International Journal of Computer Applications (0975 8887)
Volume 80 - No. 15, October 2013

A Robust Audio Steganographic Scheme in Time Domain (RASSTD)

Dipankar Pal
Dept. of Computer Science and Engineering
Techno India
EM 4/1 Salt Lake, Sec-V, Kolkata-700091, India

Nabin Ghoshal
Dept. of Engineering and Technological Studies
University of Kalyani
Kalyani, Nadia-741235, West Bengal, India

ABSTRACT

Digital Steganograpic techniques hide secret messages in a cover media (mostly image, audio or video) in an imperceptible manner which cannot be detected by unintended recipient. In addition to imperceptibility, security, capacity and robustness are the other major challenges for an effective steganographic technique. This article proposes a novel steganographic method, considering maximum secrecy, high capacity and robustness against certain attacks. The method utilizes uncompressed digital audio signals as the carrier and hides different types of digital payloads (image/text/audio) in the time domain. In the process of embedding multiple payload bits (either 2 bits or 3 bits) are embedded in each of the sample values at pseudo-random positions. The pseudo-random positions are generated using a logical expression which is devised as a function of both the cover and the payload involved to make the algorithm inherently robust against potential collusion attacks. Various objective and subjective metrics have been used to measure the performance of the proposed technique. Also test results have been presented to analyse its robustness against white noise and collusion attack.

Keywords:

Steganography, HAS, MSE, SNR, PSNR, MOS, SHA-1, White Noise Attack, Collusion Attack

1. INTRODUCTION

In recent years, the use of various kinds of digital media, such as image, audio or video have been rapidly increased in many real life applications. This has urged the development of new and effective ways to ensure their security for different purposes, namely copyright protection or transmitting sensitive information through electronic communication channel. Though cryptographic techniques can conceal secret messages they are unable to conceal their very existence as well as the sender and the receiver. Steganographic techniques, such as the one described in this paper, hide secret information in digital media in an imperceptible manner, so that they can only be detected or extracted by the intended recipient. Steganography employs an innocent-looking cover media for imperceptible transmission of secret data. At the receiver's end, the secret data can be recovered from the stego signal using the reverse algorithm. For assured security, the main concerns with steganographic methods [1] are the hiding capacity of the cover media and the quality of the stego media. Almost all digital file formats can be used as the carrier for steganography, but image, audio and video files are more suitable because of their widespread use and availability of redundant bits in them.

Audio steganography is more challenging than image steganography because Human Auditory System (HAS) has wider dynamic range as compared to Human Visual System (HVS). Audio Steganography basically exploits the properties of Human Auditory System (HAS) which is considered as a very sensitive proposition. The critical band analysis in the inner ear where a frequency-to-location transformation takes place along the basilar membrane controls audio perception. Critical bands are defined as the power spectra of the received sounds on limited frequency bands [2]. But, common alterations in small differential ranges are also tolerated by HAS, i.e. loud sounds tend to mask out quiet sounds. There are some common environmental distortions, which may be ignored by listeners in most cases. Depending on these remarkable features, the researchers have started to utilize audio signals as carriers to hide data. Digital audio steganography [3] has emerged as a prominent source of data hiding across novel telecommunication technologies such as covered voice-over-IP, audio conferencing, etc. The particular importance of hiding data in audio files results from the prevailing presence of audio signals as information vectors in the human society.

Most audio steganographic methods, proposed in the past few years, hide messages either in the time domain [4] by directly altering the bits of the cover audio samples, in transform domain [5, 6] using various transformation techniques or in a combination of both [7]. Different domains have their special features which make them suitable for different applications. The discrete format of digital audio is created by sampling a continuous analog signal at a specified rate. In computer system, digital audio is stored as a sequence of 0's and 1's. Using appropriate algorithm, it is possible to change the individual bits of a digital audio file, but this change in the binary sequence is not discernible to the human ear.

In one of the earlier works by the authors[8] a technique had been proposed that hides different types of information (image, text or audio) in a cover audio signal with enhanced security and greater imperceptibility than other similar techniques. This paper presents a method that extends that idea with increased capacity and robustness against certain attacks. It increases hiding capacity by embedding multiple (2 or 3) bits per sample of the cover audio signal as compared to only 1 bit per sample in the earlier one. As we know that hiding capacity [9] and imperceptibility are two major

aspects of steganography, they are inversely related, i.e. when capacity goes high imperceptibility gets affected. But the proposed method in this paper is capable of keeping the imperceptibility of the stego audio signals high with respect to HAS. Also analysis has been done with the help of various objective metrics for the two scenarios, inserting 2 bits/sample and 3 bits/sample using the same algorithm. This paper is organized in the following order. Section 2 presents a discussion on the background and related work in LSB technique of Audio steganography. The methodology of the proposed technique is explained in section 3. The embedding and extraction algorithms of the technique are detailed in section 4. Experimental results based on subjective and objective measures are depicted in section 5 and application of white noise and collusion attacks are explained in section 6. Finally conclusion is drawn in section 7 followed by acknowledgement and references.

