Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Hiding Technique in Frequency Domain

Professor Dr. Saad Najim Al-Saad
Computer Sciences, AL- Mustansiriyah University
Iraq

Lecturer, Ahlam Mejeed Kadum
Physics, AL-Mustansiriyah University
Iraq

***Abstract-** In this paper hiding technique using adaptive method for discrete wavelet transform (DWT)has been proposed for the purpose embedding speech message signal (8bit resolution, 8 KHZ) or to hide color image message signal (24bit resolution) within speech cover signal. The algorithm that has been used in this work is integer to integer lifting wavelet transform (Int2IntLWT). The proposed algorithm showed high security and high embedding capacity. Least significant bits (LSB) used to replace bits of message in the coefficient of detail sub-band1 and detail subafter implemented two levels of Int2Int LWT. Secret message data is encrypted using chaotic key generation1 (CKG1) to mixing and changing randomlysamples or pixels of secret message locations. Two chaotic keys are used as secret keys (CKG2, CKG3) with embedding stageto select random coefficients and replace its LSB bits with bits of secret message. The proposed method offers lossless and unnoticeable changes in the quality of the host speech file and imperceptible by human auditory system (HAS).*

***Keywords:** Speech steganography, color messageor sound message hiding, (LSB) technique, DWT, Int2Int LWT.*

I. INTRODUCTION

The traditional conversions such as Discrete Cosine Transform (DCT), Discrete Furrier Transform (DFT), and DWT have been used for hiding data in frequency domain. All these methods provide high embedded data and good quality for the stego file, but the main disadvantage in these conversions is in the require information type transformation(from integer-to-floating and vice versa)[1].

In all these methods there is a need to scaled coefficients which are converted to binary, to embedsecret message by replacing LSBs coefficients with bits of message. Subsequently, the message bits are embedded in the LSBs of the binary scaled coefficients. The reconstruction of the stego signal is achieved by descaling and inverting the DWT (IDWT) processes.Theerrorscould beoccurring inthe messages thatrecoveredbecause of thelosinghas occurredinroundingoperations.Toreduction and eliminationthis type of errorin retrieve hidden data there is need to technique avoid this errors [1].

In 1996, Swildens[2] displaysInt2IntLWT for a fastDWT, which can be easily achievedby the computer due to the greatreductionin calculations. This approachis totally based onthespatial performance ofthe DWT. In addition, it provides the capability to fabricate new motherwaveletfor theDWT, based onproperties time-space domain.In liftingscheme the structuralprocessing elements are arranged, including multipliers are adjustment sequentially. The major challengesin thebuildings devices for1-D DWTis thespeed processingand thenumber ofmultiples, where the memoryissue which dominate the hardware costand complexity of thearchitecture. The reason for thisis the reduction ofthe on-chipmemory and power consuming[2].

II. LWT STRICTURE

Let us that we have speech signal$(x = x_k), k \epsilon \text{z}$ with $x_k \epsilon \text{R}$, consider that signal divided to disjoint set of samples which is called even indexed set $(x_e = (x_{2k}), k \epsilon \text{z}$ or evens for short, and the odd indexed set $(x_o = (x_{2k+1}), k \epsilon \text{z}$ or "odds". These two set are correlated each with other, so that one can be consider a good predictor (P) for the other set, e.g. Because of the predictor need to be exact, so the difference or detail (d) need to be exact:[3, 4]

$$d = x_o - P(x_e) \ldots (1)$$

The odd can be recovered by reversible transform as:

$$x_o = P(x_e) + d \ldots (2)$$

Predictor for add set x_{2k+1} is the average of its two even neighbors; detail set is as follows (in case of Haar filter for linear waveform):

$$d_k = x_{2k+1} - \frac{(x_{2k}+x_{2k+2})}{2} \ldots . (3)$$

Another lifting step has been proposed, even set is replaced with smother (s) by use updater (U) that achieved on detail set (d):

$$s = x_e + U(d) \ldots . (4)$$

In reversible transform this step is trivially: given (s, d) the even set recovered as:

$$x_e = s - U(d) \ldots (5)$$

It is easy to see that an update operator in case of Haar filter for linear waveform given as:

$$s_k = x_{2k} + \frac{(d_{k-1} + d_k)}{4} \dots (6)$$

The block diagram of the two lifting steps is given in Figure 1.

