Implementation of Image Steganography in QR Code Using Mid-Band DCT

ER. Harpreet Singh
M.Tech scholar in Computer Engineering, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Sabo (Bathinda), Punjab, India

Abstract: Image steganography is taking a new turn in present day world. Now day's strong technique in computer science and security of the digital content. The use of QR code is increasing day by day and this advance version of 2D bar code proves to provide higher content capacity. The cover image in previous works is used as jpeg or bmp images. These types of images assist to handle greater distortion, providing higher PSNR. In this research paper, I have implemented, image steganography on QR code as cover image. The PSNR has to be maintained so that the message in the QR cod is not lost.

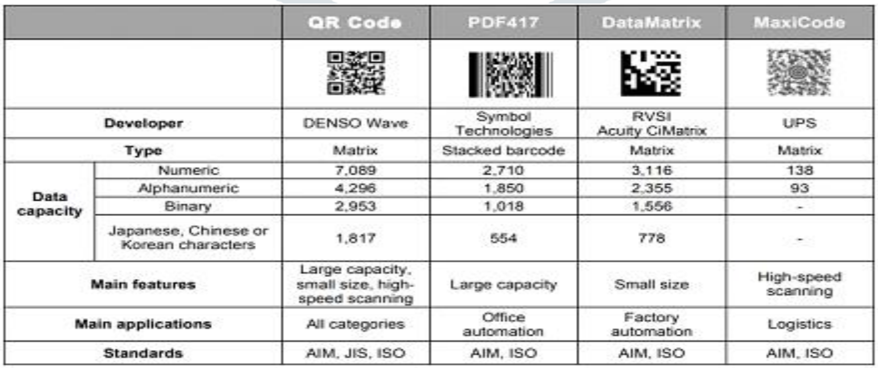
Keywords: Image Steagnography, LSB, QR Code, Image PSNR, MSE, Data Hiding, Bit Sequence Message.

Introduction

QR code shortened of Quick Response Code is that the trademark during a matrix barcode or two- dimensional barcode. It absolutely was initially designed for the automotive trade in Pacific Ocean (Japan). QR code is a machine-readable visible label which contains data regarding the item in which this is to be attached. A QR code have uses four standardized secret writing modes like as, character set, numeric, computer memory unit, and kanji and binary to store itself with efficiency.(Fig.1.1).

Fig 1.1 Quick Response Code

The Quick Response Code may be a two-dimensional (2-D) matrix code that belongs to a big set of computer readable codes, these all are usually named as barcodes, regardless whether they made up of squares, bars parts. (Table 1.1) QR codes technology is Easy to use, Low-cost and easy to implement. In this technology provides a lot of bang for the buck, when implemented wisely.



		QR Code	PDF417	DataMatrix	MaxiCode
Developer		DENSO Wave	Symbol Technologies	RVSI Acuity CiMatrix	UPS
Type		Matrix	Stacked barcode	Matrix	Matrix
Data capacity	Numeric	7,089	2,710	3,116	138
	Alphanumeric	4,296	1,850	2,355	93
	Binary	2,953	1,018	1,556	-
	Japanese, Chinese or Korean characters	1,817	554	778	-
Main features		Large capacity, small size, high-speed scanning	Large capacity	Small size	High-speed scanning
Main applications		All categories	Office automation	Factory automation	Logistics
Standards		AIM, JIS, ISO	AIM, ISO	AIM, ISO	AIM, ISO

Table 1.1: Features of codes

Related Work

Steagnography

Steganography is that the technique of fix the secret message in such the simplest method no one read this message easily [12]. Steganography implements by replace bits each other in which contains text, graphics and sound, etc. with bits of various hidden or secret messages. This secret info can be simple text, images or cipher text [14]. Steganography may be used once cryptography isn't supported. Associate encrypted file should still hide info exploitation Steganography, therefore though the encoded file is decoded, in this case hidden text or image isn't seen. Generally, a steganographic message can seem to be one thing else: an image, an article, a searching list, or another message - the quilt text [17].

