

A Proposed Implementation Method of an Audio Steganography Technique

Mazhar Tayel, Ahmed Gamal, Hamed Shawky

Electrical Engineering Department, Faculty of Engineering, Alexandria University, Egypt

profbasyouni@gmail.com, gamalahmed8566@yahoo.com, dr.hamedzied@gmail.com

Abstract:

Steganography is the art of science dealing with hiding secret data inside image, audio, video or text files. In audio steganography; secret message is embedded in the digital sound by slightly altering the binary sequence of the sound file. Existing audio steganography software deal with WAV, AU, and even MP3 sound files. Embedding secret messages in the digital sound is usually a more difficult process than embedding messages in other forms, such as digital images. Audio steganography uses different algorithms, but (LSB) least significant bit is applied in this paper. The quality of sound is depended on the size of the audio which the user selects and length of the message.

Keywords:

Steganography, information hiding, least significant bit (LSB)

I. INTRODUCTION:

Audio steganography is one of the popular data hiding techniques that embeds secret Data in audio signals. It is based on the masking effect of Human auditory system (HAS). This means that a weak sound is undetectable in the presence of the large one. Data hiding in audio signals has numerous applications such as; protection of copyrighted audio signals and safely covertly communication government data. There are many different techniques for hiding information or messages in audio files such as (LSB) Least Significant Bit algorithm, Parity coding technique, phase coding technique, Spread Spectrum technique (SS) and Echo hiding technique. The LSB is the simplest way to embed information in a digital audio file by substituting the least significant bit of each sampling point with a binary message [1]. The sender embeds the secret audio message in the audio media cover which called host and create a stego file then send it to the receiver which extracts the message from the stego file. Figure (1) shows the Blocks diagram for the audio steganography.

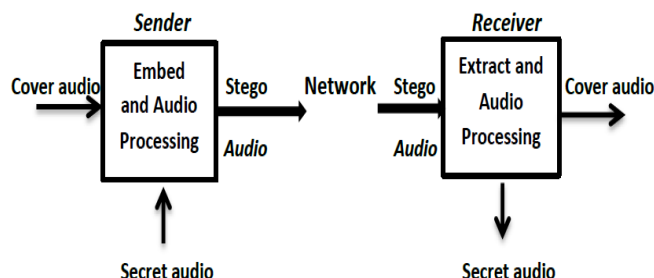


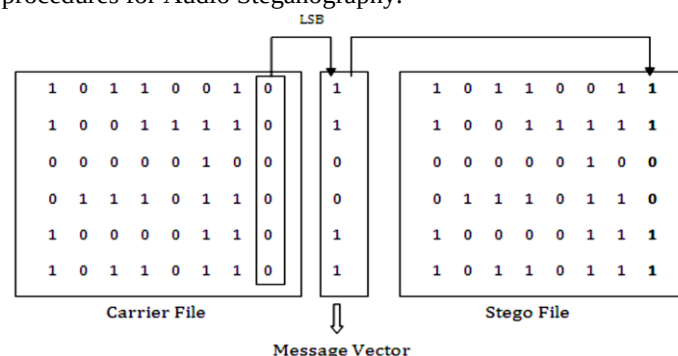
Fig (1): Blocks diagram for the audio steganography.

II. TECHNIQUES OF AUDIO STEGANOGRAPHY

1-Temporal Domain:

1.1 Least Significant Bit (LSB):

LSB is one of the earliest, simplest and the commonly used technique for audio steganography [2]. In this technique the binary sequence of each sample of the digitized audio file is replaced with a binary equivalent of the secret message. It is consisted of embedding each bit of the message in the least significant bit of the audio cover. The LSB hiding schemes provide very high channel capacity for transmitting many kinds of data and are easy to implement and combine with other hiding techniques. The length of the secret message to be encoded should be smaller than the total numbers of samples in the sound file. The LSB technique takes advantage of the Human auditory system (HAS) which cannot identify the slight variation of the audio frequencies at the high frequency side of the audible spectrum. The LSB technique allows high embedding rate without degrading the quality of the audio file. Furthermore, it is relatively effective and easy to be implemented. Figure (2) shows LSB modification procedures for Audio Steganography.



