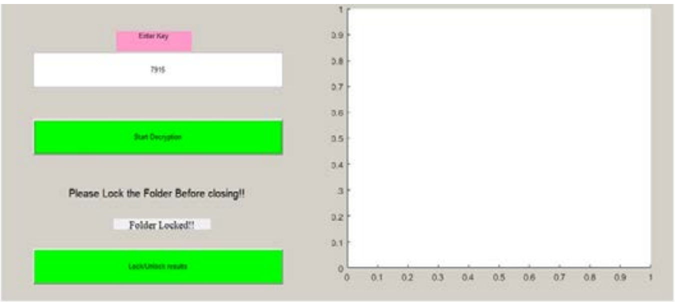
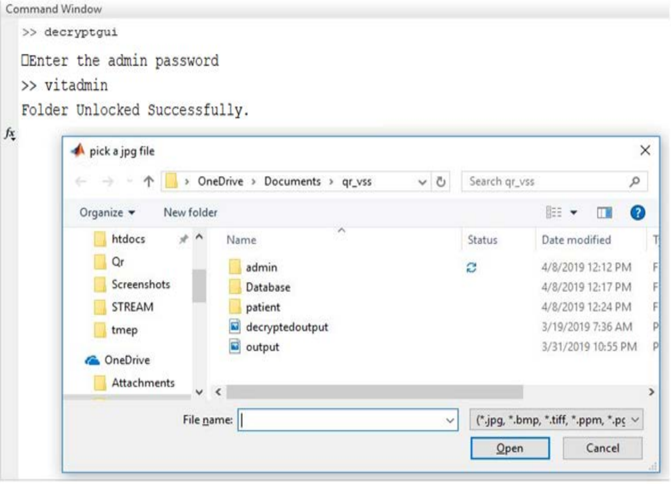


Figure 15: Decryption GUI to enter key and start Decryption

- When we click start decryption, we will get a dialog box to enter admin password.
- After entering the password, admin folder get unlocked and admin has to select the all the four shares.


```
Command Window
>> decryptgui
Enter the admin password
>> vitadmin
Folder Unlocked Successfully.
```

Name	Status	Date modified
admin		4/8/2019 12:12 PM
Database		4/8/2019 12:17 PM
patient		4/8/2019 12:24 PM
decryptedoutput		3/19/2019 7:36 AM
output		3/31/2019 10:55 PM

Figure 16: Selecting all the shares to Decrypt

- We will get the key encrypted QR code by merging the all the shares.

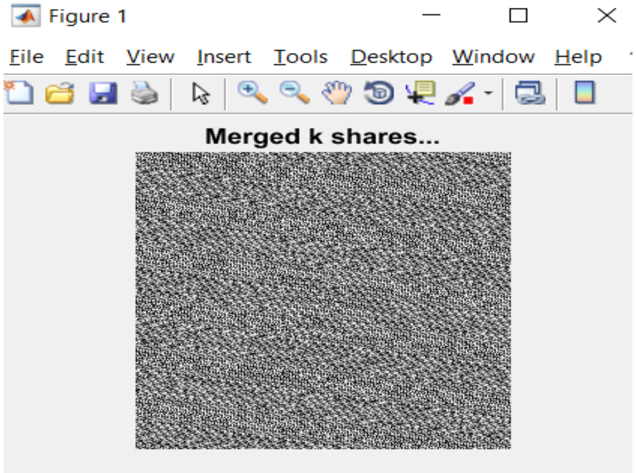


Figure 17: QR code Encrypted with the key

- Now, Admin has to enter the results folder password in order to store the decrypted original QR code of the user.

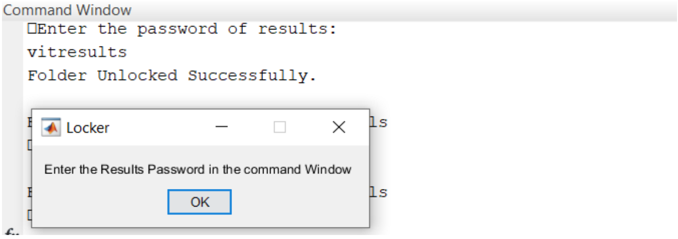

```
Command Window
Enter the password of results:
vitresults
Folder Unlocked Successfully.
```

Figure 18: Unlocking the Results folder

- After unlocking the results folder, we get the decrypted original QR code of the user.

