International Journal of Engineering & Technology, 7 (2.29) (2018) 24-26

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Enhancing data transfer architecture using LSB steganography combined with reed solomon code

H. A. Jassim[1 *], Z. K. Taha [2], M. A. Alsaedi [3] and B.M. Albaker[4]

[1,2,3,4]Department of Network Engineering, College of engineering, Al-Iraqia University, Iraq
**Corresponding author E-mail: hebahaj1985@gmail.com*

Abstract

In this paper, new steganographic systems employing least significant bit technique and wavelet transform for embedding are proposed. These systems incorporate threshold level technique to enhance the performance of embedding scheme. Further, Forward error correcting code is used to improve the system performance. In the proposed system, the cover image is a gray image and the wavelet transform is applied directly. The secret image is coded using Reed Solomon code for preparing to embedding process. The locations of embedding are randomly selected according to pseudorandom number sequence. The combination between the ciphering process and steganography gives the system high level of security. This idea makes unauthorized retrieval is difficult. The simulation results show that the stego image is visually similar to the original one and does not have any suspension about embedded image. The extracted secret image is similar to the original secret image. The results indicate that using one-level Haar wavelet transform increases the capacity of the secret image that can be embedded. Hence, the steganographic goals are achieved in these systems. The proposed systems are simulated using MATLAB® software package.

Keywords: *Cryptography; Steganography; Reed Salomon code.*

1. Introduction

It is useful to start our research with the important of image security first. As it is well known in during the recent years, and due to the fast growth of image security, this topic is becoming an issue for developers. In this research, these techniques are used for more security and robustness: cryptography, steganography discrete wavelet, and Reed Solomon code. The cryptography is the process of encrypting and decrypting the data. The data is encrypted by the sender who wants to send to the receiver and decrypted on the other side [1]. The Greek word "steganos" meaning covered writing is the concept behind the theory of steganography. It is difficult to detect that a message has been sent. This type of ciphering called steganography, the old art of hiding messages sent which is unknowable. This method is gaining importance with every day because of its singular properties and those days are not far off when it would be used by armies of the world for secret message passing [2]. Discrete Wavelet Transform (DWT) is used also in combination with the embedding method to make the secret image more firm against offense from the interceptors that try to damage the communication between the sender and receiver [3]. Reed-Solomon (RS) codes are the most used error correcting codes. It has long been known how to decode them up to half the minimum distance. This gives a decoding algorithm that corrects a fraction 1−R /2 of errors in an RS code of rate R [4].

2. Wavelet transform

The discrete wavelet transform (DWT) analyzes the signal according to scale. DWT of a signal is calculated by multiply the signal by coefficients of Low pass filter and high pass filter. It spilts the signal into four subband namely LL, LH, HL and HH [5]. Figs.1 and 2 show the process. 2D-DWT is executed by applying 1D DWT on each row and then on each column.

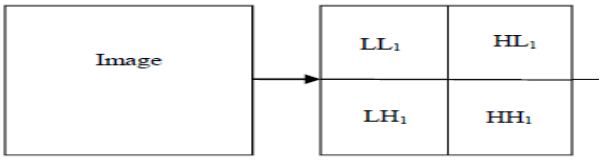

Fig.1. One level decomposition of 2D-DWT.

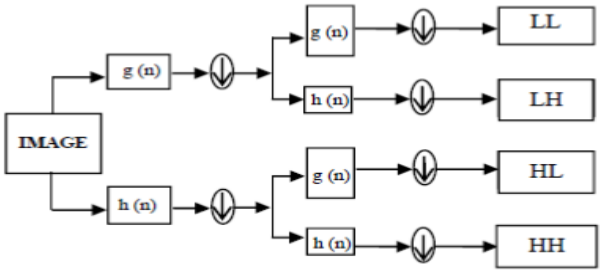

Fig.2. Steps for one level decomposition of 2D-DWT.

