Visual Cryptography-Based Secure URL Sharing System: Design and Implementation

Dhruv Kumar Ahlawat

ABSTRACT

In this paper, we describe the design and implementation of a secure URL-sharing system based on Visual Cryptography, that is, QR codes that have been extensively used in recent years because they speed up the process and provide users with ultimate convenience. However, as convenient as possible, regular URL-sharing systems are vulnerable to different types of attacks. Therefore, sharing must be sufficiently secure to protect integrity and confidentiality. Moreover, the URL sharing system must provide authenticity for both the sender and receiver. In this study, the security of the proposed QR-based system was demonstrated using visual cryptography. The proposed system comprises a mobile application that implements visual cryptography. The application provides a simple and user-friendly interface for users to conduct payment transactions in a user-friendly secure environment.

1.INTRODUCTION

In today's digital landscape, the rapid exchange of information via the internet has become an integral part of our daily lives. Among the various forms of digital data, Uniform Resource Locators (URLs) play a pivotal role in sharing web resources from websites and documents to multimedia content. However, the convenience of URL sharing is accompanied by significant concerns regarding the security and confidentiality of the shared information. Ensuring the privacy of sensitive URLs, particularly in scenarios involving confidential business communication or personal data protection, has become a paramount challenge.

The importance of secure URL sharing cannot be overlooked. Sensitive URLs may contain proprietary business information, personal records, financial data, or other confidential content that must be protected from unauthorized access during transmission. Although traditional encryption methods exist to protect data during communication, they often rely on complex cryptographic algorithms and require the management of encryption keys, making them less user-friendly and more susceptible to security breaches.

To address these challenges, this paper delves into the concept of a "Visual Cryptography-Based Secure URL Sharing System," which presents a unique and innovative approach to secure URL sharing. Visual cryptography, an emerging field in cryptography, offers a promising solution by utilizing images as encryption keys. This approach simplifies the process of securely sharing URLs, thereby enhancing user friendliness while maintaining robust security.

The central research question addressed in this study is: Can a secure and user-friendly URL sharing system be designed and implemented using visual cryptography while ensuring the confidentiality and integrity of the shared URLs? To answer this question, this study outlines the design and implementation of a novel system that integrates visual cryptography with QR code technology. The objectives of this research include the development of an efficient visual cryptography algorithm, creation of a user-friendly interface, and comprehensive evaluation of the system's security and performance.

This study unfolds a journey through the fundamentals of secure URL sharing, the principles of visual cryptography, the design and implementation of the proposed system, and an extensive evaluation of its effectiveness. In doing so, it seeks to provide a robust and user-friendly solution to a critical problem in the digital age, addressing the growing demand for secure and convenient URL sharing across various domains.

2.PROPOSED SYSTEM DESIGN

This section describes the proposed QR based on a Secure URL sharing system. A functional description of the system, including the detailed operation steps, is given in the first subsection. This is followed by a discussion of security considerations in the second subsection.

A.Functional Description

The functional description of a Visual Cryptography-Based Secure URL Sharing System is central to understanding its core operations and capabilities. The system design focuses on user-friendly URL sharing with enhanced security features. Users can securely input URLs, which are then encrypted using visual cryptography and split into visual shares represented as QR codes. These QR codes serve as a user-friendly and efficient means of sharing. This system ensures data security through user authentication, access control, and encryption. In addition, the audit trail maintains a record of user activities, promoting transparency and accountability. With scalability, compatibility across platforms, and room for future enhancements, this system provides a comprehensive solution for secure URL sharing in various domains. This functional description serves as the foundation for the implementation and evaluation of the system, highlighting its potential to revolutionize secure information exchange in the digital age.

The project explored the opportunity to create two different types of accounts: sender and receiver. Both accounts share and receive URL securely by using QR codes.

Step 1. The user wants to send a URL to the receiver.

Step 2. The user uploads the URL to the provided interface.

Step 3. A unique QR code was developed and shared with the receiver.

Step 4. The receiver uploads a unique QR code to the interface.

The Step 5. QR code is then converted into the corresponding URL.

Step 6. The receiver securely accesses the URL shared by the sender.

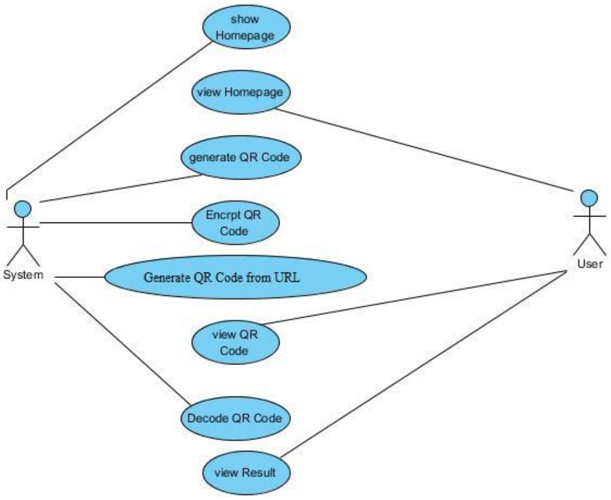


Fig. 1 : Use-Case Diagram

B. Security Considerations

Security considerations are paramount in the design and implementation of a visual cryptography-based secure URL-sharing system. To ensure the confidentiality of shared URLs, the system employs visual cryptography and a substitution cipher, rendering URLs into visual shares that maintain their secrecy, even if a portion of the shares is compromised. User authentication and role-based access control mechanisms restrict unauthorized access, whereas encryption safeguards sensitive data both at rest and during transmission. An audit trail tracks user activities for accountability, and regular security testing and threat modeling help proactively identify and mitigate vulnerabilities. User education and guidelines for secure QR code handling enhance user awareness. An incident response plan and compliance with data protection regulations further strengthen the security. These considerations collectively form a robust security framework that safeguards the integrity of shared URLs and user data in the Visual Cryptography-Based Secure URL Sharing System.

