

Robust and Secured Image Steganography using LSB and Encryption with QR Code

Hazim Noman Abed

Computer Science Department, College of Science, University of Diyala, Iraq

Hazim_numan@ sciences.uodiyala.edu.iq

Recived : 24\5\2017

Revised : 14\6\2017

Accepted : 18\6\2017

Abstract

The great development obtained with digital communication system depends on the improvement of the amount and security of transmitting information, the secrecy of data transmitted becomes a main subject for the researcher. Cryptography and Steganography play a major role for secured data transfer. In this research, the cryptography and steganography method was proposed for information security. In cryptography, the encrypted message was obtained by XOR the secret message with QR code. While, in Steganography the encrypted message was embedded inside cover image using LSB technique. The new approach in this research is use of the QR technique as well as the encrypted message was hidden in places selected using the bat algorithm. Secret message with different sizes was tested with many cover imagesto verify the efficiency of the proposed method. In the end, to measure the quality of cover image after the process of embedding, a group of standard parameters has adopted. The results of parameters showed the proposed method has the highest security and integrity.

Keyword: Steganography, Cryptography, Bat algorithm, QR code.

1. Introduction

The great development obtained with digital communication system depends on the improvement of the amount and security of transmitting information, and with the growing of networks, the secrecy of data transmitted over this network becomes a main subject for the researcher and network engineers. Multi techniques of

encryption are applied on transmitted data specifically for multimedia application to provide protection and security. The most wide multimedia application used in digital communication system is the digital image which requires protection to verify the privacy of this application

and prevent the illegally gained. Encryption is the key of transmitting data securely over open networks by achieving the protection for transmitting digital image which converted from the original form to another form [1]. Data security keeps the privacy for the transmitted data, secure transmission of data prevents any unauthorized person from obtaining the data such as personal e-mail, contact lists and other important data. According to the demand of data security, several techniques and algorithm have been proposed for data encryption, these algorithms stand to protect the content of transmitted digital image and provide privacy for transmitted data. The levels of security provided by the algorithm depends on the features of transmitted image and the capability of the applied algorithm. There are different techniques and algorithm for encryption, each one is comfortable for certain transmitted data, such as image, text, and audio etc [2].

2. Steganography

With the growing of demand of data transmission especially for internet application, the factor of security has been a rise for the transmitted information, which consider the important factor for internet application. The techniques of cryptography are created for the information security, several techniques and methods are developed to encrypt and decrypt the transmitted information to maintain the security of messages. Unfortunately it is sometimes not enough to keep the contents of a message secret. The process of Hiding the information inside the image and text called steganography [3].

Steganography provides a good security when combined with the cryptography, and delivers better confidentiality and security. Steganography is the art of communicating in a way which conceal the existence of the communication [4]. The main four categories of file formats used for steganography like image, text, audio and video protocol. Historically, the most important method is hiding information in the text, the simple method is to hide securely message within every n^{th} Letter of word of a text message [5]. Using digital files with text steganography is not common, since the text file has a little data redundancy. Digital images amount has been increased with the application of the internet and large amount of redundancy bit is presented with digital image, images are the most popular cover objects for steganography. Figure (1) shows the steganography encoding and decoding[4].

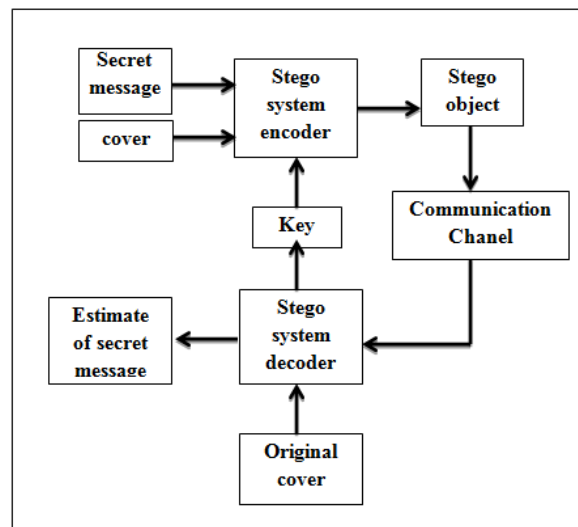


Figure (1): Steganography Encoding and Decoding[4].

