International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

DOUBLE IMAGE STEGANOGRAPHY WITH QR CODE USING PYTHON

Karthikeyan N[1], Sriram M[2], Thilagan C[3]

[1,2,3]*Student, Computer Science and Engineering, S. A Engineering College, Chennai, India*

ABSTRACT : *Hiding secret data within an ordinary, non-secret, file or message in order to avoid detection Steganography technique is used. It deals on the image with QR code . Where the message (payload) will be encrypted and set into a QR code(container). It also converted to string which will be used to for the image steganography .This may secure the message (payload) in multiple levels. By using the QR code we could easily make less distorted image steganography. Where using the LZW algorithm makes the data compression and gives a security from RS attack .By using the compression we could achieve the high storage capacity which would be comparatively higher than the standard LSB approach.*

Key Word: Double Steganography, LSB, LZW, QR code,RS attack, Information security

1. INTRODUCTION

In recent years, enormous research efforts have been utilized in the improvement of digital image steganographic techniques. The major goal of steganography is to secure communication mechanism by embedding secret messages into digital images by modifying the nonessential pixels of the images . After the embedding of the secret message these images are called as stegano-image and it is used to communicate through a public channel. Used public channel may be intentionally monitored by some opponent in the transmission process, who tries to prevent successfully communications and he/she may randomly attack few stegano-images in case of doubt on stegano-images. High imperceptibility (similarities between the cover-image and the stegano-image) is the only way to reduce the chances of doubt on stegano-images and increases the chances of secure communications. An alternative was proposed by , it make use of a stegano key to provide additional security on the secret data.

2. EXISTING SYSTEM

It uses Single Level of security-It gives only single level of security with encrypting the data which requires a key for decryption. LSB algorithm is used for transcription which is common algorithm but still its older and can store only lesser data when compare to few enhanced version of it. This may mislead someone who reads his without the knowledge of the message being encrypted behind this image. The size of the message which could hide is less and noise is higher can be easily found in steg-analysis.

3. PROPOSED SYSTEM

Proposed method is a LSB based data hiding method with inherited property of kekre's method. Kekre's algorithm is proposed: hides data in the upper LSB bit only when its adjacent LSB bit of all the pixel have conceived a bit of secret data for better quality of the stegano-image. It uses LZW compression technique for data compression which helps in storing large amount of data. It uses blow fish algorithm for encrypting the data to give a level of high security. Here we append the key with the encrypted string so its easy for receiver for decrypting the message. Using a QR code as container for doing steganography which diverts to some other websites .It uses base64 a python library for converting the image to text and vice versa .Here in this proposed algorithm can uses any image from lena_grey to rgb_colour images, so it covers various types of images files for steganography without loss.

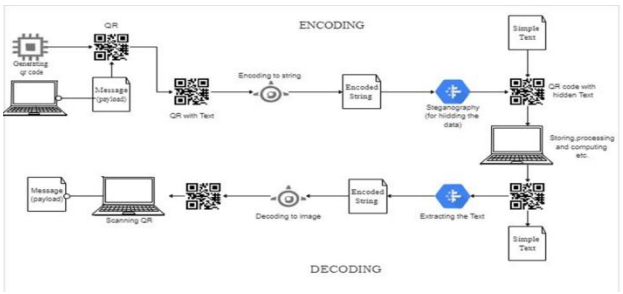
4. SYSTEM DESIGN

Frameworks configuration is the way toward characterizing components of a framework like modules, engineering, segments and their interfaces and information for a framework dependent on the predefined prerequisites.

4.1 SYSTEM ARCHITECTURE

At first the secret message will be encoded with the QR code it will be converted to string, which will be encrypted using blowfish algorithm which will be again encoded into a QR code which act as a container. The reverse process of the encryption is the decryption.

Fig 4.1 System Architecture



5. MODULES

A module is one of a bunch of parts from which a few structures are made. Every module is made independently, and the finished modules are then consolidated to shape the structure.

5.1 QR CODE GENERATION

The version parameter is an integer from 1 to 40 that controls the size of the QR Code (the smallest, version 1, is a 21x21 matrix). Set to None and use the fit parameter when making the code to determine this automatically. Fill Colour and Black Colour can change the background and the painting colour of the QR, when using the default image factory. The Error Correction parameter controls the error correction used for the QR Code. The following four constants are made available on the QR code package.

5.2 DATA ENCRYPTION

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks

5.3 CONVERTING IMAGE TO STRING

*This module uses base64 library to covert the the image file to string .Next, We Opened Our Image File In **rb** Mode Which Is Read In Binary Mode. The We Read Our Image With **image2.read()** Which Reads The Image And Encode it Using b64encode() It Is Method That Is Used To Encode Data Into Base64 Finally, we Print Our Encoded String .*

5.4 IMAGE STEGANOGRAPHY

It refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and the image obtained after steganography is called the stegano-image. This module is used here to hide the string which we got from the base64 encoding.

