A Survey on Audio Steganography Approaches

Kamred Udham Singh
Department of Computer Science,
Faculty of Science Banaras Hindu University,
Varanasi, (U.P.), India

ABSTRACT
Today's internet community the secure data transfer is bounded due to its attack on data communication. Security of data can be achieved by implementing steganography techniques. All of the existing steganographic techniques use the digital multimedia files as a cover mediums to conceal secret data. Audio file use as a cover medium in steganography because of its larger size compare to other carrier's file such as text, image. So there are more possibilities to hide large amount of data inside digital audio file. Signals and digital audio files make suitable mediums for steganography because of its high level of redundancy and high data transmission rate. This is not easy to hide data in real time communication audio signals. In this paper we will survey the overall principles of hiding secret data in audio file using audio data hiding techniques, and deliver an overview of present techniques and functions and also discuss the advantages and disadvantages of different types of audio steganographic methods.

General Terms
Robust, Security, Information, Signal, stego.

Keywords
Digital data security, stego signal, audio steganography, H.A.S, information hiding, embeds.

1. INTRODUCTION
Steganography technique is the art and science to hide information in any digital object like image, audio, video only recipient knows of the existence of the information [1]. Literally meaning of steganography is covered message and includes transmitting secret information through the seemingly innocuous files. Steganography is gaining popularity due to growing necessity for security of data [2]. The main objective of steganography is to transfer information from sender to receiver securely in a completely untraceable way and to evade depiction suspicion to the transmission of concealed information [3] [4]. The idea of message hiding in any object is not a novelty; this has been used form centuries all over world under different regimes. It is a technique for hiding information so that it does not even seem to exist.

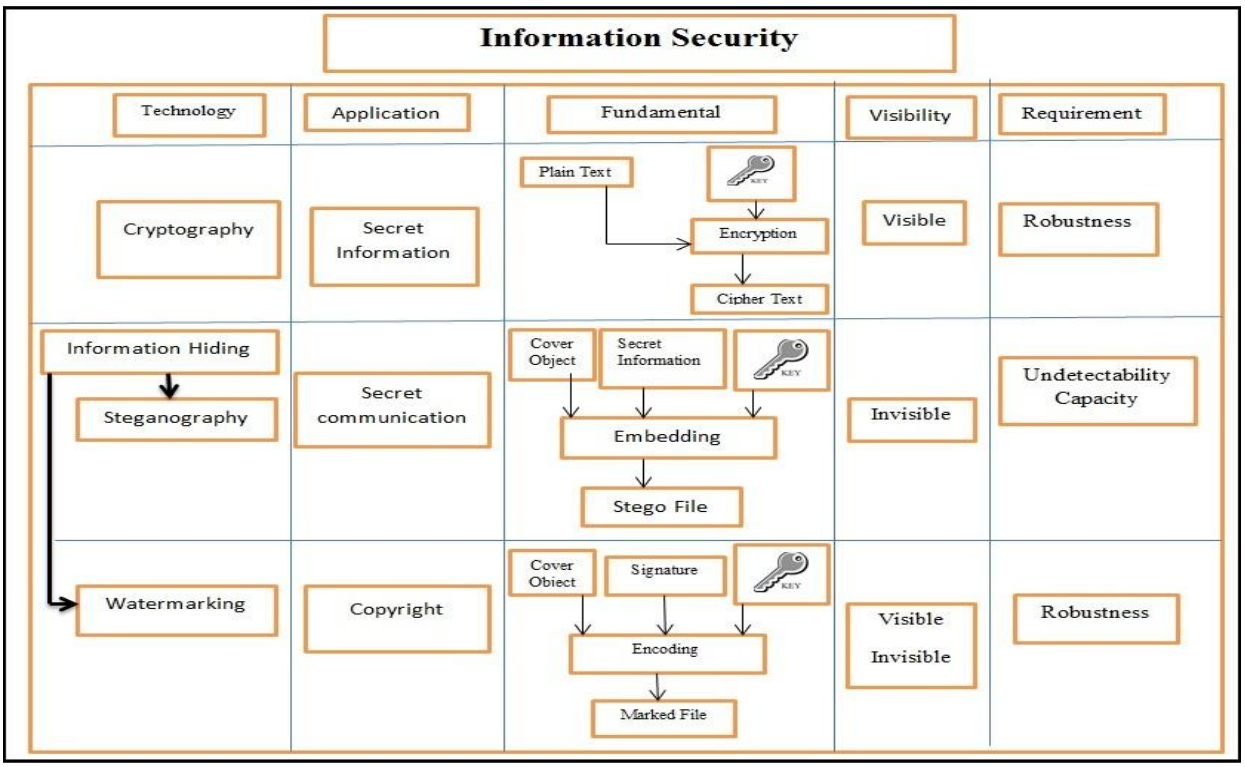

Fig 1: Information security disciplines.

