ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Embedding in Images Using QR Codes

Hanumantraya
Department of Electronics and Communication Engineering, National Institute of Engineering, Mysuru.

Kruthik
Department of Electronics and Communication Engineering, National Institute of Engineering, Mysuru.

Venkateshwar
Department of Electronics and Communication Engineering, National Institute of Engineering, Mysuru.

Arun M
Department of Electronics and Communication Engineering, National Institute of Engineering, Mysuru.

Dr.Narasimha Kaulgud
Department of Electronics and Communication Engineering, National Institute of Engineering, Mysuru.

Abstract

Transmitting medical data from one location to other can provide better healthcare services in remote locations. Image steganography is an approach, where patient reports are embedded in lower bit planes of an image and are then transmitted. Former techniques employ encoding of raw text and placing them on lower bit planes providing single layer of security. Standard encoding and decoding methods are incorporated to cipher the information .In this proposed method encrypted data is inserted into quick response codes as it increases data holding capacity and also provides an extra layer of security. The Stego (image in which QR code is hidden) image and original image are similar in appearance ensuring secrecy. There will be no loss of any information in QR code as original pixel values are retained during the reception. Data retrieval is smooth and can be performed without having any distortion. Implying this mechanism provides multilayer security, improved readability and makes transmission of information easy.

Keywords: ***Digital watermarking, LSB, PSNR, QR-code, Grayscale images, Spatial domain watermarking***

1.INTRODUCTION

In recent years information sharing has become convenient due to evolution and improvements in field of communication and networking, but information security still remains as a question. In this paper we present a robust and most efficient watermarking algorithm using the third and the fourth least significant bits (LSB) technique. This proposed algorithm is more impactful than any other algorithm used for the same purpose. Experimental results prove that the quality of the water marked image is highly remarkable. With the rapidly growing technology and usage of internet illegal copying, modifying and tampering have become a major issue. Presently, usage of public channels has become an insecure environment to share the information that is exchanged between sender and the receiver. There are several technologies emerging today in the market to prevent attacks from the hackers. Encrypting the information providesthe basic security. Algorithm and next one is detecting algorithm. These two processes are common for all types of water marking techniques.

2. EXISTING SYSTEM

There are numerous methods that are readily obtained to unauthorized parties who can access the secured information. Lower significant bit (LSB) replacement is one of the most predominant techniques used in image steganographyin this technique the secret data is embedded in the least significant bits of the image. This may marginally change the pixel properties. Most recent works on this line is hiding data using adaptive LSB substitution method. This method provided satisfactory protection for the patient data by exploiting the brightness, texture and edges of image. Another

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

technique of image steganography is proposed by C.Nagaraju and Parthsarthy was able to securely transmit data only of size 1/8th times of cover image [2]. Reversible watermarking technique using QR codes was able to hide small amount of data in images but this technique included complex image operations which made it difficult to use. So using QR codes a new steganography technique is proposed in this paper to overcome the limitations of some of the image stenographic techniques discussed.

3. PROPOSED METHOD

The idea is to encode the text message to be hidden and then a QR code for the same is generated. This QR code is then embedded into LSB plane of the cover image. The image is reconstructed and sent to the destination where it is recovered. Based on LSB technique, we propose a new watermarking algorithm. Most of researchers have proposed the first LSB but our proposed watermarking algorithm is using the third and fourth LSB for hiding the data. This is because of the security reason. So, no one will expect that the hidden data in the third and the fourth LSB. First, we select the image which is a grayscale image and we will transfer the data to binary value after typing it. Then, we hide the data in the image using the proposed algorithm.

4. METHODOLOGY

The proposed method is simple and it is represented as block diagram in Fig.1& Fig.2

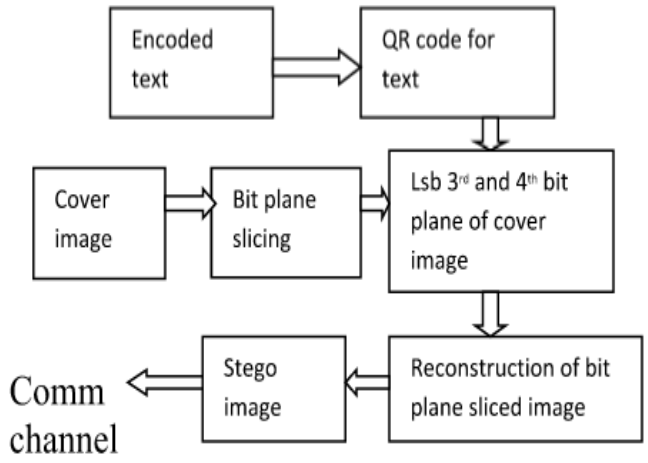

Fig.1 Transmition side

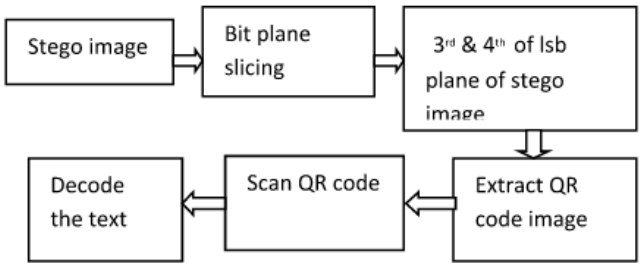

Fig.2 Receiver side

There are numerous methods that are readily obtained to unauthorized parties who can access the secured information. Lower significant bit (LSB) replacement is one of the most predominant techniques used in image steganographyin this technique the secret data is embedded in the least significant bits of the image. This may marginally change the pixel properties. Most recent works on.Encoding the secrecy of the message is maintained using Encoding technique. The text is converted to other form by altering ASCII characters. Message encryption is done using below formula

$$Hf = (\log (T0 * 2) * 100) - 300$$

Where Hf is the Modified ASCII value and T0 is the ASCII value of text message. The ASCII values for Hf ranges from 116 to 255 for all printable characters. For the encoded message a QR code is generated.

