Optimization of Steganography on Audio Wave and Embedding Minimum and Maximum Message into Various Layers

[1]Sachin Kumar, [2]Sumit Dalal, [3]Ravi Kant Kaushik
[1,2,3]Dept. of Electronics and Communication Engineering, SKITM, Bahadurgarh, Haryana, India

Abstract
Steganography is a sub-discipline of information hiding that focuses on concealing the existence of messages. It is the study of techniques for hiding the existence of a secondary message in the presence of a primary message. Here we embed minimum and maximum message in to the various layers of audio wave. Digital audio is stored ona computer as a sequence of 0's and 1's with the right tools, it is possible to change the individual bits that makeup adigital audio file. Such precise control allows changes to be made to the binary sequence that are not discernible to the human ear. In a computer-based audio steganography system, secret messages are embedded by slightly altering the binary sequence of a sound file. We propose complete steganography on wav audio files using four stages of genetic algorithm – Encryption, Modulation, Decryption and Demodulation. We can hide any text within the layer of data structure of wav files.

Keywords
Stego, SNR, WAV, Min., Max.

I. Introduction

The steganography on Audio wav files were successfully implemented. After the implementation, Spy Analyses was done to test the algorithm on various parameters already introduced in Genetics based algorithm like Robustness, Capacity and Clarity. A GUI was created for easy interaction with the user. Spy Analyses is the step-by-step methods coded in Matlab to break the security loop holes in extreme tests to see the clarity, robustness and capacity of the encryption and encoding used in steganography. Spy Analyses includes these methods used in our model of study – SNR ratios testing, Time Domain Analyses, Frequency Domain Analyses, Spectogram Analyses, Transformation Analyses etc. Message added in steganography was of maximum length possible. Testing using Spy Analyses was done using clear, robust, genetic and high capacity encoding – Inverter Method of encoding that negates the message bits embedded in wav file and provides higher capacity but low robustness than spread spectrum methods.

A. Signal to Noise Ratio Test

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 audiostegano.m file which contains the algorithms for Encryption and Decryption along with GUI for performing steganography.

Table 1: Signal to Noise Ratio for Message Embedding

Embedding Layer	SNR (Min. embedding)	SNR (Max. embedding)
FirstLayer	122.33	114.67
SecondLayer	122.33	114.68
ThirdLayer	122.33	114.69
FourthLayer	122.33	114.70
Fifth Layer	122.33	114.71

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. Embedding is good at layer of encryption.

Alteration: Message bits substitute with the target bits of samples.

To find out the values of sample we use the formula 2^n

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	0	1	1	1	1

0+0+32+0+8+4+2+1 = 47

Modification: It decreases the amount of error and improves the transparency.

Example of adjusting for expected intelligent algorithm

Sample bits are: 00101111 = 47

Bit Position	8	7	6	5	4	3	2	1
Values	0	0	1	0	1	1	1	1

Target bit position is 5, and message bit is 1

Without adjusting: 00111111 = 63 (difference is 16)

After adjusting: 00110000 = 48 (difference will be 1 for 1 bit embedding)

Sample bits are: 00100111 = 39

Bit Position	8	7	6	5	4	3	2	1
Values	0	0	1	0	0	1	1	1

Target bit positions are 4&5, and message bits are 11 without adjusting: 00111111 = 63 (difference is 24) After adjusting: 00011111 = 31 (difference will be 8 for 2 bits embedding)

Verification: This stage is quality controller. Check again the difference

Without adjusting = 63

-Sample bits = -47, Difference is 16

We design algo such that this difference will be minimized

Noise will be minimum , noise increases if we change the bits From left to right for example

1. If LSB bit change, difference will be minimum.
2. If MSB bit change, difference will be maximum.

Reconstruction

This is the last step for new audio file (stego file) creation. This is done sample by sample.

