International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 4 (2018) pp. 1931-1935
© Research India Publications. https://dx.doi.org/10.37622/IJAER/13.4.2018.1931-1935

Steganography on Audio Wave Tenth Layer by Using Signal to Noise Ratio Test and Spectrogram Analyses

Sumit Kumar Moudgil
Assistant Professor

Dr. Amit Kumar Goel
Professor

Dr. Manish Sharma
Professor

Department of Computer Science and Engineering, FET,
Shree Guru Gobind Singh Tricentary University, Gurugram 122505, Haryana, India.

Abstract

Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and it is important that communication be made secret. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an unstable growth in the field of information hiding. Steganography is a popular method available to provide security. In steganography, the data is embedded in an Audio wave and the Audio wave is transmitted. In this paper Signal to Noise Ratio and Spectrogram analyses method is proposed which will ensure the robustness of an audio wave embedded with the secret message. Our aim is to make a secure and safe communication. This paper focuses on the strength of stegnography methods to enhance the security of communication over an open channel.

Keywords: Steganography, message, audio wave, smawawist (send more army with advance weapons in short time), spy analyses, GUI (Graphical User Interface)

INTRODUCTION

The word Steganography was originated from the Greek words "stegos" symbolic value is "cover" and "grafia" symbolic value is "writing" meaning is "covered writing". It is a field of concealment secret information in a hiding media. The secret message is being concealed in a audio wave file in a certain way so that the occurrence of the message remains unidentified to the one who makes observations [1]. A systematic plan behind Audio wave Steganography process is to conceal the hidden text message in an audio wave called carrier audio wave. The audio an outcome after this process is called stego audio, which is send to the receiver from a channel which is free from attack. At the decryption side audio wave is modified to extract secret text message from it by the act of applying a secret key. There are a large number of other steganography techniques which are in repetition these days for improvement, amidst which Text, Picture and Video Steganography are common. The actual existence of this paper is to send secret message in an audio wave and check the safety and security of the audio wave by doing spy analyses which include Signal to Noise ratio test and spectrogram analyses.

Section I of this paper describes previous related work regarding different LSB method. The proposed methodology is presented in section II. Experimentation and Discussion of the suggested method looks in Section III and finally Section IV concludes the paper.

The Indexing Key determines exact bit position and channel where the secret message bit has to be placed [2]. In [3], a design is suggested which enhances the secrecy of the secret message and also enhances the potential of the steganographic method. If such alteration is not possible in any sample then a separate sample is chosen. In this paper Signal to Noise Ratio and Spectrogram analyses method is proposed which will ensure the robustness of an audio wave embedded with the secret message. Our aim is to make a secure and safe communication. This paper focuses on the strength of stegnography methods to enhance the security of communication over an open channel.

PROPOSED TECHNIQUE

There are many other steganography techniques which are in practice in present days, amongst which Text, Image (Picture) and Video Steganography are popular.

Table I

Existing Techniques	Week point
Least Significant Bit	1-Simple to extract 2-Addition of noise 3-Compression can damage the data
Parity coding	Easy to extract and destroy
Echo hiding	Low embedding capacity and security
Phase coding	Low Capacity
Spread spectrum	1-Occupies more bandwidth 2-Unprotected to time scale modification
Wavelet Domain	Extracted data may be lossy

Table I shows the two columns. In the first column we have listed six existing techniques and in the second column we have shown their week points.

In our technique there is no weak point because an intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers of audio wave to achieve higher capacity and robustness. Our technique depends heavily on identity/key for its security.

Steganography is well known and widely used technique that manipulate information in order to hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication.

The aim of this thesis is to describe a method for integrating steganography through some media such as audio.

By using a algorithm Graphical User Interface (GUI) was created for easy interaction with the user as shown.