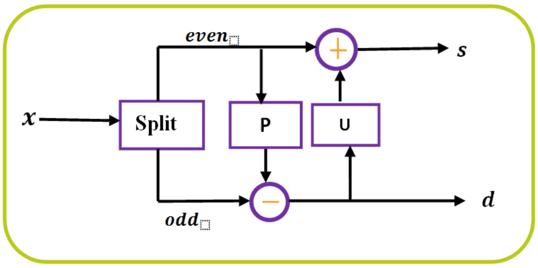

Figure 1 Block diagram of lifting steps

III. CHAOTIC SYSTEM

The chaotic systems have been used in the field of cryptography applications by Digital techniques,these algorithms are based in iterative computations of chaotic functions that produce digital signals. Then, basic cryptographic operations (substitution and mixing) are used to mask the clear message with the chaotic signals. These cryptosystems involve one or more chaotic systems in the algorithm and use their initial conditions and /or control parameters as secret keys[5, 6].

One of the simplestchaoticfunctionsthat have been studiedinapplications tocryptographicis the logisticsmap. The following equation describes the logistic map function for chaotic key Generator CKG [6, 7]:

$$\boldsymbol{y_{n+1} = r . y_n . (1 - x_n) \dots\dots (7)}$$

Where y_n have values in rang [0, 1], and the parameter(r) is a positive real number takes values (3.6 to 4). The chaotic system has different Characteristics with parameter (r, x) and length of key which is named bifurcation parameter, it's decides and explores the attributes of the logistic map. One of the numbers in the rage can be changed to get a new key. The main feature of CKG is its higher sensitization to change one or both of the initial conditions (r, x)[6].

IV. THE PROPOSED SYSTEM DESIGN

The basic design ofthe proposed steganography systemconsists oftwo phases, embeddingand extraction. The embedding phase consists of two stages and carried out by message senderside. Extractionphaseiscarried out bythe receiver messageside. The general structure of the proposed system is illustrated in figure (2).

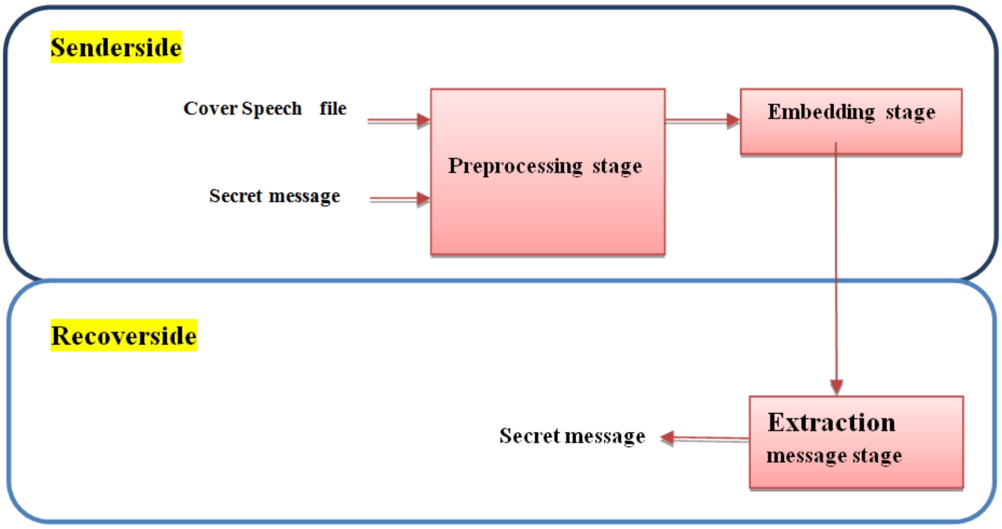

Figure (2) Block diagram of the proposed system

4.1 Embedding phase

Format of the sounds cover is (.wav) with sampling frequency 8 KHz, 1 channel for speech sounds. The length of frame is 512 samplesand time of each frame is 64 mile sec,total number of frames in tested cover file is 3750 frames. Int2IntLWT and DWT have been implemented to each frames of cover. The bits resolution for each sample is 16 bits. The two main stages of embedding phase are as follows:

1. Preprocessing stage.
2. Embedding stage.

4.1.1 Preprocessing Stage

The preprocessing stage is depicted in Figure (3).This stage contains two steps:

Comparing: This step consists of two inputs signals (matrix of encrypted message and sound cover file). A comparisonbetween thesize of the messageand the size ofcover has been calculated to ensure the cover file size is enough for embedding.

