Multi Stage Secure Audio Steganography using Image to Cipher Text Conversion

Uma Shankar Anant[1], Keshav Tiwari[2], Amit Thakur [3]

[1]M-Tech Research Scholar,[2]Assistant Professor,[3]HOD

Department of Computer Science and Engineering, Swami Vivekanand College of Science & Technology, Bhopal, India

Abstract: The Present world of information sharing is gaining popularity by sharing audio, image, and videos. For sharing of Secret data, Audio Steganography is the science that gives communication of secret data in an appropriate multimedia carrier, e.g., audio. This work is concerned with implementing Steganography for audio, with an improvement in both security and audio quality. This work presents a unique system for audio steganography based on multi-stage audio Steganography & Least significant bit (LSB) of each of the pixel's concentrations of wrapping audio. In addition, with LSB and multi-stage the secret image is converted into ciphertext so that no one can understand the message and then this text is embedded in the cover image. The experimental result shows that the methodology has a high security and a good sound quality. It also showed that the anti-detection robustness of audio steganography combined with pre-processing of the multi-stage pattern is initiated much better than the way using LSB steganography algorithms directly.

Keywords: Steganography, LSB, Multi Stage Steganography, Cipher Text, Audio.

I. INTRODUCTION

Steganography, or data hiding is the technique of embedding a message (pay¬load) in a medium (carrier), without causing suspicion about the existence of hidden data in the medium. The perturbations to the medium are carried out in such a manner that there is no perceivable noise component introduced. One way to illustrate the concept of steganography would be to analyze the Sim¬mons' Prisoners' problem. Two prisoners are allowed to communicate through a medium via an agent trusted by the warden. The prisoners' are discouraged from discussing any plans of an escape from the prison. The warden himself, though, has a vested interest in letting them communicate as he wants to catch them in the act of Hatching an escape plan or by foiling their plans by modifying the message itself. In the case of a passive warden, a cryptographic technique would have worked. In this case which involves an active warden, however, the message needs to look innocuous and hence cryptography fails. Steganography comes to the priceowners, rescue. The prisoners', with a strong intention of planning an escape, have already exchanged a code word before they were captured. They use this codeword to secretly exchange messages in the process deceiving the warden by hiding the message in plain sight. The codeword lets them embed and extract information. A possible technique would be to use the code word as a position compass for hiding and extracting letters of the message exchanged. The warden is oblivious to the existence of a secret message. The medium mentioned in the problem above could be photographically produced microdots used by espionage agents during World War II, a Bacon cipher that uses different typefaces to hide information or a digitally altered JPEG image hide using Steg hide. In all the above mentioned methods the priority is to hide messages in plain sight and make the carrier look innocuous.

Digital steganography often uses the compressed/uncompressed image, video, and audio formats. Image steganography has grown in prominence with tools like Outguess, Steg hide, to name a few. Compressed audio formats like audio and Ogg lag in their usage as a medium for steganography. The only known steg tools that use Audio as a carrier are AUDIO Stego and Under audio Cover. Audio Steno hides data into an audio hide during the encoding process. The technique uses the power of parity to embed a bit in the part length of a granule in an audio file. The desired value of part length is obtained in the inner loop that quantizes the input data (spectral data) by increasing the quantizer step size until the quantized data can be encoded using the available number of bits. The additional condition that hides the data bit is the check on the parity of the part length variable.

If the parity is the same as the bit to be hidden the loop exits. The outer loop checks if the bound put on the quantization noise has been breached. Under audio, Cover is a steg tool that embeds data by applying LSB steganography on the global gain parameter in an audio granule. LSB or Least Significant Bit steganography as the name suggests embeds data in the least significant bit of a carrier byte. In the case of Under audio Cover, the carrier byte is the global gain value. Under audio, Cover worked on an already encoded audio hiding, unlike the audio stage, which hides data during the encoding process of Pulse Code Modulation (PCM) samples to audio.

A new method of steganography in audio hides in the big-value region of long blocks using a spectral pair swap method. The research gives an overview of the MPEG layer III audio encoding algorithm.

II. SYSTEM MODEL

As explained above Steganography is the art of concealing the existence of information within seemingly innocuous carriers. It includes various methods of secret communications that conceal the very existence of the message. Among these methods are undetected inks, microdots, character arrangement (other than the cryptographic methods of transposition and substitution), digital signatures and hidden channels and spread-spectrum communications. “In steganography “cover” is the mode which is used to hide the secret message.

The data to be hidden can be a plain text message, a cipher text, another image, or anything that can be characterized in binary.

The file commonly acts as the cover to hold the information. If an image is used as cover, then it can be altered in the noisy areas with a lot of color variation so that the alterations are less accessible. The message can also be sprinkled randomly throughout the image.

Common methods of hiding data in digital images include:

Least significant bit insertion: This is a very simple method of hiding the message in a digital image. In this method, the LSB of each byte in the image is used to store the secret data. Changes in the new image in which the message is hidden are too little to be identified by the human eye. The pros of this technique are that since it uses individual pixel in an image, a lossless compression pattern like Bmp has to be used for the image.

Masking and filtering: “These approaches hide information in an appearance similar to study work steganography. This can be done, for example, by modifying the fluorescence of parts of the image. It does alter the visible properties of an image, but if done with care the distortion is almost discernable.”