Hiding information in any object has a long history. Greek historian Herodotus writes, Histaeus, who wanted to communicate with his son-in-law in Greece. First Histaeus shaved the head of one of his most faith slaves and tattooed the information on the slave's scalp. After some days slave's hair grew up again the slave was dispatched with the hidden

information [5]. Other historical tricks include tiny pin punctures on selected characters, invisible inks, pencil marks on type written characters and so on. Steganography is dissimilar from cryptography. The main goal of cryptography is that to secure the communications by modifying the data into a form but on the other side, steganography methods tend to conceal the existence of the message in any digital object, which makes it very difficult for a spectator to find out where exactly the message is[6], [7]. The message to be hidden in the cover object is known as embedded data. The "stego" object containing both the cover signal and the "embedded" message. The process of hiding data, into the cover digital media object, is known as embedding. The sender hides secret information of any type using a key in a digital cover object to produce a stego file, in such case observer cannot notice the existence of the hidden information. At the receiver end, the receiver extracts the received stego-file to get the hidden message.

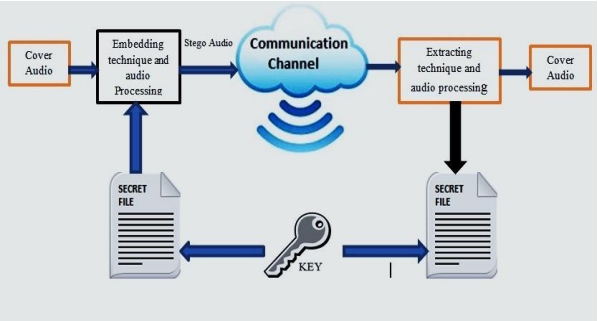

Figure 2 Audio steganography

Different types of Covers can be used like image, video, audio, text, and IP datagram. Video and Image based steganography trusts on the limited HVS (Human Visual System) in observing luminance difference at levels greater than 1 in 240 in constant gray levels or 1 in 30 of random patterns. Though, audio steganography feats the masking affects property of HAS (Human Auditory System) [8]. Numerous features impact on the quality of audio steganographic technique. The importance and the impact of all features depend on the transmission environment and the application. Most important properties of audio steganography are robustness to noise and to signal manipulation, concealing-capacity of embedded message and security. Robustness requirement is strongly linked to the application and is the most stimulating to satisfy in a steganographic system. In audio steganography system, secret data is embedded in digital audio object. The binary sequence of a cover audio object is majorly altered by adding secret data in it. The digital audio file formats used by in audio steganography technique are AU, WAV and MP3 sound files. The modified audio file should not be made identified to the human ear. In this review paper we will discuss several works in audio steganography and use of audio files as a cover medium to conceal secret message for secure communications.

1.1 Properties of the Human Auditory System

The process of hiding data in the audio signal is a challenge task because the Human Auditory System (HAS) efforts dynamically in a vast range of frequencies, which is between (20Hz - 20000Hz), so it is very sensitive to add random noise in audio signal, the disruption in a sound file can be noticed as low as on part in ten million but 80dB is below ambient level. Embedding other additional information into audio sequences is a more exhausting task than the images, due to the dynamic sovereignty of the Human Auditory System over the Human Visual System (HVS) [11][12]. The amount of data which can be embedded in the video frames is more than the amount of data which can be embedded transparently into audio sequences because of audio signal has fewer dimensions than video. On the other side, many malicious attacks are against image and video steganography algorithms (e.g., spatial scaling and geometrical distortions) cannot be implemented against audio steganography schemes. Moreover, the Human Auditory System is unable to observe absolute phase however relative phase. Some environmental distortions are so common as to be avoided by the listener in maximum case [11].

Two attributes of the HAS dominantly used in steganography algorithms are: temporal masking and frequency masking. Concept of perceptual holes of the HAS is occupied from wideband audio coding e.g., MPEG Compression 1, Layer 3, usually called MP3. Holes are used in order to decrease the quantity of the bits required to encode audio signal without producing a perceptual distortion to the coded in audio signal, in the compression algorithms. Laterally the data hiding scenarios, masking properties are used to embed supplementary bits into existing bit stream, again without producing perceptible noise in the audio signal used for data hiding [12].

2. RESEARCH OBJECTIVES

Generally, data hidden has two techniques named digital steganography and watermarking. According to the researchers, data hidden methods have two main limitations first is the size of the hidden data and second is robustness of the watermark techniques. We will try to achieve the following objectives in this review paper:

1. To analyze the structures of audio file this can be used to implement the high rate data hiding.

2. To carry out intensive literature reviews of the existing techniques and demonstrate the advantage and the disadvantage of every technique.

3. DIGITAL AUDIO SIGNAL

Digital audio signals are dissimilar from other traditional analogue sound signal in fact that are discrete signal rather than continuous. Discrete signals are formed by sampling continuous analogue signals at precise rates. For example the typical sampling rate for CD digital audio is 44 kHz. Figure 3 depicts a continuous analog audio signal wave being sampled to produce digital audio signal wave.

