Holo-Entropy and Advanced Encryption Standard for Wavelet-Based Image Steganography

Wrushali Waghmare[1], S. I. Nipanikar[2], P. V. Mulmule[3]

[1]*Student, Dept. of Electronics & Telecommunication, Padmabhusan Vasantdada Patil Inst. of Tech., Pune, India*
[2]*HOD, Dept. of Electronics & Telecommunication, Padmabhusan Vasantdada Patil Inst. of Tech., Pune, India*
[3]*Asst. Prof., Dept. of Electronics & Telecomm., Padmabhusan Vasantdada Patil Inst. of Tech., Pune, India*

***Abstract*—Image Steganography is an approach employed for transferring the hidden message or information by modifying an image in an imperceptible manner. Various techniques are available in the literature for image steganography, among which wavelet transform based approaches are widely used. In this paper, a method of hiding the audio message in the image is done, for which a Discrete Wavelet Transform (DWT) is employed. At first, the input secret message, which is in audio, is normalized and encrypted using Advanced Encryption Standard (AES) method. Then, the encrypted message is converted into binary data to embed into the cover image. The cover image is transformed using wavelet transform and the transformed coefficients are selected using holo entropy function for optimal embedding. The selected coefficients are used to embed the encrypted audio data. Finally, the embedded band is transformed to the spatial domain and subsequently, compressed using JPEG. In the receiver side, the same procedure is reversibly applied to extract the audio message. Simulation of the proposed framework is done by considering three standard images for the processing, and different states of noise are introduced for the analysis. Simulation results reveal that the proposed technique achieved PSNR and MSE of 56.70632 dB and 0.0009, respectively.**

***Index Terms*—Image Steganography, audio, Discrete Wavelet Transform, AES, holoentropy function**

I. Introduction

Image steganography [5] can be deprived as one of the efficient approaches for sending and receiving the secret message. Various multimedia information, such as text, and audio can be embedded with the image during the steganography. It ensures security to the sensitive information content, as it protects the information against data corruption and unaccepted access. It is applied to the fields, such as medical, forensic reports, etc. [4]. One of the major criteria to be satisfied during the image steganography is that the embedded image and the cover image must be same during the visualization [2]. Thus, the hacker cannot retrieve the actual information content. The secret message to be embedded is send to the system via the transmission channel [11] [7]. For performing image steganography, the following elements, like cover image, secret message, secret key, and embedding algorithm, are required [6] [9]. The embedding algorithm needs to ensure that the hacker does not find the hidden secret message embedded in the cover image [8].

In the image steganography [12], sensitive information present as audio or text are embedded in the cover image and send to the receiver. The embedding is done through various techniques, from which the Discrete Wavelet Transform (DWT) is the commonly used one. DWT transform makes the image into the wavelet image and hence, the incorporation of the wavelet image with the audio or text message will be easier. In the medical field, incorporation of the medical information into the image needs to be provided with high security. Incorporating the audio information into the image faces further challenges as the audio is affected by various noise factors, such as salt and pepper, Gaussian noise, etc. During the embedding, it is necessary to develop the system robust towards the noise. Also, literature has suggested using some encryption algorithm, such as AES, DES for encrypting the audio message, which again improves the security.

This research intends to develop the image steganography scheme by incorporating the AES. The entire process involved in images steganography is explained as follows: Initially, the secret message is encrypted using the AES encryption algorithm, and formulated as the AES signal. Then, the AES signal is subjected to binarization and thus converted to the bit message. Now, the cover image is subjected to the wavelet transform using the DWT process. The resulted image and the bit message are embedded with the holoentropy function, used in the cost matrix. The cost matrix contains other parameters, such as edge and intensity for dealing with the steganography process. The embedding process identifies the embedded/ stego image. During extraction, the audio message embedded in the cover image is extracted through reversing the above mentioned process.

The contribution of this work is the development of the steganography scheme through the AES encryption and the holoentropy based cost function. Further, the paper is organized as follows: Section 2 reviews some literature works related to the image steganography. Section 3 describes the proposed scheme by explaining the embedding and the extraction process. Section 4 discusses the simulation results by introducing different standard images and section 5 concludes the paper.

