Research Journal of Applied Sciences, Engineering and Technology 7(19): 4124-4129, 2014
DOI:10.19026/rjaset.7.776
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2014 Maxwell Scientific Publication Corp.
Submitted: December 14, 2013 Accepted: January 01, 2014 Published: May 15, 2014

Research Article

Hiding Secret Text in Quick Response Code and Transforming the Position of the Secret Data using Rotation Transformation

V. Ramya and G. Gopinath
School of Computer Science, Engineering and Applications, Bharathidasan University,
Tiruchirappalli, Tamil Nadu, 620023, India

Abstract: In order to provide high security and safety in the field of information hiding, this study proposes a novel technology using Steganography. An exotic steganographic algorithm, is used in this study, which Hides the secret text data in a 2D plane (Here, in our case let the 2D plane be the QR code), after encryption and the position of the secret data will be changed using rotation transformation. The proposed algorithm has been tested under various imperceptibility characters such as PSNR, MSE, Human Vision Quality Metrics and Histograms are compared to both cover image and the stego image. This novel algorithm shows Lower MSE, higher PSNR values and it is evident that the proposed algorithm is robust to JPEG attacks.

Keywords: Cryptography, information hiding, quick response codes, steganography, transformation

INTRODUCTION

During the past few decades, there is a tremendous development in Steganalysis. The art of detecting Steganographically hidden messages is called Steganalysis. Many of the Steganographic methods deal with embedding the secret message in the Least Significant Bit (LSB) of the Cover image. This technique is most popular because of its simplicity. However many of the LSB techniques used has been detected by the steganalysers effectively because of the unbalanced embedding making the system easily detectable by histograms images.

Steganography the magical word in the world of information hiding, now-a-days has got various other faces. The word Steganography means “Concealed writing”, which casts its importance more because of today’s world of fully automated and completely networked transactions in all kinds of industries right from an information transfer in a grocery shop to the great giants of financial sources and militaries, where the secrecy and security of the information should be maintained strictly. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than that necessary for the objects use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Thus this proposed method use the QR code as the cover media, which is highly undetectable.

The QR barcode is a 2-D symbology developed by Denso Wave in 1994. The code contains information in both the x and y-axis. Generally QR Codes are used for distributing small information like URL, a phone number or even small text. The Government of Canada uses QR Codes for efficient and faster processing of the Passport application forms. The main structure of the QR barcode is shown in Fig. 1. The outer range is the quiet zone. The upper-left, upper-right and left-bottom square areas are used for position detection and pattern separators for positioning. There are six smaller squares which are the alignment patterns. Additionally, the main area, which is colored gray, is the kernel area of data and error correction code. The QR code’s size is decided by determining a symbol version based on data capacity, character type numeric, alphanumeric, Japanese characters, etc. and error correction level and by setting a module size based on the target printer’s or scanner’s performance level.

With this brief overview about the QR codes, we will see how these QR codes are used in our proposed system in the later sections.

LITERATURE REVIEW

Holan *et al*. (2011) proposed a classification framework to combine different thresholding methods and produce better performance for document image binarization. In their work, the framework is divided into three sets of document image pixels namely, foreground, background and uncertain pixels. And then they further bifurcate the uncertain pixels to either

Corresponding Author: V. Ramya, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, Tamil Nadu, 620023, India

