Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

Enhanced Security Audio Steganography by Using Higher Least Significant Bit

S. Krishnan[*,a], *M. S. Abdullah*[b]

Advanced Information School, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra (Jalan Semarak), 54100 Kuala Lumpur, Malaysia

[a,*]*surenthiran@mod.gov.my*, [b]*mshahidan@utm.my*

Abstract – *Data hiding is an approach that conceals secret data into a carrier. Steganography is the art and science of storing information so that its existence is hidden. The goal of steganography is to communicate securely in a completely undetectable manner and hiding data efficiently to avoid unintended recipients to suspect the existence of steganographic medium that contains hidden data. The study had found that that the audio steganography using LSB technique can be easily broken to retrieve the data and vulnerable in security due to its low robustness. In this research, the scheme of Audio Steganography will be investigated to enhance LSB scheme with AES encryption and evaluate the robustness and quality of the scheme. This research presents Enhanced Security in Audio Steganography by using Higher Least Significant Bit to improve security and robustness by embedding bits of secret message in higher LSB of a cover audio. The stego key and AES encryption are applied to increase the security of the stego audio. Encoding process embeds the secret message while decoding process retrieves the secret message. In audio steganography, the secret message is embedded into a digitized audio signal which results in significant altering of binary sequences of the corresponding audio file. The result shows the scheme is robust and able to withstand steganography unintentional attack which is compression till 17% at maximum payload of 953 bps at 11th LSB. This new scheme model is proven to increase the robustness using higher LSB and will be useful as a basis for Audio Steganography.*

Keywords: Audio Steganography, LSB, Payload, Imperceptibility, Robustness

1.0 INTRODUCTION

Steganography is one of the mean used for safe and protected transmission of confidential information [1]. Hiding information in audio is safe and less doubtful than communicating an encrypted file. The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as image, audio or video [2, 3]. These objects are called cover objects or carrier objects of the steganographic method.

A review on list of journals show that LSB method of audio steganography is vulnerable for data leakage of secret message on a steganography medium [4, 5, 6]. LSB technique is simple and modest that allows hiding secret message on least significant bits. This technique can be easily broken to retrieve the secret message due to its low robustness. Therefore, the hidden

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

data should be retrieved by authenticate user without any tolerance. This shows that there is an immediate need to protect the secret message by enhancing the security of the LSB technique. Many researches have been carried out to enhance the quality and performance of audio steganography, but yet the robustness of LSB technique still can be compromised. Most of the techniques are less effective to provide a robust and strong LSB method. In contrast, the proposed research is an enhancement of the security of the LSB scheme.

The term Steganography derives from the Greek steganos which is protected or secret and graphy which is writing or drawing [7, 8]. In other words, Steganography can be well-defined as the art of storing information to be hidden and concealed [9, 10]. The goal of steganography is to establish a secure communication in an absolutely untraceable way and to hide data well enough that unintentional recipients do not doubtful about the steganography object which comprehends secret data [11].

Cryptography and steganography are inimitable ways to defend information from intruders nonetheless technology and skills are perfect to lead those ways to be compromised [9, 12]. The purpose of steganography can be considered partially defeated if the hidden information is revealed or even suspected, [9, 13]. Cryptography supports in keeping the message as a secret while steganography supports in keeping the existence of the message as a secret. They can be considered as defeated if the data hidden is discovered [13].

Table 1: Summary of Audio Steganography Techniques [4]

Method	Strength	Drawbacks
Least Significant Bits	Simple, Modest	Easy to extract and retrieve data
Parity coding	More robust than LSB	Easy to extract and retrieve data
Echo hiding	Evades problem with additive noise	Low capacity
Tone insertion	Exploits masking property	Low embedding capacity
Phase coding	Robust, Higher resistance	Low capacity
Spread spectrum	Increases transparency and imperceptibility	Occupies more bandwidth
Wavelet domain	Capable to hide large amount of data, higher hiding capacity and transparency	Lossy data retrieval A portion of data might be lost due to compression.

The basic model of Audio Steganography consists of Carrier (Audio file), Message, Password, Stego file. The carrier is also known as a cover file which conceals the secret information [5, 14]. Audio steganography is an apprehensive with a data hiding in cover audio signal in an imperceptible way. The secret message is embedded into a digitized audio signal which results into altering binary sequence of the corresponding audio file [7, 15].

Table 1 shows a summary of audio steganography techniques. Least Significant Bit is one of the most simple and modest technique of data hiding compared to other domain with its different techniques studied. This simplicity allows for frequent modification and alteration of

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

the techniques which is desired by the users. Unfortunately, Least Significant Bit shows the tolerance to extract and retrieve data and which is vulnerable for data hiding compared to other domain with its different techniques studied and become the drawbacks for this method compared to other domain.

In this section, there are many ways to implement steganography especially in audio which can be combined with encryption to enhance its security. Eventually, the LSB technique needs a thorough alteration to form Audio Steganography with good robustness and security. This leads to the next stage of proposing the methodology, which is discussed in the next section of this paper.

2.0 METHODOLOGY

2.1 Proposed Model

The Proposed Model for audio steganography to enhance the security of the LSB method has been designed as presented in Figure 1. The proposed model output will be an encrypted stego-audio which is similar as cover audio. The extracted secret message during the decoding process and AES decryption would have a trade-off between capacity and robustness. The capacity will be a trade-off with robustness which uses higher LSB and another layer of security which is AES encryption.

