Diyala Journal of Engineering Sciences

ISSN 1999-8716
Printed in Iraq

Vol. 05, No. 02, pp. 99-113, December 2012

DESIGN & EVOLUTION OF A STEGANOGRAPHY SYSTEM FOR SPEECH SIGNAL BY SLANTLET TRANSFORM

Tarik Z.Ismaeel[1], Ahlam Hanoon[2]
University of Baghdad, College of Engineering
Electrical Eng. Dept .[1], Computer Eng. Dept.[2]
(Received:20/9/2011 ; Accepted:29/1/2012)

ABSTRACT: In this paper a Stegan graphic system was proposed to hide up a secret speech signal in a cover speech signal, using Slant let transform. The combination of a Stegan graphy and cryptography is used to increase the level of security and to make the system more rigid and complex to be defeated by attackers. In cryptography the secret speech signal is converted from 1-D to 2-D signal, divided into blocks each of size (8*8) sampled and then the samples are converted to the binary form, after that, columns transposition is applied to get the ciphered signal. This cipher signal will be the next stage, we are driving the key which is used in cyphering process from the slantlet coefficients.

The proposed system increases the imperceptibility property because it is based on replacing each secret bit with one of the host coefficient bit (the host coefficient may be the same as secret bit). So that changing of host signal due to embedding process was decrease d but the dimension of the cover signal will be a tradeoff between the imperceptibility and the capacity of the system. Imperceptibility and security test s are implemented to check the system. Peak signal to Noise Ratio(PSNR) & Correlation(Corr.) between cover signal & the stego - signal are carried out to evaluate the perform ance of the proposed algorithm.
Keywords: ".wav" file, Slantlet transform, PN, Corr, PSNR.

1- INTRODCTION

Steganography is the art of invisible communication. The term invisible is not linked to the meaning of the communication, as in cryptography in which the goal is to secure communications from an eavesdropper; on the contrary it refers to hiding the existence of the communication channel itself. The general idea of hiding messages in common digital contents, interests a wider class of applications that go beyond Steganography[1]. Depending on the meaning and goal of the embedded metadata, several information hiding fields can be

defined, even though in literature the term 'information hiding' is often used as a synonym for Steganography. In digital watermarking, for instance, the information is used for copy prevention, copy control, and copyright protection. In this case the embedded data should be robust to malicious attacks in order to preserve its goal[1]. The dual goal of Steganography pertains to S teganalysis by Steganography. For each Steganographic method, several techniques(i.e. *targe t*) *Steganalysis*[5 -7], i.e. techniques that are designed to detect the widest possible range of Steganography.

A common Steganographic algorithm known as §1 embedding, also called LSB matching, which, is a common used technique to embed message in the pixel domain. Due to its simplicity, efficiency, and its undetectability, §1 embedding is often used as a benchmark for Steganalysis and Steganography. This simple evolution from classical LSB is highly undetectable especially when the length of the embedded message is smaller than the length of the in military dictatorship countries or connected to homeland security. Steganography has also been supposed to be used by terrorists to design terroristic attacks. Example, about the terrorism is the technical jihad manual. [8]

2- CRYPTOGRAPHY

Cryptography can be defined as the area within cryptology that is making communication unintelligible to all except the intended recipient [9]. In the cryptography, the structure of a message is changed to render it meaningless and unintelligible unless the decryption key is available. Cryptography makes no attempt to disguise or hide the encoded message.

3- CRYPTANALYSIS

The science of breaking cryptosystems is called cryptanalysis. It is the area within cryptology which is concerned with techniques for deciphering encrypted data without prior knowledge of which key has been used [9].

Cryptanalysis could be defined as the process of attempting to discover the plaintext or key. The strategy used by the cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst [10].

4- SLANTLET TRANSFORM (ST) [11].

