International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 06, June 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Data encryption through QR code and steganography

Prof. Shrikant Dhamdhere[1], Sarthak Thorat[2], Shweta Patil[3], Sejal Dolas[4], Omkar Panchal[5]

Professor, Department of computer engineering, Moze college, wagholi, Pune, India[1]

Students, Department of computer engineering, Moze college, wagholi, Pune, India[2,3,4,5]

ABSTRACT

In the modern era of the internet, the security of information is of utmost importance. As a result, there is a growing focus on the practice of concealing information. Two fundamental techniques used for secure data transfer are cryptography and steganography. While cryptography involves encrypting the content of a message, steganography conceals the message within a cover medium. Quick Response (QR) Codes, which can encode text in both vertical and horizontal directions, are widely used for information storage.

This research introduces a novel method that combines QR codes and steganography for confidential communication. The proposed approach consists of two key phases. Firstly, the message is encrypted using a QR code encoder, resulting in a QR code representation of the encrypted content. Secondly, the encrypted QR code is seamlessly embedded within a color image, ensuring that the cover image appears unaltered to the naked eye. Importantly, this hiding process minimizes any visible distortions and maintains an exceptionally low Bit Error Rate (BER).

By merging the principles of steganography and QR codes, this approach enables secure and covert transmission of information. It offers a reliable and efficient means of transferring data while maintaining secrecy and safeguarding against unauthorized access. This innovative technique holds great potential for various applications in the digital realm where data privacy and confidentiality are critical concerns.

KEYWORDS- *Cryptography, Steganography, LSB, Data hiding, Stego-image, Diffie-Hellman Key Exchange, Security.*

INTRODUCTION

In today's digital era, the secure transmission and protection of sensitive information have become crucial concerns. As data breaches and unauthorized access continue to pose significant risks, the need for robust encryption techniques and covert communication methods has grown exponentially. This research paper delves into the exploration of data encryption through the combined utilization of QR code technology and steganography, offering a comprehensive study of their principles, methodologies, and potential applications in enhancing data security.

QR (Quick Response) codes have gained widespread popularity due to their capacity to store large amounts of data in a compact two-dimensional barcode format. With the ability to encode information in both horizontal and

vertical directions, QR codes offer versatility and ease of scanning, making them an ideal carrier for various types of data. Steganography, on the other hand, focuses on concealing information within cover media, making it virtually indistinguishable to unauthorized individuals.

The synergy between QR codes and steganography presents a unique opportunity to combine the strengths of both techniques, thereby enhancing data encryption and concealing the very existence of sensitive information. By encrypting data using QR codes and embedding them within cover media through steganographic methods, a multi-layered approach to data security can be achieved.

The objectives of this research paper are twofold: to explore the fundamental concepts and mechanisms of QR code technology and steganography, and to investigate their integration for data encryption and concealment purposes. Through a comprehensive analysis of QR code encoding and decoding algorithms, error correction techniques, steganographic methodologies, and encryption algorithms, the paper aims to provide insights into the strengths, challenges, and potential applications of this innovative approach to secure data communication.

Furthermore, this research paper will examine the security implications, performance metrics, and potential vulnerabilities associated with the combination of QR codes and steganography. It will also explore the practical applications of data encryption through QR code and steganography, including secure communication, digital rights management, authentication, and covert information exchange.

In conclusion, the integration of QR code technology and steganography offers a promising avenue for data encryption and covert communication in today's security-conscious environment. By leveraging the unique characteristics of QR codes and the concealment capabilities of steganography, this research paper aims to contribute to the advancement of secure data transmission and inspire further exploration in the field of information security.

LITERATURE SURVEY

In recent years, a range of research papers that explore different steganographic techniques for hiding information in images. Each paper investigates various aspects of steganography and proposes innovative approaches to enhance data security.

1. Parisa Gerami et al. (2012):

Gerami et al. optimize two image hiding techniques to improve the quality of stego-images. The paper focuses on finding the best block matching matrix and optimal substitution matrices. Particle swarm optimization (PSO) is utilized to determine the best pixel locations, leading to the transformation of the secret image into a new secret image. The proposed method aims to enhance the performance of image hiding techniques. (Gerami, 2012)

2. Rig Das et al. (2012):

This paper introduces a novel image steganography technique based on Huffman Encoding. The secret message is Huffman-encoded before embedding, and each bit of the Huffman code is hidden by altering the LSB of the pixel intensities in the cover image. The technique demonstrates the potential of utilizing Huffman Encoding for secure data hiding in images. (Das, 2012)

3. Mandal J. K., and Debashis Das et al. (2012):

The authors utilize the pixel value differencing (PVD) method for embedding secret data in each component of a pixel in a color image. However, they acknowledge that this approach may result in pixel values exceeding the range of 0-255. The paper highlights the challenges associated with PVD-based steganographic schemes. (Das M. J., 2012)

