IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Analysis Of Image Steganography And Data Hiding In QR Code Using R-CNN Algorithm And Advanced Encryption Standard Cryptography Algorithm, Efficiency Measured By Peak Signal-To-Noise Ratio

[1]Mrs. S Sindhu, [2]Mrs. S Suriya, [3]D Monesh, [4]M Tharunkumar, [5]M Akash
[1,2] **Assistant Professor**, [3,4,5] UG tudents
[1]Department of Computer Science and Applications,
[1]SRM Institute of Science and Technology, Ramapuram, Chennai, India

Abstract: This essay focuses on the idea of employing a Quick Response Code (QR) code to embed an encrypted secret message into image data as a means of steganography. The Advanced Encryption Standard (AES) cypher algorithm is utilised in conjunction with the Discrete Wavelet Transformation (DWT) domain to protect the QR code embedding process. Additionally, the system is more secure because the encryption was able to defeat common QR code characteristics. This study attempts to develop an image steganographic technique with a high level of security and non-perceptibility. The QR code was specially compressed before being embedded, which improved the relationship between the method's capacity and security. Peak Signal-to-Noise Ratio (PSNR) was used to gauge the effectiveness of the suggested approach, and the outcomes were assessed against those of other steganographic techniques.

Index Terms **- QR Code, Steganographic method, R-CNN Algorithm, Peak Signal-to-Noise Ratio (PSNR).**

I. I INTRODUCTION

Image steganography is the art of concealing hidden messages in images in a way that the naked eye cannot see them[1]. The least significant bits of each pixel in the image are changed to achieve this. The concealed message is not visible because the human eye cannot distinguish minute differences in the smallest components of an image. The cover image and the hidden message are the two primary parts of the image steganography technique. The image that will be used to conceal the hidden message is the cover image. The information that must be concealed within the cover image is the secret message. Image steganography can be carried out using a variety of methods[3-6]. The least significant bit (LSB) method is one of the most often used methods. The secret message is substituted with the least important sections of the cover image's pixels using this technique.

This approach is straightforward and efficient, but it is susceptible to assaults that try to find a hidden message. Frequency domain, spread spectrum, and phase encoding methods are further approaches utilised in image steganography. Although these techniques are more difficult than the LSB method, they are more secure and resilient. Numerous uses for image steganography exist, such as covert communication, digital watermarking, and copyright defense[2]. But it can also be employed maliciously, such as to cover up malware or other destructive code inside an image.

II RELATED WORD

Quick Response Code (QR) codes are used in this picture steganographic technology to insert the encrypted secret message into the image information[8]. The QR code is embedded using the Discrete Wavelet Transformation (DWT) domain, and the embedding process is further protected by the Advanced Encryption Standard (AES) [11] cypher algorithmic rule. The method is more secure because applying the encryption allowed the conventional QR code characteristics to be broken[12]. Prior to the embedding method, a particular compression of the QR code was used to strengthen the relationship between security and capabilities of the strategy[13]. They claim that embedding tactics can be used on any colour or grayscale image with full space coverage and are made to work with common decoding software.

III PROPOSED WORK

Image steganography is a method of concealing confidential information within an image file without affecting the visual quality of the image. A two-dimensional barcode known as a QR code is frequently used to store brief pieces of information including URLs, product details, and contact information. Combining these two methods can result in a safe and effective way to conceal data.

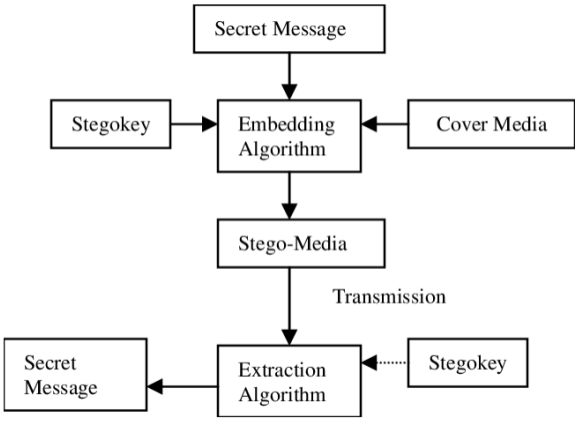

Fig 1 Workflow of the proposed work

In Fig 1, Here is a proposed Work for image steganography in data hiding in QR code:

Data encryption is the first step in securing confidential information. A safe encryption technique is used in this step. This action is required to guard against unauthorised access to the secret data.

Step 2: Generating a QR Code The encrypted data will be stored in a QR code, which will be created in the following step. Several open-source libraries for programming languages including Python, Java, and C++ can be used to create QR codes.

