Indian Journal of Research Communication Engineering (IJRCE)
Vol.2.No.1 2014 pp 7-11.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

HIGHLY SECURE SECRET OR CODE TRANSFORM BY COMBINATION OF STEGANOGRAPHY & ENCRYPTION TECHNIQUE USING SOCKET COMMUNICATION

Harilakshmi.M[1] and Arul flora .T.G [2]
Department of Electronics and Communication Engineering,
K.C.G. College of Technology,
Karapakkam, Chennai, Tamil Nadu, India – 600097.
harilakshmir@gmail.com and arulflora@kcgcollege.com

ABSTRACT

Image Steganography is the art of hiding the secret data into a cover image. The proposed method presents a steganographic method which is based on DWT-Arnold method, where DWT is used to convert the cover image into frequency domain and Arnold method is used for encoding the QR code of secret message. The quality of the image can be maintained by preserving the low frequency coefficients since most of the information lies in that area. QR code payload guides the alteration of the ARNOLD values of DWT block. This method can be used by smart phones, smart video-cameras, email or LAN connection for business and consumer applications. This method has high PSNR and SSIM and survived chi-square test with 100% message recovery. However satisfactory security will be maintained as the QR code is difficult to decode.

Keywords: Cryptography, QR Code generation, ARNOLD Encryption, DWT, Digital Watermarking.

1. INTRODUCTION

Multimedia content and electronic information exchanges systems are rapidly growing in the industrial electronics area. Information confidentiality of such content is of a high significance. Cryptography provides the necessary method for securing the information; however, studies prove that it can be broken by the steady progress of the skill. Therefore, considering robust and cheaper alternatives are unavoidable.

One possible practical alternative is digital Steganography. Steganography is an art of hiding secret data in an innocent looking container called cover data. This cover data may be any digital media such as digital image, audio, movie file etc. Usually the embedded secret data is called payload. Once the payload has been embedded into a cover media it may be transmitted to the receiver or posted in public place from where intended receiver can download it. Multimedia message passing in cell and iPhone are getting more popular day by day and sending secret message with steno-image would be an interesting addition [3]. In the proposed Steganographic method, the DWT- Haar transform has become an important feature in order not only to embed the data securely, but also retrieve it based on the parametric key. A DWT based image Steganography scheme where they embed their secret message in the high frequency components of the DWT using 2 LSB substitutions with wavelet coefficients of LH, HL, and HH Sub bands. They obtained steno-image [4].

2. STEGANOGRAPHY

The Steganography looked up on 1995. Steganography is the art of transmitting data through apparently harmless carriers in an effort to conceal the existence of the data, the word Steganography exactly means covered or hiding writing as derived from Greek. Steganography is mainly used for security.

It is not proposed to replace cryptography but enhancement it. Hiding a message with Steganography methods reduces the message detection. If the message is also encrypted then it provides another layer of protection. Therefore, some Steganographic methods combine traditional

Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover. Recently this technique has become important in a number of applications. For example, digital video, audio, and images are gradually more embedded with invisible marks, which may contain hidden signatures or watermarks that helps to prevent illegal activities. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not clear. In this paper will address on the traditional and popular methods [5].

3. QUICK RESPONSE (QR) CODE

QR (Quick Response) Code is a 2-Dimensional barcode that can store different kinds of information such as a link, plain text, SMS text message, addresses, URLs (Uniform Resource Locator), email, phone numbers or contact information. QR Codes was introduced in Japan by Denso Wave in 1994 to track automobile parts but they become popular when they were used as an advertising medium to distribute additional information to the users. When a user scans a QR Code with his/her Smartphone camera using the suitable QR Code software reader, he/she can reach the additional information. Thus QR Codes can be described as paper-based hyperlinks [2]. Moreover, QR code error correction capability makes it ideal for Steganography. For different version of QR code, there are different module configurations where modules refer to the black and white dots which construct the QR Code. The largest standard QR Code is V-40 symbol, which is 177x177 modules in size and can hold up to 4296 characters of alphanumeric data [3].

