ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

ENHANCED SECURITY IN STEGANOGRAPHY USING ENCRYPTION AND QUICK RESPONSE CODE

P.Rajendiran*, B.Elangovan and B.Srinivasan
Department of Information Technology, School of Computing, SASTRA University, Thanjavur-613401, India.
Email: rajendranap@it.sastra.edu

Received on: 18.10.2016 *Accepted on: 11.11.2016*

Abstract

Transferring confidential data is a real challenge and is the need of the hour. Steganography deals with concealing secret message in the image whereas cryptography is about altering the message into a distorted form, so that it is prevented from unauthorized access. Combining both the steganographic and cryptographic techniques will yield a secure and sophisticated system for exchanging the secret information between the sender and receiver. QR codes, also known as two-dimensional barcodes are used for increased encoding space. In this paper, a secure information model is built by combining cryptography and steganography.

QR codes are employed for encoding the encrypted message. A nested image steganography is performed with QR codes on a suitable cover image. The proposed approach has a potential to be employed in communicating confidential information.

Keywords: Steganography, QR code steganography, Scrambling, Encryption, QR codes, Nested Steganography.

1. Introduction

Due to advancements in communicating technologies and proliferation of internet facilities, it is a necessity to build a system for transferring confidential data securely over a network. Steganography involves concealing messages in the images which are referred as cover images. These cover images are then transferred across the network securely. The hidden messages are overlooked and cannot be retrieved without knowing the exact steganographic technique. Cryptography includes modifying the message format by applying various techniques and finally rendering a distorted message which is not intelligible. Both the techniques have their own pros and cons. By combining both the techniques, a secure and more sophisticated system can be built.

2. Literature Survey

Damir Omerasevic et al. [1] proposed an implementation of secure key exchange by using QR codes. Their work proposed the term RICA which stands for Robustness, Integrity, Confidentiality and Authentication. Addition of robustness to the data communication is the novelty of their proposed work. The robustness is achieved by the utilization of Quick Response (QR) codes, which has resistance on errors up to a certain limit. Their work has utilized many properties of QR codes to achieve the efficiency along with robustness. Yin-Jen Chiang et al. [2] proposed a new and efficient steganographic QR code algorithm which maintains the robustness of QR codes by preserving the content readability of QR codes and by holding the error correction capability. The proposed mechanism suggests communicating a large secret payload along with the adjustment of error correction level and version details. Their work also includes the blind property which allows the recipient to realize the communicated message without considering the embedded position of the modules in the QR code. Ji-Hong Chen et al. [3] suggested an identification recovery scheme using water marking technique and QR codes. Their work suggests a matrix barcode for the verification of copyrights for an image. The proposed scheme involves copyright text, QR codes, watermarking techniques to built an efficient identification scheme, also by implementing direct sequence spread spectrum and varying the modified code division multiple access for hiding the QR code. Peter Kieseberg et al. [4] in their paper explained the QR code security. Their work analyzed QR codes and their utilization to attack systems and interactions. Uma Maheswari et al. [5] proposed a frequency domain image steganographic technique, with the help of QR code and fresnelet transform. QR code has been utilized effectively for encoding the secret message and also scrambling technique technique has also been employed to enhance the security. Somdip Dey et al. [6] proposed an advanced steganography algorithm for hiding the message. They suggested a two step hiding technique for effectively communicating the message. Their scheme involves message to undergo encryption, encoding into QR codes, scrambling and then embedding into cover image. Wai Wai Zin [7] proposed in his work an embedding scheme for messages using LSB steganographic technique. The embedding technique is mainly concerned with PNG file format. The scheme includes encrypting the message before embedding it into the cover image using BBS generator produced random sequence of numbers. Kaustubh choudhary et al. [8] presented a detailed report on image properties in LSB plane. His work describes the bit plane slicing technique in detail, which summarizes the significances of MSB and LSB planes of an image.