3. Security Methods

In these years of this information world, and as the investigation to the need for data protection becomes more pre-eminent. There is more interest in steganographic systems in set of programs. Steganography is a type of information hiding in a host data set, usu-

ally are image, audio signal, or video. Cryptography is used within steganography which adds an extra layer of security. In general, multimedia security is is accomplished by strategies used to ensure the interactive media content against unapproved get to or against unapproved circulation. These modes are mainly based on cryptography and they provide either communication security, or security against piracy. In many cases, when the multimedia is textual or static data, one can address it as an ordinary binary data and use the encryption mechanisms [5-6]. With the expansion of Internet technologies, digital media can be transmitted over the Internet. In any case, message transmissions over the Internet still have to face a wide range of security issues. Therefore, the way to protect secret messages during transmission becomes an fundamental issue for the Internet. Encryption methods scramble the secret message so that it cannot be understood. . However, it makes the message suspect enough to attract eavesdropper's attention. Hence, a new plan, called "steganography", arises to suppress the secret messages within some other ordinary media so that it cannot be spotted [7-8]. Steganography is the art and science of hidden communication. This is done through embedding information in another information, thus hiding the presence of the communicated information. One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh, who proposed a method, which resembles embedding into the LSBs (least significant bits) [8]. As a cover object, one can select image, audio or video file. Depending on the type of the cover object, definite technique is followed in order to obtain security.

4. The Proposed System Cryptography

Reed–Solomon (RS) codes are a class of linear, non-binary, cyclic block codes. Reed-Solomon codes are having a broadly scope of uses in wireless communications. Stego systems incorporating forward error correcting codes are proposed and described in this research. The proposed stego system, which hides a gray secret image into a gray cover image, selects a discrete wavelet transform domain technique for embedding to achieve robust systems. The fundamental concept of the suggested system is to use LSB scheme established on wavelet coefficient. In this method, the wavelet decomposition of the cover image and the private image are companied into a single image result. The proposed system uses new embedding mapping to enhance the performance of the systems.

Two groups of systems are proposed in this research. The proposed system contains coded systems that depend on coding the secret image by RS code. The coding is applied for the secret image and then the coded image is embedded using LSB scheme based on wavelet coefficient. The proposed systems can be used for steganographic applications that need these characteristics: more imperceptibility, high capacity, high fidelity, and more robustness. The general model of the proposed system is shown in Fig.3.

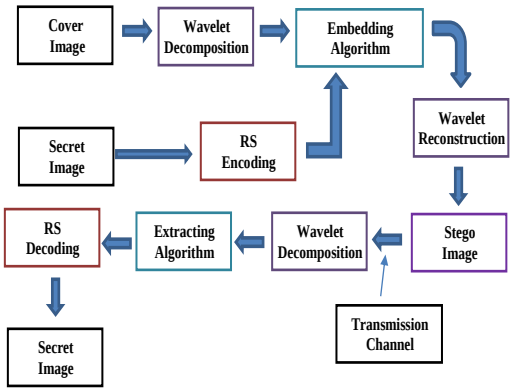

Fig.3: The block diagram of the proposal method.

Wavelet transform can analyze images into various sub bands. The aim of decomposition is to isolate the low frequency part, which has the most energy of the image, from the high frequency part. For wavelet transform, the cover image of size (512x512) pixels is decomposed up to level 1 using Haar filter as a basis function as shown in Fig.4.

(a) (b)

Fig.4: (a) Cover image (b) One level decomposition of 2D-DWT.

It is clear from Fig.4 that the energy is mostly concentrated in (LL) band and the other bands represent its reflection. Each sub band unless (LL) band is used to hide sub matrix from encrypted secret image as described in embedding procedure is shown in Fig.5.

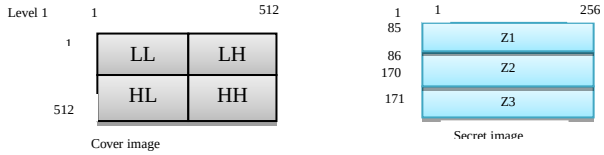

Fig.5: The embedding procedure

The selected secret image is channel coded using RS coded and product RS coded system. Each vector of ciphered image pixels is encoded by using outer RS encoder and then grouping the coded vectors into one coded image. This coded image has been transported to form the interleaved image. The interleaved image is encoded again by using the inner RS encoder. The results of this process are shown in Fig.6. In this figure, (a) is the selected secret image, (b) is the coded form of the obtained ciphered image and (c) is image after product RS coded.

(a) (b) (c)

Fig.6: (a) secret image (b) RS coded image (c) product RS coded image.

The coefficients obtained in the wavelet decomposition that used in the embedding are randomly selected according to a threshold, which is named embedding threshold. For each sub-band of secret block embedded in the cover, there is a key matrix which is produced by the pseudorandom (PN) sequence and contained the values of PN1. This matrix is transmitted through the secure communication channel, only the sender and the receiver know each matrix that is belonged to each sub-band block of the secret message.

The cover image is 256-gray scale because the used cover image is a gray image. If the condition of the threshold accepts the coefficient, then the coefficients can be extended into any number of bits. In this paper, the coefficients are extended into 24 bits. This extension is taken to compromise the accuracy and the complexity of extension.

