SCIENTIFIC OASIS

Decision Making: Applications in Management and Engineering

ISSN: 2560-6018, eISSN: 2620-0104

HYBRID ADVANCED ENCRYPTION MECHANISM TO GENERATE VISUAL QR CODE FOR PREVENTING PHISHING ATTACKS

Mrs Ch. B. V. Durga[1], Maddi. Lakshmi Sai Kundana[2] , Teki. Vijaya Mahalakshmi[3] , Padamata. Usha[4] , Vankamamidi Subrahmanya Saketh Ram[5]

[1,2,3,4,5]Department Of Computer Science and Engineering, PSCMR College Of Engineering and Technology, Vijayawada, A.P.

ABSTRACT

Visual Cryptography is a technique that allows for encrypting information and protects the information from various attacks. Phishing is a wide range of attacks, an attempt made by an individual to steal a user's information for identity theft and economic benefit. Existing methods, such as URL and HTML features, are limited to detecting attached malware because they do not read and process subjects within the web page's external files, whether cross-domain or not. To resolve these problems, website detection uses visual cryptography and OTP. The QR code is split into two shares using a visual cryptography secret-sharing technique, which can be sent separately. When the two shares are merged, OTP is generated. Time Passwords (OTP) remain valid for one session and can mainly use to validate the User within a particular period. The proposed model generates the OTP using the Enhanced AES algorithm to provide a more secure QR code to prevent users from entering Phishing websites. AES gives more robust security and is highly resistant to attacks.

Keywords:

Visual Cryptography ; One Time Password ; Quick Response code ; Phishing ; Encrypt

1.Introduction

The QR code has become increasingly popular in recent years. First, computer parts like smartphones and checking guns easily recognize the QR code. Second, the QR code has a massive storage capacity, excellent resistance to damage, relatively inexpensive, and so on. Because of the benefits of the QR code, it is widely used. Resource packaging in the shopping centre now uses QR codes to distinguish between true and false. The QR code is now the most commonly utilized application. The most usual payment method is to complete Phonepay and Gpay by scanning the quick response codes. QR code logos are nearly all over our lives. With the widespread use of QR codes, there are severe security issues, such as information leaks and data corruption. The researchers are becoming more familiar with the QR code's coding

principles. The encoding requirements state that some attackers wrongfully forged the same code for the QR code pattern. For example, attackers can obtain the User's information from waste and then forge the same code pattern with the same encoding. It is no longer safe to use QR codes. As a result, the launch of novel technologies is critical to make QR

code authentication more secure and reliable. The study of secure and trustworthy QR code authentication is a significant focus for many researchers.

There are different techniques to detect phishing websites likewhitelisting, blacklisting, URL-based, content-based, visual cryptography, and steganography. In the Blacklisting technique, the URLs of phished sites are stored in a database, so whenever a new URL is entered, it compares it to the web addresses in the database. Database, and if it matches, the browser prevents and stores it in the database for future use. This technique's limitation is that it cannot identify Zero-hour phishing attacks.

In the Whitelist technique, the valid URLs are saved in the database and used to validate new ones. When a new URL is entered into this process, the database is first checked for that URL; if no record of that URL is discovered, the entire information of that URL, including SSL certificates, domain names, age, and hyperlinks connected to the website, is checked and stored in the database. The disadvantage of the allow listing technique is that the websites enrolled to be trusted can either be genuinely genuine or present themselves as genuine. One downside of listing techniques is that they take up much space.

In this paper, visual cryptography technique, Secret sharing divides a secret into several shares, each controlled by a different participant. The secret message can only be recovered by qualified participants working together; one participant knows nothing regarding the secret message. VCS is one method for secure image sharing. Visual cryptography Scheme is one of the new technology for secret sharing. It enhances the intimate sharing of images to restore the secret's complexity, depending on human visual decryption. It outperforms traditional cryptography in terms of hiding, confidentiality, and ease of total secrecy recovery. The visual cryptography method meets the users' high-security requirements and protects them from various security attacks.

In Visual Cryptography, Share A image pixels in the fundamental matrix of the visual encryption are chosen at random. In contrast, Share B image pixels are chosen for the other basic matrix. These two fundamental matrices are a combination. They produce two grey images due to their encryption, which prevents the original image data from being visible through the two images. So, it is impossible to obtain the information contained in secret images.