II. Motivation

A. Literature Survey

This section surveys some of the related works to the image steganography. The four literature works are discussed below: Vipul Sharma and Sunny Kumar [10] proposed the steganography technique by developing the enhanced version of the LSB technique. The scheme further made use of the compression technique to improve the hiding capacity. The model achieved high performance, but the model was less robust towards the noise. Weiqi Luo et al. [3] presented the edge selection scheme, for hiding the signal in the medical image. The scheme maintained improved quality throughout the process. The edge selection process performed the embedding by finding the pixel difference between the consecutive images. The model lacked visual quality after the embedding. Nameer N. El-Emama and Mofleh Al-Diabat [1] presented the adaptive image filtering and the adaptive segmentation algorithms for the image steganography. The model tried to overcome visual, structural, and statistical attacks prevailing in the image. The scheme is more complex as it provides seven layers of security. Da-Chun Wu and Wen-Hsiang Tsai [8] presented the simple least significant-bit replacement method for hiding the sensitive information content. The embedding of information is done by replacing the significant bits present in the cover image. The model lacked to provide optimized security level for the secret message.

III. Proposed Holo entropy and Advanced Encryption Standard for Wavelet-Based Image Steganography

This section presents the description to the proposed image steganography process through the holo entropy and AES encryption scheme. The Fig. 1, describes the architecture of the proposed image steganography through the AES and the proposed cost function. The embedding and the extraction of the secret audio signal are done through AES encryption and further, the cost matrix uses the holo entropy parameter, for selecting the optimal location for embedding.

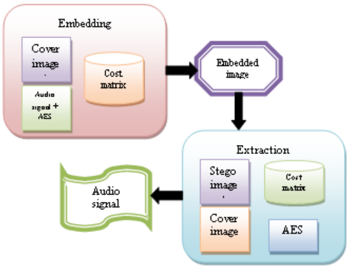

Fig. 1. Architecture of proposed Holoentropy and AES based wavelet-based image steganography

A. Embedding

Here, the embedding process involved in the proposed image steganography process is explained and described in Fig. 2.

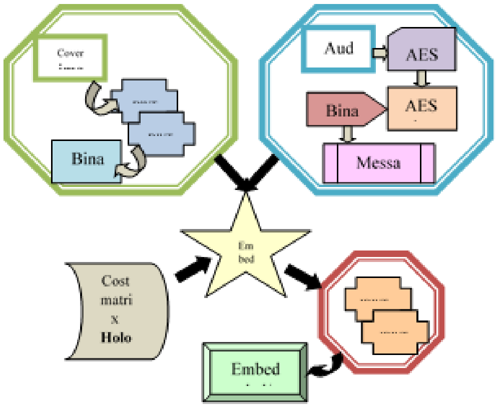

Fig. 2. Embedding the audio signal to image via AES and proposed cost function

Consider the cover image C for hiding the audio signal S. The audio signal has the size of $1 \times N$. The cover image is subjected for the DWT to yield four bands, represented as

$$\left[C_1 \quad C_2 \quad C_3 \quad C_4\right] = DWT(C) \tag{1}$$

Where, C_1 ,C_2, C_3 , and C_4 indicate the LL, LH, HL and HH bands, respectively, obtained from the DWT transform. Again, the process undergoes DWT and it is represented as,

$$\left[C_r^1\right] = DWT(C_1) \tag{2}$$

The above image is represented as the DWT image. The secret message is the audio message represented as S with the size of $1 \times N$. The audio signal is subjected to the AES for the encryption. The steps involved in AES encryption algorithm for encrypting the secret message are given as follows:

1) The signal of size $1 \times N$ is provided to the encryption. The AES algorithm initially finds the cipher key from the Rijndael's key schedule and generates the 128-bit round key for performing the key round operation.
2) The round key is combined with each block through the XoR operation.
3) A lookup table is initialized in AES algorithm, based on which the byte in the block is substituted with new value.
4) Then, the transposition is applied, where the last three rows of the block are shifted in a cyclic manner.
5) Here, mixing of the columns is done, for combining the four bytes of the columns to form a new value.
6) Now the round key is added to the block, mix row operation is carried out, followed by adding the round key.

After the encryption, the signal is converted as AES signal. $A_{,}$ which has the same size as the input audio signal S. After the AES encryption, the AES signal is subjected to the binarization. Here, binarization converts the AES matrix into

11 bit representation, and hence, the converted message bit is represented as M and it has the size of $11 \times N$.