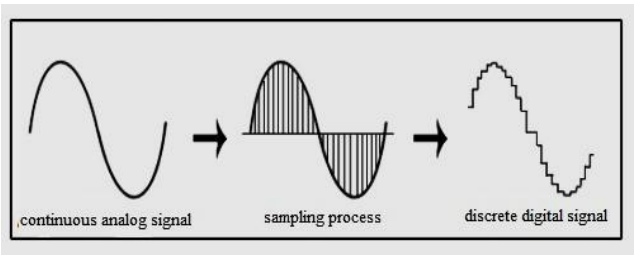

Figure 3 Sampling of audio signal

Figure 3 indicate the discrete nature of digital audio signals. Typical sampling rate is usually set at a level on that produced discrete signal is not imperceptibly different from the original continuous signal. Audio files are stored in computers in sequence of 0's and 1's. It is possible to modify the bits which structure a digital audio file. Such type of accurate controls permits alterations to be performed to the binary bits which are not perceptible to the Human Auditory System.

4. AUDIO ENVIRONMENTS

4.1 Digital representation

Sample quantization and temporal sampling rate are two parameters of digital audio representations. Most common digital audio format for representing samples of high quality digital audio file is a 16-bit linear quantization like Audio Interchange File Format (AIFF) and Windows Audio Visual (WAV) [9][10].Logarithmically scaled 8-bit m-law is another popular audio format for lower quality audio. These quantization methods present some signal distortion, rather more conspicuous in the case of 8-bit m-law. Common temporal sampling rates for audio include 8 kHz (kilohertz), 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz, and 44.1 kHz. Sampling rate impacts on data hiding, it puts an upper bound on the operational section of the frequency spectrum. For most data hiding methods developed, operational data location increases at least linearly with increased sampling rate [11].

4.2 Transmission Environments

There are various transmission environments in which a signal might experience on its way from sender to receiver. We consider four general classes for illustrative purposes [11]. First is the digital end -to -end environment in this environment of a sound file that is copied from machine to machine, but it never altered in any way. Sampling is exactly the same at the sender and receiver. This class places the least constraints on data hiding techniques [10] [11]. Next consideration is that when a signal is resample to a higher or lower sampling rate, but it remains digital throughout. This transformation preserves the absolute magnitude and phase of most of the audio signal, but alterations the temporal characteristics of the signal. Third case is when a signal is "played" into an analog state and transmitted on a reasonably fresh analog line and resample. Absolute signal magnitude, temporal sampling rate and sample quantization are not preserved. In common, phase will be preserved. Last case is that when the signal is played into the air and resample with a microphone. The signal will be exposed to possibly unknown nonlinear alterations resulting in phase changes, drift of different frequency components, echoes, amplitude changes etc. Transmission pathway and signal representation must be reflected when choosing a data hiding technique. Data rate is dependent on the sampling rate and the type of sound being encoded.

5. AUDIO STEGANOGRAPHIC METHODS

5.1 Hiding in temporal domain

The popular temporal domain techniques employ low-bit encoding techniques, and that we describe next. Other techniques which fall under temporal domain class are also presented in the following sections.

5.1.1 Low-bit encoding

Low-bit encoding also known as Least Significant Bit (LSB) technique, this technique is one of the earliest approaches used for information hiding [13][14]. Generally, it is based on embedding each bit from the data in the least significant bit of the cover audio object in a desired way (see Figure 4). So, for in a16 kHz sampled audio sequences, 16 kbps of data are hidden. Least Significant Bit technique allows high embedding capacity for data and it is relatively simple to implement or to combine with other data hiding techniques. But, this technique's security performance is reduced due to low robustness to noise addition in audio since it becomes susceptible even to simple attacks. Stego-audio will very likely destroy the data due to amplification, noise addition, filtration and lossy compression. Additionally, data are embedded in a deterministic way, but an attacker can simply uncover the data by just eliminating the entire LSB plane. A simple LSB plan has been applied to embed voice information in a wireless communication [15]. While this method achieves the security robustness of hidden data and imperceptibility at high embedding rate are easily compromised. In an attempt to augment the concealing capacity while reducing the error in the stego audio, adopted minimum error-replacement method whereas embedding four bits per sample [16]. Then embedding error is diffuse on the subsequent four samples.

We can increase the depth of the embedding layer from 4th to 6th and to 8th LSB layers without disturbing the perceptual transparency of the stego audio signal, to improve the robustness of LSB technique against distortion and noise addition, [17][19].Only bits at the sixth place of each 16 bits sample of the original signal are substituted with bits from the data [17] [18]. To reduce the embedding error, the other bits can be flipped in order to have a new sample that is nearer to the original one.