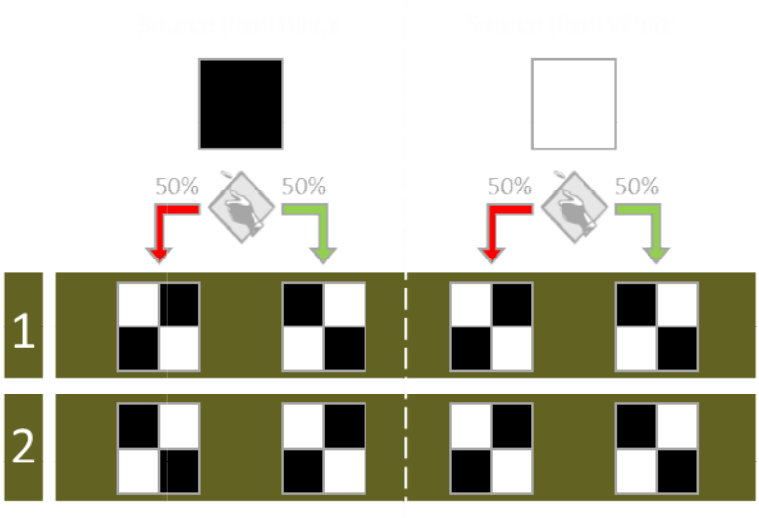

Fig:1 Probability of Images

According to Fig. 1, when they are added together, they result in a half-black square and add up to a black square.

If the source pixel is black:

- Give pattern 1 to the first grayscale image for half the time and pattern 2 to the second.
- For the other half of the span, give the first image pattern 2 and the second image pattern 1.

If the source pixel is white:

- Give pattern 1 to the first and second encrypted images for half the time.
- Instead, use pattern 2 for the other half of the time.

In this paper, we proposed a hybrid advanced encryption mechanism to generate a visual qr code for preventing phishing attacks and technology from preventing data theft. The plan can be applied in various fields, including records management, healthcare security, banking, and pharmaceutical industries.

2. Methodology

AES Advanced Encrypted Standard is the most commonly used encryption algorithm. It provides a high level of security and is trusted for protecting sensitive information. AES has a well-defined and robust cryptography structure. It operates on fixed-size blocks (128 bits) and

employs symmetric key operations, including byte substitution, row shifting, column mixing and key expansion. The combination of these operations provides a high level of cryptographic strength and resists various attacks.

Visual Cryptography allows a secret image to be divided into multiple shares, which can be distributed to multiple parties. The secret image can only be revealed when the shares are

combined in a specific way, without the need for complex computation or encryption algorithms. Here is a high-level description of the Visual Cryptography algorithm.

Start with a binary image (black and white only) representing the secret message to share. Divide the image into n shares, where n is the number of parties receiving a share. Each share will be a binary image with the same size as the original. For each pixel in the original image, choose one of the parties at random and assign the pixel value to that party's share. For example, if the pixel value is 0 (black), assign it to party A's share. Otherwise, assign it to party B's share.

Divide the image into n shares, where n is the number of parties receiving a share. Each share will be a binary image the same size as the original. For each pixel in the original image, choose one of the parties at random and assign the pixel value to that party's share. For example, if the pixel value is 0 (black), assign it to party A's share. Otherwise, assign it to party B's share.

Distribute the shares to the parties. To reconstruct the secret image, each party overlays their share with the other parties' shares, using a transparency or superposition technique. This reveals the original binary image in the overlapping areas, while the non-overlapping areas remain random

noise. The original image can be obtained by digitizing the overlapping areas and discarding the non-overlapping areas.

The critical advantage of Visual Cryptography is that it does not require any computation or knowledge of encryption algorithms, making it easy to implement and understand. It can also be used to share secrets among multiple parties without revealing the secret to any single party. However, it has some limitations, such as the need for many shares to preserve the quality of the secret image and the fact that the shares must be physically distributed to the parties.