The next step in the embedding is the identification of the suitable pixel location in the cover image for performing the embedding process. This can be done through building the cost matrix with the elements, such as holoentropy, edge and intensity. The constructed cost matrix can be represented as,

$$Z_{ij}^{C} = \frac{1}{3}\left(\chi_{ij}^{C} + \alpha_{ij}^{C} + \beta_{ij}^{C}\right) \qquad (3)$$

Where, Z_{ij}^{C} refers to the cost function for the cover image. The terms χ_{ij}^{C}, α_{ij}^{C}, and β_{ij}^{C} represent holoentropy, intensity and edge of the cover image C. Each of these factors is defined as follows,

The holoentropy [16] can be obtained as the weighted parameter of the entropy function, and further, it is identified based on the canny function. The holoentropy based on the entropy function is expressed as follows,

$$\chi_{ij}^{C} = W * E(C) \qquad (4)$$

Where, $E(C)$ indicates the entropy of the cover image C and it is expressed as,

$$E(C) = \sum_{i=1}^{p} P_i \log P_i \qquad (5)$$

Where, P_i refers to the probability value for the unique pixel i. The weighted function used in the holoentropy is expressed as,

$$W = 2\left[1 - \frac{1}{1 + \exp(-E(C))}\right] \qquad (6)$$

Other factors, such as edge and intensity refer to the edge pixel and the intensity value of the pixel and thus, it can be referred as follows,

$$\alpha_{ij}^{C} = \frac{1}{8}\sum_{n=1}^{8} \alpha_{ij}^{n} \qquad (7)$$

$$\beta_{ij}^{C} = \frac{1}{8}\sum_{n=1}^{8} \beta_{ij}^{n} \qquad (8)$$

After identifying the cost matrix, the message bit M and the DWT image $\left[C_r^1\right]$ are subjected to embedding process. The cost matrix defines the cost value for each pixel to embed the image. Based on this value, embedding is carried out, and it is expressed by the following equation,

$$C_1^{r\bullet} = C_1^{r} + G * M \qquad (9)$$

Where, $r \in \{a, b, c, d\}$, $C_1^{r\bullet}$ indicates the modified sub band after embedding, G is the binary converted cost matrix, and M is the binary message. The embedded image $C_1^{r\bullet}$ has high frequency, and thus, it can be converted into time domain by applying IDWT. The spatial domain of the image after the IDWT process is expressed as follows,

$$C_1^{\bullet} = \mathrm{IDWT}\left(C_1^{r\bullet}\right);\ r \in \{a, b, c, d\} \qquad (10)$$

Finally, the IDWT is again applied to obtain all the four bands, and it is expressed as,

$$C^{\bullet} = \mathrm{IDWT}\left(C_1^{\bullet} \quad C_2 \quad C_3 \quad C_4\right) \qquad (11)$$

Where, $C^{\bullet}$ refers to the stego image achieved through the embedding process.

B. *Audio Signal Extraction*

The extraction makes the user to obtain the secret message from the cover image. In the extraction, the reverse process of the embedding is done. Figure 3 presents the architecture of the extraction process carried out in the proposed scheme. The stego image identified by the embedding process is subjected for the transformation using DWT. Then, the modified pixels of the image are subtracted with the actual cover image. Difference in cover image and the DWT image yields the binary message of size $11 \times N$. Then, it is reversed to $1 \times N$ size, and subjected to AES decryption. After the decryption, the audio secret message is retrieved and it is represented as $S*$

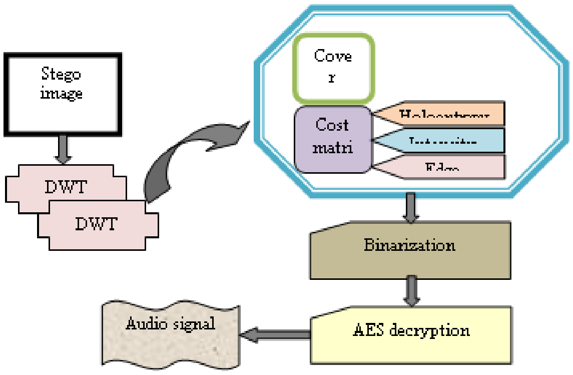

Fig. 3. Extraction of audio signal from the stego image

IV. Results and Discussion

This section presents the experimental results of the proposed holoentropy scheme for achieving the image steganography. The results are evaluated by considering two medical images for the processing.