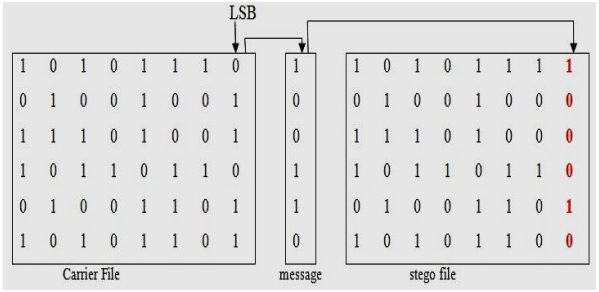

Figure: 4 LSB in 8 bits per sample signal is overwritten by one bit of the hidden data

5.1.2 Echo hiding

Echo hiding method embeds secret information in audio signals by introducing a short echo in to the discrete signal. Resonance is added to the host audio signal. The stego signal retains the same perceptual and statistical characteristics after the echo has been added. In comparison to other methods echo hiding provide a high data transmission rate and superior robustness. To hide date in echo signal, manipulate three parameters: the initial amplitude, the offset (delay) and the decay rate thus the echo is not perceptible [20] (Figure 5).A delay up to 1 MS between the echo and original signal, the effect is indistinguishable. Only one bit of secret data could be encoded if only one echo was generated from the original signal. Before the beginning of encoding process the original signal is broken down into chunks. After the completing of encoding process, the chunks are concatenated back together to produce the final signal [21]. Drawback of Echo hiding technique is the limitation of persuaded echo signal size that restricts its related application domains. No audio steganography system based on echo hiding has been

presented in recent researches because of low security and low embedding rate. Furthermore, some techniques have been proposed, alike for audio watermarking. Echo hiding-time spread technique has been proposed in [22] for improving the watermark system robustness against common signal processing. Compared to the conventional echo hiding system, this proposed technique detects the watermark bits throughout the entire signal and it recover them based on the correlation amount at the receiver not on the delay.

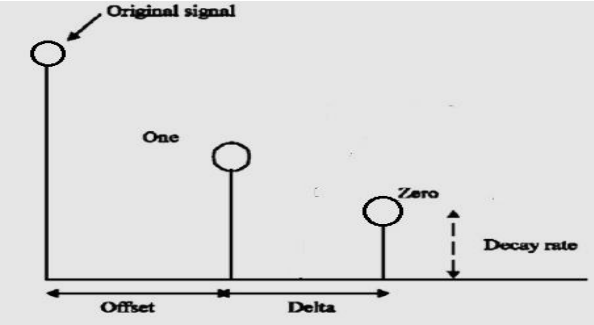

Figure 5 Echo data hiding adjustable parameters

5.1.3 Parity coding

The parity coding technique breakdowns a signal into separate regions of samples, Instead of breaking down a signal into individual samples because Parity coding method works on a group of samples instead of individual samples. In this technique individual samples are grouped and parity of each group is computed for inserting data bit one by one, check the parity bit of a group of samples. If the parity bit and data bit matches do nothing. Otherwise modify the LSB's of any one of the individual samples in that group to make the parity bit equal to the data bit. Thus, the sender has more option in encoding the secret data bit, and the signal can be altered in a more unobtrusive fashion [23].

5.1.4 Hiding in silence intervals

It is a simple and effective embedding technique has been used to exploit silence intervals in speech signal [24]. Initially determine the silence intervals of the audio and their respective length (the number of samples in a silence interval). These values are decreased by a value a where $0 < z < 2^{n\ bits}$and n bits is the number of bits needed to represent a value from the data to hide. For the data extraction process z is assessed as$mod\left(\text{New Interval Length}, 2^{n\ bits}\right)$. I.e. if we want to hide the value 6 in a silence interval with the length=109, we eliminate 7 samples from this interval that makes the new interval length 102(109 - 7) samples. Now we compute mod (102, 8) =6 to extract the hidden data from the silent interval in the stego signal. Small silence intervals are left interrupted since they usually arise in continuous sentences and changing them might alter the quality of the speech. This technique has a good perceptual transparency but apparently it is sensitive to compression. Modifications in silence intervals length will lead to incorrect data extraction. To overcome this inadequacy, [25] suggested slightly amplifying speech interval samples and decrease the silence interval samples. Therefore, silence sample intervals will not be interpreted speech samples and vice-versa. First and last intervals added to the speech during MP3 coding are ignored in data hiding and retrieval.

Strengths and weaknesses of temporal domain techniques

Robustness and security are not the main characteristics of temporal domain steganographic approaches, conventional Least Significant Bit technique and its variants provide a very easy and simple way for data hiding. Tolerance to noise addition at low levels and some robustness criteria have been achieved with LSB variants' techniques [17] [18] [19], but at a very low hiding capacity. At present time only few time domain hiding techniques have been developed.

