Information Hiding Using Haar Wavelet (Wave in Wave)

Ali Shaker Mahmood[*]

المستخلص :

منذ ظهور الحاسوب والانترنت وتطورهما المتزايد الذي أدخلهما في كل نشاطات حياتها اليومية والعملية وحتى وقتنا الحاظر والعمل جار على ايجاد طرق تقنية حديثة في حفظ وتبادل المعلومات بدلا من تلك التقليدية القديمة.

فدعت الحاجة الى تطوير طرق اخرى مثل اخفاء البيانات وتقوم فكرة هذا البحث على تعديل طريقة البت الاقل اهمية (Least Significant Bit) والتي لها القدرة على تحويل المعلومات المقروءة الى معلومات مخفية داخل وسط ناقل وبذلك تمكن المستخدم من اخفاء بياناته وحمايتها من غير الاشخاص الغير مسموح لهم الاطلاع عليها.

تم اختبار البرنامج على ملفات صوتي من نوع (Wave)، حيث تم تضمين ملف صوتي ضمن اخر ليتم تكوين (Stego Object) والذي هو عبارة عن الملف السري مضمن في الملف الناقل. كذلك تم استخدام مجموعة من المقاييس الخاصة بجودة الصوت المخرج ومقدار الضوضاء المرافقة له لقياس نسبة التشويش في الصوت الناتج.

[*] الجامعة المستنصرية / كلية التربية / قسم علوم الحاسبات

Abstract

The widely growth of the internet and the revolution of transferring information among it, that highlighted the need for mechanisms to protect the secret digital information from the attackers by encrypting or hiding it into another innocent multimedia covers.

Information hiding has become an interesting topic that receives more and more attention. Recently, many hiding techniques are proposed to directly conceal secret information on an audio file, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying.

The proposed work introduces a technique for hiding process using a modified least significant bit, where the hiding process is done and generate stego object some quality and noise measures are applied to know the amount of distortion in the generated Wave file.

1. Introduction

The use of steganography begin many centuries ago, this filed recently became an important area of interest of individuals, companies and governments because of communication technology. People are transferring important information among internet, that communication must privet or secure **[1]**.

The two most common methods for secure communications are cryptography and steganography both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated.

Large amount of multimedia data (Audio, Video) are available in digital form via the internet, everyone is able to copy this data without loss of quality or need to permission. This data can be used as cover to involve the secret message **[2]**, **[3]**.

2. Information Hiding Classifications [4], [5]

The fields of steganography, digital watermarking and fingerprinting have been more growing and interesting. The general model of hiding data in other data can be described as follows, see figure (1).

