International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Image Steganography and Data hiding in QR Code

Rutuja Kakade[1], Nikita Kasar[2], Shruti Kulkarni[3,] Shubham Kumbalpuri[4], Sonali Patil[5]

Student, Dept of Computer Engineering, PCCOE, Maharashtra, India
[5]Associate Professor, Dept of Computer Engineering, PCCOE, Maharashtra, India

---

Abstract - *Sometimes there is a need to keep our data safe and as at many places there is private data which needs to be secured. For this reason steganography is a technique which can be applied. Also we can add data in QR code for the ease of access of sending information. Steganography is using the DWT technique and LSB steganography. The data to be steganographed is encrypted using AES algorithm to enhance the security.*

Key Words: **Information security, Steganography, DWT, AES algorithm, QR code**

1. INTRODUCTION

In this paper QR code and Steganography is used to provide the security to important data.

1.1 QR Code

QR codes are 2 dimensional matrix. It allows to store a large volume of unique data. Bar-codes are one dimensional vector. So compare to bar-codes QR codes are having more storage capacity. QR codes can hold up to 7,089 numeric characters and up to 4,296 alphanumerical letter values as an information. The following figure shows the structure of a QR code.

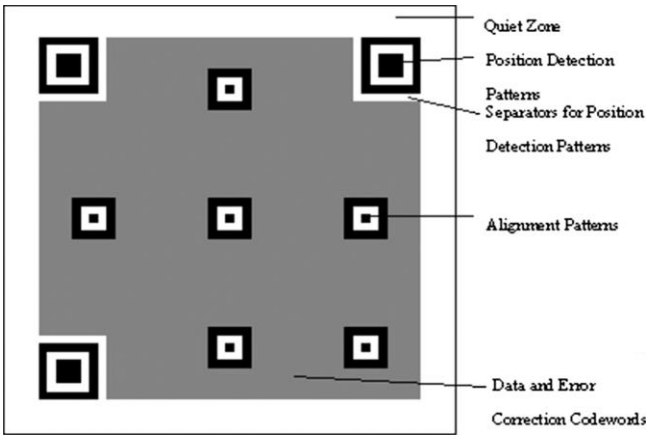

Fig- 1: QR code

1.2 Steganography

Steganography is an embedding technique to hide the data in the form of an image or text. the modern-day sense of the word sometimes refers to data or a file that has been hid within a digital image, Video or Audio file. What Steganography basically does is exploit human perception; the human senses aren't trained to look for files that have data hidden inside them. Generally, in steganography, the particular data isn't maintained in its original format and thereby it's converted into an alternate equivalent transmission file like image, video or audio that successively is being hidden among another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, wherever the particular message is separated from it. Steganography are used to achieve data privacy over secrecy.

2. LITERATURE SURVEY

2.1 Image steganography with using QR code and cryptography[1]

In this there is image steganographic methodology that's able to embed the encoded secret message using Quick Response Code (QR) code into the image information. Discrete Wavelet Transformation (DWT) domain is employed for the embedding of the QR code, whereas embedding method is in addition secured by Advanced Encryption Standard (AES) cipher algorithmic rule. In additionally, typical characteristics of QR code was broken using the encryption, therefore it makes the method more secure. The relation between security and capability of the strategy was improved by special compression of QR code before the embedding method.

2.2 Information Hiding using Image Embedding in QR Codes for Color Images[2]

They say that embedding strategies are designed to be compatible with standard decoding applications and might be applied to any color or gray scale image with full space coverage. The embedding technique consists of 2 elements. Initial is that the use of halftoning techniques for the choice of changed pixels to interrupt and reduce the coarse square structure of the QR code and second is that the brightness level level to that the pixels square measure to be remodeled in such some way that it mustn't visible to naked eye on the color image. Later decode the QR code from the color image with minimum errors.

2.3 Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System[4]

In this paper, there's totally different methodology, where the marks obtained by a candidate will be encoded in QR Code in encrypted type, so that if an intruder tries to change the

marks within the mark sheet then he cannot do this , as a result of the encryption key is unknown to him. In this method encryption of the mark sheet data is done using TTJSA encryption algorithm. The encrypted marks are entered inside QR code and that QR code is also printed with the original data of the mark sheet. The marks can then be retrieved from the QR code and can be decrypted using TTJSA decryption algorithm and then it can be verified with marks already there in the mark sheet.