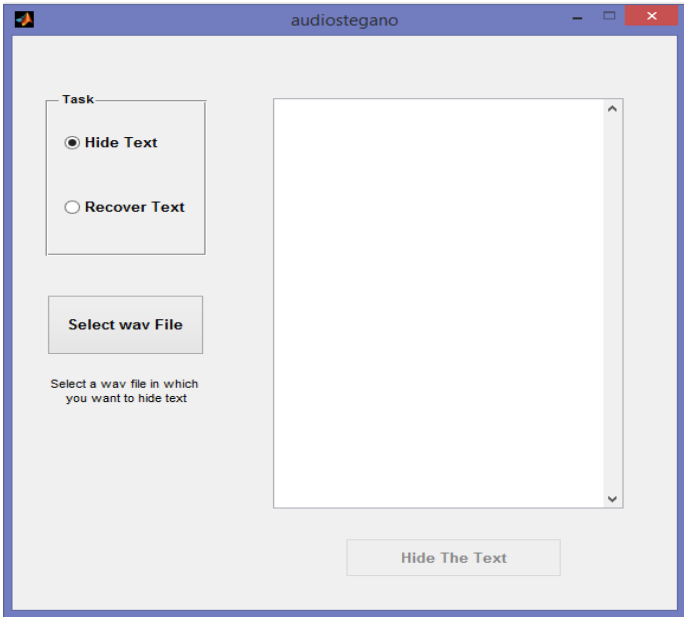

Figure 1: GUI for performing steganography obtained from audiostegano.m file in MATLAB

We are doing Spy Analyses so that we can think from the enemy army point of view and what steps they can take in order to extract out the secret information from an audio wave. Spy Analyses includes SNR ratio test and Spectrogram Analyses.

SIGNAL TO NOISE RATIO TEST

We are doing SNR ratio test in MATLAB for minimum and maximum message embedded in Wav file – 'LC_House_Beat_123_1.wav'

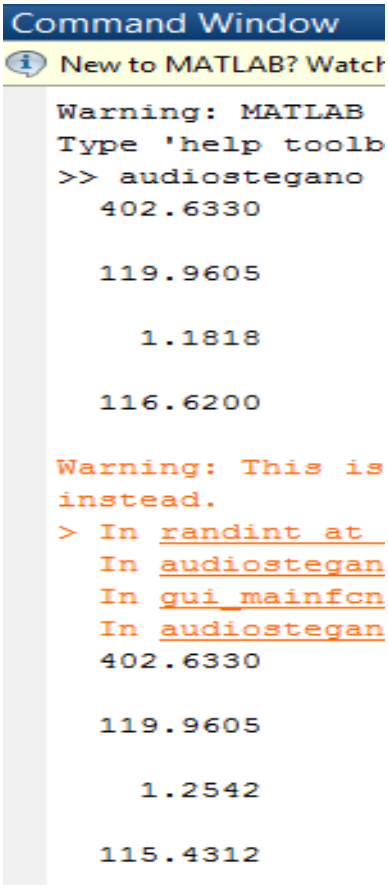

Figure 2: Command window in MATLAB shows the SNR for minimum embedding message is 116.6200 dB and SNR for maximum embedding message is 115.4312 dB.

From the above we can conclude that there is an inverse relationship between SNR and Message. For example if the message is minimum then the SNR is maximum and if the message is maximum then the SNR is minimum. Message During SNR Ratio testing, we have calculated the SNR ratios of audio wav files before and after embedding. The code for this test and all the tests, including the genetics based more robust algorithms covering capacity and robustness at high levels. Code for SNR ratio calculation is already in included in audio stegano.m file which contains the algorithms for Encryption and Decryption along with GUI for performing steganography.

Table II

Embedding	SNR (Min. embedding)	SNR (Max. embedding)
Tenth Layer	116.6200 dB	115.4312 dB

Table II shows Signal to Noise Ratio for message embedding on Tenth Layer

It can be observed from the table that this algorithm does not show up significant changes in the audio signal under the spy analyses test.