When the threshold accepts the coefficient, the coefficient is extended to 24 bits. The 1st bit is the most significant bit (MSB) and

the 24th bit is the LSB. Then the 8 bits of the ciphered image are distributed over the 24 bits of the wavelet coefficient according to pseudo random (PN1). The reason of using PN1 is to embedding the 8 bits of the final ciphered image into best location of the host coefficient.

Experimentally, four best locations are used to embed the byte of the secret byte; these locations are taken between (bit14 - bit 21, bit15 - bit22, bit16 - bit 23, and bit17 - bit24). The decision of selection is taken from the value of the PN1. The PN1 has five decimal values (0, 1, 2, 3 and 4) that indicate the location used in the embedding process. This process continues until all bits of the sub-band block are hidden completely. The fifth value of PN1 (4) is to indicate that this coefficient does not content.

After the embedding process is completed, the wavelet coefficients are reconstructed. The same wavelet filter that is used in the wavelet decomposition must be used in the inverse wavelet, that used in this research.

Now, two objects must be transmitted to reconstruct the embedded images. First, the stego image is transmitted via a public communication channel. While the second, the stego keys that contain the manner of grouping, arranging, and sorting process, as well as the PN1 (key matrices) are transmitted via a secret channel. The wavelet filter, which is used in the sender, is also transmitted through the secure channel to the receiver.

The secret keys are used by the receiver terminal, hence the extraction process will be started. This is achieved by handling the stego image that received from public communication channel by the level 1 of wavelet decomposition and the same filter which is used in the sender. Then by using PN1, the coefficient that contains secret information is converted to 24 bits. The secret byte is extracted from the locations using PN1. Each byte is converted to its equal pixel value. This leads to extract the ciphered image. This image is deciphered firstly by rearrange the blocks in its location (large blocks and small blocks). Fig.7 shows the matching between secret image and extracted image.


Fig.7: (a) Secret image (b) Extracted image

5. Results and discussion

In this section, both peak signal to noise ratio and mean square error are calculated for each proposal methods. The results is shown in table 1

Table 1: Results of proposed methods

Methods	PSNR	COR	PSNR	COR
RS coded	inf	1	inf	0.9966

According to Table1. the results that are obtained from the objective tests prove that the coded system is more secure This means that high level of the similarity exists between the stego images and cover images and the same is for secret images and extracted ones.

In the used RS coding system, the encoder adds parity bits to the secret images. Parity bits has no effect on the similarity between the stego image and their correspondence cover image because it has been added to the secret image resized by the encoder.

6. Conclusion

In this paper, the proposed system hides the secret image in the cover image using LSB based on wavelet coefficient and ciphering process. This leads to increase the imperceptibility and robustness of the system. The performance evaluation of the proposed method is measured two Factors PSNR and MSE. Applying the idea of LSB based-wavelet provides a better performance than the other existing methods. The using of Haar Wavelet Transform provides good extracted secret image. Employing RS code in the stego systems offer good extracted image. The advantage of the proposed coded system is the ability to change the code-word length and the information length. The experiments prove that the suggestion methods are more active for secure data communication.

References

[1] R. Gupta and T. P. Singh. New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters. Proceeding of the International Conference Contemporary Computing and Informati**cs**, (2014), N**o**v. 27-29; United States

[2] B. Mehboob and R. A. Faruqui. A stegnography implementation. International Symposium on Biometrics and Security Technologies, (2008) April 23-24; Islamabad, Pakistan

[3] V. Ashok, T. Balakumaran, C. Gowrishankar, I. Vennila and A. N. kumar. The Fast Haar Wavelet Transform for Signal & Image Processing. International Journal of Computer Science and Information Security. 7, 1 (2010)

[4] I. Márquez-corbella and J. Tillich. Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography. IEEE International Symposium on Information Theory, (2016) July 10-15; Barcelona, Spain

[5] C. Lai and C. Tsai, Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. IEEE Transactions on Instrumentation and Measurement. 59, 11 (2010)

[6] MIT-DB, The MIT-BIH Arrhythmia database - third edition. Massachusetts institute of technology, United States (1997)

[7] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, A novel technique for image steganography based on Block-DCT and Huffman Encoding. International Journal of Computer Science and Information Technology. 2, 3 (2010)

[8] S. K. Bandyopadhyay and I. K. Maitra, An Alternative Approach of Steganography using Reference Image. International Journal of Advancements in Technology. 1, 1 (2010)