Slantlet transform is based on an improved version of the usual discrete Wavelet transform (DWT) where the support of discrete-time basis functions is reduced (Selesnick, 1999;Pratt et al.,1972).The DWT is usually implemented in form of an iterated filter bank, where a tree structure is utilized. ST owes its inspiration from an equivalent form of the DWT implementation, where filter bank is devised in form of a parallel structure, with some of the parallel branches employing product form of basic filters. "Slantlet" filter bank employs a similar parallel structure (Selesnick, 1999; Pratt et al.,1972). However, the component filter branches do not rely on any product form of implementation and hence ST possesses extra degrees of freedom. Fig.(1) Shows an equivalent form of two-scale orthogonal DWT iterated filterbank with two zero moments, called D_2 (proposed by Daubechies) and the corresponding filterbank realized using ST, which maintains desirable properties of orthogonality and two vanishing moments (Selesnick, 1999). Here, different filters are conceived for each scale. For the case in Fig.1, iterated D_2 filters are of lengths 10 and 4, while the corresponding Slantlet filters are of lengths 8 and 4, respectively. As we keep on increasing the number of scales (and subsequently number of parallel branches), the difference in the number of supports keeps growing. While iterated D_2 filters require $(3.2^i - 2)$ supports at the ith scale, Slantlet filters require 2^{i+1}supports. Hence, Slantlet filters can be implemented with shorter supports and they can yet maintain all desirable, characteristic features of iterated DWT filterbanks. Each type of filter bank is orthogonal, has an octave-band characteristic, has same number of zero moments and provides a multiresolution decomposition. In fact, while iterated DWT filters can approximately provide a scale-dilation factor of 2. Slantlet filters can exactly provide a scale-dilation factor of 2. Slantlet filters are essentially piecewise linear filters and are particularly suitable for analyzing piecewise linear functions with discontinuities. However, due to the shorter supports of component filter, ST provides A filter bank which is less frequency selective, than DWT, although ST Provides better time-localization compared to DWT. To provide a mathematical perspective of Slantlet transform, let us fall back on a generalized representation of Fig.1, for l scales. Let $g_i(n)$, $f_i(n)$ and $hi(n)$ be the filters employed in scale i to analyze the signal, where each of these filter has an exact support of 2^{i+1}. For l scales, ST filter bank employs l number of channel pairs, i.e. a total of $2l$ channels. Hence, the low pass filter $h_i(n)$ is paired with its adjacent filter $f_i(n)$, where each filter is followed by a down sampling by 2^i .ach of the other $(l\text{-}1)$ channel pairs constitutes of a $g_i(n)$ filter and its shifted time-reversed version ($i=1,2,3,.....,l\text{-}1$), followed by a down sampling by

2^{i+1}.The filters $g_i(n)$,$f_i(n)$ and $h_i(n)$ are implemented in piecewise linear forms and they can be represented

as: $g_i(n)=\begin{cases} ao,o+ao,1n, & \text{for } n=0,...,2^{i}-1 \\ a1,o+a1\,1n, & \text{for } n=2^{i},...,2^{i+1}-1 \end{cases}$ .....(1)

$h_i(n)=\begin{cases} \text{bo,o} + \text{bo,1n}, & \text{for n} = 0,...2^{\text{i}}-1 \\ b1,o+b1,1n,, & \text{for n} = 2^{\text{i}},...,2^{\text{i+1}}-1 \end{cases}$ .....(2)

$f_i(n)=\begin{cases} co,o+co,1n, \text{ for n} = 0,...,2^{\text{i}}\text{ -1} \\ c1,o+c1,1n & \text{for n} = 2^{\text{i}},...,2^{i+1}-1 \end{cases}$ .....(3)

The objective is to determine the parameters as, bs and cs, to perform the filter design procedure for each *i*th scale. These filters must satisfy the following constraints, which, in turn, satisfy orthogonality and two vanishing: moments

(a) each of $g_i(n)$, $f_i(n)$ and $h_i(n)$ is of unit norm, i.e.

$$\sum_{n=0}^{2^{i+1}-1} g_i^2(n)=1 \qquad .....(4a)$$

$$\sum_{n=0}^{2^{i+1}-1} f_i^2(n)=1 \qquad .....(4b)$$

$$\sum_{n=0}^{2^{i+1}-1} h_i^2(n)=1 \qquad .....(4c)$$

(b) $g_i(n)$ is orthogonal to its shifted time reverse, i.e.

$$\sum_{n=0}^{2^{i+1}-1} g_i(n)g_i^{\left(2^{i+1}-1-n\right)}=0 \qquad .....(5)$$

(c) each of $g_i(n)$ and $f_i(n)$ annihilates linear discrete time polynomials, i.e.