4. Ankit Chadha et al. (2013):

This paper introduces a novel steganographic method based on least significant bit manipulation and the inclusion of redundant noise as a secret key in the message. The technique is applied to data hiding in images and audio using discrete cosine transform (DCT) and discrete wavelet transform (DWT). The proposed method shows promising results in terms of efficiency and effectiveness. (Chadha, 2013)

5. Arun K. et al. (2015):

The authors devise a multi-level encrypted reversible data hiding (RDH) scheme for gray-scale cover images with highly sensitive content. The scheme utilizes histogram shifting for configurable embedding rate. The proposed approach aims to enhance data hiding capabilities while maintaining reversibility, thereby offering potential applications in sensitive data transmission. (K, 2015)

6. Muhammad Khan et al. (2015):

This research presents a secure image steganography method that combines cryptography, image transposition, and gray-level modification for true color images. Multiple encryption algorithms are employed to encrypt the secret key and secret information, which are then hidden within the host image pixels. The approach highlights the integration of encryption and steganography techniques for improved data. (Khan, 2015)

7. Jiayu Deng (2019):

The paper titled "LSB Color Image Embedding Steganography Based on Cyclic Chaos" proposes a technique for hiding secret messages in color images using a method based on cyclic chaos. It introduces an embedding algorithm that utilizes the chaotic function of generating seeds and a pseudo- random number generator (PRNG). The algorithm finds a pixel through the chaotic cycle system and embeds a three-bit secret message into the R, G, and B channels of the pixel. Compared to other color image embedding methods, the proposed algorithm offers higher visual quality and improved security. The paper includes a literature review on image steganography, an explanation of cyclic chaos, the design of the proposed scheme, a comparison with other image steganography techniques, and a conclusion. (Deng, 2019)

8. Jawwad A R. Kazi (2020):

The paper addresses the technique of steganography, which involves hiding data within an image to protect it from unauthorized access. The authors propose a new algorithm that aims to satisfy the requirements of steganography. In their approach, a cover image and a secret message are considered. The algorithm works by embedding each bit of the secret text into the pixels of the cover image. This process continues until the last bit of the secret text is embedded, effectively hiding the data under the image. The resulting image is then sent to the recipient, who

can reverse the process to retrieve the original text. They also assess the output image quality generated by both algorithms using the structural similarity measure. (Jawwad, 2020)

9. Nandhini Subramanian (2021):

The paper provides a comprehensive overview of the advancements made in the field of image steganography. In this paper, the authors specifically focus on steganography techniques applied to images. The objective is to provide readers with a summary of recent developments in this area. The paper likely discusses various steganography techniques used to embed information in images, such as LSB (Least Significant Bit) substitution, frequency domain techniques (e.g., Discrete Cosine Transform), and spatial domain techniques (e.g., spatial domain transformations). The authors may also explore advanced methods, such as adaptive steganography, in which the embedding process adapts dynamically based on image characteristics. The review paper aims to highlight the strengths and weaknesses of different image steganography techniques, as well as their applicability in real-world scenarios. It may discuss the challenges faced in steganalysis, which is the process of detecting hidden information in digital media. (Subramanian, 2021)

SCOPE

The scope for Data Encryption through QR Code and Steganography is extensive and encompasses various domains and applications.

1. Secure Communication: Data encryption through QR code and steganography can be utilized for secure communication channels, such as messaging platforms, email systems, and file transfers. By encrypting sensitive data and concealing it within QR codes embedded in images, the system ensures privacy and confidentiality during data transmission.
2. Digital Rights Management: In the digital content industry, protecting intellectual property and preventing unauthorized distribution is crucial. Data encryption through QR codes and steganography can be employed to embed watermarks, copyright information, or licensing details within digital media files, allowing content creators and distributors to track and control the usage and distribution of their content.
3. Authentication and Anti-Counterfeiting: The integration of QR codes and steganography can provide an additional layer of authentication and anti-counterfeiting measures. By embedding encrypted QR codes within product labels, packaging, or identification documents, manufacturers and authorities can verify the authenticity of products, documents, or credentials.
4. Covert Information Exchange: Data encryption through QR code and steganography enables covert information exchange in scenarios where secrecy is crucial, such as intelligence operations or confidential data transfers. By concealing encrypted information within innocuous-looking images or documents, the system allows for discreet communication while maintaining the appearance of non-sensitive content.
5. Secure Storage and Archiving: QR code-based encryption and steganography can be utilized for secure storage and archiving of sensitive data. By encrypting the data and embedding it within QR codes, organizations can

store information within images or documents, making it less susceptible to unauthorized access or data breaches.

