International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 01 | January - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Secure Link Sharing through QR Code Encryption Using Visual Cryptography

D.Bharath, Dr. Arun. A, Sushant Kumar Singh

Department of Networking and Communications, SRM Institute of Science and Technology

Department of Networking and Communications, school of computing, Faculty of Engineering and Technology, SRM Institute of Science and Technology

Department of Networking and Communications, SRM Institute of Science and Technology

---

Abstract - For the purposes of this study, we will examine what goes into creating a QR-code-based system for disseminating links. QR codes' ability to facilitate the sharing of links has led to their steady growth in popularity. However, it is crucial to address any security concerns raised by QR-based online platforms. Our first priority is guaranteeing the safety and integrity of each link sharing operation while maintaining the authenticity of all parties involved in the transaction, from the sender to the recipient. Our proposed solution makes use of QR codes and incorporates cryptography through a web-based application. As a result, we'll be able to reach our objective. Our website's intuitive design allows visitors to quickly and easily share website addresses through the use of QR codes.

***Key Words*:** Secure Link Sharing, QR Code Encryption, Visual Cryptography, Data Protection, Digital Information Exchange, Privacy and Security, Visual Representation, Reconstruction Key, Usability Testing, Secure Data Transmission.

1.INTRODUCTION

In today's age, which is increasingly defined by the predominance of digital technology, there has never been a greater demand for secure and efficient information-sharing techniques. The proliferation of mobile devices and the widespread adoption of quick-response (QR) codes as a vehicle for spreading data have opened up new horizons in the field of secure link sharing. These two changes have happened within the past several years. This paper, titled "Secure Link Sharing through QR Code Encryption Using Visual Cryptography," takes a fresh look at the issue of insecure link sharing by combining QR codes with visual cryptography.
Keeping private information and connections safe is of paramount importance in today's interconnected digital environment [1]. When it comes to protecting the privacy and security of the content being shared, traditional means of link exchange—such as manually copying and pasting URLs or utilizing unencrypted QR codes—often fall short. Methods such as cutting and pasting URLs from an address bar are examples.

Because of their widespread popularity and adaptability, QR codes are a prime candidate for the method we've devised, which builds on these codes' natural strengths while also bolstering their security through the use of visual cryptography. Visual cryptography is a subset of encryption that uses images to protect information [2]. As a result, the secret is protected from prying eyes and is difficult to uncover.
This article's primary goal is to offer a comprehensive breakdown of the reasoning behind our unique approach to secure link sharing, as well as an in-depth examination of its implementation and the advantages that come with adopting it. In this article, you'll learn not just how QR codes and visual cryptography operate but also the underlying concepts that power them [3]. This study aims to prove that when these two technologies are combined, a secure and efficient system is created for exchanging communications and data.

Furthermore, we will investigate potential applications of our secure link-sharing strategy. Our journey will take us across many different industries, including those concerned with the security of sensitive data during transmission, such as healthcare, finance, e-commerce, and communication.

In the next sections, we'll explore the theoretical foundations of our approach as well as the finer technical specifics. Real-world examples and practical applications will illuminate the way forward [4]. We'll be upfront about some of the challenges and restrictions that may stand in the way of widespread use of encrypted QR codes and other forms of visual cryptography for sharing links over the web with confidence. We will also be upfront about the difficulties and restrictions that may arise.

After reading this article, you will have a firm grasp on the unique paradigm we provide, as well as an appreciation for how it might help modern digital communities share links more securely and efficiently. This is what will happen when the research is finished [5]. The ability of a QR code, a two-dimensional matrix barcode, to efficiently encode and store massive amounts of data has earned it widespread praise. This is due to the factors discussed in the preceding sentence. QR codes are useful in many different fields because of their flexibility, including medicine, education, and finance. These programs facilitate efficient and straightforward information sharing. Many QR-based secure methods have been created for the purpose of exchanging links over the internet, with varying degrees of speed and security.

Users' privacy is of paramount importance as the usage of digital images continues to grow in the context of multimedia technologies [6]. To achieve the necessary level of privacy and security, picture encryption has emerged as a crucial tool. Military communications, telemedicine, medical imaging, and multimedia systems are just a few of the many areas that might benefit from image encryption. Improvements in multimedia and network technology have led to widespread use of the Internet and mobile networks for storing and transmitting images, especially those in color. The aforementioned progress is what made this pattern possible.