QR code generation QR code is generated for the encoded text. The online QR code generator used here automatically decides its size based on the size of the encoded data. Maximum size of QR code generated is of 177×177 (version40). The image can be enlarged to improve the readability of QR code. Cover image. An 8 bit grayscale image of, PNG format is selected as cover image. Also TIFF, JPEG and GIF image formats are also supported. Bit plane slicing The 8-bit cover image is sliced along the bit planes. Visual appearance of the cover image is due to the contributions made by MSB planes of the image. LSB planes of the image convey very less information about the image. These LSB planes are used to hide the data. This method uses only one LSB plane to embed the QR code image consisting encoded data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Embedding QR code The QR code image consisting encoded message data is not directly embedded into the LSB plane of cover image. A unique technique is used to embed the QR code which conserves data space and also delivers security for the data.

Pixel values of LSB plane are now replaced by pixel values of QR code image. At the time of replacement, the pixel values for all white bars of QR code image having the value 255 is substituted by value 1(bit). Therefore for each white bar in QR code 7 bits of data is conserved. As this creates additional space in cover image, another QR code can be inserted into it if necessary. As the pixel values are altered, LSB plane consists only of data but not the QR code itself. Consequently this features auxiliary security.

Reconstruction Stego image is obtained after reconstructing the bit plane sliced cover image. Stego image thus formed consists of QR code data at LSB plane. Using any available transmission techniques the stego image is relayed to the destination.

The receiver side, The received stego image is sliced along its bit planes to get LSB plane. Actual pixel values are retained at this stage to obtain the QR code. The QR code image thus procured is scanned using QR code scanner. Text extracted consists of encoded message data. One can decode the message if and only if the encoding technique and decoding formula is known. Encoded data is then decoded using decoding formula.

$$H1 = \exp((Hf + 300)/100 - \log(2))$$

Hf is rounded off to next digit to get smooth result. Original text is completely recovered at receiving side and then analyzed.

5. RESULTS

Different sizes of QR code image and cover image are used to test the method. To verify the quality of image, Peak Signal to Noise Ratio (PSNR) is taken as measuring parameter.

A QR code with correction level M (15%) of size 243×243(figure 3.2) is embedded into the greyscale cover image (PNG format) of size 256×256(fig 3.1).

Sample Text message: QR Code for encoded text Reff Number of patient: 12345685403 Name of the Doctor: Dr. XYZZZZZZ Name of the Patient: ABCDDDDDDD Age: 45 years
Case type: HHHHHH
Date of Admission: 05/05/2017
Result: Cardiac arrest
Diagnosis: Heart failure
Treatment: Heart transplantation.

Fig.3.1 Cover image

Fig.3.2QR code for encoded text

Fig.3.3 Stego image

The number of data bits that can be embedded using this technique depends upon
1. Version of QR code
2. Number of white bars in QR code
3. Size of cover image

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The Table 1 shows the experimental results for different sizes of cover and QR code image. For the QR code of version 37, size is enhanced from 165×165 to 243×243 in order to get better readability. As shown by the first value of table 1, it has 95616 bits of storage capacity.

The second value of table 1 is for the QR code of the version 40. No change is done to the size of QR code in this case and has storage capacity of 112032 bits. This clearly illustrates that it is the version of the QR code which determines the storage capacity not the size of it.

Sizes of other QR codes in the table are not disturbed. The storage capacities for these are tabulated in table 1.

Table1

Size of cover image(pixels)	Size of QR code image(pixels)	Capacity (bits)
256x256	243x243	35616
	177x177	112032
	65x65	69600
	133x133	81088
512x512	243x243	394568
	177x177	410784
	65x65	306080
	133x133	314672

The data storage capacity is compared with LSB substitution method.

6. CONCLUSION

Information embedded inside the QR code and then insertion of this QR code into cover image provides multilayer security and also enhances the storage capacity.

As shown in results, stego and cover image have similar visual appearances. Data loss is zero as decoded data and encoded data are same. Using current method readability can be improved as QR codes are made use. Special features of QR code add as an advantage to the proposed technique.

7.REFERENCES

[1]. Cheddad, Abbas, et al. "Digital image steganography: Survey and analysis of current methods." Signal processing 90.3 (2010): 727-752.

[2]. Nagaraju, C., and S. S. ParthaSarathy. "Embedding ECG and patient information in medical image."Recent Advances and Innovations in Engineering (ICRAIE), 2014.IEEE, 2014.

[3]. Sheth, Ravi K., and Rashmi M. Tank. "Image Steganography Techniques "International Journal Of Computer Engineering And Sciences 1.2 (2015): 10-15.

[4]. Hussain, Mehdi, and MureedHussain. "A survey of image steganography techniques." (2013).

[5]. ThotaSriram, K.V.Rao, S Biswas, Basheer Ahmed, “Application of barcode technology in automated storage and retrieval systems”, BHEL.

[6]. Kaushik, Sona. "Strength of Quick Response Barcodes and Design of Secure Data Sharing System."International Journal on Advanced Computing & Science (IJACSA) (2011).

[7]. Yang, Hengfu, Xingming Sun, and Guang Sun. "A high-capacity image data hiding scheme using adaptive LSB substitution." Radio Eng 18.4 (2009): 509.