Classically, it should be hidden by exploitation invisible ink between the visible lines of innocuous documents, or perhaps written onto consumer goods. In WW2, a message was one time written in code on two-colour knitting yarn. Another methodology is just like pin prick of individual letters during a news story, so forming a message. It should even be a couple of words written below postage, the stamp then being the quilt text Show in Fig. 2.1.

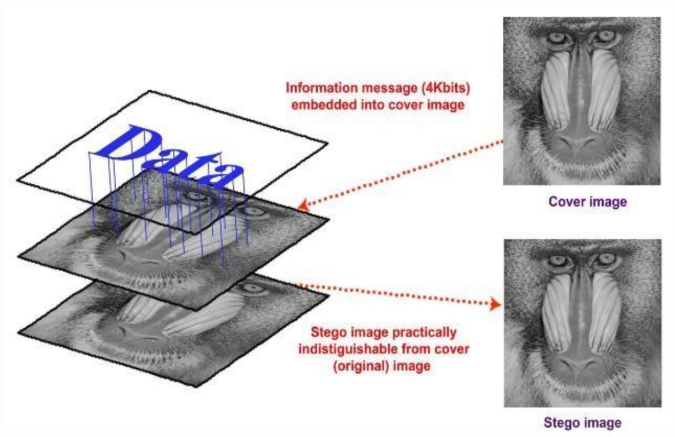

Information message (4Kbits)
embedded into cover image
Data
Cover image
Stego image practically
indistiguishable from cover
(original) image
Stego image

Fig.2.1 Embedding of the message

2.1 Image Based Steganography

To embed a message into a QR code image needs two files. The first file contains the image that may hold the hidden info, known as the cover image. The second file is that the message—the info to be hidden. A message is also plain-text, cipher-text, alternative pictures, or something that may be embedded during a bit stream. Once combined, the quilt image and therefore the embedded message create a stego-image [17]. Astego-key (a sort of password) may be accustomed hide then later rewrite the message. Most steganography package recommends the utilization of lossless 24-bit pictures like BMP [19].

2.1.1 Least Significant Bit (LSB) Technique

In the LSB technique, firstly the image is transformed into 3 planes i.e. red, green and blue. Each plane has the pixel representation of the image with fixed intensity values (Fig.2.2).

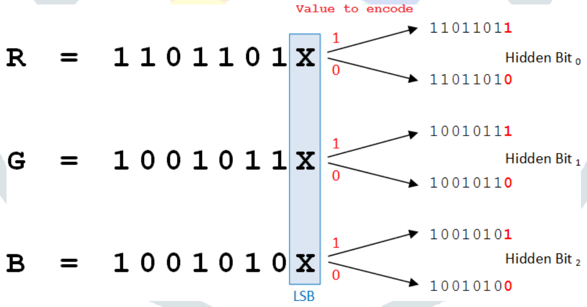


Fig. 2.2 Least significant bit insertion (LSB)

The intensity change in smaller values is unrecognizable by human eyes. This key idea is utilized and the LSB of any pixel can be replaced and no effect is manually visible in the image. These pixels are replaced by the pixels of the message image. As a result, the message gets hidden inside the cover image. Inserting the message into the QR code label image is known as encryption process and extracting the message back from the stego file is known as decrypting.

Literature Survey

Kumawat et al. [1] this paper represents the showcase one in every of the newest automatic identification technology ideas. Within the recent past the concept of quick Response Code (QR Code) has earned a major recognition and is getting used as information illustration mean. Second Barcode square measure wide used because of high capability storage and quick process step, QR Code is one in every of such varieties of second barcode. Education and Advertising square measure the highest most span wherever usability is continuous grow. This paper aims on providing elaborated data on all the ideas of fast Response Code.

It expresses significance; structure and full procedure accustomed represent knowledge within the variety of barcode. Initial experiment is to use noise in QR Code (encoding) and second is De-noising (decoding) victimization Median filters and Wiener filters. This document conjointly provides a sight of the affect of Noise on the QR code and bar chart of the PSNR values that shows the differentiate of the images.

Luo et al. [2] QR code is 2D barcode have a huge QR code data storage as well as correction of errors. QR code reader may scan the contents of the QR label. When the content of the QR code information is confidential then the information security becomes foremost. To save the secretness of secure information, the new advance technique can embed secret information into the content of QR code.