It's crucial to remember that image encryption is distinct from data encryption. Image encryption has its own challenges for protecting sensitive information during the processing and transmission of digital images. Maintaining a picture's

authenticity and privacy is something that must be constantly thought about. The resilience of digital images to even small changes is greater than that of data, with changes to individual pixels having far less of an effect on the final image than would be the case with data. While every modification to a digital image might theoretically leave it open to future security breaches, the margin of error for such alterations is typically larger than that for analogous data modifications [7]. As part of our research article titled "Secure Link Sharing through QR Code Encryption Using Visual Cryptography," we will start looking into how the rudiments of visual cryptography can be used to increase the security of QR codes that are used for link sharing. We will be focusing on the practical implications of these ideas. The demand for privacy and data security is on the rise in the age of digital technology, and this effort addresses that need.

1.1. Visual Cryptography

Visual cryptography refers to a specific method of encrypting visual information, which includes a wide range of media forms including images and text. Information is encrypted throughout this process. This method of decryption produces a visual representation, which makes advantage of the human visual system's natural features to transform encrypted data into visuals [8]. Although visual cryptography provides a robust foundation for safe digital communication, it is important to note that it is primarily designed for one-time-use purposes. This has to be stressed since it is crucial to understanding the argument.

1.2. Fundamentals of Visual Cryptography

Visual cryptography relies on the principle that image segments should be created in such a way that they cannot be used to reconstruct the original image. The whole field of visual cryptography is predicated on just one simple idea. On the other hand, when they are assembled, they show what was concealed within the picture all along [9]. The techniques for creating and reconstructing shares are discussed in detail, along with the mathematical foundations of visual cryptography. It also explains the ideas behind visual cryptography, which is useful background information.

1.3. Visual Cryptography Schemes

The term "visual cryptography" is used to refer to a broad subject that includes many distinct types of schemes, such as (2,2), (2, n), and (k, n). In the same way that a toolbox has several implements, each software is tailored to perform a certain task. In this part, we will examine these tactics in greater depth so that you know when and how to employ them. In this section, we'll talk about the pros and cons of each approach and how you might use them in different contexts to determine which one is best for your needs [10]. You may use the data in this post to figure out what approach will benefit you the most.

2. PROBLEM STATEMENT

It is more critical than ever before to maintain the secrecy of private information and sensitive connections in a society that is both digitally linked and driven by data. Traditional methods of link sharing, such as passing around unencrypted URLs or protecting shared content with a password, do not provide the kind of robust security that is required to guarantee the confidentiality and authenticity of the information that is being sent around [11]. As a method of communicating data between mobile devices, the use of Quick Response (QR) codes is gaining popularity and is expected to become more widespread in the near future [12]. This will provide new options for the sharing of links that are both safer and more efficient. There is a pressing need for innovative planning that might potentially overcome the limitations of currently available technology and deliver increased safety.

The task at hand is to devise a solution that makes use of the well-established efficacy of QR codes in information sharing and combines the principles of visual cryptography in order to further enhance the safety of hyperlinks. This is the challenge that lies ahead. It is possible to generate a visual representation of encrypted data that is unreadable even if the data is intercepted in its whole if it is first divided up into several parts and then reassembled [13]. The challenge lies in the development and testing of this new technology to guarantee that it is not only very risk-free but also simple to use and relevant in real-world scenarios across a variety of fields, including but not limited to healthcare, banking, electronic commerce, and communication.

With this issue description in hand, researchers might start working on a solution that would fulfill the expanding need for private and secure internet communication by offering a failsafe way of exchanging connections [14]. This would be a solution that would meet the growing demand for private and secure internet communication.

2.1. *Literature review*

N. Senthilkumar, A. Sathish, S. Sasikumar, S. Satheesh and P. Sridhar, et. al [1], This specific reference details a work concerning the development of a security algorithm for image encryption, focusing on employing the AES (Advanced Encryption Standard) Crypto Processor. The aim appears to be achieving high security while optimizing power consumption, likely with relevance to the broader context of sustainable computing and data communication systems as per the conference's theme.

C. Bhardwaj, H. Garg and S. Shekhar, et.al [2], The paper seems to discuss a method or approach focusing on the security enhancement of QR codes by utilizing both cryptography and visual cryptography techniques [15]. This likely explores innovative methods to safeguard QR code information through a combination of cryptographic principles and visual encryption methods, ensuring increased protection and privacy in the realm of QR code usage, possibly within the context of computational intelligence and sustainable engineering solutions, as aligned with the conference theme.