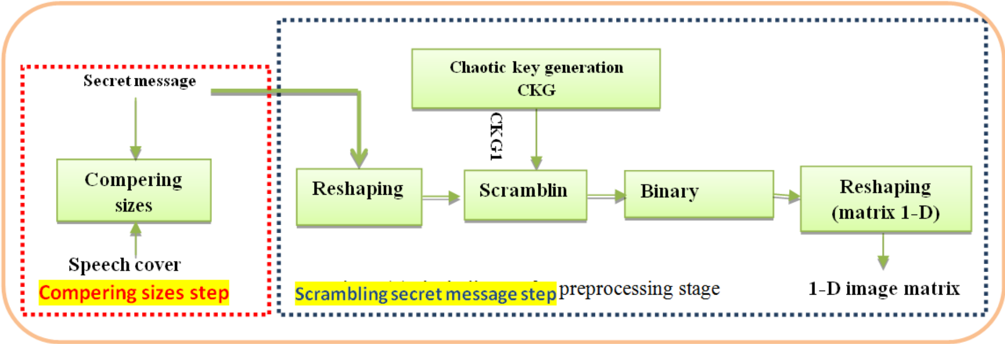

Figure (3)Block diagramfor preprocessing stage

Scrambling secret message: The aim of this stage is produce stego speech file. As depicted in figure (3) the combination oftwo known techniques (cryptography and steganography) has been using for hiding image or sound performed, encryption secret message achieve by using CKG1. The pixels or samples locations of messagearemixing andarrangementin randomlocations different from original locations. If thesecret messageis image the resulting from preprocessing stageappeared like set color mixedwith each other and do not seemanyfeatures for theoriginal image, andif the message issound theoutputsound as a resulting to this stageis merelynoise.The algorithm of this stage is listed in algorithm (1):

Algorithm (1): Preprocessing stage

Input: Image // Secret message (color image)
Cover // Cover speech file
CKG 1 // Chaotic Key Generation
B // Length of frame

Output: Scrambled image

Began

Step1: Reade secret image and calculate its size

$$msg \leftarrow imread\ (Image)$$

$[c1\ c2\ c3] \leftarrow size(msg)$

Step2: Reade speech file and findingits bits resolution (nbits) and rate samples(F_s) its size

$[\,\mathrm{Y}, F_s, nbits] \leftarrow$ wavered (Cover) // Store speech file in matrix Y

$[\mathrm{c4}\ ,\mathrm{c5}] \leftarrow \mathrm{size(Y)}$

Step3: Calculate size secret message and size of cover file

$Len \leftarrow c1 * c2 * c3 * 8$

$L \leftarrow c4 * c6 * nbits$

Step3: Calculate total numberof frames in speech file$(\mathrm{Frm_{cov}})$andtotal frames that will be needed to hide message$\mathrm{Frm_{msg}}$

$$\mathrm{Frm_{cov}} \leftarrow \frac{\mathrm{L}}{\mathrm{B}}$$

$\mathrm{Frm_{msg}} \leftarrow \frac{\mathrm{Len}}{\mathrm{X} * (\frac{\mathrm{B}}{2} + \frac{\mathrm{B}}{4})}$

Step4: Compering the size cover with size message in bits

$$\text{If } \mathrm{Frm_{msg}} > Frm_{Cov}$$

Error $\leftarrow$ Message Box (Cover is small to hide this message)

Break

Step5: Reshaping secret image from matrix in 3-D to matrix in 1-D and scrambled result matrix by using CKG1

$msg1 \leftarrow reshape(\,msg\,, 1, c1 * c2 * c3)$

$msg22 \leftarrow reshape(msg2, c1, c2, c3)$ // the result matrix in 3-D is the scramble image