Salim M. Wadi et al. [9] presented a rapid encryption method based on AES algorithm for grey scale HD image Encryption. Few modifications were presented in their work which ensures enhancements in the AES algorithm in terms of pattern appearance and time ciphering. The modification includes decreasing the number of rounds and replacing the S-box for minimizing the hardware requirements. These modifications results in the faster execution of AES algorithm without compromising the security. Padmavathi et al. [10] conducted a performance analysis survey on various algorithms like DES,AES,RSA combining with LSB substitution technique which serves well to draw conclusions on the three encryption techniques based on the their performances in any application. Their work includes the implementation of the three techniques along with Least Significant Bit substitution method to rate their performances in terms of buffer size and stimulated time at encryption and decryption processes. It has been concluded from their work that AES encryption is better than other techniques as it accounts for less encryption, decryption times and also uses less buffer space.

Shashi Mehrotra Seth et al. [11] analyzed encryption algorithms for data communication based on computation time, output byte and memory usages.

3. RELATED WORK

3.1. Advanced Encryption Standard

The Advanced Encryption Standard (AES), referred as Rijndael, is an effective cryptographic algorithm widely employed to protect electronic data. The design principle involved in AES is referred substitution-permutation network. The AES technique functions on a 4×4 column-major order matrix of bytes, referred as the state. The AES encryption technique is an iterative symmetric-key block cipher with varying key sizes (128, 192, and 256 bits). The same key is utilized by symmetric-key ciphers for encrypting as well as for decrypting data, unlike public-key ciphers, which utilizes different keys.

The size of the key utilized in AES cipher defines the number of cycles of transformation rounds that transform the input, referred as plaintext, into the final output, referred as the cipher text.

- 10 repetition cycles - 128 –bit keys.
- 12 repetition cycles - 192 –bit keys.
- 14 repetition cycles - 256 –bit keys.

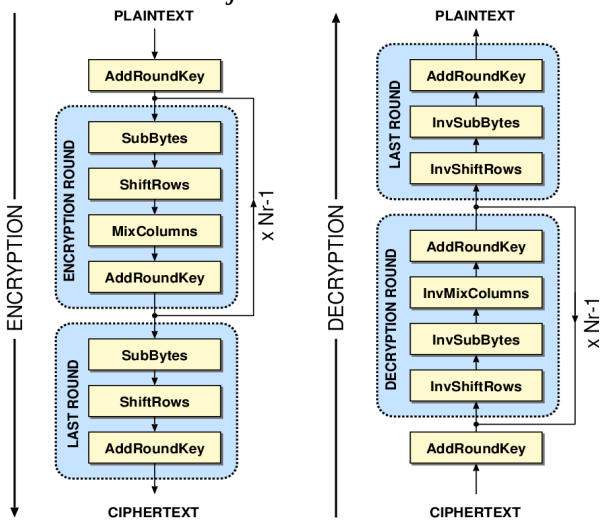


Fig.1 AES Encryption and Decryption.

In AES, the data encryption and decryption is accomplished in 128 bit (16 bytes) blocks. The returned encrypted data by block ciphers contains the exact number of bits as the input data. AES algorithm consists of several rounds each containing many processing steps. They include

Key Expansions

From the cipher key, utilizing Rijndael's key schedule the round keys are derived.

First Round

- **Add Round Key**: Employing the bitwise xor a block of the round key is combined with each byte of the state.

Rounds

1. Sub Bytes: This is a non-linear substitution where every byte is substituted with another according to a look up table.

2. Shift Rows: This is a transposition step, in which the last three rows of the state are shifted cyclically a certain number of steps.

3. Mix Columns: Operates on the columns of the state, referred as mixing operation. It combines four bytes in each column.

4. Add Round Key: One block of the round key is combined with each byte of the state with the help of bitwise xor.

Last Round

1. Sub Bytes: This is a non-linear substitution where every byte is substituted with another according to a look up table.

2. Shift Rows: This is a transposition step, in which the last three rows of the state are shifted cyclically a certain number of steps.

3. Add Round Key: One block of the round key is combined with each byte of the state with the help of bitwise xor.

AES is regarded as the de facto standard for carrying out the encryption for all types of electronic data in telecommunications, banking and financial transactions, private and Federal information exchange.

