Haar Transformation for Compressed Speech Hiding

Meaad Mohammed Salih
Dept. Computer Science, Faculty of Science , University of Mosul /Iraq
Teba Muhammed Ghazi Sami
Dept. Computer Science, College of Computer And Mathematic Science , University of zakho /Iraq
Khalil Ibrahim Al-Saif
Dept. Computer Science, College oOf Education For Pure Science , University of Mosul /Iraq
meaad_muhammad@yahoo.com teba.sami@uoz.edu.krd
khalil_alsaif@hotmail.com

ARTICLE INFO
Submission date: 17 / 3 / 2019
Acceptance date: 11 / 9/ 2019
Publication date: 31/ 12 / 2019

Abstract

Steganography science is one of the most popular field in security direction. In this paper an algorithm will be adopted to embed a compressed speech inside a gray image using discrete wavelet (Haar transformation). In the beginning the speech was compressed up to its half original size by applying (Daubechies) then convert the speech data from decimal code to binary code and embed it inside Haar coefficients of the cover _image using the Four sub bands (cA : Low Low,cH: High Low,cV:Low High,cD: High High) which got by applying the wavelet on the cover_ image. Measuring Peak Signal to Noise Ratio (PSNR) to determine the accuracy of the stego_image with respect to the original image, MSE and the correlation factors were checked show that the proposed algorithm has positive effect in field of speech hiding.The proposed technique in this research turned out to be able to hide speech data (audio) in the cover image and then extract the hidden data with storage rate (1) bits per pixel. Hiding capacity can be achieved using this method proportionally depends on cover_image size. High frequency coefficients have also been shown to be better for data hiding in terms of perceptibility and intruders' cannot be able to recognize the cover medium (stego_image) which included secret data.

Keywords: gray image , steganography , wavelet transformation ,stego_image.

1. Introduction

Steganography is the art of information hiding imperceptibly in a cover medium. "*Steganography*" is a word of Greek origin which means *"covered or hidden writing"*. The main aim in steganography is to hide the presence of the secret data in the in the cover medium [1]. “Data hiding involves” embedding secret data inside the cover with a reasonable deformation. Multiple applications can be applied for example: “copyright protection (watermarking), image authentication, secret communication (steganography) and so on”. Though different requirements needed for various applications. Science of Data hiding has two main fundamentals: First, the deformation caused by the inclusion of confidential data inside the cover should be minimized as there are no obvious changes to the cover. Secondly, the capacity of hiding (cover image) should be enough to include an acceptable amount of hidden data[2][3].

However, "a tradeoff between the hiding capacity and embedding distortion and is inevitable result " [3].

Few basic requirements have to comply with all steganographic algorithms. Steganographic algorithm has to be imperceptible is the most important requirement [4]. There are two domains for steganography techniques " spatial domain methods and Spread Spectrum Technique "[5][2]. In spatial domain approaches most secret data are embedded in the Least Significant Bit (LSB) of image pixels or by one bit shifting or more. In frequency domain, secret message is embedded in some of the cover media coefficients. In frequency domain cosine transform, wavelet transform….etc are used as transforms [6]. The most essential requirements for data hiding systems are "payload capacity, stego quality, undetectability, and resistance against active attacks". These requirements cannot be provided together. Increasing the size of secret data, usually weakens the "undetectability" and stego quality [7].