Mehboob et al. [4] several techniques ar used to conceal the information in various format in steganography. the most wide used apparatus on account of its simplicity is that the utilization of the smallest amount significant Bit. LSB Method is used to conceal the confidential information of image. The other bits are additionally used but it's extraordinarily possible that image would be distorted. This research article is the art associated science of Steganography usually and proposes a totally unique technique to

Conceal data in a passing colourful images using LSB Method.

Barhate et al. [9] in this paper Image Steganography is implement a test for watermarking algorithms. In Least Significant Bit (LSB) comparison is made between Mid Band Discrete Cosine Transform (DCT) domain and spatial domain technique. After computing the results by using coefficient DCT Mid-band watermarking algorithm is much reliable than LSB.

Proposed Methods

In this part, the structure of the proposed technique is described, where a QR code will be generated according to the format described by a JAPANESE company DENSO wave [2]. The versions of the QR code are from 1 - 40 it depends on the message size. For the correction level: QR code has four correction levels, from high to low L, M, Q, H corresponding to the error correction rate of 7 %, 15 %, 25%, 30 % respectively.

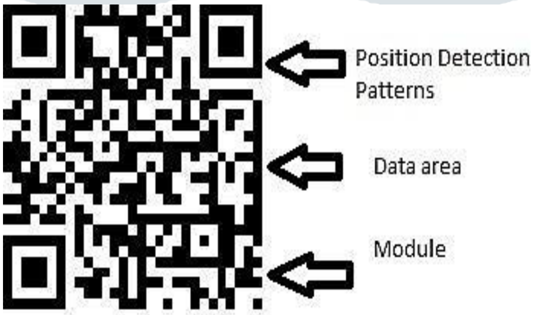


Fig.4.1 2D bar code

The QR code generated is considered as the cover image and using Mid-Band DCT technique; steganography is performed so as to embed the secret message. For fixing the secret code, a secret message has to be incorporated in order to provide greater security. The first part of the technique generates the QR code having version number 1 – 40 based on the size of message to be embedded. Larger the size of QR code, higher is the error correction level. The original form of an image is changed due to the unwanted information: termed as Noise. Due to the embedding of secret message noise gets induced. When the QR code is generated it is converted into the form of image having JPEG format. Upon the analysis of this image, based on image histogram it is found to have high and low intensity pixels (pels) in a well-defined format shows in Fig. 4.1. These pels can be used to embed the secret message which results in poor image quality of QR code.

Explanation

The transform domain based technique "DCT" helps to embed the hidden secret message effectively as we know that transform domain technique is far more superior than the spatial domain technique since robustness against lossy compression and different filtering options such as median, high- pas and low- pass filters etc. This technique gives a greater assurance about the quality at the receiving ends. The middle band frequency coefficients of an 8*8 DCT block are shown in the Fig.4.1

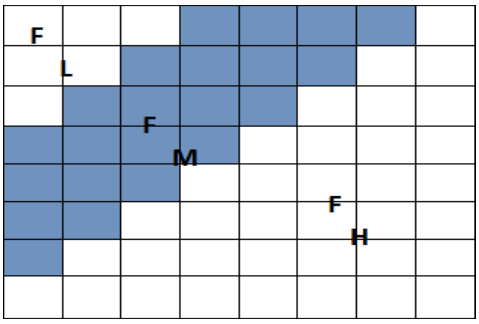


Fig 4.2: DCT region for Mid-frequency

The DCT Technique divides the image into blocks of 8x8. Low frequency (FL) is used to denote the lower frequency coefficients of the block where as high frequency (FH) is used to denote the higher frequency coefficients. The mid band is used for embedding to provide additional resistance to lossy compression techniques while avoiding significant modifications of the cover image. By selecting two locations from mid frequency region DCT technique will be used to provide distortion less steganography. Low frequencies are avoided to embed secret data since human vision system is more sensible to modifications in this band. The quality of the secret image embedding is measured with the parameters PSNR and MSE while maintaining the identification of the QR code. The secret message embedded in the QR code is a kind of noise signal for the QR code which emerges in the form of BLUR in the QR code. This BLUR can reduce the readability of the code by the scanner. As a result, the integrity of the QR code is not lost. Our proposed technique will maintain equilibrium between the efficiency and security of this scenario.