$desiply \leftarrow show(msg22)$ // Show Scrambled image on screen computer

Step6: Converted msg2 from decimal to binary with 8 bites for each pixel

$msg3 \leftarrow dec2bin(msg2{,}8)$

Step7: reshaping msg3 from matrix 8 column to matrix 1 column and calculate length matrix

$msg4 \leftarrow reshape(msg3{,}1, size(msg3))$

$Len \leftarrow length(msg4)$

End

4.2 Embedding Stage

The steps of this stage are depicted in figure (4).Two levels of Int2IntLWT or DWT have been implemented on cover, the result is four sub bands:High-sub band1 and low-sub band1 (256 coefficients), high-sub band2, Low-sub band2 (128 coefficients).

Hiding process of secret message is achieved by replacing LSB bits ofcoefficientsfor high sub-band1and high sub-band2.The totalreplaced bitsare 384 bits.

The total number ofsum elements matricesofhigh sub-band1and high sub-band2 is exploitation in hiding process. The number hidden bits of secret messageineachframeincrease 384bitwith increasing number of replacedbitsonebit.Digital matrix of secret message is segmented the in to blocks, each block consists of set of bits. Each one of block bits was being hidden in one frame of cover.At embedding step the LSB is used for replacement with two chaotic keys CKG2and CKG3 are used to generate random values with length 256 and 128 respectively.

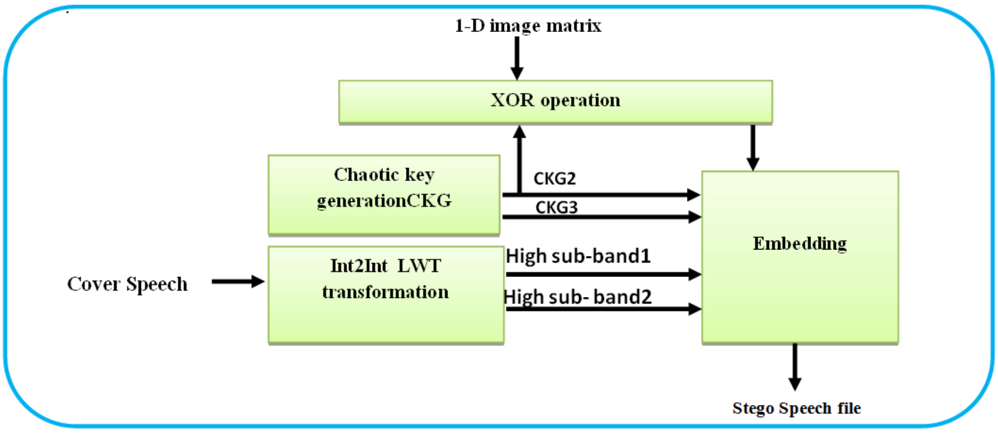

Figure (4)Block diagramfor preprocessing stage

The second step of encoding secret message is achievingby implementing XOR operation for the matrix message that resultingfromthe preprocessing stage with real numbers bits which are produced by using CKG2. XOR operation is implemented during the embedding process.The embedding stage algorithm is listed in algorithm (2):

Algorithm (2): Embedding secret message

Input: Cover // Cover speech file

Msg4 // Binary matrix of secret message

X // Number LSB replaced for each coefficient of Int2IntLWT

B // Length each frame

CKG2, CKG3 // chaotic keys using in selection hiding positions

Output: Stego // Stego file that contains embedded secret image

Begin:

Step1: Reade speech file and calculating its length and size

Y← wavered (Cover) // Store speech file in matrix Y

L ← length(Y)

Z ← size(Y)

Step2: Calculate total numberof frames in speech file and that will be needed to hide message

$$\text{Frm}_{\text{cov}} \leftarrow \frac{L}{B}$$

$$\text{Frm}_{\text{msg}} \leftarrow \frac{\text{Len}}{X * (\frac{B}{2} + \frac{B}{4})}$$

Step3: Test if the size of speech file is enough to hide secret message

If $\text{Frm}_{\text{msg}} > Frm_{\text{Cov}}$

Error ← Message Box (Cover is small to hide this message)

End if

Step4: Beginning hiding process for all framesof speech file that needed to embedded message