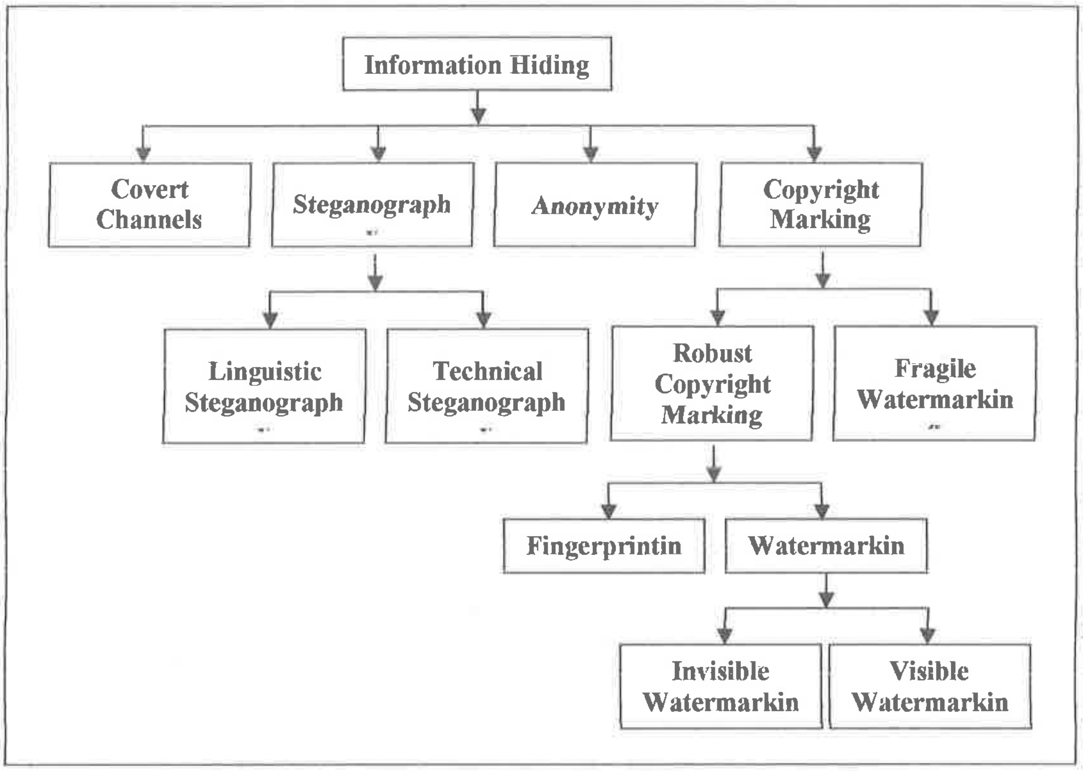

Figure (1): Information hiding classification

- Covert Channels: Communication paths that are neither designed nor intended to transfer information at all.
- Steganography: The art and science of hiding information by embedding messages within other message cover.
- Anonymity: Obfuscate the link between the information that we wish to keep hidden and the observed cover.
- Copyright Marking: Embedding information within an object to keep the property intellectual.

- Linguistic Steganography: Consists of linguistic of language form of hidden writing. These are the semagrams and the open code. A semagram is a secret message that is not in a written form, Open codes are illusions or code words.
- Technical Steganography: The sense of messages is hidden physically.
- Robust Copyright Marking: It was invisible watermarks and can not remove it without destroying the object.
- Fragile Watermarking: A fragile watermark is sensitive to a modification of the object. A fragile watermarking scheme should be able to detect any change in the signal and identify where it has taken place and possibly what the signal was before modification.
- Fingerprinting Digital: fingerprinting produces a metafile that describe the contents of the source file.
- Watermarking: The message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.
- Invisible Watermarking: It undetectable to casual observer and not revealed until some action is taken to the source.
- Visible Watermarking: Visible watermarking used to indicate ownership origins, so an observer might be encouraged to patronize the institutions that own the material.

3. Steganography Types [6], [7]

Most Steganography applications share one general principle, shown in figure (2).

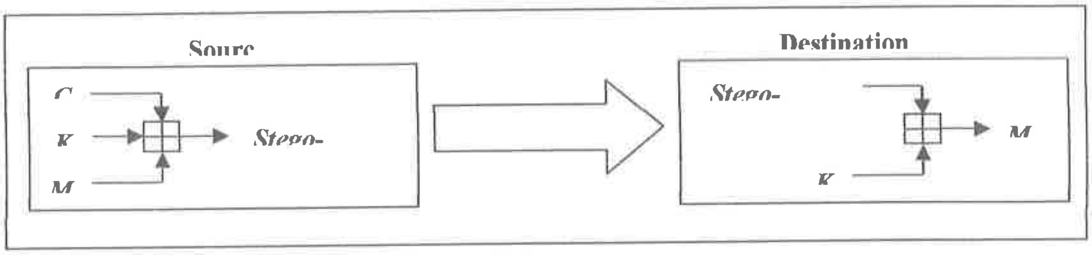

Figure (2): General model of steganography

Where *C* is a cover media, *K* is an embedding key and *M* is a message all of these are parameter to embedding function to produce *Stego-Object* (Cover and Message), this object are send to the destination, where it have a reverse embedding function, Where the input is *Stego-Object* and the *K* is an embedding key to produce the M message.

There are basically three types of steganography protocols used, which are :

3.1 Pure steganography

Pure Steganography is defined as a steganography system that does not require the exchange of a cipher such as an embedding key. This method of steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message.

3.2 Secret key steganography

Secret Key steganography is defined as a steganography system that requires the exchange of a secret key (embedding key) prior to communication.

Embedding Key steganography takes a cover message and embeds the secret message inside of it using a secret key. Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure steganography where a perceived invisible communication channel is present, Secret key steganography exchanges an embedding key, which makes it more susceptible to interception. The benefit of the Secret key steganography is even if it is intercepted; only parties who know the secret key can extract the secret message.

