International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 22 | MAY - 2022 ISSN: 2582-3930

DATA ENCRYPTION THROUGH QR CODE AND STEGANOGRAPHY

Aditya Pol, Bhushan Raut, Sahil Aryan.
Prof. Pramod Dhamdere
Computer Engineering
Parvatibai Genba Sopanrao Moze College of Engineering, Wagholi, Pune

***Abstract*—The art of information hiding has become an important issue in the recent years as security of information has become a big concern in this internet era. Cryptography and Steganography play major role for secured data transfer. Steganography stands for concealed writing; it hides the message inside a cover medium. Cryptography conceals the content of a message by encryption. QR (Quick Response) Codes are 2-dimensional bar codes that encode text strings. They are able to encode information in both vertical and horizontal direction, thus able to encode more information. In this paper a novel approach is proposed for secret communication by combining the concepts of Steganography and QR codes. The suggested method includes two phases: (i) Encrypting the message by a QR code encoder and thus creating a QR code (ii) Hiding the QR code inside a color image. This hiding process embeds the quantized QR code so that it will not make any visible distortion in the cover image and it introduces very minimum Bit Error Rate (BER). Experimental result shows that the proposed method has high imperceptibility, integrity and security.**

Keywords Steganography, QR code, BER

I. IN TROD UCTION

Cryptography, Steganography and Watermarking techniques can be used to obtain security, secrecy, privacy and authenticity of data. Cryptography encrypts the message and makes it unreadable and unintelligent form called cipher. Steganography hides the data in a medium such as text file, image, audio, video etc., and conceals the very existence of the message in the medium. QR code is a two dimensional bar code capable of encoding different types of data like binary, numeric, alphanumeric, Kanji and control code. A piece of long multilingual text, a linked URL, an automated SMS message, a business card or just about any information can be embedded into the QR code. QR codes (Quick Response codes) were introduced in 1994 by Denso-Wave, a Japanese company subsidiary of Toyota. Initially, these codes where conceived as a quick way to keep track of vehicle parts, being nowadays extremely popular in Asian countries like Japan, South Korea, China or Taiwan and becoming more and more popular in western countries by the day. [1] QR codes are capable of encoding the data both in horizontal and vertical direction, thus able to encode several times more data than the bar codes. The following table shows the maximum number of characters encoded in a QR code (version 40) with and minimum error correcting level L:

S.No.	Data Type	Characters
1	Numeric data	7,089
2	Alphanumeric data	4,296
3	8-bit byte data	2,953
4	Kanji data	1,817

Fig. 1.

Fig.1 shows a QR code and Error Correction (EC) levels. [2] The technology of QR codes has proved out to be successful even if the code is partially damaged. This is feasible due to the error correction in QR codes, which is based on the Reed-Salomon Codes. There are four levels of error correction; Low (L) which can tolerate up to 7% damage, Medium (M) can tolerate up to 15% damage, Quartile (Q) can tolerate up to 25% damage and High (H) can tolerate up to 30% damage. The reason why the Low (L) error correction level is preferred is that the High error correction levels raise the percentage of code word used in error correction thereby decreasing the amount of data that can be stored in the code

II. LITERATURE REVIEW

The primary tool used in the research of steganography is the Internet. The first objective was to understand the various terminologies related to the field. This was done through the Wikipedia and the hyper dictionary websites. Additional technical details were obtained from various articles listed under the References and Bibliography section. The following points can be attributed to the renaissance of steganography:

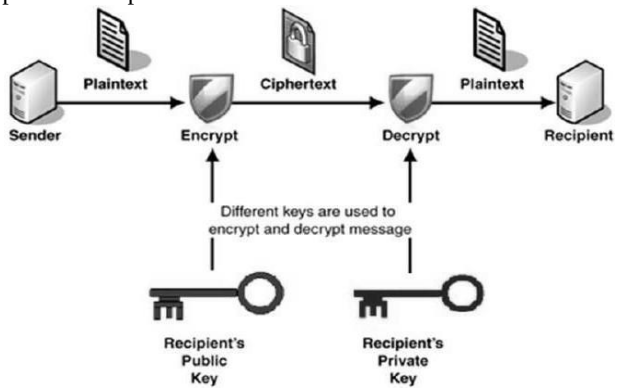
- Government ban on digital cryptography. Individuals and companies who seek confidentiality look to steganography as an important complementary since combining cryptography and steganography can help in avoiding suspicion and protect privacy.