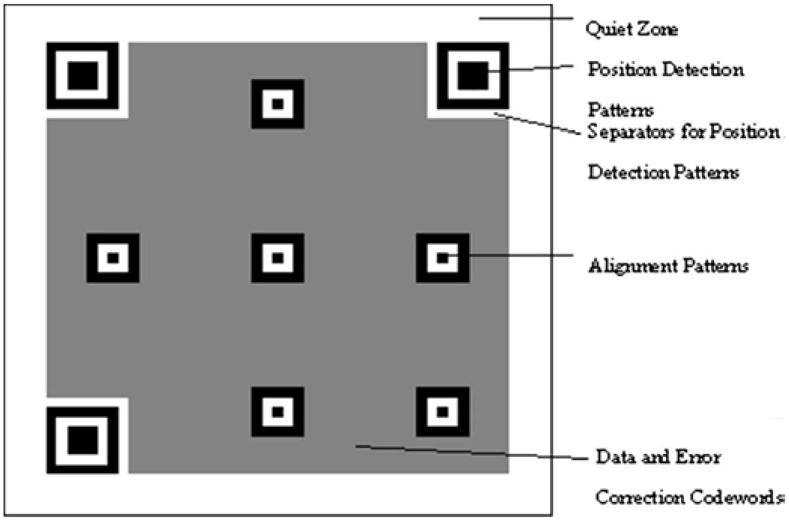
Quiet Zone
Position Detection Patterns
Separators for Position Detection Patterns
Alignment Patterns
Data and Error Correction Codewords

Fig. 1: Structure of QR code

background or foreground, based on already selected pixels. This study produces better binarization results of images, but still more classified methods are required for betterment of the results.

A Method of Image Analysis for QR Code Recognition has been described by Liao *et al*. (2010). Their work better describes the distortion algorithm, geometry revision on images when Quick Response Code is recognizing. This study better deals with the symbol and structure of QR codes and it extracts the central coordinates of the image and necessary rotation algorithm is used. This study is helpful in understanding the algorithm for image rotation and geometry correction. Though this proposed method involves more on hiding the information inside a 2D plane, than simple recognizing the QR code, this method of image analysis stand as a base study for the feature work.

An useful citation on Image Hidden Technique Using QR-Barcode has been given by Chin-Ho *et al*. (2009). This study deals with nested steganography scheme which involves QR (Quick Response) bar code and image processing techniques. Here the text data is first encoded into a Quick Response code. The error correction module of the QR code is carefully designed in this study, so that it makes the lossless compression holds good. This study is robust to JPEG attacks, but still it is limited to BMP, gray scale images and binary images.

Jiejing *et al*. (2010) in their work tried to improve the accuracy of Quick Response codes while decode it through a mobile image processing. Sauvola's thresholding algorithm has been modified in a better way that QR codes can be recognized even in uneven lighting conditions.

From this study, the idea of binarization of QR code has been well explored and average elapsed time could still be maximized.

A good work on QR code security presented by Peter *et al*. (2010), examines more about attacks on QR Codes and the possible consequences. Since Quick Response codes are only machine readable the author explored the various ways of anti phishing and showed the different kinds of attack strategies from the attackers' point of view. The Vulnerability of the QR code depends on the type of the attack and its characteristics.

Wang *et al*. (2005) proposed a steganography scheme in that the message to be hidden into the cover image is incorporated with the use of modulus operation. In his study, a half of the size and a quarter of the size of the chosen host-image were used to demonstrate the secret image can totally be embedded and preserved high image quality. Based on an embedded zero tree wavelet compression method and bit-plane complexity segmentation skill, Spaulding *et al*. (2002) proposed a steganography scheme. From his experimental results, it achieved a large embedding capacity of around 255 of the compressed image size with minor noticeable degradation in image quality.

Also many authors in the recent past, Arash *et al*. (2011), Islam and Zahir (2013), Su and Niu (2010), Vavilis and Ergina (2011) and Zou *et al*. (2010) proposed novel steganographic view that stays a good ideate for this proposed study.

PROPOSED METHODOLOGY

Embedding algorithm:

Step 1: Read the Cover image Ci as a 2D file.
Step 2: Binarify the QR code.
Step 3: Consider the Secret data as text data. And each 8 bits forms a character.
Step 4: Convert the secret data into binary row matrix
Step 5: Input the 4 digit key, (Ck).