5.5 CONVERTING STRING TO IMAGE

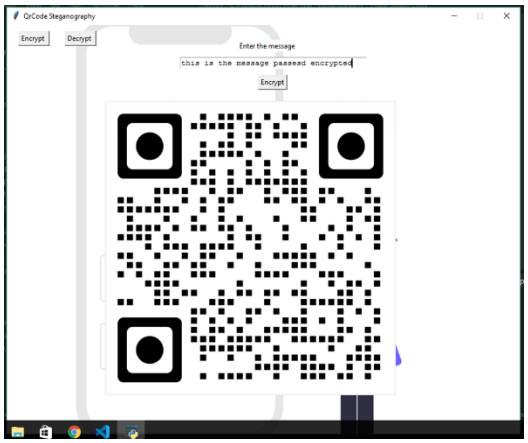
This module uses base64 library to covert the string to image file .Next, We Opened Our Image File In rb Mode Which Is Read In Binary Mode.base64.decode Which Reads The String And Decode it to form image. Finally, we Print Our Decoded Image

5.6 DATA DECRYPTION

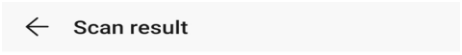
The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

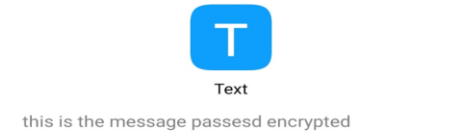
6. EXPERIMENTAL RESULT

Enter the message to be encrypted ->



Encrypted QR ->





Decrypted ->

message

7. CONCLUSION

We have tried the message hiding technique efficiently to make a message secure. The use of QR code which can be easily read through any scanner. It makes the third party user to get a wrong data.So that we achieved fast, efficient and high data security.

8. FUTURE ENHANCEMENT

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. "You never know if a message is hidden", this is the dilemma that empowers steganography. As more emphasis is placed on the areas of copyright protection, privacy protection, and surveillance, we believe that steganography will continue to grow in importance as a protection mechanism. This project deals with Steganography in Image and Audio files using Least Significant Bit (LSB) coding. This project can uplifted by considering following measures: A more sophisticated approach can be implemented by using a pseudo-random number generator to spread the message over the image file in a random manner. This project can be extended by using other media files like video and other complex formats of audio and image.

9. REFERENCES

[1] T. Morkel, J. H. Eloff, and M. S. Olivier, ``An overview of image steganography,'' in Proc. ISSA, 2005, pp. 111.

[2] B. Dunbar, ``A detailed look at steganographic techniques and their use in an open-systems environment,'' in The Information Security Reading Room. Bethesda, MD, USA: SANS Institute, 2002.

[3] S. R. M. Mary and E. K. Rosemary, ``Data security through QR code encryption and steganography,'' Adv. Comput., Int. J., vol. 7, nos. 12, pp. 17, Mar. 2016.

[4] J.Waleed, H. D. Jun, S. Saadoon, S. Hameed, and H. Hatem, ``An immune secret QR-code sharing based on a twofold zero-watermarking scheme,'' Int. J. Multimedia Ubiquitous Eng., vol. 10, no. 4, pp. 399412, Apr. 2015.

[5] T. J. Soon, ``QR code,'' Synth. J., vol. 2008, no. 3, pp. 5978, 2008.

[6] Information TechnologyAutomatic Identication and Data Capture TechniquesQR Code bar Code Symbology Specication, ISO/IEC Stan- dard 18004:2015, 2015.

[7] M. Charikar and D. Ramakrishna, ``Lossless compression of fragmented image data,'' U.S. Patent 16 276 411, Jun. 13 2019.

[8] 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. 159174, Sep. 2019, doi: 10.1007/s11277- 019-06393-z.

[9] S. A. Kumar and S. Gandharba, ``High delity based reversible data hiding using modied LSB matching and pixel difference,'' J. KingSaud Univ.-Comput. Inf. Sci., to be published. [Online]. Available:http://www.sciencedirect.com/science/article/p

ii/S1319157819304124, doi: 10.1016/j.jksuci.2019.07.004.

[10] A. K. Sahu and G. Swain, ``A novel n-rightmost bit replacement image steganography technique,'' 3D Res., vol. 10, no. 1, p. 2, Dec. 2018, doi: 10. 1007/s13319-018-0211-x.

[11] G. Swain and A. Sahu, ``A novel multi stegano-image based data hid-ing method for gray scale image,'' Pertanika J. Sci. Technol., vol. 27, pp. 753768, May 2019.