ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

A Survey Paper on Audio Steganography and It's Applications

Namrata Singh

P.G Student, Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad, U.P, India

ABSTRACT : Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message . There are often cases when it is not possible to send messages openly or in encrypted form. This is where steganography can come into play. While cryptography provides privacy , steganography is intended to provide secrecy .This paper contains a survey on hiding of text behind multimedia, i.e. digital images,wave audio, real media audio, etc.

KEYWORDS : Audio Steganography, Cryptography, Transform Domain, LSB Insertion

I. INTRODUCTION

The word steganography comes from the Greek Steganos, which means covered or secret and -graphy means writing or drawing. Therefore, steganography means, literally, covered writing.[1]
It is the practice of concealing information by attaching it with other files in a manner that its presence remains undetectable to alien third party users. It's different from cryptography in the sense that it not just necessarily encrypts information but conceals its very existence. Thus, a person other than the sender or recipient of the message will be unable to suspect that it exists. [2]
Cryptography - conceals identity
Steganography - conceals existence
In modern day digital steganography, data is first encrypted, then embedded into other files which makes data unintelligible as well as invisible, preventing it from access by an unintended recipient.[3]
Steganography aims to ensure secure communication in a completely undetectable manner and to avoid drawing suspicion to the transmission of secret data. Hence it is not only a way to prevent others from having access to the hidden information, but to also prevent them from suspecting that the message even exists [4, 5]

II. RELATED WORK

1. **Audio Steganography Using Dual Randomness LSB Method :** Authors used approach in this paper is to randomize the point of embedding of the secret file in the audio file sample points. The size of the secret data file is of a great significance to the randomization algorithm. The randomization pattern used in this design is two fold the first step finds out the byte numbers that will be the sample point for embedding data the second step will be the bit place in that byte where the one bit of the secret data will be embedded. By this way the robustness and transparency of the steganographic technique is increased.[7]
2. **Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method:** A subjective listening test done in our laboratory showed 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, if 16 bits per sample audio sequences are used. The tests were performed with a large collection of audio samples and individuals with different backgrounds and musical experience. None of the tested audio sequences had perceptual artifacts when

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

the fourth LSB has been used for data hiding, although in certain music styles, the limit is even higher than the fourth LSB. The robustness of the watermark, embedded using the LSB coding method, increases with increase of the LSB depth used for data hiding.[11]

3. **Lossless Audio Steganography in Spatial Domain :** In this paper authors devised a hash function in order to generate pseudorandom position for insertion and extraction of secret message bits from an audio sample. In each audio sample, secret bits are embedded in LSBs based on pseudorandom position generated .This technique supports text, image and audio as a secret message.[6]

III. AUDIO STEGANOGRAPHY

Audio steganography refers to hiding information in a cover (host) audio signal in an imperceptible way. This information from the embedded signal can be read by using the key which was initially used to insert the information. One challenge posed to hiding data in audio signals is the sensitivity of the human auditory system (HAS) which is sensitive to slight distortions in audio so, in order to successfully utilize this technique, alterations must be made within the limitations that can be tolerated by HAS. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.[6]

IV. CONDITIONS FOR STEGANOGRAPHY

To implement any audio steganography successfully, it must satisfy the following 3 conditions:

1. Capacity – It is the amount of data that can be inserted into the cover audio while maintaining the quality of the audio.[7]
2. Robustness – It is a measure of the embedded data's capability to maintain its secrecy against third party attacks such as filtering attacks, rescaling, resizing and random chopping etc. or common data manipulations like resampling and requantization. [8]
3. Transparency – Transparency shows how flawlessly the hidden message is embedded into the host signal. An immaculate steganography will have negligible difference in audio before & after performing it. [7]

V. INFORMATION HIDING PROCESS

In audio steganography, the cover file is an audio file which hides different types of data. The secret message file or the data to be embedded is inserted in the cover file using a key. This results in a modified version of the cover file that contains embedded message. This becomes the stego file. On reaching from the sender to the recipient the extraction process begins. If the key supplied by recipient is the same as the one employed by the sender, then it will produce a message identical to the input. [9, 10]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

VI. AUDIO STEGANOGRAPHY METHODS

In audio steganography, data embedding can be performed in spatial domain as well as frequency domain.