The encrypted data is then incorporated into the QR code by changing a few of its pixels in Step 3. Many steganography techniques, including LSB (Least Significant Bit) insertion, LSB matching, and spread spectrum, can be used to accomplish this[21]. The preferred level of security and the QR code's data storage capacity will determine the technique to use.

Step 4: Scan a QR code. Using a smartphone or a QR code reader, scan the QR code to complete the process. Using the same encryption process used for data encryption, the reader will be able to extract the concealed information from the QR code and decode it.

Step 5: Data Decryption: The encrypted data is decrypted using the same encryption algorithm that was used to encrypt it after being retrieved from the QR code.

4 SCOPE OF THE PROPOSED WORK

The work might concentrate on enhancing steganography algorithms' power to incorporate more data in carrier files, such images or audio files. Strength and security: The work might concentrate on creating stronger and more secure steganography algorithms that can withstand common attacks like data extraction and steganalysis. assistance for many media Creating steganography algorithms that can embed data into various media files, including photos, audio files, and video files, could be the main goal of the work. Real-time software[14] . Creating steganography algorithms that are quick enough to embed and discover concealed data in real-time applications, such video conferencing or live streaming, could be the main goal of the work. novel methods[11] The work might concentrate on creating unique steganography

methods that have never been investigated, like embedding and detecting hidden data using machine learning or artificial intelligence.

V ARCHITECTURE OF THE PRPOSED WORK

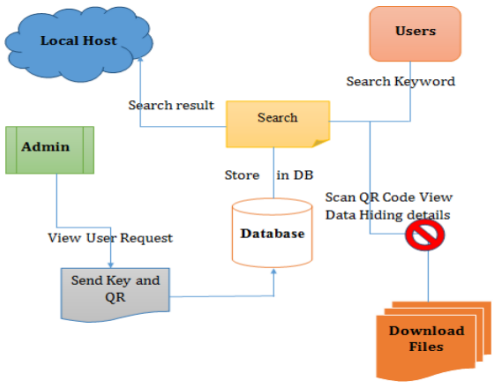

Fig 1 Architecture of the proposed work

The above-mentioned proposed model combines Steganography and cryptography. The strategy aims to make it challenging for the unauthorised individual to ascertain whether information is present. The information is safer because to dual security. With this model, sending several pieces of information over a public network is simple.

In industries like defence, business, banking, communication, and various government portals where information transmission is more important, this concept is highly helpful. In the future, massive amounts of data will be transmitted to the public network using audio or video steganography and cryptography without security violence since audio and video have a greater potential for data concealment than an image. The proposed model described above combines cryptography with mathematical modelling and stegnography.

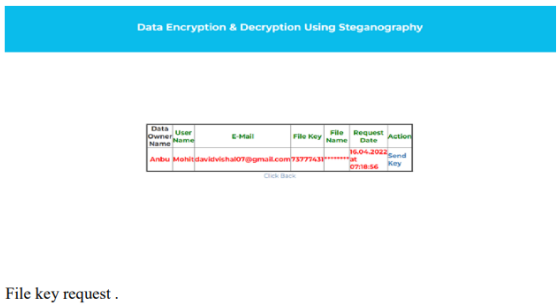

Fig 3 File key request send to QR code generator

The strategy aims to make it challenging for the unauthorised individual to ascertain whether information is present. Information is more safe thanks to dual security [18]. With this model, sending several pieces of information over a public network is simple. In industries like defence, business, banking, communication, and various government portals where information transmission is more important, this concept is highly helpful. The ability of audio and video to conceal data is greater than that of a picture, therefore in the future, massive amounts of data will be transmitted over a public network without the threat of security breach.

VI DATASET

Break Our Steganographic System (BOSSBase) is a benchmark dataset intended to assess the effectiveness of steganography techniques. 10,000 512x512 pixel grayscale images in four separate categories—natural images, binary images, camouflage images, and textured images—make up the collection.

The Universal Image and Video Dataset (UERD) is a sizable dataset that includes a variety of images and movies for use in steganography and other computer vision tasks. Over 350 000 photos and 10,000 films in various sizes and formats are included in the dataset.

A collection of pictures and videos called the Media Forensics and Integrity of Work (MIW) dataset is used to assess the security of digital media. The collection consists of stego-pictures created using a variety of steganography techniques as well as natural photographs. Break Our Steganographic System (BOSSBase) is a benchmark dataset intended to assess the effectiveness of steganography techniques. 10,000 512x512 pixel grayscale images in four separate categories—natural images, binary images, camouflage images, and textured images—make up the collection.