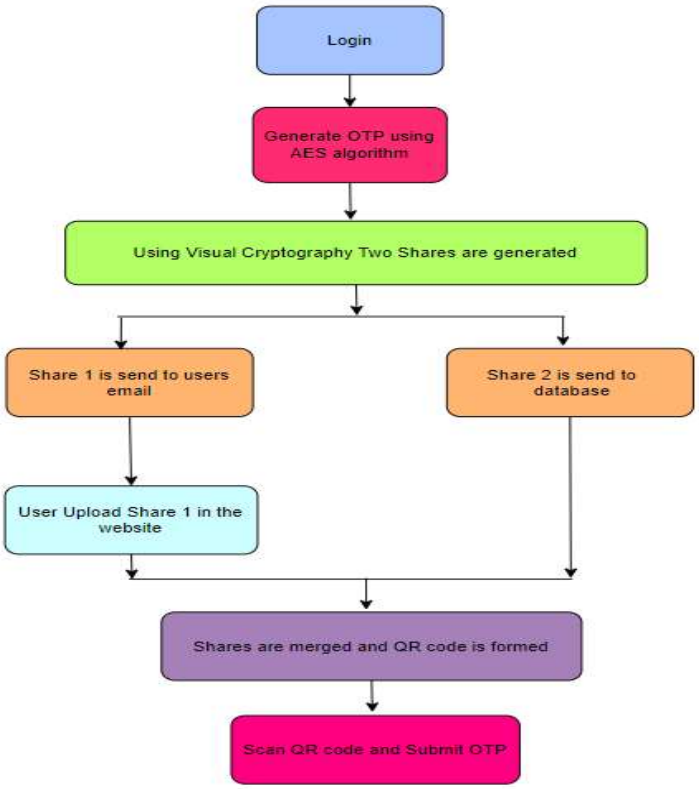

Fig. 2. Proposed Model

2.1 QR Code Generation

When the user login into the page. The User will enter the user id for OTP generation. The OTP is generated using aes algorithm

Algorithm:

Input: text

Output: Cipher text

Begin

for k=0 to Darray. length

f =0

If Darray[i] <0 then

Begin

Pos=-Darray[k]

```
                f = 1
                Else:

                pos = Darray[k]

                array[k]= parray[pos]

    If f =1 then

                Cipher[k] = -cipher[k]

            End If

End
```

When the User is registered User, then OTP is generated, and it is converted into a QR code. This process is done in the backend. The QR code is generated by using default settings after OTP is entered. If non-ASCII objects are to be used, the data must be a Unicode object.If the programme is successful, it returns a value of 0 and stores the QR code in the temp folder.

2.2 Shares Generation

After QR code generation using visual cryptography, two shares are generated. One share is sent to the registered User's mail, and the other is sent to the database. After merging the two shares, only we can get the QR code. If the share is not correct at the time of merging, the QR code is not formed.

2.3 QR code generation by merging the shares

When the User uploads the share to the website, the uploaded share will be combined with the share in the database. If the uploaded image is correct, then the two shares are merged and produce the original QR code. Otherwise, it will not produce the QR code. So this is how the QR code is generated by merging the shares, and it will display on the webpage. By scanning the QR code, the OTP will be generated.

3. Results

After finishing the registration, the User's personal information will be used to create a unique ID, making it particular to each User. A token created particularly for that User. The User can log in to the login page using the unique id generated during registration.

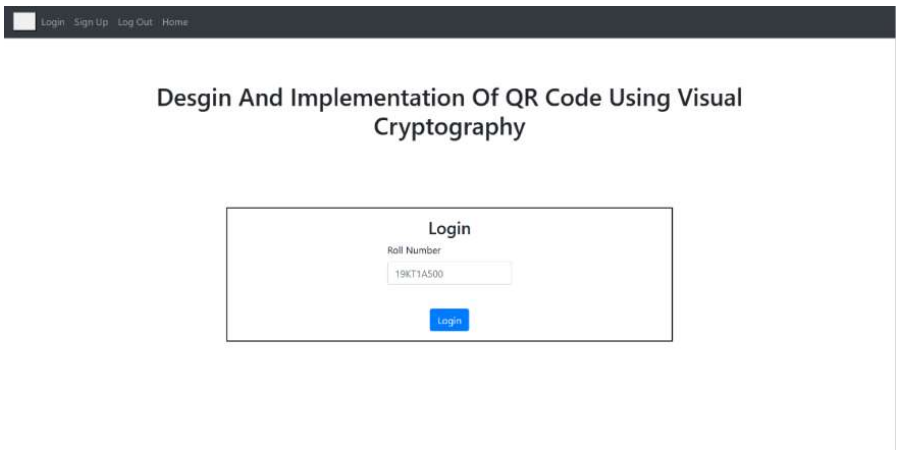

Fig. 3. Login Page

Users must enter the unique id as shown in Fig.3 to log into the website. If the User is registered, it will generate an OTP and the OTP is converted into a QR code. By the Visual Cryptography technique, two shares are generated. From these two shares, one share to the User's mail id. If the User is not registered, it will redirect the User to the registration page.