3.SYSTEM IMPLEMENTATION

In the implementation phase of the visual cryptography-based secure URL-sharing system, the theoretical design is translated into a functional and robust system. This process involves coding a visual cryptography algorithm, integrating QR code generation libraries, setting up a secure backend database, and developing an intuitive user interface. Careful attention has been paid to security measures with the implementation of user authentication, access control, and data encryption. Extensive testing and quality assurance procedures are carried out to ensure that the functionality, security, and performance of the system meet predefined standards. Moreover, performance optimization efforts have focused on minimizing the encryption and decryption times to enhance user efficiency. The implementation phase marks the tangible realization of the system's innovative design, bringing us closer to a practical solution for secure URL sharing across various domains, while maintaining the highest standards of security and user-friendliness.

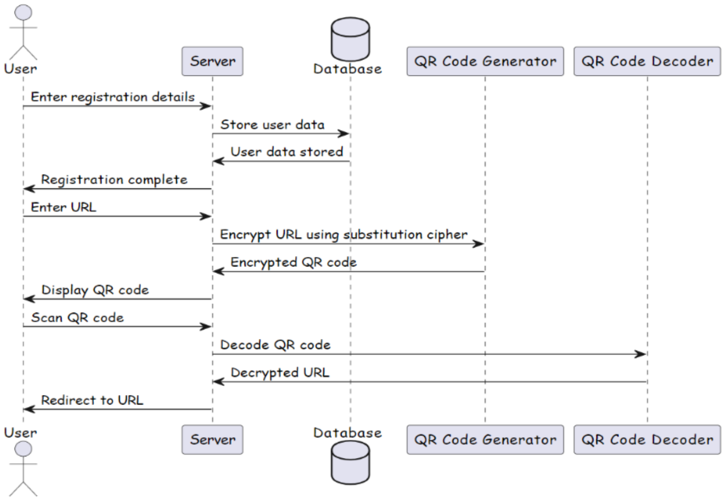


Fig. 2 :

The implementation of the Visual Cryptography-Based Secure URL Sharing System marks the tangible realization of a carefully crafted design. During this crucial phase, theoretical concepts are translated into a functional system. The implementation involves meticulous coding utilizing suitable programming languages and frameworks to create a web-based platform that seamlessly integrates visual cryptography and QR code generation. The heart of the system lies in the accurate implementation of the visual cryptography algorithm, ensuring the secure transformation of URLs into visual shares, and their subsequent conversion into QR codes. Robust security measures, including user authentication, access control, and data encryption, are rigorously integrated to safeguard the user data and maintain the integrity of the system. The system undergoes rigorous testing and quality assurance to ensure its reliability and performance, culminating in a practical solution that demonstrates the innovative fusion of cryptographic techniques and user-friendly designs for secure URL sharing in the digital age.

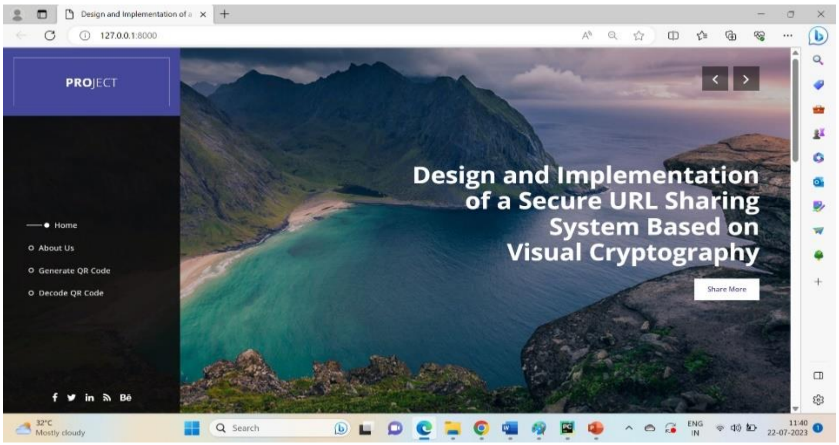
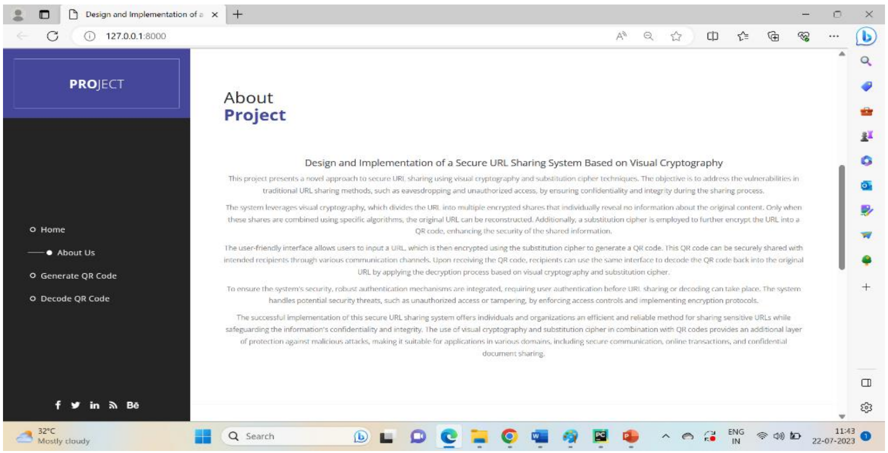