4. ARNOLD TRANSFORM

Arnold transform, also known as cat map transform, is only suitable for encrypting N×N images. It is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{matrix} 1 & 1 \\ 1 & 2 \end{matrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N \qquad (1)$$

Where (x, y) and (x', y') are the pixel coordinates of the original image and the encrypted image respectively. Let **A** denote the left matrix in the right part of equation (1**),** $\mathbf{I}(x, y)$ and $\mathbf{I}(x', y')^{(n)}$ represent pixels in the original image and the encrypted image obtained by performing Arnold transform n times, respectively. Thus, image encryption using n times Arnold transforms can be written as

$$\mathbf{I}(x', y')^{(k)} = \mathbf{A}\,\mathbf{I}(x, y)^{(k-1)} \pmod N \qquad (2)$$

Where k = 1, 2… n, and $\mathbf{I}(x', y')(0) = \mathbf{I}(x, y)$.

Obviously, one can multiply the inverse matrix of A at each side of equation (2) to obtain $\mathbf{I}(x, y)^{(k-1)}$. In other words, the encrypted image can be decrypted by iteratively calculating the following formula n times.

$$\mathbf{J}(x, y)^{(k)} = \mathbf{A}^{-1}\mathbf{J}(x', y')^{(k-1)} \pmod N \qquad (3)$$

Where $\mathbf{J}(x', y')^{(0)}$ is a pixel of the encrypted image, and $\mathbf{J}(x, y)^{(k)}$ is a decrypted pixel by performing k iterations [6].

5. Haar-DWT

[4]The frequency domain transform applied in this paper is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Fig. 1. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

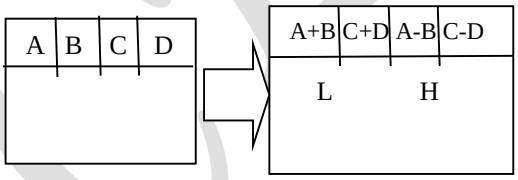

Figure. 1 The horizontal operation on the first row

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference in the bottom as illustrated in Fig. 2. Repeat this operation until all the columns are processed. Finally obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

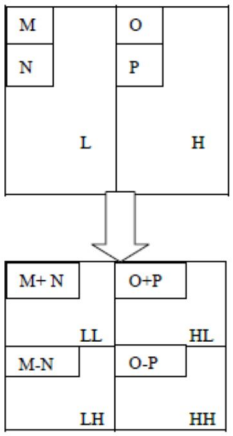

Figure. 2 The vertical operation

6. WATERMARKING OVERVIEW

The purpose of digital watermarking is to embed or insert a message into a signal in a secure and imperceptible manner and to detect the embedded information from a watermarked signal. A watermarked image may be attacked, such as JPEG compression, before it is available to the watermark detector. A block diagram of a typical watermarking system is as follows in Fig. 3. Although the techniques described can be applied to other medial fundamentals, here mainly focus on still images [1].

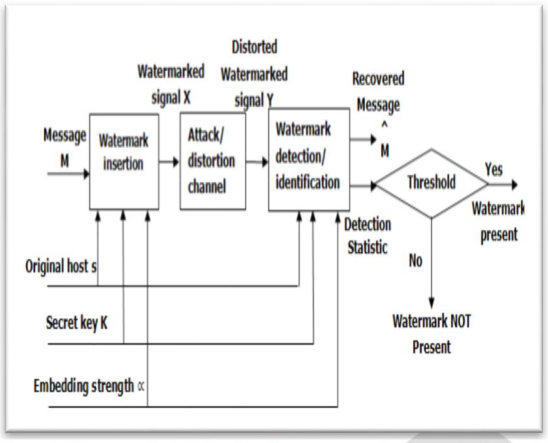

Figure. 3 A block diagram of a typical watermarking system

A. Watermark Embedding

Watermark embedding is hiding a message into an image by mapping the message to another signal and adding that signal to an image. That signal is also called the watermark as in fig.3. A watermark embedded accepts as inputs the host image S, secret key K, and message M and produces the watermarked signal X. The embedding key K is the secret that is necessary to detect the watermark and decode the message in the watermark. The embedding strength parameter α is a parameter to control the energy of the watermarked signal. As the signal strength of the watermark increases, usually the visibility of the watermark and the probability to detect or decode the watermark increases. A secret key K or key pair is used for watermark embedding and detection.

This key is analogous to the secret PN-sequences (chips) used in spread spectrum communications. Although, the size of the watermark key space has no direct impact on some properties of watermark such as fidelity and robustness, it plays an important role in the security of the system. The key space, that is the range of all possible values of the watermark keys, must be large enough to make exhaustive search attacks impossible [1].

