Audio Steganography using Modified Enhanced Least Significant Bit in 802.11n

Carolus Ferdy Setiaji Hartoko[1], Dr. Suhartono Tjondronegoro[2], Dr. Bambang Hidayat[3]
[1] The School of Electrical Engineering Telkom University
[2] The School of Electrical Engineering and Informatics, Bandung Institute of Technology
[3] The School of Electrical Engineering Telkom University
[1]carolusferdy@students.telkomuniversity.ac.id, [2] shtntjnegoro@stei.itb.ac.id, [3]bhidayat@telkomuniversity.ac.id

Abstract

Steganography is a technique to improve the security of data, which is by inserting messages or confidential information using a medium called the host or carrier or cover. A wide variety of digital media can be used as a host, among others audio, image, video, text, header, IP datagram, and so forth. For audio steganography, the embedded audio is called stego-audio. Steganography can be cracked by using steganalysis. By exploiting the weaknesses of each steganography method. Many steganography method has been developed to increase its performance. This work proposed audio steganography scheme called MELSB which is modified version of ELSB. This method use Modified Bit Selection Rule to increase SNR and robustness of stego-audio. SNR result after applying MELSB scheme is increased. MELSB scheme also increase robustness of stego-audio. MELSB still work fine until amplification level 1.07. MELSB also work fine against noise addition better than ELSB and LSB. It give BER and CER with value 0 at SNR 33 dB. MELSB work fine in real-time condition on 802.11n WLAN if there is no transcoding and noise addition between sender's and recipient's computer

Keywords: Steganography, Modified Enhanced Least Significant Bit, 802.11n

1. Introduction

In this era of technology, electronic communication has become a necessity in human life. Internet growth accelerated to encourage various researches to improve the security of data, whether they are public or private. There are three techniques used, namely cryptography, steganography and watermarking.

Steganography is a technique to improve the security of data, which is by inserting messages or confidential information using a medium called the host or carrier or cover. A wide variety of digital media can be used as a host, among others audio, image, video, text, header, IP datagram, and so forth. As cryptography that can be solved by cryptanalysis, steganography can be solved by using steganalysis. By exploiting the weaknesses of a steganography method, steganalysis continue to be developed in order to solve steganography for a variety of media and methods of insertion.

For this reason, it is necessary to develop a new steganographic method or develop from existing methods. Modified Enhanced Least Significant Bit (MELSB) is a method developed from the Enhanced Least Significant Bit (ELSB) method which is included in the temporal domain insertion method category. The differences that owned by MELSB is the Modified Bit Selection rule and Sample Selection rule making confidential information is not easily detected. MELSB method will be tested on 802.11n channel to determine the performance and resistance in wireless channel.

2. Basic Theory

2.1 Steganography

Steganography comes from the Greek Steganos, which means "hidden" and graphein which means "to write" [7]. Media used to hide secret messages referred to as the host and confidential information that would embed into the host called a message. Media used as a host or a message in the form of multimedia files such as images, audio, video, or text. Steganography is used to send a very important message so as not to be stolen in transmission or to give a sign to a file that can contain information about copyright or hidden serial number.

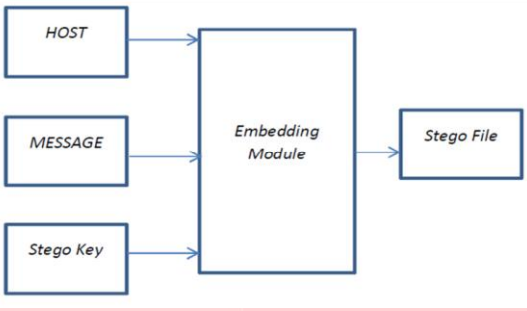

Fig 1. Steganography General Scheme

2.2 Enhanced Least Signficant bit (ELSB)

Enhanced Least Significant Bit is a modification of the method of Least Significant Bit. This method can be done in two ways. The first way is to randomize the number of bits of the host file that is used for embedding secret messages. While the second way is to randomize the sample host containing a secret message bits the next. In Enhanced Least Significant Bit, where the bits on the host used to embed message is not always the same. Ashima Wadhwa [16] identifies that ELSB work fine against steganalysis attacks and has advantages compared to the LSB.