Time Domain, Frequency Domain and Power Spectrum Analyses

Amplitude and Frequency Analyses (Discrete Fourier Transforms,

Power Plots) forembeddedlayer. This plot gives us any change in Amplitude or Frequency part of the wav audio. The plots of Time-Domain, Frequency Domain and Power Spectral Densities of the Base Wav Signal which was used as a base file on which embedding was done i.e. 'LC_House_Beat_123_1.wav'. We can plot this by running 'plots.m' file script. We can easily zoom the plots in Matlab up to any resolution of sample point.

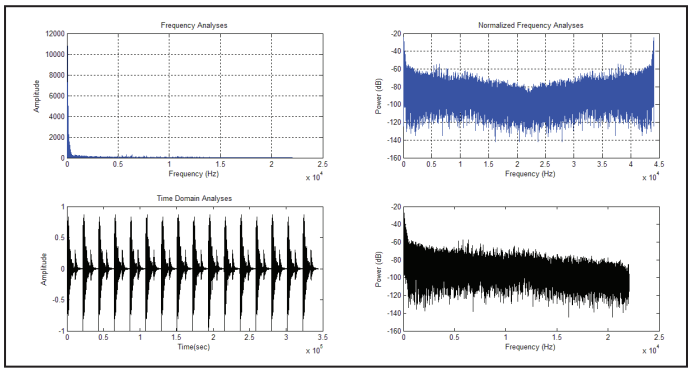

Fig. 3: Original Wav Spectrum and Time Domain Signal Analyses

First plot is the Amplitude vs. Frequency plot, right to it is the Power Spectrum, third is the Amplitude vs. Time Analyses and fourth one is Single Side Frequencies' Power Spectrum which does not show half repeated alias frequencies. Note the amplitude pattern (3rd Plot) which shows the beat wav pattern. Modifying the beat pattern in frequency domain has also led us to create new types of music beats ex: Risset Beats, which is not possible through modern instruments. Now, we will see the embedded files' spectrums one by one and can easily infer from it that all are very co-related thus we can predict that our algorithm is not only robust in detection but is also of high capacity.

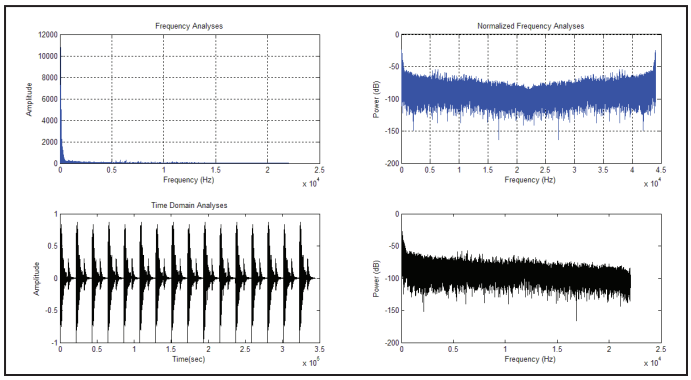

Fig. 4: Layer 2 Max Embedded Audio Wav Signal Analyses

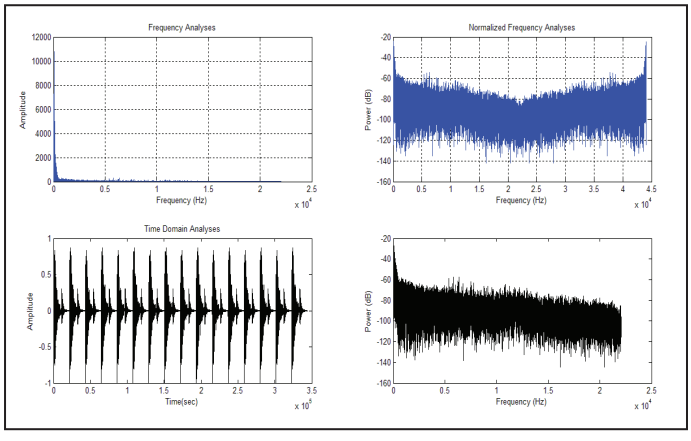

Fig. 5: Layer 2 Min Embedded Audio Wav Signal Analyses

B. Spectrogram Analyses

Now we will see the spectrum analyses of audio wavfiles 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'