1. Spatial Domain Approaches

a)LSB Insertion

In this technique, there is always a trade-off between the two parameters, transparency and capacity. It is done by hiding information in the least significant bits of audio files since data in audio samples is mostly stored in the most significant bits (MSBs).

Changing the LSBs induces distortion in the file but remains undetectable if kept below a threshold level. Hence, more the number of altered LSBs, more the noise. Also, altering more LSBs per sample increases the capacity of the sample to carry information. Hence, using more LSBs increase capacity while decreasing transparency. [11]

Standard LSB ALGORITHM:

It performs bit level manipulation to encode the message.

The following steps are :

a. Receives the audio file in the form of bytes and converted into bit pattern.

b. Each character in the message is converted in bit pattern.

c. Replaces the LSB bit from audio with LSB bit from character in the message.

b)Echo Hiding

This technique embeds secret information in an audio file by introducing an echo and embedding data in it. It provides a high transmission rate and excellent robustness but low embedding rate and security. Since only one bit of information can be stored is an echo, the original signal is broken down into blocks to produce numerous echos and later joined back to make the original signal. offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.[12, 13]

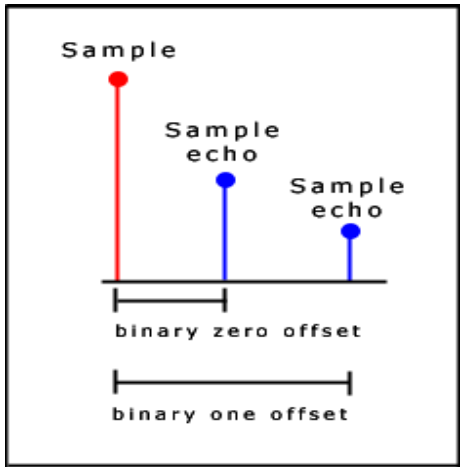

Fig 1. Sampling Binary zero And One Offset

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The "one" echo signal is then multiplied by the "one" mixer signal and the "zero" echo signal is multiplied by the "zero" mixer signal. Then the two results are added together to get the final signal. The final signal is less abrupt than the one obtained using the first echo hiding implementation. This is because the two mixer echoes are complements of each other and that ramp transitions are used within each signal. These two characteristics of the mixer signals produce smoother transitions between echoes. Below Figure 2 shows the implementation of echo hiding Process.