Fig(2): LSB modification procedure for Audio Steganography.

1.2 Parity coding:

Parity coding technique operates on a group of samples instead of individual samples. Here individual samples are grouped and parity of each group is calculated. For inserting message bit one by one, the parity bit of a group of samples is checked. If the parity bit and the message bit matches do nothing. Otherwise change the LSB's of any of the individual samples in that group to make the parity bit equal to the message bit [3]. Figure (3) shows the parity coding procedures.

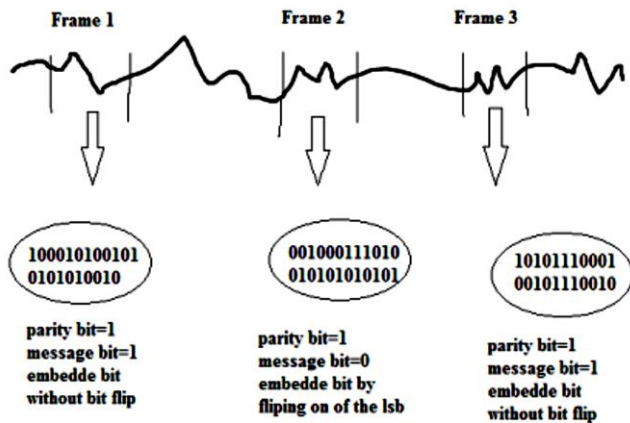


Fig (3): Parity coding procedures.

1.3 Echo hiding:

In echo hiding method; data is embedded in the echo part of the hosting audio signal. The echo is a resonance added to the host signal and therefore the problem with the additive noise is avoided. While using echo hiding three parameters are to be considered: they are initial amplitude, offset (delay), and decay rate, in order that echo becomes audible. The main disadvantage of this method is the lenient detection and low detection ratio. Due to low embedding rate and low security, no researches are performed on echo hiding techniques [4]. Figure (4) shows the Echo Hiding.

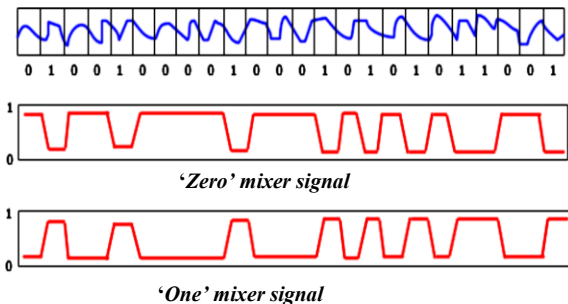


Fig (4): Echo Hiding.

2- Transform domain:

2.1 Phase coding:

The phase coding technique works by replacing the phase of the initial audio segment with a reference phase which represents the secret information. The remaining segments are adjusted in order to preserve the relative phase in between. This method is based on the fact that the phase components are not audible to human as noise components. It embeds the secret message bits as a shift phase in the spectrum phase of the original audio signal. It tolerates better signal distortion, better robustness but it does not survive low pass filtering. The secret message is inserted only at the vector phase of the first signal segment [5]. Figure (5) shows the phase coding procedure.

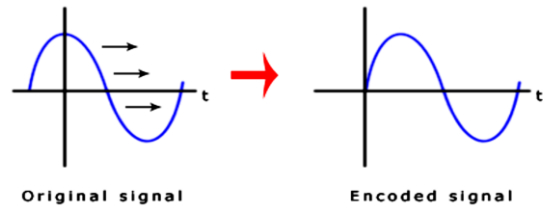


Fig (5): phase coding.

2.2 Spread spectrum technique:

The Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which does not depend on the actual signal. This technique takes advantage of the masking property of HAS. Masking threshold is calculated using a psycho-acoustic model, and the spread signal lies below the masking threshold. Apart from the shifted phase the secret message is distributed along with the host signal. The final signal occupies a bandwidth which is more than what is actually is required for transmission [6].