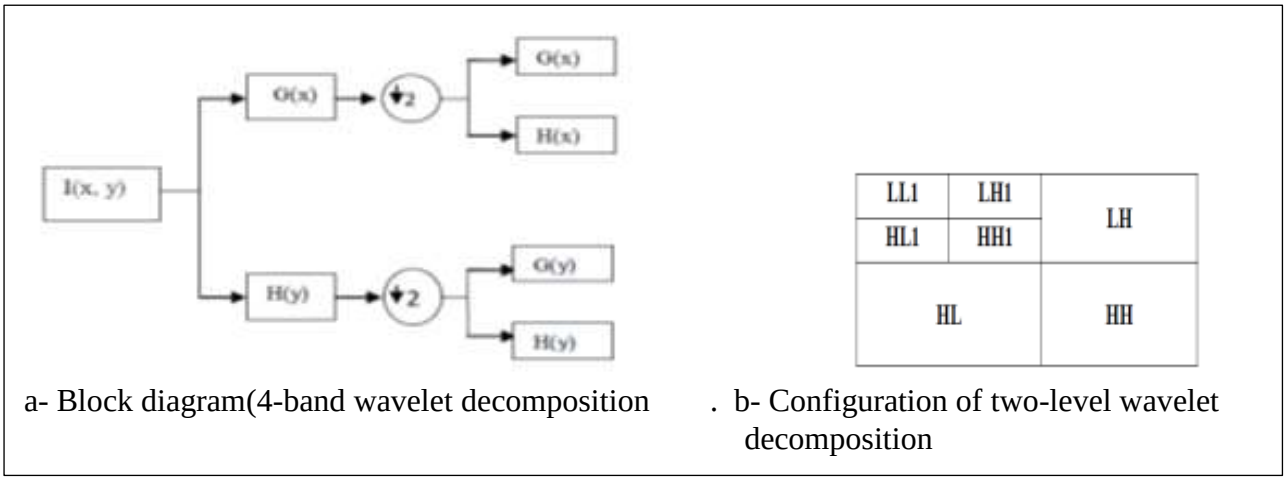
2. Related Works

Abdulla, Alan A. and et. al were interested in originate a novel image operations and steganography schemes that are take advantage of consistencies between secret bits and the cover image LSB plane. they have applied "a bit-plane(s) mapping technique instead of bit-plane(s) replacement" in their paper to hide data[8]. iswarya, Mansi ,Aishwarya and Pallavi presented in 2017 presented image steganography to hide encrypted and compressed audio signal using DCT in RGB image by Transfer the first two bits of audio to last two bits of image. They use PSNR and MSE to estimate quality of stego image,they embed 40231 audio samples in image with size 512×512 [9]. In 2017 Asawari and Dr. Archana proposed in their paper a technique to embed an audio image, this technique include decompose audio by wavelet transform into (cA ,cD) and cover image into (LL,LH,HL,HH) , the approximate coefficient of audio hided in HH and detail coefficients in HL subband,max capacity reach to (106345) samples with PSNR (43)[10].Another method for audio hiding in image steganography based on wavelet suggested by Nitin Kaul and Nikesh Bajaj .they used LSB to embed (10137) samples in cover image[11].

3. Discrete Haar Transform

"Haar wavelet transform" that undergoes for stego_image will be composed at each of the transform level into four bands (LL: low low, LH:low high, HL:high low, HH:high high). The LL-sub band (first sub band) it is the input stego_image filtered with a LPF which cause image compression into half of its main dimension. This band (LL-subbande) contains more energy of Stego_image . The other three subbands, where High Pass Filter (HPF) is applied, are called 'details' (LH, HL, and HH) which hold directional characteristics for example vertical characteristics can be seen in the second subband while the third subband contains characteristics in the horizontal direction finally diagonal characteristics of the input image represented in the last subband (HH-subband). Since image has 2_D, doing wavelet transform twice in each of its level (at row then at column). LPF is defined by G(x) while HPF is defined by H(x). At each level, the HPF associated with detail information; while the LPF inherent with scaling function extract "coarse approximations" [12][13]. For an A x B image, the first level wavelet transformation decomposes the image into four sub-images of size A/2 x B/2, representing the subbands in the frequency domain, The second transformation level decomposes the LL subband "Approximation" of stego_image into another four subimages of size A/4 x B/4, and so on[14]. To reconstruct the original size of stego_image at the recipient, "Inverse Haar Wavelet Transform (IHWT)" should apply

with help of 'details' bands[13], "Fig.1" represent both decomposition based on wavelet transformation. "Daubechies wavelet perform perfect reconstruction conditions for audio signal and it useful for audio compression and denoising" [15], therefore we using (db1) for speech compression and Haar transform for speech hiding because it is the first and simplest and does not have overlapping windows, Haar reverberate changes between neighboring pixel pairs. its filters has (2) taps in both Low pass and high pass.