$$\sum_{n=0}^{2^{i+1}-1} g_i(n)=0 \qquad .....(6a)$$

$$\sum_{n=0}^{2^{i+1}-1} ng_i(n)=0 \qquad .....(6b)$$

$$\sum_{n=0}^{2^{i+1}-1} f_i(n)=0 \qquad .....(6c)$$

$$\sum_{n=0}^{2^{i+1}-1} nf(n)=0 \qquad .....(6d)$$

(d) $f_i(n)$ and $h_i(n)$ are orthogonal to their shifted versions, i.e.

$$\sum_{n=0}^{2^i-1} f_i(n) f_i\left(n+2^i\right) = 0 \quad \text{.....(7a)}$$

$$\sum_{n=0}^{2^i-1} h_i(n) h_i\left(n+2^i\right) = 0 \quad \text{.....(7b)}$$

$$\sum_{n=0}^{2^i-1} h_i(n) f_i(n) = 0 \quad \text{.....(7c)}$$

$$\sum_{n=0}^{2^i-1} h_i(n) f_i\left(n+2^i\right) = 0 \quad \text{.....(7d)}$$

Hence, ST will produce a filter bank, where each has its length in power of 2. In case of a finite length signal (with length in power of 2), this results in a periodic output for the analysis filter bank and an orthogonal transformation can be constructed. The ST filter bank gives a reduction of (2^i-2) samples or supports for scale i ,compared to iterated D_2 DWT filterbank, and the reduction in support approaches one thirds as i increases (for coarser scales)((Selesnick, 1999).

5-PROPOSED SYSTEM

The proposed system composed of two stage Cryptography & Steganography, to hide up secret a speech signal inside cover speech signal. The suggested method is based on time-frequency domain uses the Slantlet transform, is consist of two parts embedding process & Extraction process. The size of the secret speech signal is one fourth the size of cover signal to increase the security of the algorithm.

5.1- The Proposed Steganography System:

The proposed Steganography system has two types of input speech signals: embedded (secret) signal & cover signal, speech signal is 1-D transformed into 2-D, the cover speech signal with the size (512*512) & the secret speech signal is (128*128) & (64*64) with the different format for cover & secret signal. 2-D Slantlet transform decomposition is applied to the cover signal and only low pass filter h_i^n result is taken, rearranges it to 1-D row vector. The encryption process is applied to signal to be embedded to get the ciphered signal. After that embedding process is started & embeds the ciphered signal into the vector of the decomposed cover signal, the reconstruction process inverse Slantlet transform to get the stego-signal. After the Steganography process is finished the stego-signal is added to a very low power signal which is defined for both partners in order to increase the complexity of the proposed system.

5-2 The system Description:

The scheme of the suggested design & evaluation of Steganography system for speech signal is divided into two main stages: Embedding process & Extraction process, each process has many steps. The flowchart of the proposed Steganography system of the sender is given in Fig. (2).

5-b-1 Pre-processing Speech Signal :

The flow chart of the preprocessing of cover signal is shown in fig. (3). This process consists of many steps. These steps are:-

1- Load speech data (reading wave file).

2-Choose the segmentation length.

3- Pre-processing speech signal (sampling, segmentation and framing).

4- Windowing each frame using rectangular window.

5- Decompose each of frames of cover signal using 2-D Slantlet transform decomposition.

6-Only low pass filter h_i^n coefficients are taken & the result 2-D matrix will be converted into 1-D as a row matrix.

7- Sorting the 1-D vector (coefficients) in a descending form.

8- Randomly select the host's samples into which the ciphered secret bits will be inserted. The selected samples are converted to their binary represent (24bit/ sample).

5-b-2 Encryption the Secret Speech Signal:

The ciphered signal is formed by processing done on the secret signal. The encryption process consists of many steps:

1-Grouping the secret signal into blocks of size (8*8)

2- Convert each eight samples to binary form.

3- Column transposition according to ***Key Generation***

Key will be generated from low pass filter h_i^n coefficients (before and after) sorting and each h_i^n coefficients of cover signal as follows:

4- Low pass filter h_i^n coefficients as row vector (1-D).

5-Sorting (1-D) row vector on descent form.

6-Each sample will replaced by h_i^n coefficients (1-D) sorting row vector such that s1→h1, s2→h2, and so on.