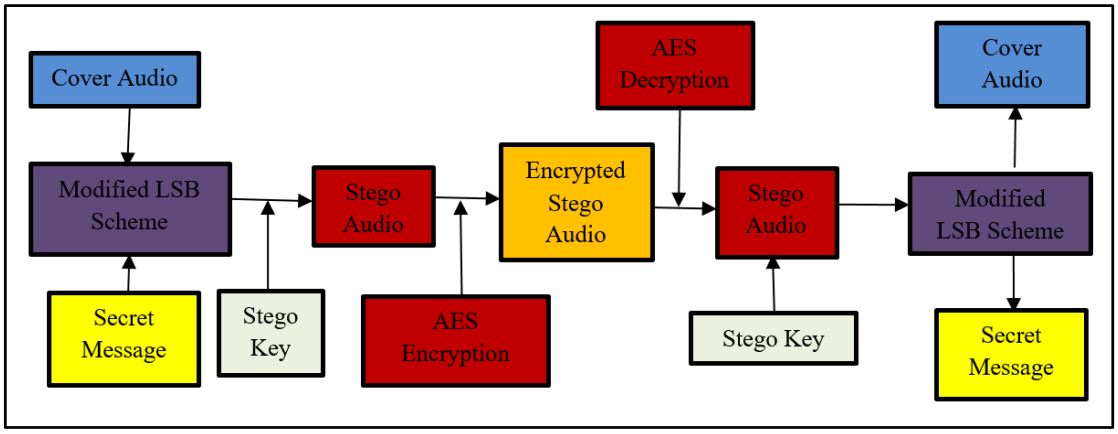

Figure 1: Proposed Model

Table 2: Process in Each Phase at Sender and Receiver

Phase	Sender	Receiver
Phase 1	Secret Message & Cover Audio Conversion to Binary	Stego Audio Receive
Phase 2	Identification and authentication	AES decryption
Phase 3	LSB Embed Secret Message with Stego Key	Identification and authentication
Phase 4	AES encryption	Inverse LSB Extract Secret Message with Stego Key
Phase 5	Stego Audio Transmit	Binary Conversion to retrieve Secret Message

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

This proposed model consists of two main parts and these are the sender and the receiver. The sender involves encoding process while the receiver functions in decoding process. Each part has been divided into five phases for simplicity and tolerance during the execution of the proposed model as shown in the Table 2.

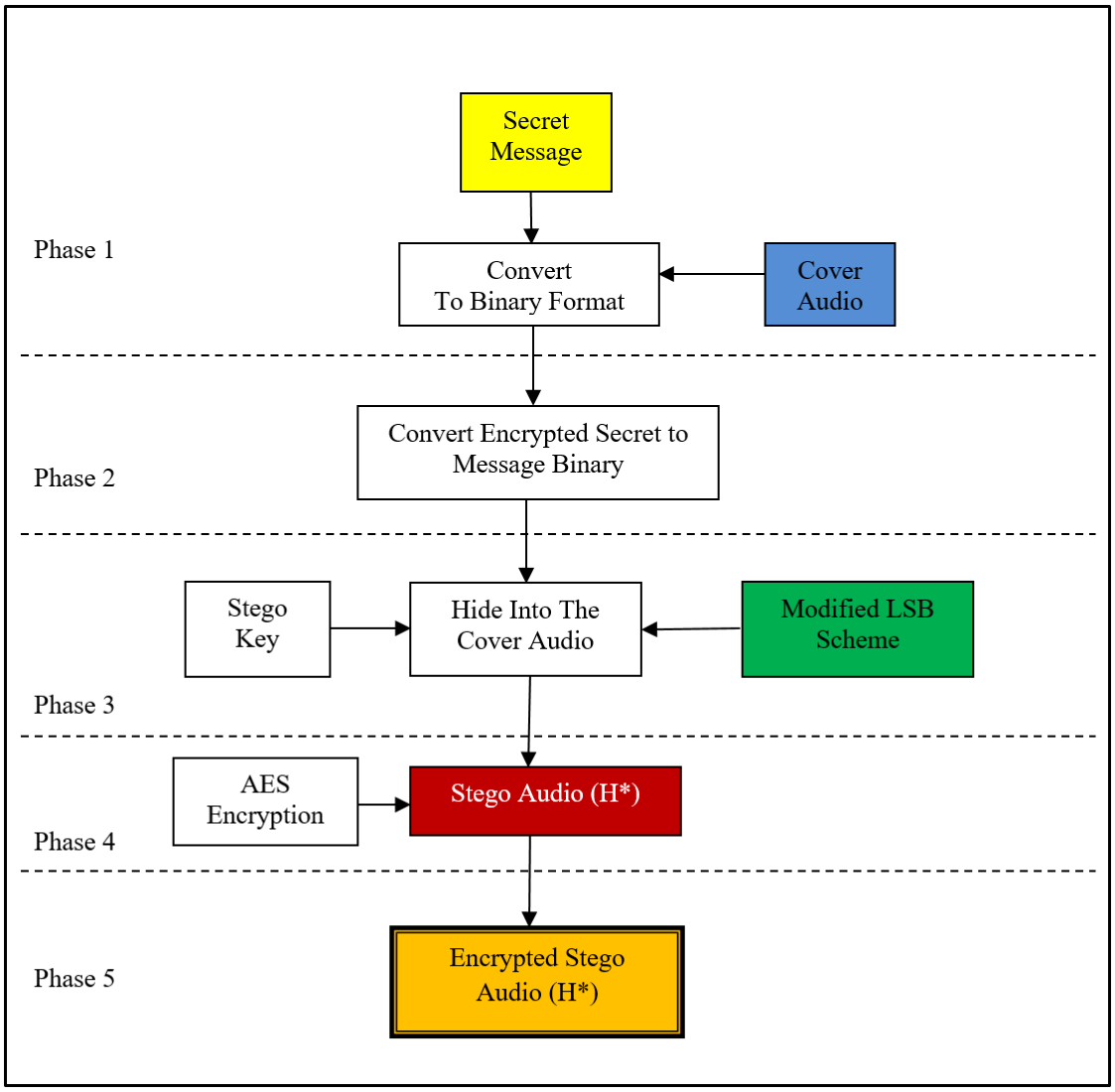

Figure 2: Encoding process for AES encryption and LSB embedding

A secret message in the form of ASCII characters is embedded within a carrier of an audio file (.wav) with LSB function. After the secret message insertion into cover audio with LSB bits selection, the Cover Audio will be encrypted again. The output will be similar to the cover audio with a secret message embedded inside it which also known as Stego Audio. The Proposed scheme consists of the following two main parts as below:

(i) Sender side (Encoding process)
(ii) Receiver side (Decoding process)

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

2.2 Encoding Process

Encoding Process on Sender Side (Secret Data Hiding) takes place at the sender side to hide the secret information. The carrier audio file and a secret message will be converted to binary formats. Bits of secret information will be hidden using modified LSB scheme in carrier audio file. The steps of encoding process in Figure 2 are as follows:

(i) Convert the cover audio file and secret message to binary format.
(ii) Stego key configured in 8 bits for identification and authentication.
(iii) Hide the secret information into a cover audio file using LSB scheme.
(iv) Generate the stego key.
(v) AES encryption applied.
(vi) Key and the stego audio are sent to the receiver.

2.2 Decoding Process

Decoding process will take place in the receiver side to extract the encrypted secret information and decrypt it to obtain the secret message the inverse of the modified scheme. The stego key is used to gain access to the secret information. Secret message can be retrieved with appropriate and correct parameter values which corresponding from the encoding process. The steps of decoding process are as shown in Figure 3 and as follows:

(i) The receiver will decrypt the AES encryption of stego audio.
(ii) The decrypted Stego Audio will be authenticate with its stego key.
(iii) The Cover Audio will be removed from the extracted Stego Audio.
(iv) The hidden bits will be extracted accordingly to its hidden scheme or pattern of LSB. Header's bits, length of secret message's bits and the secret message's bits will be extracted accordingly.
(v) The binary formats of secret message will be converted to decimal and coupling with ASCII code to retrieve its Secret Message.
(vi) The secret message will be displayed immediately.

3.0 RESULT AND DISCUSSION

3.1 Hiding in Higher LSB

Initially, a cover audio file which is '.wav' file is chosen for the data hiding. This is because Matlab R2014a works easily for modification and analysis purpose in '.wav' file. Other formats show much more error due to smaller size or compressed features.
The composition of key embedding elements in an audio sample in cover audio is visualized in Figure 4. The first 40 bytes are used to make as a header for the cover audio. The header function as a reference point for other bits modification. The next 3 bytes which is from 41st byte to 43rd byte is used as a length of wav data samples of the cover audio. The next 16^{th} bit will be the space to embed the secret message, which is from 44^{th} to 60^{th} byte. The higher LSB for embedding the bits from the secret message will be determined in the encoding process.