Discrete Wavelet Transform (DWT) is used in the source compression standard JPEG 2000. This transform has been used in image watermarking. The reason for using DWT closely follows those for using DCT i.e. preventing watermark removal by JPEG 2000 lossy compression, reusing previous studies on source coding regarding the visibility of image degradations, and offering the possibility of embedding in the compressed domain. In addition to these criteria, the multiresolution aspect of wavelets is helpful in spreading the watermark in regions where the watermark is less visible than other regions [1].

7. PROPOSED METHOD

A novel DWT-ARNOLD based watermarking is presented. Here, a method for integrating cryptography and Steganography through image processing is described. In particular, a system which is able to perform Steganography and cryptography at the same time using images as cover objects for Steganography by DWT method and cryptography by Arnold method is presented. The block diagram is as in Fig. 4.

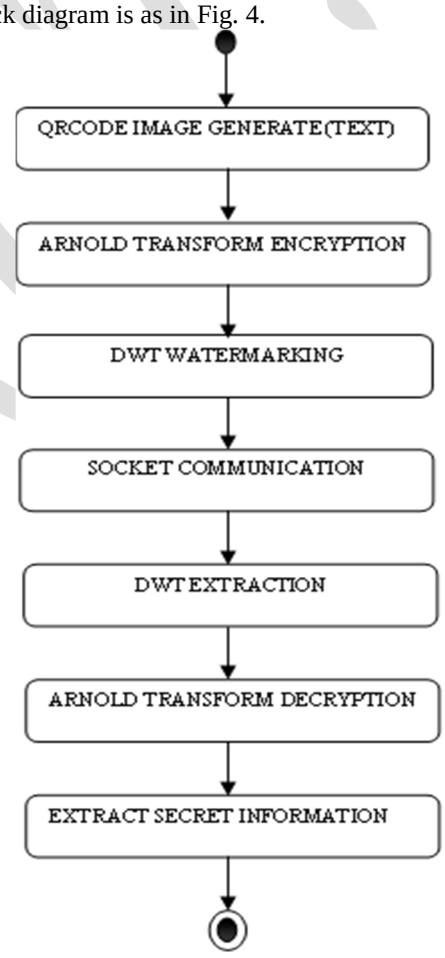

Figure. 4 Block Diagram of DWT-ARNOLD based Watermarking.

A. Watermarking Part:

Here a QR code generator is used to produce a payload (secret message) which is

converted to a one dimensional vector with a sequence of 1's and 0's. Then the QR code is encrypted by Arnold transform. Arnold transform is defined only for squares to use it in rectangles, firstly empty rows or columns are added to make the square which represents the iterations of the transform. In DWT transform, the image is divided into four corners, upper left corner of the original image, lower left corner of the vertical details, upper right corner of the horizontal details, lower right corner of the component of the original image detail (high frequency). Then the secret encrypted image is watermarked by each wavelet component. Finally by applying inverse wavelet transform the watermarked image is obtained.

***B. Extraction Process*:**

In the extraction process four components of the wavelet transform for the watermarked image are separated, the encrypted image is extracted and then the QR code will be extracted from encrypted image by applying inverse Arnold transform. Finally the secret message is extracted into a text file using a decoding process and finally the text is converted to an image.

The proposed method can be used in iterative manner, significance, if the exact payload cannot recover in the first time, re-execute the process on stego-image until obtain the payload.

8. SIMULATION RESULTS

In order to validate the image reliability, and Steganography method, we have performed extensive simulation with MATLAB 7.9 on image processing.

***A. Arnold Encryption*:**

In ARNOLD Encryption, first secret information is taken as input as in Fig. 5

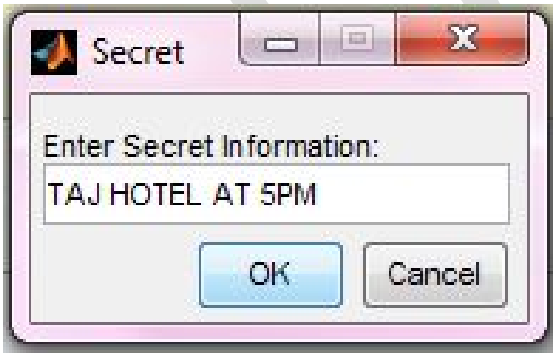

Figure. 5 Secret message

Then, by using QR Code generator the secret message was covered as follows in Fig. 6