2. BACKGROUND AND RELATED WORK

Secret data embedding in digital audio file can be implemented by methods [10, 11] like LSB Coding, Phase Coding, Parity Coding and Spread Spectrum. In LSB coding technique least significant bit is used to fabricate the secret data. In phase encoding scheme the phase of the cover audio is replaced with reference phase derived from the payload. In parity coding mechanism the cover signal is divided into regions, the parity bit of each region is calculated and matched with the payload bit. Then depending on the parity matching result embedding is done. In spread spectrum method the secret information is spread over the cover audio's frequency spectrum as much as possible.
In this context, some of the notable research works are mentioned in the domain of Least Significant Bit encoding based audio steganography:

(1) LSB Modification and Phase Encoding Technique of Audio Steganography Revisited - Dr. Samir K Bandopadhyay et al. [12] focused on the negative aspects of both the techniques on individual application and proposed different environments of using these two techniques to their fullest capacity.

(2) Information Security using Audio Steganography - A Survey - B. Santhi et al.[13] emphasized on the improvement of efficiency and robustness of LSB technique by incorporating even parity coding with LSB technique.

(3) Higher LSB Layer Based Audio Steganography Technique - Dr. Samir K Bandopadhyay et al. [14] proposed a audio steganographic method that can adjust other bits in such a way such that the stego audio signal resulting from embedding data in higher LSB layer is perceptually indistinguishable from the host audio signal.

(4) Information Hiding in Audio Signals - Prof. H.B. Kekre et al. [15] implemented two tiers encoding technique to provide an additional level of security. In the first method, the information is hidden by altering LSBs indirectly considering parity of samples of cover audio and in the second method information is hidden by performing XOR operation on LSBs.

(5) An audio steganography by a low-bit coding method with wave files - Masahiro Wakiyama et al. [16] propose a new method of high-capacity embedding in digital audio by improving the low-bit coding. Emphasis is made on the position of embedding and obtains big capacity without the variation in original data context.

(6) Reduced distortion bit-modification for LSB audio steganography - Nedeljko Cvejic et al. [17] present a novel LSB audio data hiding method that reduces embedding distortion of the host audio. Hidden bits are embedded into the higher LSB layers, i.e. from 4^{th} to 6^{th} LSB layers while still maintaining the perceptual transparency of the watermarked audio signal. This improvement in robustness in presence of additive noise significantly lowers the bit error rates as compared to other standard algorithms.

(7) Hiding Text in audio using Multiple LSB Steganography - S.S. Divya et al. [18] proposes an approach of substitution technique of audio steganography that embeds message bits into multiple and variable LSBs to improve the capacity of data hiding of cover audio by 35% to 70%.

The facts described in the existing algorithms reveal that digital data can be effectively hidden in an audio with imperceptible degradation to the host audio but less protection against some attacks. Moreover, the payload, that needs to be hidden, is not confined only to audio, but can also be text or image.

3. PROPOSED METHODOLOGY

RASSTD technique improves document authenticity by performing multi-layer embedding of payload data in an audio signal. This blind steganographic method uses both the channels of a stereo audio signal for embedding. In addition to this, the capacity of payload is significantly increased by implementing the same algorithm in two ways, i.e. embedding 2 bits per sample and 3 bits per sample of each channel. Though size of the payload is highly escalating still different test results show high imperceptibility of the stego audio signals.
A 160-bit (SHA-1) message digest of the payload is also computed and embedded in the cover audio along with the payload data itself. This particularly becomes advantageous when it is necessary to detect the integrity and authenticity of the carrier audio signal at the time of extraction. This can be done at the receiving end, where the extraction algorithm recomputes the message digest of the extracted payload and compares it with the extracted message digest. They will never match, had there been a single bit of change in the carrier audio signal. Figure 1, shown below, demonstrates the overall insertion and extraction processes of this algorithm.