Table 1. ELSB bit selection rule [12]

1st MSB	2nd MSB	Secret message bit
0	0	3rd LSB
0	1	2nd LSB
1	0	1st LSB
1	1	1st LSB

Table 2. ELSB sample selection rule [12]

1st MSB	2nd MSB	3rd MSB	Sample containing next secret message bit
0	0	0	i + 1
0	0	1	i + 2
0	1	0	i + 3
0	1	1	i + 4
1	0	0	i + 5
1	0	1	i + 6
1	1	0	i + 7
1	1	1	i + 8

2.3 Modified Enhanced Least Significant Bit (MELSB)

Bit selection rule from ELSB method, in this work will be changed. Changes made when 1st MSB and 2nd MSB are 0 and 0. In ELSB when first two MSB is 0 and 0, 3rd LSB is used to embed message bit. In MELSB when first two MSB is 0 and 0, 1st LSB is used to embed message bit. This is done in order to make changed value on the host are not too visible when message insertion process is done. MELSB has complexity like ELSB. For N message characters to embed, MELSB need $8N_m$ to 64 N_m substitution operation which needs 3 cycles per operation. If 1 sample need 1 Byte, MELSB need 8 N_m to 64 N_m Bytes of memory.

Table 3. MELSB bit selection rule

1st MSB	2nd MSB	Secret message bit
0	0	1st LSB
0	1	2nd LSB
1	0	3rd LSB
1	1	3rd LSB

Table 4. Complexity and Memory Comparison of LSB, ELSB, and MELSB. N_m is Number of Message Characters

Method	Complexity	Memory
LSB	$8N_m$	$8N_m$ Bytes
ELSB	$8N_m$ to $64N_m$	$8N_m$ to $64N_m$ Bytes
MELSB	$8N_m$ to $64N_m$	$8N_m$ to $64N_m$ Bytes

Table 5. Comparison of LSB, ELSB, and MELSB insertion method

Method	Strong Points	Weak Points
Lowest Bit Coding (LSB)	• Low computational complexity • High bit rate • Easier implementation	• Less prone to attacks • Amplifying, noise addition and compression of audio will destroy the data • Extraction is easy
Enhanced Least Significant Bit (ELSB)	Randomness in the bit selection and sample selection providing more security.	Compression will destroy the data
Modified Enhanced Least Significant Bit (MELSB)	Modified Bit Selection give higher SNR to stego-audio.	Compression will destroy the data

2.4 MELSB Steganography Block Diagram

A block diagram of steganography of this thesis can be seen in Figure 2. Input host data is speech signal mono with a sampling frequency 8000 Hz and each sample is encoded to 8 bits. The use of sampling frequency 8000 HZ and 8-bit encoding in order MELSB insertion pattern in Table 2 and Table 3 can be met. In this Thesis using 802.11n Wireless LAN with 1 spatial stream and 20 MHz channel.