Begin

$For\ i \leftarrow 1\ to\ \ Frm_{msg}$

F1 ← 0

F2 ← 1

$Frm \leftarrow Y(F1 * B + 1: F2 * B)$

[low1 $(1:\frac{B}{2})$, high1 $(1:\frac{B}{2})$]←Int2Int LWT (Frm) // Implemented 2 levels of Int2Int LWT on frame
[low2 $(1:\frac{B}{4})$, high2 $(1:\frac{B}{4})$]←Int2Int LWT (low1)
Replacing LSB of matrixes coefficients high1 and high2with block bits message
$For\ j \leftarrow 1\ to\ X$
$high11\left(1:\ \frac{B}{2}\right) \leftarrow replace\ (high1(CKG2\left(1:\ \frac{B}{2}\right)), j, msg4\left(1{:}\left(\frac{B}{2}\right)\right))$
End if // j
$For\ k \leftarrow 1\ to\ X$
$high22\left(1:\ \frac{B}{2}\right) \leftarrow replace\ (high2(CKG2\left(1:\ \frac{B}{4}\right)), j, msg4\left(1{:}\left(\frac{B}{4}\right)\right))$
End if // k
$hig1 \leftarrow InversInt2It\ LWT[low2, hig22]$ // Implemented invers Int2IntLWTfor two levels
$D1 \leftarrow InversInt2It\ LWT[low1, hig1]$
$YY(F1 * B + 1{:}F2 * B) \leftarrow D1$ // Store output frame in stego speech file

V. EXTRACTION STAGE

Figure (6) shows the steps of extraction stage. It is implemented as the same way of embedding stage but in reverse form

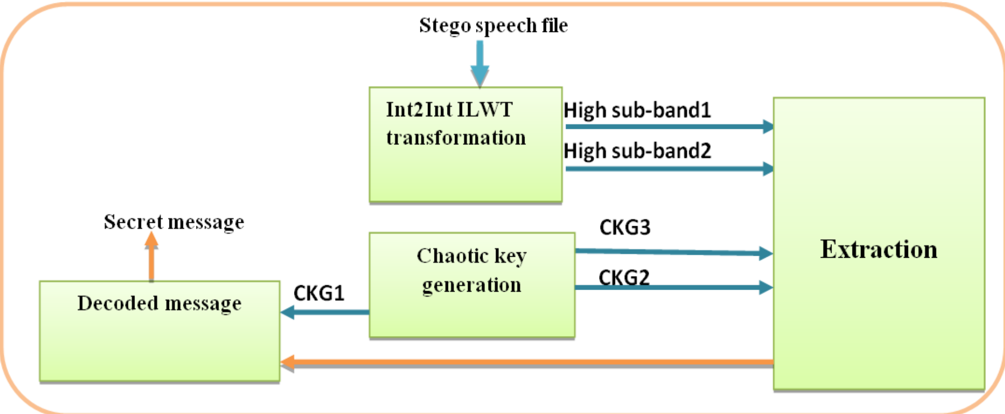

Figure (5) Block diagram for extraction stage

VI. EXPERIMENTAL RESULTS

Several experimental results have been conductedusing four speakers(twofemales andtwo males).The timefor each speech filesis four minutes. The experimental results are considered from two perspectives, the first one from cover file perspective and the second one from secret message (image or speech) file perspective.