5.2 Hiding in transform domain

Human Auditory System has certain peculiarities which must be exploited for effective data hiding. For frequencies masking from weaker frequencies to stronger resonant, apply the "masking effect" phenomenon on frequencies [26] [27]. Several approaches are defined next which have been proposed in in the transform domain. All these approaches exploit the frequency masking effect of the HAS directly to achieve the inaudibility by explicitly changing only masked regions [28] [29] [30] [31] or indirectly by modifying slightly the audio signals samples [32] [33].

5.2.1 Discrete Wavelet transform domain

Discrete Wavelet Transform (DWT) Audio steganography is described in [34] [34]. Data is embedded with signal in the LSBs of the wavelet coefficients of audio signal. To improve the inaudibility of embedded data, [36][31] employed a hearing threshold when hiding data in the integer wavelet coefficients, while[38] avoided data hiding in the silent parts of audio signal. In addition an algorithm is proposed for high capacity and inaudibility audio steganography scheme which is based on discrete wavelet packet transform with adaptive embedding in least significant bits [39]. The cover audio signal is break down into wavelet coefficients; each signal is scaled according to its maximum value and the number of bits per sample. The algorithm determines the number of bits that can be safely hidden in each sample. After that stego key is embedded in the lowest frequency details signal that makes the stego key more resistant against distortion and then stego signal is reconstructed.

5.2.2 Spread spectrum

In audio steganography, spread spectrum technique attempts to spread out hidden information through the frequency spectrum across the available frequencies as much as possible. In data communications, spread spectrum (SS) concept is developed to ensure a proper recovery of a signal sent over a noisy channel by generating redundant copies of the data signal. There are two versions of spread spectrum which can be used in audio steganography first is the direct-sequence and second is frequency hopping schemes. In the direct sequence SS, the secret information is spread out by a constant which called the chip rate and after that it modulated with a pseudorandom signal. Then it is interleaved with the cover audio signal. In the frequency hopping SS, audio signal frequency spectrum is modified so it hops quickly between frequencies. Fundamentally, information are multiplied by an M-sequence code which are known by both sender and receiver [40], and then information hidden in the cover audio object. So, if noise corrupts some data values, it kept copies of each value left to recover the hidden information. Conventional direct sequence spread spectrum (DSSS) technique was applied to conceal private information in WAVE and MP3 digital audio signals [41]. Data are hidden under a frequency mask to control stego-audio distortion.

Spread spectrum is combined phase shifting to increase the robustness of transmitted information against additive noise and to allow simple detection of the hidden information. Spread Spectrum technique has one main disadvantage that it can introduce noise into an audio file.

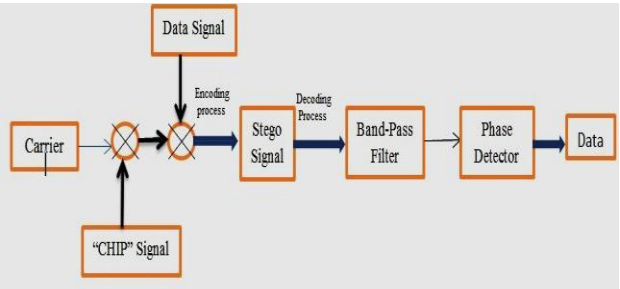

Figure: 6 Spread Spectrum

5.2.3 Tone insertion

In tone insertion method frequency masking property is exploited [42]. In the presence of a stronger tone a weak pure tone is masked. This property of imperceptibility is used in distinct ways to hide data. Tone insertion methods rely on the imperceptibility of inferior power tones in the presence of higher ones. Inserting imperceptible tones in cover audio signals for data embedding is given in [32] [43]. To hide one bit of data in an audio frame, this research proposes a pair of tones which is produced at two selected frequencies f1 and f2.The power level of the two masked frequencies is pf1 and pf2. It is set to a known ratio of the power of every audio frame pi where: i =1……..n, here n is the frame number as depict in Figure 7. To achieve concealed embedding and correct data extraction, insert tones at known frequencies and at low power level. The power pi for each frame is calculated as well as the power pf1 and pf2 for the selected frequencies f1 and f2 for detecting the tones and thus the hidden data from the stego audio frames. If the ratio, $\frac{pi}{pf1} > \frac{pi}{pf2}$ then the hidden bit is '0', otherwise it will be '1'.Tone insertion technique can prevent to attacks like bit truncation and low-pass filtering. Besides the low embedding capacity, hidden data could be extracted since inserted tones are very easy to detect. So the authors suggest overcoming these drawbacks by varying four or more pairs of frequencies in a keyed order.