2.3 Wavelet Domain:

Wavelet domain is suitable for frequency analysis because of its multi-resolution properties that provide access to both most significant parts of spectrum. Wavelet domain techniques works with wavelet coefficients. By applying the inverse transform, the stego- signal can be reconstructed [7].

Table (1): Comparison Between different Audio Steganography Techniques.

Technique	Strong point	Weak point
Least Significant Bit	1-Simple 2-High bit rate 3-Easier implementation	1-Easy to extract 2-Addition of noise 3-Compression can destroy the data
Parity coding	1-More robust than LSB 2-More choices in encoding the secret bit	1-Easy to extract and destroy
Echo hiding	1-Avoids problem with additive noise 2-Compression of audio will not destroy the data 2-All parameters are set below threshold value of human hearing so echo is not easily resolved	1-Low embedding capacity and security
Phase coding	1-High Robust 2-Effective technique in terms of signal to perceived noise ratio	1-Low Capacity
Spread spectrum	1-Increases transparency 2-Highly Robust	1-Occupies more bandwidth 2-Unprotected to time scale modification
Wavelet Domain	1-High hiding capacity and transparency	1-Extracted data may be lossy

III. THE PROPOSED METHOD

The human auditory system is sensitive to small amplitude variations in the audio files, this paper presents a hiding technique developed to hide audio secret data in an audio cover data by using the Least Significant Bit (LSB) technique. The technique is applied on two cards of arduino due with processor of (80) MHZ storing sound samples as (8, 16 or 24) bit values in order to hide secret data. The two cards are programmed with the (Arduino 1.0.5) program. The block diagram in figure (6) shows the procedures that applied by the Arduino program on the two cards. The first card is used as a transmitter to produce the Stego-data which replaces the most Significant Bit (MSB) of the audio cover and the audio secret message after converting them from analog signals to digital signals by using analog to digital converter (A/D). After that the stego-data is converted from digital to analog data by using digital to analog converter (D/A). As a result the audio secret message is embedded in the audio cover and stego-data is the output of the transmitter. The other card is used as a receiver. The input of this card is the output of transmitter which is converted from analog to digital by using analog to digital converter (A/D) in the receiver. The audio secret message can be extracted by replacing the four Least Significant Bits (LSB) of the digital stego-data, the most Significant Bit (MSB) of the digital audio secret message. By using digital to analog converter (D/A) the audio secret message is heard. The audio cover can be extracted by replacing the most Significant Bit (MSB) of digital stego-data, which was the most Significant Bit (MSB) of the digital audio cover. By using digital to analog converter (D/A) the audio cover is heard. The previous procedures are applied when the communication channel is pure.

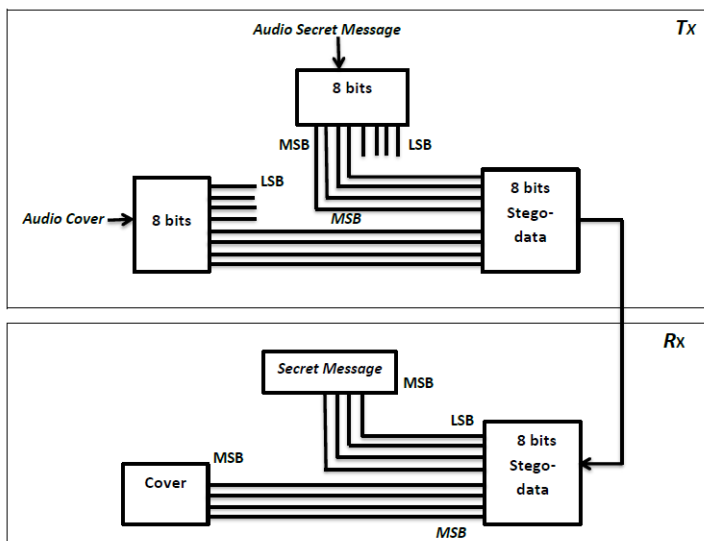


Fig (6): block diagram of the proposed method procedures.