3. Encryption and Decryption

The process of encoding transmitted information from its original format to another format is called encryption, this process is carried out to prevent any unauthorized person from reading the message. Many encryption algorithms are used in the encryption scheme to encrypt the message or transmitted information, turning it into ciphered text (ibid). this is usually carried out using an encryption key, which explain how the data is to be encoded. The ciphered text is undetermined for the enemy or any unauthorized person, on the other hand the authorized person has ability to read and decipher the text with the help of an algorithm designed for decoding, which is usually need the secret decryption key, that the invaders do not have access to. For technical purposes, an encryption scheme usually requires a key-generation algorithm to randomly produce keys[6].

4. QR Code

The most common type of scanned code used at checkouts around the area of the country holds a limited amount of information, on the contrary; barcode can hold a huge amount of information and one type of the barcode is QR code which has great response. As a reference to the speed at which the large amounts of information they contain can be decoded by scanners, the QR stands for quick response. QR code was invented in 1994, initially used in Japan for tracking shipping. QR is a two dimension barcode which represents the brand of type for matrix barcode. Several standards of QR encoding modes are used, such as (numeric, byte/binary, alphanumeric and kanji), used to store data efficiently. A QR code is involving of the black square modules organized in a square grid on a white background. Camera and scanner are devices used to read the QR code and then process

the code by applying an RS code (Reed-Solomon codes) for error detection and correction to interpret the code appropriately. The QR Code's is designed uniquely which gives it many unique advantages, such as; Small size, Fast, High-capacity data storage, omnidirectional scanning, Error correction[7].

5. Bat Algorithm

In 2010; Xin-She Yang develop the Bats algorithm, which has been applied for image processing application. Bats algorithm depends on the echolocation behavior of micro Bats which is represent main aspect of the algorithm. Bats Algorithm is the first algorithm of its kind in the context of computational and optimization intelligence due to its use frequency adjusting. Each Bats are encrypted with a location x'_i and a velocity v'_i , at iteration t , in a d -dimensional solution space or search. The location can be represented as a solution vector to an interesting problem. In between the n Bats in the population, the best of current solution x_* found so far can be archived through the iterative search process [8].

The mathematical equations for updating the velocities v'_i and locations x'_i depended on the main paper by Yang [9] can be written as:

$$f_i = f_{min} + (f_{max} - f_{min})\beta, \quad (1)$$

$$v'_i = v_i^{t-1} + (x_i^{t-1} - x_*)ff_i, \quad (2)$$

$$x'_i = x_i^{t-1} + v'_i, \quad (3)$$

Where $\beta \in [0, 1]$ is a random vector derived from a uniform distribution.

In addition to, the pulse emission rates and loudness can be diverse during the iterations. Simplicity, the next equations can be used for varying the pulse emission rates and loudness [10]:

$$A_i^{t+1} = \alpha A_i^t, \quad (4)$$

$$r_i^{t+1} = r_i^0 [1 - \exp(-\gamma t)], \quad (5)$$

Where $0 < \alpha < 1$ and $\gamma > 0$ are constants.

6. Related Work

Through many centuries, many studies present large efforts in data encryption and decryption using different techniques. Most of these studies used digital images to transmit the secure image via network. Many studies have been conducted in area of hiding information inside image using variant methods and techniques. As well as Steganography, Cryptography techniques, QR can also be used in the process of communication protection. Rani & Euphrasia proposed a unique technique for data security using QR codes and steganography. A message encrypted in a QR code can be read easily by any QR code scanner. But since the proposed technique incorporates steganography, it enhances the confidentiality and security [11]. Dey and colleagues introduced a new data-hiding algorithm, where a secret message is encrypted with combined cryptographic method and then hide the encrypted data in a QR Code [12]. Hajduk and et al proposed image steganography tool by using LDWT and QR coding. Upgrading of security was achieved via AES ciphering of QR code. The advantage of the method is compression of the module size in the QR code before embedding process [13]. Sharma and Sejwar presented another implanting calculation for QR Code Image Steganography and Text Hiding, which is based on 3-discrete wavelet transform (DWT) and enhanced RSA algorithm. Firstly, enter the text message and choose four random numbers for RSA encryption. Next, take four pictures: one is cover image and another is secret image. In the process of embedding, we split RGB image into three planes: Red, Green and Blue. In this work, embed multiple color secret images into a single cover image for providing security. Finally, encrypted text message is hidden in an embedded picture using the least significant bit (LSB) [14]. All the above methods are reviewed

and a new method is proposed in this research for secret data communication by integrating the encryption text file with steganography technique. Encrypted text file will be produced by XOR the original text file with QR code then embedding using LSB technique.