1. Original Wav:

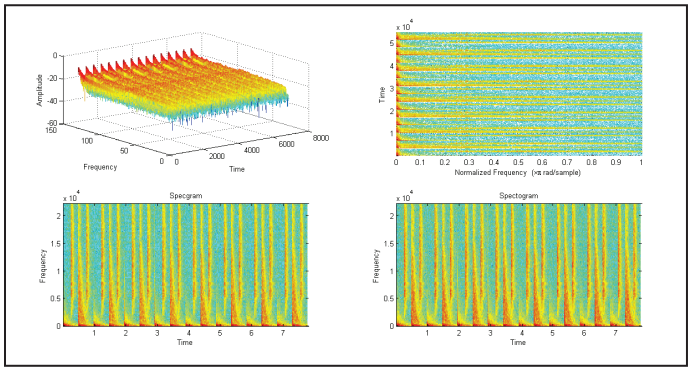

Fig. 6: Original Spectrograms of Wav File A

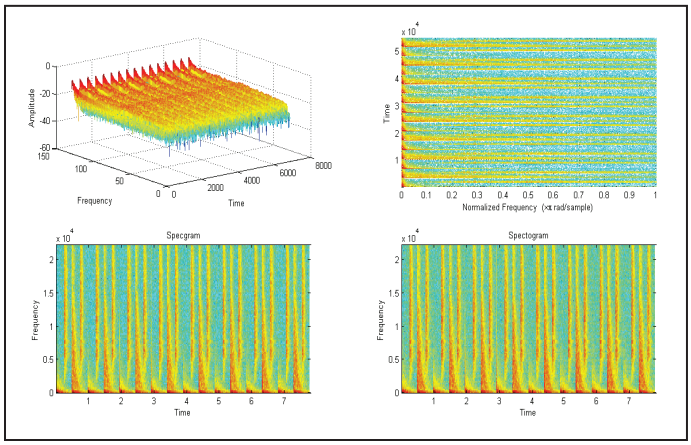

Fig. 7: Spectrogram of Layer 2 Max Embedded Wav File a1

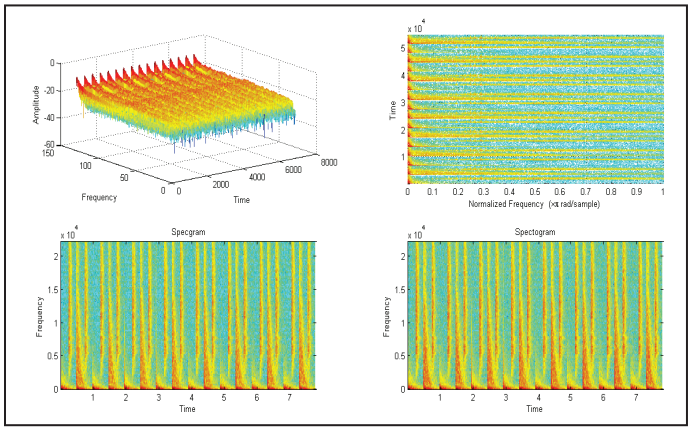

Fig. 8: Spectrogram of Layer 2 Min Embedded Wav File b1

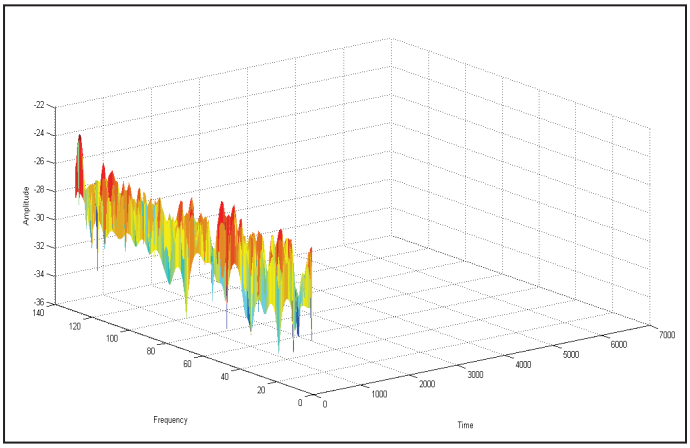

Fig. 9: Difference Spectra of Original and Layer 2 Max Embedded Wav (A-a1)

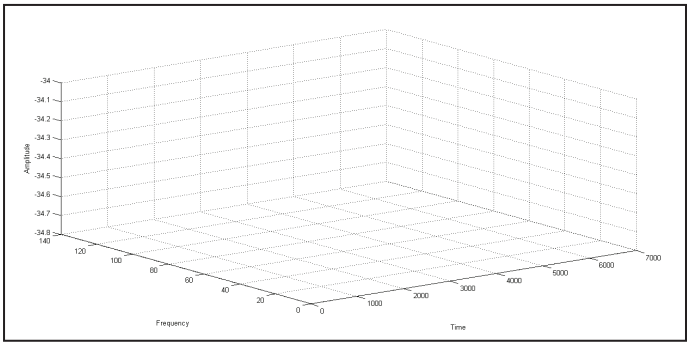

Fig. 10: Difference Spectra of Original and Layer 2 Min Embedded Wav (A-b1)

II. 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 wav 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 wav 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.

III. Conclusion

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 two problems of substitution technique of audio steganography. First problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power. 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 wav 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 wav file due to steganography that even gives much more security. Also our encoding method depends heavily on identity/key for its security. We have tried to implement different methods to encrypt and encode the steganography in audio wav files, and also gave the spy analyses methods to break through the security hole. Both things can be made tougher and smarter.

References

[1] Cvejic N., Seppänen T.,"Increasing the capacity of LSB based audio steganography", Proc. 5th IEEE International Workshop on MultimediaSignal Processing, St. Thomas, VI, December 2002, pp. 336-338.