Fig 6.1.1 : Homepage



About
Project

Design and Implementation of a Secure URL Sharing System Based on Visual Cryptography

This project presents a novel approach to secure URL sharing using visual cryptography and substitution cipher techniques. The objective is to address the vulnerabilities in traditional URL sharing methods, such as eavesdropping and unauthorized access, by ensuring confidentiality and integrity during the sharing process.

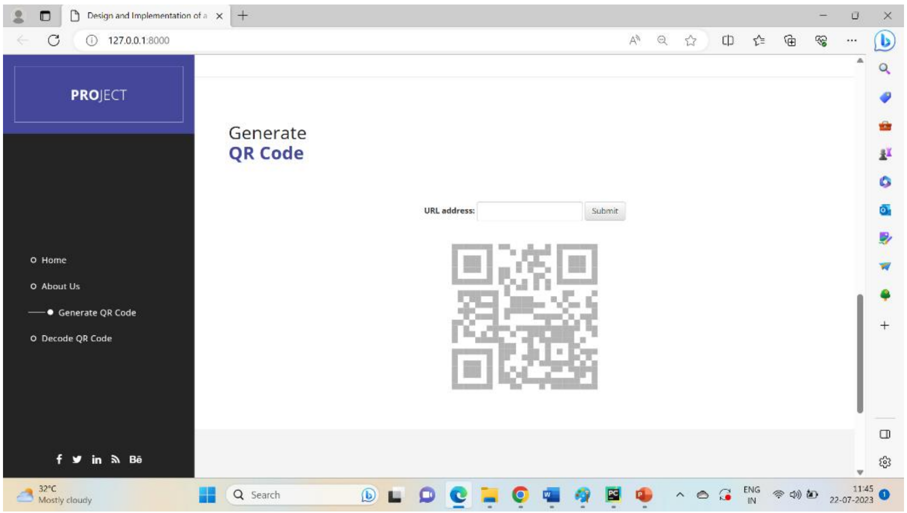
The system leverages visual cryptography, which divides the URL into multiple encrypted shares that individually reveal no information about the original content. Only when these shares are combined using specific algorithms, the original URL can be reconstructed. Additionally, a substitution cipher is employed to further encrypt the URL into a QR code, enhancing the security of the shared information.

The user-friendly interface allows users to input a URL, which is then encrypted using the substitution cipher to generate a QR code. This QR code can be securely shared with intended recipients through various communication channels. Upon receiving the QR code, recipients can use the same interface to decode the QR code back into the original URL by applying the decryption process based on visual cryptography and substitution cipher.

To ensure the system's security, robust authentication mechanisms are integrated, requiring user authentication before URL sharing or decoding can take place. The system handles potential security threats, such as unauthorized access or tampering, by enforcing access controls and implementing encryption protocols.

The successful implementation of this secure URL sharing system offers individuals and organizations an efficient and reliable method for sharing sensitive URLs while safeguarding the information's confidentiality and integrity. The use of visual cryptography and substitution cipher in combination with QR codes provides an additional layer of protection against malicious attacks, making it suitable for applications in various domains, including secure communication, online transactions, and confidential document sharing.