Stego Lena image by LWT Original Lena image Stego Lena image by DWT

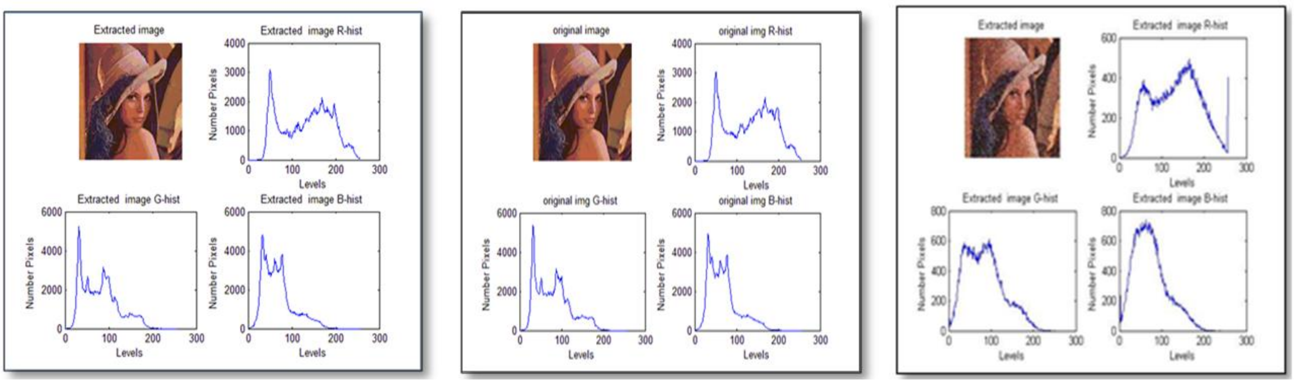

Figure (6) Histogram for components (RGB) of Lena image for original image, extracted image by LWT, extracted image by DWT.

Figure 7 show the histogram for speech secret message as original form. The two histograms are figured,the left one extracted by Int2IntLWT and the right one on the right side the histograms point that the speech extracted from by Int2IntLWTis closed to the original rather than speech extracted by DWT.

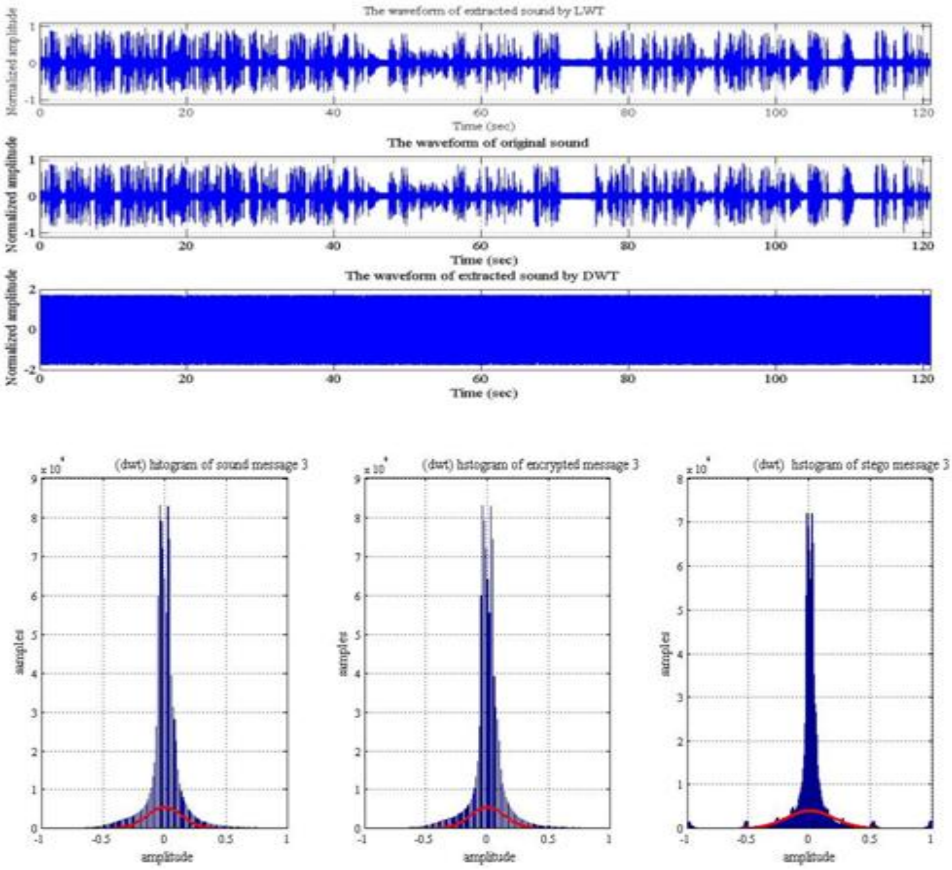

Figure (7) Histogram and waveform fororiginal sound, extracted sound by LWT, extractedsound by DWT for sound secret message.