6. Multimedia Protection: The combination of QR code encryption and steganography can be employed to protect multimedia content, such as images, videos, and audio files. By encrypting and concealing watermarks, copyright information, or ownership details within the multimedia files, content creators can deter unauthorized usage and protect their intellectual property.

PROPOSED SYSTEM

The proposed system aims to enhance data security through the integration of QR code technology and steganography. By leveraging the strengths of both techniques, the system provides a robust framework for data encryption and concealment. The following components and processes are involved in the proposed system:

1. QR Code Encryption:

1. The system employs a QR code encoder to encrypt the data that needs to be transmitted securely.
2. The QR code encoder utilizes encryption algorithms to transform the original data into encrypted form.
3. This encryption process ensures that the sensitive information is protected and cannot be easily accessed by unauthorized individuals.

2. Steganographic Concealment:

1. The next step involves hiding the encrypted QR code within a cover medium, such as an image.
2. The system utilizes steganography techniques to embed the encrypted QR code into the cover medium without causing any visible distortion.
3. Various steganographic methods can be employed, such as LSB (Least Significant Bit) replacement, spatial domain modification, or transform domain modification, to conceal the encrypted QR code within the cover medium.
4. The choice of the steganographic method depends on factors like imperceptibility, capacity, and robustness.

3. Transmission and Extraction:

1. The steganographically concealed image, containing the encrypted QR code, can be transmitted through a secure channel.
2. At the recipient's end, the concealed image is extracted.
3. The system utilizes steganographic extraction techniques to retrieve the encrypted QR code from the concealed image.
4. Once extracted, the encrypted QR code can be decoded using a QR code decoder to retrieve the original data.

4. Security and Evaluation:

1. The proposed system ensures data security by combining encryption and steganography techniques.
2. The system should undergo thorough security testing and analysis to evaluate its resistance against various attacks and vulnerabilities.

3. Performance metrics, such as bit error rate (BER), image quality, and data retrieval accuracy, should be measured and evaluated to assess the effectiveness and efficiency of the system.

Applications:

1. The proposed system has diverse applications in secure data communication, digital rights management, authentication, and covert information exchange.
2. It can be utilized in scenarios where data privacy and confidentiality are paramount, such as secure messaging, confidential document transmission, and secure storage of sensitive information.

Overall, the proposed system combines the encryption capabilities of QR codes with the concealment techniques of steganography to provide a comprehensive approach to data security. By encrypting data through QR codes and concealing them within cover media, the system offers enhanced protection against unauthorized access and ensures secure data communication in various applications.