4. THE TECHNIQUE

Using the insertion algorithm, the bits of the payload data (image, text or audio) are embedded into the sample values of the host audio signal which produces a stego audio signal. The produced stego audio is then transmitted to the receiver and the payload is retrieved from the stego audio using the extraction algorithm. Insertion is performed in sample amplitude values of the carrier audio depending on the volume of the payload and bits are embedded at pseudo-random positions $(1^{st} - 4^{th})$, generated using a self-devised logical function. In the process of extraction, the payload is retrieved from the sample amplitude values of the stego audio. The process of retrieval works by extracting bits from the sample values sequentially and bytes are formed to reproduce the payload and the 160-bit message digest. The location of extraction of each bit is derived with the help of the same logical function, used in the insertion process. The algorithms for insertion and extraction are vividly explained in the following sub-sections.

4.1 Insertion Algorithm

Input: A PCM WAVE source audio and a payload file (image/text/audio).

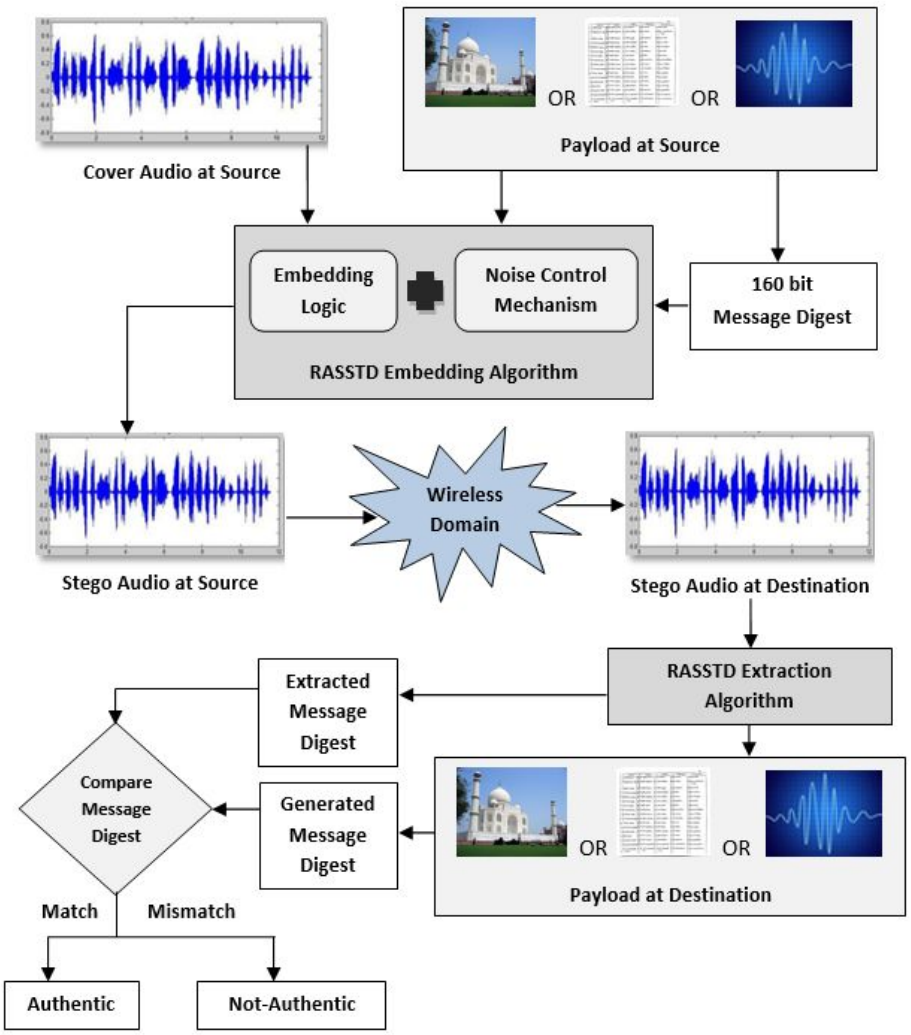


Fig. 1: Insertion and Extraction Process of RASSTD

Output: A stego PCM WAVE audio.
Steps:

1 Read the header information (RIFF, FMT and DATA) from the source audio and write into the output audio.
2 Generate a 160-bit message digest (SHA-1) of the payload.
3 Repeat the following steps until 32-bit payload size (in bytes), the message digest and all the bits of the payload itself are embedded,
  3.1 Read a sample amplitude value from the source audio.
  3.2 Generate 2 or 3 distinct pseudo-random values (ranging between 0 and 3) depending on the requirement for 2 bit or 3 bit embedding.
  3.3 Embed payload bits into the sample value at the positions obtained in the previous step.
  3.4 Reduce degree of noise by adjusting the modified sample value (see subsection 4.2).
  3.5 Write the sample value into the output audio.
4 Copy rest of the source audio (if any) into the output audio.
5 Stop.