IV. IMPLEMENTAION OF THE PROPOSED METHOD

The audio Steganography is implemented or simulated in (protues7.10) and Electronic Work Bench. Figure (7) shows the implementation proposed method. Figure7 (a) shows the simulated transmit. igure7 (b) shows the simulated receiver.

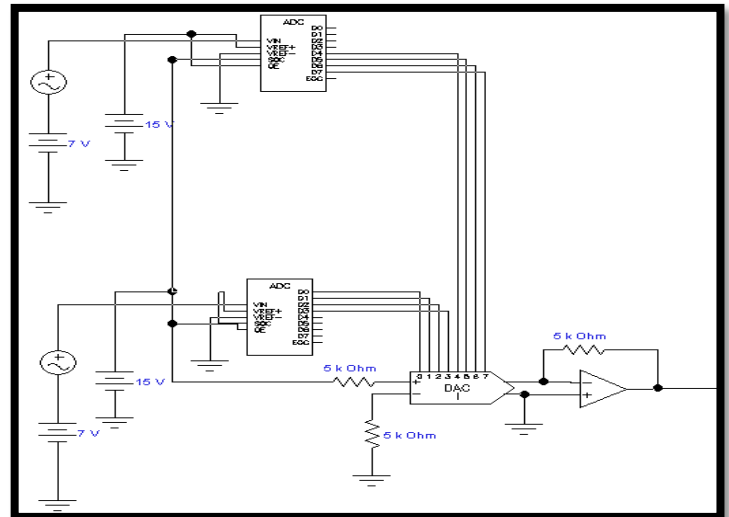


Fig 7(a): The simulated transmitter.

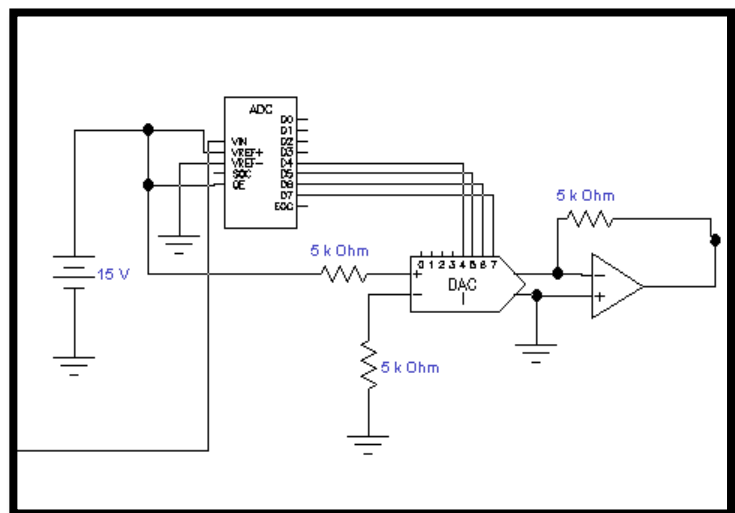


Fig 7(b): The simulated receiver.

Figure (8) shows the input and the output for the transmitter and the receiver by using a simulated oscilloscope. Figure8 (a) shows the embedded cover and the message in the transmitter. Figure8 (b) shows the stego-data that is performed in the transmitter and the extracted message from the receiver.

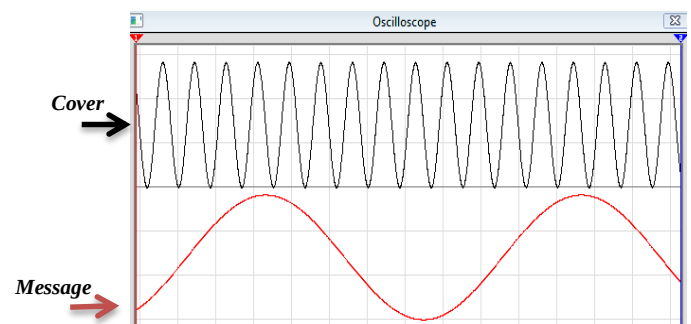


Fig 8(a): The input of transmitter.