3.3 Public key steganography

Public key steganography is defined as a steganography system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the embedding process and only the private key, which has a direst mathematical relationship with the public key, can be use to extracting the secret message.

Public key steganography provides a more robust way of implementing a steganography system because it can utilize a much more robust and researched technology in Public key cryptography.

4. Steganography Methods [8], [9]

There are several approaches to classify steganography methods. One could categorize them according to the type of covers are used for secret communication; a classification according to the cover modifications applied in the embedding process is another one. This paper follows the second approach and classifies the steganography methods in six groups, which are

4.1 Substitution system

This system try to encode secret message by substituting insignificant parts of the cover by secret message bits, the receiver can extract the message if has knowledge of the positions where secret message has been embedded. Since only minor modifications are made in the embedding process, the sender assumes that they will not be noticed by attacker.

4.2 Transform domain technique

It has been noted early in the development of steganography system that embedding information in the frequency domain of a signal can be must more robust than embedding rules operating in the time domain. Most robust steganography system known today actually operates in some sort of transform domain.

Transform domain method hide message in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping and some image processing, while they are more robust to various kinds of signal processing, they remain imperceptible to the human sensory system.

4.3 Spread spectrum technique

This technology define as means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to sent the information, the band spread is accomplished by means of a code which is independent of the data, as a synchronized reception with the code at the recover is used for dispreading and subsequent data recovery.

The power of the signal to be transmitted can be large, the signal to noise ratio in every frequency band will be small. Even if parts of a signal could be remover in several frequency bands, the spread spectrum makes it difficult to detect or remove from a signal. This situation is very similar to a steganography system which tries to spread a secret message over a cover in order to make it impossible to perceive. Since the spread signal tend to be difficult to remove, embedding methods based on spread spectrum should provide a considerable level of robustness.

4.4 Statistical steganography

This method utilize the existence of 1-bit steganography system, which embed one bit of information is a digital carrier. This is done by modifying the cover in such a way that some statistical characteristic change significantly if a 1 is transmitted. Otherwise the cover is left unchanged. So the receiver must be able to distinguish unmodified covers from modified ones.

The detection of a specific bit is done via a test function which distinguishes modified block from unmodified block.

The embedding function can be interpreted by a hypothesis testing function, where test the null hypothesis was not modified, against the alternative hypothesis was modified. Therefore this class of steganography system called statistical steganography. The receiver successively applies function to all blocks in order to restore every bit of the secret message.

4.5 Distortion technique

This technique requires the knowledge of the original cover in the decoding process. The sender applies a sequence of modifications to a cover in order to get a stego-object, where chooses this sequence of modification in such a way that it corresponding to a specific secret message. The receiver measure the differences to the original cover in order to reconstruct the sequence of modification apply by sender, which corresponding to the secret message.

In many applications, such systems are not useful, since the receiver must have access to the original cover. The attackers also have access to the cover and can easily detect the cover modifications and have evidence for a secret communication. If the embedding and extracting functions are public and do not depend on an embedding key.

4.6 Cover generation technique

All embedding methods explain above, where secret information is embedded to a specific cover by applying an embedding algorithm; some steganography systems generate a digital object only for the purpose of being a cover for secret communication.

5. Text Steganography [10]

Encoding secret messages in text can be a very challenging task because text files have a very small amount of redundant data to replace with a secret message, another drawback is the ease of which text based steganography can be altered by unwanted parties by just changing the text itself or reformatting the text to some other form (from txt to doc). There are numerous methods by which to accomplish text based steganography.

- Null Ciphers: Where use text to hide secret messages, which often appeared to be innocent message about ordinary occurrences, would not alert suspicion, and would thus not be intercepted.
- Line Shifting: The encoding involves actually shifting each line of text vertically up or down by specific length. Depending on whether the line was up or down from the stationary line would equate to a value that would or could be encoded into a secret message.
- Word Shifting: According to a secret message, horizontal spaces between selected words of the cover are altered. It is possible to alter every space between two words the only limitation is that the sum of all movements in one specific line equals zero so that the line keeps properly aligned.
- Open Space Method: There are many ways to employ the open space in text files to encode the information. This method works because to a casual reader one extra space at the end of line or an extra space between two words does not prompt abnormality. This method works, but requires a large amount of data to hide only little information. Also many word processing tools automatically correct the spaces between sentences.