Methodology

In the proposed technique, while inserting a secret message image into carrier image, two files are required. One is the QR code Image and second image contains the hidden information.

Algorithm

Phase- I Algorithm used to insert data image into the QR code cover image:

Step 1: Upload the QR code cover image. Step 2: Upload the image consist a Message.

Step 3: Conversion of the text message into binary bit sequence and divide into even and odd bits.

Step 4: notice LSB of every picture element of the QR code cover image and calculate it.

Step 5: Replace each bit of message image with the Mid Band of cover image.

Step 7: Store the Stenographic image.

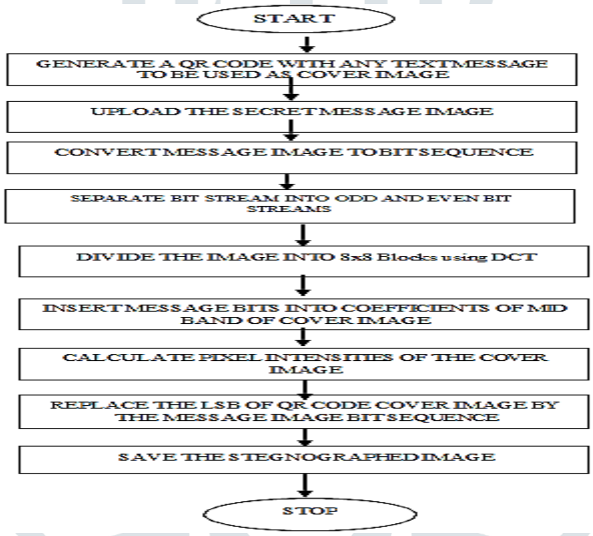

START
GENERATE A QR CODE WITH ANY TEXTMESSAGE TO BE USED AS COVER IMAGE
UPLOAD THE SECRETMESSAGE IMAGE
CONVERTMESSAGE IMAGE TOBITSEQUENCE
SEPARATE BIT STREAM INTO ODD AND EVEN BIT STREAMS
DIVIDE THE IMAGE INTO 8x8 Blocks using DCT
INSERTMESSAGE BITS INTO COEFFICIENTS OF MID BAND OF COVER IMAGE
CALCULATE PIXEL INTENSITIES OF THE COVER IMAGE
REPLACE THE LSB OF QR CODE COVER IMAGE BY THE MESSAGE IMAGE BITSEQUENCE
SAVE THE STEGNOGRAPHEDIMAGE
STOP

Fig 6.1 Working of Proposed Algorithm

Using this method, the message image is converted to bit sequence and each message is converted to the two groups of even and odd sequence. Similarly, all the even groups are concatenated on the other hand odd groups are concatenated. Now the LSB substitution is implemented. The algorithm alters the LSB's of the all images in the mid band section of the cover image and a final image is reconstructed. Not this final image is compared against the original image to calculate out the image quality factors.

The image quality factors are PSNR and MSE [3]. The image steganography system hides the secret message inside the QR code which is being used as QR code. The image content may reduce the visual resolution of the image. Thus, to check this sensory activity result, the peak signal to noise ratio (PSNR) [6, 12] and MSE (t) is used to calculate weighted average of squares. The most effective live of the centre, relative to the current line of error, is that the worth of t that minimizes MSE.

Results

Experiment results of various Images using proposed algorithm in table.

Table 7.1 Experiment results of Image Steganography using proposed technique

Sr. No	Payload	Cover Image	Message Image	PSNR	MSE
1	Harpreet			42.4207	0.0586442
2	https://www.facebook.com/mastercomputerpoint/		f	42.4528	0.0582124
3	Punjabi University Patiala		A	42.4453	0.0563643
4	Hello		PayTM	42.593	0.0577844
5	Steganography			42.5239	0.0572684

In table 7.1. First Step is input text(Payload) to generate the QR Code Cover image, similarly we Embed the massage image (steganographed image) and then Extract the massage whenever needed. To measure the image quality PSNR and MSE image quality parameters used.