Neamah, A. F. et.al [3], The paper likely presents a case study examining the implementation and utilization of a data warehouse in the context of university management, specifically focusing on Wasit University. The study could encompass aspects related to the adoption, functionality, and impact of data warehousing technology in handling university data for administrative, academic, or decision-making purposes [16]. Such analyses are significant in understanding the practical implications and benefits of data warehouse systems within educational institutions, shedding light on their effectiveness, challenges, and potential improvements for managing and utilizing university-related data.

Snehal Kundlik Waybhase, Prashant Adakane, et.al [4], The content likely focuses on the application and implementation of the Advanced Encryption Standard (AES) for ensuring data security. This paper may delve into the technical aspects and practical applications of AES in safeguarding data, discussing its algorithms, methodologies, and the significance of utilizing AES in contemporary information security. The objective might be to explore how AES contributes to data protection, potentially highlighting its advantages and relevance in the realm of engineering and technology, particularly within the context of information security and data protection strategies.

Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, and ChinChen Chang, et.al[5], This paper likely explores various authentication methods or schemes for mobile payment systems, utilizing a combination of QR codes and visual cryptography techniques. The authors might discuss different strategies or approaches involving the use of QR codes and visual cryptography to enhance the security and authentication processes in mobile payment transactions. The focus might be on proposing and evaluating different mechanisms to ensure secure and reliable authentication in the context of mobile financial transactions, contributing to the field of mobile information systems and security.

2.2. Objective

The fundamental objective of this study is to provide a reliable and efficient method of transferring links using QR codes. Visual cryptography will be used to further strengthen the security of this method. There were initial goals in mind when developing this technique. First and foremost, it seeks to enhance data security by successfully shielding public connections from interception and illegal access. Second, the approach strives to be equally effective and simple to use, so that people of diverse educational backgrounds and technical proficiency may benefit from it. Another major objective is to demonstrate the method's practicality in settings including healthcare, banking, e-commerce, and communication by protecting critical data in transit [17]. In addition, we'll conduct usability tests to see how straightforward it is to use the strategy. As long as the reconstruction key is not accessible, sensitive information will remain concealed even if individual QR code sharing is intercepted, as confirmed by the security evaluations. When assessing the effectiveness of the method, it will be crucial to think about how it scales over many different data-sharing use cases. Finding and fixing major issues and limitations is crucial to this study since it will shed light on the real-world effects of the proposed approach. The study will conclude with a forward-looking view, elaborating on possible changes and adjustments in light of new technology and shifting security norms. To maintain its usefulness and flexibility to satisfy the evolving needs of digital data security and link sharing, this is essential.

2.3. Existing system

Existing systems and practices for link sharing relied mostly on traditional techniques for transferring links and sensitive data until the advent of the proposed technology. When the new strategy was created, things started to shift. These methods sometimes lacked the substantial protection required to safeguard the information being transferred, leaving the door open to risks and data breaches. The existing mechanism for link sharing is broken down into the following sections, each of which will be discussed in detail below.

Uniform Resource Locators (URLs) were often exchanged in an unsecured format when links were shared in the past. Despite the apparent ease of this method, no measures have been taken to ensure the confidentiality of the transferred data [18]. The information on the website is accessible to anybody with the URL.

Password-protected links are an effort by some of the currently available systems to increase security beyond what is already there. Users would need to enter a password in order to gain access to the content. However, because it relies on users' ability to develop and keep strong passwords, this technique is vulnerable to breaches that are related to passwords.

SSL and HTTPS encryption When sending private information over the internet, both HTTPS and SSL encryption were employed [19]. While this approach works wonderfully for interactions on websites, it is limited to web links and does not deal with the broader issue of link sharing. The approach is efficient, but it can't be implemented.

Two-Factor Authentication (2FA): When 2FA was deployed, it added an extra layer of security to all shared connections. Users were often required to provide a password and a one-time code sent to their mobile device as two separate forms of authentication before gaining access.

The Public Key Infrastructure (PKI) was utilized for user authentication and encrypted data communications in more complex computer systems. Pairs of cryptographic keys were used for both encryption and decryption via PKI.

URL Security-Focused Shortening Services In an effort to make their abbreviated URLs safer, certain URL shortening providers have included security measures, including link expiration and access restriction [20]. People can choose to disable links after a certain period of time has passed or restrict access to specific individuals.

