Sindh Univ. Res. Jour. (Sci. Ser.) Vol.46 (1) 53-58 (2014)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Efficient Variable Least Significant Bits Audio Steganography (VLSBAS) Algorithms

ALAUDDIN[++], H. ZAFAR*, T. JAN*, N. AHMAD**, S. R. HASSNAIN***

Department of Electrical Engineering, University of Engineering and Technology, Peshawar (Kohat Campus)

Received 18th January 2014 and Revised 24th February 2014

Abstract: This research work proposes Efficient Variable Least Significant Bits algorithms for hiding data in an audio file having less distortion. In this work some of the earlier implemented algorithms are also modified to get better results and to reduce the tradeoff between capacity of the host (cover) audio signal and the distortion produced in the output signal (stego). First technique named Modified Multiple Least Significant Bits is proposed that increases the performance of already implemented Multiple Least Significant Bits algorithm. In the second method process of Xoring is used to get better results. In third proposed method both of these methods are combined to get even better results. At the end an Enhanced Variable Least Significant Algorithm is implemented which also increases the quality at the cost of some decrease in the capacity. Signal to Noise Ratio (SNR), Peak SNR (PSNR), Mean Squared Error (MSE) and Root MSE (RMSE) are used as key quality metrics to measure the results. Using these parameters it is shown that the proposed schemes can be used to get better results.

Keywords: Variable Least Significant Bits algorithm, SNR, MSE

1. INTRODUCTION

Information hiding is a very old science. During the time of ancient Greece (Kahn, 1996) many stories narrated has shown use of the science of 'Information hiding' for conveying a secret message. Information hiding can be achieved using Cryptography, Steganography and Watermarking. *Cryptography* is a technique in which a message is scrambled so that it cannot be understood (Dutta *et al.*, 2009). *Steganography* means *covered writing* (SANS, 2001). In this technique the primary concern is how to keep the *existence* of a message secret. Detection of the existence of any hidden data will be considered as a failure. Capacity, security and robustness are three parameters that can be used to measure the performance of any steganographic method. *Watermarking* is a technique used to embed an indelible mark on the host data for the establishment of identity or ownership (Dutta *et al.*, 2009).

The steganographic techniques can be classified on the basis of the hiding medium as well, e.g. *Text based steganography*, *Audio steganography* and *Image steganography* (Raphael and Sundaram, 2011).
The signal used to hide data is termed as 'Cover' signal, while after embedding the data the signal is known as 'Stego' signal.

Another way of classification is based on the domain in which steganography techniques are implemented. For example *Time/Spatial Domain* and *Transform Domain*. Discrete Cosine Transform (DCT) and Discrete Wavelet (DW) domain are examples of two techniques used in transform domain (Cvejic, 2004).

2. MATERIALS AND METHODS

2.1 Previous Work

In time domain many algorithms has been implemented earlier to hide data using Least Significant Bit(s). In one of the earliest methods discussed in (Gopalan, 2003), only one bit was embedded at different bit positions in the host audio signal. No great difference in the original (host) and stego signals were detected. XOR operation was performed during the insertion, so not all the bits located at Least Significant Bit position were changed. However inserting data at higher bit positions showed that if the message bit to be embedded is different from the original host bit then the noise produced will be noticeable.

Another algorithm (Cvejic and Seppänen, 2004) suggested that the embedding error can further be reduced if the bits of the host sample, other than the watermark bit, are flipped in such a way that minimizes the embedding error.

To improve the data rate, another method proposed that the values of the first 2 Most Significant Bits (MSBs) will be checked to decide the number of inserting message bits without any noticeable distortion. The capacity can be found by using the following formula (Kekre *et al.*, 2010).

$$CP=C4*7+C3*6+C2*5+C1*4$$

[++]Corresponding Author: alauddindcse@gmail.com, Ph. +92-315-9145806
*Department of Electrical Engineering, University of Engineering and Technology Peshawar, Pakistan
**Department of Computer Systems Engineering, University of Engineering and Technology Peshawar, Pakistan
***Department of Electronics Engineering, University of Engineering and Technology Peshawar (Abbotabad Campus), Pakistan

Some other algorithms were also proposed in (Zamani, *et al.*, 2009) (Singh and Aggrawal, 2010)

(Gopalan and Shi, 2010) (Marvel, 2002) (Sharma, 2011). However in all the algorithms proposed earlier a trade off can easily be observed i.e. by increasing the capacity of hiding data the distortion in the host signal (cover) will also increase. Thus if we want to get less distortion the data rate (capacity) must decrease.