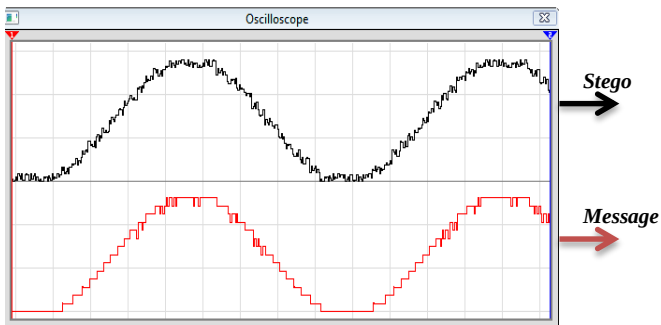


Fig 8(b): The input Stego and extracted message from receiver.

VI. EXPERIMENT RESULTS

1-The Experiment was carried out on various wave files according to the shown in figure (6). Figure (9) shows different waves files which were used as the input of the transmitter and the receiver displaying the output of them using a real oscilloscope. Figure9 (a) shows the audio secret message wave file. Figure9 (b) shows the audio cover wave file. Figure9 (c) shows the Stego-audio that is performed in the transmitter. Figure9 (d) shows the first extracted audio secret message wave file from the receiver with no delay time. But the extracted audio secret message is low efficient than the embedded audio secret message applied into the transmitter.

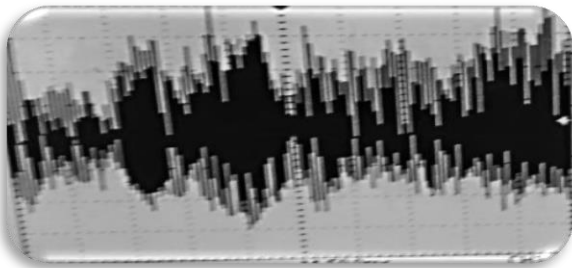


Fig 9(a): The audio secret message wave file.

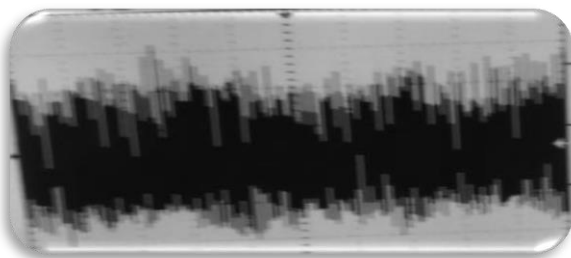


Fig 9(b): The audio cover wave file.

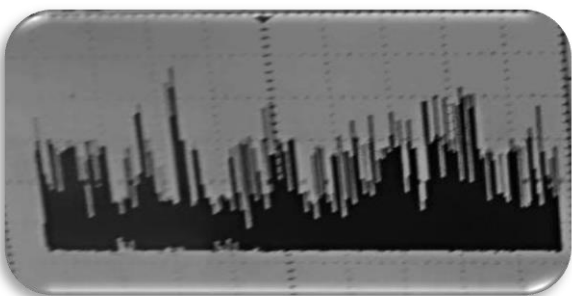


Fig 9(c): The Stego-audio.

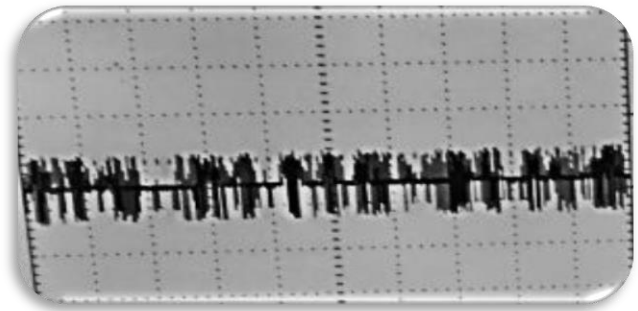


Fig 9(d): The first extracted audio secret message wave file.