Blockchain technology has been implemented in cutting-edge systems to ensure the trustworthiness of hyperlinks. Such networks facilitate the distribution of links. The immutability and decentralization of blockchain technology ensure its security.

In terms of security, user friendliness, and flexibility, the prior systems covered a broad spectrum. Despite this, there is a need for improvement in the area of secure link sharing methods that are also easy to use. The need for such a system motivated the development of "Secure Link Sharing through QR Code Encryption Using Visual Cryptography." This method uses visual cryptography to protect QR codes.

2.4. Proposed system

The proposed system is designed to revolutionize the way links and sensitive data are shared in the digital age. It leverages the power of Quick Response (QR) codes, recognized for their efficiency in data sharing, and integrates the principles of visual cryptography to enhance the security of shared links [21]. This innovative system addresses the limitations of existing link sharing methods by offering a comprehensive and secure solution.

Key Features of the Proposed System:

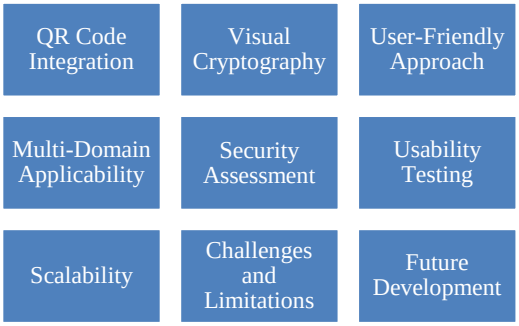

Figure 1: key features of the proposed system

Figure 1 shows the proposed system utilizes secure link sharing via QR codes encrypted using visual cryptography. Key features include robust encryption for secure data transmission, visual cryptographic methods for enhanced security, and convenient QR code technology for sharing sensitive information while ensuring privacy and integrity.

QR Code Integration: The heart of the system is the use of QR codes. These two-dimensional barcodes can efficiently encode a wide range of data, including URLs, text, and more. QR codes are versatile and accessible to a wide audience, making them an ideal choice for link sharing.

Visual Cryptography: The proposed system employs visual cryptography to divide the encrypted data into multiple shares, creating a visual representation of the information [22]. Each share, when viewed individually, reveals no information about the original content. The security of shared links is significantly enhanced through this innovative technique.

User-Friendly Approach: The system is designed to be user-friendly, ensuring that individuals with varying technical proficiencies can easily share and access links [23]. The process of sharing and accessing links is made as intuitive as possible.

Multi-Domain Applicability: The system's practical applicability spans diverse domains, including healthcare, finance, e-commerce, and communication. It provides a secure means of sharing sensitive data in various real-world scenarios.
Security Assessment: The security of the proposed system is rigorously evaluated to ensure that even if QR code shares are intercepted, the shared content remains confidential without the reconstruction key.

Usability Testing: Usability testing is conducted to assess the approach's ease of use, ensuring that users can effectively navigate the system.

Scalability: The system is assessed for scalability, ensuring its effectiveness in handling a wide range of data sharing scenarios, from simple text-based URLs to complex data sets.
Challenges and Limitations: The system identifies and addresses potential challenges and limitations, offering insights into the practical implications of its use.

Future Development: The proposed system takes a forward-looking approach, considering potential advancements and adaptations to emerging technologies and evolving security trends to ensure its ongoing relevance and adaptability.
By integrating QR codes with visual cryptography, the proposed system aims to set a new standard for secure and user-friendly link sharing. It addresses the increasing demand for data protection and privacy in the digital age and provides a robust solution for secure link sharing in a variety of real-world applications.

3. METHODOLOGY

The implementation stage is crucial in developing the proposed strategy into a workable and effective system. In this phase, the infrastructure necessary for safe link sharing is built and put into place. Here is a rundown of the most crucial steps taken and the participants involved in the implementation process:

The Evolution of Computer Programs:

Develop the system's software by designing and developing its individual parts. This includes the front-end, the QR code generator, and the visual cryptography techniques. The method should be adhered to, and development should be carried out, so that they are in harmony with the structure and operation of the system.

Integrating Visual and Textual Security:

Use various forms of visual cryptography to decipher QR codes and obtain the underlying data. Develop the required procedures and algorithms to guarantee the integrity of the creation and distribution of these shares.

User-Friendly Interaction Design:

Develop a simple and intuitive graphical user interface for the software. With this interface, users can easily share links and gain access to those links through QR codes. Focus on making everything simple and easy to use.