- The increased need to protect intellectual property rights by digital content owners, using efficient Encryption

- The trend towards electronic communications and humans desire to conceal messages from curious eyes. With rapid advancement in technology, steganography software is becoming effective in hiding information in image or text files

III. METHODOLOGY

A. . **Genetic Algorithm:** Genetic algorithm in cryptography can be used for generating the key. Key generation in cryptography is the most important part of encoding data. If the key is randomly chosen and non-repeating used than this cypher is called one-time pad (or one-time system). The one of the most used one-time pad is in Verna cipher. Verna cipher is a stream cipher where plaintext is converted into cipher text by using XOR operation between plaintext and the key. One of the possible methods of generating the key is described in the work. It consists of: 1. Generating binary population. For this step, pseudo random number generator can be used. 2. Selection. Where the two parents will be chosen for reproduction. 3. Crossover. From parents by using crossover operator we gain child. 4. Mutation. After crossover we applied mutation operator. 5. Fitness function. If value from fitness function is satisfactory random chromosome is selected as the key else process is repeated.



B. **QR Code Steganography:** Steganography is the art and science of writing secret messages in such a way that aside from the sender and the intended receiver, no one even suspects the existence of the secret message. Notice that steganography goals are in contrast to the goals of cryptography because encrypted messages or images attract attention. In steganography, the mere suspicion of a hidden message existence is sufficient to declare the failure of the scheme, even if the hidden message cannot be deciphered. QR codes have been previously used to exchange encrypted content, but there is no such research that uses them for steganography in the same fashion as this research. Being able to hide secret messages within general QR code symbols creates endless possibilities for discreet communication through QR codes. The idea behind this research is to show how to communicate a secret message between the sender and the receiver using QR codes without arousing any suspicion. Additionally, we show two ways to extract the secret message from the QR codes: first, using a private shared key between the sender and receiver, and second, without a shared key. For the purpose of this experiment, we show how person A (Adam) will communicate a secret message with person B.

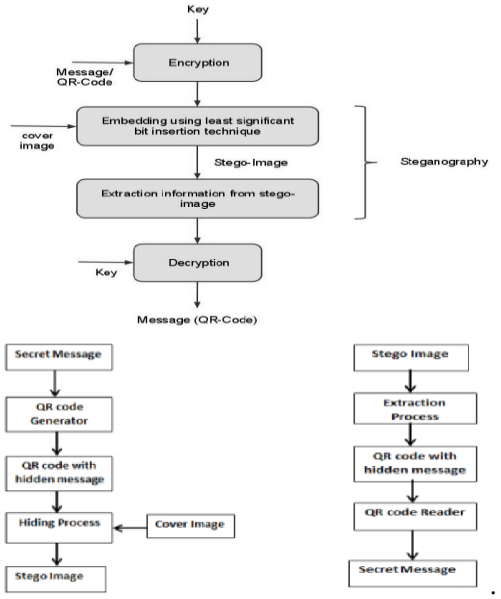


Fig. 2

C. **Proposed work**

A QR code generator encrypts the given message into QR codes which could not be read or understood by human beings. But the message hidden in these QR codes can be easily decoded by any smart phone with built in camera. In order keep the message secret and to protect it from unauthorized access a new method is suggested by merging QR codes with Steganography technique. The proposed method encompasses an encoding process at the sender and a decodingprocess at the receiver.