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

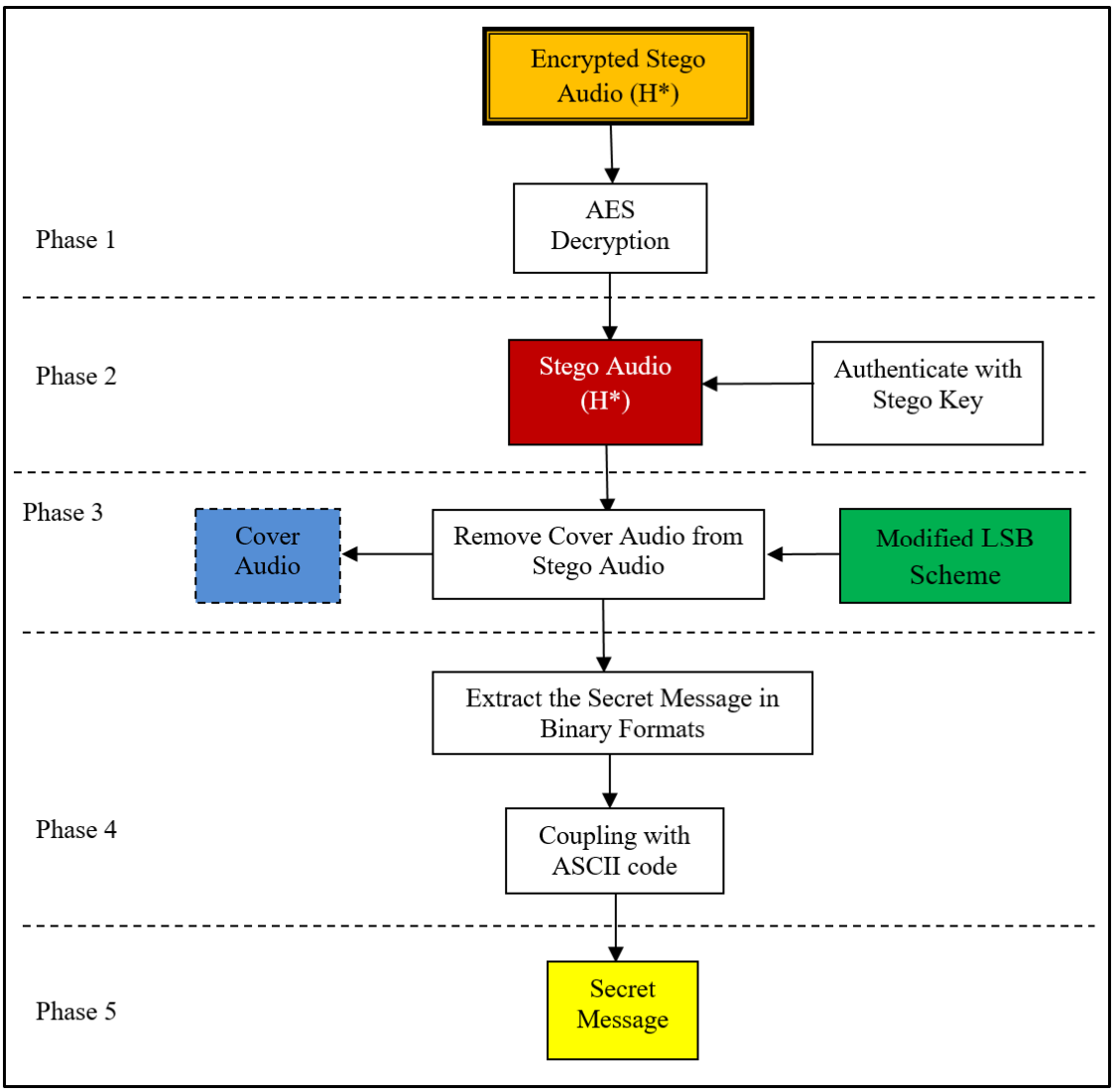

Figure 3: Decoding process for AES encryption and LSB extraction

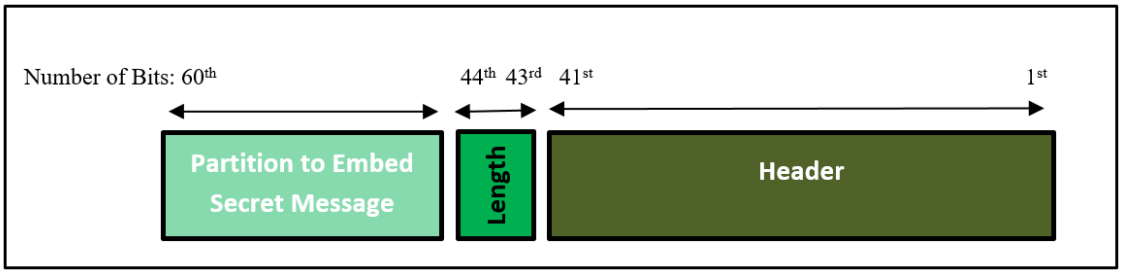

Figure 4: Diagram of Composition of an Audio Sample in Cover Audio for Embedding

Pseudocode for Encoding in Matlab R2014a as shown below:

1. Set total to zero
2. Open a wav file for hidding text
   Call uigetfile

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

Call wavread

3. Store the header and the length of wav data samples
   Call uint (unsigned integer)
4. Copy the 16 bit wav data samples
5. Select LSB to embed
   Call lsb
6. Insert secret message
7. Binary conversion and reshape
   msg_double=double(msg);
   msg_bin=de2bi(msg_double,8)
   [m,n]=size(msg_bin);
8. Insert stego key
9. Embed the bits of stego key and secret message
10. Generate new .wav file – stego audio
    Call fopen
11. Compare cover audio with stego audio for PSNR
    for j = 1:size_host
    s = s+(stegoaudio_double() - coveraudio_double())^2
12. Plotted Normalized Cross Correlation (NCC) for both audio
13. Apply AES encryption

While Pseudocode for Decoding as shown below:

1. Set total to zero
2. Apply AES decryption
3. Open a wav file for extracting text
   Call uigetfile
   Call wavread
4. Open stego audio
   if stego key
   Call fopen
   Else end
5. Binary conversion
   Call uint (unsigned integer)
6. Extract the header and the length of wav data samples
   Call fread
7. Extract 16 bit wav data samples
   Call fread
8. Select LSB to extract
   Call lsb
9. Secret message Size Bits retrieval
   m_bin( )=bitget(dta( ),lsb)
   n_bin( )=bitget(dta( ),lsb)
10. Secret message bits retrieval
    secmsg_bin(:len)=bitget(dta(:+len),lsb)
    secmsg_bin_re=reshape(secmsg_bin,len/8,8)
11. Convert to ASCII code
    secmsg_double=bi2de(secmsg_bin_re)
12. Display secret message

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

3.2 Steganography Attack

Compression is one of the unintentional attacks which will be performed on the audio steganography scheme to measure the ability of embedded data to withstand against the attacks. This attack refers to common data manipulation which is compression and decompression. Different level of compression will be performed on the stego audio to validate the robustness of this scheme.

This section presented the proposed model to enhance security in Audio Steganography by using the higher LSB scheme and AES encryption. The encoding and decoding processes are developed accordingly to meet the requirements of higher LSB to fulfill a better robustness for this scheme. Therefore, this research will implement the proposed scheme and the outcome will be analyzed and validated in the next section.

3.3 Analysis

Embedding a secret message which is 'Surenthiran Krishnan' within a cover audio and the process of decoding the hidden message from stego audio, and finally retrieval of the secret message as shown in Figure 5. Binary conversion and reshape in the vector form plays an important role to carry the bit, channel the bits for embedding and for extraction as well. A good vector matrix should be an appropriate size to fit the possible secret message size. A suitable vector determines the performance and stability of a scheme in Matlab environment.

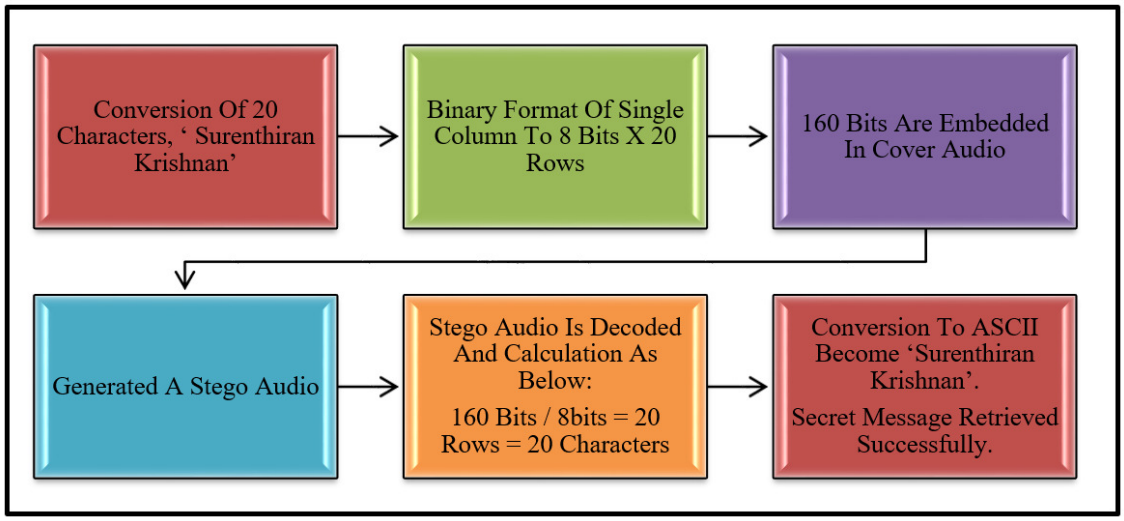

Figure 5: Flow Chart of Encoding and Decoding in Higher LSB Scheme in Matlab R2014a