2.2 Proposed Variable Least Significant Bits Algorithms

The main objective of this research is to propose some efficient techniques for data hiding, using Multiple Least Significant Bits technique. These schemes should have higher capacity as well as better quality, when compared with earlier algorithms implemented. Matlab a high-level technical computing language and product of mathworks will be used as a simulation tool. The measuring parameters will be Signal to Noise Ratio (SNR), Peak SNR (SNR), Mean Squared Error (MSE) and Root MSE (RMSE).

a. Modified Multiple Least Significant Algorithm

In this proposed algorithm the work of Kekre *et al.* (Kekre *et al.*, 2010) has been modified. Kekre *et al.* used two Most Significant Bits (MSBs) to select the number of embedding bits. In our proposed algorithm, an attempt has been made to make it more efficient by reducing the difference between the values of stego audio and original host audio signals. For this purpose, the following algorithm has been applied. On the sender side first the values of the MSBs are checked, and the message bits are inserted accordingly. If MSBs are 1 1, so 7 bits are embedded. Similarly 6 secret message bits are embedded for 1 0, 5 bits for 0 1 and 4 bits for 0 0. (Let *'n'* represent the number of message bit inserted).

After embedding the message bits, the bit value of the stego sample at bit location *n* is found. Similarly the bit values of the host (cover) audio at position *n* and *n*+1 are also found. On the basis of these bit values (1 or 0), the value of the bit located at *n*+1 is complemented. As a result of this change, the difference between the host (cover) audio signal and the stego audio signal must be reduced. If this does not happen or the difference increases so no change will be made at bit position *n+1*. Applying this technique showed a great improvements in the results in terms of SNR, PSNR, MSE, RMSE without affecting the capacity. At the receiving side by checking the values of the MSBs the embedded message bits can be retrieved easily.

b. Applying Simple Xoring Method

In this approach message bits are not embedded directly, in fact each message bit is first Xored with its corresponding bit in host audio sample and the result is than inserted at its location in the host (cover) sample. To further improve the results , the modifications proposed in Modified MLSBs algorithm, are also implemented here i.e. after Xoring the values of the *n* and *n*+1 are shuffled as per above described technique if required. It can be seen that while using simple Xoring the results can be made more desirable. However at the receiver side we will require a copy of the host (cover) sample. With the help of this host (cover) sample and the received stego signal the embedded message can be retrieved easily.

c. Combining Modified-MLSBs and Xoring techniques

In the previous two proposed techniques, it could have been observed that depending on the values of the host (cover) sample and the secret message in some scenarios these methods gives very good results, while in few other, the results may be worse. For example consider a host sample = 1 1 1 1 1 1 0….1 1 0 $_2$ =24576$_{10}$ and message bits = 1 1 1 1 0 0 0 . Now if direct embedding method is used so the output stego sample will be 1 1 1 1 0 0 0….1 1 0 $_2$ =24639$_{10}$ On the other hand using Xoring method will give stego sample = 0 0 0 0 0 0 0..1 1 0 $_2$ =24591$_{10}$.

It shows that in this example using Xoring method will give good results as compared to Multiple LSBs (or its modified version).

In order to get better results both of these methods proposed earlier are combined in such a way that one bit is reserved as an indicator to the type of method used for each sample. Thus depending on the results for each sample, one of the two methods will be selected and implemented for each sample. Thus the quality will be increased to a remarkable level at the cost of decrease in capacity of 'one' bit per sample.

In this proposed scheme, first Modified Multiple Least Significant Algorithm is applied and the difference between the stego sample and the host (cover) audio sample is calculated then Xoring method is applied and the difference is calculated. Based on the results of the difference, one (out of two) method is selected and for indication a '1' (for Mod-MLSBs) and '0' (for Xoring method) is inserted at bit 1 position (no message is embedded at this location).

