Audio Wave Steganography

Ajay.B.Gadicha1

Abstract*— Present paper explores a new 4th bit rate LSB audio Stegnography method that reduces embedding distortion of the host audio. Using the proposed algorithm, Message bits are embedded into 4th LSB layers, resulting in increased robustness against noise addition. In addition, listening tests showed that perceptual quality of audio is higher in the case of the proposed method than in the standard LSB method.

Index Terms*— Audio stegnography, carrier file, keyfile, payload, transmission medium.

I. INTRODUCTION

In present scenario, Information security is the major part of computer world and it's a rapidly growing area in IT sector. The concepts of secure transmission of data over insecure channel are inspired by many ancient kings. In the past, these people were using the various techniques for the secure message transmission. Demaratus first used the technique of steganography for the secure data transmission. Steganography is the way to hide data in such a way that an existence of message is not known. Steganography technique was mostly used during word war II. Concept begins with the higher bit replacement of audio wave file called carrier file. Sample of audio wave file are taken & 4th layer bit is replaced with the message bit, but the care is taken for not having too much quantization error.

Standard method: Data hiding in the least significant bits (LSBs) of audio samples in the time domain is one of the simplest algorithms with very high data rate of additional information. The LSB watermark encoder usually selects a subset of all available host audio samples chosen by a secret key.[1] The substitution operation on the LSBs is performed on this subset, where the bits to be hidden substitute the original bit values. Extraction process simply retrieves the watermark by reading the value of these bits from the audio stego object.

As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. [7-9]Therefore, there is a limit for the depth of the used LSB layer in each sample of host audio that can be used for data hiding.

Subjective listening test shown that, in average, the maximum LSB depth that can be used for LSB based watermarking without causing noticeable perceptual distortion is the fourth LSB layer when 16 bits per sample audio sequences are used. The tests were performed with a large collection of audio samples and individuals with different background and musical experience.

Proposed algorithm: developed a novel method that is able to shift the limit for transparent data hiding in audio from the first LSB layer to the fourth LSB layer, using a two-step approach. In the first step, a watermark bit is embedded into the 4th LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by watermark embedding is shaped in order to change its white noise properties. The standard LSB coding method simply replaces the original host audio bit in the 4th layer with the bit from the watermark bit stream. In the case when the original and watermark bit are different and ith LSB layer is used for embedding the error caused by watermarking is 2:1 quantization steps (QS) .The embedding error is positive if the original bit was 0 and watermark bit is 1 and vice versa.

The key idea of the proposed LSB algorithm is watermark bit embedding that causes minimal embedding distortion of the host audio. It is clear that, if only one of 16 bits in a sample is fixed and equal to the watermark bit, the other bits can be flipped in order to minimize the embedding error. For example, if the original sample value was (0...01000)2=(8)10, and the watermark bit is zero is to be embedded into 4th LSB layer, instead of value (0...00000)2=(0)10, that would the standard algorithm produce, the proposed algorithm produces sample that has value (0...00111)2=(7)10, which is far more closer to the original one. However, the extraction algorithm remains the same; it simply retrieves the watermark bit by reading the bit value from the predefined LSB layer in the watermarked audio sample.

1. Select a carrier wave file. Payload is directly proportional to size of carrier file.
2. Select a key file. Key file may be any file like .exe, .txt, .pdf, .doc, .rar, .zip, .html etc. length of key file should be less than 16% of carrier file.
3. Hide the data in a carrier file.
4. Select a random sample of carrier file using key file data.
5. Select a file for hiding. The file may be of any type like .bmp,.txt etc.
6. Replace the 4th bit of audio carrier file with the message bit.
7. Flipped the other bits of carrier file so as to minimize quantization error.
8. Save the resultant wave file.
9. Read the message bit from resultant file. Too many questions are arises that are how to select sample from carrier file & how to replace 4th layer LSB audio bit with the message bit? One may think that replacing 4th layer bit will cause the different quantization error & the error will depend on the sample value.

Manuscript Received October 10, 2011.

Ajay.B.Gadicha1, Department of Computer Science & Engg, P.R.Patil College of Engg & Tech, Amravati (MH),India.
(Email- ajjugadicha@gmail.com).

This is true & that why the other bits of the samples are flipped so as to minimize the quantization error. The below portion of chapter explain how to minimize quantization error.).

TABLE 1

SAMPLE CARRIER FILE	AFTER INSERTING BIT '0'	QUANTIZASION ERROR
0000 1000	0000 0000	8
0000 0100	0000 0000	4
0000 0010	0000 0000	2
0000 0001	0000 0000	1

TABLE 2

SAMPLE CARRIER FILE	AFTER INSERTING BIT '0' & FLIPPLE 4TH LSB	QUANTIZASION ERROR
0000 1000	0000 0111	1
0000 0100	0000 0011	1
0000 0010	0000 0001	1
0000 0001	0000 0000	1

In table1, after inserting message bit in 4th LSB of carrier, the quantization error is high. It can be reduced by flipping other bits as shown in table2.