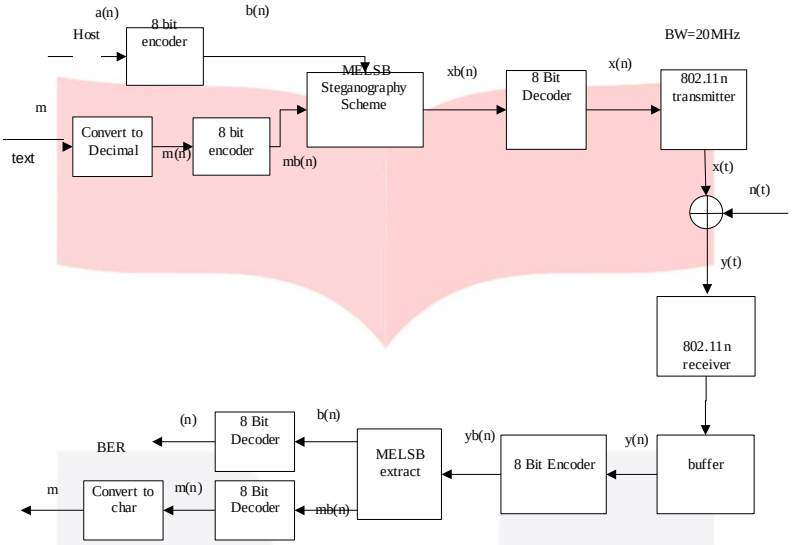

Fig 2. MELSB Steganography Block Diagram

3. Implementation and Testing

3.1 Non Real-Time Implementation

3.1.1 Message embedding process

The message that will be inserted into the host is prepared beforehand. Decimal ASCII value of each character is obtained. Then the decimal ASCII value of each character is converted into 8 bits binary number. While user talk through a microphone each voice samples are converted into 8 bits binary form and message bits embedded at the same time. After embedding process done stego-audio will be stored in a variable. This variable can be send to recipient computer at different time.

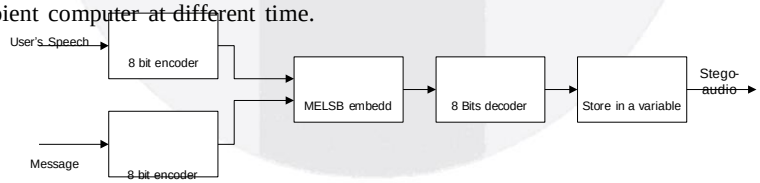

Fig. 3 Message Embedding Process

3.1.2 Non Real-Time Sending Process

Transmission between two computers using TCIP / IP which is works on the client-server principle. The sender computer will act as the server and the recipient's computer acts as the client. The network used is Wireless-LAN 802.11n. After sender and recipient is connected in network, sender will load the variable that contain stego-audio data. This variable is then sent to the recipient's computer.

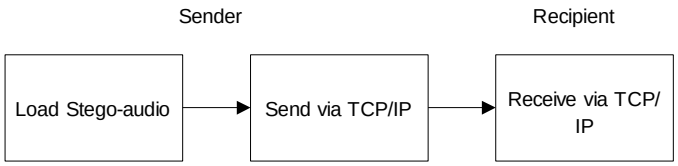

Fig 4. Non Real-Time Sending Process

3.1.3 Non Real-Time Extraction

Variable contains the stego-audio data that has been received in the recipient's computer will go through the process of extraction. The extraction process is done when stego-audio data is completely received, given the real condition of the recipient does not know how long the message is sent. The extraction process is the process of taking all the bits along the received stego-audio data with following the pattern in Table 1 and Table 3.

3.2 Real-Time Implementation

3.2.1 Real-Time Embedding and Sending

Real-time embedding and sending process is similar to the process of non-real-time sending. The message that will be inserted is prepared beforehand and converted into 8 bits binary for each character. Once the sender and receiver are connected, the user at the sender will speak at the microphone and embedding process will be carried out simultaneously. The voice that already contains the message will be sent directly to the recipient without being stored into a memory or a variable.

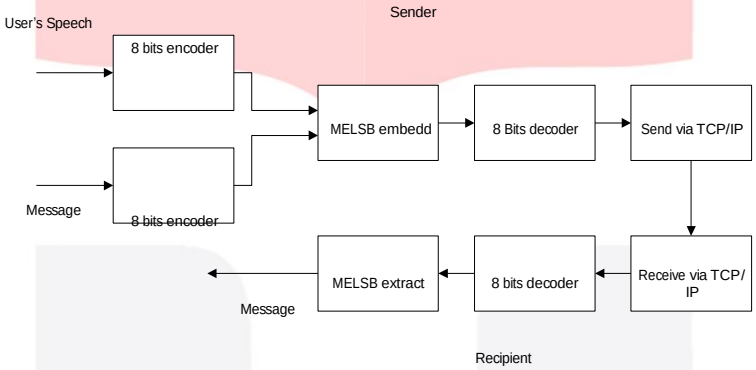

Fig 5. Real-time Implementation Block Diagram

3.2.2 Real-Time Extraction

Extraction process in recipient computer will be carried simultaneously while Recipient's computer receive stego-audio data from sender's computer. The received data will get straight through extraction process by taking the message bits in the received stego-audio data based on the pattern in Table 2 and Table 3.