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 4 (2018) pp. 1931-1935
© Research India Publications. https://dx.doi.org/10.37622/IJAER/13.4.2018.1931-1935

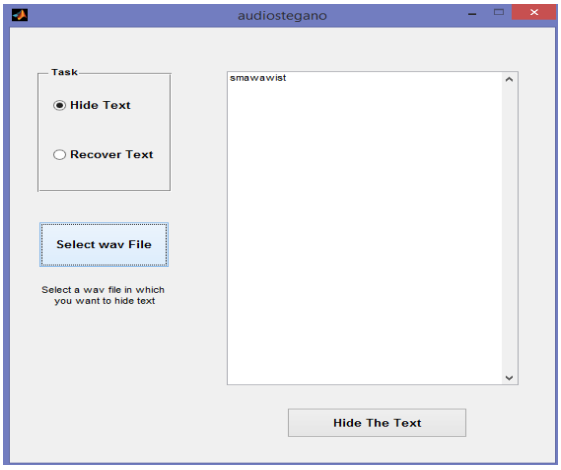

Figure 3: GUI showing Minimum message (i.e smawawist) encryption

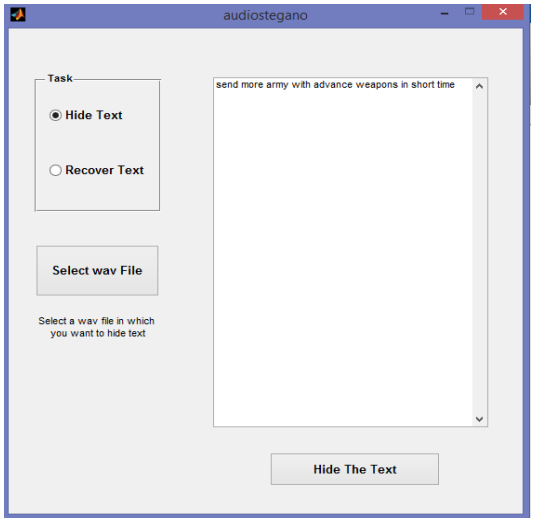

Figure 4: GUI showing Maximum message (i.e send more army with advance weapons in short time) encryption

When enemy nation wants to know what is the communication being done between our army the minimum message which they get on their computer screen is

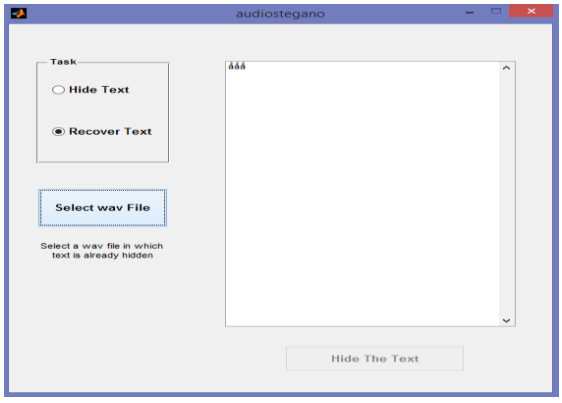

Figure 5: GUI showing Minimum message decryption by enemy army (i.e aaa)

The above message (i.e aaa) on GUI obtained by enemy army confirms that our secret message is safe and secure in an audio wave which is being transmitted, But when the message (i.e aaa) seen on GUI when decrypted by our army they use a secret key on the receiver side and the message which they get on their computer screen is smawawist. This confirms that the communication which we are doing is safe and secure with our confidential secret key.