3.2. Quick Response Codes

Quick Response codes alias QR codes are known as two dimensional codes are increasingly used now-a-days. Invented by Denso-Wave in 1994 QR codes are handy, portable and can be generated efficiently. The QR codes provide large space for encoding. QR Codes are generally employed for communicating small information like URL, a phone number or even small text. QR codes are the generalization of barcodes. QRs have been widely accepted as they are being used by large number applications on iOS and Android mobile platforms due to the advancements in smart-phone technology. The QR codes can be generated easily from many online open sources and also by utilizing software. And the decoding can be easily carried out with help of a smart phone equipped with a camera and a suitable decoding application. The QR codes come with a predefined structure, with specific allocations for information in encoding the data. QR codes also provide many desirable features like high capacity encoding of data, small size, resistant to dirt and damages. And also it is readable from any direction.

The QR code has a cell architecture arranged in the square and is a matrix type symbol. The functionality patterns in the QR code enable the reading of the data area. The QR code architecture as shown in Fig.2, has position patterns, alignment patterns, timing patterns, quite zone, and data area. A symbol arranged at the three corners determines the position pattern, from which the position, the angle and the size of a QR code can be found. It is because of this the QR code can be detected in all directions. For adjusting nonlinear distortions Alignment patterns are extremely efficient. The distortion of the symbol can be corrected by identifying the central coordinate of the alignment pattern. The QR Code contains white and black patterns arranged in an alternate fashion, which is used by timing pattern for identifying the central coordinate of each cell. Its main purpose is, adjusting the central coordination of the data cell when the symbol is distorted. The quiet zone enables easy spotting of the code from the image by the CCD sensor.

Error Correction in QR Codes is grounded on Reed-Solomon Codes, which is a particular form of BCH error correction codes. While creating a QR code, a user can choose an error level from the available four levels of error correction. Each level extends to a certain limit and are suitable for particular applications.

- L - 7%

- M - 15%
- Q - 25%
- H - 30%

The higher the error correction level the higher the number of code words available for correcting errors and hence the space available to store the data inside the code is low.

3.2.3 Scrambling

Image scrambling is a way which deals with securing the picture information by scrambling the image into an ambiguous organization. Image scrambling aims to mitigate security issues related to images. In image scrambling and descrambling, it is necessary to have simple algorithm to 'shuffle' the pixel values and reorder it to reveal the original. A pseudorandom sequence can be used to generate a scramble order. The amount of scrambling achieved determines the amount of distortion in the image. There are many ways to achieve scrambling in the images. Mostly scrambling approaches are grounded on Arnold Transform or on a combination of Arnold Transform and other techniques. Scrambling can also be achieved by employing random sequences grounded on chaos or pseudo random number generation grounded on parameters. The key based scrambling techniques are also reliable, where a key is generated which is shared by both parties to communicate. The main objective of image scrambling is to generate a non-intelligible image in order to prevent the understanding of the true content by human visual system or computer vision system.

3.4. LSB Transform

The Least Significant Bit technique is applied to imbed the bits of the secret message in a deterministic sequence, straight into the LSB (Least Significant Bit) plane of another image, referred as cover image. As the measure of the change is not much, varying the least significant bit does not lead to a human perceptible difference. LSB method comes with easy implementation and acceptable outputs. First, a proper cover image is chosen to hide the secret image. as bits of each pixel in the image are utilized in this method. A lossless compression format is utilized, to hold the hidden information during the transformations of a lossy compression algorithm.

A principle well known as least significant bit insertion is utilized to accomplish the digital image steganography. Color and appearance of the pixel are described by specific bytes contained in the pixel itself. The existence of a set number of bytes for every pixel depends on the resolution of the particular image. When the image is freed from least significant

bits, it can be considered as a slope of redundant bits that matches a black plus white star burst, when the image is freed from the least significant bits. In short, the bits which are not concerned with the integrity of the photograph are manipulated and replaced for the secure transfer of the message.

4. Proposed Methodology

The use of QR codes in steganography is not novel but the novelty of the proposed methodology lies in the utilization of QR codes for achieving security levels [1] in transmitting the secret message. The proposed methodology suggests a combination of strong encrypting algorithm and steganographic technique to make the communication of confidential information safe, secure and extremely hard to decode. It includes efficient encoding techniques in encrypting a secret message before encoding it in to the QR codes. The QR code is then scrambled to achieve another security level. Standard embedding technique is employed for embedding QR code in a suitable cover image. The cover image is then transferred securely for exchanging secret information, from which the information is retrieved using proposed retrieval procedure at the receiver's side.