A. *Experimental Setup*

The entire setup involving the AES algorithm and the proposed cost function for the image steganography is implemented in the MATLAB tool. The experimentation requires the configuration of PC with 4 GB RAM, Intel I3 processor, and Windows 10 OS.

B. *Performance Metrics*

The proposed image steganography technique with the holo entropy cost function and the AES algorithm is evaluated based on MSE and PSNR. The expression for the PSNR and detection error rate is given as follows: *MSE:* MSE measures the deviation of actual performance from the desired response, and it is indicated as follows,

$$MSE = \frac{1}{q}\sum_{p=1}^{q}\left(O_p - \hat{O}_p\right)^2 \tag{12}$$

Where, O_p and $\hat{O}_p$ refers to the output of the steganography process, and the desired response, respectively.

PSNR: The quality of the image subjected to the steganography process is evaluated by the PSNR measure. It directly depends on MSE metric, and is expressed as follows,

$$PSNR = 10\log\frac{255^2}{MSE} \tag{13}$$

C. Comparative Techniques

The entire experimentation of the proposed work is compared with state of art techniques, such as AES, Haar + cost, and DB1 + cost. The comparative techniques are explained as follows: *AES:* The AES encryption standard is one of the formerly developed techniques for encrypting the secret message into the image. After the encryption, the size of the text does not alter. *Haar + cost:* Here, the Haar wavelet function is used for the encryption, and the embedding is done through the newly developed cost function. *DB1 + cost:* The embedding of signal is done through the DB1 wavelet and for the embedding process, the cost function developed in this work is utilized.

D. Experimental Results

This subsection presents the performance of the proposed cost function along with AES for the image steganography and the simulation results of the proposed scheme are presented in Fig. 4. Fig. 4 (a), depicts the performance of the proposed cost function with the AES for the image not affected by noise. Further, the Fig. 4.a.i, 4.a.ii, 4.a.iii, and 4.a.iv depict the original audio signal, extracted audio signal, original image and embedded image, respectively. Fig. 4(b), depicts the performance of the proposed cost function with the AES while the image is affected by salt and pepper noise. The noise density for the experimentation is chosen as 0.1. Further, the figure 4.b.i, 4.b.ii, 4.b.iii, and 4.a.iv depict the original audio signal, extracted audio signal, original image and embedded image, respectively, for the same analysis.

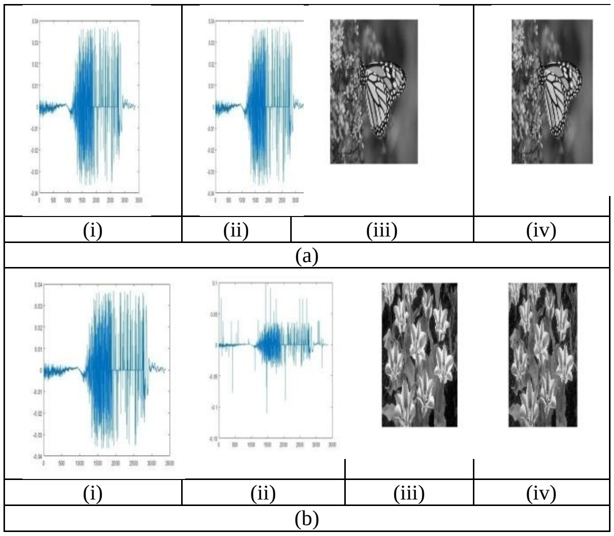

Fig. 4. Simulation results of proposed cost function with AES based image steganography scheme with embedding done on the image (a) without noise, ((i) input signal, (ii) Extracted signal, (iii) original image and (iv) extracted image) and (b) with noise ((i) input signal, (ii) Extracted signal, (iii) original image and (iv) extracted image).

E. Comparative Analysis

The comparative analysis is done in two terms i.e.) 1) Without noise, and 2) With noise. In the first type, the image considered for the analysis is free from noise, while in the second type, two types of noises, such as salt and pepper, and Gaussian noise, affect the image. During comparative analysis with the noise signals, the noise density of salt & pepper and Gaussian noise is varied.