2-According to figure (6) some adjustments taking place:

(A)-In the transmitter, the Stego-data is performed by embedding the audio secret message in the (LSB) of the audio cover data after converted them from analog to digital by using an analog to digital converter (A/D). In this case all bits of the audio secret message are sent one bit only and accumulate them before the receiver then sending them bit by bit and perform Stego-data then converting them from digital to analog data by using digital to analog converter (D/A).

(B)-In the receiver, Stego-data is embedded and converted from analog to digital by using an analog to digital converter (A/D). The audio secret message and audio cover are extracted from the digital Stego-data (audio cover + accumulated audio secret message) by converting accumulated audio secret message from digital to analog using digital to analog converter (D/A). Thus the audio secret message is heard. This extracted audio secret message is efficient and the same as the audio secret message that was embedded but delay in the time occurs when hearing the sound.

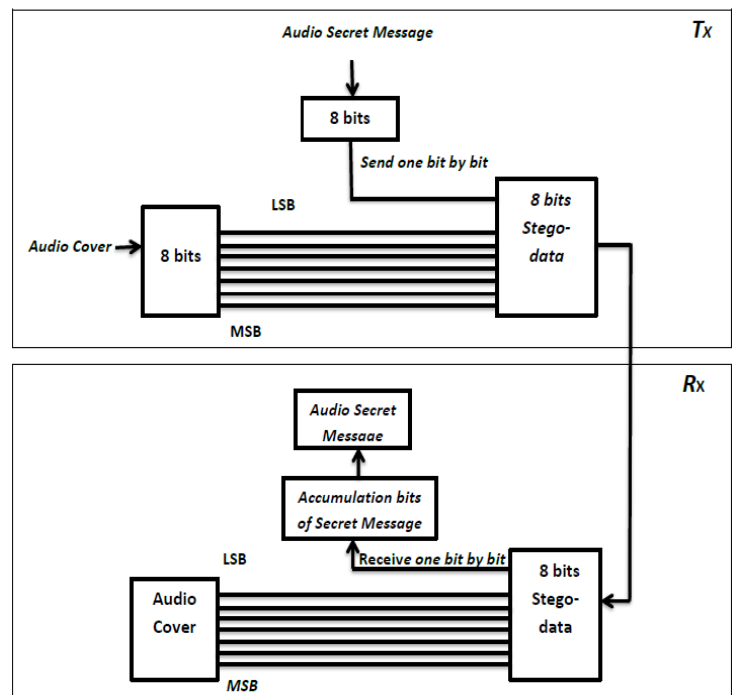


Fig10 (a) shows the amendments in figure (6).

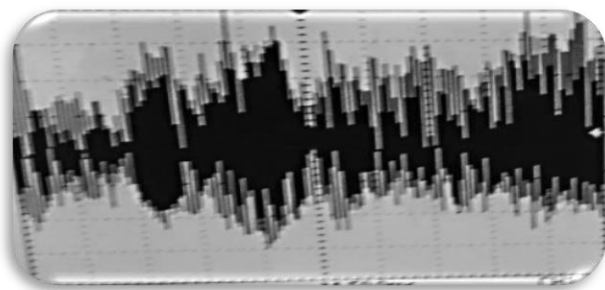


Fig 10(b): The second extracted audio secret message wave file.

Figure 10 (a-b) shows the amendments in figure (6), and the shape of the second extracted audio secret message that was embedded in transmitter and extracted from the receiver by a real oscilloscope.

3- Peak Signal to Noise Ratio (PSNR) is used to measure the quality of the extracted audio secret message. And compare between the audio secret message and stego-audio.

$$PSNR = 10 \log_{10} \left(\frac{Max^2}{MSE} \right) \quad (1)$$

Where 255 is the Max value of audio intensity and MSE (Mean Square Error) is the average value of the total square of absolute error between audio cover file and stego-audio file.

$$MSE = \frac{1}{N} \sum_{i=1}^N (Ci - Si)^2 \quad (2)$$

Ci represents the sample value of cover audio and Si represents the sample value of stego-audio.

Table (2): Comparison between First and Second extracted audio secret message wave file.

