Proceedings of the Federated Conference on Computer Science and Information Systems pp. 641–644
DOI: 10.15439/2016F521
ACSIS, Vol. 8. ISSN 2300-5963

An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System

Essam H. Houssein [1,*],Mona A. S. Ali [2,*], and Aboul Ella Hassanien[3,*]
[*] Faculty of Computers and Information
[1]Minia University [2]Benha University [3]Cairo University
[*]Scientific Research Group in Egypt (SRGE) http://www.egyptscience.net

***Abstract*—The security of data over the internet is a crucial thing specially if this data is personal or confidential. The transmitted data can be intercepted during its journey from device to another. For that reason, we are willing to develop a simple method to secure data. Data encryption is one method to secure the messages but the intruders can still try to crack it, in order to overcome this, steganography has been used to hide the data into a cover media(i.e. audio, image or video). Recently steganography attracts many researchers as a hot topic. This paper proposes an advanced technique for encrypting data using Advanced Encryption System (AES) and hiding the data using Haar Discreet Wavelet Transform (HDWT). HDWT aims to decrease the complexity in image steganology while providing less image distortion and lesser detectability. One-forth of the image carrying the details of the image in a region and other three regions carrying a less details of the image then the cipher text is concealed at most two Least Significant Bits (LSB) positions in the less detailed regions of the carrier image, if the message doesn't fit in the first LSB only it will use the second LSB. This proposed algorithm covers almost all type of symbols and alphabets.**

***Index Terms*—Steganography, Cryptography, Encryption, AES Encryption, LSB, DWT**

I. Introduction

STEGANOGRAPHY is a data hiding technique that has been mainly used in information security applications. It is similar to watermarking and cryptography techniques, but these three techniques are different in some aspects. Firstly, watermarking mainly tracks illegal copies or claims of the ownership of digital media. It is not geared for communication. Secondly, cryptography scrambles the data with the mixture of permutation(s) and substitution(s) so that unintended receivers cannot perceive the processed information. However, the fact that information has been embedded into a medium (i.e., watermarking) and communication has been carried out (i.e., cryptography) is known to everyone, or at least it is acceptable to reveal such a fact. Finally, steganography transmits information by embedding messages into innocuous looking cover objects, such as digital images, to conceal the very existence of communication. As a result, steganography is the art and science of data smuggling since its goal is to hide the presence of communication [1].

Each image hiding system consists of an embedding process and an extraction process. An innocuous-looking original image is used as the cover-image to conceal the secret data. The secret data are embedded into the cover-image by modifying the cover-image to form a stego-image. Cryptography [2], [3] and steganography [4] are the two important aspects of communications security. Although cryptography is a primary method of protecting valuable information by rendering the message unintelligible to outsiders [3], steganography is a step ahead by making the communication invisible. A possible formula of the process may be represented as: $Stegomedium = Covermedium + Embeddedmessage + Stegokey$

In this paper, an advanced technique for encrypting data is proposed using AES and hiding the data using Haar DWT technique, carrying the details of the image in a region and other three regions carrying a less details of the image then the cipher text is concealed at most two LSB positions. Extensive experiments show the effectiveness of the proposed method. The results obtained also show significant improvement than the method proposed in [5]. The remainder of the paper is organized as follows. Section II briefly describes the related work. In Section III, the related main knowledge is described. Section IV, discusses the features of the proposed technique. The performance is analyzed. Experimental results are given in Section V. Finally, Section VI concludes this paper.

II. Related Work

A few steganography approaches are briefly reviewed here.In [6], Tiegang et al. proposed a new image encryption algorithm based on hyper-chaos, which uses a new image total shuffling matrix to shuffle the pixel positions of the plain-image and then the states combination of hyper-chaos is used to change the grey values of the shuffled-image. In [7], Chin-Chen et al. proposed a new steganographic method to increase the message load in every block of the stego-image while keeping the stego-image quality acceptable. In [8], B. T. NilanjanDey, et al, proposed a method for hiding multiple images in an image based on DWT and DCT. In [9], Chen Po-Yueh et al. proposed a new steganography technique which embeds the secret messages using the DWT in the frequency domain to divide the image into 4 sub bands, and it will embed the secret data in the LSB of the lowest priority band and it wouldn't use the low frequency sub band that holds the most

details to preserve the quality of the image, and it have 2 modes and 5 cases because of the demands of the capacity or quality.

In [10], Chiang-Lung et al. proposed method adopts the complementary embedding strategy to reduce the loss of statistical property of the stego-image in spatial domain. In [11], Chi-Kwong Chan et al. proposed a data hiding method by simple LSB substitution with an optimal pixel adjustment process. The image quality of the stego-image can be greatly improved with low extra computational complexity. In [12], KokSheik et al. presented a novel Mod4 steganographic method in discrete cosine transform (DCT) domain. Mod4 is a blind steganographic method.