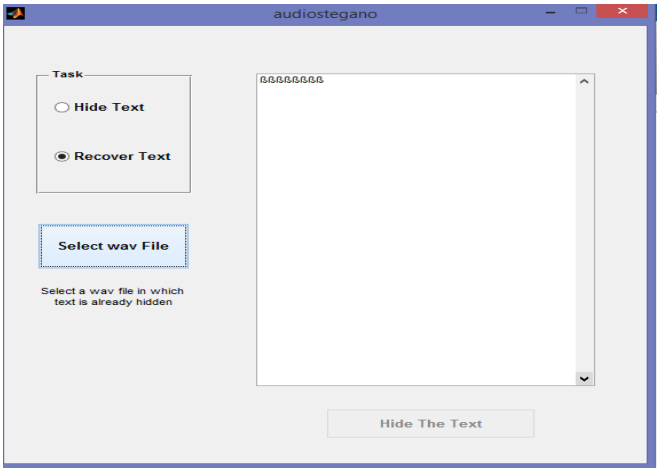

Figure 6: Maximum message decryption by enemy army (i.e BBBBBBBB)

When the above message is decrypted by our army they use a secret key on the receiver side and the message which they get on their computer screen is send more army with advance weapons in short time.

SPECTROGRAM ANALYSES

Now we will see the spectrum analyses of audio wav files on Time vs. Frequency vs. Amplitude response of the signals. Modulation spectrum analysis is emerging as a novel sound representation which has found applications in both ASR as well as most recently in audio coding.We will see spectrogram of original wav file and then *difference* spectrum analyses between (original and max embedding wav) and (original and min embedding wav).Original Signal Wav file – 'LC_House_Beat_123_1.wav' and after embedding it is named as 'lsb1_max.wav' and 'lsb1_min.wav'. We will first plot the original Wav spectrum and then difference of 3D spectrums.

Code for all spectrograms is given in two MATLAB script files –

'spectogram.m' and **'DifferenceSpectogram.m'**

The actual existence of the proposed technique is to add more protection against steganalysis. There is always an advantage on the state and data strength for big data [4]. The proposed method minimizes this trade of using more event that is described by a probability distribution. Fig.3 shows spectrogram of carrier audio signal having size 1.97MB and stego audio corresponding to the same carrier audio, which contains a message load of 4bytes [5]. We can clearly analyse that there is a minimal change in the structure of the stego

audio.

A. Original Wav:

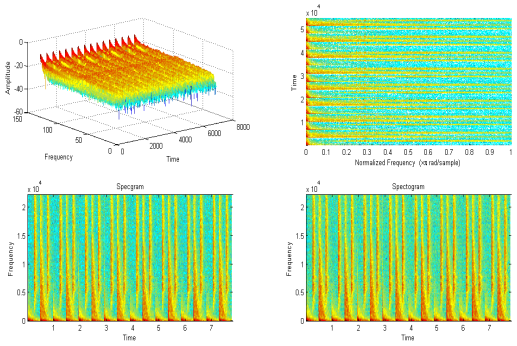

Figure 7: Original Spectrograms of Wave file A

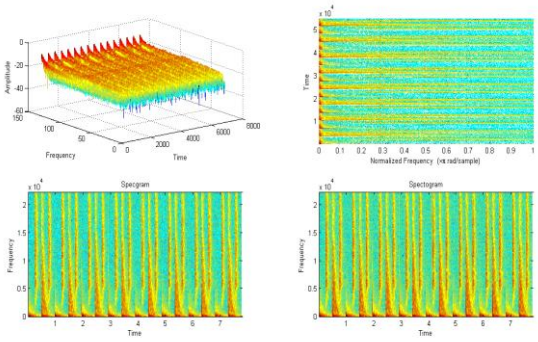

Figure 8: Spectrogram of layer 10 max embedded Wave file a1

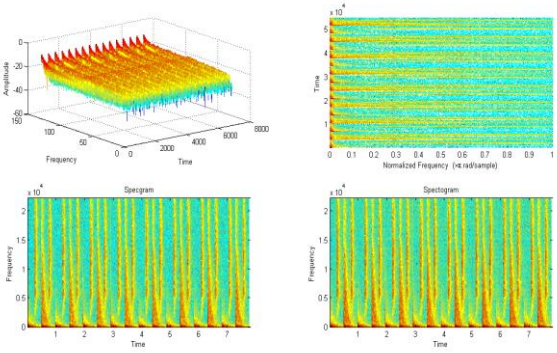

Figure 9: Spectrogram of layer 10 min embedded Wave file b1

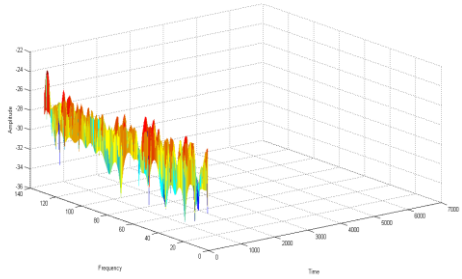

Figure 10: Difference Spectra of Original and Layer 10 Max Embedded Wave (A-a1)