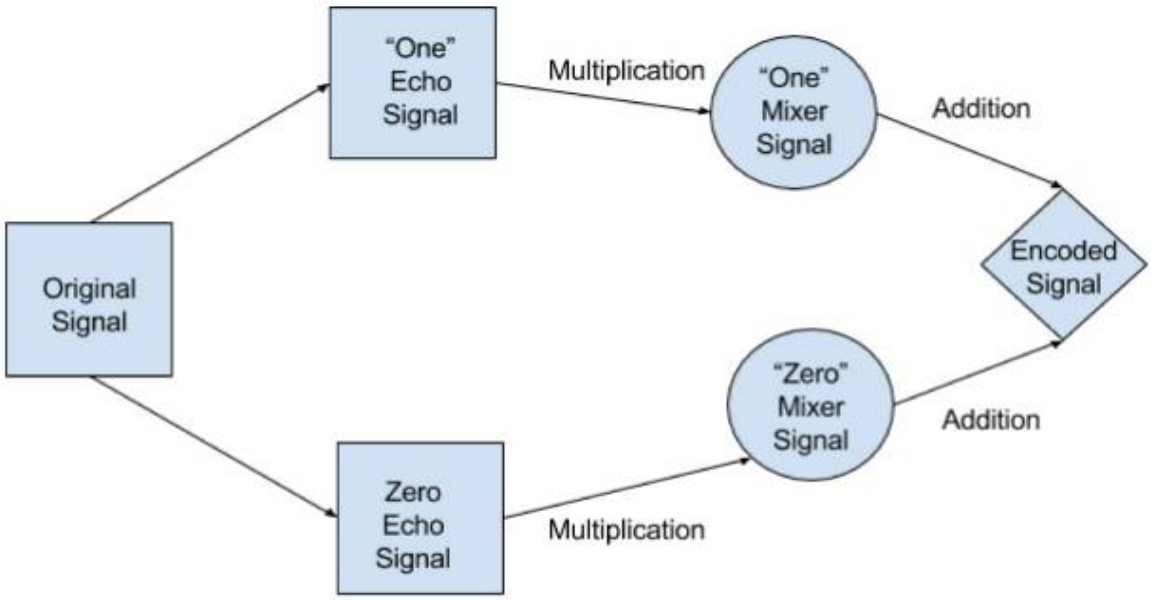

Fig.2 Second Implementation Of The Echo Hiding Process

To extract the secret message from the stego-signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process. Then the autocorrelation function of the signal's spectrum (the spectrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed. Much like phase encoding this has considerably better results than Low Bit Encoding and makes good use of research done so far in psychoacoustics. As with all sound file encoding, we find that working in audio formats such as WAV is very costly, more so than with bitmap images in terms of the "file size to storage capacity" ratio. The transmission of audio files via e-mail or over the web is much less prolific than image files and so is much more suspicious in comparison. It allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods.

c) Parity Coding

In this method, a signal is broken down into regions of samples instead of individual samples of the audio signal. Each bit of the secret message is then encoded in the sample region's parity bit. But in case the secret message is then encoded in the sample region's parity bit. But in case the secret bit & the parity bit aren't the same in a region, the LSB of the same in a region, the LSB of one of the samples in region gets inverted, thereby giving the sender more choice in encoding information on the audio signal. [16]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

2. Transform Domain Approaches

These methods hide information along the frequency distribution of the carrier signal.

a) Spread Spectrum technique

This method spreads the secret information over the frequency spectrum of the audio signal using a code which is independent of the audio sample and is known only y to the sender and the receiver.

It offers a moderate data transmission rate & superior robustness but can introduce noise into the audio file. [14, 15]

Two versions of SS can be used in audio Steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies. Spread Spectrum Steganography has significant potential in secure communications – commercial and military. Audio Steganography in conjunction with Spread Spectrum may provide added layers of security. Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, but it can introduce random noise to the audio thus creating the chance of data loss. They have the potential to perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques. Figure 3 below shows the procedural diagram of spread spectrum technique.

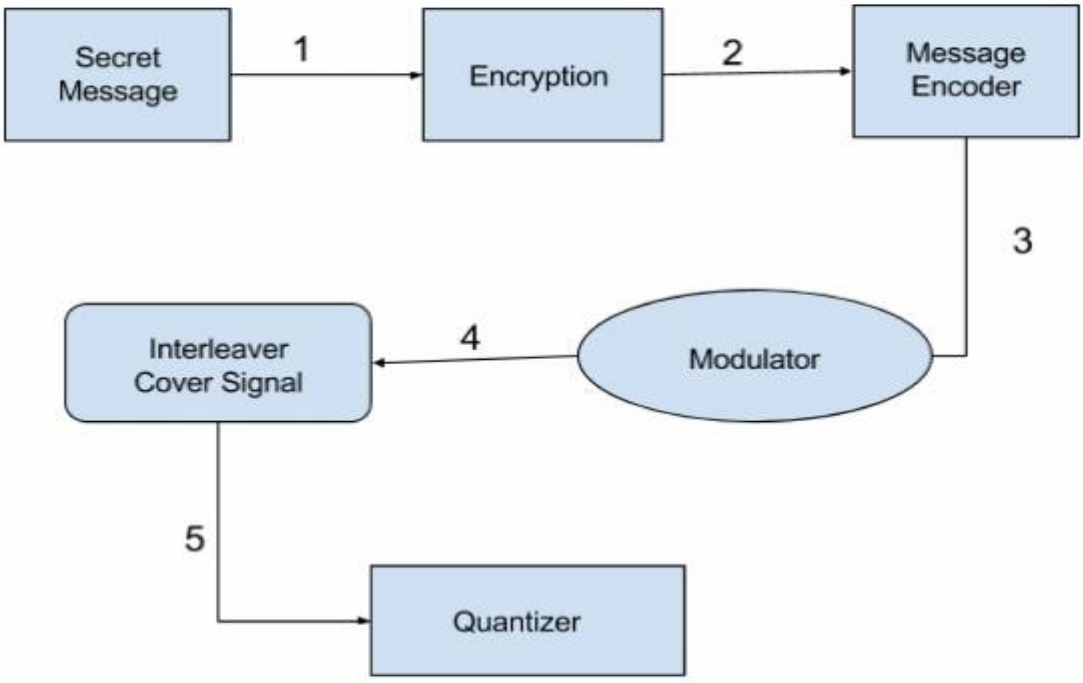

Fig.3 Procedural Diagram Of Spred Spectrum

1. Secret Message Encrypted Using Symmetric Key
2. Encoding Of Encrypted Message
3. Modulation Of Encoded Message

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

4. Resulting Random Signal is Interleaved with Cover Signal
5. Final Signal Is Quantized
6. Process Is reversed for Message Extraction