a- Block diagram(4-band wavelet decomposition . b- Configuration of two-level wavelet decomposition

Fig.1 wavelet decomposition

4. Proposed Algorithm:

The proposed idea falls into two main phases can be seen clearly in "Fig.2" which explain the scheme of proposed algorithm. The included two phases of the algorithm are : first for embedding secret speech after compression in gray cover_ image while the second one is to extract the hidden data from Stego_image then apply decompression on compressed speech. Adopt embedding on LSB for whole subband coefficients to provide more complexity in the way of attackers in order to delay their action.

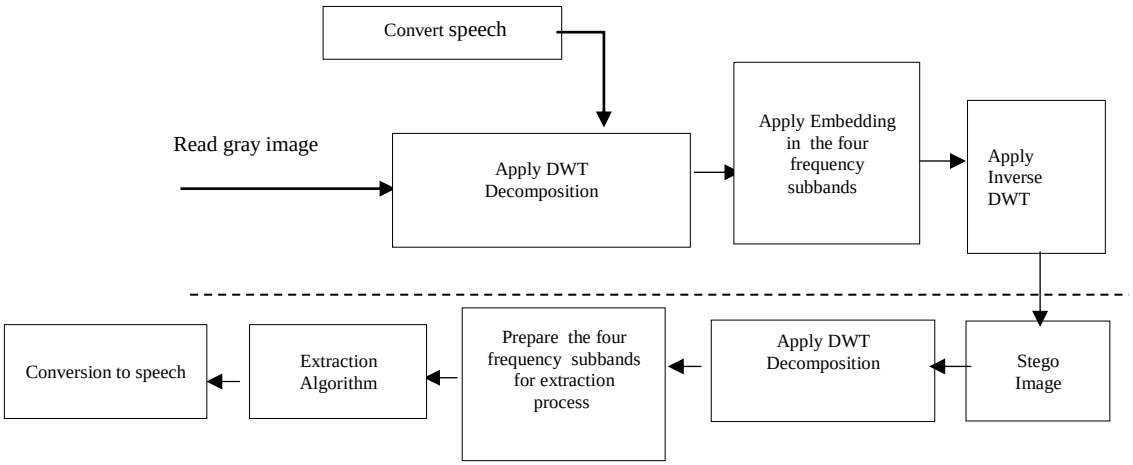


Fig.2. Block diagram of proposed algorithm

a. Embedding Phase :

Define abbreviations and acronyms the first time they are The embedding phase process will be covered by the following steps:

Step 1: Gray image acquisition as a cover_image, decomposed it with DWT [all coefficients with 1/4 size of the original one].

Step 2: Embedded data should be represented in ASCII code.

Step 3: Embedding steps :

- Select frequently cover subband in order to hold one bit from the speech data.
- Bit with (" 0" or " 1") of the data to be inserted [d] by adding it to the value of Subband coefficients [co_value] .

$$m=d+co\_value \quad \ldots..3$$

This process run over the whole speech data.

Step 4 : Processed coefficients will be used to reconstruct stego_image.

b. Extraction Phase :

The suggested method is Non blind steganography so the recipient person needs Cover_image to extract secret data, extracting algorithm is done as:

*/Step*1: The recipient person received stego_image and then, decomposed it by (DWT) into four frequency subbands and specified one of them Sub_stego.

*Step*2: specified the corresponding subband Sub_cover from decomposed cover_image .

*Step*3:compute the variance between Sub_cover and Sub_stego to obtain the difference matrix(Diff_mat).

*Step*4 : rounded each value in Diff_mat to obtain a binary sequence, The process is run over and over till the whole covered speech data will extracted .