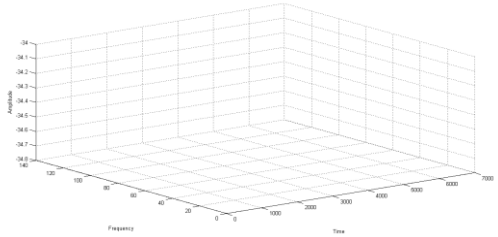

Figure 11: Difference Spectra of Original and Layer 10 Min Embedded Wave (A-b1)

DISCUSSION

By modifying different encoding algorithms, we can make even high capacity, highly robust algorithms which can provide even higher security than spread spectrum techniques. Robustness of audio wave can be made even better by the use of more audio spectrographic algorithms. One of the possibilities could be taking a transform of the given signal and choosing the low power coefficients for embedding. This could result to a decrease in the noise in the output signal thereby improving the SNR ratio. We can even make new music wave files by studying the spectrograms of beats and can also produce music that is not possible through the use of instruments i.e. Risset Beats etc.

CONCLUSION

The steganography on Audio wave files were successfully implemented. It is safer to send an audio wave which was minimum embedded by a secret message in communication. In this paper a new approach is proposed to resolve problem of substitution technique of audio steganography. Problem is having low robustness against attacks which try to reveal the hidden message. An intelligent algorithm will try to embed the message bits in the deeper layer of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layer to achieve higher capacity and robustness. Spy Analyses is a good algorithm that can make a few nuts go loose and can break the security of even some of

the good encryption and encoding algorithms, so we must be sure of the fact that it can only detect that there is a large hidden message in the wave files due to steganography but to break the encryption security we need to break the encoding of communication codes that gives much security, and it cannot detect that there is a small hidden message in the wave file due to steganography that even gives much more security. Also our method depends heavily on Secret key for its security. We have tried to implement different methods to encrypt and encode the steganography in audio wave files, and also gave the spy analyses methods to break through the security hole. Both things can be made tougher and smarter.

REFERENCES

[1] TanmyBhaowmik, PramathaNathBasu, "On Embedding of text in Audio – A case of Steganography", International Conference on Recent Trends in Information, Telecommunication and computing, IEEE 2010.

[2] Ashis Kumar Mandal, Mohammed Kaosar, Md. Olioul Islam and Md. DelowarHossain, "An Approach for Enhancing Message Security in Audio Steganography", IEEE 16th International Conference on Computer and Information Technology, 8-10 March, 2014.

[3] JithuVimal and Ann Mary Alex, " Audio Steganography Using Dual Randomness LSB Method" , IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014.

[4] Dr.Amit Kumar Goel, Mr. Sumit Kumar Moudgil. "Optimization of Steganography on Audio wave by embedding the minimum and maximum message in various layers and spy analysis" AKGEC International Journal of Technology, January-June 2017, Vol. 8, No. 1, ISSN 0975-9514.

[5] Sumit Kumar Moudgil, Dr. U Ragavendran "Effective Use of Steganography on Audio Wave and Spy Analysis" International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 7, Issue 4, July-August 2016, pp. 32-39; ISSN Print: 0976-6464 and ISSN Online: 0976-6472; Journal Impact Factor (2016): 8.2691; InfoBase Index IBI Factor for the year 2015-16 is 3; Thomson Reuters Researcher ID: H-9822-2016.