3.3 Robustness Test

This test is conducted to measure MELSB robustness compared with LSB and ELSB method. Bit Error Rate (BER) and Character Error Rate (CER) will be calculated in this test.

3.3.1 SNR Testing

This test was conducted to prove that the SNR of audio after embedding messages is larger when using the MELSB scheme (ELSB with modified bits selection rules). This test was conducted using LSB, ELSB, and MELSB scheme. SNR is obtained by using this formula

$$SNR = 10 \log_{10} \quad (1)$$

3.3.2 Amplification Test

Amplification test conducted to determine the robustness of the MELSB methods against amplification compared with ELSB and LSB. Amplification here is increasing the amplitude of the audio signal that had been inserted by a message. Stego-audio is amplified with amplification level from 1 to 2 with interval 0.01. After amplified, message will be extracted from stego-audio depend on how stego-audio was made. If stego-audio was made using LSB method, the message will be extracted using LSB extraction scheme. If it was made using ELSB method, the message will be extracted using ELSB scheme, and as well as when using MELSB method. BER and CER of the extracted message will be calculated.

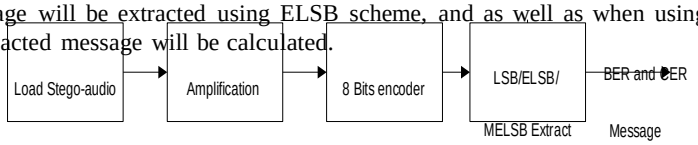

Fig 6. Amplification Test Block Diagram

3.3.3 Testing Against Noise Addition

Testing is conducted by add AWGN noise in the audio signal that had been inserted with a message (stego-audio) using LSB, ELSB, and MELSB insertion method. SNR of stego-audio continuously increased from 1 dB to 50 dB. After adding noise, message in stego-audio will be extracted depend on how stego-audio is made. BER and CER of the inserted message will be calculated.

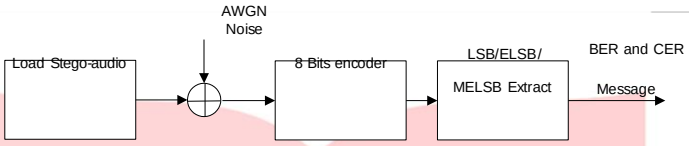

Fig 7. Noise Addition Test Block Diagram

3.3.4 Compression / Transcoding Test

Stego-audio is compressed from 64 Kbps to ADPCM 32 Kbps. After stego-audio is compressed, message in stego-audio will be extracted, then BER and CER of extracted message is calculated.

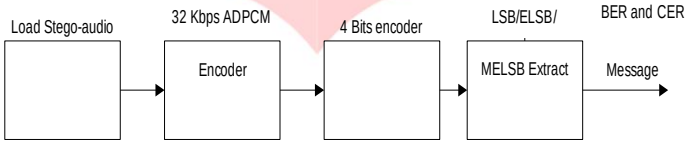

Fig 8. Compression / Transcoding Test Block Diagram

3.4 MELSB Steganography Testing on 802.11n WLAN

Testing was performed using 802.11n WLAN network in the campus of the Faculty of Engineering, Telkom University to measure MELSB method performance and latency. Tests carried out at three different places using two computer act as sender and recipient using Real-time scheme without taranscoding and noise addition. The message that will be embedded is '**The quick brown fox jumps over a lazy dog 1234567890**.'.