4.2 Adjustments for Noise Control

The additional noise resulting from the embedding of payload data is reduced by modifying the unaffected bits of the stego audio sample. This procedure is applied only if the original sample and the resulting stego sample differ and is done by altering the bits on the right (i.e. towards LSB) and/or left (i.e. towards MSB) of the stego sample with respect to the value of highest LSB position obtained for embedding.

4.3 Extraction Algorithm

Input: A stego PCM WAVE audio.
Output: The extracted payload and the message digest.
Steps:

1 Read a sample amplitude value from the input audio.

2 Generate 2 or 3 distinct pseudo-random values (ranging between 0 and 3) depending on the requirement for 2 bit or 3 bit embedding.
3 Extract 2 or 3 bits from the sample value from the positions obtained in the previous step.
4 Repeat steps 2 to 3 to extract 8 consecutive bits to form a byte of the payload data.
5 Write the generated byte obtained in step 4 into the output file.
6 Repeat steps 1 to 5 until all the bytes of the payload are extracted.
7 Generate a 160-bit message digest (SHA-1) of the extracted payload.
8 Compare the two message digests to check the authenticity of the extracted payload.
9 Stop.

4.4 Generation of Pseudo-random Position

A function $f(x, y)$ [8] has been devised to generate 2-bit pseudo-random values to dynamically determine positions for embedding/extraction of message bits. Here, x is a Boolean variable and its value is deduced from the cover audio signal, whereas, y is a positive integer variable and its value may range between 0 and 7, which is derived from the payload data. Consideration of these two parameters from two sources, one from the cover and the other from the payload, has some specific purpose which has been discussed in subsection 6.2.

5. EXPERIMENTAL RESULTS AND ANALYSIS

Extensive study has been made on various types of audio used in the proposed technique. After executing the insertion algorithm the quality of each output stego audio is examined using various objective and subjective metrics [19].

5.1 Objective Measures

(1) Mean Square Error (MSE): Computes an error signal by subtracting the test signal from the reference, and then computing the average energy of the error signal. It is expressed as,

$$MSE = \frac{1}{N}\sum[|e| - |\bar{e}|]^2 \quad (1)$$

where, N denotes the total number of samples in the original audio, e corresponds to the original audio sample and $\bar{e}$ corresponds to the stego audio sample.

(2) Signal to Noise Ratio (SNR): It is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power and a ratio higher than 1:1 indicates more signal than noise. It is mathematically expressed as,

$$SNR = 10\,log_{10}\frac{E(x)}{MSE} \quad \text{dB} \quad (2)$$

where,

$$E(x) = \frac{1}{N}\sum[|e|]^2$$

represents the energy of the original audio and x corresponds to the original audio sample.

(3) Peak Signal to Noise Ratio (PSNR): Defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. It is expressed as,

$$PSNR = 10\,log_{10}\frac{(2^b - 1)^2}{MSE} \quad \text{dB} \quad (3)$$

where, b is the bit depth of the original audio signal.

5.2 Subjective Measure

Though objective measures are considered as the most common procedure for the measurement of noise difference between the original and stego audio signals, they do not prove authentic during consideration of some specific characteristics of HAS. So a different metric named Mean Opinion Score (MOS) is used as the subjective measure. MOS provides a numerical measure of the quality of audio signals. To determine MOS, a number of listeners rate the quality of both original and stego audio signals as shown in table 1. The final MOS is the arithmetic mean of all the individual scores, and can range from 1 (worst) to 5 (best).

Table 1. : MOS Grading Scale

MOS Grade	1	2	3	4	5
Remarks	Very Annoying	Annoying	Slightly Annoying	Perceptible, Not Annoying	Imperceptible

5.3 Results

This section describes the test results and performance analysis of RASSTD in terms of MOS, MSE, SNR and PSNR. Also a comparative study has been done with LASSD [8] in terms of Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR) analysis.
The proposed scheme has been tested with a variety of CD quality stereo audio signals, sampled at a rate of 44.1 KHz with 16 bit resolution. Three types of payload, image (figure 3a), text (figure 3b) and audio (figure 3c) were separately embedded in each of the cover audio signals. Some example stereo cover audio signals (both original and stego) involved in the experimentation are visualised in Figure 2.

1. Subjective Test - More than 30 listeners were involved to test different types of audio signals (Original and Stego). Fifteen pairs of audio, produced by both 2 bits/sample and 3 bits/sample embedding, were put to tests. Each pair consisted of one original and the corresponding stego audio. The listeners were requested to listen to the pairs very minutely. The results, as in table 2, are the final grades for the respective pairs and reveal high performance of the algorithm.