Additional Safeguards:

Implement strong security measures to guard any shared connections. Data encryption and decryption, user authentication, and secure file distribution are all possible examples.

In-the-wild Evaluation:

Put the system through its paces in a wide range of real-world settings, including healthcare, finance, e-commerce, and communication. Find out if it can be used in the real world and how well it performs under such conditions.

The functionality of:

You may gauge the system's ease of use by conducting usability testing with potential end users. Seeking user feedback and making necessary improvements may enhance the user experience.

Scalability Analysis:

Verify that the system can handle a broad range of data sharing situations, from simple text-based URLs to more complex data sets, by looking into its scalability. See how it does when subjected to varying loads.

Verifying Safety Efforts:

Test the system thoroughly to ensure that it can withstand data interception and other forms of intrusion. Protect the anonymity of all shared URLs, even if the sharing of individual QR codes is being tracked.

Challenges to overcome and boundaries to respect help lower the chances of:

Plan ahead for any roadblocks and challenges that may arise during deployment. Adjust the system so that it may continue to be utilized in practice while also addressing these issues.

Supplying Evidence:

Software development, security precautions, and test results should all be recorded as part of the implementation process. This documentation is crucial for both current and future system upkeep and enhancements.

User Instructions:

Training and support should be made available to users who will be utilizing the system for the purpose of exchanging secure links. Make sure they have a firm grasp on how to make the most of the system.

Utilization of:

Put the software in place in the appropriate application contexts and make it accessible to users who require the capacity to exchange encrypted connections.

If this system is implemented as planned, the proposed method for adding an extra layer of security based on visual cryptography to the exchange of links via QR codes will become a reality, providing a safe and effective solution. The need to keep private data safe is growing in importance in the era of ubiquitous digital connectivity. This will be a useful step in meeting that need.

4. ALGORITHMS OF THE PROPOSED METHOD

Developing algorithms for the proposed system requires the creation of step-by-step procedures to guarantee the safe and effective exchange of links via QR codes. The following is a list of the most important algorithms used by the system:

The Algorithm for Generating QR Codes:

This technique describes the procedure for producing QR codes that may be used for links and other types of data. It also includes modifying the look of the QR code based on the requirements, in addition to encoding the data into a QR code.

An Algorithm for the Segmentation of Visual Cryptography:

The QR code is segmented into many parts by the segmentation algorithm, which makes use of visual cryptography techniques. This guarantees that no information about the original material is revealed in any of the individual shares.

The algorithm for distributing shares is as follows:

This method describes in detail how the shares that are produced via the use of visual cryptography are then given to the

appropriate receivers. It concerns the safe distribution of these shares, whether they are sent out in physical form or sent electronically.

Algorithm for the Generation of Reconstruction Keys:

The technique that is used to generate the reconstruction key is extremely important since it is required in order to decode the shared QR code. It describes the process that is used to generate this key and then safely distribute it to the receivers.

The Algorithm for Reconstructing a QR Code:

Through the use of the reconstruction key and an overlay of the shared QR codes, this technique describes how receivers may rebuild the original QR code. It guarantees that the URL that has been shared may be viewed.

Algorithm for Assessing the Level of Security:

The security evaluation methodology outlines the steps that must be taken in order to determine how resistant the system is to being intercepted or accessed by unauthorized parties. It involves evaluating the secrecy of shared connections in the event that individual shares are snooped on.

Testing Methods for User Friendliness:

This method provides a step-by-step guide for doing usability testing, which may be used to evaluate how user-friendly and effective a system is. Collecting input from customers and making adjustments based on that feedback are both part of this process.

Testing Method for Scalability Algorithm:

The technique for assessing scalability provides an explanation of how the system's capacity to manage a broad variety of data sharing situations is evaluated. It entails evaluating performance under a variety of different loads.

Mitigation Algorithm: Obstacles and

Limitations Challenges and Limitations:

During the process of putting the system into action, there is the possibility that a number of difficulties and constraints may develop. This method provides a solution to such problems. It outlines the measures that must be taken in order to modify the system in order to address these concerns.

The User Training Algorithm is as follows:

The user training algorithm provides an overview of the training and assistance that will be made available to users of the system who will be using it to share secure links. It guarantees that users have a clear understanding of how to make efficient use of the system.