II. RESULT & DISCUSSION

The different experiments were conducted to prove the given method under different circumstances. The signal to noise ratio for the various audio sample can be calculated as

$$SNR=10 * \log10\{\sum n\ x^2(n)/\sum n\ [x^2(n)-y^2(n)]\}$$

Original audio signal:44100 samples/s, 16 bits/sample, 10 seconds duration Figure (a)

ResultantSignal: Bit-replacement (Layer 4) watermarked signal: Figure (b)

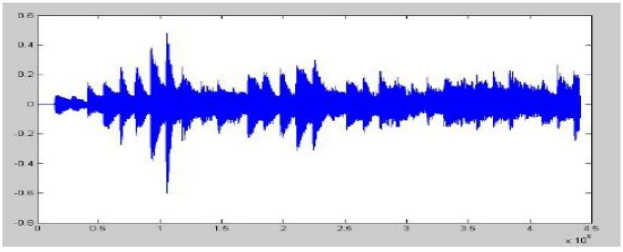

Figure (c) Waveform of original audio

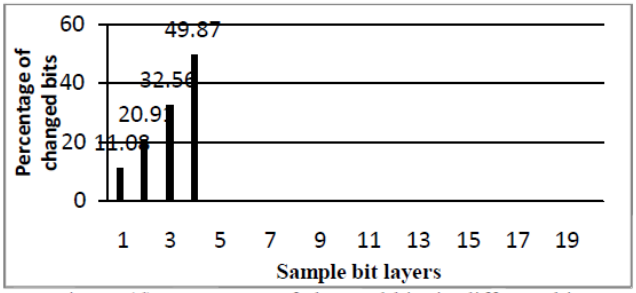

Figure (d) Percentage of changed bits in different bit layers

TABLE 3: Embedding rate of signal under different signal to noise ratio

		Embedded layer of watermarked nth			
		1st LSB	2nd LSB	3rd LSB	4th LSB
Resulting SNR	No noise	100	100	100	100
	20dB	53.02	75.02	81.21	84.39
	40dB	51.87	52.02	52.04	52.05
	60dB	53.02	75.02	81.21	84.39