In [13], M. Juneja et al., proposed a secure methods of information security using steganography, the first method embeds In the LSB of the blue components partial green components of random positions in the edges of the green component, the second method is an adaptive method that uses the data of the MSB of the red, green and blue components to embed the message in the random pixels across smooth areas, the third method is a hybrid feature detection filter that predicts the edges in noisy conditions.

In [5], Avval et al, proposed steganography technique to embed audio into the edges of a color image, this technique uses the chaotic map to select the random edge pixels to embed the bits and to choose which random LSB bit location in the selected pixel. In [14], Hemalatha S. et al. proposed a method to hide multiple secret keys and images in a color image using integer wavelet transform (IWT). In [11], T. Garima, proposed an approach to encrypt message using RSA 1024 algorithm then it will be embedded in a cover image by modifying the LSB technique. In [15], L. S. Ahmed et al., proposed a method of encrypting the message by a substitution cipher then it will be embedded using LSB insertion techniques to achieve high capacity to be embedded and security of the steganography method. In [10], Liu Lung et al. proposed a jpeg steganographic using complementary embedding technique, this method is achieved by dividing the quantized DCT coefficients and the secret bits into two parts according to a predefined partition ratio. The two parts of DCT coefficients are used to embed the corresponding parts of secret bits with different embedding algorithms. Specifically, the secret bits are embedded by subtracting one from one part of coefficients, and adding one to the other part of coefficients.

III. The steganography

A. 2D-Haar-wavlet Transform

Wavelet transform has the capability to offer some information on frequency-time domain concurrently. In this transform, time domain is passed through high-pass and low-pass filters to extract high and low frequencies respectively. This process is repeated for a number of times and each time a section of the signal is drawn out. DWT analysis splits signal into two classes (i.e. Approximation and Detail) by signal decomposition for different frequency bands and scales. DWT employs two function sets: scaling and wavelet which associate with low and high pass filters orderly. Decomposition follows the manner of dividing time separability. Meanly, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability.

Haar wavelet operates on data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One important feature of the Haar wavelet transform is that the transform is equal to its inverse. Each transform computes the data energy in relocated to the top left hand corner.

Figure 1 shows the image Lena after one Haar wavelet transform

Fig. 1: 2D Haar Wavelet Transform Example

After each transform is performed the size of the square which contains the most important information is reduced by a factor of 4 as seen in Figure 2.

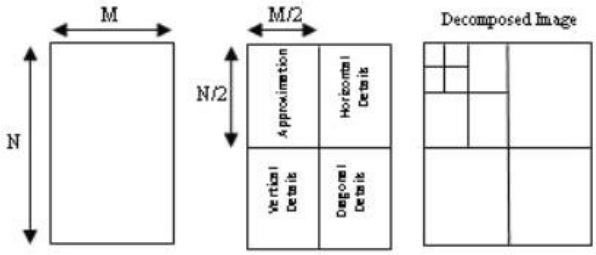

Fig. 2: Detailed 2D Haar Wavelet Transform

B. AES encryption technique

The cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits). Data block of 4 columns of 4 bytes is state key expanded to array of words. Ordering of bytes within a matrix is by column. The cipher consists of rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and so on, each transformation takes one or more 4 X 4 matrices as input and produces a 4 X 4 matrix as output (the cipher text).The key expansion function generates N + 1 round keys, each of which is a distinct 4 X 4 matrix. Each round key serves as one of the inputs to the Add Round Key transformation in each round.

C. LSB substitution technique

The wide used technique of hiding messages into the image without affecting the whole image is the LSB technique that uses the least significant bit of each pixel to embed the message into it. Figure 3 shows how the pixel can be illustrated from the most important bit to the least important bit. The basic concept of LSB substitution is to embed the message in the least important bit (least significant bit) of the pixel the equation for the LSB is

$$X_i^{'} = X_i - X_i mod 2^k + m_i \tag{1}$$

in this equation the $X_i^{'}$ is the i^{th} pixel value of the stego image, X_i is the i^{th} pixel of the image (cover image) and m_i denotes the decimal value of the i^{th} block in confidential data. K denotes the number of LSB places. we will use or substitute from the pixel. In the process of extracting the message from the image pixel is to copy the least significant bit directly, and this process is showed in the following equation (2):

$$m_i = x_i^{'} mod 2^k \tag{2}$$

This technique is easy and fast but it have drawback if the message have a great size, it will affect the image and it can be noticeable.