4 Result and Analysis

4.1. SNR Result after Embedding

The results of 30 attempts of SNR test can be seen in the table 6.

Table 6. SNR Testing Result Using ELSB, MELSB, and LSB

Attempt	SNR (dB)		
	LSB	ELSB	MELSB
1	44.36173	35.99525	40.63282
2	46.65434	33.80618	40.15372
3	40.87727	36.28362	44.21818
4	43.2815	37.17845	40.86791
5	41.99188	34.13527	41.3105
6	38.92647	33.24726	39.17588
7	41.01622	33.14977	40.84485
8	43.90634	37.20582	42.06382
9	37.84235	34.53976	40.69677
10	39.4386	35.54426	42.48434
11	38.70683	37.42117	40.53558
12	47.17619	39.3466	42.74927
13	43.26216	33.07516	41.107
14	41.38815	38.06389	38.62263
15	41.50903	41.08978	38.74961
16	44.02229	36.82805	44.90617

17	41.01958	37.15722	39.32776
18	40.61701	36.71136	41.71994
19	40.16404	47.53137	42.00134
20	39.40574	34.52373	42.4399
21	42.13484	34.77714	42.42505
22	44.81598	33.63326	39.55485
23	38.88055	34.71129	40.29103
24	40.32901	34.43852	42.49332
25	40.51863	38.9727	39.04027
26	38.34437	32.67965	41.21652
27	40.05223	45.22093	44.81666
28	40.73492	37.20063	42.3634
29	42.29691	34.49359	39.68386
30	49.53513	43.07145	45.23205
Average	41.77368	36.73444	41.39083

As seen in Table that average SNR after embedding using MELSB scheme is smaller than LSB scheme but larger than ELSB. Modified Bit Selection Rule in MELSB method replace 1st LSB of host-audio when the first two MSB is "00", while Bit Selection Rule in ELSB replace 3rd LSB. So the difference value between host-audio and stego-audio is smaller when using MELSB, with the result that MELSB scheme give larger SNR than ELSB.

4.2 Amplification Test Result

Result of amplification test can be seen in table 7 and table 8. As seen in table, MELSB method still works well until amplification 1.07, which means amplitude value is enlarged by 7% from previous value. It means amplification mostly affecting 1st LSB of stego-audio. When the amplitude value of stego-audio is enlarged by amplification 1st LSB of stego-audio is mostly changed .Modified Bit Selection Rule in MELSB have better robustness against amplification, because it replace 3rd LSB when first two MSB is "10" or "11", while Bit Selection Rule in ELSB replace 1st LSB.

Table 7. BER after Amplification Testing Result for file 'rekamanlagi.wav'

Amplification	Message BER		
	LSB	ELSB	MELSB
1	0	0	0
1.01	0	0	0
1.02	0	0	0
1.03	0	0	0
1.04	0	0	0
1.05	0	0	0
1.06	0.018868	0.023585	0
1.07	0.044811	0.051887	0
1.08	0.153302	0.134434	0.113208
1.09	0.283019	0.20283	0.113208
1.1	0.384434	0.264151	0.113208

Table 8. CER after Amplification Testing Result for file 'rekamanlagi.wav'

Amplification	Message CER		
	LSB	ELSB	MELSB
1	0	0	0
1.01	0	0	0
1.02	0	0	0
1.03	0	0	0
1.04	0	0	0
1.05	0	0	0
1.06	0.056604	0.113208	0
1.07	0.056604	0.150943	0
1.08	0.301887	0.245283	0.528302
1.09	0.320755	0.264151	0.528302
1.1	0.566038	0.471698	0.528302

4.3 Result Against Noise Addition

The test results of noise addition test can be seen in the image below. All of method work fine if SNR is above 30 dB. MELSB produce BER and CER with value 0 at SNR 33 dB, ELSB at SNR 34 dB and LSB at SNR 35 dB. Sample Selection Rule combined with Modified Bit Selection Rule in MELSB method increase the robustness against noise addition.