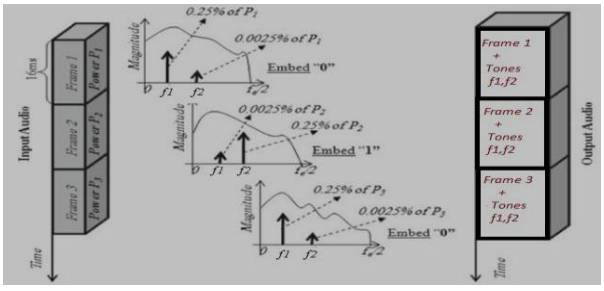

Figure: 7 Data hiding by inserting tones at two distinct frequencies

5.2.4Phase coding

Phase coding technique exploits HAS (Human Auditory System) insensitivity to relative phase of distinct spectral components. This is based on substituting selected phase components from the original audio signal spectrum with concealed data. Though, to ensure imperceptibility, phase components alteration should be kept minor [44]. Phase coding tolerates better signal distortion among data hiding techniques [45]. Authors in [44] have inserted data in phase components using an independent multi-band phase modulation. Imperceptible phase modifications are achieved by controlled phase alteration of the host audio which is shown in Figure 8. QIM (Quantization index modulation) technique is applied on phase components, in this method phase value of a frequency bin is substituted by the nearest O point to conceal '0' or X point to conceal '1'. Robustness is also achieved in phase quantization. Human Auditory System is not very sensitive to phase distortion; it against the fact which shows that phase quantization is robust to perceptual digital audio compression. When Phase coding approaches applicable, it is one of the most efficient audio steganographic techniques in terms of the signal to noise ratio (SNR). Phase dispersion will occur when the phase relation between each frequency component is dramatically changed. On the other side, on condition that the modification of the phase is small enough, an imperceptible steganography can be accomplished [45], [46].

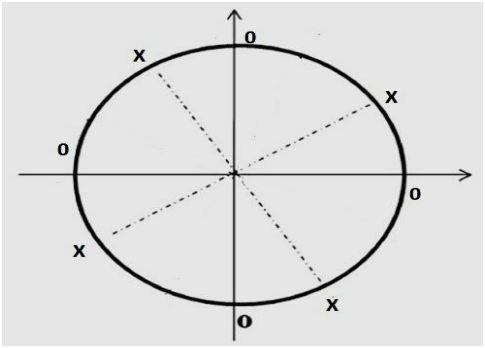

Figure 8 Phase quantization

Strengths and weaknesses of transform domain methods

In terms of signal to noise ratio, it has been proven that hiding of data in frequency domain rather than time domain will give better results [47]. Certainly, all audio steganography techniques are in the transform domain advantage from the frequency masking effect. Maximum of data hiding algorithms in audio steganography are based on transform domain use a perceptual model to determine the allowable amount of hidden data to avoid stego signal distortion. A huge number of transform domain have been proposed in the previous decade and to a certain expansion, all these methods have succeeded in realizing the security and robustness of concealed data against simple audio signal manipulations like filtration or resampling, amplification. Though concealed data robustness against simple audio signal manipulation is the main features of transform domain methods, hidden data will unlikely survive noisy transmission environment or data compression induced by one of the encoding processes.

6. AUDIO STEGANOGRAPHY ANALYSIS

The imperceptibility and the detectability rate of hidden data are measured by utilizing signal-to-noise ratio SNR for the evaluation of the performance of the reviewed audio steganography techniques [48]. In Imperceptibility evaluation signal-to-noise ratio SegSNR which represents the average of the SNRs of all altered audio signal frames and the PESQ measure are used. SegSNR's indicates the distortion amount

persuaded by the hidden data in the cover audio signal $S_c(m,n)$. In digital audio signals i.e. SNR below 20 dB is denoted a noisy audio signal but an SNR of 30 dB and above denoted that the quality of audio signal is preserved. SNR value is given by the following equation.

$$SNR_{db} = 10 \log_{10}\left(\frac{\sum_{n=1}^{N} |S_c\ (m,n)|^2}{\sum_{n=1}^{N} |S_c(m,n) - S_s(m,n)|^2}\right) \quad ..(1)$$

$S_s(m,n)$is the stego audio signal where m=1.....M and n=1.....N. where M is the number of frames in milliseconds and N is the number of samples in each frame. The SNR (dB) values and payload (kbps) are used to evaluate the methods. Maximum audio steganography technique which are based on transform domain use a perceptual model to determine the permissible amount of data hiding without distorting the audio signal , for control the distortion induced by the hiding process .Numerous audio steganography algorithms use most often frequency masking and auditory masking as the perceptual model for steganography embedding. Some frequency domain approaches, such as phase hiding implicitly inherit the phase properties that include robustness to mutual linear signal manipulations like amplification, filtering, attenuation, resampling etc. The performance of the technique is analysed in terms of Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR) and Signal to Noise Ratio (SNR). Quality evaluation of these approaches can be approved by performing compassion between original audio signal and stego audio signal.