Table 1 Show error percentage in extracted data from stego images with different subband

Image size	cA subband	cH subband	cV subband	cD subband
1024×1024	0	3.057861	0.259399	0.357056
512 ×512	0	3.076172	0.793457	1.306152
256 × 256	0	3.369141	0.439453	1.171875

5. Result And Disscussion

MATLAB was used to simulate and to assess the application of the proposed hiding algorithm .

In proposed method speech data compressed using DWT with "daubechies (db1)", Fig.3. show speech before and after compression also extracted speech.

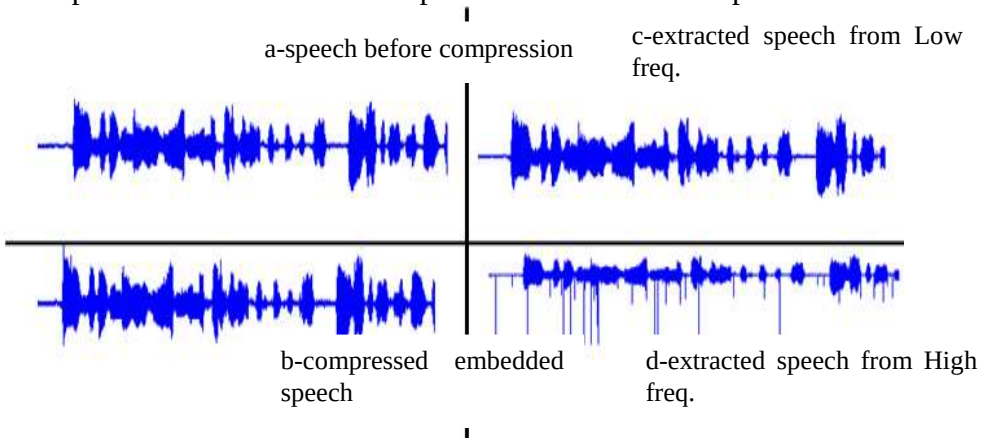


Fig.3. Show speech signal after compression and extraction

Fig.4. show speech data size in kilo byte (KB) before and after compression. To transform the gray cover_image into frequency domain, by applying discrete haar transform, the cover_image will composed into single level:the approximation coefficients matrix cA , details coefficients matrices cH, cV,and cD (horizontal, vertical, and diagonal, respectively) .

The suggested algorithm tested using each subband (cA,cH,cV,cD) which obtained from decompose images with different sizes to embed speech data. Fig.5. show that capacity for hiding data increases according to image size in each subband. Also in Table 1 shows that the error percentage in extracted data changed from one Subband to another, The error rate in retrieved data was the lowest in the subbband CA. Fig.6. shows error percentage in extracted data from each subband.

Metrics are evaluated hiding Efficiency MSE , PSNR and Correlation . the metrics are computed between cover_ image and Stego_image, Fig.7. shows cover image and stego image.

MSE "mean squared error " computed by Equation(1) I_{ij} and K_{ij} are values of pixels at i th row and j th column in cover_image and stego_image respectively[16], shows the MSE and PSNR evaluation .Equation (2) compute PSNR "peak signal to noise ratio" which used for image accuracy measurement, It gives the ratio between the signal (cover_image) and the noise [10].

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}||Iij - Kij| \qquad (1)$$

$$PSNR = 10 \times log\left[\frac{255^2}{MSE}\right] \qquad (2)$$

correlation computed by Equation(3) to show how much the retrieval image "Stego image" similar to the original one "cover image",where $\overline{A}$, $\overline{B}$ = the average of the values in A and B respectively[16].

$$Correlation = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{\left[\sum_m \sum_n (A_{mn} - \overline{A})^2\right]\left[\sum_m \sum_n (B_{mn} - \overline{B})^2\right]}} \qquad (3)$$