7-Return to h_i^n coefficients row vector (1-D) before sorting and give each coefficient its sample number (according to step 4 above) equivalent it.

8-Key will be generated and coefficients will be randomly transmitted.

9-(1-D) row vector that represent key will represent the scrambling of original signal.

10-Convert to the decimal mode and then, construct the ciphered signal.

Numerical Example for Key Generation

Take any voice signal (original signal) and perform preprocessing on this signal (sampling, segmentation, and framing), and Slantlet transform decomposition. Only low pass filter (h_i^n) coefficients is taken. The resulting coefficients will be 2-D, and then convert them into 1-D row vector for example

Step 1: h_i^n coefficients 15 1 3 4 6 2 14 23 17

h_1 h_2 h_3 h_4 h_5 h_6 h_7 h_8 h_9

Then sorting (1-D) row vector in an ascending form, the sorting of h_i^n coefficients will be:

Step 2:↑ 1 2 3 4 6 14 15 17 23

h_2 h_6 h_3 h_4 h_5 h_7 h_1 h_9 h_8

The cover speech signal will be converted from (2-D→ 1-D) row vector:

Step 3: s1 s2 s3 s4 s5 s6 s7 s8 s9

Each sample of cover speech signal will match one of the h_i^n coefficients

Step 4: 1 2 3 4 6 14 15 17 23

s1 s2 s3 s4 s5 s6 s7 s8 s9

Then return to the original distribution h_i^n coefficients before sorting and each coefficient will take sample represent it from above step.

Step 5: h_i^n coefficients 15 1 3 4 6 2 14 23 17

Key generation h_1 h_2 h_3 h_4 h_5 h_6 h_7 h_8 h_9

→ s7 s1 s3 s4 s5 s2 s6 s9 s8

At last cover (speech signal) will be transmitted in random sequence that later will be converted from 1-D row vector into 2-D matrix which represent scrambling signal.

Hint 1:

The purpose of using PN is to distribute the secret bit over wide range of cover samples which may increase the imperceptibility of the stego-signal as well as to increase the robustness, which represents the main important property of the system. Three PN will be used in the proposed Steganography algorithm are PN1, PNsec, PN_{bit}.

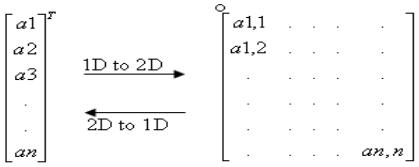
PN1: is used to select random host samples from the decomposed signal.

$PN_{sec:}$ to increase the robustness of the proposed algorithm, PN_{sec} is used to select random bit.

PN bit: is used to select the position within the host samples bits to insert the secret bit.

Hint 2:

Resizing is very important for the purpose of mapping in all sections. Since the data must be converted to a suitable dimensional. Figure (4) illustrates the main procedure of matrix resizing operations for both 1-D vector to 2-D matrix and 2-D matrix to 1-D vector conversions [12].



6-EMBEDDING PROCESS

The merging of the cover speech signal & secret speech signal are accomplished by combining the Pre-processing Speech Signal & Encryption the Secret Speech Signal the basic steps of embedding process is shown in fig.(5) & described as follows:

- Take the randomly binary representation of the randomly selected sample (each sample is converted by 24 bit binary number). The number of samples must be equal to the ciphered secret bits, the selection of samples according to PN1.
- Take the binary representation of the secret signal; these bits are selected randomly according to PN_{sec}.
- Insert the selected bit according to PN_{sec} inserted of the bit identified by PN bit within the host sample binary representation selected by PN1.
- After bit insertion return the whole signal host samples from binary representation to its original form.
- Reshaping the cover samples from signal row (1*262144) sample to its original shape (decomposed cover).
- Apply the 2-D inverse Slantlet transform to obtain the stego-signal.

7-THE EXTRACTION PROCESS

The extraction of the secret signal can be accomplished without the need of the original signal. To extract the embedded signal exactly, only four keys are required.

PN1: to identify the host samples from the whole signal samples.

PN_{sec}: to rearrange the secret bits exactly in its location.

PN bit: to extract the secret bits from the 24 bit of each host sample.

Ciphering key: to rearrange the column of the bit matrix.