These algorithms are absolutely necessary for the proposed system to work correctly and to maintain its level of safety. They give a clear set of instructions for each stage in the process of link sharing and guarantee that users may share links with confidence and access them securely through the use of visual cryptography and QR codes by providing the clear set of instructions

5. RESULT AND DISCUSSION

This section highlights the research related to secure link exchange via QR code encryption utilizing visual cryptography. The performance of our technique is initially examined across several model architecture configurations. The most effective algorithm we identified for secure link sharing via QR code encryption with visual cryptography, These results constitute a significant step towards improving the security and reliability of link sharing via QR codes with visual cryptography.

Figure 2: message Encryption

Figure 2 shows the message encryption involves converting plain text into a coded form using algorithms or ciphers, safeguarding its content from unauthorized access. It ensures data confidentiality by transforming information into an unreadable format, requiring a decryption key for interpretation, bolstering security and privacy in digital communication and sensitive data transmission.

Figure 3: QR Generation of encrypted message

Figure 3 illustrates the message undergoes encryption using cryptographic algorithms, transforming it into an unreadable format. The encrypted text is then embedded within a QR code, creating a scannable image that, when decoded, reveals the original message. This method enhances data security during transmission and storage, combining encryption with the convenience of QR codes for sharing sensitive information.

Figure 4: encrypted QR code

Figure 4 combines the elements of encryption, visual cryptography, and QR code technology. Initially, the information undergoes encryption, transforming it into an unreadable format to secure its content. Visual cryptography further enhances security by splitting the encrypted data into multiple shares or components. These components are then embedded within a QR code, creating a scannable image. When these separate parts are visually combined or superimposed, the original encrypted information is revealed, ensuring higher security for sensitive data stored or transmitted via QR codes.

Figure 5: scaling of QR code

Figure 5 shows the "scaling of QR codes" refers to the process of adjusting the size of a Quick Response (QR) code while maintaining its readability and functionality. Scaling involves resizing the QR code, either enlarging or reducing its dimensions, without compromising its scanning and decoding capabilities. Proper scaling ensures the QR code remains scannable by devices, retaining its information content and accuracy even when adjusted in size, allowing for versatility in its application across various mediums and sizes without losing its scanning functionality.

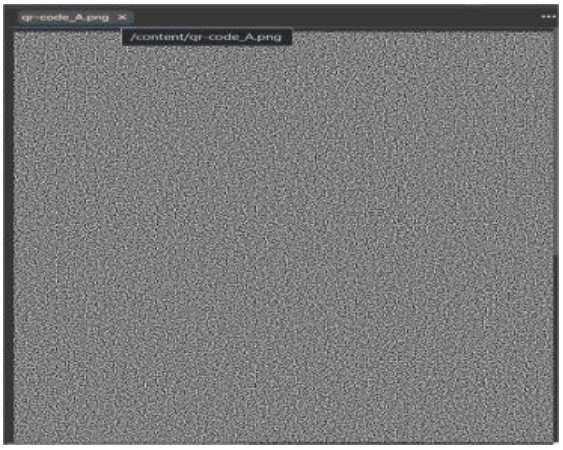

Figure 6: shadow image (1)

Figure 6 shows that in QR code visual cryptography, a "shadow image" refers to a component of a visual cryptographic scheme used to secure information within a QR code. Visual cryptography involves breaking an image or data into multiple shares or layers, where each share individually reveals only partial information. These shares are then combined to reveal the complete content.

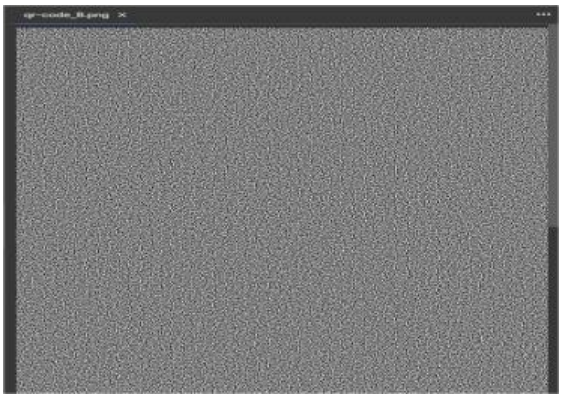

Figure 7: shadow image (2)

Figure 7 shows the concept of a "shadow image" involves using layers or shares of an image that, individually, seem like random noise or patterns. When overlaid or combined in a specific way, these separate components visually merge, revealing the encoded information or image. The shadows or individual components, when put together, form the complete visual information embedded within the QR code. This method enhances security by requiring all the different "shadows" to be visually superimposed to decode the hidden message, providing

a layer of protection for sensitive information stored or transmitted via QR codes.