Future Scope

Further in future, this technique as it can be implemented in any product selling companies, departments like ecommerce, military, business and even in daily life. New algorithms with better performance for the implementation of hiding the secret message which are compatible with new technologies are always required. In future work of this algorithm, random plane selection (in case of colored QR code) or pixel wise message bit sequence distribution can be implemented for replacing bits with Least Significant Bit (LSB), which in turn provide very high confidentiality of the embedded message.

References

[1] Kumawat, D., Kumar, R., Gupta, D. and Gupta S., 2013. Impact of Denoising using Various Filters on QR Code, International Journal of Computer Applications, Vol. 63, pp.21-26.

[2] Luo, M., Wang, S. and Lin, P. Y., 2016. QR code steganography mechanism with high capacity,

International Conference On. IEEE, pp.1-2.

[3] Chaturvedi, R., Sharma, A., Hemrajani, N. and Goyal, D., 2012. Analysis of robust watermarking technique using mid band DCT domain for different image formats, International Journal of Scientific and Research Publications, pp. 1-4.

[4] Mehboob, B. and Faruqui, R. A., 2008. A stegnography implementation, In Biometrics and Security Technologies(ISBAST), pp. 1-5.

[5] Saravanan, V. and Neeraja, A., 2013. Security issues in computer networks and stegnography, Intelligent Systems and Control (ISCO), 7th International Conference on. IEEE, pp.363-366.

[6] Agarwal, A. 2014. Stretching the Limits of Image Steganography, International Journal of Scientific and Engineering Research, pp. 1253-1256.

[7] Pandit, A. S. and Khope, S.R., 2016. Review on Image Steganography." International Journal of Engineering Science, pp. 6115-6117.

[8] Soni, A. and Badodia, S.K., 2015. Implementation of Improved Steganography For Hiding Text On Digital Data, International Journal of Science and Research (IJSR), pp. 80-84.

[9] Barhate, B. H. and Ramteke, R. J., 2015. Comparative Analysis and Measuring Qualitative Factors using Colour and Gray Scale Images for LSB and DCT-Mid Band Coefficient Digital Watermarking, International Journal of Computer Applications, pp. 34-38.

[10] Banik, B. G. and Bandyopadhyay, S.K., 2015. Review on Steganography in Digital Media, International Journal of Science and Research, Vol.4, pp.265-274.

[11] Islam, M. W. and Zahir, S., 2013. A novel QR code guided image stenographic technique, Consumer Electronics (ICCE), International Conference on. IEEE, pp. 586-587.

[12] Basit, A. and Javed, M. Y., 2007. "Iris Localization via Intensity Gradient and Recognition through Bit Planes", Department of Computer Engineering, College of Electrical and Mechanical Engineering, National University of Sciences and Technology (NUST), Peshawar Road, Rawalpindi, Pakistan. pp.23-28.

[13] Devi, M. and Sharma, N., 2014. Improved Detection of Significant Bit Steganography Algorithms in Color and Gray Scale Images, RAECS UIET University Chandigarh, IEEE, pp.97-115.

[14] Rahma, A. M., Abdulmunim, M. and Janabi, J.S., 2015. New Spatial Domain Steganography Method Based On Similarity Technique, International Journal of Engineering and Technology Volume 5, pp. 122- 125.

[15] Mondal, A. and Pujari, S., 2015. A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients, I. J. Computer Network and Information Security, Vol.3, pp.42-49.

[16] Gulve, A. K. and Madhuri, S.J., 2015. A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution, I.J. Image, Graphics and Signal Processing, pp. 66-74.

[17] Nguyen, B.C., Yoon, S, S. and Lee, H. K., 2009. Multi Bit Plane Image Steganography, Department of EECS, Korea Advanced Institute of Science and Technology, Guseong-dong, Yuseong-gu, Daejeon, Republic of Korea. pp.276-284.

[18] Manikandan, G. and Jeya, R., 2015. Steganographic Technique Involving JPEG Bitstream, Department of Computer Science and Engineering SRM University, Kattankulathur, Kancheepuram, Tamil Nadu , India IJEDR, Vol. 3, pp.124-129..