Table (1) measurements of hiding sound message (2 minutes) within speech file (4 minutes) using LWT

cover name	number replaced bits	Run time sec	SNR db	SNRseg db	SNRspc db	MSE	R_{xy}
female1	4	75.093701	25.2662	42.9236	45.9527	4.6832e-06	0.9852
	6	46.246519	37.0823	37.7377	30.6940	2.1420e-05	0.8928
	8	40.546171	18.1191	18.9847	21.9407	1.2892e-05	0.8598
	10	39.030017	5.6084	6.8732	9.0596	1.9298e-04	0.7263
fremale2	4	76.160499	37.9484	40.9902	44.0345	1.6235e-07	0.9724
	6	59.789818	27.4321	28.0859	31.1528	9.9374e-07	0.8634
	8	46.836198	13.7820	15.1975	18.1524	1.4537e-05	0.7273
	10	39.674871	1.0249	2.7009	4.7078	2.1247e-04	0.5937
male1	4	78.288991	42.2731	42.5332	45.5977	8.5342e-08	0.9881
	6	57.663274	30.2783	30.5828	33.6316	9.2334e-07	0.9330
	8	46.668153	17.4341	18.2436	21.0292	1.2562e-05	0.8501
	10	40.543313	4.8812	6.0975	7.8694	1.9572e-04	0.7018
male2	4	78.843726	38.4430	40.5040	43.5593	1.2973e-07	0.9956
	6	57.465477	28.4453	28.6725	31.7340	9.0643e-07	0.9859
	8	47.165034	15.6543	16.2027	18.7644	1.2323e-05	0.9328
	10	40.367314	2.0741	2.9440	4.3405	2.0770e-04	0.6858

a. Cover file perspective**:**

Table1and 2 declares five objective measurements that are implemented for Lena image. Table 1 and 2 declare the measurements of Int2IntLWT and DWT respectively. The measurements point the quality of Int2IntLWT is more effective than DWT. Also table 3 and 4 are declaring for the same result when the secret message is speech.

b. Secret file perspective:

Figure 6 and 7 show comparison between the quality of secret message (image and speech) by using DWT and Int2IntLWT respectively. Figure 6 illustrate that for secret message (Lena) that extracted from Int2IntLWT is clearer than Lena image extracted the DWT. The histograms of the figure support that the idea.

Table (2) measurements of hiding sound message (2 minutes) within speech files (4 minutes) using DWT

cover name	number replaced bits	Run time sec	SNR db	SNRseg db	SNRspc db	MSE	R_{xy}
female1	6	126.32264	33.5135	33.3563	36.2505	9.9225e-07	0.9512
	8	102.33661	22.1578	29.7409	31.7601	1.3558e-05	0.8842
	10	88.494732	10.3744	20.4740	23.4269	2.0442e-04	0.7501
fremale2	6	128.18788	32.0886	33.0722	35.7826	1.0550e-06	0.8906
	8	103.31946	20.6007	18.0552	21.0193	1.4861e-05	0.7800
	10	88.907806	8.8415	17.1506	20.3860	2.2283e-04	0.6421
male1	6	129.638551	32.2804	32.2293	35.2556	9.8904e-07	0.9528
	8	102.261992	20.9745	20.0997	23.0082	1.3360e-05	0.8697
	10	90.192607	9.0919	35.8173	38.2483	2.0609e-04	0.7282
male2	6	129.012821	31.3839	30.5352	33.5272	9.6375e-07	0.9892
	8	104.813462	20.1105	23.3031	25.5184	1.2921e-05	0.9409
	10	95.338978	7.9361	18.2179	20.9772	2.1318e-04	0.7459

Table (3) measurement for hiding Lena image (512*512) within speech file (4 minutes) using LWT.

cover name	number replaced bits	Run timesec	SNR db	SNRseg db	SNRspc db	MSE	R_{xy}
female1	6	170.944758	30.5255	30.7450	33.8158	1.8195e-06	0.9420
	8	129.914342	17.0110	18.6924	21.6420	3.1337e-05	0.8677
	10	108.554049	5.2050	6.4452	8.6766	3.8694e-04	0.7249
fremale2	6	168.183745	28.896	29.4841	32.5412	1.9897e-06	0.8672
	8	135.452409	15.6055	16.7605	19.7394	2.7844e-05	0.7582
	10	115.360735	2.3473	3.9022	6.0993	4.2115e-04	0.6285
male1	6	172.335422	29.5169	29.7940	32.8294	1.8401e-06	0.9385
	8	133.899631	17.4367	18.3724	21.1543	2.5989e-05	0.8548
	10	111.060060	4.7313	5.9337	7.6580	3.8966e-04	0.7037
male2	6	178.693643	28.359	28.5172	31.5740	1.8065e-06	0.9872
	8	135.669186	15.3795	16.1597	18.7585	2.6267e-05	0.9187
	10	116.023805	2.6365	3.5133	5.0326	4.1279e-04	0.6941