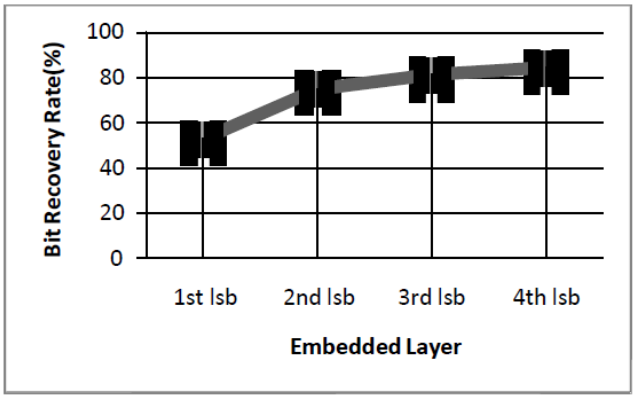

Figure (e): bit recovery rate for signal with SNR of 60dB

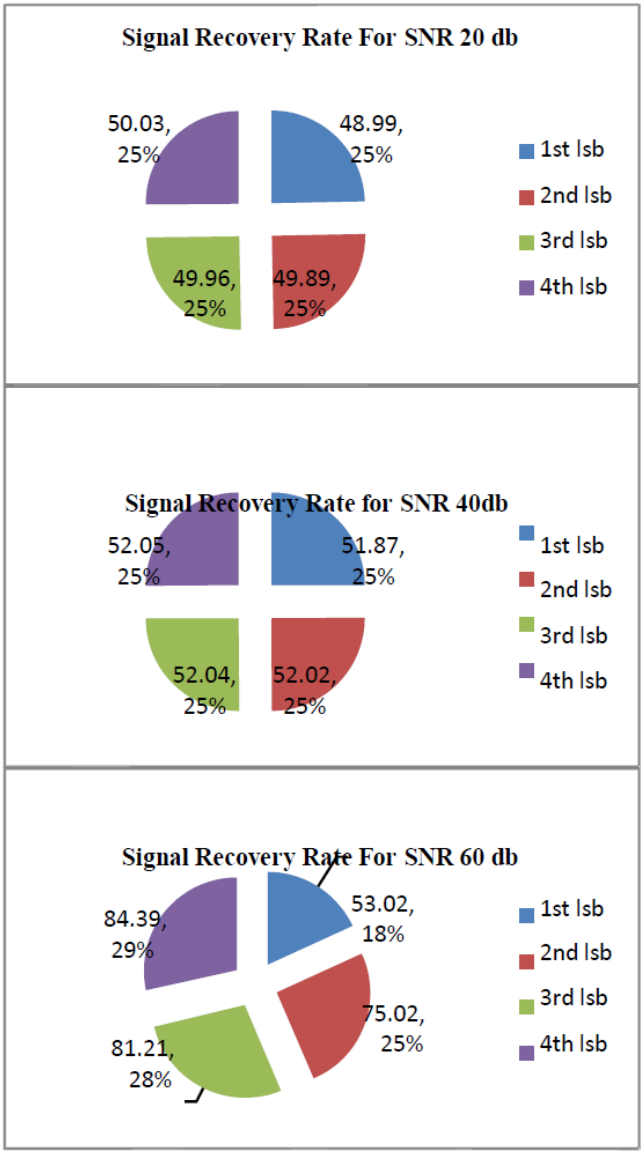

Figure (f): Signal Recovery Rate for various Signal to noise ratio

From table 3, When the level of noise is high such that the resulting SNR is low, embedding at higher layer does not improve the rate of recovery by a significant amount .In fact, when the SNR is 20dB, the rate of recovery is about 50% [Figure(f)],which is the level of random guess. At SNR of 40dB, the recovery rate is not significantly different across the 4 embedded layers and is close to 52% [Figure(f)].At SNR of 60 dB; however, the recovery rate using higher layers are significantly better.
For example, the rate of recovery for embedding using the 4th layer is 84.39% and that using the least significant bit is 53% [Figure (f)].Thus, it can be concluded that when noise is present, the least significant bit will be severely affected and that 'weak' noise will be less harmful to watermark bits embedded at higher layers.

Detecting the hidden data: now a question comes, is it is really possible to recover the data for intruder. Question is yes but not a simple task. The key file used to select the samples of original wave file contains the combination of various characters, symbols, digits & many more. Detecting single password may be possible for the intruder but to locate a file contain is quite impossible for the intruder.

III. CONCLUSION

It is clear that the proposed method introduces smaller error during watermark embedding. If the 4th LSB layer is used, the absolute error value ranges from 1 to 4 QS, while the standard method in the same conditions causes constant absolute error of 8 QS. The average power of introduced noise is therefore 9.31 dB smaller if the proposed LSB coding method is used. In addition to decreasing objective quality measure, expressed as signal to noise ratio (SNR) value, proposed method introduces, in the second step of embedding, noise shaping in order to increase perceptual transparency of the method.

REFERENCES

1. [Lee and Chen2000] Lee, Y., Chen, L.: High capacity image steganographic model,IEE Proceedings on Vision, Image and Signal Processing, 147, 3, 288-294.
2. [Mintzer et al. 1998] Mintzer, F., Goertzil, G., Thompson, G.: Display of images with calibrated colour on a system featuring monitors with limited colour palettes, Proc.SID International Symposium, 377-380.
3. [Mobasseri 1998] Mobasseri, B.: Direct sequence atermarking of digital video using m-frames, Proc. International Conference on Image Processing, Chicago, IL, 399-403.
4. [Yeh and Kuo 99]Yeh, C., Kuo, C.: Digital Watermarking through Quasi m-rrays,Proc. IEEE Workshop on Signal Processing Systems, Taipei, Taiwan, 456-461.
5. S. Lyu, H. Farid, Steganalysis using color wavelet statistics and one-class support vector machines, in: SPIE Symposium on Electronics Imaging, 84.39, 29%, 81.21, 28%, 53.02, 18% 75.02, 25% 1st lsb 2nd lsb 3rd lsb 4th lsb San Jose, CA, 2004
6. M.K. Johnson, S. Lyu, H. Farid, Steganalysis of recorded speech, in: SPIE Symposium on Electronics Imaging, San Jose, CA, 2005.
7. A.Westfeld, Detecting low embedding rates, in: F.A.P. Petitcolas (Ed.), Information Hiding. 5th nternationalWorkshop, IH 2002 Noordwijkerhout,The Netherlands, October 7–9, 2002, Springer-Verlag, Berlin, 2003, pp. 324–339
8. [Zwicker 1982] Zwicker, E.: Psychoacoustics, Verlag, Berlin, Germany. N.F. Johnson, S. Jajodia, Steganalysis of images created using current steganography software, in:
9. D. Aucsmith (Ed.), Information Hiding,LNCS, vol. 1525, Springer-Verlag, Berlin, 1998, pp. 32–47.