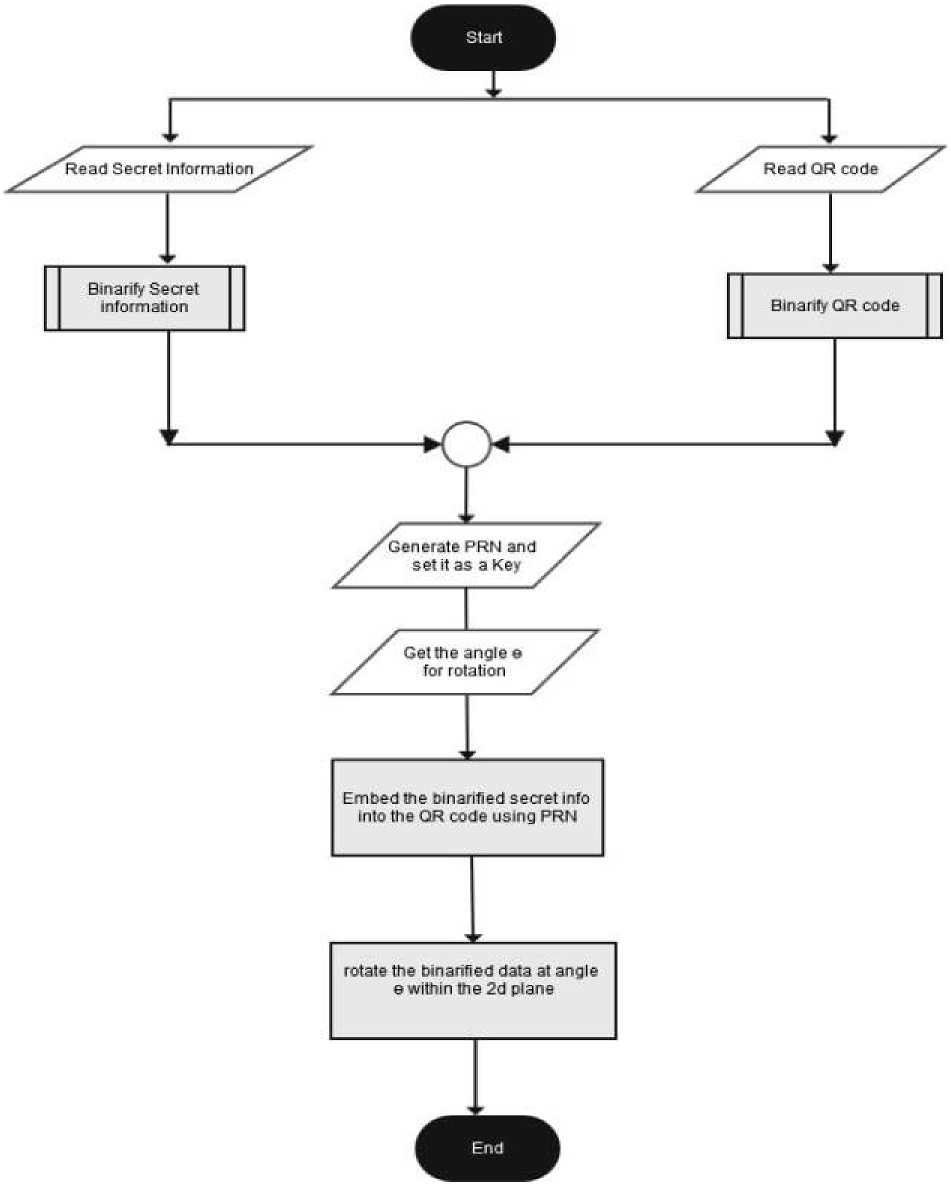
Start
Read Secret Information
Read QR code
Binarify Secret information
Binarify QR code
Generate PRN and set it as a Key
Get the angle e for rotation
Embed the binarified secret info into the QR code using PRN
rotate the binarified data at angle e within the 2d plane
End

Fig. 2: Embedding workflow

Step 6 : Select a Pseudo Random Number N between 0-9.
Step 7 : Select a Pseudo Random Number degree for θ between 0-360.
Step 8 : Iterate till the length of secret Message Len (msg). Till no. of transformations N.
Step 9 : Rotate all the bits of the secret message msg by calling the rotaion function along the 2D plane of the Ci for Selected Degree of angles.
Step 10: Save the image as Stego Image, Si.
Step 11: End process.