2. Objective Tests - Results produced by the quality metrics are shown below in table 3 and table 4 respectively. Table 3 shows a noticeable increase in amount of secret data embedded in different source audio along with appreciable SNR and PSNR values. In comparison with table 3, table 4 shows an increase in the size of payload by 32000 bytes with average decrease in SNR values by 2.5 dB and PSNR values by 2.0 dB respectively.

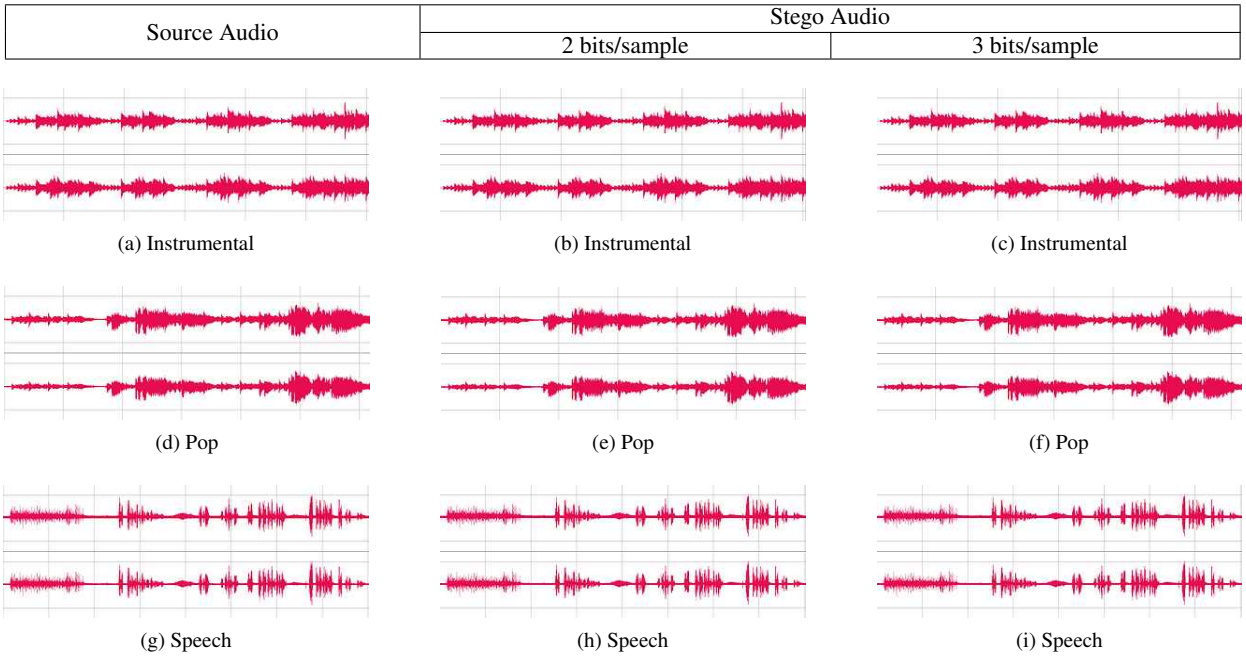


Fig. 2: Visual Representation of Source and Stego Audio Signals of RASSTD

Fig. 3: Visual Representation of Payload data used in RASSTD

Table 2. : Subjective Measure of Audio signals in RASSTD

Source Audio	Payload	MOS Grade	
		2 bits/sample	3 bits/sample
Instrumental	Audio	5	5
Pop		5	5
Rock		5	5
Speech		5	5
Instrumental	Image	5	5
Pop		5	5
Rock		5	5
Speech		5	5
Instrumental	Text	5	5
Pop		5	5
Rock		5	5
Speech		5	5

It is also observed that in comparison to the earlier technique, Lossless Audio Steganography in Spatial Domain (LASSD), the average SNR and PSNR values has impressively increased in case of 2 bits/sample and are competitive in case of 3 bits/sample, even when the embedded payload sizes are significantly greater than that of LASSD. The results obtained after comparison are presented in tables 5 and 6 respectively and graphical analysis of SNR and PSNR have been done in figure 4.

6. PERFORMANCE AGAINST SPECIFIC ATTACKS

6.1 White Noise Attack

The samples used for embedding procedure introduce low power Additive White Gaussian Noise (AWGN) [20] which is highly detectible by HAS. Subjective listening tests prove that, in average, the maximum LSB depth that can be used for LSB based steganography without causing noticeable perceptual distortion is the fourth LSB layer when 16 bits per audio samples are used. Robustness of the algorithm using the LSB coding method increases, with the increase of the LSB depth used for hiding data. Hence, improvement of robustness due to increase of depth of the used LSB layer is restrained by perceptual transparency bound, which is the fourth LSB layer for standard LSB coding algorithms.