With these keys, the overall extraction process is clearly demonstrated by the following steps:

1-Decomposed the stego-signal using Slantlet transform decomposition & then convert the h_i^n matrix to a single row size (1*262144).

2-Separate the host sample (by PN1) in which the secret bits inserted from the samples & then convert them to its binary representation (24 bit/sample).

3-Using PN bit extract secret bits from the 24 bit of the host sample. Till the step 1 has only a single row of secret bits.

4-Obtain the secret bits and rearrange them to their original locations within the row according to PN_{sec}.

5-Reshape the rearranged rows to a binary matrix & the rearrange its column according to the ciphering key.

6- Convert the binary matrix into the corresponding decimal number in order to obtain the exact signal.

8-EXPERMENTAL RESULTS

This section shows the performance of the proposed algorithm. The practical results obtain by embedding a speech signal secret signal in a speech signal cover signal. The evaluation tests of the results obtained are illustrated. The multimedia head set of the specification is described below:

8-1 Specification:

Speaker: 30 mm dynamic type.

Impedance: 32 ohm.

Sensitivity: 10dB± 4dB.

Frequency: 100 – 15000 Hz.

Max. Input power: 100 ohm.

Microphone: condenser type.

Polar pattern: omi-direction.

Sensitivity: 62 dB ±3 dB.

Frequency: 50 – 16000 Hz.

Weight 10, (with card).

Card length: 6 feet (1.8 m).

Connector: 3.5 mm steroplugx2.

8-2 The Test Speech Samples:

The test material will contain four speech samples stored in four files, the format of these files are wave format, each has a different size with respect to the other files of normal. Arabic sentences altered by different speakers. The properties of tested wave data are presented in table (1).

9-EVALUATION TEST

A goal of Steganography is to avoid suspicion to the transmission of hidden information. That means make the stego-signal to be close as to the cover-signal, to measure the secrecy of stego-system, two objective tests (correlation & peak signal to Noise Ratio).

9-1The Correlation Test (Corr.).

This test measures the similarity between the stego-signal & cover-signal. When the stego-signal is perceptually similar to the original cover signal the correlation will be equal to one. The correlation can be calculated as:

$$cor = \frac{\sum_{r=1}^{m}\sum_{c=1}^{n}\left(C_{(r,c)} - c'\right)\left(S_{(r,c)} - s'\right)}{\sqrt{\left[\sum_{r=1}^{m}\sum_{c=1}^{n}\left(c_{(r,c)} - c'\right)^2\right]\left[\sum_{r=1}^{m}\sum_{c=1}^{n}\left(s_{(r,c)} - s'\right)^2\right]}} \quad \text{.....(8)}$$

Where:

r: row number

c: column number

M: height of cover

N: width of cover signal

C(r,c): cover-signal

S(r,c): stego-signal

c' : mean of cover-signal

s' : mean of stego-signal

9-2 Peak Signal to Noise Ratio Test (PSNR):

This test measure the distortion between the original signal and stego-signal, the main test, gives a good metric for the imperceptibility and equality of the stego-signal.

The PSNR is usually measured in d B and can be calculated as:

$$PSNR = 10\log_{10}\frac{M \times N \times (L-1)^2}{\sum_{r=1}^{M}\sum_{c=1}^{N}\left[S_{(r,c)} - c_{(r,c)}\right]^2} \quad (9)$$

L: is the number.

10- RESULTS

Speech signal system Steganography has been built using Matlab (2008 a), the test was performed on a system with personal computer. After applying the proposed embedding and extracting process, the result are arranged in table (2) gives brief information about the tested signals and the obtain Corr. and PSNR using Slantlet transform.

10-1 Graphical result:

It shows the waves, the original cover signal, the secret signal, stego-signal and cross correlation between cover signal and secret signal as shown figures (7).

11- CONCLUSIONS & DISCUSSION

This paper aims to design and test a strong, robust and secure Steganographic system using Slantlet transformer technique. The goals of the paper are to hide up speech signal inside speech signal without rising suspicious to the transmission of a hidden message.

The Steganographic system can be more complicated by adding a low power speech signal which is defined for both the transmitter and receiver to make the extraction of secret speech signal bits more complicated.