F. Comparative Discussion

This section presents the comparative discussion of the state of art techniques while analyzing the image with and without noise. The Table-1 discusses the best performance of the comparative techniques for different simulation condition. When the image is not affected by noise, the proposed AES + cost technique achieved improved results with the values of 56.7063 and 0.0009, for PSNR and MSE, respectively. When the image is affected with salt and pepper noise, the proposed model has the values of 33.3463 dB and 0.00082, for PSNR and MSE, respectively. Similarly, for the Gaussian noise, the proposed model has the values of 28.5349 dB and 0.00084, for PSNR and MSE, respectively.

TABLE I
COMPARATIVE DISCUSSION

Methods	**Without noise**		**With noise**			
	PSNR (dB)	MSE	PSNR (dB)		MSE	
			Gaussian	Salt and pepper	Gaussian	Salt and pepper
AES	50.1849	0.00096	31.1948	0.00088	26.7199	0.006114
DB1 + Cost	54.4215	0.00094	32.1708	0.00086	27.2952	0.00593
Haar + cost	55.6137	0.00092	32.5672	0.00084	27.9164	0.005436
AES +cost	**56.7063**	**0.0009**	**33.3463**	**0.00082**	**28.5349**	**0.00084**

V. Conclusion

This paper introduces an image steganography technique, for hiding the audio secret message within the medical image. During the embedding phase, the cover image is subjected to DWT and thus, produces the DWT image, and the audio signal is subjected to AES encryption and binarization to convert the signal as the bit message. Both the bit message and the DWT image are embedded through the cost matrix. The cost matrix is developed in this work with the parameters, such as holoentropy, edge and intensity factors, and it finally produces the embedded image of high quality. The entire analysis of the proposed work is implemented by considering three standard images and an audio message for embedding. Experimentation of the proposed technique is done by introducing two different noises, and evaluated based on PSNR and MSE metrics. The experimental results reveal that the proposed technique with the AES and the cost function achieved values of 56.7063 and 0.0009, respectively, for PSNR and MSE. When the image is affected with salt and pepper noise, the proposed model has the values of 33.3463 dB and 0.00082, for the PSNR and the MSE, respectively.

References

[1] Nameer N. El-Emam and Mof leh Al-Diabat, "A novel algorithm for colour image steganography using a new intelligent technique based on three phases", Applied Soft Computing, vol.37, pp.830–846, Dec, 2015.

[2] Sahar A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information", Computers & Electrical Engineering, 19, Sep, 2016.

[3] Weiqi Luo, Fangjun Huang and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, vol.5, no.2, 17, February, 2010.

[4] Bin Li, Shunquan Tan, Ming Wang, and Jiwu Huang, "Investigation on Cost Assignment in Spatial Image Steganography", IEEE Transactions on Information Forensics and Security, vol. 9, no.8, 29 May,2014.

[5] Bingwen Feng and Wei Lu; Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE Transactions on Information Forensics and Security, vol.10, no.26, November, 2015.

[6] Soodeh Ahani and Shahrokh Ghaemmaghami,"Colour image steganography method based on sparse representation", IET Image Processing, vol. 9, no.6, 01 June 2015.

[7] Chi-Kwong Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, vol.37, no.3, pp.469–474, March, 2004.

[8] Da-Chun Wu and Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol.24, no.9–10, pp.1613–1626, June, 2003.

[9] Petros L. K. Mantos and Ilias Maglogiannis, "Sensitive Patient Data Hiding using a ROI Reversible Steganography Scheme for DICOM Images", Journal of Medical Systems, 11 May, 2016.

[10] Vipul Sharma and Sunny Kumar ,"A New Approach to Hide Text in Images Using Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering ,vol.3, no.4, pp. 701-708 ,April, 2013.

[11] Hayat Al-Dmour and Ahmed Al-Ani, "Quality optimized medical image steganography based on edge detection and hamming code", In Proceedings of the IEEE 12th International Symposium on Biomedical Imaging (ISBI), pp.1486 - 1489, 2015.

[12] [12] Mamta Jain, Saroj Kumar Lenka and Sunil Kumar Vasistha, "Adaptive circular queue image steganography with RSA cryptosystem", Perspectives in Science, vol.8, pp.417–420, Sep, 2016.