In the above mentioned example using simple Xoring would give better result so we will use Xoring method and will insert a 0 at bit 1 position of stego sample. At the receiver, first the value of the bit 1 of the stego sample is examined and then the retrieving method is used accordingly. However on the receiver side the copy of host (cover) sample will be necessary.

d. Enhanced Variable Least Significant Bits Algorithm

In this proposed algorithm, an attempt has been made to decrease the distortion in the stego signal and recover it on the receiver side without any limitations. Following steps are followed to implement this algorithm.

- The values of the MSBs are found and the message bits are embedded accordingly. Let the number of message bits embedded are '*n'*.
- No message bit is embedded at bit position '1' in stego signal. The bits to be embedded in the stego sample are decided on the basis of the **Table 1**.

Table 1 Value of the Embedding bit

Selected LSB value	Corresponding bit value	Value of the LSB in stego sample (If msg bit =0)	Value of the LSB in stego sample (If msg bit =1)
0	0	0	1
0	1	1	0
1	0	0	1
1	1	1	0

- The corresponding bit value is predefined for each least significant (explained in the coming section).
- After embedding the bits, again the modifications proposed for the MLSBs algorithm is applied in this algorithm, to get better results.

In order to understand how this table is used and how the concerned corresponding bits are selected, an explanation is given below. Suppose the total number of message bits to be embedded is 6(*n*). Now the bit values at 1st bit and 6th bit (*n*) is examined and on the basis of the message bit, either 0 or 1 (looking from the Table 1) is embedded at 6th (*n*th) bit of the stego sample. Similarly the value at 2nd bit and 9th (2+(*n*+1)) bit, 3rd bit and 10th (3+(*n*+1)) bit, 4th bit and 11th (4+(*n*+1)) bit, 5th bit and 12th (5+(*n*+1)) bit, 7th bit and 14th (7+(*n*+1)) bit are found and on the basis of the message bits to be inserted, 2nd, 3rd, 4th, 5th ,6th and 7th bits of stego sample are changed using **Table 2.** It can be seen that no message is inserted at 8th bit (*n*+2).

To further understand the proposed scheme, consider an example.

Host (Cover) sample
= 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 0_2 =24639_{10}
Message bits = 1 1 1 1 0 0
Now using Table 1 and 2

Table 2 Value of the embedding bit and its corresponding bit values

Selected LSB value	Corresponding bit value	msg bit	Output value of selected LSB
1_{2nd}	0_{9th}	1	1_{1st}
1_{3rd}	0_{10th}	1	1_{2nd}
1_{4th}	0_{11th}	1	1_{3rd}
1_{5th}	0_{12th}	1	1_{4th}
1_{6th}	1_{1st}	0	1_{5th}
0_{7th}	1_{14th}	0	1_{6th}

Stego sample (out put)= 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 0_2 = 24703_{10}
The difference between this stego signal and the host (cover) sample is '64'. To reduce this difference two methods are used.

1. First use the modified MLSBs proposed method i.e. take complement of the value of 8th bit of stego sample and compare its value with the previous one, if any improvement is found so send it as it is . If, however no improvement is observed, no change is made in 8th bit.

2. The value at 6th bit (*n*) and it corresponding 8th bit are complemented. And after taking complement, decimal value of this sample is compared with the previous value of the stego sample, if the value of new stego sample is closer to the host (cover) audio sample , these complements are sent as it is. However even if by taking the complement of 6th bit and 1st bit do not bring any improvement than the previous value of the stego sample is retained.

In this example, implementing 1st method does not improve the results (or does not decrease the difference of the host and stego sample, in other words). However implementing 2nd method i.e. by taking the complement of the values of 1st and 6th bits, give better results.
Host sample = 0 1 1 1 1 0 1 0 0 0 0 0 0 0 1 1 0_2 = 24670_{10}
Now the difference of the host sample and stego sample has reduced to 31, which is inacceptable range.