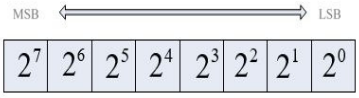

Fig. 3: The places of the bits in the pixel

IV. Proposed Approach

In this research the proposed approach includes two main process: Embedding process and Extracting process.

A. Embedding process

As seen in Algorithm 1, we started first by reading the cover image C and the message to be embedded M. The cipher message S is extracted by applying the AES encryption technique on message M. After performing the AES technique on the message, it is ready to be concealed in the image. Suppose that the 8-bit gray level cover image of size M_CxN_C as :

$$C = \{x_{i,j} | 1 \leqslant i \leqslant M_c, 1 \leqslant j \leqslant N_c, x_{i,j} \in \{1, 2, 3..., 255\}\} \tag{3}$$

S is the n-bit secret message represented as:

$$S = \{S_i | 1 \leqslant i \leqslant n, S_i \in \{0, 1\}\} \tag{4}$$

From Algorithm 1, the embedding steps will be as follows:

1) Apply the DWT on the cover image and get the four sub-bands obtained are denoted LL, HL, LH and HH.
2) Get three bits iteratively from the cipher message and distribute only one bit from the three bits in every one LSB of the three sub bands HH, HL and LH respectively, if the cipher message require more LSB, our algorithm will move cursor to the second LSB of each pixel in the three sub bands. This improves the capacity and permits high capacity with no effect on the pixel value. As the embedding process is done on the sub bands that don't contain details of the image.
3) Perform the inverse DWT on the result of step 2, by performing this step the resulted matrix is H, some pixels of H are not integers ranging from 1-255 due to LSB substitution. So we obtain (K-matrix) that contains the possible non-integer situation (0.0, 0.25, 0.5 and 0.75).
4) Round the matrix H to obtain the stego image E, in order to reconstruct the secret message we will use the k-matrix for reconstruction.
5) Send the Stego image to the receiver with the k-matrix in the description file or tag with the total number of message bits too.

Algorithm 1 Proposed Approach

1: input=gray scale cover image C and message to be embedded M
2: output= StegoImage
3: $S =$ Encrypt M using AES technique
4: $IfSize(S) >$ total first three bit of LSB in C
5: Then get another cover Image AC and go to step 4
6: D = Apply the DWT on C
7: Embed S in the coefficient of D
8: Inverse D
9: obtain (K-matrix) that contains the possible non-integer situation (0.0, 0.25, 0.5 and 0.75)
10: Calculate inverse 2D-DWT on each block to get the stego image.

B. Extraction process

In order to extract the original image the following steps are followed:

1) Extract the k-matrix of the file tag of E.

$$K = \{K_{i,j} | 1 \leqslant M_F \leqslant n, 1 \leqslant j \leqslant N_F, K_{i,j} \in \{00, 01, 10, 11\}\} \tag{5}$$

Transform all elements of k into (0.0, 0.25, 0.5 and 0.75).
2) Obtain the H by performing DWT which is calculated as H=E+K-matrix.
3) Obtain the total number of the message from the file tag of E, extract 3 bits iteratively from the LSB of the three sub bands HHH, HHL and HLH. After completing the first LSB and there are more bits of the message is still not extracted (bits extracted message size of E != 0) Get the remaining bits from the second LSB in the same way as the last step. Extracting the two LSB of the remaining bits, example [A,B]
4) After extracting the whole bits perform the inverse AES on the encrypted bits to obtain the original message.

V. Results and Discussion

The proposed approach is applied on 512x512 8-bit grayscale images Jet, Boat, Baboon and Lena. The messages

are generated randomly with size upto maximum hiding capacity. To measure the quality, a parameter is developed to compute the quality of the image this parameter is called PSNR and defined as follows:

$$PSNR = 10\log_{10}(255^2/MSE) \tag{6}$$

The root mean square error (RMSE) has been used as a standard statistical metric to measure model performance in meteorology, air quality, and climate research studies. The mean absolute error (MAE) is another useful measure widely used in model evaluations, denotes the mean error and it's the deference between the original image and the stego image as seen in Figure 5, and the equations to compute the MAE and MSE are:

$$MSE = \frac{1}{MXN}\sum(a-b)^2 \tag{7}$$

Where a denotes the pixel in the original image and b denotes the pixel in the stego image, with high PSNR means a high quality, this means that while the dB is low this means that the image has been modified or there is a noise or distortion.