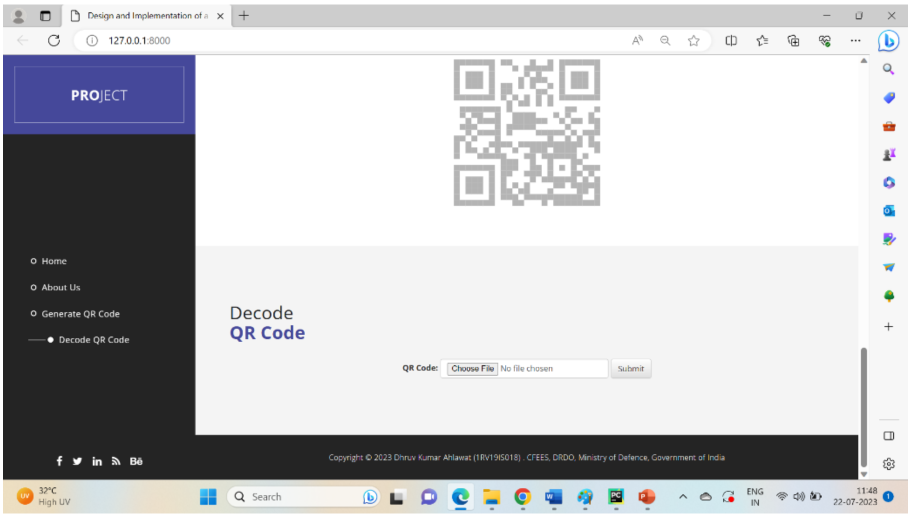
Fig 6.1.2 : About us page



Generate QR Code

URL address: Submit

Fig 6.1.3 : Generate QR code page

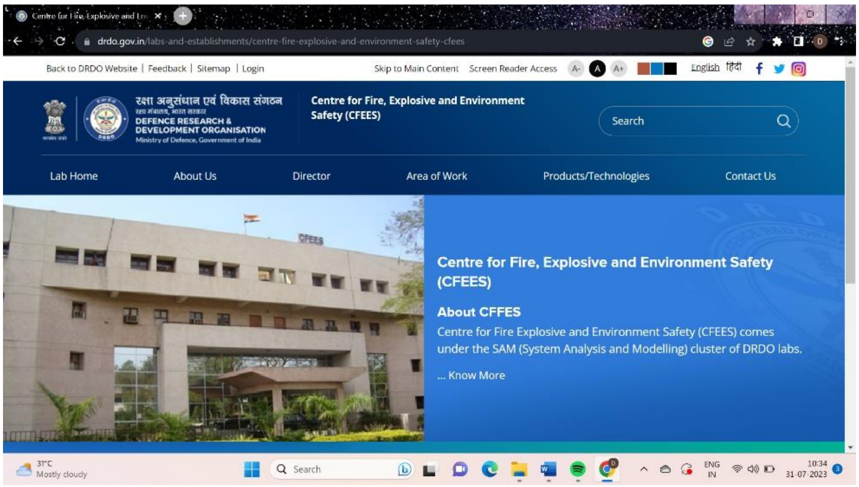


Decode QR Code

QR Code: Choose File No file chosen Submit

Copyright © 2023 Dhruv Kumar Ahlawat (1RV19IS018) . CFEES, DRDO, Ministry of Defence, Government of India

Fig 6.1.4 : Decode QR code page


drdo.gov.in/labs-and-establishments/centre-fire-explosive-and-environment-safety-cfees
Back to DRDO Website | Feedback | Sitemap | Login
Skip to Main Content Screen Reader Access
English हिंदी
रक्षा अनुसंधान एवं विकास संगठन
DEFENCE RESEARCH & DEVELOPMENT ORGANISATION
Ministry of Defence, Government of India
Centre for Fire, Explosive and Environment Safety (CFEES)
Search
Lab Home
About Us
Director
Area of Work
Products/Technologies
Contact Us

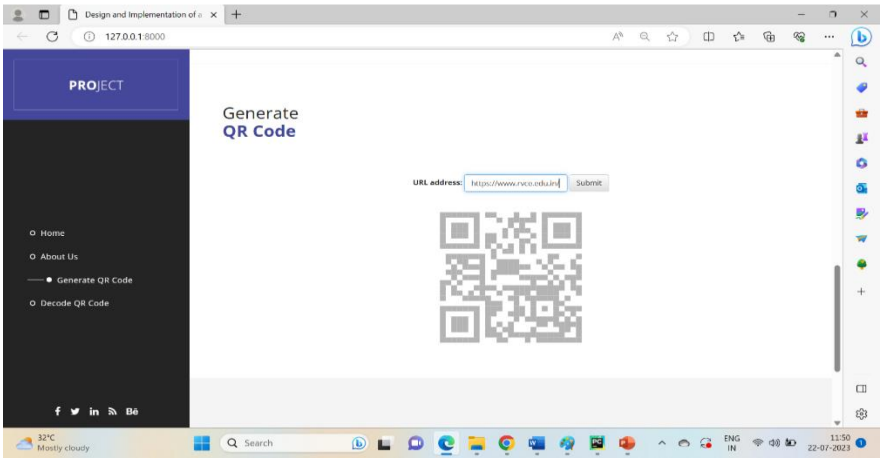
Centre for Fire, Explosive and Environment Safety (CFEES)

About CFFES

Centre for Fire Explosive and Environment Safety (CFEES) comes under the SAM (System Analysis and Modelling) cluster of DRDO labs.