6. Image Steganography [11]

Coding secret messages in digital images is most widely used of all methods in the digital world. This is because it can take advantage of the limited power of the human visual system. Almost any plain text, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image.

- Least Significant Bit Insertion: This method is probably the most known image steganography technique. It is a common, simple approach to embedding information in a graphical image file. Unfortunately, it is extremely vulnerable to attacks, such as image manipulation. A simple conversion from a GIF or BMP format to a lossy compression format such as JPEG can destroy the hidden information in the image.
- Transformation: Transform Domain tools use an algorithm such as the discrete cosine transformation or wavelet transformation to hide information in significant areas of the image. The least significant bits of the quantized coefficients are used as redundant bits into which the hidden message is embedded.
- Masking and Filtering: Masking and filtering techniques hide information by marking an image in a manner similar to paper watermarks. Because watermarking techniques are more integrated into the image, they may be applied without fear of image destruction from lossy compression. By covering, or masking a faint but perceptible signal with another to make the first nonperceptible, we exploit the fact that the human visual system cannot detect slight changes in certain temporal domains of the image.

7. Audio Steganography [12]

The human hearing system could not recognize every voice or noise that is combined with the original audio signal because the human auditory system works over a wide dynamic range, therefore, it can exploit this property to hide the data into audio signals but at the same time being aware because the human auditory system is very sensitive to additive random noise.

- Low Bit Encoding: The encoding data is embedded by replacing the least significant bit of each sampling point by a message. This results in a large amount of data that can be encoded in a single audio file.
- Phase Encoding: This technique is the most effective coding in terms of signal to noise ratio. In this method the phase of the original audio signal is replaced with the reference phase of the data to be hidden.
- Speared Spectrum Encoding: Modern steganography systems are used spread spectrum communications to transmit a narrowband signal over a much larger bandwidth so that the spectral density of the signal in the channel looks like noise.
- Echo Data Hiding: This is a method for embedding information into an audio signal. It seeks to do so in a robust fashion, while not perceivably degrading the host signal (cover audio). Echo hiding introduces changes to the cover audio that are characteristic of environmental conditions rather than random noise, thus it is robust in light of many lossy data compression algorithms. Like all good steganography methods, echo hiding seeks its data into data stream with minimal degradation of the original data stream, that mean the change in the cover audio is either unperceivable or simply dismissed by the listener as a common environmental distortion. The particular distortion are introducing is similar to the resonances found in a room due to walls, furniture, etc. The difference between the stego audio and

the cover audio is similar to the difference between listening to a compact disc on headphones and listening to it form speakers. With the headphones, we hear the sound as it was recorded. With the speakers, we hear the sound plus echoes caused by room acoustics.

8. Wave File Format [13], [14]

The Wave is a short of Waveform Audio File Format, is a Microsoft and IBM audio file format standard for storing an audio bit stream on the PCs. It is the main format used on Windows systems for raw and typically uncompressed audio.

Uncompressed Wave files are quite large, so, as file sharing over the Internet has become popular, the Wave format has declined in popularity. However, it is still a commonly used file type, suitable for retaining and archived files of high quality, for use on a system where disk space is not a constraint, or in applications such as audio editing, where the time involved in compressing and uncompressing data is a concern.

The usage of the Wave format has more to do with its familiarity, its simplicity and simple structure, which is heavily based on the RIFF file format. Because of this, it continues to enjoy widespread use with a variety of software applications, often functioning as a 'lowest common denominator' when it comes to exchanging sound files between different programs.

The Wave format is limited to files that are less than 4 GB; because of its use of a 32-bit unsigned integer to record the file size header, it is sometimes necessary to exceed this limit, especially when greater sampling rates or bit resolutions are required.

The Wave file consists a number of chunks, each one include an identifier and measured in byte. The main advantage of using chunk structure is that when parsing a Wave file you don't need to interpret every chunk type but can skip over the ones you don't understood, for detail descriptions see table (1).