7. Proposed Method

Sometimes hiding a file inside an image can be exposed to many threats that pose a risk to the files to be hidden. In order to preserve the confidentiality of this information and prevent it from being exposed to any threat that may lead to its disclosure, a new method has been proposed in this search is the XOR secret message with QR code to configure an encrypted message and then embedded it in a cover image to get a stego image. Embedded the encrypted message in the cover image by LSB technology while hiding places is chosen by the bat algorithm through which the best places to hide are selected. The proposed method encompasses an encoding process at the sender and a decoding process at the receiver. Figure (2) shows the process of the proposed method.

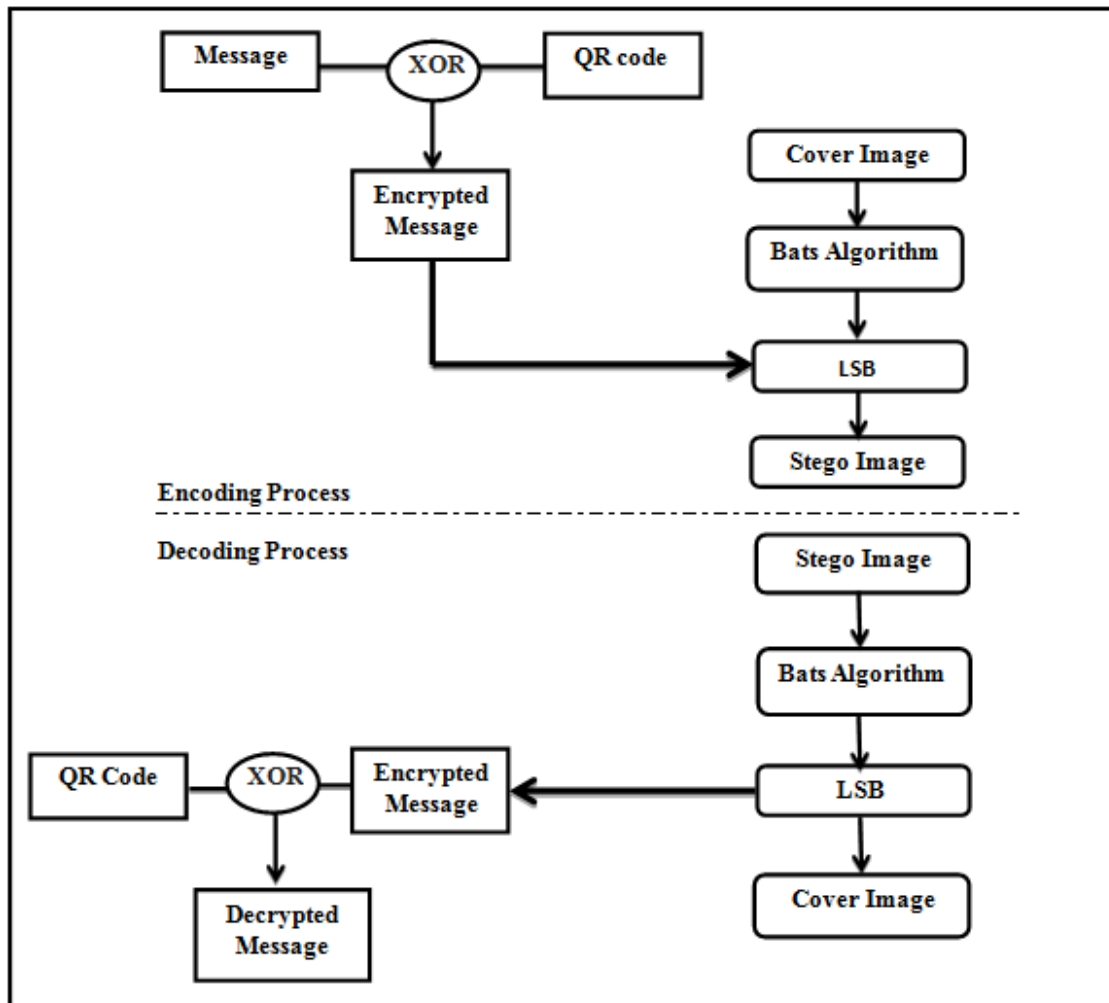


Figure2: Architecture of Proposed Method

7.1 Encryption and Embedding algorithm

The algorithm for encryption and the embedding process is as follows:

Input:

Secret message : Different size (400-1000)byte

QR: with size(200*200)

Cover Image: BMP image with different size to be cover image

Output: Stego Image

Step1: Generate QR code.