D. Architecture

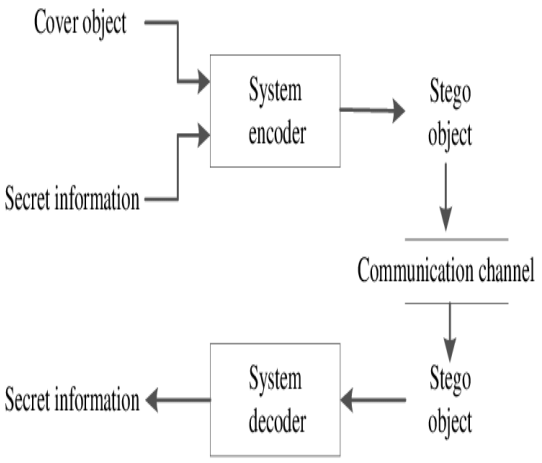


Fig. 3

IV. RESULTS

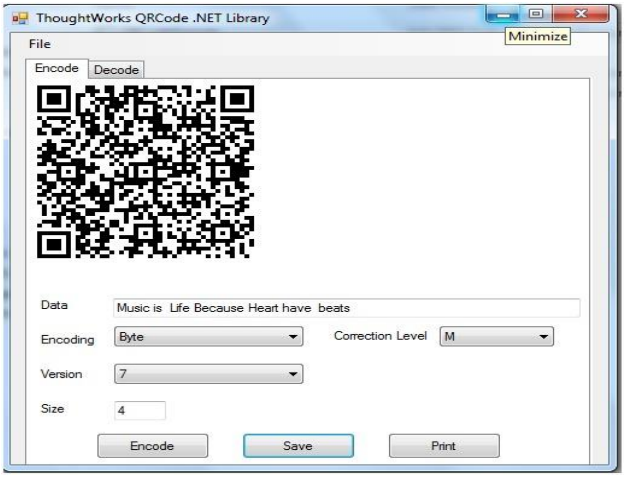


Fig.4. Converting plan text in QR code format

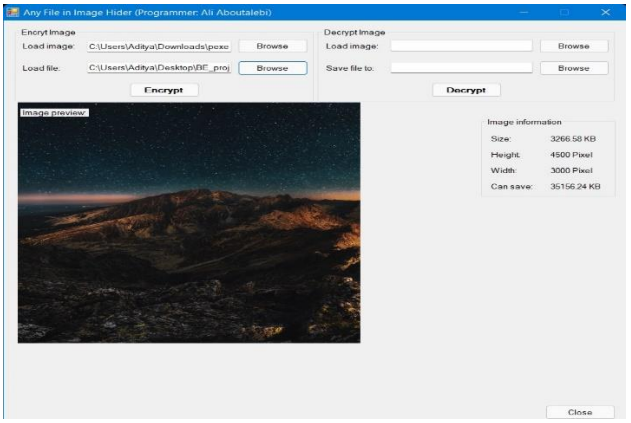


Fig. 5. Hiding QR code in Cover Media

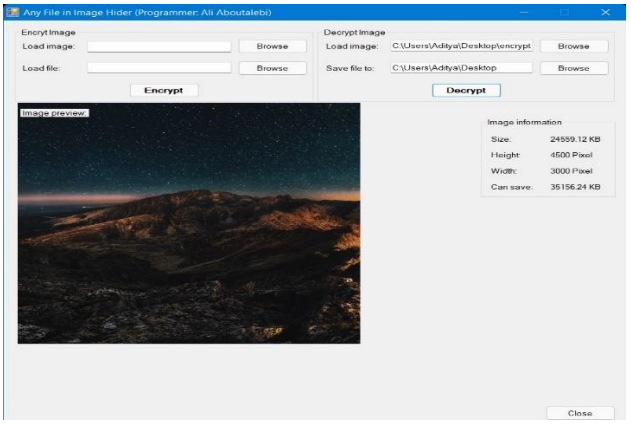


Fig.6.decrypting The Image (Separating The hidden message and cover media)

V. CONCLUSION

QR codes can be used for various applications such as business, marketing, education, data security, authentication etc. In this paper a novel method is suggested for data security using QR codes and steganography. Message encrypted in a QR code can be read easily by any QR code scanner. But since the proposed method incorporates steganography, it enhances theconfidentiality and security. Similar work could be done in future using color QR codes so thatmore information can be encrypted and sent secretly.

VI. FUTURE WORK

Due to the rich availability of choices and the masking features offered by the massive utilization in Internet, malware developers could find the highest potential in network steganography. So, the future work will be possible to make deeper analysis in order to understand the steganography process of hider man and masker. The research can be expanded by doing analysis of steganography process of other tools in the audio and video media file. Identifying the maximum capacity of information that can be hidden in an image using a particular stenographic tool has to be modeled.

VII. ACKNOWLEDGEMEN T

We take this opportunity to thank our Project Guide Prof. Pramod Dhamdere and Head of the Department Prof. Shrikant Dhamdere for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of computer Engineering of Parvatibai genba sopanrao moze college of Engineering, wagholi, Pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

VIII. REFER ENCES

[1] Mrs. G. Prema, S. Natarajan, "Steganography using genetic Algorithm along with visual Cryptography for Wireless Network Application", International conference on information communication and embedded systems (ICICES), 2019.

[2] Fridrich J., Goljan M. And Du R, “Reliable Detection of LSB Steganography in Color and Grayscale Images”, Proceedings of Workshop on Multimedia and Security, Ottawa, pp. 27-30, , October 5 2018.

[3] J. Fridrich, M. Goljan and D. Hogea, “Steganalysis of jpeg images: Breaking the f5 algorithm”, In Proc. Of the ACM Workshop on Multimediaand Security, 2015.