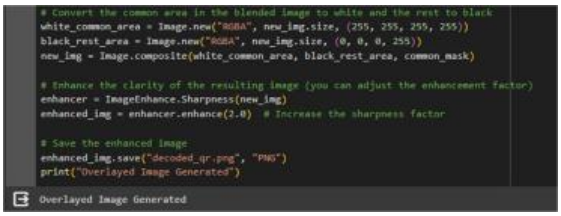

Figure 8: overlaying of image

Figure 8 shows overlaying of images in visual cryptography involves the process of combining or superimposing multiple encrypted images to reveal hidden information. In visual cryptography, a single image or piece of information is encrypted and divided into multiple shares or layers. Each individual share on its own does not disclose the original content and may seem like random noise or patterns.

Figure 9: overlayed image

Figure 9 shows an "overlayed image" refers to a composite image created by combining or superimposing two or more individual images or graphical elements. This overlaying process involves placing one image on top of another, allowing their contents to merge or coexist within the same space.

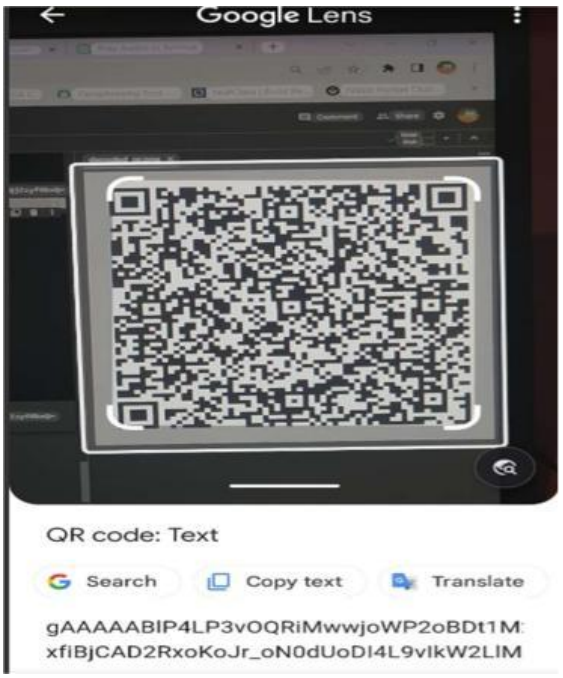

Figure 10: scanning the QR code

Figure 10 shows that scanning a QR code involves using a smartphone or a dedicated QR code scanner device equipped with a camera to read and interpret the information stored within a Quick Response (QR) code.

Figure 11: encrypted message in QR code

Figure 11 shows an "encrypted message in a QR code" involves encoding sensitive or confidential information in a manner that secures it from unauthorized access and embedding it within a Quick Response (QR) code.

Figure 12: decryption of message to original message

Figure 12 illustrates the decryption of a message involves reversing the process of encryption to restore the original, understandable content from its unreadable, encrypted form. The decryption process requires a specific decryption key or algorithm that can convert the encrypted data back into its original form.

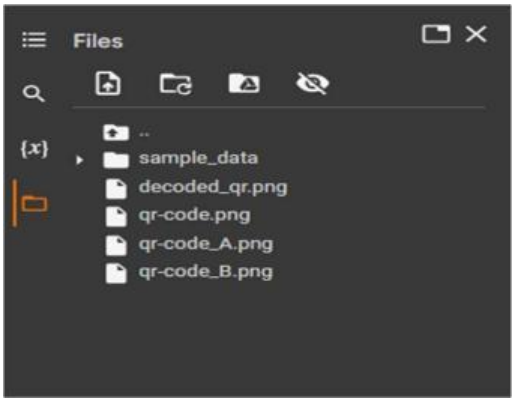

Figure 13: images stored

Figure 13 shows the process of creating, saving, and interpreting QR codes using digital images.

6. CONCLUSIONS

In light of the security flaws plaguing QR-based online services, we came up with a foolproof method of sharing links that leverages both visual cryptography and QR codes. Our work ensures the credibility of both parties in link-sharing transactions by addressing issues of security, authenticity, and secrecy.
By allowing access to only approved parties, visual cryptography significantly reduces the likelihood of data breaches and unwanted access. This new solution provides a simple and secure way to share site addresses using encrypted QR codes, all through a straightforward online service.