Table 3. : Results obtained for 2 bits/sample embedding of RASSTD

Source Audio	Capacity (Bytes)	Payload	Embedded (Bytes)	MSE	SNR (dB)	PSNR (dB)
Instrumental	665891	Audio	638223	5.82121	62.7973	82.6588
Pop	681969			5.60039	63.3314	82.8268
Rock	661822			5.81660	68.1375	82.6623
Speech	640468			5.95143	62.9127	82.5627
Instrumental	665891	Image	638066	5.91133	62.7306	82.5922
Pop	681969			5.66952	63.2781	82.7735
Rock	661822			5.91529	68.0644	82.5892
Speech	640468			6.04068	62.8481	82.4981
Instrumental	665891	Text	625656	5.62806	62.9438	82.8054
Pop	681969			5.41261	63.4795	82.9749
Rock	661822			5.37144	68.4833	83.0080
Speech	640468			5.47360	63.2762	82.9262
Average			**633982**	**5.71568**	**64.4402**	**82.7398**

Table 4. : Results obtained for 3 bits/sample embedding of RASSTD

Source Audio	Capacity (Bytes)	Payload	Embedded (Bytes)	MSE	SNR (dB)	PSNR (dB)
Instrumental	998835	Audio	959216	10.3709	60.2892	80.1508
Pop	1022954			9.9990	60.8940	80.3093
Rock	992733			10.4715	65.5841	80.1089
Speech	960703			10.7099	60.3610	80.0111
Instrumental	998835	Image	956538	9.9942	60.4499	80.3114
Pop	1022954			9.6233	60.9804	80.4757
Rock	992733			9.9742	65.7954	80.3201
Speech	960703			10.2435	60.5544	80.2044
Instrumental	998835	Text	958416	10.0082	60.4438	80.3054
Pop	1022954			9.6512	60.9678	80.4631
Rock	992733			10.1149	65.7345	80.2593
Speech	960703			10.3556	60.5072	80.1572
Average			**958057**	**10.1263**	**61.8808**	**80.2563**

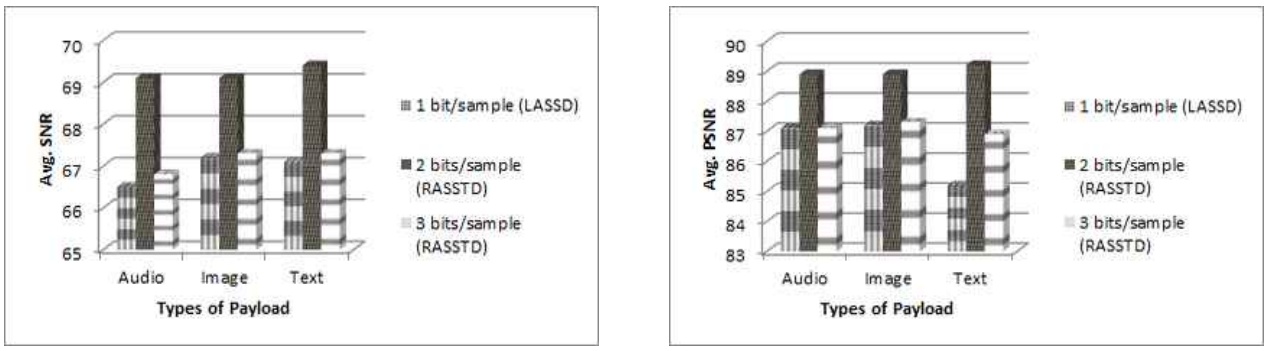
Table 5. : Comparison of SNR

Payload	LASSD		RASSTD			
	1 bit/sample		2 bits/sample		3 bits/sample	
	Embedded Bytes	SNR	Embedded Bytes	SNR	Embedded Bytes	SNR
Audio	367844	66.5	510265	69.1	750132	66.8
Image	344064	67.2	510133	69.1	749763	67.3
Text	499845	67.1	502292	69.4	750806	67.3

Table 6. : Comparison of PSNR

Payload	LASSD		RASSTD			
	1 bit/sample		2 bits/sample		3 bits/sample	
	Embedded Bytes	PSNR	Embedded Bytes	PSNR	Embedded Bytes	PSNR
Audio	367844	87.1	510265	88.9	750132	87.1
Image	344064	87.2	510133	88.9	749763	87.3
Text	499845	85.2	502292	89.2	750806	86.9

Generally the value of signal-to-noise ratio (SNR) above 20dB guarantees a reasonable good audio quality. Our algorithm has addressed this problem by making necessary adjustments for noise control during embedding and keeping the SNR value well above 20dB. This minimizes the effect of noise on the audio quality and the intended receiver receives clear audio. The experimented audio signals are analyzed carefully during listening. Figure 5 shows the amplitude comparison of some of the source and stego audio