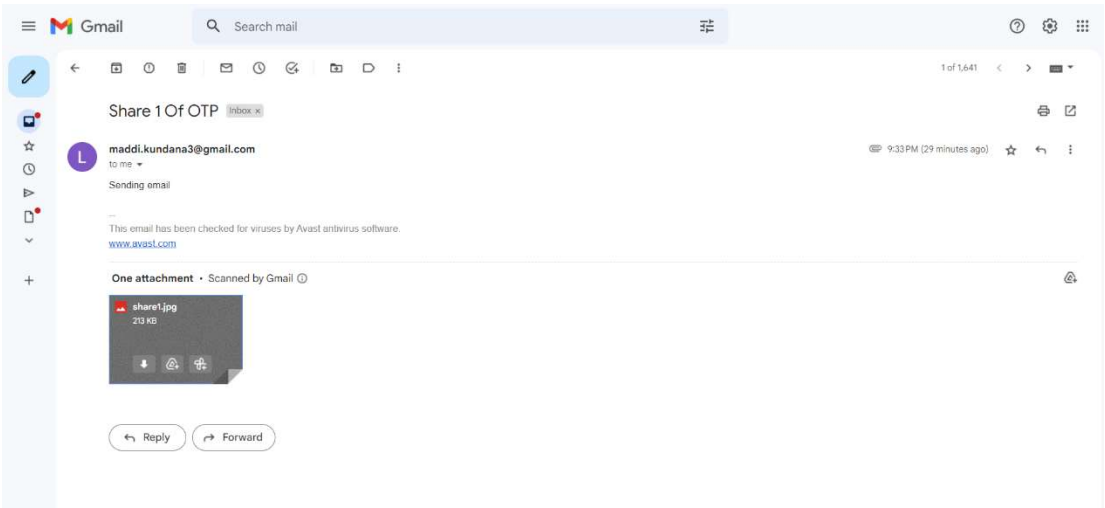

Fig. 4. Share is sent to users mail id

As shown in Fig 4, the User will get a Share via mail. After the share is received from the website, the User has to download the share and then upload share 1 on the upload page, as shown in Fig 5. If the uploaded image is not correct, it will not generate OTP. We have to upload the correct image to the upload page.

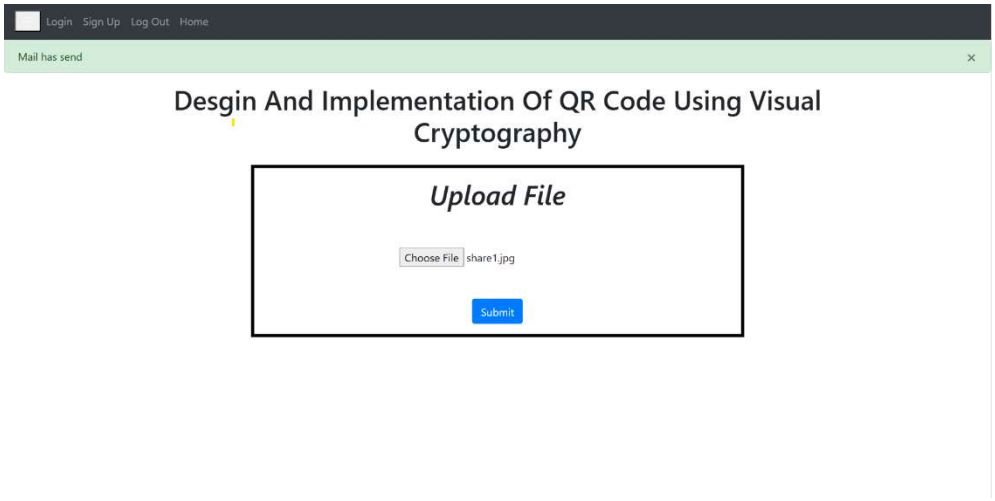

Fig. 5. Upload Page

After uploading the image as shown in Fig 5, submit the image. If we upload the correct image, it will redirect to the Verification page, as shown in Fig 6. This page will regenerate the QR code by merging the share in the database and the share uploaded by the User.