Secret Audio File	Bit Per Samples	MSE	PSNR [db]
First Extracted	8 Bit	269.0174	23.833
Second Extracted	8 Bit	0.092125	58.487

VII. CONCLUSIONS

This paper presents implementation of an audio steganography using two cards of arduino due applying successfully the Least Significant Bit (LSB) technique on a pure communication channel. The proposed method is applied to various audio files such as speech and music envelope signals. These audio files were used as covers and secret messages and it all giving remarkable results on steganography concept. Further research on data hiding in audio signal through steganographic techniques such what is discussed in the previously to secure data transmission and overcome noisy communication channel.

References

- [1] X. Dong, M. Bocko, Z. Ignjatovic, "Data hiding via phase manipulation of audio signals", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), vol. 5, pp. 377-380, 17-21 May 2004.
- [2] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography", 2011 International Conference on Computer Networks and Information Technology (ICCNIT), IEEE, 2011.
- [3] P. Jayaram, H. Ranganatha, and H. Anupama, "Information hiding using audio steganography-a survey", International Journal of Multimedia and its Applications, 2011.

- [4] F. Djebbar, B. Ayad, H. Hassmam, and K. Abed-Meraim, "A view on latest audio steganography techniques", 2011 International Conference on Innovations in Information Technology (IIT), IEEE, 2011.
- [5] M. Nutzinger and J. Wurzer, "A novel phase coding technique for steganography in auditive media", 2011 Sixth International Conference on Availability, Reliability and Security (ARES), IEEE, 2011.
- [6] S. Md, B. Vijaya, and V. Shiva Nagaraju, "An optimized method for concealing data using audio steganography", International Journal of Computer Applications, 2011.
- [7] Mazhar Tayel, Ahmed Gamal, Hamed Shawky "Denoising of Stego-images for different noise models" The 18th International Conference on Advanced Communications Techonolgy, 2015.



Mazhar B. Tayel was born in Alexandria, Egypt on Nov. 20th, 1939. He was graduated from Alexandria University Faculty of Engineering Electrical and Electronics department class 1963. He published many papers and books in electronics, biomedical, and measurements. Prof. Dr. Mazhar Basyouni Tayel had his B.Sc. with honor degree in 1963, and then he had his Ph.D.

Electro-physics degree in 1970. He had this Prof. Degree of elect. And communication and Biomedical Engineering and systems in 1980. Now he is Emeritus Professor since 1999. From 1987 to 1991 he worked as a chairman, communication engineering section, EED BAU-Lebanon and from 1991 to 1995 he worked as Chairman, Communication Engineering Section, EED Alexandria. University, Alexandria Egypt, and from 1995 to 1996 he worked as a chairman, EED, Faculty of Engineering, BAU-Lebanon, and from 1996 to 1997 he worked as the dean, Faculty of Engineering, BAU - Lebanon, and from 1999 to 2009 he worked as a senior prof., Faculty of Engineering, Alexandria. University, Alexandria Egypt, finally from 2009 to now he worked as Emeritus Professor, Faculty of Engineering, Alexandria University, Alexandria Egypt. Prof. Dr. Tayel worked as a general consultant in many companies and factories also he is Member in supreme consul of Egypt. E.Prof. Mazhar Basyouni Tayel.



Ahmed Gamal Abdalatif is a Post Graduate Student (master), Alexandria University, Egypt. He was born in Sharkia, Egypt on june, 1985. He received many technical courses in electronic engineering design and Implementation.



Hamed Shawky Zied is an affiliate instructor in Faculty of Engineering, Alexandria University, Alexandria, Egypt. And became a Member of IEEE in 2012. He was born in Minoufia, Egypt in 1973. He holds B.Sc. in Electronics and Communications from Faculty of Engineering, Alexandria University, M.Sc. in Electrical Engineering from Faculty of Engineering, Alexandria University. And Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University. He received many technical courses in electronic engineering design and Implementation. Teach up to 10 undergraduate subjects; publish more than 10 papers in different international conferences and journals.