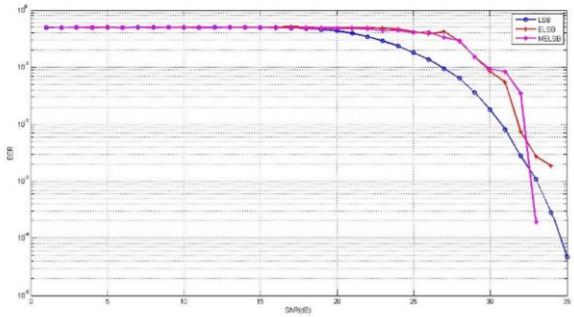

Fig. 9 BER Result after Noise Addition

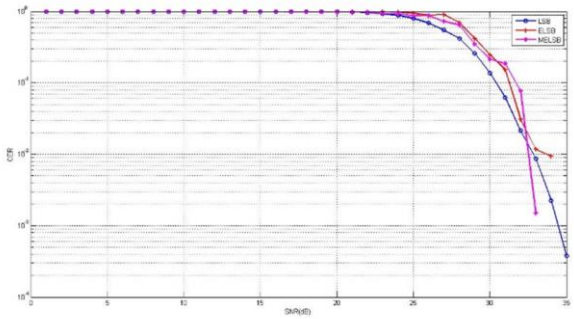

Fig 10. CER Result after Noise Addition

4.4 Compression / Transcoding Test Result

All of embedding method is weak against compression / transcoding because the amplitude value is changed after compression, so when it encoded into 8 bits binary form, the binary value of amplitude and embedded messages is changed as well.

Table 9. Message BER and CER after Compression Result for file 'rekamanlagi.wav'

Method	BER	CER	Extracted message
LSB	0.466981	0.981132	'^| '
ELSB	0.436321	0.981132	''
MELSB	0.474057	1	''

4.5 MELSB Steganography Testing Results on 802.11n WLAN

As seen in Table 10 MELSB scheme works fine in 802.11n WLAN in real time condition. It gives CER with value 0, if there's no transcoding and noise addition between sender and recipient. Total average latency in real time condition on 802.11n is between 900 milliseconds to 1200 milliseconds, while WLAN latency is between 0.8 milliseconds to 5.8 milliseconds. This means MELSB scheme (embedding and extracting process) takes more time be processed. Latency also affected by speech data retrieval process from microphone and 8 bit encoder/decoder in sender and recipient side.

Table 10. Steganography Testing Result on 802.11n Network

Attempt	Room/Place	WLAN Bit rate	Number of User	Sender-recipient distance	Result	Average total Latency (second)	WLAN latency (second)
1	DSP Research Lab, Telkom University	65 Mbps	49	± 3m	Voice is clean, CER = 0	0.968906574	0.000984625
2	DSP Research Lab, Telkom University	11 Mbps	94	± 3m	Voice is clean, CER = 0	1.135028181	0.005818192
3	DSP Research Lab, Telkom University	11 Mbps	94	± 3m	Voice is clean, CER = 0	1.159217845	0.005818192
4	B Building, Telkom University	72.2 Mbps	9	± 3m	Voice is clean, CER = 0	1.219979404	0.000886437
5	B Building, Telkom University	72.2 Mbps	9	± 3m	Voice is clean, CER = 0	1.158339406	0.000886437
6	B Building, Telkom University	72.2 Mbps	9	± 3m	Voice is clean, CER = 0	1.147673246	0.000886437
7	Graduate School G206, Telkom University	21 Mbps	6	±7m	Voice is clean, CER = 0	1.160236403	0.003047642
8	Graduate School G206, Telkom University	21 Mbps	6	±7m	Voice is clean, CER = 0	1.149752728	0.003047642
9	Graduate School G206, Telkom University	21 Mbps	6	±7m	Voice is clean, CER = 0	1.153833861	0.003047642