This proposed higher LSB scheme does not stand for high compression due to the stronger congestion of bits. However, it may stand compression at a level of 17% and below. The maximum compression that can be applied is 17% as shown in Table 3.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

Table 3: Robustness Validation through Compression

Ser	LSB Selection	Cover Audio (kB)	Secret Message Size (kB)	Percentage of Payload (%)	Compression			Ability to retrieve secret message
					Stego Audio Size after Compression	Percentage of Compression (%)	Audio file format	
1.	4	1820	0.035	0.0357	390	80	.acc	No
2.	4	1820	0.035	0.0357	203	90	.ogg	No
3.	4	1820	0.035	0.0357	728	61	.wma	No
4.	4	1820	0.035	0.0357	392	79	.m4a	No
5.	4	1820	0.035	0.0357	501	74	.ape	No
6.	4	1820	0.035	0.0357	1220	33	.wv	No
7.	4	1820	0.035	0.0357	529	72	.flac	No
8.	4	1820	0.035	0.0357	39	98	.mmf	No
9.	4	1820	0.035	0.0357	1596	17	winrar	Yes
10.	8	1820	0.035	0.0357	390	80	.acc	No
11.	8	1820	0.035	0.0357	203	90	.ogg	No
12.	8	1820	0.035	0.0357	728	61	.wma	No
13.	8	1820	0.035	0.0357	392	79	.m4a	No
14.	8	1820	0.035	0.0357	501	74	.ape	No
15.	8	1820	0.035	0.0357	1220	33	.wv	No
16.	8	1820	0.035	0.0357	529	72	.flac	No
17.	8	1820	0.035	0.0357	39	98	.mmf	No
18.	8	1820	0.035	0.0357	1596	17	winrar	Yes
19.	11	1820	0.035	0.0357	390	80	.acc	No
20.	11	1820	0.035	0.0357	203	90	.ogg	No
21.	11	1820	0.035	0.0357	728	61	.wma	No
22.	11	1820	0.035	0.0357	392	79	.m4a	No
23.	11	1820	0.035	0.0357	501	74	.ape	No
24.	11	1820	0.035	0.0357	1220	33	.wv	No
25.	11	1820	0.035	0.0357	529	72	.flac	No
26.	11	1820	0.035	0.0357	39	98	.mmf	No
27.	11	1820	0.035	0.0357	1596	17	winrar	Yes
28.	16	1820	0.035	0.0357	390	80	.acc	No
29.	16	1820	0.035	0.0357	203	90	.ogg	No
30.	16	1820	0.035	0.0357	728	61	.wma	No
31.	16	1820	0.035	0.0357	392	79	.m4a	No
32.	16	1820	0.035	0.0357	501	74	.ape	No
33.	16	1820	0.035	0.0357	1220	33	.wv	No
34.	16	1820	0.035	0.0357	529	72	.flac	No
35.	16	1820	0.035	0.0357	39	98	.mmf	No
36.	16	1820	0.035	0.0357	1596	17	winrar	Yes (Partially)

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

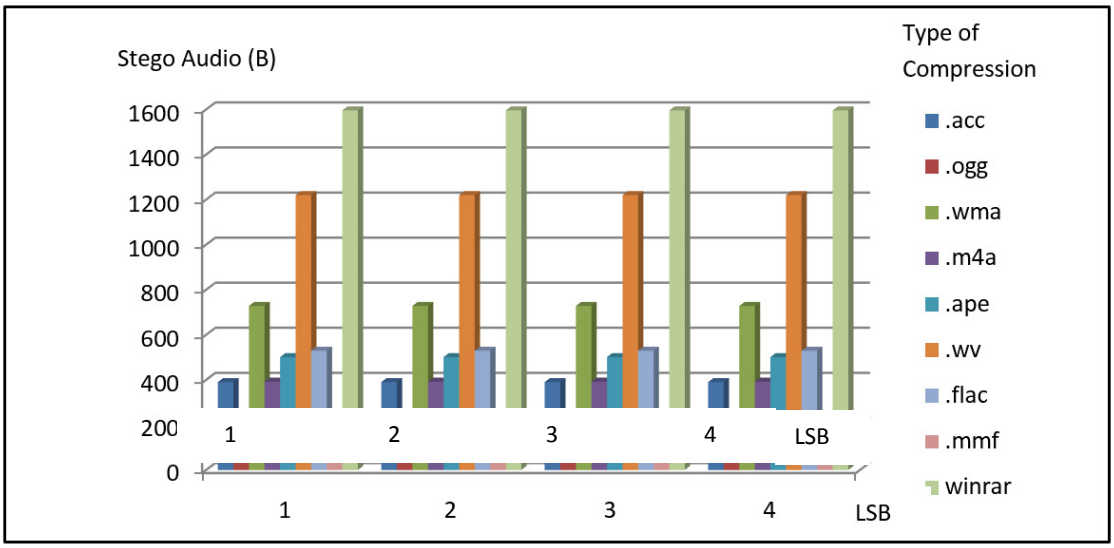

Figure 6: Stego Audio Size after Different Type of Compression

The comparison of the cover audio and the decompressed stego audio from 17% compression which resulted in 83% size of the cover audio. This compression bowdlerized 320kB, which is 257,519 bps. The compression has expurgated most of the lost data. During the decompression process, the scheme will only able to retrieve those data which are strongly attached to the cover audio. So, the bits at higher LSB are safely located in their respective position and sequence with less distortion. In other words, the compression of the stego audio only holds the higher LSB able to sustain.