The Universal Image and Video Dataset (UERD) is a sizable dataset that includes a variety of images and movies for use in steganography and other computer vision tasks. Over 350 000 photos and 10,000 films in various sizes and formats are included in the dataset.

A collection of pictures and videos called the Media Forensics and Integrity of Work (MIW) dataset is used to assess the security of digital media. The collection consists of stego-pictures created using a variety of steganography techniques as well as natural photographs.

VII EXPERIMENTAL WORK

Convolutional Neural Networks (CNN) have been applied to a number of computer vision problems, including segmentation, object identification, and image categorization. In recent years, the use of CNN for image steganography has also been investigated. An overview of how CNN can be applied to image steganography is provided below:

choosing a carrier file:

Choose the appropriate carrier file type (such as an image, audio, or video). To ascertain the carrier file's capacity and suitability for steganography, examine its properties. Analyse the potential effects of embedding concealed data on the carrier file's quality.

Steganography algorithm selection:

Choose the best steganography algorithm for the Work after analysing the available options. Analyse the chosen algorithm's security and detection capabilities. Analyse the algorithm's resilience to common attacks like steganalysis. Since they can only embed a minimal amount of data in the carrier file, many existing steganography systems have a low data-hiding capability. This restricts how useful these systems are for real-world use.

Low robustness: Some steganography algorithms aren't resistant to widely used assaults like steganananalysis or file compression. The embedded data may be lost or damaged as a result.

Limitations on carrier file types: Some steganography methods can only be utilised with certain carrier file types, such as audio or image files. Difficulties with detection: It may be difficult to tell whether a particular file includes hidden data since some steganography methods are hard to spot. Security issues and challenges in confirming the veracity of the data can result from this.

Limited ability to embed data across several types of media files: Many steganography solutions only handle a single form of media file, such as photos or audio files.

Slow embedding and detection rates: Some steganography systems could need a lot of processing time to embed and find concealed data, rendering them unsuitable for real-time applications.

VIII OBJECTIVE OF THE PROPOSED WORK

The feasibility study provides the essential information needed to determine if it is feasible to fix the issue or take advantage of the opportunity. Additionally, it generates a final proposal for the management, which might be included in this final report.

Embedding technique

Examine the hidden data embedding process using the chosen algorithm in the carrier file. Find the best procedure for choosing the embedding sites in the carrier file. Analyse the effects of embedding on the overall size and quality of the file.

Detection process:

Analyse the carrier file's hidden data detection method. Identify the most effective way to apply the chosen steganography algorithm to locate the embedded data. Examine the detection system's defences against frequent threats like file conversion and data extraction.

Embedding Data

The mapping between the cover image and the hidden data that will be embedded can be taught to CNN. The CNN can be fed the cover picture as input, and the result could be a changed cover image with concealed data. This can be done by adding a second CNN branch for embedding the data, where the network's weights are trained to reduce the difference between the original and the altered cover picture.

Data Extraction

CNN can also be used to reveal hidden information in the stego-image. The CNN receives the stego-image as input, and one possible output is the hidden data that was extracted. This can be accomplished by adding a second CNN branch just for extracting the hidden data, where the network's weights are trained to minimise the difference between the hidden data that was originally there and the hidden data that was removed.

IX SECURITY EVALUATION

The security of a steganography method can also be examined using the suggested algorithm. It is possible to train the CNN to differentiate between cover images and stego-images produced by steganography. The security of the steganography approach can be evaluated by how well CNN can differentiate between cover images and stego-images. Overall, there is hope for image steganography because of the potential uses it could have for data extraction, data extraction, detecting adversarial attacks, and security analysis. Use a secure encryption algorithm to encrypt the confidential information.

Fig 4 Information Hidden by QR Code Generation

Create a QR code using an appropriate open-source library. Calculate the QR code's maximum storage capacity to ascertain the volume of data that can be concealed. Select a steganography method such as spread spectrum, LSB matching, or LSB Find the maximum number of pixels that can be changed without impairing the readability of the QR code.