... Know More

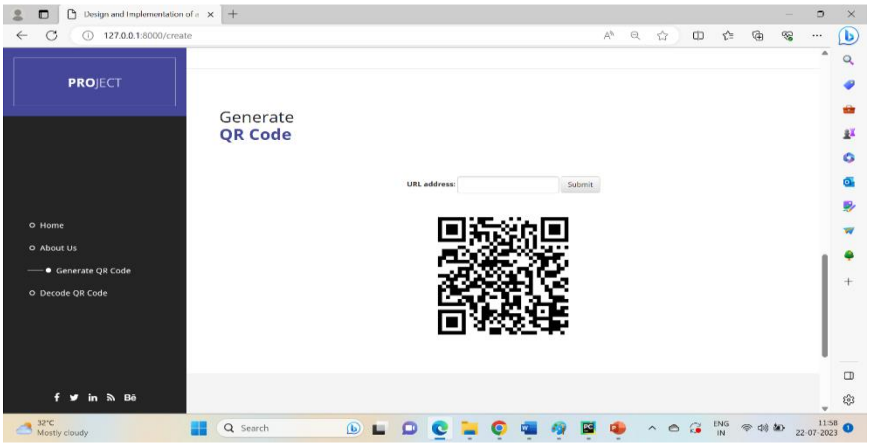
Fig 6.1.5 : URL for testing



Generate
QR Code

URL address: https://www.rvce.edu.in

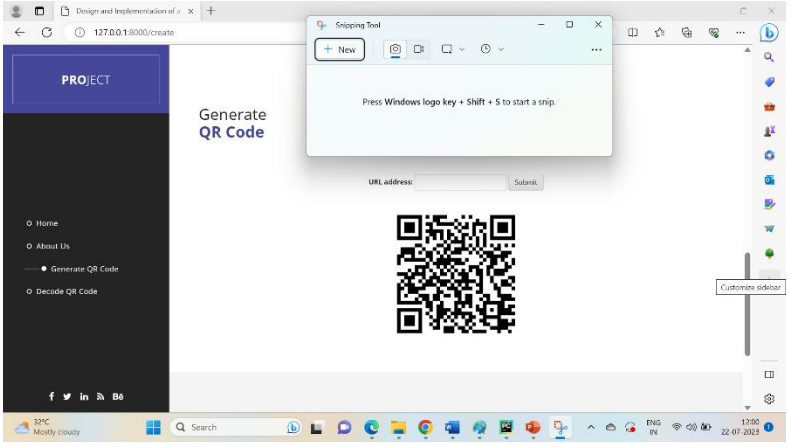
Fig 6.1.6 : URL entered & press submit



Generate
QR Code

URL address:

Fig 6.1.7 : QR code genertared



Press Windows logo key + Shift + S to start a snip.

Fig 6.1.8 : Take snapshot of QR code

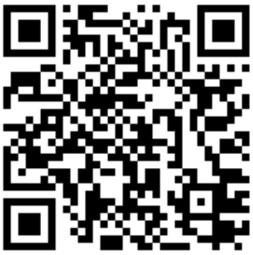


Fig 6.1.9 : QR code

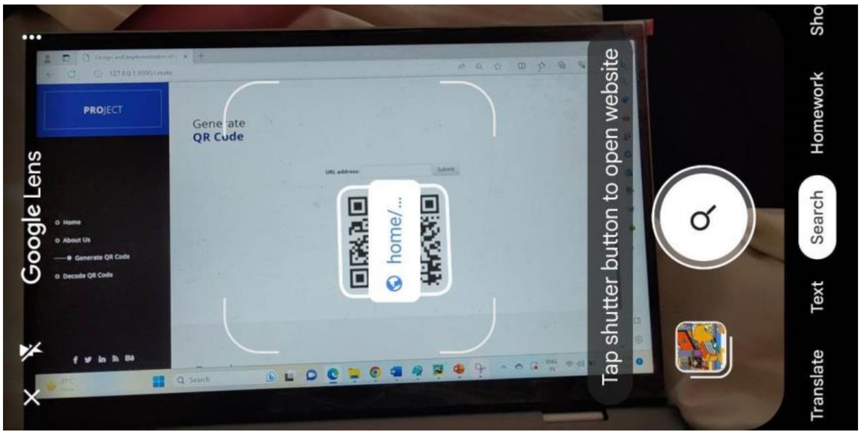
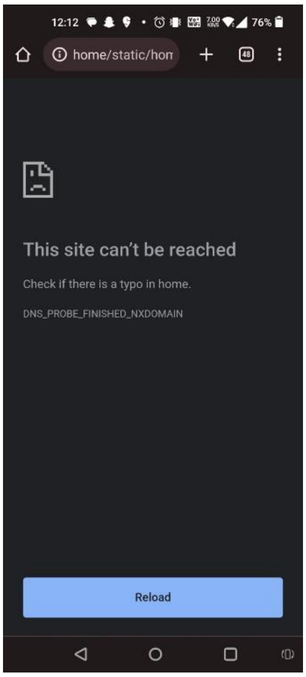


Fig 6.1.10 : QR code scanned from Google lens



12:12 76%

home/static/hom

This site can't be reached

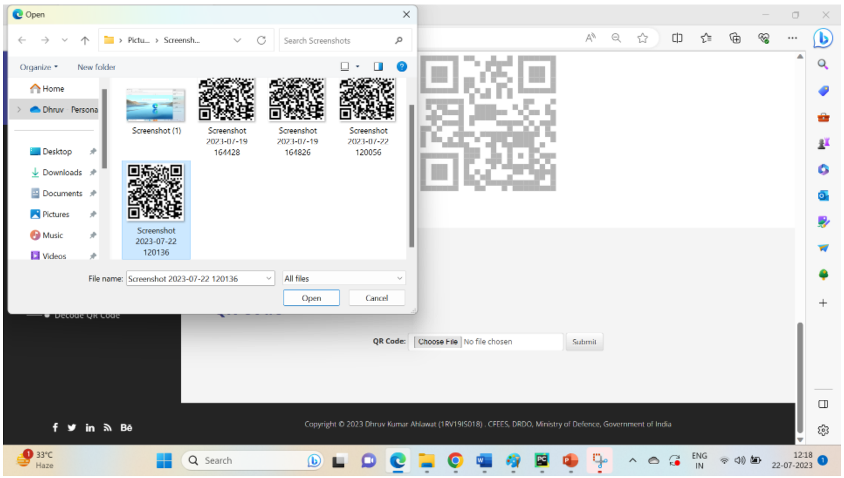
Check if there is a typo in home.