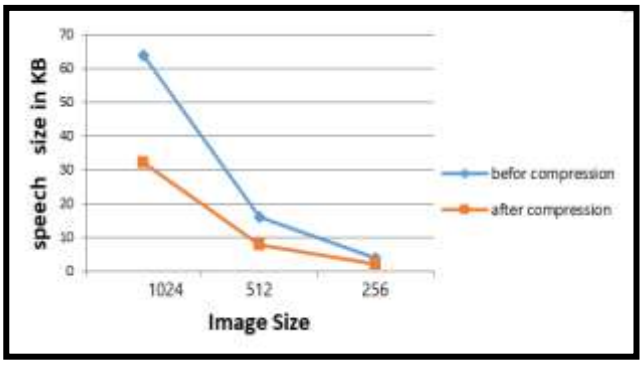


Fig.4. Show speech data size before and after compression

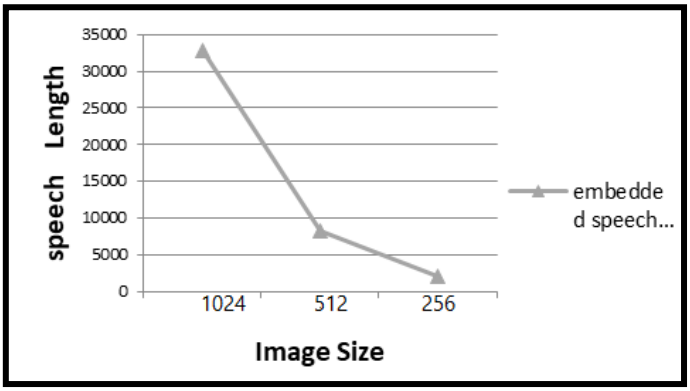


Fig.5. Show embedding capacity according to image size

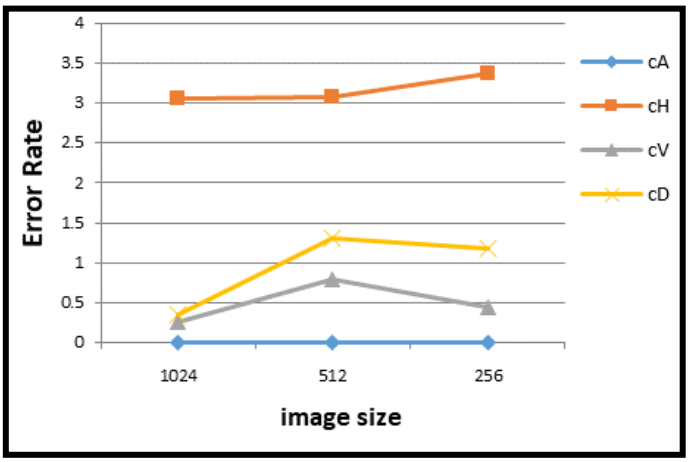


Fig.6. Shows error percentagein extracted data from each subband.

It is obvious from the efficiency coefficients illustrated in Table 2, the Directional subbands (LH, HL, HH) are more suitable for hiding data from the low-frequency subband (LL). Fig.8. shows the normalized values of efficiency coefficients.

Table 2 shown efficiency coefficients for all subbbands (LL,LH,HL,HH)

Image size	Subband Frequency	Correlation	PSNR	SNR	MSE
1024×1024	cA	1	50.48	inf	0.5815
	cH	1	53.4531	21.8028	0.2936
	cV	1	53.47	32.5096	0.2923
	cD	1	53.47	31.0628	0.2923
512×512	cA	1	50.56	inf	0.5713
	cH	1	53.51	21.5253	0.2891
	cV	1	53.52	27.6450	0.2885
	cD	1	53.53	25.4399	0.2881
256×256	cA	1	50.59	inf	0.5670
	cH	1	53.55	21.3271	0.2871
	cV	1	53.56	30.1731	0.2859
	cD	1	53.56	25.9134	0.2858