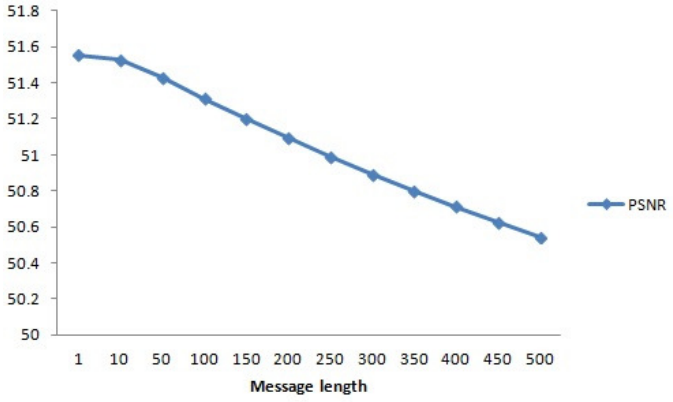

Fig. 4: PSNR Results

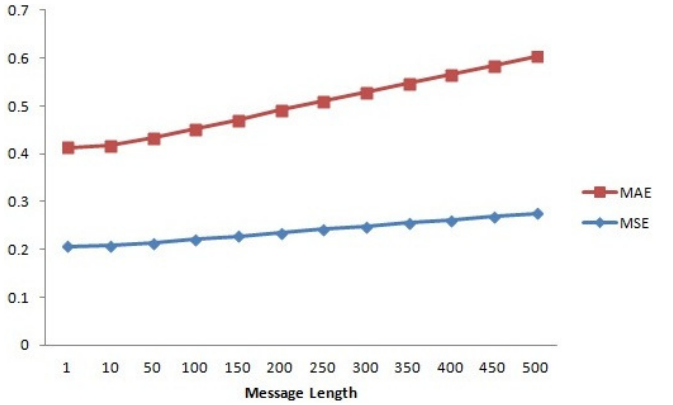

Fig. 5: MSE and MAE Results

Verification of the results has been done for various length of message (LM) and calculates error for all different messages the proposed technique works fine show in Figure 5. When compare our technique with scheme [5]. It gets results better than other method. Result of PSNR for other method between 75, 80 but PSNR of our method smaller than it as seen in Figure 4.

VI. Conclusion

There are demands of the algorithms of steganography to progress with the capacity or with quality, so with this method we aimed at the capacity demand to store as high as possible messages in the image with reduced effect of the quality of the image, and made it even harder to get the message by encrypting it before storing the message in the cover image, with this method the message is secured and hidden, and the cover image can take much more message size to hide. As the main goal of steganography is to hide and secure the message.

References

[1] S. Katzenbeisser and F. Petitcolas, *Information hiding techniques for steganography and digital watermarking*. Artech house, 2000.
[2] A. Nissar and A. Mir, "Classification of steganalysis techniques: A study," *Digital Signal Processing*, vol. 20, no. 6, pp. 1758–1770, 2010.
[3] S. Williams, "Cryptography and network security: Principles and practices," 2006.
[4] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Shamsuddin, "Information hiding using steganography," in *Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on*. IEEE, 2003, pp. 21–25.
[5] N. Bhardwaj and S. Agarwal, "A new technique for extracting image information beyond visibility," *International Journal of Information and Computation Technology*, vol. 3, pp. 539–548, 2013.
[6] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.
[7] C.-C. Chang, T.-S. Chen, and L.-Z. Chung, "A steganographic method based upon jpeg and quantization table modification," *Information Sciences*, vol. 141, no. 1, pp. 123–138, 2002.
[8] T. Bhattacharya, N. Dey, and S. Chaudhuri, "A session based multiple image hiding technique using dwt and dct," *arXiv preprint arXiv:1208.0950*, 2012.
[9] P.-Y. Chen, H.-J. Lin *et al.*, "A dwt based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006.
[10] C.-L. Liu and S.-R. Liao, "High-performance jpeg steganography using complementary embedding strategy," *Pattern Recognition*, vol. 41, no. 9, pp. 2945–2955, 2008.
[11] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple lsb substitution," *Pattern recognition*, vol. 37, no. 3, pp. 469–474, 2004.
[12] K. Wong, X. Qi, and K. Tanaka, "A dct-based mod4 steganographic method," *Signal Processing*, vol. 87, no. 6, pp. 1251–1263, 2007.
[13] M. Juneja and P. S. Sandhu, "A new approach for information security using an improved steganography technique," *Journal of Information Processing Systems*, vol. 9, no. 3, pp. 405–424, 2013.
[14] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A secure and high capacity image steganography technique," *Signal & Image Processing*, vol. 4, no. 1, p. 83, 2013.
[15] S. A. Laskar and K. Hemachandran, "High capacity data hiding using lsb steganography and encryption," *International Journal of Database Management Systems*, vol. 4, no. 6, p. 57, 2012.