In order to recover the message bits at the receiver side. Each LSB and its corresponding bit of the received stego sample is Xored. The result of this Xoring will help us to find out the actual sent message bit i.e. if result is zero, the actual message bit is 0 and if the result is 1 then the message bit is 1. It can be understood why 6th bit and its corresponding 1st bit are both complemented. By taking complement of one of them and leaving other will create problem on the receiver side, as the resultant Xored value and hence the

recovered embedded message bit will not be correct. Implementing this method has shown very good results. However the capacity of the cover (host) sample has decreased one bit per sample.

3. RESULTS AND DISCUSSION

Experiments were carried out using electric piano as cover audio signal and piano, guitar and other musical organs were used as a secret message. All the proposed algorithms were implemented. 100000 host samples were selected and 20000 bits from the secret message were embedded. Each host sample was represented in 16 bits. Simulation was carried out using Matlab. The results of all the performed experiments along with the results are shown in **Table 3** and the results of one of them (i.e. using Electric piano as host (cover) signal and another piano as secret data) is shown with the help of graphs **(Fig. 1 to 6)**.

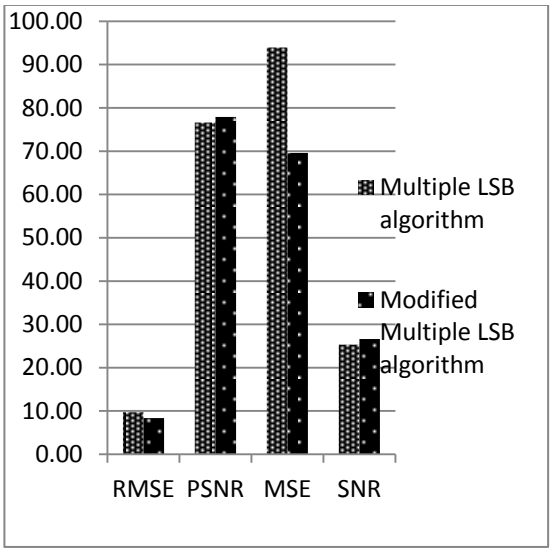

Fig. 1 Comparison of the Multiple LSB algorithm and Modified Multiple LSB algorithm