[2] Westfeld A., Pitzmann A.,"Attacks on Steganographic Systems", Lecture Notes in Computer Science, Vol. 1768, Springer-Verlag, Berlin, pp. 61-75, 2000.

[3] Fridrich, Jessica,"Steganalysis of LSB Encoding in Color Images", Proceedings of the IEEE International Conference on Multimedia. 1279–1282. New York: IEEE Press, 2000.

[4] Martín Alvaro, Sapiro Guillermo, SeroussiGadiel,"Is Image Steganography Natural?", IEEE Transactions On Image Processing, Vol. 14, No. 12, December, 2005.

[5] Lee, Y. K., Chen L. H.,"High Capacity Image Steganographic Model", IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000.

[6] MazdakZamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, Shahidan Abdullah,"World Academy of Science, Engineering and Technology". "A Genetic-Algorithm-Based Approach for Audio Steganography", pp. 355-358, 2009.

[7] MazdakZamani, Azizah A. Manaf, Rabiah Bt. Ahmad, FarhangJaryani, Hamed Taherdoost, Akram M. Zeki,"A Secure Audio Steganography Approach", Institute of Electrical and Electronics Engineers Inc., 2009.

[8] MazdakZamani, HamedTaherdoost, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki,"Robust Audio Steganography via Genetic Algorithm", IEEE.

[9] S.Geetha, Siva S.Sivatha Sindhu, A. Kannan "Stego Breaker: Audio Steganalysis using Ensemble Autonomous Multi-Agent and Genetic Algorithm".

[10] Marcus Nutzinger, Jurgen Wurzer,"A Novel Phase Coding Technique for Steganography in Auditive Media", pp. 91-98, 2011, IEEE