b) Phase Coding

In this method, the initial phase of the audio segment is replaced with the reference phase of the secret message. The subsequent segment's phases are altered in accordance. Phase shifts between adjacent segments can be easily detected. Hence, the relative phase difference between them must be maintained. During extraction of the message, the receiver uses the length of the segment to get the output[13]. Phase coding addresses the disadvantages of the noise-inducing methods of audio Steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio. Below you can see the original signal and the phase coded signal in the figure.

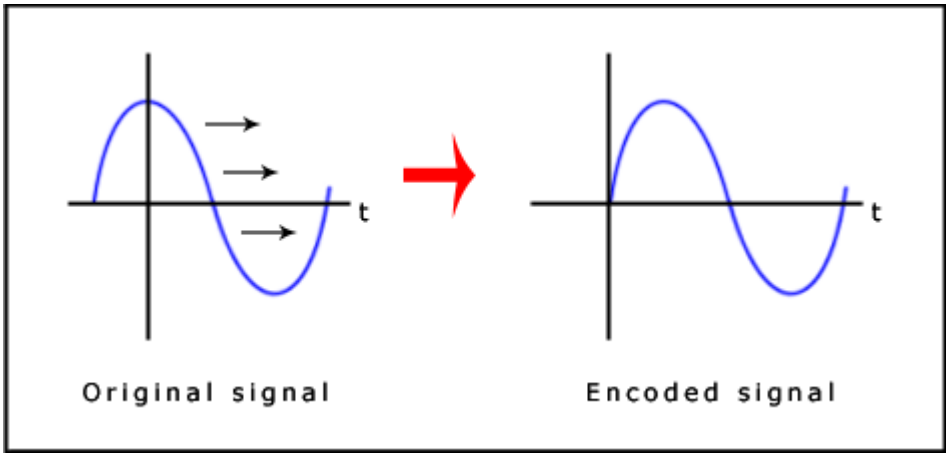

Fig.4 Depicting Original And Phase Coded Signal

The phase coding method breaks down the sound file into a series of N segments. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phase and magnitude. The phase difference between each segment is calculated, the first segment (s0) has an artificial absolute phase of p0 created, and all other segments have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new segments are then concatenated to create the encoded output and the frequency remains preserved. In order to decode the hidden information the receiver must know the length of the segments and the data interval used. The first segment is detected as a 0 or a 1 and this indicates where the message starts. This method has many advantages over Low Bit Encoding, the most important being that it is undetectable to the human ear. Like all of the techniques described so far though, its weakness is still in its lack of robustness to changes in the audio data. Any single sound operation or change to the data would distort the information and prevent its retrieval.

c) Discrete Wavelet Transform

This method is used to hide data transform coefficients if the sound signal. It decomposed with different resolutions so as to find the most suitable sub-band for encoding information. It provides with a high embedding rate but a possibility of inaccuracy in recovering the hidden info. [2]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Encoding Algorithm Steps :
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2D Haar transform on the cover image.
Step 3: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Decoding Algorithm Steps :
Step 1: Read the stego image.
Step 2: Obtain the horizontal and vertical filtering coefficients of the cover image.
Step 3: Extract the message bit by bit and recomposing the cover image.
Step 4: Convert the data into message vector. Compare it with original message.