Table (4) measurementfor hiding Lena image (512*512) within speech files (4 minutes) using DWT.

cover name	number replaced bits	Run time sec	SNR db	SNRseg db	SNRspc db	MSE	R_{xy}
female1	6	142.32264	28.0125	30.7624	33.7994	1.0785e-06	0.9406
	8	118.33661	20.2730	18.6912	21.5878	6.4084e-06	0.8700
	10	109.494732	8.3776	6.4101	8.5656	9.9150e-05	0.7188
fremale2	6	140.185927	23.0825	29.0302	32.0421	2.5645e-06	0.8697
	8	119.985373	18.6929	16.2564	19.1114	7.0464e-06	0.7583
	10	105.997294	6.9676	3.4716	5.5435	1.0483e-04	0.6120
male1	6	140.826537	28.9784	30.2733	33.2991	6.4582e-07	0.9416
	8	117.277074	19.0530	18.2795	21.0117	6.3482e-06	0.8525
	10	106.628252	7.0295	5.6963	7.3487	1.0116e-04	0.6931
male2	6	138.298899	28.6313	28.3945	31.4098	5.5536e-07	0.9858
	8	115.692198	18.0927	16.3337	18.8796	6.2869e-06	0.9234
	10	100.194249	5.9092	3.3968	4.7740	1.0394e-04	0.6927

VII. CONCLUSIONS

From notes the previous four tables(2, 4), it is found that the quality of stego sounds is lower than that presents in tables (1, 3) which represent the results of hiding Lena image and sound message within speech files. The distortion associated hiding in sound files by using DWT technique come from two operations:

- Errors as a result of embedding secret message within speech cover.
- Errors as a result of rounding operation to get integer numbers from floating number of coefficients that getting from implemented DWT for speech cover file.

REFERENCES

[1] Haider Ismael Shahadi, [2] RazaliJidin and [2] Wong Hung Way, *A Novel and High Capacity Audio Steganography Algorithm Based on Adaptive Data Embedding Positions*, Research Journal of Applied Sciences, Engineering and Technology 7(11): 2311-2323, 2014 ISSN: 2040-7459; e-ISSN: 2040-7467 , March 20, 2014.

[2] INGRID DAUBECHIES AND WIM SWELDENS, 1996,*FACTORING WAVELET TRANSFORMS INTO LIFTING STEPS*, Princeton University, Princeton, New Jersey

[3] Sayed Ahmad Salehi and RasoulAmirfattahi, *VLSI Architectures of Lifting-Based Discrete Wavelet Transform*, Isfahan University of Technology, Department of Electrical and Computer Engineering,, Isfahan Iran , Prof. HannuOlkkonen (Ed.), ISBN: 978-953-307-482-5, InTech, Edited by Prof. HannuOlkkonen.

[4] INGRID DAUBECHIES AND WIM SWELDENS, *FACTORING WAVELET TRANSFORMS INTO LIFTING STEPS,* September 1996, revised November 1997.

[5] Pellicer-LostaoCarmen **,***Notions of Chaotic Cryptography:Sketch of a Chaos Based Cryptosystem***,** Department of Computer Science and BIFI, University of Zaragoza,Spain , 2012 www.intechopen.com.

[6] Jamal NasirHasoon ,*Speech Hiding Using Vector Quantization*, thesis, University of Mustansiriyh, January 2014.

[7] Dipankar Pal , *A Robust Audio Steganographic Scheme in Time Domain (RASSTD),* International Journal of Computer Applications (0975 8887)Volume 80 - No. 15, October 2013 Kalyani, Nadia-741235, West Bengal, India.