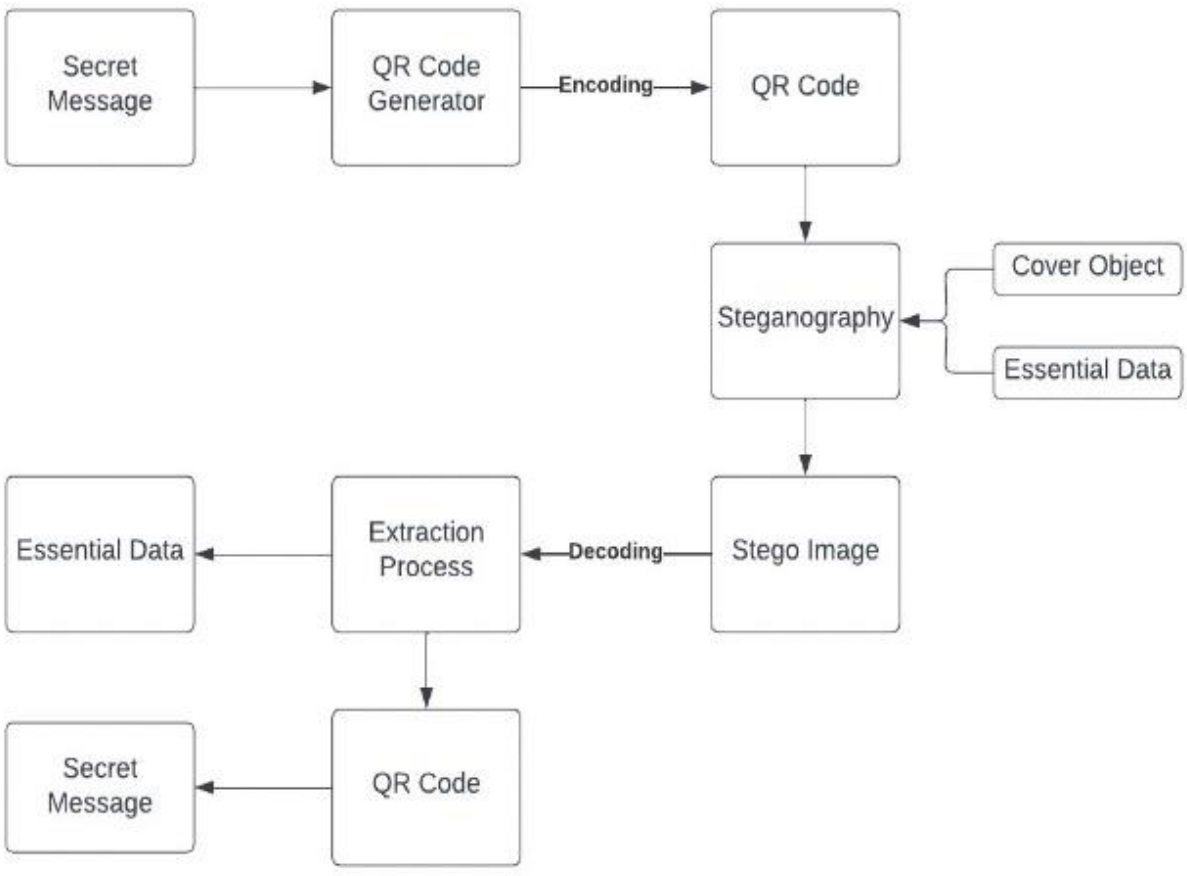

Fig 1. System Architecture

International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 06, June 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

I. RESULTS

Image File:

Fig 2. Original Image.

Text File Content:

Avengers, Assemble.

Stego Image:

Fig 3. Steganograted Image.

CONCLUSION

1. In this study, a novel steganography algorithm with dual-layer security was proposed. A system called "QR code generation of plain text and Stego Image" was developed using this algorithm. The effectiveness of the proposed algorithm was evaluated by testing various images with different sizes of hidden data. The results demonstrated that the stego image generated by the algorithm did not exhibit any noticeable distortion visible to the naked eye. This indicates that the new steganography algorithm is highly efficient in concealing data within an image.
2. The Stega Image system provides a valuable solution for users who seek to hide their data within images while maintaining privacy and confidentiality. By employing double-layer protection through encryption and steganography, the system ensures a high level of security for the embedded message.

3. Moreover, the system has a wide range of applications in various sectors. Notably, Stega Image offers several advantageous features. It supports input and output in all image formats, distinguishing it from other steganography tools that have limitations in supported formats. Additionally, it has the capability to hide various types of data or files, whereas other tools often support only text information or specific file types. The algorithm employed by Stega Image allows for embedding a larger amount of information, including text and images, compared to other steganography tools.
4. Overall, the proposed system presents a robust and versatile solution for secure data hiding within images. Its features, efficiency, and wide applicability make it a valuable tool for individuals and organizations seeking to protect their data while maintaining privacy and accuracy.

REFERENCES

[1] R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journalof Selected Areas in Communications, Vol. 16, No. 4, May 1998. [offline]

[2] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003 [offline]

[3] Animesh Shaw, Feb 24, 2015. Cryptography vs Steganography. https://www.slideshare. net/AnimeshShawRana/cryptography-steganography. Accessed 3rd Nov, 2017.

[4] Implementation Analysis of Covert Data Hiding Techniqueshttp://shodhganga.inflibnet. ac.in/bitstream/10603/56270/12/12_chapter%202.pdf Accessed on 11st Nov 2017

[5] Pramod Dhamdhere "semantic patent extended based on conceptual comparability of text with utilizing histogram arithmetic for illustrations to minimize trade mark", journal of data acquisition and processing, ISSN: 1004-9037,vol. 37 (5) 2022.

[6] David Kahn, May 30 - June 01, 1996. The History of Steganography https://www. researchgate.net/publication/220722213_The_History_of_Steganography Accessed on Nov 22nd 2017.

[7] Harpreet Kaur,Jyoti Rani; Sept 18, 2016.A Survey on different techniques of steganography https://www.matecconferences.org/articles/matecconf/pdf/2016/20/matecconf_ icaet2016_02003.pdf Accessed on Dec 3rd 2017.

[8] Abbas Cheddad, Kevin Curran, Paul Mc Kevitt; Aug 2009. Digital image steganography: Survey and analysis of current methods https://www.sciencedirect.com/ science/article/pii/S0165168409003648Accessed on Dec 8th 2017

[9] Pramod Dhamdhere "semantic trademark retrieval system based on conceptual similarity of text with leveraging histogram computation for images to reduce trademark infringement", Webology (ISSN: 1735-188X), Volume 18, Number 5, 2021.

[10] International Journal of Soft Computing and Engineering (IJSCE)ISSN:2231- 307,Volume3, Issue-5, November 2013 [offline]. Access on Dec 21st

[11] Champakamala .B.S, Padmini.K, Radhika .D. K; INTERNATIONAL JOURNAL OF ADVANCE COMPUTER TECHNOLOGY — VOLUME 3, NUMBER 4, http:// ijact.org/volume3issue4/IJ0340004.pdf Access on Jan 5th 2018