Table (1): Wave file format

Byte Number	Field Name	Field Size	Description
4	Chunk ID	4	Contains this letter (RIFF)
8	Chunk Size	4	The size of the rest of the rest of the chunk.
12	Format	4	Contains this letter (WAVE)
16	Sub Chunk-1 ID	4	Contains this letter (fmt)
20	Sub Chunk-1 Size	4	The size of the rest of the rest of the sub chunk.
22	Audio Format	2	Compression type (Auto Format PCM=1)
24	Number Channels	2	Mono=1, Stereo=2
28	Sample Rate	4	Number of samples per second
32	Byte Rate	4	Standard value according to Wave specification
34	Block Align	2	Number of byte per one channel
36	Bit Per Sample	2	Number of bit per one sample
40	Sub Chunk-2 ID	4	Contains this letter (data)
44	Sub Chunk-2 Size	4	Number of bytes in the data
N	Data	N	Actual sound data

related to a mathematical operation called the haar transform explained in the following equations [15].

$$F(j) = \begin{cases} 1 & \textit{for } 0 \le j < 0.5 \\ -1 & \textit{for } 0.5 \le j < 1 \end{cases} \qquad \textit{Equ}\ (1)$$

$$F(s) = \frac{1}{js}\left[1-\exp\left(-\frac{js}{2}\right)\right]^2 \qquad \textit{Equ}\,(2)$$

$$HWf(a,b) = \frac{j}{2\pi\sqrt{a}}\int_{-\infty}^{\infty}\frac{F(s)}{s}\exp(jsb)\left[1-\exp\left(\frac{jas}{2}\right)\right]^2 ds \qquad \textit{Equ}\,(3)$$

The haar transform serves as a prototype for all other wavelet transforms. Like all wavelet transforms, the haar transform decomposes a discrete signal into two sub signals of half its length. One sub signal is a running average or trend; the other sub signal is a running difference or fluctuation. The haar wavelet transform has a number of advantages like, it is conceptually simple and fast, memory efficient and it is exactly reversible without the edge effects that are a problem with other wavelet transforms.

9.2 (Part 3)

This part will embedding the message wave file in a cover wave file by using Modified Low Bit Encoding Method (The insertion process done in the second least significant bit to be more immune, from other point of view the noise, distortion and confusion are increased but still in acceptable level), where each byte in cover file will replaced the second least significant bit in it by a bit from message file as shown in figure (4) the message file contain two byte that mean the cover file should be at least contain sixteen byte.

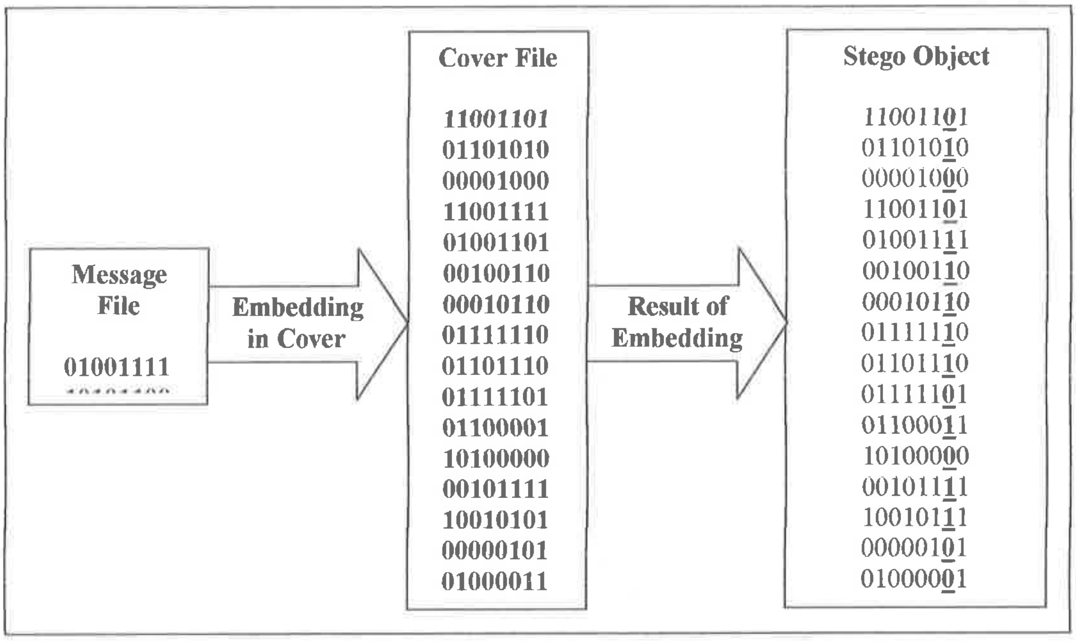

Figure (4): Example of embedding process

9.3 (Part 4)