This section presented the analysis of the proposed scheme to enhance security in Audio Steganography by using LSB and AES encryption. This proposed scheme prevents the intruders or third party to be suspicious about the existence of secret information in the cover audio. The cover audio has same audio performance with good quality and high PSNR which present no detection of audio distortion. A file format that used is .wav format which consists of large bytes compare to other bytes. The scheme shows the trade-off relation between the payload and the robustness of the stego audio. This scheme provides a solution to embed a secret message on other than LSB only where the capacity is traded off with the robustness. The higher LSB is robust, but capable to carry the little secret message.

Enhancement of Security in Audio Steganography by Using Higher Least Significant Bits (LSB) and Advanced Encryption Standard (AES) provides a better data hiding specific in the robustness and the security. AES encryption and stego key have provided double layer security before accessible, partially to the stego audio. As in the higher LSB scheme, the secret message will be embedded at selective positions of higher LSB within the audio carrier where the positions to be determined during the encoding process. It can be considered as a better and efficient method for hiding the data. This proposed scheme is embedding secret bits in higher LSB and increases the robustness and withstands audio compression. AES encryption has increased the level of security before the secret information is being shifted to steganography environment where higher LSB embedding is embarked. This scheme is a combination of steganography and cryptography, which combines secured communication with protected of information. Therefore, there is a need for future study on the combination of steganography and cryptography for the robustness, capacity and quality with a greater data hiding.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

3.4 Noise Added

Basically, the noise is added through the normalized process and noise addition with variations of dB and sensitivity as shown in Table 4.

Table 4: Robustness Validation through Noise Addition

Ser	LSB Selection	Cover Audio (kB)	Secret Message Size (kB)	Noise Addition		Ability to retrieve secret message	Error character in the message
				Noise (dB)	Sensitivity		
1.	2	1820	0.035	10	1	No	-
2.	2	1820	0.035	20	2	No	-
3.	4	1820	0.035	10	1	No	-
4.	4	1820	0.035	20	2	No	-
5.	6	1820	0.035	10	1	No	-
6.	6	1820	0.035	20	2	No	-
7.	8	1820	0.035	10	1	No	-
8.	8	1820	0.035	20	2	No	-
9.	10	1820	0.035	10	1	Yes	Partially
10.	10	1820	0.035	20	2	Yes	Partially
11.	12	1820	0.035	10	1	Yes	Partially
12.	12	1820	0.035	20	2	Yes	Partially
13.	14	1820	0.035	10	1	Yes	Minor
14.	14	1820	0.035	20	2	Yes	None
15.	16	1820	0.035	10	1	Yes	None
16.	16	1820	0.035	20	2	Yes	None

Cover audio and stego audio have an identical spectrum as shown in Figure 6 (a) and (b). Stego audio has been applied with noise and results in an increased wavy signal at a higher frequency of audio properties as shown in Figure 6 (c).

3.5 Quality Analysis

Listening tests showed that perceptual quality of stego audio is higher in the proposed improvised audio steganography than in the standard audio steganography based on LSB. A sample of 20 Malaysian Armed Forces personnel has been taken for this listening test as shown in Table 4 and conducted in a training lab. However, listening tests were conducted on different LSB selection where there, the changes in PSNR value can be noticed and the effect on HAS.

Table 4 indicates the higher PSNR value for lower LSB while the PSNR is reduced when the LSB move from 1st LSB to 16th MSB.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