The suggested algorithm is estimated based on symmetry between original speech data and extracted data. This symmetry between retrieved speech and original speech is evaluated using SNR "Signal to Noise Ratio" calculated by Equation(4). Highest value of SNR means that there is less variance in embedded and extracted data[10]. Fig.9. shows SNR values for three subbands (cH,cV,cD) while the value in cA is infinite because MSE in this subband equal to zero.

$$SNR=10\times\log 10\left(\frac{\frac{1}{N}\sum_{i=0}^{N}x_i^2}{MSE}\right) \qquad (4)$$

a b

Fig.7. shows cover image and stego image

we implement proposed method to embed secret audio in the all details coefficients to calculate maximum embedded data(24576) samples and compare PSNR of stego image in proposed method with previous work [9][10][11] ,the bellow Fig.10. Illustrate PSNR values of A1,A2,A3 and proposed method.

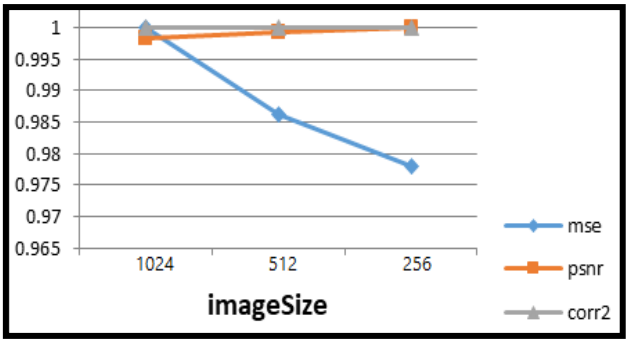


Fig .8. a- Shows PSNR and MSE and correlation for cD

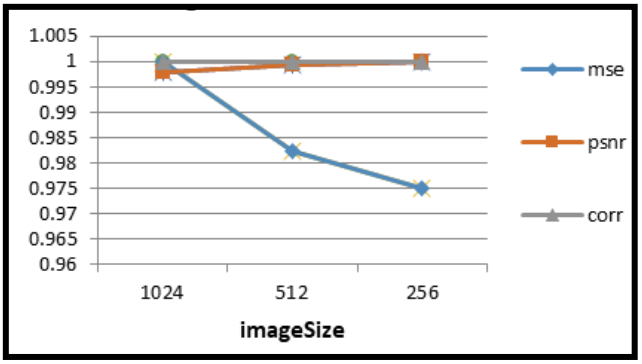


Fig .8. b- Shows PSNR and MSE and correlation for cA

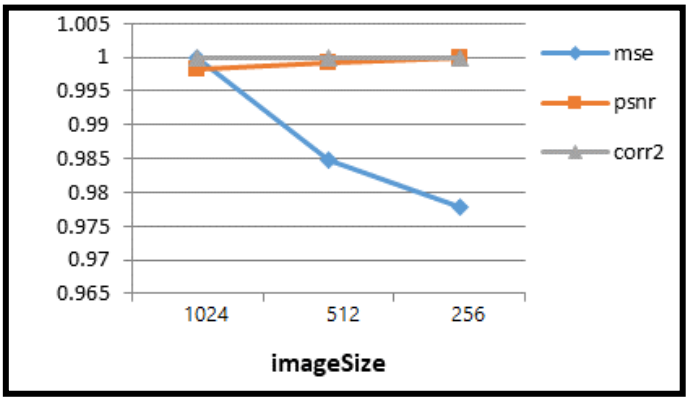


Fig .8. c- Shows PSNR and MSE and correlation for cH

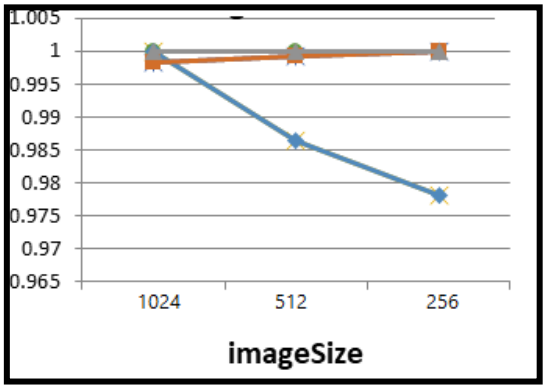


Fig .8. d- Shows PSNR and MSE and correlation for cV

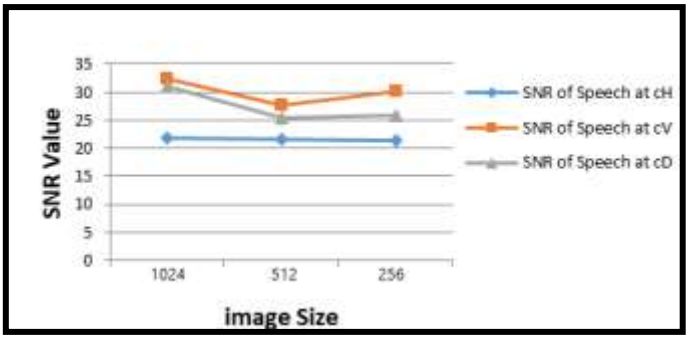


Fig.9. Shows the variation in SNR for each subband

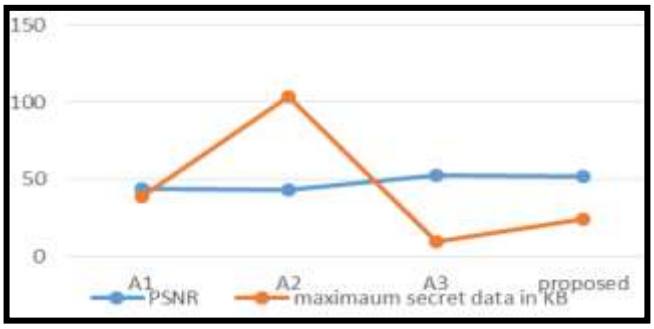


Fig.10. illustrate PSNR values of some previous work and proposed one.

6. Conclusion

From the applied example and according to efficiency metrics measured, the offering algorithm of using DWT coefficients , presents that :

- embedding data in the coefficients of the high pass subband provide powerful in addition to highly secure technique.