The work combines between cryptography and Steganography so as to get a high level of security and to prevent the eavesdroppers from recognizing the existence of the hidden message. Some important conclusions are:

1-Each secret bit replaced with one of the host coefficients bit (which may be the same as secret bit). So that embedding technique allows increase the imperceptibility property.

2- The amount of information can actually be hidden in a signal, depends upon the composition of the signal. A signal that has more high frequency component can be better used in embedding process. Since signal that contains high frequency areas can be manipulated more than a signal containing primarily low frequency areas.

3-There is an inverse proportion between the imperceptibility property and payload capacity.

4-The result with Slantlet transform improve the system from many sides, such as compression, since only low frequency coefficients are used, so that increased security of the algorithm .

5-Four keys are used in the embedding process PN1, $PN_{sec,}$ PN_{bit} and ciphering key so that is increased degree of security.

12- REFERENCE

1-G. Canelli, Supervisor: Prof. MauroBarni," New Techniques for Steganography and Steganalysis in the Pixel Domain.", UNIVERSITÀ DEGLI STUDI DI SIENA, Dipartimento di Ingegneria dell' lnformazione. Ph.D. Thesis – Ciclo XXI- May 13th, 2009.

2-B. Roue and J. Chassery, "(Improving LSB Steganalysis Using Marginal and Joint Probabilistic Distribution", Proceeding of the 2004 workshop on Multimedia and security. ACM New York, NY, USA, 2004, pp.75-80.

3-S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis", IEEE Transactions on Signal Processing, Vol. 51, No. 7, pp. 1995-2007, 2003.

4-P. Lu, X. Luo, Q. Tang, and L. Shen ,"An improved sample pairs method for detection of LSB embedding", Proc. 6th Information Hiding Workshop, vol. 3200. Springer, 2004, pp.116-127.

5- S. Lyu and H. Farid, "Steganalysis Using Higher-Order Image Statistics", IEEE Transactions on Information Forensics and Security, Vol.1, No.1, pp.111-119, 2006.

6- R. Bohme and A. Westfeld, "Exploiting Preserved Statistics for Steganalysis", Sixth Workshop on Information Hiding, Toronto, Canada(2004, May). Springer, 2004.

7- J. Fridrich, M. Goljan, D. Hogea, and D. Soukal, "Quantitative Steganalysis of Digital Images: Estimating the Message Length", Multimedia Systems, Vol. 9, No. 3, pp.288-302, 2003.

8-R.Givner-Forbes, "Steganography: Information Technology in Service of Jihad", The International Centre for Political Violence and Terrorism Research, March 2007.

9-E. H. Ibrahem, "EVALUATION OF INFORMATION HIDING FOR STILL IMAGE", M.Sc. Thesis, University of Baghdad, College of Engineering, Electrical Engineering Department 2005.

10-M. S. A. AL-Kanany, "A SYEGANOGRAPHY SYSTEM USING SLANTLET TRANSFORM" M.Sc. thesis, University of Baghdad, College of Engineering, Electrical Engineering Department, 2007.

11-M. M. S. K. Goswami, "Classification of Over Current and Inrush Current for Power System Reliability Using Slantlet Transform and Artificial Neural Network" Jadavpur University, Department of Electrical Engineering, Kolkata, West Bengal7 00 032, India, Expert System with Application 36 (2009) 2391-2399.

12-L. A. A. Rahaim, Member IEEE, "Proposed Realization of Modified Scrambling Using 2D-DWT Based OFDM Transceivers", MASAUM Journal of Computing, Vol. 1, Issue (2), September, 2009.

Table (1): The tested speech signal properties.

Signal	S1	S2	S3	S4
File Type	Wave File	Wave File	Wave File	Wave File
File Size	4MB	6MB	1MB	1.5MB
File Format	PCM 8KHZ File Format 8-bit mono	PCM 22KHZ 16-bit mono	PCM 8KHZ 8-bit mono	PCM 22KHZ 16-bit mono

Table (2): Particular result of tested signals.