Step2: Load secretmessage.

Step3: Convert QR code and secret message into a matrix.

Step4: XOR of resultant matrix from step3 to obtain the encrypted message.

Step5: Select cover image.

Step6: Extract the best point of applying bat algorithm.

Step7: Embedding encrypted message by LSB to get the stego image.

7.2 Extraction Process algorithm

The algorithm for decrypted and the extraction process is as follows:

Input: Stego Image.

Output: Decrypted secret message ,QR and Cover Image.

Step1: Load Stego Image.

Step2: Extract best point in the stego image by applying bat algorithm.

Step3: Extract the encrypted message using LSB.

Step4: Result from step3 will be encrypted message and cover image.

Step5: XOR again to get the decrypted message.

8. Experimental Results

In the proposed system the advantages of Steganography and the power of QR code are

combined to improve data security. In this system, the encrypted message in this system is obtained through the XOR original message with QR code. After that, the encrypted message embedded in the BMP cover image using LSB. The algorithm has been tested through different samples of image with different sizes, while the text message sizes ranged from (400-1000 byte). QR code was generated by [15] with size 200 * 200. The style and the intricacy of the QR code vary based on the size of the secret message. The intricacy of the QR style will increase when a large amount of data is encrypted. Figure 3 shows the results of encoding process.


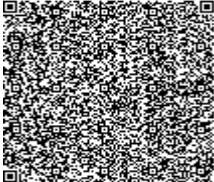



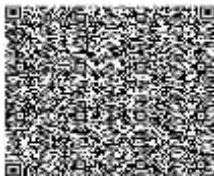



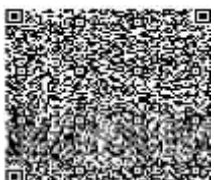






Cover image	Text Message Size(Byte)	QR Code (200*200)	Bat image	Stego Image
 512*512	1000			
 256*256	800			
 128*128	600			
 64*64	400			

Figure 3: Results of Encoding Process

9. Performance Evaluation

In order to determine the quality of the method used for information hiding, this research adopted a number of Standard parameters for the purpose of measuring the quality of images resulting from the system which are:

Mean-Squared Error(MSE): is to estimate or measures the mean of the squares of the error betweenstego image and the original image [1].

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [I_1(i,j) - I_2(i,j)]^2}{M.N}$$

Peak Signal-to-Noise Ratio (PSNR): This ratio is often used as a quality measurement the difference between the original and the stego image[1].

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

Normalization Correlation (NC):is Standard parameters used to test the quality of the extracted cover image by measure the similarity between the cover image and the extracted one. Table 2 illustrates the results of MSE, PSNR and NC with different size of the cover image and text file [1].

$$NC = \frac{\sum_{i=1}^X \sum_{j=1}^Y (W_{originalij} \times W_{recoveredij})}{\sum_{i=1}^X \sum_{j=1}^Y W_{originalij}^2}$$

Cover image size	Text file size	PSNR	MSE	NC
512*512	64 KB	81.6013	0.9897	1
256*256	64 KB	79.1692	0.9563	0.9789
128*128	64 KB	76.9845	0.9212	0.9779
64*64	64 KB	73.6724	0.8974	0.9687

Table 2: Results MSE, PSNR and NC

10. Conclusion

Cryptography and Steganography are the two main parts in information security. In this paper, a new method is proposed for data security using two phases cryptography and steganography. In cryptography, the encrypted message was produced by XOR the secret message with QR code. While, insteganography the embedded process was achieved by using LSB technique and the embedded location is chosen by applying bats algorithm on the cover image. Many standards are applied to prove the quality of the proposed method. As the result, experimental results showed that this proposed method delivers good performance in regards to invisibility and robustness.