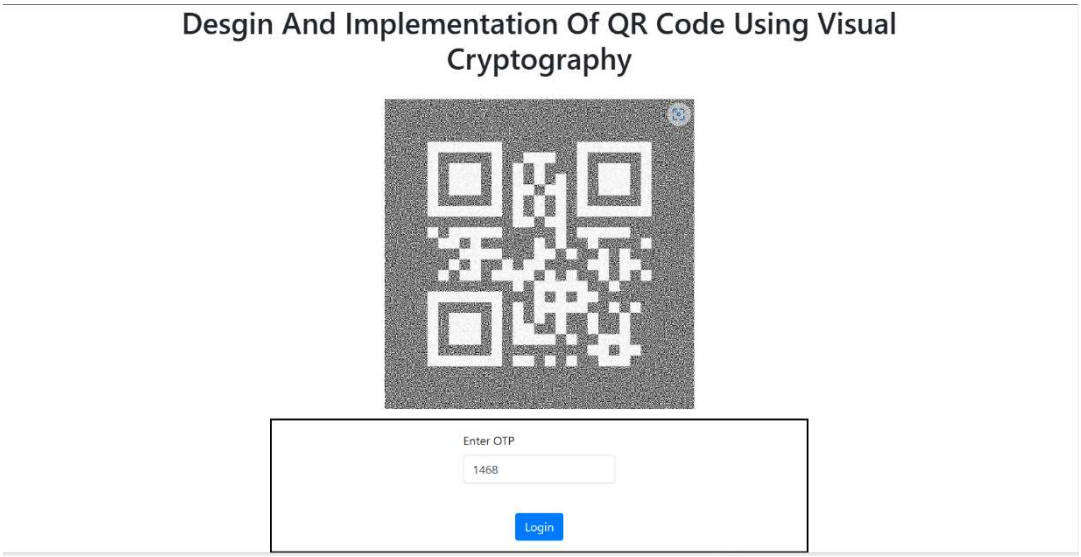

Fig. 6. Verification Page

After merging two shares, a QR code image is formed and displayed on the verification page. By scanning the QR shown in Fig 6 using mobile, the User will get an OTP. The User has to enter the OTP on the verification page. If the OTP is correct, it will redirect you to the website. Otherwise, it will show that the OTP needs to be corrected.

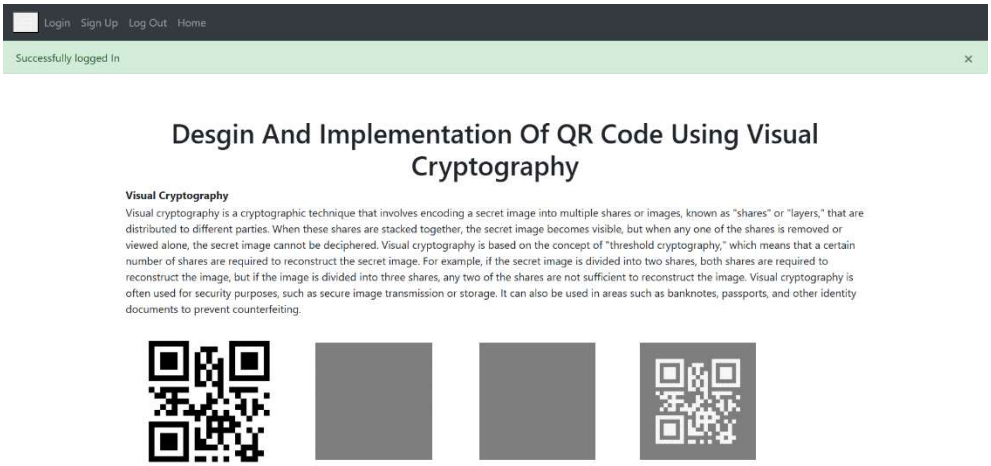

Fig. 7. Website

(1)

4. Conclusions

In this paper, we use visual cryptography and run experiments to prove its potential. Experiments demonstrate the effectiveness of this paper. It also demonstrates that this scheme is a secure method for detecting hackers by combining visual cryptography. It enhanced the safety of QR codes. This paper's scheme can be applied to the commercial platform due to its adaptability. The image that was shared can be applied to a variety of products. The likelihood of data leakage is extremely low. When the two images are subjected to the procedure, the issuing authority maintains one of the shared images to restore the original QR code image. The images which are shared are meaningless images with a random distribution of white pixels and black pixels. Using mathematical analysis and other techniques, the attacker cannot determine whether a pixel is white or black. In the meantime, the plan ensured that the data on users of the issuing authority was stored securely.