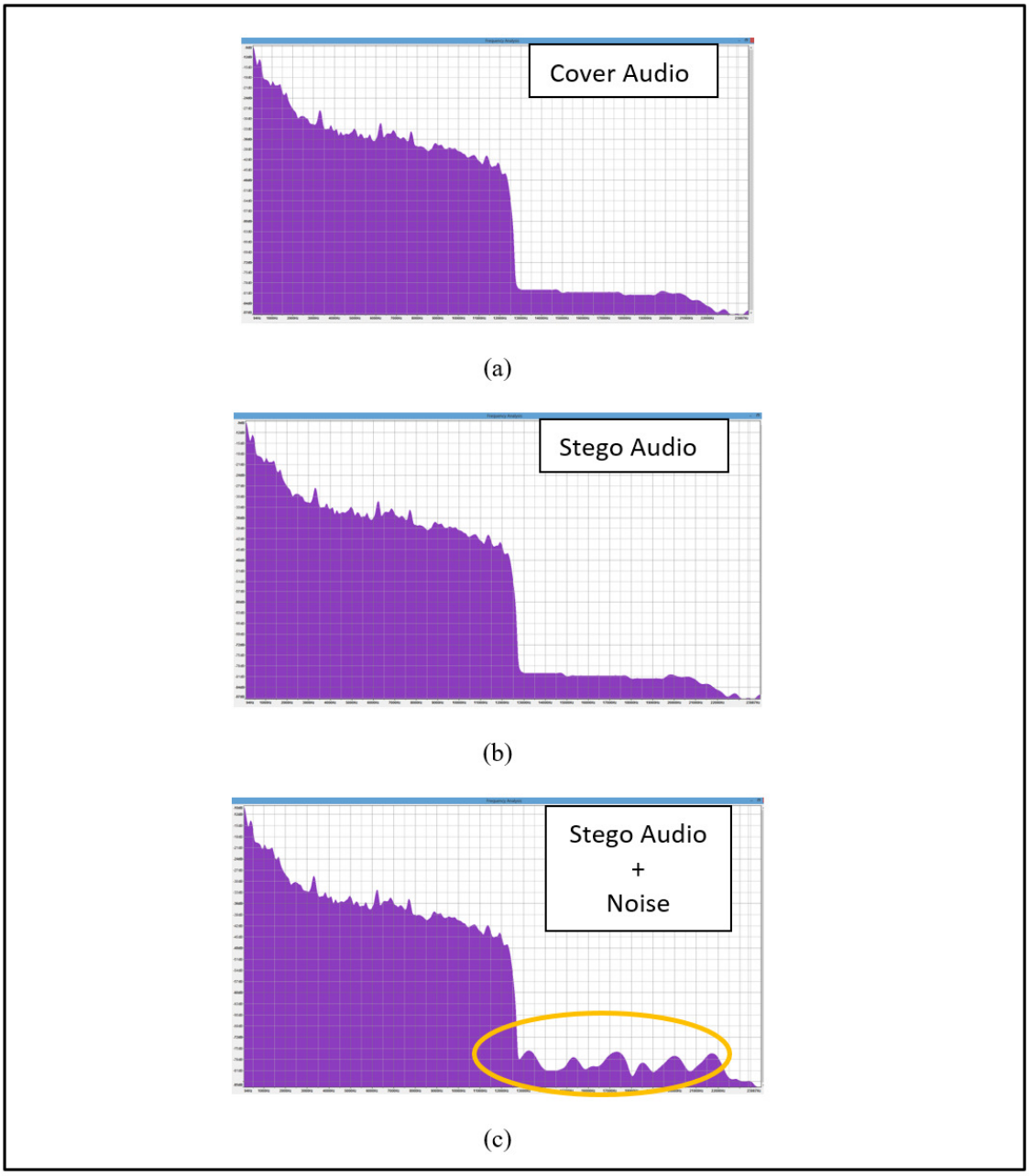

Figure 7: Comparison of Spectrum for Audio Steganography Elements on Cover Audio (a), Stego Audio (b) and Stego with Noise Addition (c) at Higher LSB

3.6 Discussion

There are two types of attacks to steganography and therefore there are two types of robustness. One type of attacks tries to reveal the hidden message and another type tries to destroy the hidden message. Substitution techniques are vulnerable against both types of attacks. Since substitution techniques usually modify the bits of the lower layers in the samples of LSBs, it is easy to reveal the hidden message if the low transparency arouses suspiciousness. Unintentional attacks like compression and distortions could destroy the hidden message if it is embedded in the bits of the lower layers in the samples -LSBs. The proposed scheme is

robust and able to withstand steganography unintentional attack which is compression till 17% at maximum payload of 953 bps at 11th LSB with good PSNR values when compared with similar approaches found in the literature [4, 15].

256 bit of AES encryption is applied on the generated stego audio to form another protection layer to increase the security of the stego audio. During the AES encryption, it allows for a password for an additional security for the stego audio.

Table 5: Imperceptibility Validation Through HAS Detection

Ser	LSB	Cover Audio (kB)	Secret Message Size (Byte)	Payload (bps)	PSNR	HAS Average Detection (%)	Comment
1.	1	1820	1000	889	162.2611	0	
2.	1	1820	2000	1778	159.1297	0	
3.	1	1820	3000	2667	157.3073	0	
4.	1	1820	4000	3556	156.1154	0	
5.	1	1820	5000	4445	155.1562	0	
6.	4	1820	1000	889	144.1643	0	
7.	4	1820	2000	1778	141.1032	0	
8.	4	1820	3000	2667	139.2638	0	
9.	4	1820	4000	3556	138.0461	0	
10.	4	1820	5000	4445	137.0629	0	
11.	8	1820	1000	889	120.1411	0	
12.	8	1820	2000	1778	116.9833	0	
13.	8	1820	3000	2667	115.1554	0	
14.	8	1820	4000	3556	113.9525	0	
15.	8	1820	5000	4445	112.9975	0	
16.	12	1820	1000	889	96.0017	5	Minor
17.	12	1820	2000	1778	92.9244	5	Minor
18.	12	1820	3000	2667	91.0555	5	Minor
19.	12	1820	4000	3556	89.8733	5	Minor
20.	12	1820	5000	4445	88.9070	5	Minor
21.	14	1820	1000	889	83.9366	20	Medium
22.	14	1820	2000	1778	80.8236	20	Medium
23.	14	1820	3000	2667	79.0705	100	Severe
24.	14	1820	4000	3556	77.8508	100	Severe
25.	14	1820	5000	4445	76.8850	100	Severe
26.	16	1820	1000	889	72.1107	100	Severe
27.	16	1820	2000	1778	68.7994	100	Severe
28.	16	1820	3000	2667	67.0215	100	Severe
29.	16	1820	4000	3556	65.8048	100	Severe
30.	16	1820	5000	4445	64.8340	100	Severe