Table: 1 Summary of Audio Steganography Techniques

Hiding domain	Methods	Data hiding Technique	Strength	Weakness
Temporal domain	Low bit encoding	LSB of each sample in the audio is substituted by one bit of hidden data	Simple and easy for hiding Information	Easy to extract
	Echo hiding	Hides the information by introducing echo in the cover signal	Avoid problem with additive noise	Low data security and low capacity
	Parity coding	Modify the LSB of parity bit of samples	More robust than LSB	Easy to extract
	Hiding in silence intervals	Uses the number of samples in silence interval to represent hidden data	Supple to lossy data compression algorithms	Low capacity
Transform Domain	Discrete Wavelet transform domain	Changing wavelet coefficients for data hiding	Provide high embedding Capacity and transparency	lossy data retrieval
	Spread spectrum	Spread the information over all signal frequencies	Provide better robustness and increase transparency	Vulnerable to time scale modification and occupies more bandwidth
	Tone insertion	insertion of imperceptible tones at selected frequencies	Exploits masking property	low security and capacity , Lack of transparency
	Phase coding	Modulate the phase of the cover signal	Robust against signal processing operation	Low capacity

7. CONCLUSION

In this paper, various audio steganography techniques are discussed as potential methods for hiding data digital audio signals. To provide better protection to data content, various new steganography techniques have been developed in recent research works, the specific requirements of each data embedding method vary from one application to another application; with each of these methods have some strengths and weaknesses. The main goal of steganography is to be unsuspected by the human eyes or human ear. The accessibility and popularity of digital audio files have made them good choice to transfer secret information. This work presents a review on audio steganography techniques and approaches and we also discussed their strengths and weaknesses. In general aim of temporal domain techniques are to maximize the embedding capacity, while in transform domain techniques exploit the masking properties in order to make the noise produced by hidden data undetectable. This survey presented that the frequency domain is preferred over the temporal domain and music signals are better covers for data embedding in terms of capacity, inaudibility and Undetectability. The flexible nature of audio file formats and signals makes them good and practical medium for steganography.

8. REFERENCES

[1] R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography" IEEE ICIP, pp. 1022-1022, Oct. 2001.

[2] R.J. Anderson, F.A.P. Petitcolas, “On the Limits of Steganography”, IEEE Journal of Selected Area in Communications, pp. 474-481, May 1998.

[3] N.F. Johnson, S. Jajodia, “Staganalysis: The Investigation of Hiding Information”, IEEE, pp. 113-116, 1998.

[4] H. Hastur, Mandelsteg, ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/

[5] Silman, J., "Steganography and Steganalysis: An Overview",SANS Institute, 2001

[6] S. Das, B. Bandyopadhyay and S. Sanyal, " Steganography and steganalysis: different sapproaches",Cornell University Library, 2011.

[7] S. K. Bandyopadhyay, B. Bhattacharyya, D. Ganguly, S.Mukherjee, P. Das, "A tutorial review on steganography", International Conference on Contemporary Computing, 2008

[8] E Zwicker, H Fastl,Psychoacoustics(Springer Verlag, Berlin, 1990)

[9] R.Anderson, F.Petitcolas: On the limits of the steganography, IEEE Journal Selected Areas in Communications, VOL .16, NO. 4, MAY 1998.

[10] FABIEN A. P. PETITCOLAS, ROSS J. ANDERSON, AND MA RKUS G. KUHN, Information Hid ing —A Survey, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999.

[11] Bender W, Gruhl D, Morimoto N, Lu A (1996). "Techniques for data hiding" IBM Syst. J., 35: 313-336.

[12] Cvejic N (2004). "Algorithms for audio watermarking and steganography", Department of Electrical and Information Engineering,Finland,University of Oulu.

[13] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography", 2011 International Conference on Computer Networks and Information Technology (ICCNIT), IEEE, 2011.

[14] K. Bhowal, A. Pal, G. Tomar, and P. Sarkar, "Audio steganography using GA", 2010 International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, 2010.

[15] K Gopalan, Audio steganography using bit modification, Proceedings of the IEEE 2003 International Conference on Acoustics, Speech, and Signal Processing (ICASSP'03), (Hong Kong, April 2003)

[16] N Cvejic, T Seppiinen, Increasing the capacity of, LSB-based audio steganography, IEEE Workshop on Multimedia Signal processing.(St. Thomas, USA 2002), pp. 336–338

[17] N Cvejic, T Seppanen, Increasing Robustness of, LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04). vol. 2, (Washington, DC, USA, 2004), pp. 533

[18] N Cvejic, T Seppanen, Reduced distortion bit-modification for LSB audio steganography. J. Universal Comput. Sci.11 (1), 56–65 (2005)

[19] MA Ahmed, LM Kiah, BB Zaidan, AA Zaidan, A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm. Appl. Sci.10, 59–64 (2010)

[20] D Gruhl, WBender, Echo hiding, proceeding of the 1st Information Hiding Workshop, Lecture Notes in Computer Science, (Isaac Newton Institute, England, 1996), pp. 295–315

[21] Jayaram P. , Ranganatha H R. , Anupama H S, " Information hiding using audio steganography – a survey" , International Journal of Multimedia & its applications ,Vol.3, No.3, August 2011

[22] Y Erfani, S Siahpoush, Robust audio watermarking using improved TS echo hiding. Digital Signal Process.19, 809–814 (2009)

[23] Fatiha Djebbar, Beghdad Ayady, Habib Hamamzand Karim Abed-Meraim, "A view on latest audio steganography", International Conference on Innovations in Information Technology, 2011, pages 409-414.