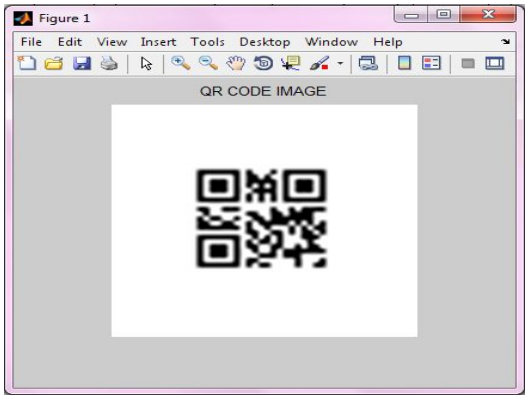

Figure. 6 QR Code image

To guard QR Code from the interpreter, it can be encrypted using ARNOLD Encryption. The Encrypted image covers as follows in Fig. 7

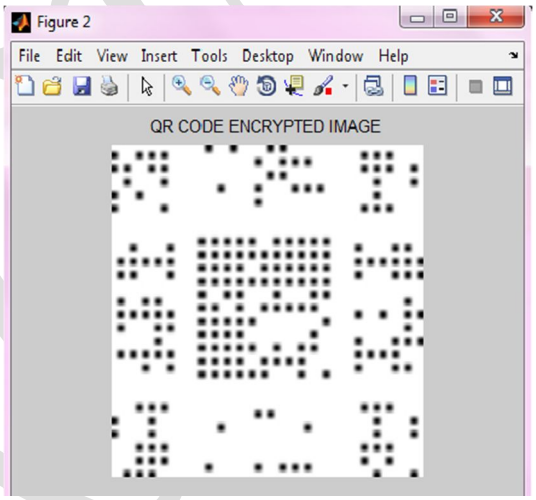

Figure. 7 Encrypted image

***B. DWT Watermarking*:**

Now, select the embedded image and cover it on the encrypted image using Steganography technique and apply watermarking on that embedded image as in Fig. 8

Figure.8 Watermarked image

***C. Extraction Process*:**

The watermarked image and encrypted image is extracted using the inverse ARNOLD transform and QR Code is extracted by that process. The secret information is recovered by decoding the QR Code generator as in Fig. 9

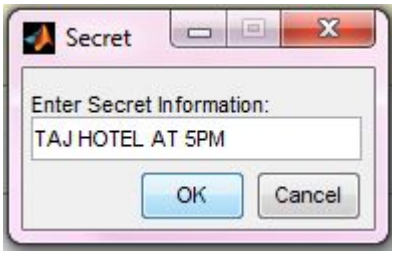

Figure.9 Extraction Secret message

9. CONCLUSION

Generally, Image stenography techniques will not provide security to cover image .In proposed technique; the cover image is secured by converting it into frequency domain by applying DWT. The QR code is generated to cover the secret text but it can be scanned by interrupter so, it is encrypted using the ARNOLD transform. Arnold transform is used to enhance security. From the transformed matrix a binary watermark was constructed and embedded within the image. The operation of embedding and extraction of cover image was done in high frequency domain of Discrete Wavelet Transform since small modifications in this domain are not perceived by human eyes. The high security is provided by well defined mathematical mapping using Arnold encryption. This method can be used by smart phones, smart video-cameras, e-mail and also through LAN connection for business and consumer applications.

REFERENCES

[1] Hyung Cook Kim, "Watermark and data hiding evaluation: the development of a statistical analysis framework: Thesis paper", Purdue University, and West Lafayette, Indiana, May 2006, in press.

[2] Ioannis Kapsalis "Security of QR Codes: Thesis paper", Norwegian university of science and Technology, June 2013, in press.

[3] Md. Wahedul Islam, Student Member, IEEE, and Saif alZahir, **"**A Novel QR Code Guided Image Stenographic Technique" IEEE International Conference on Consumer Electronics (ICCE), pp. 586-587, 11-14 Jan.2013,inpress.

[4] Po-Yueh Chen* and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, pp. 275-290, 10 Dec.2006, 4, 3,in press.

[5] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi**,** "Overview: Main Fundamentals for Steganography", journal of computing, volume 2, issue 3, March 2010, ISSN 2151-9617, in press. https://sites.google.com/site/journalofcomputing/158

[6] Zhenjun Tang and Xianquan Zhang, "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies", Journal of multimedia, vol. 6, no. 2, April 2011, in press.