References

[1] Ren, L., Zhang, D. A QR code-based user-friendly visual cryptography scheme. Sci Rep12,7667 (2022). https://doi.org/10.1038/s41598-022-11871-9

[2] Zhengxin Fu, Liguo Fang, Hanging Huang, Bin Yu, Distributed three-level QR codes based on visual cryptography scheme, Journal of Visual Communication and Image Representation, Volume87,2022,103567, ISSN10473203,https://doi.org/10.1016/j.jvcir. 2022.103 567.

[3] L. Ahmad, R. Al-Sabha and A. Al-Haj, "Design and Implementation of a Secure QR Payment System Based on Visual Cryptography," 2021 7th ICIM, 2021, pp. 4044, doi: 10.1109/ICIM52229.2021.9417129.

[4] Emperor Journal of Applied Scientific Research ISSN No. 2581-964X(O) Vol. 4 Issue–04 April2022©TheAuthor(s)2022http://ejasr.may as.infohttp://dx.doi.org/10.35338/EJASR.2022.44 02

[5] Saurabh Kumar, Madhu Lata Nirmal, Advanced Visual Cryptography Secret Sharing Schemes Based on QR Codes, UGC Care Group I Journal, Vol-11 Issue-01 – 2021, ISSN: 2347-7180

[6] Mathivanan, P., Balaji Ganesh, A. QR code based-colour image cryptography for the secure transmission of ECG signal. Multimed Tools Appl 78, 6763–6786 (2019). https://doi.org/10.1007/s11042-018-6471-x

[7] Shuming Jiao, Jun Feng, Yang Gao, and Xiaocong Yuan, Visual cryptography in single-pixel imaging, optic Express, Vol. 28, Issue 5, pp. 7301-7313(2020). https://doi.org/10.1364/OE.383240

[8] Zhengxin Fu, Yuqiao Cheng, Sijia Liu, Bin Yu, A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions, Measurement,Volume141,2019,Pages267276,ISSN02632241,https://doi.org/10.1016/j .measurement.2019.03.0 80.

[9] Jeng-Shyang Pan, Tao Liu, Hong-Mei Yang, Bin Yan, Shu-Chuan Chu, TongtongZhu, Visual cryptography scheme for secret colour images with colour QR codes, Journal of Visual Communication and Image Representation, Volume 82,2022,103405, ISSN 1047- 3203,https://doi.org/10.1016/j.jvcir.2021.1034 05.

[10] Z. Fu, Y. Cheng and B. Yu, "Visual Cryptography Scheme With Meaningful Shares Based on QR Codes," in IEEE Access, vol. 6, pp.5956759574, 2018, doi:10.1109/ACCESS.2018.2874527.

[11] Yen-Wu Ti,1Shang-Kuan Chen, 1 and Wen-Chieh Wu2, A New Visual Cryptography Based QR Code System for Medication Administration, Open access Volume 2020 | Article ID 8885242 | https://doi.org/10.1155/2020/8885242

[12] Jeng-Shyang Pan, Tao Liu, Hong-Mei Yang, Bin Yan, Shu-Chuan Chu, TongtongZhu, Visual cryptography scheme for secret colour images with colour QR codes, Journal of Visual Communication and Image Representation, Volume82,2022,103405, ISSN 10473203,https://doi.org/10.1016/j.jvcir.2021. 103405.

[13] Xuncai Zhang, Zheng Zhou, Yangyang Jiao, and Ying Niu, Yanfeng Wang, A Visual Cryptography Scheme-Based DNA Microarrays, Int J Performability Eng ›› 2018, Vol. 14 ›› Issue (2): 334-340.doi: 10.23940/ijpe.18.02.p14.334340

[14] Yupeng Zhu, Wenhui Xu, Yishi Shi, High-capacity encryption system based on single-shot ptychography encoding and QR code, OpticsCommunications, Volume 435,2019, Pages426- 432, ISSN0030-4018,https://doi.org/10.1016/j.optcom.2018.11 .040.

[15] Ren, L., Zhang, D. A QR code-based user-friendly visual cryptography scheme. Sci Rep 12, 7667 (2022). https://doi.org/10.1038/s41598-022-11871-9.

[16] Mahendar, A., and Dr K. Shahu Chatrapati. "Detection and Prevention of Cyber Attacks on Cloud-Based Data Centers using Machine Learning." International Journal of Computing and Digital Systems 12.1 (2022): 1063-1070.