The calculation process of noise and quality is done in this part, where measures the amount of noise and quality of stego object by using the following equations **[16]**:

- Mean Squared Error (MSE): Where f represent an object before embedding, $\bar{f}$ represent an object after embedding and N signal size, see equation (4).

$$MSE = \frac{1}{N}\sum_{k=1}^{N}(f_k - \bar{f}_k)^2 \qquad Equ(4)$$

- Signal to Noise Ratio (SNR): Is define as explained in equation (5).

$$SNR = 10\log_{10}\frac{\sum_{k=1}^{N} f_k^2}{\sum_{k=1}^{N}(f_k - \bar{f}_k)^2} \qquad Equ(5)$$

- Peak Signal to Noise Ratio (PSNR): Expresses the quality of the stego object compared to the original Cover object, as explained in equation (6).

$$PSNR = 10\log_{10}\frac{f_k^2}{\sum_{k=1}^{N}(f_k - \bar{f}_k)^2} \qquad Equ(6)$$

The above parts can be illustrated in figure (5), where it explains the proposed system.

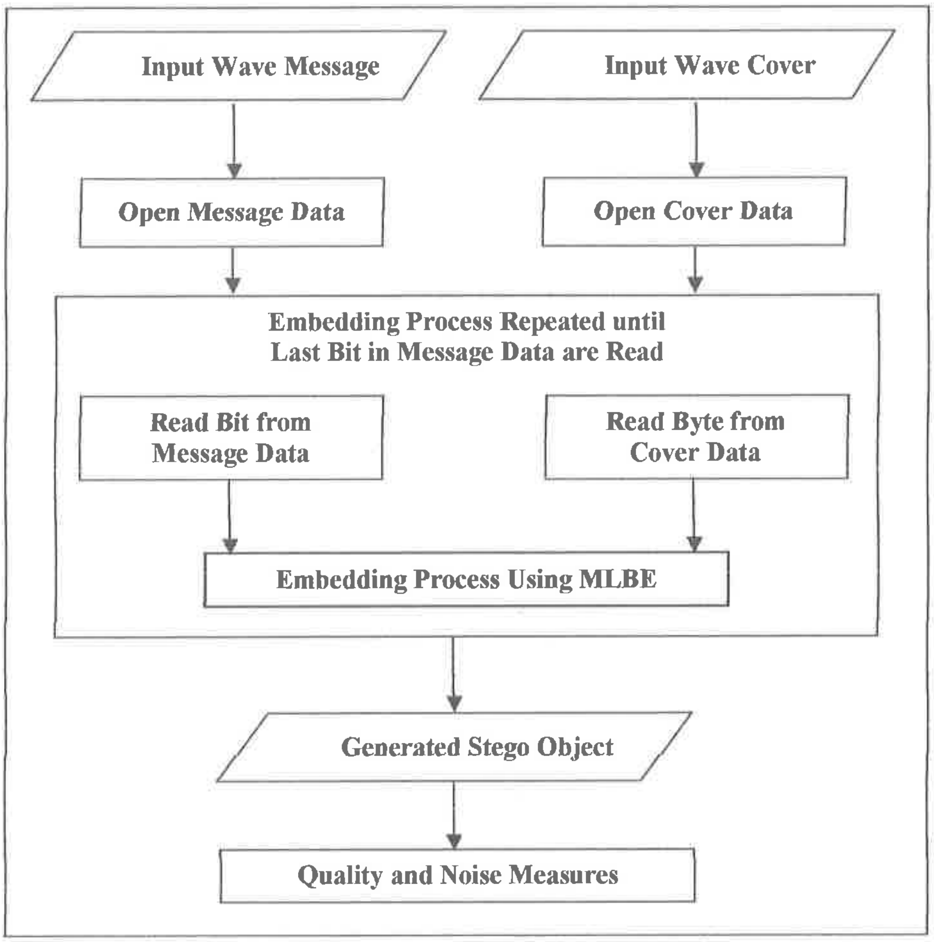
Input Wave Message
Input Wave Cover
Open Message Data
Open Cover Data
Embedding Process Repeated until Last Bit in Message Data are Read
Read Bit from Message Data
Read Byte from Cover Data
Embedding Process Using MLBE
Generated Stego Object
Quality and Noise Measures