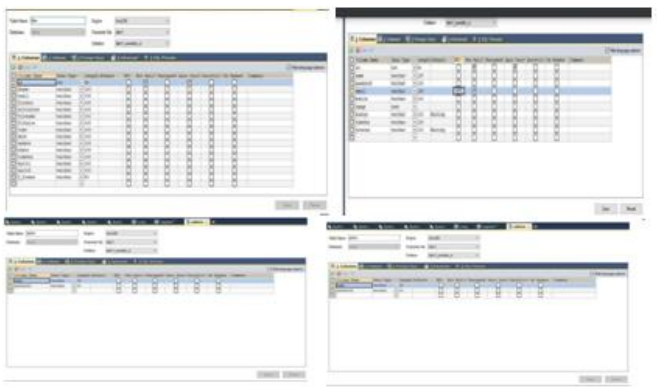

Fig 5 Embed the encrypted data into the QR code image

by changing the selected pixels' least significant bits. Make sure the encoded data has no impact on how readable the QR code image is scanning a QR code Using a smartphone camera or a QR code reader, scan the modified QR code. Recognise the secret information in the QR code image. Decryption of Data Utilising the identical encryption algorithm as that used to encrypt the data, decrypt the extracted data.

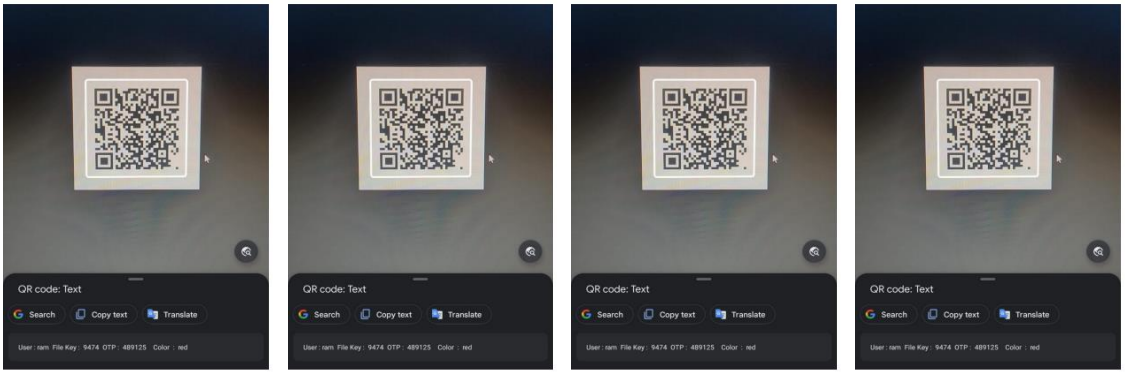

Fig 6 Decrypted data result with QR Code

This approach can be implemented in a number of programming languages, including Java, to display the concealed data that has been decrypted. Depending on the steganography method selected and the open-source library used to create the QR code, the implementation may differ.

X CONCLUSION

In conclusion, QR code steganography is an effective method for concealing data inside of photographs. However, it must only be used responsibly and with due caution. Knowing the hazards involved in using QR code steganography for illicit purposes is crucial because doing so can have serious repercussions. Image steganography is a method of concealing information in an image in a way that is difficult to identify. A common technique for image steganography is using QR codes to conceal information. This process is referred to as QR code steganography. In order to hide information, data must be inserted into a QR code image. By adjusting the colour and shape of the QR code modules, data can be embedded. Then, by examining the variations in the module's colour and shape, the data is extracted from the QR code. In order to send private information over a network, conceal copyright information in photographs, or embed metadata, QR code steganography can be employed. It can also be employed for unlawful purposes, like as concealing malware or other harmful programming within an image.

XI FUTURE ENHANCEMENT

Improved Steganographic Algorithms: The algorithms used to embed data into a QR code can constantly be improved. Future developments in steganography might concentrate on creating more complex, secure, and data-embedding algorithms. Multi-level steganography: This method of enclosing data within data uses the embedded data as a carrier for more hidden data. This method may be helpful for more delicate applications and add another layer of security and complexity to steganography approaches.

Data can be concealed in QR codes while they are being created thanks to the development of real-time steganography techniques, enabling faster and more secure data transfer. blockchain technology integration By offering a tamper-proof and decentralised record of all data transfers, the combination of steganography and blockchain technology can improve the security and traceability of concealed data. User-friendly software A wider range of users will be able to benefit from steganography if more user-friendly applications are created, increasing the technology's usability and accessibility. Overall, steganography in QR codes using picture principles can be improved in the future to increase security, functionality, and usability, making the technology a more dependable and effective way to secure data transfer.

REFERENCES

[1] K.VijiyaKumar, B.avanya, I. Nirmala, S. Sofia Caroline, "Random Forest Algorithm for the Prediction of Diabetes ".Proceeding of International Conference on Systems Computation Automation and Networking, 2019.

[2] Y. K. Qawqzeh, A. S. Bajahzar, M. Jemmali, M. M. Otoom, and A. Thaljaoui, "Classification of diabetes using photoplethysmography (PPG) waveform analysis: logistic regression modeling," BioMed Research International, vol. 2020, Article ID 3764653, 6 pages,2020.