- High performance of compressing plus hiding speech data in different images.
- Retrieving secret data was hard and not easy.
- Using intelligent algorithms like ant colony to pick random coefficients for embedding a secret text message.

Conflict of Interests.
There are non-conflicts of interest

References

[1] Piyush Goel. " Data Hiding in Digital Images: A Steganographic Paradigm", M.S. thesis ,Indian Institute of Technology _Kharagpur;.Kharagpur,West Bengal ,India , 2008

[2] R. J. Mstafa and K. M. Elleithy, "Compressed and raw video steganography techniques: a comprehensive survey and analysis," Multimedia Tools and Applications, vol. 76, pp. 21749-21786, 2017

[3] W. Tai , C. Chang, "Data ahiding based On VQ Compressed Images Using Hamming Codes And Declustering ", International Journal of Innovative Computing, Information and Control , Vol.5 ,No.7 ,pp. 2043-2052, Jul. 2009

[4] M. Mohan and P.R. Anurenjan,"A new algorithm for data hiding in images using contourlet transform". in 2011 IEEE Recent Advances in Intelligent Computational Systems (pp. 411-415). IEEE,Sept. 2011

[5] A. Divya. and S.Thenmozhi, " Steganography: Various Techniques In Spatial and Transform Domain", International Journal of Advanced Scientific Research and Management, Vol.1 ,No.3,pp. 81-89 ,mar. 2016

[6] S. Rubab and Dr. M. Younus ,"Improved Image Steganography Technique for Colored Imagesusing Huffman Encoding with Symlet Wavelets", IJCSI International Journal of Computer Science Issues,Vol. 9,No.2 ,pp.194-196,mar. 2012

[7] A. A. Abdulla, S. A. Jassim and H. Sellahewa, " Efficient high-capacity steganography technique" In Mobile Multimedia/Image Processing, Security, and Applications 2013 (Vol. 8755, pp. 875508). International Society for Optics and Photonics, May 2013