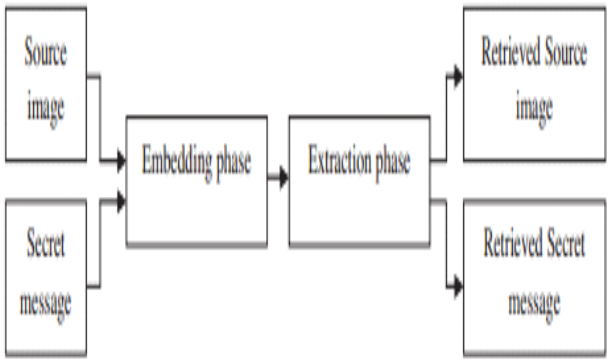


Fig.3. Framework for proposed methodology.

The proposed methodology is categorized into four modules at both sender's side as well as receiver's side.

4.1 SENDER'S SIDE

The procedure at the sender's side includes four modules. They are

- Encryption
- Encoding
- Scrambling
- Embedding

Every module imparts a layer of security to the secret message to be transmitted. The final stego image is the result of enhanced security imparted to the steganography. A detailed description of each module is given below.

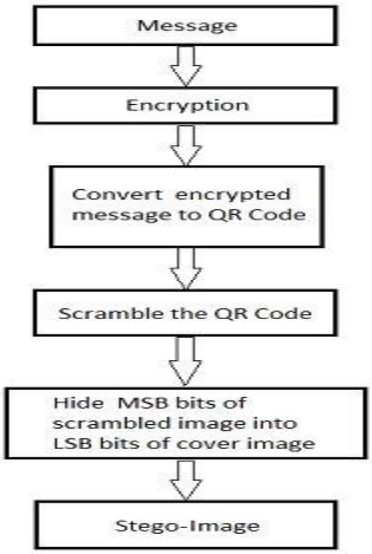


Fig.4 Block diagram for sender's side procedure.

4.1.1. Encryption

The first module at the sender's side deals with the encryption of the secret message. Here the message which has to be conveyed is encrypted using an efficient encryption technique. In the proposed methodology, AES-128 key encryption technique is chosen for this purpose. The technique takes a 16 character password (8 bits per character) for encrypting the message.

The encrypted message, in UTF-8 format is converted in to base64 format to make it compatible for further processing, which is then written in to file and stored for further processing.

4.1.2. Encoding

The second module includes the encoding of the encrypted text (base64 format) in to QR code. For the encrypted text written in to the file, a unique QR code is generated. The QR encoding is unique and serves well for hiding the message. QR codes come with large encoding space. It can be transferred easily and has error correction capabilities.

4.1.3. Scrambling:

Scrambling includes realignment of the pixels of QR code to make it deceivable and also it make QR code elusive for human eyes.

The main purpose of this manipulation is to prevent QR codes from getting scanned by QR scanners. A scramble order is generated at random and the RGB values are extracted for the QR code and both are stored. The random scramble order

is applied on the RGB values extracted from the image and the same is communicated to the receiver's side. The resulting values of the scramble operation are reshaped according to the image size (Rows *Columns). Finally a scrambled image is generated concatenating the three RGB values and then generating an image from it.

Algorithm 1: Scrambling

Step 1: Read the image

Step 2: Generate a random scramble order

Step 3: Save the scramble order and the size of the image

Step 4: Extract the RGB values of the image

Step 5: Apply scramble order on RGB values

Step 6: Reshape RGB values according to the image size

Step 7: Concatenate the RGB values

4.1.4. Embedding:

Embedding refers to embedding the secret image which in this case is altered QR code in to a cover image. The implanting operation is performed to get a stego picture, which is then transmitted safely to the beneficiary's side. In this strategy the bits of the message are specifically installed into the minimum huge bit plane of the spread picture in a deterministic arrangement.