2.4 Nested image steganography scheme using QR-barcode technique [8]

There are two types of secret data lossless and lossy embedded into a cover image. The lossless data is text that is initially encoded by the QR barcode and its data doesn't have any distortion when comparing with the extracted data and original data. The lossy data is a kind of image in that case the face image is appropriate as a result of the extracted text is lossless, the error correction rate of QR encoding should be carefully designed. In image embedding, as a result of it will sustain minor perceptible distortion so they adopted the lower nibble byte discard of the face image to reduce the secret data. Once the image is extracted, a median filter is used to separate out the noise and procure a smoother image quality. After simulation, it's tried that scheme is powerful to JPEG attacks. Compared to different steganography schemes, the proposed technique has 3 advantages: i) the nested theme is an increased security system never previously developed; ii)our scheme will conceal lossless and lossy secret data into a cover| image simultaneously; and iii) the QR barcode used as secret data can widely extend this method's application fields.

2.5 Reversible Data Hiding with Histogram-Based Difference Expansion for QR Code Applications[6]

As the QR code looks like random noise and it occupies a corner of the original image, its existence will greatly cut back the worth of the first content. Thus, how to retain the value of original image, whereas keeping the capability for the moment access for webpages, is that the major concern of this paper. With the help of reversible data concealment technique, the QR codes are often hidden into the original image, and there's hefty increase in embedding capability. They propose a scheme such that when the image containing the QR code is browsed, the hyperlink like the QR code is accessed first. Then, the QR code may get nonexistent and also the original image would be recovered to retain the information sent in that.

3. PROPOSED SYSTEM

The proposed system is considered to keep the criminal data secured. QR code is used to store every record of particular criminal. The sensitive data is hidden in the image which is first encrypted using AES algorithm. The cover image or original image undergoes DWT(Discrete Wavelet Transformation) and the data is hidden in the HH band.

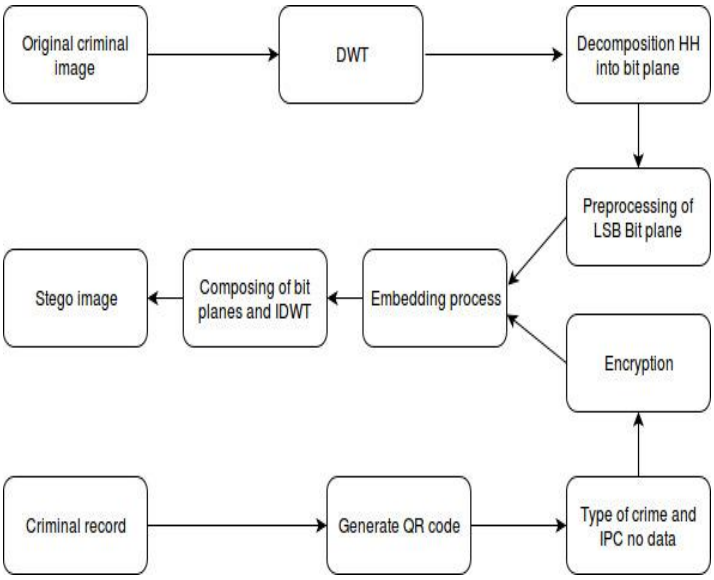

Fig-2 : Proposed system

4. CONCLUSIONS

There are many applications of this technique wherever more security is required. We have considered securing criminal data as one of its applications. The criminal information may be changed for misleading the police department. The data that can be changed or tampered is mainly the type of crime performed, which can be changed for reducing the punishment of the culprit. The proposed system provides security to criminal data from unauthorized access and tampering.

REFERENCES

[1] V.Hajduk , M.Broda , O.Kováþ and D.Levický, "Image steganography with using QR code and cryptography," 26th Conference Radioelektronika, IEEE pp. 978-1-5090-1674-7, 2016

[2] A. Gaikwad and K.R.Singh, "Information Hiding using Image Embedding in QR Codes for Color Images: A Review," International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015

[3] M. Broda, V. Hajduk, D. Levický, "Image steganography based on combination of YCbCr color model and DWT," in ELMAR, 2015 57th International Symposium, pp. 201-204, 28-30, 2015.

[4] S. Dey, A.Nath and S. Agarwal, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," International Conference on Communication Systems and Network Technologies, 2013

[5] S. Dey, K. Mondal, J. Nath and A. Nath, "Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted

secret message: ASA- QR algorithm," International Journal of Modern Education and Computer Science, vol. 6, pp. 59-67, 2012.

[6] H. C. Huang, F. C. Chang and W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR Code applications," IEEE Transactions on Consumer Electronics, vol. 57, no. 2, pp. 779-787, 2011.