References

[1] Badr, A. M., Talal, M. L., & Mahmood, G. S. A. (2015). Novel Digital watermarking technique based on STD (standard division). International Journal of Scientific & Engineering Research. Vol. 6. No. 11. pp 98-102.

[2] Bani Younes, M. A., & Jantan, A. (2008). Image encryption using block based transformation algorithm. International journal of computer sciences, 35:1, IJCS_35_1_03. pp(407- 415).

[3] Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In ISSA (pp. 1-11).

[4] Sheth, R. K., & Tank, R. M. (2015). ImageSteganographyTechniques. International Journal Of Computer Engineering And Sciences, 1(2), 10-15.

[5] Krenn, R. (2004). Steganography and steganalysis.

- [6] Sethi, P., & Kapoor, V. (2016). A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. *Procedia Computer Science*, 87, 61-66.
- [7] Dey, S., Agarwal, S., & Nath, A. (2013, April). Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System. In *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*(pp. 512-517). IEEE.
- [8] Yang, X. S. (2010). A new metaheuristic Bats-inspired algorithm. In *Nature inspired cooperative strategies for optimization (NISCO 2010)* (pp. 65-74). Springer Berlin Heidelberg.
- [9] Yang, X. S., (2011). Bat algorithm for multi-objective optimisation, *Int. J. Bio- Inspired Computation*, Vol. 3, No. 5, pp. 267–274.
- [10] Xing, B., & Gao, W. J. (2014). Bats inspired algorithms. In *Innovative Computational Intelligence: A Rough Guide to 134 Clever Algorithms* (pp. 39-44). Springer International Publishing
- [11] Rani, M. M. S., & Rosemary Euphrasia, K. (2016). Data Security Through QR Code Encryption and Steganography. *Advanced Computing: An International Journal (ACIJ)*, 7(1/2), 1-7.
- [12] Dey, A. S., Nath, B. J., & Nath, C. A. (2012, January). A New Technique to Hide Encrypted Data in QR Codes (TM). In *Proceedings on the International Conference on Internet Computing (ICOMP)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- [13] Hajduk, V., Broda, M., Kováč, O., & Levický, D. (2016, April). Image steganography with using QR code and cryptography. In *Radioelektronika (RADIOELEKTRONIKA), 2016 26th International Conference* (pp. 350-353). IEEE.
- [14] Sharma, S., & Sejwar, V. (2016). QR Code Steganography for Multiple Image and Text Hiding using Improved RSA-3DWT Algorithm. *International Journal of Security and Its Applications*, 10(7), 393-406.
- [15] QR Code generated by <https://www.the-qrcode-generator.com/>

صورة قوية وامينة بواسطة الاخفاء باستخدام تقنية البت الاقل اهمية والتشفير مع رمز الاستجابة السريعة

حازم نومان عبد

قسم علوم الحاسوب، كلية العلوم، جامعة ديالى، العراق

Hazim_numan@sciences.uodiyala.edu.iq

المستخلص :

التطور الكبير في انظمة الاتصالات الرقمية يتوقف بشكل كبير على تحسين نقل وتامين المعلومات. وعليه فان امن البيانات اصبح محل اهتمام الكثير من الباحثين. التشفير وإخفاء تلعب دورا رئيسيا في الحفاظ على سرية البيانات بين المرسل والمستلم. في هذا البحث تم اقتراح طريقة جديدة لامن المعلومات تتضمن عملية تشفير وإخفاء. في عملية التشفير، تم الحصول على الرسالة المشفرة من خلال بوابة الاختيار الحصري أو بوابة اكس اور (XOR) للرسالة المراد تشفيرها مع رمز الاستجابة السريع (QR Code). بينما، في عملية التضمين فان الرسالة المشفرة تم اخفائها في صورة باستخدام تقنية البت الاقل اهمية (LSB). بالاضافة الى ذلك فان مواقع الاخفاء تم اختيارها بالاعتماد على خوارزمية الخفافيش. العديد من الصور والنصوص في مختلف الاحجام تم اختبارها للتحقق من كفاءه الطريقة المقترحة. في النهاية، لقياس جوده صورته الغلاف بعد عمليه الاخفاء تم الاعتماد على مجموعه من المعايير القياسية والتي وأظهرت ان الطريقة المقترحة لديها اعلي درجات الأمان والسلامة.