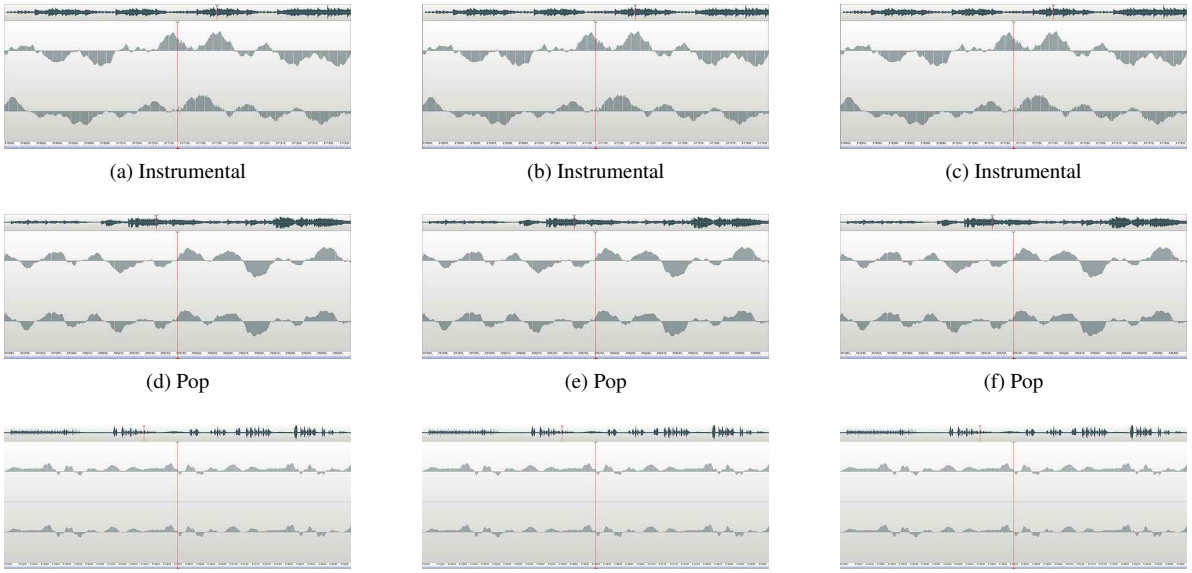


(a) Analysis of SNR

(b) Analysis of PSNR

Fig. 4: Graphical comparison of SNR and PSNR of RASSTD and LASSD

Magnified Source Audio	Magnified Stego Audio	
	2 bits/sample	3 bits/sample



(a) Instrumental (b) Instrumental (c) Instrumental

(d) Pop (e) Pop (f) Pop

(g) Speech (h) Speech (i) Speech

Fig. 5: Amplitude comparison of source and stego audio signals, shown in figure 2

signals and it can be observed that there is hardly any visible difference between the source and stego audio signals.

6.2 Collusion Attack

Collusion attack [20] is one of the most common steganalytic attacks which can be effective in two different scenarios. Firstly the attacker has more than one stego audio with the same payload in his/her possession. This enables the attacker to extract and identify the pattern of payload. The second method is effective when the adversary acquires several copies of a stego audio, each having a different payload. These copies can be combined to make the payload undetectable. To combat this attack, every copy of the cover audio must have different embedding policy, so the attacker cannot predict the embedding location and the payload by colluding many copies of the stego audio. The word "policy" actually means that there are multiple copies of a single audio such that no two audio have the same embedding pattern. The owner always has a set of different policies used to embed the payload and can always extract the payload from the stego audio by applying appropriate policies. For example, if the payload X is embedded in 4 different cover audio namely A, B, C and D then the attacker may not be able to detect the payload X by colluding the set of stego audio A', B', C' and D' respectively. As a counter-measure, certain information from both the cover audio and the payload data are involved to generate the pseudo-random positions for embedding and extraction of the payload bits. Considering the odd parity of the current sample of the cover audio, the last embedded bit of the payload data and the position of the current embedded bit, two or three distinct pseudo-

random values between 0 and 3 have been computed. This unique feature makes this algorithm inherently immune to any potential collusion attack.

7. CONCLUSION

The proposed algorithm RASSTD has put an effort to efficiently utilize audio signals to hide and transmit any type of message in the form of image, text or audio. Capacity for hiding data has been significantly increased by efficiently embedding multiple bits per sample while maintaining imperceptibility of the stego audio signal at a substantial rate. In support to this, experimental results are presented and assessed by both objective and subjective metrics. Security aspect has been enhanced by embedding the data bits of the payload in pseudo-random positions of the carrier samples and also emphasis has been given to make this algorithm robust against certain steganographic attacks. Comparative analysis has also been made with the earlier work of the authors in the same domain to highlight the improvements in RASSTD in several aspects.