Extracting algorithm:

Step 1 : Read the Stego image Si as a 2D file.
Step 2 : Read Secret key, (Sk).
Step 3 : Compare Secret keys, If Sk = Ck perform the following tasks Else go to Step 10.
Step 4 : At the selected Degree angle θ.
Step 5 : Till the rotations transformations PRN.
Step 6 : Get the secret message msg from Si.
Step 7 : Now convert each 8 bits of the row matrix into a character.
Step 8 : Hence the required secret message msg is recovered.
Step 9 : Save the message msg.
Step 10: End process.

Explanation: Figure 2 and 3 demonstrates about the embedding and extracting workflow respectively. The proposed method, first binarify the QR code and also

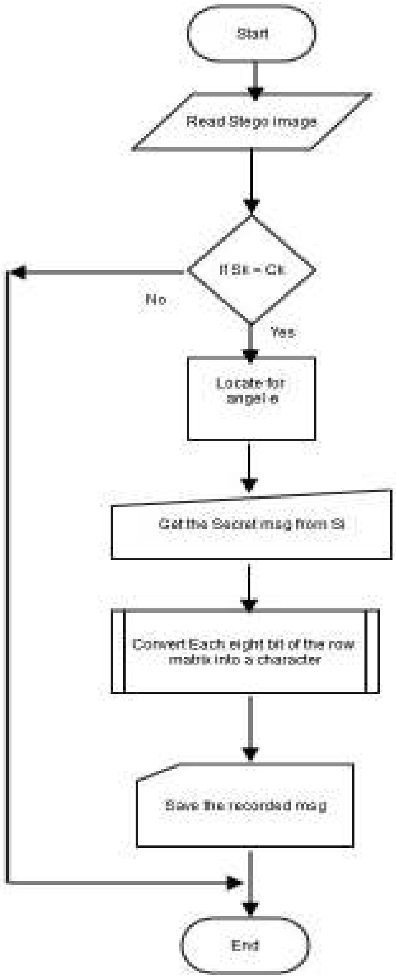
Start
Read Stego image
If Si = Ck
No
Yes
Locate for angel θ
Get the Secret msg from Si
Convert Each eight bit of the row matrix into a character
Save the recorded msg
End

Fig. 3: Extracting workflow

the secret message. Then by setting the symmetric key for authentication, without which the algorithm is highly impossible for steganalysis. Generate the Pseudo Random Number N, where N signifies the No. of rotation transformations to be performed about the 2D plane of the QR code. After fixing the No. of rotations, the angle of rotation has been identified by fixing the Degree θ value. So that the secret message will rotate on the fixed angle along the 2D plane of the QR code. After the No. of rotation transformation set by the value N, the Secret message has been hidden inside the QR code.

RESULTS AND DISCUSSION

Original image with its binary representation and their histogram comparisons:

Histogram of binarified cover image before and after embedding the secret message: Figure 4 shows the comparison of the QR code before call of binarization algorithm and after the QR code is binarized. The histogram clearly shows that after binarifying the QR code image all the gray level that varies from 0-255, has been converted efficiently to either the value 0 or value 1.

Figure 5 shows the real outcome of the work, where the binarified images of the Quick response codes before and after embedding the secret data are compared. The histogram result shows that there is no major deviation in the values of the pixel before and after embedding the data, thus makes the algorithm highly undetectable and robust for steganalysis.