5 Conclusion

a) Modified bit selection rule in MELSB can increase SNR of stego-audio better than ELSB. Because it replace 1st LSB of host-audio when the first two MSB is "00", while Bit Selection Rule in ELSB replace 3rd LSB. So the difference value between host-audio and stego-audio is smaller when using MELSB, with the result that MELSB scheme give larger SNR than ELSB.

b) MELSB is stronger than ELSB against amplification. Amplification mostly affecting 1st LSB of stego-audio. When the amplitude value of stego-audio is enlarged by amplification 1st LSB of stego-audio is mostly changed .Modified Bit Selection Rule in MELSB have better robustness against amplification, because it replace 3rd LSB when first two MSB is "10" or "11".

c) MELSB is stronger than ELSB and LSB against noise addition due to combination of Sample Selection rule and Modified Bit Selection rule.

d) LSB, ELSB, and MELSB method is cannot work against transcoding. Transcoding changed the amplitude value of stego-audio. When amplitude value is encoded into 8 bits binary form, the binary value of amplitude and embedded messages bits is changed as well

e) MELSB can work fine in real time transmission using 802.11n Network if there is no transcoding and noise addition between sender and recipient.

f) MELSB scheme takes more times to be processed in real-time condition. As seen in Table 5.9, total average latency is larger than WLAN latency.

Reference:

1. Babu, Linu, et al.2013. *Steganographic Method for Data Hiding in Audio Signals with LSB & DCT*, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 8, pg.54 – 62
2. Bing, Benny. 2008. *Emerging Technology in Wireless LANs Theory*, Designs, and Deployments. Cambridge University Press
3. Codr, Jessica. 2009. *Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide*. jmc5@cec.wustl.edu (A project report written under the guidance of Prof. Raj Jain)
4. D. Gruhl and W. Bender. 1996. "*Echo hiding*", Proceeding of Inforomation Hiding Workshop, pp. 295315
5. Eldad Perahia, Robert Stacey. 2008. *Next Generation Wireless LANs*. Cambridge University Press
6. Fatiha Djebbar, Beghdad Ayad Karim, Abed Meraim and Habib Hamam. 2012. " *Comparative Study of Digital Audio Steganography Tech-niques*," EURASIP journal on audio, speech and music processing 2012, 2012:25
7. Jayaram P, Ranganatha H R, Anupama H S. 2011. *Information Hiding Using Audio Steganography – A Survey*. The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3
8. Jhoni Verlando Purba, Marihat Situmorang, Dedy Arisandi. 2012. *Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan Modifikasi Jarak Byte Pada Algoritma Least Significant Bit (Lsb)*, Jurnal Dunia Teknologi Informasi Vol. 1, No. 1, 50-55
9. Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski. *4 New Ways to Smuggle Messages Across the Internet*. IEEE Spectrum (http://spectrum.ieee.org/telecom/security/4-new-ways-to-smuggle-messages-across-the-internet)
10. Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski. *Principles and Overview of Network Steganography*. Institute of Telecommunications, Warsaw University of Technology, Warsaw: Poland
11. M.Baritha Beguma, Y.Venkataramanib. 2012. *LSB Based Audio Steganography Based On Text Compression*. International Conference on Communication Technology and System Design. Volume 30, pages 703–710
12. Muhammad Asad, Junaid Gilani, Adnan Khalid. 2011. *An Enhanced Least Significant Bit Modification Technique for Audio Steganography*, International Conference on Computer Networks and Information Technology (ICCNIT), pages 143-147
13. Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik," *LSB Modification and Phase Encoding Technique of Audio Steganography Revisited*," International Journal of Advanced Research in Computer and Communication gineering Vol. 1, Issue 4, June 2012.
14. Richer, Pierre. 2003. Steganalysis: *Detecting hidden information with computer forensic analysis*. SANS Institute
15. Richey, Rodger. 1997. *Adaptive Differential Pulse Code Modulation using PICmicro™ Microcontrollers*. Microchip Technology Inc.
16. Wadhwa, Ashima. 2014. *A Survey on Audio Steganography Techniques for Digital Data Security*. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 4