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

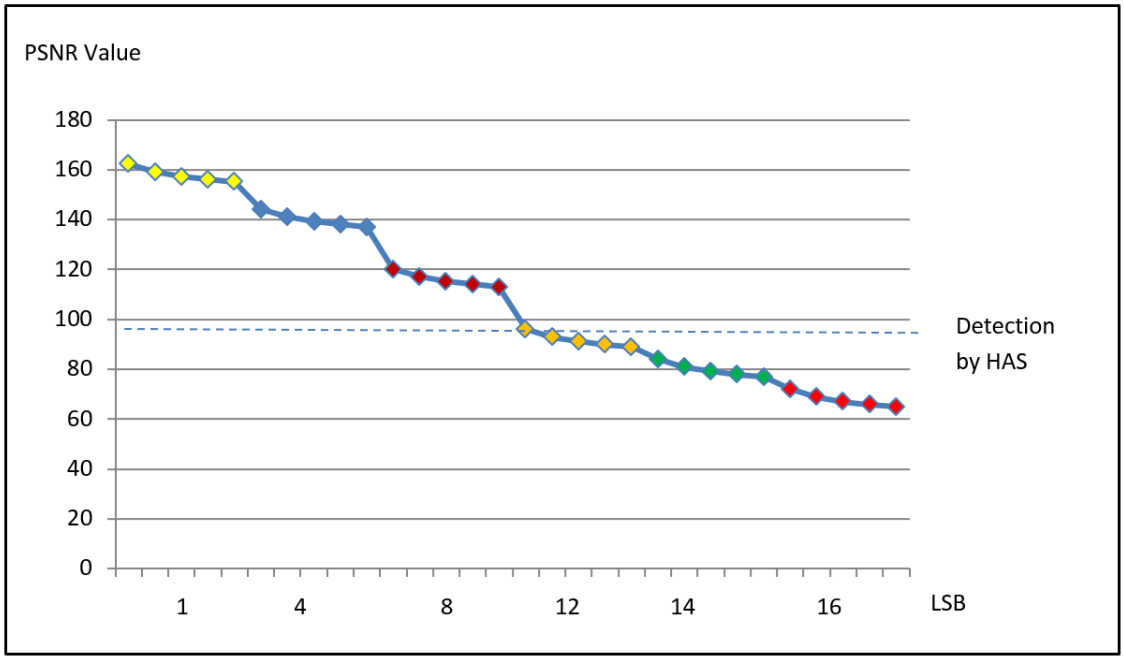

Figure 8: PSNR for different LSB

Security, performance and steganalysis resistance are conflicting trade-offs. Robustness or security versus Imperceptibility of the audio steganography has proven the identity or stego key and AES ensures higher data security which allows deniable of steganalysis. On the other hand, it requires a lot of extra carrier bits or larger cover audio. New security layer has been added at the bottom of the data process in encoding which is AES encryption. AES and Most Significant Bits ensure higher data security, but their random-like statistical response marks carriers as more suspicious.

4.0 CONCLUSION

Consequently, embedding information into audio looks more secure due to less existing steganalysis techniques for attacking to audio. Furthermore, natural sensitivity, complication and difficulty of working on audio steganography are the main reason there are less algorithms and techniques exists for image in steganography.

Though it is a well-built scheme, it has been limited to some restrictions. There is a need to explore Audio Steganography with appropriate NCC and BER values for a better interpretation and study of this scheme. There are a number of ways that this project can be extended. Its performance can be upgraded to higher levels by using a better algorithm for encoding and decoding.

Future work will be focused on developing more efficient, higher LSB scheme with better PSNR, MSE, NCC and BER values to improve for Audio Steganography. Besides that, a study should be conducted to define a benchmark for imperceptibility of PSNR value for Audio Steganography.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

ACKNOWLEDGMENT

The author would like to thank for the support given to this research by Malaysian Armed Forces and University Teknologi Malaysia (UTM) for guidance throughout this research. This work would not have been possible without their expertise in the area of steganography. They have provided me with valuable insights, and guided me accurately through this research.

REFERENCES

[1] P. Pathak, K. Arup, Chattopadhyay, A. Nag, A New Audio Steganography Scheme Based On Location Selection With Enhanced Security, IEEE (2014).

[2] A. Chadha, N. Satam, R. Sood, D. Bade, An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution, International Journal of Computer Applications 77 (2013) 37-45.

[3] D. Job, V. Paul, Image Steganography Technique Using Sudoku Puzzle And Ecc Algorithm For Secured Data Transmission, Journal of Theoretical and Applied Information Technology 66 (2014) 447-459.

[4] J. Antony, C.C. Sobin, A.P. Sherly, Audio Steganography in Wavelet Domain – A Survey, IEEE (2012) 310-312.

[5] P. Jayaram, H. R. Ranganatha, H.S. Anupama, Information Hiding Using Audio Steganography – A Survey, The International Journal of Multimedia & Its Applications (IJMA) 3 (2011) 86-96.

[6] A. Bhagyashri Patil, V.A. Chakkarwar, Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach, IOSR Journal of Computer Engineering (IOSR-JCE) 9 (2013) 30-34.

[7] D. Job, V. Paul, Image Steganography Technique Using Sudoku Puzzle And Ecc Algorithm For Secured Data Transmission, Journal of Theoretical and Applied Information Technology 66 (2014) 447-459.

[8] C. Chantrapornchai, K. Churin, J. Preechasuk, S. Adulkasem, Video Steganography for Hiding Image with Wavelet Coefficients, International Journal of Multimedia and Ubiquitous Engineering 9 (2014) 385-396.

[9] M. Kumar, M. Yadav, Image Steganography Using Frequency Domain. International Journal of Scientific & Technology Research 3 (2014) 226-230.

[10] W. Frączek, W. Mazurczyk, K. Szczypiorski, Multi-Level Steganography: Improving Hidden Communication in Networks, Journal of universal computer science 18 (2012) 1967-1986.

[11] N. Nameer El-Emama, R. Abdul Shaheed AL-Zubid, New Steganography Algorithm to Conceal a Large Amount of Secret Message Using Hybrid Adaptive Neural Networks with Modified Adaptive Genetic Algorithm, Journal of Systems and Software 86 (2013) 1465-1481.

[12] S.-N. Cheong, H.-C. Ling, P.-L. Teh, Secure Encrypted Steganography Graphical Password Scheme For Near Field Communication Smartphone Access Control System. Expert Systems with Applications 41 (2014) 3561-3568.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 39-54, 2016

[13] M. Kameswara Rao, K. Pradeep Reddy, K. Eepsita Sarany, Security Enhancement in Image Steganography a MATLAB Approach, Middle-East Journal of Scientific Research 23 (2015) 357-361.

[14] R. Kaur, A. Thakur, H. Singh Saini, R. Kumar, Enhanced Steganographic Method Preserving Base Quality of Information Using LSB, Parity and Spread Spectrum Technique, Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on, (2015) 148 – 152.

[15] M. Zamani, A. A. Manaf, R. B. Ahmad, Knots of Substitution Techniques of Audio Steganography. Proceedings Of 2009 International Conference on Computer Engineering and Applications. World Acad Union-World Acad Press, England 415-419.