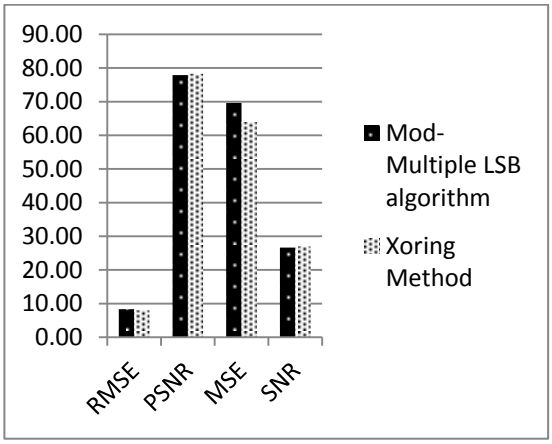

Fig. 2 Comparison of the Modified Multiple LSB algorithm and Xoring method

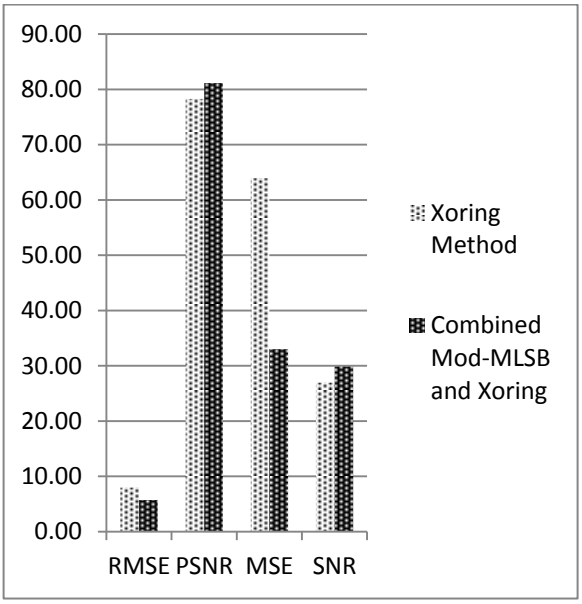

Fig. 3 Comparisons of the Xoring method Mod-Multiple LSB, and Xoring method

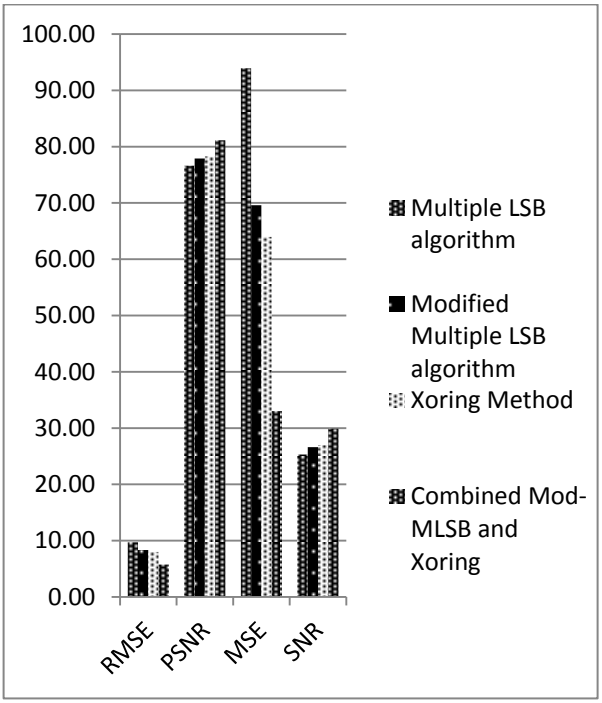

Fig.4 Comparison of the Multiple LSB , and Combined Mod-MLSB algorithm

Table 3 presents all the results calculated for the different secret messages used. It clearly shows that for all the cases the values of the RMSE and MSE has decreased and the values of the SNR and PSNR has increased.

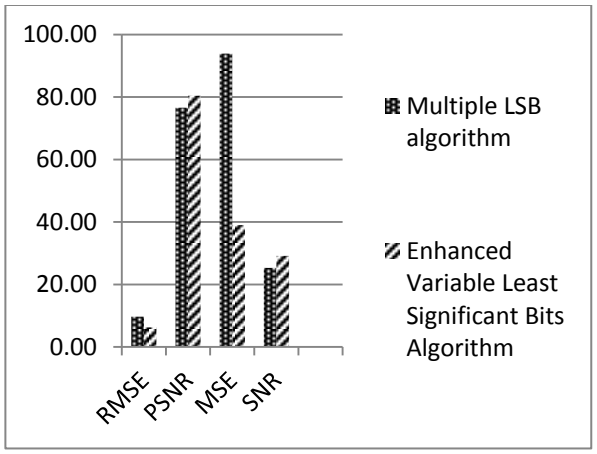

Fig. 5 Comparison of the Multiple LSB Algorithm Combined Mod-MLS and Enhanced VLSB Algorithm

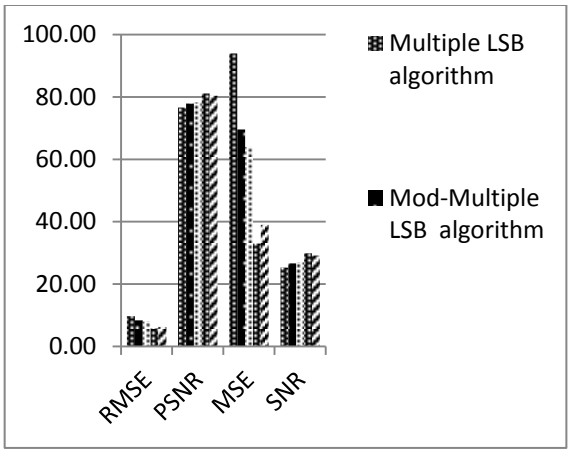

Fig. 6 Multiple LSB, Mod-MLSB, Xoring, and Enhanced Variable LSBs

Table 3 Comparison of SNR, PSNR, MSE and RMSE using different audio files as secret messages for same cover file (Electric Piano)