8. ACKNOWLEDGEMENT

The authors express their deep sense of gratitude to the faculty members of the Dept. of Engineering and Technological Studies, University of Kalyani, West Bengal, India, where the work has been carried out.This project has been financially supported by DST - PURSE.

9. REFERENCES

[1] Bret Dunbar, SANS Institute, Info. Sec. Reading Room, "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment".

[2] Cvejic, Nedeljko, "Algorithms for audio watermarking and Steganography", Information Processing Laboratory, University of Oulu, Finland, (2004).

[3] Kekre, H.B., Archana, A.A., "Information hiding using LSB technique with increased capacity", International Journal of Cryptography and Security 1(2), October 2008.

[4] Nedeljko Cvejic, Tapio Seppben, "Increasing the capacity of LSB-based audio steganography", FIN-90014, University of Oulu, Finland ,(2002).

[5] M. Pooyan, A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Trans-form", 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), Egypt, December 2007.

[6] Yiqing Lin, Waleed H. Abdulla, "A Secure and Robust Audio Watermarking Scheme using Multiple Scrambling and Adaptive Synchronization", International Conference on Information, Communications & Signal Processing, DOI: 10.1109/ICICS.2007.4449673, (2007).

[7] Foo S.W., Ho S.M., Ng L.M., "Audio watermarking using time-frequency compression expansion", IEEE Inter-national Symposium on Circuits and Systems, 201-204, (2004).

[8] Dipankar Pal, Anirban Goswami, Nabin Ghoshal, "Lossless Audio Steganography in Spatial Domain", Int. Conf.on Frontiers of Intelligent Computing:Theory and Applications, AISC 199, pp. 575-582. DOI: 10.1007/978-3-642-35314-7_65, Springer, (2012).

[9] Sunita V. Dhavale, R. S. Deodhar, L. M. Patnaik, "High Capacity Lossless Semi-fragile Audio Watermarking in the Time Domain", Advances in Computer Science, Engineering & Applications, Volume 167, 2012, pp 843-852 , ICCSEA - 2012 (Springer).

[10] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, "Information hiding - A Survey", Proceedings of the IEEE 87, 1062-1078, (1999).

[11] Xuping Huang, Ryota Kawashima,Norihisa Segawa, Yoshihiko Abe, "The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream",Technical Report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[12] Samir Kumar Bandyopadhyay, Barnali Gupta Banik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, ISSN : 2278 - 1021, June 2012.

[13] B. Santhi, G. Radhika, S. Ruthra Reka, "Information Security using Audio Steganography - A Survey", Research Journal of Applied Sciences, Engineering and Technology 4(14): 2255-2258, 2012, ISSN: 2040-7467, Maxwell Scientific Organization, (2012).

[14] Samir Kumar Bandyopadhyay, Biswajita Datta, "Higher LSB Layer Based Audio Steganography Technique", International Journal of Electronics & Communication Technology, Vol. 2, Issue 4, ISSN: 2230-7109 (Online) — ISSN: 2230-9543 (Print), Oct. - Dec. 2011.

[15] Dr. H.B. Kekre, A. Archana, Swarnalata Rao,Uttara Athawale, "Information Hiding in Audio Signals", International Journal of Computer Applications (0975 8887), Volume 7 - No.9, October 2010.

[16] Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nozaki, "An audio steganography by a low-bit coding method with wave files", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 978-0-7695-4222-5/10, DOI 10.1109 / IIHMSP.2010.135, IEEE, (2010).

[17] Nedeljko Cvejic, Tapio Seppnen, "Reduced distortion bit-modification for LSB audio steganography", ICSP proceedings, IEEE, (2004).

[18] S.S.Divya, M.Ram Mohan Reddy, "Hiding Text in audio using Multiple LSB Steganography and provide security using Cryptography", International Journal of Scientific & Technology Research, Volume 1, ISSUE 6, ISSN 2277-8616, JULY 2012.

[19] Dermot Campbell, Edward Jones, Martin Glavin, "Audio quality assessment techniques - A review and recent developments", Journal of Signal Processing, Elsevier, 0165-1684 / - 2009 Elsevier B.V. doi:10.1016 /j.sigpro.2009.02.015.

[20] Nedeljko Cvejic, Tapio Seppnen, "Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks", InformatIon Science Reference, Hershey, New York, ISBN 978-1-59904-515-3 (ebook), 2008, pages - 79, 239.