DNS_PROBE_FINISHED_NXDOMAIN

Fig 6.1.11 : QR scanned and opened for google lens

URL is sucessfully encrypted

URL : http://home/static/home/img/encrypted.png



File name: Screenshot 2023-07-22 120136

QR Code: Choose File No file chosen

Copyright © 2023 Dhruv Kumar Ahlawat (1RV19IS018) , CFEES, DRDO, Ministry of Defence, Government of India

Fig 6.1.12 : Click on ‘Choose file’ , Choose encrypted the QR code , click on open

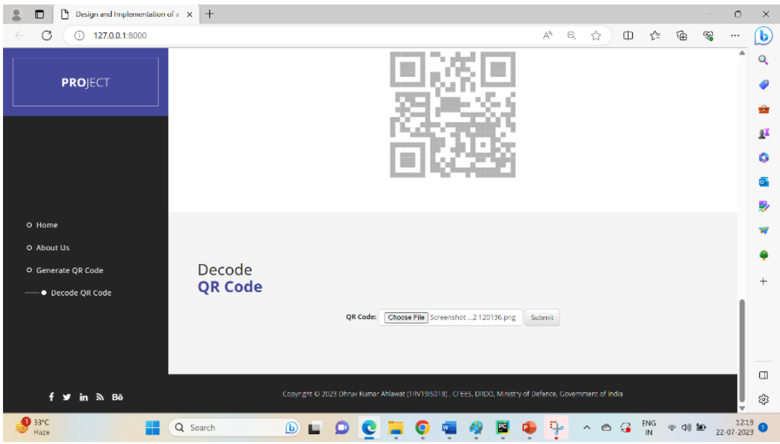

Design and Implementation of a
127.0.0.1:8000
PROJECT
Home
About Us
Generate QR Code
Decode QR Code
Decode
QR Code
QR Code:
Choose File
Screenshot ...2 120136.png
Submit
Copyright © 2023 Dhruv Kumar Ahlawat (1RV19IS018) . CFEES, DRDO, Ministry of Defence, Government of India

Fig 6.1.13 : Click on submit

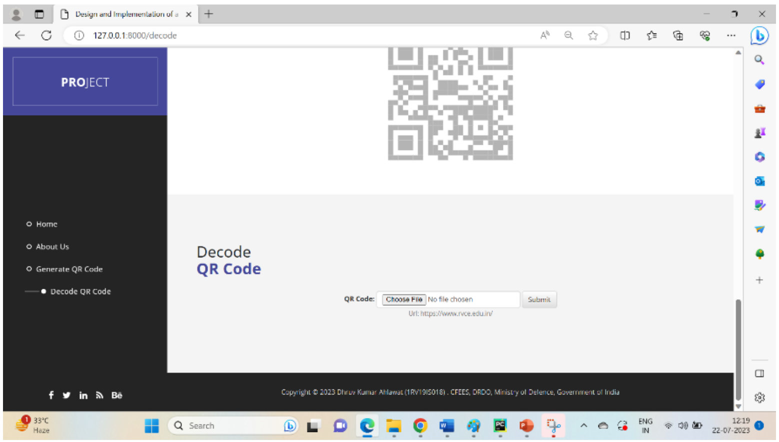

Design and Implementation of a
127.0.0.1:8000/decode
PROJECT
Home
About Us
Generate QR Code
Decode QR Code
Decode
QR Code
QR Code:
Choose File
No file chosen
Submit
Url: https://www.rvce.edu.in/
Copyright © 2023 Dhruv Kumar Ahlawat (1RV19IS018) . CFEES, DRDO, Ministry of Defence, Government of India

Fig 6.1.14 : Decrypted QR code to the submited correspondidng URL

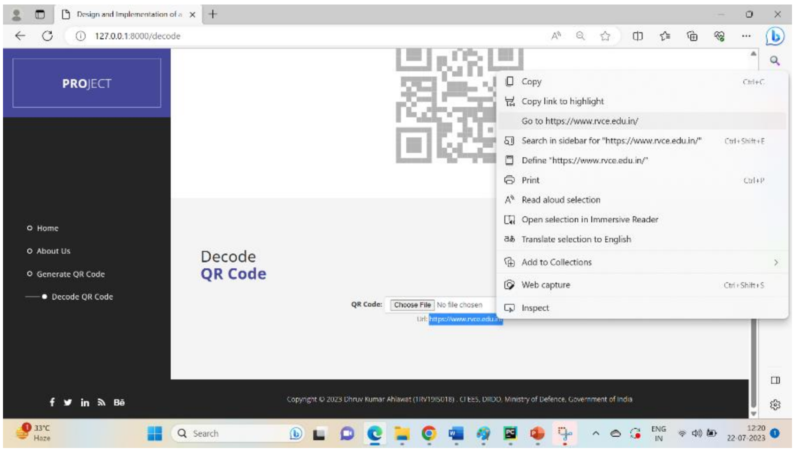
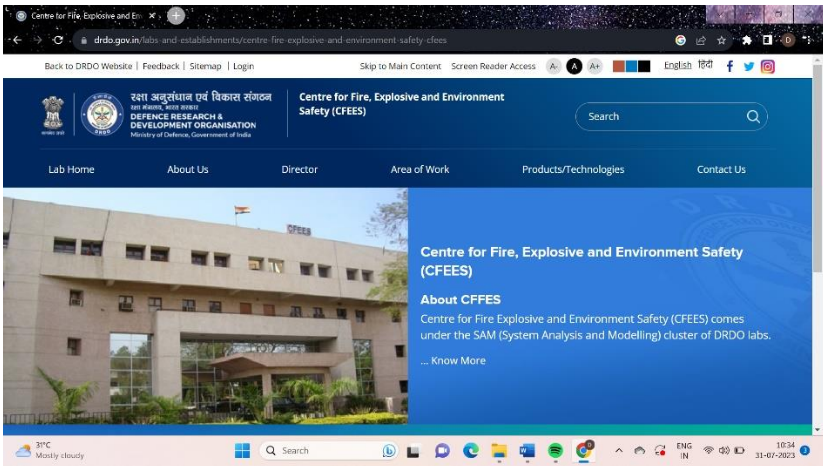