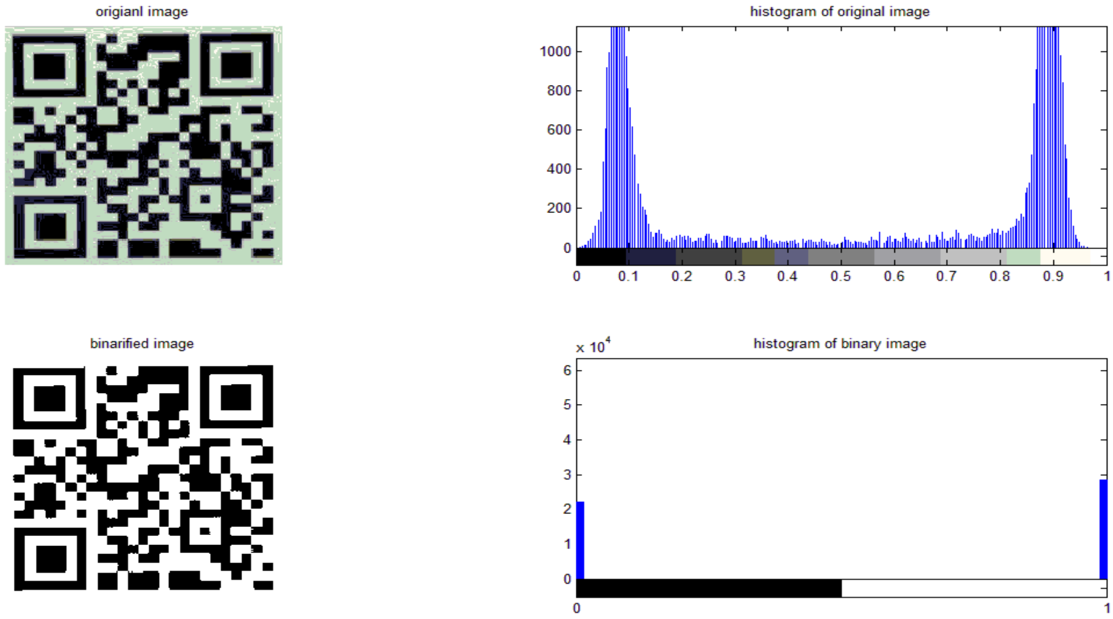

Fig. 4: Histogram comparison of QR codes before and after binarification

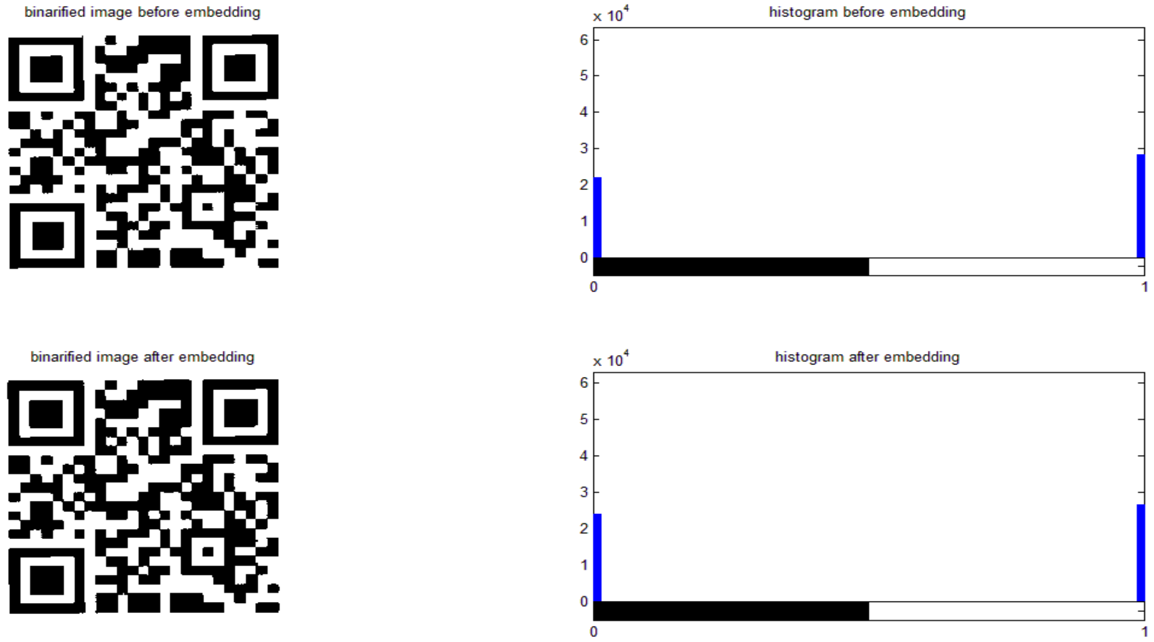

Fig. 5: Histogram comparison of QR code before and after embedding the secret text