In conclusion, our research makes important contributions to the development of secure link-sharing practices, fostering a safe digital environment for users and lessening the risks associated with QR-based link sharing. Our proposed method has the potential to increase the safety and dependability of link-sharing systems as a whole, hence boosting people's faith in their online interactions.

REFERENCES

[1] N. Senthilkumar, A. Sathish, S. Sasikumar, S. Satheesh and P. Sridhar, "High Security and Low Power AES Crypto Processor Security Algorithm for Image Encryption," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS),Erode, India, 2023, pp. 1251-1255, doi: 10.1109/ICSCDS56580.2023.10105112.

[2] C. Bhardwaj, H. Garg and S. Shekhar, "An Approach for Securing QR code using Cryptography and Visual Cryptography," 2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2022, pp. 284-288, doi: 10.1109/CISES54857.2022.9844332.

[3] Neamah, A. F. (2021, March). Adoption of Data Warehouse in University Management: Wasit University Case Study. In Journal of Physics: Conference Series (Vol. 1860, No. 1, p. 012027). IOP Publishing.

[4] Snehal Kundlik Waybhase, Prashant Adakane, 2022, Data Security using Advanced Encryption Standard (AES), INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 11, Issue 06 (June 2022)

[5] Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, and ChinChen Chang, "Multiple Schemes for Mobile Payment Authentication UsingQR Code and Visual Cryptography," Mobile Information Systems, vol. 2017, Article ID 4356038, 12 pages, 2020.

[6] R. Mohamad, "Data hiding by using AES Algorithm: Data hiding by using AES Algorithm," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 4, pp. 112-119, 2022.

[7] W.-P. Fang, "Offline QR code authorization based on visual cryptography," in Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP '11), pp. 89–92, October 2020

[8] H. T. Hazim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[9] L. Yu, D. Zhang, L. Wu, S. Xie, D. Su and X. Wang, "AES Design Improvements Towards Information Security Considering Scan Attack," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 322-326, doi: 10.1109/TrustCom/BigDataSE.2018.00056.

[10] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

[11] Saha, R., Geetha, G., Kumar, G., & Kim, T. H. (2018, November 6). RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys. Security and Communication Networks; Hindawi Publishing Corporation. https://doi.org/10.1155/2018/9802475

[12] 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," 2018 International Conference on Network and Information Systems for Computers, Wuhan, 2018, pp. 435-440

[13] M. F. Tretinjak, "The implementation of QR codes in the educational process," 2019 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2019, pp. 833- 835

[14] M. Xu, L. Lv, J. Zhang, M. Xu, C. Zhang, and J. Zhang, "A New QR Code Multi-layer Encryption System based on Image Geometric Processing," in 2019 IEEE International Conference on Mechatronics and Automation (ICMA), 2019: IEEE, pp. 1-5. https://doi.org/ 10.1109/ICMA.2019.8816462

[15] R. Dudheria, "Evaluating features and effectiveness of secure QR code scanners," in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017: IEEE, pp. 40-49. https://doi.org/10.1109/CyberC.2017.23

[16] L. Feng and Q. Y. Wei, Cheating Prevention of Visual Cryptography, Springer International,Berlin, Germany, 2015

[17] N. Buckley, A. K. Nagar, and S. Arumugam, "Visual secret sharing between remote participants," International Journal of Computer Applications, vol. 103, no. 2, pp. 8–17, 2014

[18] Sangeeta Singh. May 2019. "QR Code Analysis" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, ISSN: 2277 128

[19] Rosziati Ibrahim and Teoh Suk Kuan, Steganography Imaging System (SIS): Hiding Secret Message inside an Image http://www.iaeng.org/publication/WCECS2010/WCECS2010_pp144-148.pdf

[20] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, Overview: Main Fundamentals for Steganography http://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pd

[21] Salim, H.T., et al., Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN. International Journal of Interactive Mobile Technologies, 2022. 16(8).

[22] Farhan, R.I., A.T. Maolood, and N. Hassan, Hybrid Feature Selection Approach to Improve the Deep Neural Network on New Flow-Based Dataset for NIDS. Wasit Journal of Computer and Mathematics Science, 2021: p. 66-83.

[23] Asgarnezhad, R., et al., An Effective Algorithm to Improve Recommender Systems using Evolutionary Computation Algorithms and Neural Network: Using Evolutionary Computation Algorithms and Neural Networks, an Effective Algorithm to Improve Recommender Systems. Wasit Journal of Computer and Mathematics Science, 2022. 1(1): p. 27-35.