[24] S Shirali-Shahreza, M Shirali-Shahreza, Steganography in Silence Intervals of Speech, proceedings of the Fourth IEEE International Conference on Intelligent Information Hiding and Multimedia Signal (IIH-MSP 2008). (Harbin, China, August 15-17, 2008), pp. 605–607

[25] S Shirali-Shahreza, M Shirali-Shahreza, Real-time andMPEG-1 layer III compression resistant steganography in speech, The Institution of Engineering and Technology Information Security. IET Inf. Secur.4 (1), 1–7 (2010)

[26] F Djebbar, B Ayad, K Abed-Meraim, H Habib, Unified phase and magnitude speech spectra data hiding algorithm. Accepted in "Journal of Security and Communication Networks" (John Wiley and Sons, Ltd, 4 April, 2012)

[27] GS Kang, TM Moran, DA Heide, Hiding Information under Speech, Naval Research Laboratory, (Washington, DC NRL/FR/5550–05-10, 126, 2005), 20375-5320

[28] B Paillard, P Mabilleau, S Morissette, J Soumagne, PERCEVAL: Perceptual Evaluation of the Quality of Audio Signals. J. Audio Eng. Soc.40, 21–31(1992)

[29] H Matsuka, in IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06)Spread spectrum audio steganography using sub-band phase shifting, (Pasadena, CA, USA, December 2006), pp. 3–6

[30] X Li, HH Yu, Transparent and robust audio data hiding in sub band domain, Proceedings of the Fourth IEEE International Conference on Multimedia and Expo, (ICME 2000), (New York, USA, 2000),pp. 397–400

[31] M Pooyan, A Delforouzi, Adaptive Digital Audio Steganography Based onInteger Wavelet Transform, Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2007). vol. 2, (Splend or Kaohsiung ,Taiwan, 2007), pp. 283–28

[32] K Gopalan,et al, Covert Speech Communication Via Cover Speech By Tone Insertion, Proceeding of IEEE Aerospace Conference, (Big Sky, Montana, March 2003)

[33] K Gopalan, A unified audio and image steganography by spectrum modification, IEEE International Conference on Industrial Technology (ICIT'09), (Gippsl and, Australia, 10-13 Feb 2009), pp. 1–5

[34] Jisna Antony, Sobin C.C., Sherly A.P., "Audio steganography in wavelet domain A survey", International Journal of Computer Applications, volume 52 -no. 13, Aug 2012.

[35] N Cvejic, T Seppanen, A wavelet domain, LSB insertion algorithm for high capacity audio steganography, Proc.

10th IEEE Digital Signal Processing Workshop and 2nd Signal Processing Education Workshop, (Georgia, USA, 13-16 October, 2002), pp. 53–55

[36] S. Nehete, S. Sawarkar, and M. Sohani, "Digital audio steganography using DWT with reduced embedding error and better extraction compared to DCT", Proceedings of the International Conference & Workshop on Emerging Trends in Technology, ACM, 2011

[37] S Shirali-Shahreza, M Shirali-Shahreza, High capacity error free wavelet domain speech steganography, Proc. 33rd Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP 2008). (Las Vegas, Nevada, USA, 30 March 2008), pp. 1729–1732

[38] Haider Ismael Shahadi and Razali Jidin, "High capacity and inaudibility audio steganography scheme", 7th International Conference n Information Assurance and Security (IAS), IEEE, 2011

[39] K Khan, Cryptology and the origins of spread spectrum. IEEE Spectrum.21, 70–80 (1984)

[40] Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, 2009, Page(s):1,5

[41] K. Gopalan and S. Wenndt, "Audio steganography for covert data transmission by imperceptible tone insertion", Proceedings of Communications Systems and Applications, IEEE, 2004.

[42] K Gopalan, S Wenndt, Audio Steganography for Covert Data Transmissionby Imperceptible Tone Insertion, WOC 2004, (Banff, Canada, July 8–10,2004

[43] L Gang, AN Akansu, M Ramkumar, MP3 resistant oblivious steganography, Proceedings of, IEEE International Conference on Acoustics, Speech, and Signal Processing. Vol. 3, (Salt Lake City, UT. 7-11 May 2001),pp. 1365–1368

[44] Kumar S. B., D. Bhattacharyya, P. Das, D. Ganguly and S. Mukherjee, "A tutorial review on Steganography", International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[45] Bender, W., W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Techniques for datahiding", IBM Systems Journal, Volume 39, Issue 3-4, July 2000, pp. 547 – 568.

[46] WBender, D Gruhl, N Morimoto, A Lu, Techniques for Data Hiding. IBM Syst. J.35(3 and 4), 313–336 (1996)