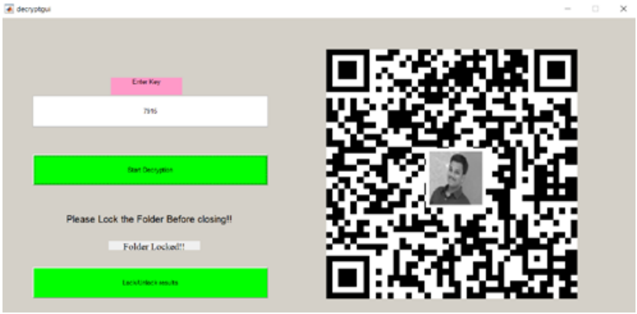
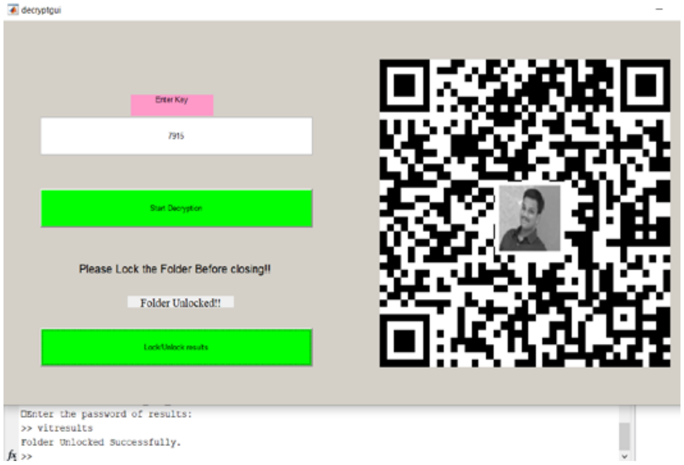


Figure 19: Original QR code with embedded user photo

- If admin has to retrieve the QR code, he/she can unlock the results folder by clicking on **Lock/unclock results** button and entering the password.



```
Enter the password of results:
>> vitresults
Folder Unlocked Successfully.
fx >>
```

Figure 20: Unlocking the Results folder manually

- After unlocking the folder, there will be a image of QR code named with the user's id. We can use that QR code image to issue the document shared by the user.

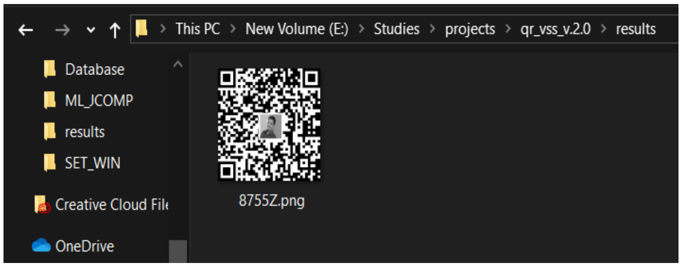
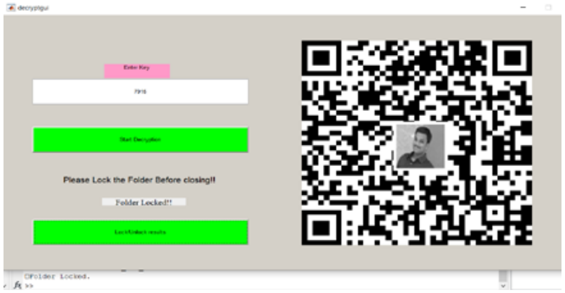

This PC > New Volume (E:) > Studies > projects > qr_vss_v.2.0 > results
Database
ML_JCOMP
results
SET_WIN
Creative Cloud Fil
OneDrive
8755Z.png

Figure 21: User QR code named with his/her ID for issuing

- After accessing the user's shared document, admin has to lock the results folder again by clicking the **Lock/Unlock results** button.



Please Lock the Folder Before closing!!

Folder Locked!!

```
CFolder Locked.
fx >>
```

Figure 22: Locking the results folder

- So, like this the user's document is accessed securely without being forged by any intruder.

Strength and Security

Security is the primary aspect for the document sharing. So, a methodology should consider and resolve as many attacks or threats as possible. Some of the security threats that can be resolved by this methodology are:

(a) Phishing
(b) Main in the Middle Attack
(c) Brute Force

Phising

Phising is often used by intruders as it is easy to execute and can get the results they need with less effort. It sends fake emails and text messages about the information they need exactly like authenticated companies or persons. Due to false anticipation one can send the information to the intruders.[14]

In this methodology phising is possible but doesn't work out for accessing the document. Because even the user sends the shares as a reply to the fake email from the intruders as admin, they need other half shares of admin which can't be accessed until or unless admin provides the password for the repository. Say somehow admin shares are also with the intruder still they need u_id to access the document for which the user is instructed not to share with anyone even with admin.