3. Tone Insertion

This techniques makes use of auditory masking. The human auditory system facilitates this as the strong tones masks the weaker tones by making them inaudible, hence undetectable. This method is strong in terms of withstanding low-pass filtering and bit truncation attacks but it offers low embedding capacity and security. [2]
It relay into frequency masking property. Masking property is exploited in tone insertion method. A weak pure tone is masked in the presence of a stronger tone. This property of inaudibility is used in different ways to embed information. By inserting tones at known frequencies and at low power level, concealed embedding and correct data extraction are achieved.
The hidden information is imperceptible if a listener is unable to distinguish between the cover- and the stego-audio signal. The first problem that all data-embedding using tone insertion method needs to address is that of inserting data in the digital signal without deteriorating its perceptual quality. Of course, we must be able to retrieve the data from the edited host signal, i.e., the insertion method must also be invertible. Since the data insertion and data-recovery procedures are intimately related, the insertion scheme must take into account the requirement of the data-embedding application. In many applications, we will need to be able to retrieve the data even when the host signal has undergone modifications, such as compression, editing, or translation between formats, including A/D and D/A conversions.Audio masking is the effect by which a faint but audible sound becomes inaudible in the presence of another louder audible sound. The masking effect depends on the spectral and temporal characteristics of both the masked signal and the masker. Frequency masking refers to masking between frequency components in the audio signal. If two signals that occur simultaneously are close together in frequency, the stronger masking signal may make the weaker signal inaudible.
The masking threshold of a masker depends on the frequency, sound pressure level, and tone-like or noise-like characteristics of both the masker and the masked signal. It is easier for a broad-band noise to mask a tonal signal than for a tonal signal to mask out a broad-band noise. Moreover, higher frequency signals are more easily masked. The human ear acts as a frequency analyzer and can detect sounds with frequencies that vary from 10 to 20 000 Hz. The HAS can be modeled by a set of bandpass filters with bandwidths that increase with increasing frequency. The bands are known as the critical bands. The critical bands are defined around a center frequency in which the noise bandwidth is increased until there is a just noticeable difference in the tone at the center frequency. Thus, if a faint tone lies in the critical band of a louder tone, the faint tone will not be perceptible. Frequency-masking models are readily obtained from the current generation of high-quality audio codec's, e.g., the masking model defined in the International Standards Organization (ISO)-MPEG Audio Psychoacoustic Model 1 for Layer I. The Layer I masking method is summarized as follows for a 32-kHz sampling rate. The MPEG model also supports sampling rates of 44.1 and 48 kHz. The frequency mask is computed on localized segments (or windows) of the audio signal. The final step into this model consists of computing individual and global masking thresholds.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

VII. APPLICATIONS OF STEGANOGRAPHY

Audio steganography used to hide data in order to prevent unauthorized people from gaining access to it. Existing audio steganography software can embed messages in wav, au, mp3 sound files. Different domains of performing it have different features which make them suitable for different applications.
In the commercial sector it can be used to hide a secret plan or invention. [17]. It can also be used by anyone who wishes to keep information private. Terrorist can make use of it to communicate and coordinate planning of attacks. [18]. For Protection of copyrighted digital media and government information system security and covert communications, data can hidden in audio and video files [14, 19]. It can also be used in forensic application to conceal data as well as in the music industry to monitor data sharing.

ADVANTAGES :

- Audio based Steganography has the potential to conceal more information:
  - Audio files are generally larger than images
  - Our hearing can be easily fooled
  - Slight changes in amplitude can store vast amounts of information
- The flexibility of audio Steganography is makes it very potentially powerful :
  - The methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone. A party that wishes to communicate can rank the importance of factors such as data transmission rate, bandwidth, robustness, and noise audibility and then select the method that best fits their specifications.
  - For example, two individuals who just want to send the occasional secret message back and forth might use the LSB coding method that is easily implemented. On the other hand, a large corporation wishing to protect its intellectual property from "digital pirates" may consider a more sophisticated method such as phase coding, SS, or echo hiding.
- Another aspect of audio Steganography that makes it so attractive is its ability to combine with existing cryptographic technologies.
  - Users no longer have to rely on one method alone. Not only can information be encrypted, it can be hidden altogether.
- Many sources and types makes statistical analysis more difficult :
  - Greater amounts of information can be embedded without audible degradation
- Security :
  - Many attacks that are malicious against image Steganography algorithms (e.g. geometrical distortions, spatial scaling, etc.) cannot be implemented against audio Steganography schemes. Consequently, embedding information into audio seems more secure due to less steganalysis techniques for attacking to audio.
  - As emphasis placed on the areas of copyright protection, privacy protection, and surveillance increases, Steganography will continue to grow in importance as a protection mechanism.
  -
  - Audio Steganography in particular addresses key issues brought about by the MP3 format, P2P software, and the need for a secure broadcasting scheme that can maintain the secrecy of the transmitted information, even when passing through insecure channels.