Figure (5): Proposed system flowchart

10. Case Study

The testing process of this system needed some parameters are chooses before the testing beginning these parameters are, cover Wave file, message Wave file, where the number channels in these two files should be equal to one (Mono Type) and sample resolution equal to (16-Bit Per Sample). Because using of Modified Low Bit Encoding, each bit in message file need a corresponding byte in cover file.

Table (2): Test Samples that applied to the proposed system

File Name	Size in Kilobytes	Wave Format	Length in Seconds
First Cover Wave File	529	16-Bit, Mono	31
Second Cover Wave File	721	16-Bit, Mono	66
Message Wave File	61	16-Bit, Mono	5.20

After embedding process is done, some calculation process are begins on the stego object to measure the amount of noise and quality, see table (3).

Table (3): Measures results

File Name	Quality and Noise Measures		
	MSE	SNR	PSNR
First Cover Wave File	0.520	44.991	50.964
Second Cover Wave File	0.502	43.288	49.122

11. Conclusion

1. The proposed system goals are achieved by hiding a secret Wave file in a Cover Wave file.
2. The noise amount decrease while used a larger cover size, that is mean an inverse relationship between cover size and noise.

3. The quality and noise of the stego object are decreased when hiding bit are increase from first bit to second bit.
4. The usage of speech Wave file as cover is better from known Wave file because the attacker can not recognize the noise and confusion in the first one but can recognize in regular Wave or music.

12. References

1. Sabu M., "*Information Hiding Techniques*", P/13, Kasaragod Kerala Publication, India, 2004.
2. Katzenbeisser S. and Petitcolas F., "*Information Hiding Techniques for Steganography and Digital Watermarking*", P/56, Artech House, USA, 2000.
3. Amin M. and Katmin R., "*Steganography Using Least Significant Bit*", P/65, Puteri Pan Press, Malaysia, 2002.
4. Kahn D. and Hartung F., "*The Story of Secret Writing*", P/130, Scribner Press, USA, 1996.
5. Fabien A., Petitcolas P., Ross J. and Markus G., "*Information Hiding Survey*", P/87-93, Proceedings of IEEE Conference on Identification and Protection of Multimedia Information, Belgium, 1999.
6. Gopalakrishna R, and Toshiyuki S., "*Information Hiding Technique using Animations*", P/2, Advance Engineering Letters Publication, Taiwan, 2006.
7. Lin C., Chang C. and Bin L., "*Secure Data Hiding Schemes*", P/369-373, Proceedings in the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, USA, 2009.

8. Mohammed M. and Hussain A., "*Steganography and Watermarking*", P/7-12, Leung Press, UAE, 2005.
9. Mehmet K., "*Information Hiding Codes and Applications for Images and Audio*", P/33, PH.D Thesis, University of Illinois, USA, 2002.
10. Chen P., and Zhang F., "*Text Information Hiding Techniques*", P/16-26, Journal of Pingdingshan Institute of Technology, China, 2007.
11. Prasad M., Nagan S., Krishna G. and Nagaraju C.,"*A Novel Information Hiding Technique for Security by using Image Steganography*", P/36, Journal of Theoretical and Applied Information Technology, India, 2009.
12. Cvejic N. and Seppanen T., "*Increasing robustness of LSB audio steganography using a novel embedding method*", P/3, Presented at International Conference on Information Technology, USA, 2004.
13. Pohlmann C., "*Principles of Digital Audio*", P/3, McGraw-Hill Inc., USA, 2000.
14. Kabal P., "*Wave File Format Specifications*", McGill University, Canada, 2003. http://www.tsp.ece.mcgill.ca/MMSP/Documents/AudioFormats/WAVE.html.
15. Adhemar B., "*Haar Wavelets with Applications in Signal and Image Processing*", P/99, John Wiley and Sons, USA, 2006.
16. Henry X., "*Fractal Audio Coding*", P/25, MSC Thesis, Queen's University, Canada, 2005.