International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

Securing Data in Images using QR Codes

[1] Nitheesh [2] K.M. Bhuvan Prasad [3] Nithin Kumar H.R [4] Sagar K.M [5] Mr. Subramanya M.B
[1][2][3][4] 8th Semester U.G Students [5] Assistant Professor
[1][2][3][4][5]Department of Electronics and Communication Engineering,
Vidya Vikas Institute of Engineering and Technology, Mysore

***Abstract*— Relaying 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 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.**

I. INTRODUCTION

In recent years information sharing has become convenient due to the evolution and improvements in field of communication and networking, but providing security to the information that is shared has still remained as a matter of concern. So security must be provided to the information that is exchanged between sender and receiver.

Data hiding in images can provide solution for the problem. The technique is known as image steganography [1]. Lot of theories is available to explain different techniques of image steganography [2-6]. Capacity and quality are the two important requirements in image steganography.

Quick Response codes are the two dimensional bar codes which were initially used to recognize automotive parts [7]. QR code is a image having only two pixel values i.e. '0' representing black color and '255' representing white color [9]. These codes are capable of storing data of definite size. The capacity of data depends upon the version of QR code used [8]. A novel method of steganography is designed using QR codes aiming at increasing the security and also the data storage capacity.

II. 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 steganography [3]. In 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 [10]. This method provided satisfactory protection for the patient data by exploiting the brightness, texture and edges of image. Another 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 [11]. Reversible watermarking technique using QR codes was able to hide small amount of data in images [12]. 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 steganographic techniques discussed.

III. 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.

IV. METHODOLOGY

The proposed method is simple to use and it is represented as block diagram in figure1

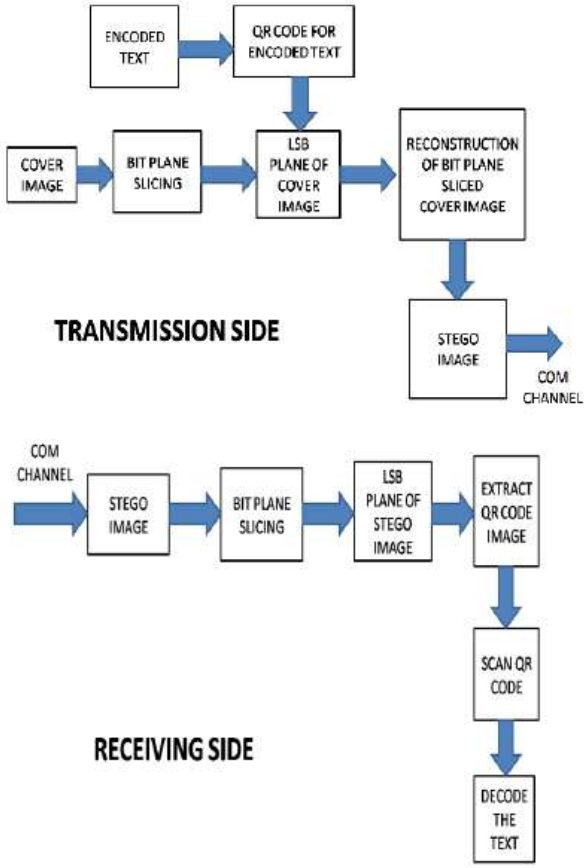

Figure 1

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 [11].

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

Where Te is the Modified ASCII value and T0 is the ASCII value of text message. The ASCII values for Te 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 [12] 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 [11]. 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.

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 [11].

$$T0 = \exp ((Te + 300)/100 - \log (2))$$

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

V. 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 4.1) is embedded into the greyscale cover image (PNG format) of size 256×256(figure 4.2).
Sample Text message: QR Code for encoded text
Reference Number of patient: 8965124
Name of the Doctor: Dr. XXXXXXXXX
Name of the Patient: YYYYYY
Age: 65 years
Case type: ZZZZZZZ
Date of Admission: 9/10/2015
Result: T Wave inversion
Diagnosis: Suspected MI
Treatment: Sublingual Nitroglycenn.
Cover image

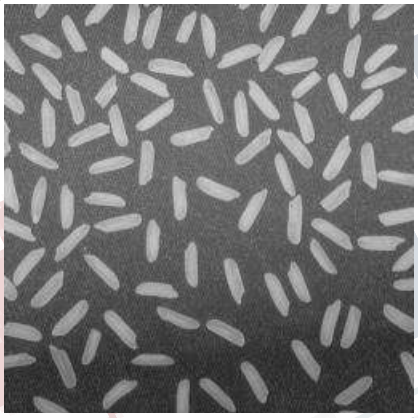

Figure 4.2
QR Code for encoded text

Figure 4.1

Stego image

Figure 4.3

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

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.

Table 1

Size of cover Image (pixels)	Size of QR code image (pixels)	Capacity(bits)
256×256	243×243	95616
	177×177	112032
	65×65	69600
	133×133	81088
512×512	243×243	394568
	177×177	410784
	65×65	306080
	133×133	314672

The data storage capacity is compared with LSB substitution method [10, 11].

Table 2 gives the comparison between two methods when applied to images of two different sizes

Name of the image	Size of cover image	Adaptive LSB Substitution Method		Proposed method	
		No of characters	PSNR	No of characters	PSNR
Rice.png	256×256	8192	49.373	14004	59.1
Lena.jpeg	512×512	32768	46.450	51348	51.3

VI. 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.

REFERENCES

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

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

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

[4]. Wu, Da-Chun, and Wen-Hsiang Tsai. "A steganographic method for images by pixel-value differencing." Pattern Recognition Letters 24.9 (2003): 1613-1626.

[5]. Zolfaghari, Behrouz, Saadat Pour Mozafari, and Mehrdad Zobeiri. "ZEDNOT: An Approach to Combining Cryptography and Image Steganography Using Reversible Logic Functions." be published in Proceedings of International Conference on Intelligent Network and Computing (ICINC 2010), Kuala Lumpur, Malaysia. 2010.

[6]. Vellaisamy, Seenivasagam, and Vyshnavi Ramesh. "Inversion attack resilient zero-watermarking scheme for medical image authentication." Image Processing, IET 8.12 (2014): 718-727.

[7]. Thota Sriram, K.V.Rao, S Biswas, Basheer Ahmed, "Application of barcode technology in automated storage and retrieval systems", BHEL.

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

[9]. Zhi Liu, Herong Zheng, Huaguo Jia; "Design and Implementation of Color Two-Dimension Barcode with High Compression Ratio for Chinese Characters", International Conference on Information Engineering and Computer Science, 2009 (ICIECS 2009).

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

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

[12]. Panyindee, C., and Chuchart Pintavirooj. "QR codes application for reversible watermarking algorithm in biomedical images." Biomedical Engineering International Conference (BMEiCON), 2013 6th. IEEE, 2013