CONCLUSION AND RECOMMENDATIONS

Over the decades steganalysis has been developed to a great extant and so, mere hiding of information is not enough. So, this study deals with an eye of enhancing security for the information in various levels. In order to increase the complexity of detecting the stego image the proposed algorithm has been designed in a way, that without knowing the key it is highly impossible to detect or extract the secret information. Since because, the secret information has been first binarified and then by generating the pseudo random numbers, the same is rotating in the 2D plane (here, QR code), with respect to the PRN generated.

This study proposed a new steganography algorithm. Images with various sizes secret text data are tested. With the proposed algorithm, it is evident that the stego image does not have a noticeable distortion on it, as seen by the naked eyes. PSNR and MSE of Stego images with various text data are calculated. Based on the PSNR value of each images, the stego image has a higher PSNR value and lower MSE. Hence this new steganography algorithm is very efficient to hide the data inside the image.

REFERENCES

Arash, H.L., A.M. Azizah and M.D. Salwani, 2011. A Survey on Image Steganography Algorithms and Evaluation. In: Snasel, V., J. Platos and E. El-Qawasmeh (Eds.), ICDIPC, 2011, Part I. CCIS 188, Springer-Verlag, Berlin, Heidelbfrg, pp: 406-418.

Chin-Ho, C., C. Wen-Yuan and T. Ching-Ming, 2009. Image hidden technique using QR-barcode. Proceeding of the 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp: 522-525.

Holan, S., L. Shijian and L.L.L. Chew, 2011. Combination of document image binarization techniques. Proceeding of the International Conference on Document Analysis and Recognition, pp: 22-26.

Islam, M.D. and S. Zahir, 2013. A novel QR code guided image stenographic technique. Proceeding of the IEEE International Conference on Consumer Electronics (ICCE), pp: 586-587.

Jiejing, Z., L. Yunfei and L. Peng, 2010. Research on Binarization of QR code image. Proceeding of the International Conference on Multimedia Technology (ICMT), pp: 1-4.

Liao, Z.L., T.L. Huang, R. Wang and X.Y. Zhou, 2010. A method of image analysis for QR code recognition. Proceeding of the International Conference on Intelligent Computing and Integrated Systems (ICISS, 2010), pp: 250-253.

Peter, K., L. Manuel, M. Martin, M. Lindsay, S. Sebastian, S. Mayank and W. Edgar, 2010. QR code security. TwUC, 1040: 8-10.

Spaulding, J. and H. Noda, Kyushu Inst. of Technol., Kitakyushu, M.N.J. Shirazi, 2002. Application of bit-plane decomposition steganography to wavelet encoded images Image Processing. Proceedings International Conference on image processing Volume 2.

Su, J. and H. Niu, 2010. Design and realization of an improved information hiding algorithm. Proceeding of the 2nd International Conference on Computer and Automation Engineering (ICCAE), 3: 177-179.

Vavilis, S. and K. Ergina, 2011. A tool for tuning binarization techniques. Proceeding of the International Conference on Document Analysis and Recognition, pp: 1-5.

Wang, N.W., T. Chwei-Shyong, H. Min-Shiang, 2005. A high quality steganographic method with pixel-value differencing and modulus function Journal of Systems and Software, 81(1): 150-158.

Zou, X., C.L. He and Z.J. Liang, 2010. A binarization method of quick response code image. Proceeding of the 2nd International Conference on Signal Processing Systems (ICSPS, 2010), 3: 317-320.