Regulating the minimum noteworthy bits in the spread picture does not influence the presence of the picture much as the abundance of the change is little..

The insertion techniques available in LSB method are 1-bit insertion, 2-bit insertion, 3-bit insertion and 4-bit insertion. For embedding the QR image into the cover image a 4 bit insertion is utilized.

Algorithm 2: LSB embedding

Step 1: Generate stream of binary bits from the cover image.

Step 2: Bits of each pixel ANDed with 240(11110000).

Step 3: **Right shift by 4 bits on the bits of pixel in the scrambled image.**

Step 4: Value of bits of two is ORed.

Step 5: **Save the new image.**

4.2 Receiver's Side:

The procedure at the receiver's side also includes four modules, which decodes the security levels. They are

1. Retrieval

2. Descrambling

3. Scanning

4. Decrypting

At the end of the process the secret message is rendered to the receiver accurately. Each process reverses the effect imparted at the sender's side.

4.2.1. Retrieval

The stego image is processed to retrieve the hidden image from the cover image. The retrieved image is the scrambled QR code here. The quality of retrieved image is not much affected and is sufficient enough to retrieve the hidden content from it.

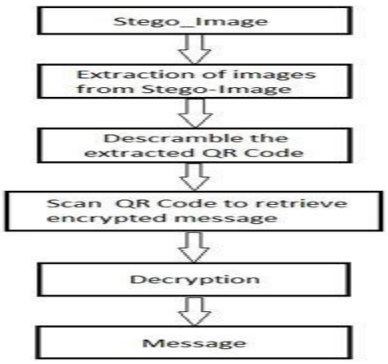


Fig.5 Block diagram of receiver's side procedure.

Algorithm 3: Retrieving the embedded image

Step 1: Generate the stream of binary bits for the received image.

Step 2: Perform reverse operation to extract cover image.

Step 3: Left shift by 4 bits on the received image

Step 4: Retain the scrambled image with acceptable data loss.

4.2.2. Descrambling

The retrieved image, which is scrambled, is then descrambled using the descrambling technique and the received random generated sequence. The scrambled image is loaded and then a reverse order is generated from the file containing the

scrambling order information. The RGB matrix values are then arranged according to the newly generated reverse order. The required QR code image can then be generated by concatenating these values to form an image. The coding specifications for descrambling are the same as scrambling. All the operations are inverted in the process.

Algorithm 4: Descrambling

Step 1: Load the image.

Step2: Generate the reverse order.

Step3: Arrange the RGB matrix values.

Step4: Concatenate RGB values.

Step5: Obtain the descrambled image.

4.2.3. Scanning

The descrambled QR code is then scanned to get the encoded information, which is here the secret message in encrypted form. The scanning can be easily carried out, with the help of mobile apps. They are handy and can be easily downloaded and installed. They use the mobile's built in camera and a decoding program to scan and display the content of the encoded QR code.

4.2.4 Decryption

The final phase, Decryption involves decrypting the encrypting the encrypted message, to retrieve the message. It takes the same 16 character key, which is used to encrypt the message at the sender's side. The retrieved message is then delivered to the person concerned

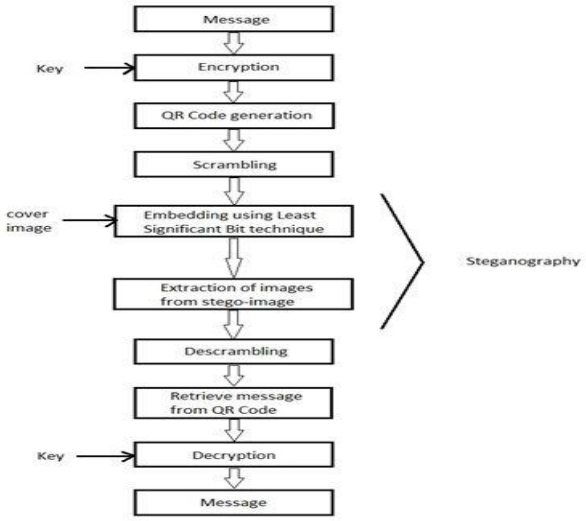


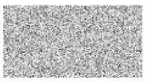
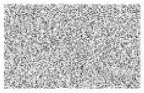
Fig.6. Block diagram of the proposed methodology.