Cover	Secret	Implemented Algorithm	RMSE	PSNR	MSE	SNR
Electric Piano	piano	MLSBs	9.69	76.60	93.93	25.31
		Mod_MLSBs	8.34	77.90	69.59	26.61
		Xoring	7.99	78.27	63.96	26.98
		Combined MMLSBs & Xoring	5.74	81.14	33.01	29.87
		EnhancedVLSBs	6.24	80.41	38.99	29.14
	Guitar	MLSBs	9.96	76.36	99.21	25.07
		Mod_MLSBs	8.51	77.72	72.44	26.44
		Xoring	7.75	78.54	60.10	27.25
		Combined MMLSBs & Xoring	5.64	81.29	31.87	30.02
		Enhanced VLSBs	6.20	80.47	38.52	29.20
	Musical organ	MLSBs	9.90	76.41	98.03	25.13
		Mod-MLSBs	8.47	77.76	71.77	26.48
		Xoring	7.80	78.48	60.89	27.19
		Combined MMLSBs & Xoring	5.70	81.20	32.54	29.93
		Enhanced VLSBs	6.27	80.30	39.32	29.11

4. CONCLUSIONS

In this research an attempt has been made to decrease the distortion produced in the stego signal by proposing different schemes in Multiple Least Significant Bits algorithm, without decreasing the capacity of the cover signal. It can very easily be observed from the results that although the tradeoff between the capacity of the host (cover) sample and the quality of the stego signal still exist but this tradeoff has been reduced to a desirable level. The decrease in the capacity observed is one bit per sample, which, by looking to the improvement in the results, is acceptable. It can also be observed from the results, that if the receiver can keep a copy of the host cover signal then the combined method of Mod-MLSBs and Xoring can produce remarkable results. However the Improved MLSBs proposed scheme may be preferred, as it has no limitations.

The algorithms proposed in the Enhanced Variable LSBs can also be used to embed the data in higher layers to get more secure transformation. Even by using this proposed scheme the capacity will not be

reduced much. However the tradeoff among noise produced , capacity and bit indices must be taken into considerations.

REFERENCES:

Cvejic N. (2004) "Algorithms for Audio watermarking and steganography", http://herkules.oulu.fi. [Last accessed on 15 Jan 2014]

Cvejic N. and T. Seppänen (2004) "Reduced distortion bit-modification for LSB audio steganography", Proc. IEEE ICSP' 04: 2318-2321, Beijing, China.

Dutta P., D. Bhattacharyya and T. Kim (2009) "Data Hiding in Audio signal: A Review", International Journal of Database theory and Application, 2 **(2):** 1-8.

Gopalan K. (2003) "Audio steganography using bit modification", Proc. IEEE ICASSP: 421-424, Hong Kong.

Gopalan K. and Q. Shi (2010) "Audio Steganography using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", Proc. ICCCN, Zurich, Switzerland.

Kahn D. (1996) "The Codebreakers,The Story of Secret Writing" Rev. edition, Scribner, New York.

Kekre H. B., A. Athawale, B.S. Rao and U. Athawale (2010) "Increasing the Capacity of the Cover Audio Signal by Using Multiple LSBs for Information Hiding", Proc. Third International Conference on Emerging Trends in Engineering and Technology, 1: 196-2 Nagpur, India.

Marvel L. M. (2002) "Information Hiding: Steganography and Watermarking" Proc. IEEE 3rd Annual Information Assurance Workshop, West Point, NY, USA.

Raphael A. J. and V. Sundaram (2011) "Cryptography and Steganography – A survey" Int. J. Comp. Tech. Appl., 2 **(3):** 626-630.

SANS Institute InfoSec Reading Room (2001) "Steganography: Past, Present, Future" www.sans.org/reading-room/.../steganography-past-present-future-552. [Last accessed on 15 Jan 2014]

Sharma M. (2011) "A Review on Cryptography Mechanisms", Int. J. Comp. Tech. Appl., 2 **(4):** 1048-1050.

Singh P. K. and R. K. Aggrawal (2010) "Enhancement of LSB based Steganography for Hiding Image in Audio", International Journal on Computer Science and Engineering, 2 **(5):** 1652-1658.

Zamani M., A. Manaf, B. Ahmad, M. Zeki and S. Abdullah (2009) "A Genetic-Algorithm-Based Approach for Audio Steganography", World Academy of Science, Engineering and Technology, 3: 355-358.