DISADVANTAGES:

- Embedding additional information into audio sequences is a more tedious task than that of images, due to dynamic supremacy of the HAS over human visual system.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

- Robustness: Copyright marks hidden in audio samples using substitution could be easily manipulated or destroyed if a miscreant comes to know that information is hidden this way.
- Commercialized audio Steganography have disadvantages that the existence of hidden messages can be easily recognized visually and only certain sized data can be hidden.
- Compressing an audio file with lossy compression will result in loss of the hidden message as it will change the whole structure of a file. Also, several lossy compression schemes use the limits of the human ear to their advantage by removing all frequencies that cannot be heard. This will also remove any frequencies that are used by a Steganography system which hides information in that part of the spectrum.

VIII. CONCLUSION

Recent research in the field of steganography has facilitated the security of digital information for several purposes. Its various techniques maintain high level of data security during transmission of valuable data amongst the method discovered so far, in each, there is an interplay of capacity, noise, accuracy, data embedding rate, data extraction rate and various other factors. Hence the method employed must be in keeping with the requirements of applications at hand.

REFERENCES

1. Vipul Singhal, Dhananjay Yadav, Devesh Kumar Bandil, Steganography and Steganalysis: A Review, International Journal of Electronics and Computer Science Engineering ISSN: 2277-1956.
2. Ifra Bilal, Mahendra Singh Roj, Rajiv Kumar and P K Mishra, “Recent Advancement in Audio Steganography” IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC) , Solan , Dec 2014, pp 402-405
3. W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, “Techniques for data hiding”, IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.
4. Nedeljko Cvejic, Tapio Seppben “Increasing the capacity of LSB-based audio steganography” FIN-90014 University of Oulu, Finland, 2002
5. Neil F.Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking-Attacks and Countermeasures”,Kluwer Academic Publishers, 2001
6. Dipankar Pal, Anirban Goswami and Nabin Ghoshal, “Lossless Audio Steganography in Spatial Domain (LASSD),” Springer Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Advances in Intelligent Systems and Computing, vol. 199, 2013, pp. 575-582
7. Jithu Vimal and Ann Mary Anex, “Audio Steganography Using Dual Randomness LSB Method” ,IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 10-11 July 2014 ,pp 941-944
8. Anupam Kumar Bairagi, Saikat Mondal and Amit Kumar Mondal , “A Dynamic Approach In Substitution Based Audio Steganography”, IEEE International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, 18-19 May 2012,pp 501-504
9. K. Gopalan, “Audio steganography using bit modification”,Proceedings of International Conference on Multimedia and Expo, Vol. 1, pp.629-632, 6-9 July 2003
10. 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, pp.533, 2004.
11. Muhammad Asad, Junaid Gilani, and Adnan Khalid, “An Enhanced Least Significant Bit Modification”, IEEE, International Conference on Computer Networks and Information Technology (ICCNIT), Abbottabad, July 2011, pp 143-147
12. Sajad Shirali-Shahreza M.T. Manzuri-Shalmani “High capacity error free wavelet domain speech steganography” ICASSP 2008
13. V. Vapnik, “Statistical Learning Theory”, John Wiley, 2008.
14. Mengyu Qiao, Andrew H. Sung, Qingzhong Liu “Feature Mining and Intelligent Computing for MP3 Steganalysis” International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009
15. R. A. Santosa, P. Bao," Audio-to-Image Wavelet Transform based Audio Steganography", 47th International Symposium ELMAR-2005 , 08-10 June 2005, Zadar, Croatia, pp 209-212.
16. Nedeljko Cvejic, Tapio Seppben “Increasing the capacity of LSB-based audio steganography ” FIN-90014 University of Oulu, Finland ,2002.
17. S. Shirali-Shahreza, M. T. Manzuri-Shalmani, "Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate", IEEE International Conference on Information and Emerging Technologies, 2007, 06-07 July 2007 pp 1-5.
18. M. Pooyan, A. Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”, in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.
19. Yincheng Qi, Jianwen Fu, and Jinsha Yuan, “Wavelet domain audio steganalysis based on statistical moments of histogram”, Journal of System Simulation, Vol 20, No. 7, pp. 1912-1914, April 2008.