5. Results and Discussion

The security for steganography has been enhanced by the proposed scheme. The secret message can be transferred successfully with four levels of security applied to it. The security is enhanced by employing Encryption technique and utilizing the QR code. The encrypted message is hard to break and the QR code is secured by applying scrambling technique to it. The stego image generated and the cover image are similar with no human perceptible errors. The **Table2** and Table-3 show the outputs and images of the proposed methodology. It is evident from the tabulated results that the stego image generated is similar to the cover image and cannot be identified by a human eye. Also it can be proved from the tabulated MSE (Mean Square Error) and RMSE (Root Mean Square Error) values of the selected images in Table1 that the stego images do not deviate much from the cover image after applying the proposed methodology and are reliable for transferring the information across network.

Table 1. Mean Square Error and Root Mean Square Error values of the selected images.

IMAGE NO	MSE	RMSE
1	**0.928**	**0.9612**
2	**0.9338**	**0.9663**
3	**0.8321**	**0.9122**
4	**0.8660**	**0.9306**
5	**0.6420**	**0.8012**

IMAGE NO	QR CODE	SCRAMBLED IMAGE	STEGO IMAGE
1			
2			
3			
4			
5			

6. Conclusion

The proposed method suggests a combination of strong encrypting algorithm and steganographic technique to make the communication of confidential information safe, secure and extremely hard to decode. It includes an efficient encoding technique in encrypting a secret message before encoding it in to a QR code. This encoded image is scrambled to achieve another security level. The scrambled QR code is finally embedded in a suitable cover image. The cover image is then transferred securely for exchanging secret information, from which the information is retrieved through the decoding process at the receiver's side. This methodology provides a four level security for the secret message to be transferred. It includes the combination of cryptography and steganography to achieve efficient results. The use of scrambling technique further distorts the QR code making it reliable for encoding important information. Scrambling protects it from any unauthorized scans. Finally, Embedding yields a standard stego image. This technique can find application in communicating confidential information in banking, defense, educational, e-Business sectors. The technique can be further improved to achieve required level of security by adopting various necessary techniques to suit the requirements.

7. References

1. Damir Omerasevic, Narcis Behlilovic, Sasa Mrdovic" An Implementation of Secure Key Exchange by Using QR Codes", 56th International Symposium ELMAR-2014, 10-12 September 2014, Zadar, Croatia.
2. Yin-Jen Chiang, Pei-Yu Lin, Ran-Zan Wang, Yi-Hui Chen," Blind QR Code Steganographic Approach Based upon Error Correction Capability", KSII Transactions on Internet and Information Systems vol. 7, no. 10, Oct. 2013
3. Ji-Hong Chen, Wen-Yuan Chen and Chin-Hsing Chen" Identification Recovery Scheme using Quick Response(QR) Code and Watermarking Technique", Applied Mathematics and Information Sciences, An International Journal, 8, No. 2, 585-596 (2014).
4. Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar Weippl "QR Code Security", 2014.
5. S. Uma Maheswari, D. Jude Hemanth "Frequency domain QR code based image steganography using Fresnelet transform", Int. J. Electron. Commun. (AEÜ) 69 (2015) 539–544.
6. Somdip Dey, Kalyan Mandal, Joyshree Nath, Asoke Nath "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm", I.J.Modern Education and Computer Science, 2012, 6, 59-67 .

7. Wai Wai Zin," Message Embedding In PNG File Using LSB Steganographic Technique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

8. Kaustubh Choudhary," Properties of Images in LSB Plane", IOSR Journal of Computer Engineering (IOSRJCE), 2278-0661 Volume 3, Issue 5 (July-Aug. 2012), PP 08-16.

9. Salim M. Wadi, Nasharuddin Zainal " Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption", 4th International Conference on Electrical Engineering and Informatics, ICEEI 2013.

10. B. Padmavathi, S. Ranjitha Kumari" A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

11. Shashi Mehrotra Seth, Rajan Mishra "Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol 2, Issue 2, June 2011.