Cover Speech signal	Format	Secret speech signal	PSNR	Corr.
S1	Wave File	S3 S4	30.578 27.876	0.9912 0.9882
S2	Wave File	S3 S4	32.443 28.349	0.9942 0.9939

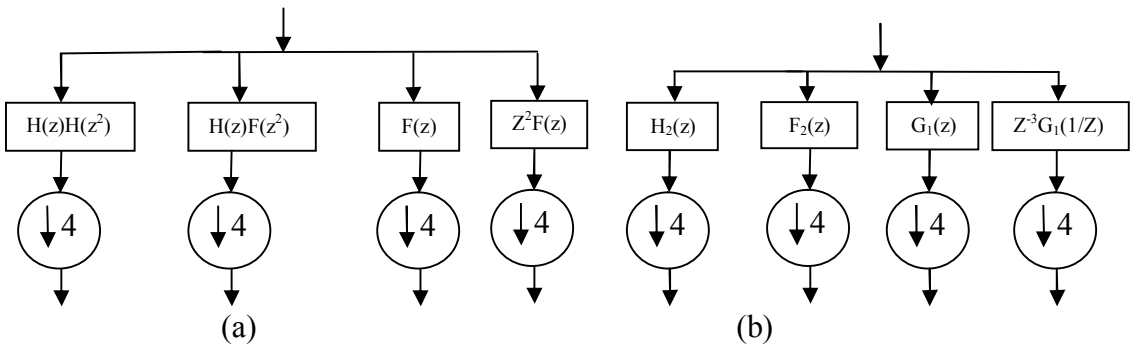


Fig.(1): (a) Two-scale iterated D_2 filter bank & (b) corresponding two-scale Slantlet filter bank.

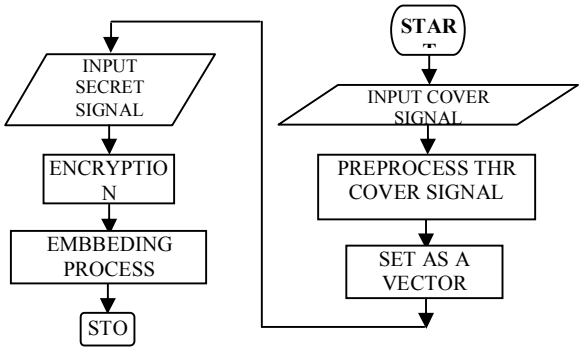


Fig.(2): Flowchart of the proposed system.

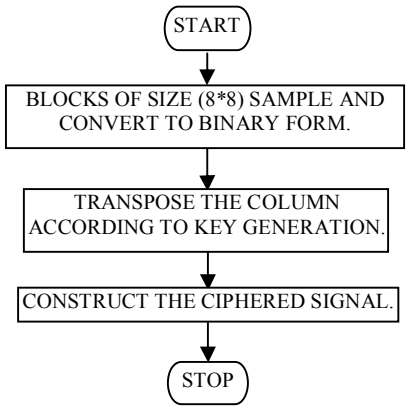


Fig.(4): The flow chart of Encryption**. process.**

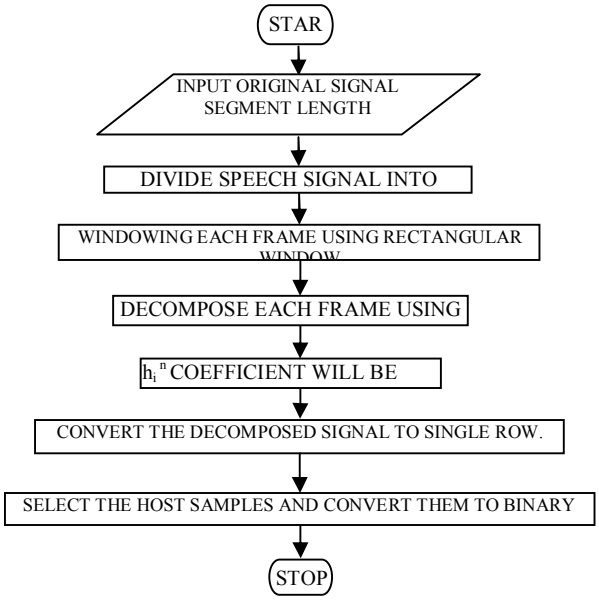


Fig.(3): Flowchart of original signal.