[3] G. A. Pethunachiyar, "Classification of diabetes patients using kernel-based support vector machines," in Proceeding of the 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–4, IEEE, Coimbatore, India, January 2020.

[4] 4. S. Gupta, H. K. Verma, and D. Bhardwaj, "Classification of diabetes using Naïve Bayes and support vector machine as a technique," Operations Management and Systems Engineering, Springer, Singapore, 2021.

[5] D. K. Choubey, M. Kumar, V. Shukla, S. Tripathi, and V. K. Dhandhania, "Comparative analysis of classification methods with PCA and LDA for diabetes," Current Diabetes Reviews, vol. 16, no. 8, pp. 833–850, 2020.

[6] M. Maniruzzaman, M. J. Rahman, B. Ahammed, and M. M. Abedin, "Classification and prediction of diabetes disease using machine learning paradigm," Health Information Science and Systems, vol. 8, no. 1, pp. 7–14, 2020.

[7] N. Singh and P. Singh, "Stacking-based multi-objective evolutionary ensemble framework for prediction of diabetes mellitus," Biocybernetics and Biomedical Engineering, vol. 40, no. 1, pp. 1–22, 2020.

[8] S. Kumari, D. Kumar, and M. Mittal, "An ensemble approach for classification and prediction of diabetes mellitus using a soft voting classifier," International Journal of Cognitive Computing in Engineering, vol. 2, 2021.

[9] M. M. F. Islam, R. Ferdousi, S. Rahman, and H. Y. Bushra, "Likelihood prediction of diabetes at an early stage using data mining techniques," in Computer Vision and Machine Intelligence in Medical Image Analysis, pp. 113–125, Springer, Singapore, 2020.

[10] S. Malik, S. Harous, and H. E. Sayed, "Comparative analysis of machine learning algorithms for early prediction of diabetes mellitus in women," in Proceedings of the International Symposium on Modelling and Implementation of Complex Systems, pp. 95–106, Springer, Batna, Algeria, October 2020

[11] A. Hussain and S. Naaz, "Prediction of diabetes mellitus: a comparative study of various machine learning models," in Proceeding of the International Conference on Innovative Computing and Communications, pp. 103–115, Springer, Delhi, India, January 2021.

[12] J. Y. Kim and J. Y. Jeon, "Role of exercise on insulin sensitivity and beta-cell function: is exercise sufficient for the prevention of youth-onset type 2 diabetes?" Annals of Pediatric Endocrinology & Metabolism, vol. 25, no. 4, pp. 208–216, 2020.

[13] S.Saru and S.Subashree.2019.Analysis And Prediction Of Diabetes Using Machine Learning from International Journal of Emerging Technology and Innovative Engineering Volume 5, Issue 4, (ISSN: 2394 – 6598).

[14] Hang Lai1, Huaxiong Huang, Karim Keshavjee, Aziz Guergachi1 and Xin Gao.2019.

[15] Predictive models for diabetes mellitus using machine learning techniques, BMC Endocrine Disorders Article.

[16] J. Bagyamani, K. Saravanapriya.2019. Data Mining Classification Techniques for the Diagnosis of Diabetes Mellitus – A Review from International

[17] T. Morkel, J. H. Eloff, and M. S. Olivier, ' An overview of image steganography,' in Proc. ISSA, 2005, pp. 1–11.

[18] M. Charikar and D. Ramakrishna, ' Lossless compression of fragmented image data,' U.S. Patent16 276 411, Jun. 13, 2019.

[19] A. K. Sahu and G. Swain, ' An optimal information hiding approach based on pixel value differencing and modulus function,' Wireless Pers. Commun., vol. 108, no. 1, pp. 159–174, Sep. 2019, doi: 10.1007/s11277- 019-06393-z.

[20] S. A. Kumar and S. Gandharba, ' High fidelity based reversible data hiding using modified LSB matching and pixel difference,' J. King Saud Univ.-Comput. Inf. Sci., to be published.

[Online]. Available: http://www.sciencedirect.com/science/article/pii/S1319157819304124, doi 10.1016/j.jksuci.2019.07.004.

[21] G. Swain and A. Sahu, ‘ Anovel multi stego-image based data hiding method for a grayscale image,’ Pertanika J. Sci. Technol., vol. 27, pp. 753–768, May 2019.

[22] G. Swain and A. K. Sahu, ‘ Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis,’ Int. J. Electron. Secure. Digit. Forensics, vol. 11, no. 4, p. 458, 2019.