[8] A. A. Abdulla, H.Sellahewa and S.A. Jassim, ," Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images" Multimedia Tools and Applications, pp.1-25,Jan.2019

[9] T. Aiswarya , S. Mansi, T. Aishwarya and R. Pallavi ," Steganography technique for hiding secret audio in an image", International Journal for Research in Engineering Application & Management ,Vol.3,No.4 , May 2017

[10] A. S. Shinde and A. B. Patankar ,"Image Steganography: Hiding Audio Signal in Image Using Discrete Wavelet Transform ", in 2017 International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017). Vol.5,No.3 ,pp.331-334 ,March 2017 .

[11] N.Kaul and B. Nikesh, "Audio in Image Steganography based on Wavelet Transform", International Journal of Computer Applications ,Vol.79,No.3 ,Oct.2013

[12] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," IEEE Access, vol. 5, pp. 5354-5365, 2017.

[13] J. Rashmi and G. Bharathi," A Wavelet Transform Based Secure Data Transfer Using Blowfish Algorithm", International Journal of Computer Science and Mobile Computing,Vol.3,No.2,pp. 794-803 ,Feb. 2014

[14] Y.T. Mshari and H. A. Younis ,"Content Based Image Retrieval using Haar Wavelet to Extracted Color Histogram and Texture Features ",International Journal of Computer Science and Mobile Computing,Vol.4,No.8,pp. 322-329 ,Aug. 2015

[15] M. I Mahmoud, M.I. M. Dessouky,S. Deyab and F.H. Elfouly, " Comparison Between Haar And Daubechies Wavelet Transformions On FPGA Technology",in 2007 World Academy of Science, Engineering and Technology, Vol.20,pp. 68-72,Apr.2007

[16] A. Pradhan, A.K.Sahu, G. Swain and K. R. Sekhar," Performance Evaluation Parameters of Image Steganography Techniques", International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016), R. L. Jalappa Institute of Technology, Doddaballapur, Bangalore, India ,2016

الخلاصة

علم الكتابة المغطاة هو واحد من أكثر العلوم شيوعا في مجال امنية المعلوم. في هذا البحث ، سيتم تعديل خوارزمية لتضمين صوتك مكبوس داخل صورة رمادية باستخدام تحويل المويجات المتقطعة (Haar). في البداية تم كبس بيانات الصوت الى نصف حجمها الأصلي ومن ثم تحويل البيانات المكبوسة من الترميز العشري إلى الترميز الثنائي وتضمينه داخل معاملات الحزم الاتجاهية الاربعة (cA :Low Low ,cH :High Low ,cV:Low High,cD:High High) الناتجة من تحليل صورة الغطاء Cover_Image باستخدام تحويل المويجة المتقطع Haar حيث ان cA تمثل حزمة الترددات الواطئة و cD, cV, cH تمثل حزم الترددات العالية .

تم اختبار كفاءة الخوارزمية بقياس معاملات كفاءة الاخفاء (MSE,PSNR,SNR,Correlation) واظهرت النتائج صعوبة اكتشاف المراقب لصورة الغطاء الحاوية على البيانات السرية المطمورة.

تظهر نتائج هذا البحث أنه يمكننا بنجاح إخفاء بيانات الكلام (الصوت) في صورة رمادية ثم استخراجها مع معدل سعة خزن (1) خلية ثنائية (bit) لكل نقطة ضوئية اي ان سعة الخزن باستخدام الطريقة المقدمة يعتمد على حجم صورة الغطاء وكذلك تبين انه معاملات الترددات العالية تكون افضل للاخفاء من حيث عدم ادراك المتطفلين بانه يوجد بيانات سرية داخل الوسط الحامل لها stego_imag.

الكلمات الدالة : الصورة الرمادية ,الكتابة المغطاة ,تحويل المويجة المتقطعة haar ,صورة الكتابة المغطاة