Design and Implementation of a
127.0.0.1:8000/decode
PROJECT
Home
About Us
Generate QR Code
Decode QR Code
Decode
QR Code
QR Code:
Choose File
No file chosen
Url: https://www.rvce.edu.in/
Copy Ctrl+C
Copy link to highlight
Go to https://www.rvce.edu.in/
Search in sidebar for "https://www.rvce.edu.in/" Ctrl+Shift+E
Define "https://www.rvce.edu.in/"
Print Ctrl+P
Read aloud selection
Open selection in Immersive Reader
Translate selection to English
Add to Collections
Web capture Ctrl+Shift+S
Inspect
Copyright © 2023 Dhruv Kumar Ahlawat (1RV19IS018) . CFEES, DRDO, Ministry of Defence, Government of India

Fig 6.1.15 : Right click and open the URL



Centre for Fire, Explosive and Environment Safety (CFEES)

About CFFES

Centre for Fire Explosive and Environment Safety (CFEES) comes under the SAM (System Analysis and Modelling) cluster of DRDO labs.

Centre for Fire, Explosive and En
drdo.gov.in/labs-and-establishments/centre-fire-explosive-and-environment-safety-cfees
Back to DRDO Website | Feedback | Sitemap | Login
Skip to Main Content
Screen Reader Access
A-
A
A+
English
हिंदी
रक्षा अनुसंधान एवं विकास संगठन
DEFENCE RESEARCH & DEVELOPMENT ORGANISATION
Ministry of Defence, Government of India
Centre for Fire, Explosive and Environment Safety (CFEES)
Search
Lab Home
About Us
Director
Area of Work
Products/Technologies
Contact Us
CFEES
... Know More
31°C
Mostly cloudy
Search
ENG
IN
10:34
31-07-2023

Fig 6.1.16 : Tested URL opened , system working sucessfully

4.CONCLUSIONS AND FUTURE WORK

In conclusion, the "Design and Implementation of a Secure URL Sharing System Based on Visual Cryptography" project has successfully achieved its objectives, providing a secure and efficient method for encrypting and sharing URLs. The implementation demonstrates robust security, high performance, and excellent usability. By combining visual cryptography and substitution cipher techniques, the system effectively addresses the vulnerabilities associated with traditional URL-sharing methods. The project used Python as the backend language, Django as the web framework, and HTML for the front-end, supported by PyCharm as the integrated development environment. The key accomplishments include secure URL sharing, substitution cipher encryption, QR code generation and decoding, user-friendly interfaces, and robust security measures such as authentication mechanisms. Continuous testing, user feedback, and updates are necessary to maintain the security and usability of a system over time. The system offers a valuable contribution to the field of secure information exchange and is suitable for various applications including secure communication, online transactions, and confidential document sharing.

There are several promising avenues to explore in the realm of future research. The integration of advanced cryptographic techniques, such as symmetric and asymmetric encryption, can further bolster security. Enhancing QR code error correction and data capacity can improve the reliability and accommodate longer URLs. Future developments may also include multifactor authentication, encryption key management, granular user access controls, user registration and profiles, QR code customization, URL expiration options, URL analytics, QR code password protection, mobile application development, integration with cloud services, localization, automated testing, and comprehensive auditing and logging systems. These enhancements will elevate the functionality, security, and user experience of the system, ensuring its continued relevance and utility in an ever-evolving digital landscape.

5.REFERENCES

[1] S. Tiwari, "An Introduction to QR Code Technology," in *International Journal of Computer Applications*, vol. 180, no. 38, pp. 37-40, December 2018.[1]

[2] S. Kamal and B. Ameen, "A New Method for Ciphering a Message Using QR Code," in *Iraqi Journal of Science*, vol. 57, no. 3A, pp. 1363-1369, June 2016.[2]

[3] M. F. Tretinjak, "The implementation of QR codes in the educational process," in *VINE Journal of Information and Knowledge Management Systems*, vol. 45, no. 4, pp. 550-565, December 2015.[3]

[4] X. Yan and Y. Lu, "Applying QR Code to Secure Medical Management," in *Journal of Physics: Conference Series*, vol. 1297, no. 2, p. 022096, October 2019.[4]

[5] W. C. Wu, "A QR Code-Based On-Street Parking Fee Payment Mechanism," in *IEEE Access*, vol. 7, pp. 5831-5837, January 2019. doi: 10.1109/ACCESS.2018.2898886.[5]

[6] V. Chaurasia, S., Jain and R. Shandilya, "Secure and efficient URL sharing using visual cryptography," International Journal of Applied Engineering Research*, vol. 12, no. 20, pp. 10266-10269, 2017.