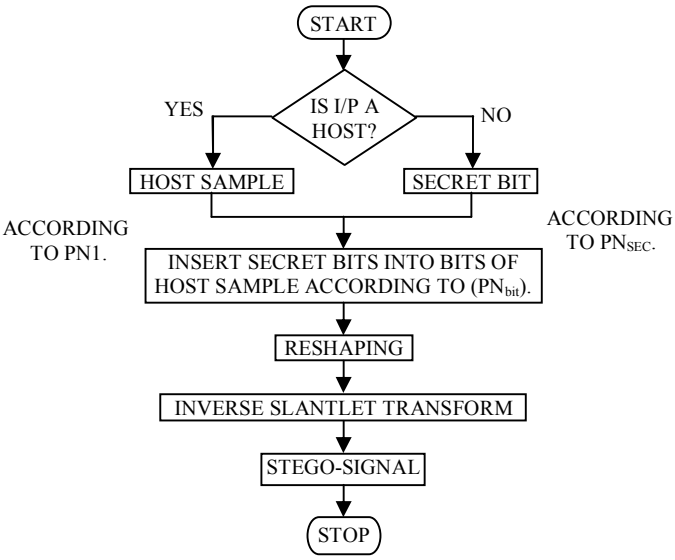
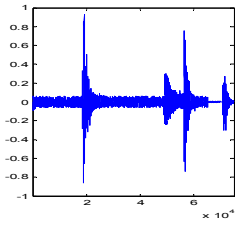
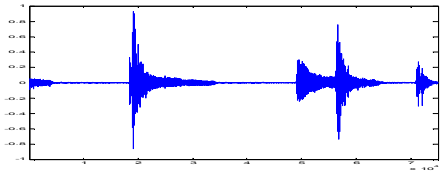


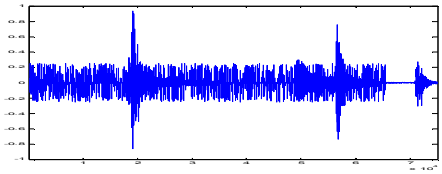
Fig.(5): The flowchart of embedding.



(a)



(b)



(c)

Fig.(7): (a)secret–signal b)original-signal c) stego-signal

تصميم و تقييم أخفاء الإشارة الصوتية بواسطة استخدام محول سلانتليت

أ.م.د. طارق زياد إسماعيل
جامعة بغداد–كلية الهندسة– قسم الهندسة الكهربائية

م.م. أحلام حنون شنين
جامعة بغداد–كلية الهندسة– قسم هندسة الحاسبات

الخلاصة

النظام المقترح يتبنى تقنية حديثة لإخفاء معلومات سرية داخل موجة صوتية هي الغطاء باستخدام تحويل المويل، فن اخفاء المعلومات يسمى steganography ولرفع مستوى السرية تم استخدام علم التشفير cryptography.

في عملية الاخفاء تقنية التحويل تظهر كأداة لاخفاء الصوت المشفر في الاجزاء الاكثر أهمية من موجة الصوت الغطاء لزيادة المتانة. النتيجة لهذه المرحلة هي الموجة الصوتية المضمنة (stego-signal). وتم استخدام تحويل المويل لزيادة متانة النظام المقترح الذي جمع بين (cryptography وsteganography) الاخفاء و التشفير لزيادة المتانة و السرية لنظام لذلك النظام و يقسم الى مرحلتين التشفير و الاخفاء. في عملية التشفير يتم تقسيم الموجة المراد اخفائها بعد تحويلها من 1-D بعد واحد الى 2-D موجة ذات بعدين و الاخيرة تحول الى كتل بحجم 8*8 ثم تحول القيم الى الصيغة الثنائية و بعدها يتم استبدال الاعمدة لاجل الحصول على الموجة الصوتية المشفرة التي تعتبر الادخال الى المرحلة الثانية. الموجة الصوتية المضمنة قريبة جدا من الموجة الصوتية الغطاء لان قيمة عامل التقارب كانت قريبة من الواحد لهذا كانت موجة الصوت الاصلي لانه يتم استبدال كل مرتبه ثنائية من الصوت الاصلي السري بواحد من (host coefficient bit) ابعاد الموجة الصوتية السرية هي ثلث ابعاد الموجة الغطاء وهنا التوازن بين اللاقابلية على ادراك الصوت الناتج وسعة النظام. تم استخدام عدة موجات لقياس فعالية النظام و كانت النتائج مطابقة.