Man in Middle Attack

In this attack intruder relays in between the communication channel of two persons and acquires the information passes over the network. This attack works out when there is complete information needed to the intruded is provided through the communication channel. But according to the proposed methodology only the half shares required to access the document is sent to the user by the admin. Another half shares of admin are not disclosed anywhere but stored and locked in a repository which can be accessed only by the admin. So, even the intruder get the shares and u_id of the user, he/she will not get the access to the document.[15]

Brute force

In this attack intruder tries all the possible combinations for cracking a security system in order to get the required information. As an example, logging in into other's account by trying various combinations of username and password until the intruder gets access into it.[16]

For this methodology brute force attack is highly impossible because intruder has to crack either shares of users and admin or the QR code in which the document link is encoded. Brute forcing each pixel of n shares (n = 4 in our case) is impossible because, lets assume each share is of size 250 pixels with values 0 or 1 then the required shares will be one among $\mathbf{2^{250\times n}}$ combinations. Another way is to crack the QR code. In this methodology QR code version is fixed to 6 which produces

$$\mathbf{(21 + (4 \times (6-1)))^2} \quad ➔ \mathbf{1681} \text{ sized}$$

QR code. So, one among 2^{1681} combinations will be the required QR code.

Conclusions

In this study, authors report a novel methodology of authentication of digital documents using visual secret sharing on QR Code. As per this mechanism, any document will be initially divided into several shares and then distributed among user and admin as per the legal agreement. This is not only will provide authentication, but also it stands against security attacks. We strongly believe that this will provide robust authentication of digital documents and very much useful to handle practical applications.

Conflict of Interest

The authors declare no conflict of interest.

References

1. G.R. Blakley. Safeguarding cryptographic keys. *1979 Int. Work. Manag. Requir. Knowledge, MARK 1979* **1979**, 313–317.
2. A. Shamir. How to share a secret. *Commun. ACM* **1979**, 22 (11), 612–613.
3. X. Yan, Y. Lu. Applying QR Code to Secure Medical Management; National University of Defense Technology, **2018**.
4. S. Wan, Y. Lu, X. Yan, Y. Wang, C. Chang. Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions; Springer-Verlag, Berlin Heidelberg, **2018**; Vol. 14.
5. Y. Alaca, Y. Çelik. Cyber attack detection with QR code images using lightweight deep learning models. *Comput. Secur.* **2023**, 126.
6. X. Yan, X. Liu, C.N. Yang. An enhanced threshold visual secret sharing based on random grids; Springer-Verlag, Berlin Heidelberg, **2018**; Vol. 14.
7. Y.-W. Chow, W. Susilo, G. Yang, et al. Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing; Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Australia, **2016**; pp 409–425.
8. A. Beimel. Secret-Sharing Schemes: A Survey. In *IWCC*; **2011**; Vol. 11–46, pp 11–46.

9. C.C. Thien, J.C. Lin. Secret image sharing. *Comput. Graph*. **2002**, 26 (5), 765–770.
10. D.S. Wang, L. Zhang, N. Ma, X. Li. Two secret sharing schemes based on Boolean operations. *Pattern Recognit.* **2007**, 40 (10), 2776–2785.
11. W.Q. Yan, J. Weir, M.S. Kankanhalli. Image secret sharing; CRC Press", Taylor and Francis Group, **2017**.
12. A. Muhammed, A.R. Pais. A Secure Fingerprint Template Generation Mechanism Using Visual Secret Sharing with Inverse Halftoning. *SSRN Electron. J.* **2022**.
13. S. Shao, J. Li, P. Shao, G. Xu. Chaotic Image Encryption Using Piecewise-Logistic-Sine Map. *IEEE Access* **2023**, 1–1.
14. B.S.H.S. Singh, M. Fathima, M. Sameer, et al. Modelling an Efficient Approach to Analyse Clone Phishing and Predict Cyber-Crimes. *Lect. Notes Data Eng. Commun. Technol*. **2023**, 166, 181–189.
15. S.K. Shandilya, C. Ganguli, I. Izonin, P.A.K. Nagar. Cyber attack evaluation dataset for deep packet inspection and analysis. *Data Br*. **2023**, 46.
16. A.F. Otoom, W. Eleisah, E.E. Abdallah. Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks. *Procedia Comput. Sci.* **2023**, 220, 291–298.