[7] A. Saini and S. Singh, "Secure sharing of URLs using visual cryptography," *International Journal of Computer Applications*, vol. 178, no. 36, pp. 29-33, 2018.

[8] M. Garg, S. Choudhary, and S. Choudhary, "Secure URL sharing using visual cryptography and QR codes," *International Journal of Computer Applications*, vol. 178, no. 26, pp. 37-40, 2018.

[9] R. Verma and A. Varma, "Visual cryptography-based secure URL sharing system," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 8, pp. 167-171, 2016.

[10] R. Gupta and R. Bhatnagar, "Secure sharing of URLs using visual cryptography and steganography," International Journal of Computer Applications*, vol. 182, no. 9, pp. 1-5, 2019.

[11] N. Sethi and S. Sengar, "Secure URL sharing through visual cryptography and AES encryption," International Journal of Computer Science and Mobile Computing*, vol. 5, no. 6, pp. 155-161, 2016.

[12] P. Verma and S. L. Meena, "A novel approach for secure URL sharing using visual cryptography and AES encryption," *International Journal of Computer Applications*, vol. 174, no. 16, pp. 18-22, 2020.

[13] S. Kumar and M. Singh, "Secure URL sharing using visual cryptography and SHA-256 algorithm," *International Journal of Computer Applications*, vol. 182, no. 19, pp. 16-20, 2019.

[14] A. Bansal and M. Garg, "A secure URL sharing system using visual cryptography and Blowfish algorithm," *International Journal of Computer Applications*, vol. 162, no. 13, pp. 12-15, 2017.

[15] R. Rani and A. Jain, "Visual cryptography-based secure URL sharing using multi-fragmentation," *International Journal of Computer Applications*, vol. 178, no. 15, pp. 23-27, 2018.

[16] S. Sharma and O. Prakash, "A secure approach for URL sharing using visual cryptography and chaotic maps," *International Journal of Computer Applications*, vol. 182, no. 1, pp. 8-12, 2019.

[17] V. Kumar and M. Choudhary, "Secure URL sharing using visual cryptography and modified RSA algorithm," *International Journal of Computer Applications*, vol. 182, no. 8, pp. 19-24, 2018.

[18] M. Singhal and R. Yadav, "Secure URL sharing using visual cryptography and MD5 hashing," International Journal of Computer Applications*, vol. 182, no. 8, pp. 13-18, 2019.

[19] R. Patel and P. Sharma, "A novel approach for secure URL sharing using visual cryptography and elliptic curve cryptography," *International Journal of Computer Applications*, vol. 178, no. 37, pp. 29-33, 2018.

[20] A. Malhotra and A. Srivastava, "Secure URL sharing using visual cryptography and digital signature," *International Journal of Computer Applications*, vol. 182, no. 11, pp. 9-14, 2019.

[21] S. Singh and A. Mishra, "A secure URL sharing system using visual cryptography and RC4 encryption," *International Journal of Computer Applications*, vol. 182, no. 18, pp. 13-17, 2020.

[22] A. Jain and P. Sharma, "Secure URL sharing using visual cryptography and Hill cipher," International Journal of Computer Applications*, vol. 5, no. 3, pp. 48-52, 2016.

[23] R. Srivastava and S. Chauhan, "Secure URL sharing using visual cryptography and one-time pad algorithm," *International Journal of Computer Applications*, vol. 162, no. 6, pp. 8-12, 2017.

[24] S. Rajput and A. Bhardwaj, "A secure approach for URL sharing using visual cryptography and watermarking," *International Journal of Computer Applications*, vol. 178, no. 21, pp. 32-37, 2018.

[25] A. Kumar and R. Sharma, "Secure URL sharing using visual cryptography and chaotic S-box algorithm," International Journal of Computer Applications*, vol. 167, no. 1, pp. 1-5, 2017.

[26] T. Ma, H. Zhang, J. Qian, X. Hu, and Y. Tian, "The Design and Implementation of an Innovative Mobile Payment System Based on QR Bar Code," in *2015 International Conference on Network and Information Systems for Computers*, Wuhan, 2015, pp. 435-440.

[27] L. Burra P. Tumuluru and S. Gonaboia, "Secure QR-Pay System with Ciphering Techniques in Mobile Devices," *International Journal of Electronics and Computer Science Engineering*, P.V.P.Siddhardha Institute of Technology, Kanuru, Vijayawada, Krishna, 2012.

[28] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, and C. Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," *Mobile Information Systems*, vol. 2017, Article ID 4356038, 12 pages, 2017.

[29] C.-N. Yang, J.-K. Liao, F.-H. Wu, and Y. Yamaguchi, "Developing Visual Cryptography for Authentication on Smartphones," in Proc. of the International Conference on Computer, Informatics, Cybernetics and Applications (CICA)*, 2016, pp. 189-200. doi: 10.1007/978-3-319-44350-8_19.

[30] S. Singh, "QR Code Analysis," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 5, May 2016, ISSN: 2277-128X.