Transformations: This is a complex way of hiding information in an image. This is thought-out as the most effective way of hiding the information. Different algorithms and transformations are used to the image to hide information in it. DCT (Direct cosine transformation) is one such method.

III. PROPOSED METHODOLOGY

The proposed, a multidisciplinary approach LSB would be applied to solving the security problems. The signal processing methods may need for steganography inserting and extracting processes, derivation of perceptual thresholds, transforms of signals to the different signal. The proposed, a multidisciplinary approach LSB would be applied to solving the security problems. The signal processing methods may use for steganography embedding and extracting processes, derivation of perceptual thresholds, transforms of signals to the different signal. The block diagram of the proposed methodology is given in the Fig. 1.1.

Among various information covering method proposed to embed secret information within the audio file, the Least Significant Bit (LSB) coding method is the easiest way to encode hidden message in a digital audio file by reconstitution the LSB of the audio file with a binary message. Hence the LSB method grants a large quantity of secret information to be encrypted in an audio file.

This proposed method provides greater security and it is an efficient method for hiding the hidden information from hackers or other unauthorized person and sent to the destination in a safe and inaudible manner. This proposed system likewise makes secure that the size of the file is not replaced even after encoding and it is also appropriate for any type of audio file format.

The above mentioned system is implemented on the MATLAB R2011a and the implemented algorithm is explained with the flow chart given below.

The flow chart is having major steps are embedding process to get audio file:

Embedding Algorithm:

A. *Start of Simulation*

B. *Reading Wave File*

C. *Read Audio File*

D. *Analog-to-Digital Conversion*

E. *Use most significant bit to store the sign*

F. *Read Secret Image and Convert into Cipher Text*

I. *Form a row vector of secret message*

J. *Embed message length in first 16 samples*

K. *Embed secret message from 17th sample*

L. *Digital-to-Analog Conversion*

M. *Check the sign from most significant bit*

N. *Analysis*

O. *Save the sound contained secret message*

P. *Display Results*

Q. *End of simulation*

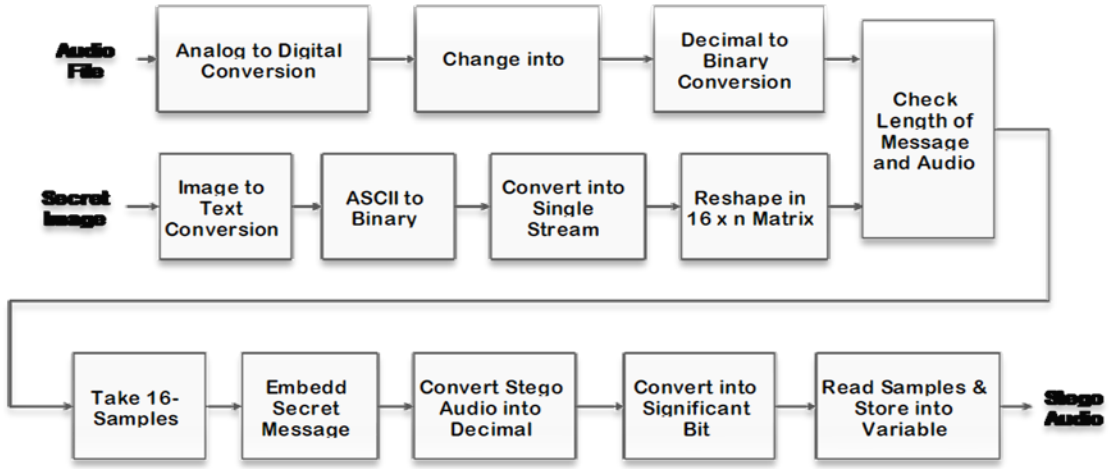

Fig.1.1 Embedding Process to Get Stego Audio File

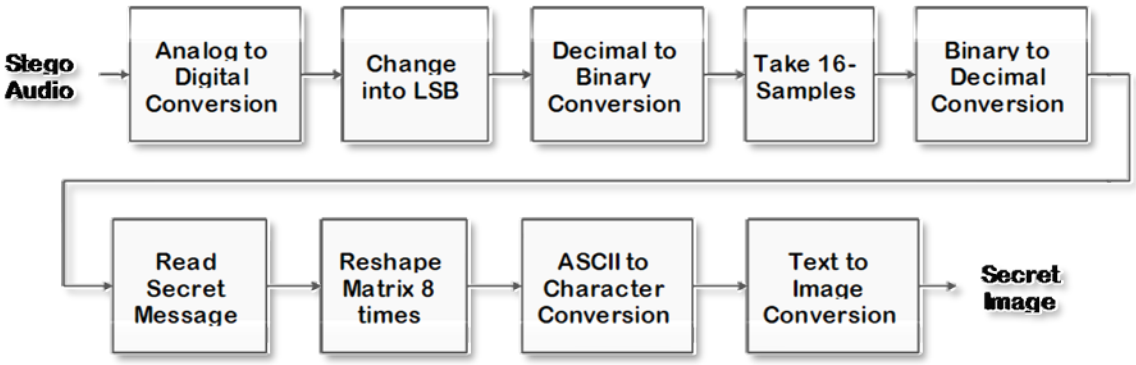

Fig.1.2 Extraction Process to Extract Secret Image

The flow chart is having major steps are extraction process to extract secret image Fig. 1.2.

Decoding Algorithm:

A. *Start of Simulation*

B. *Decoder*

C. *Reading Wave File*

D. *Analog-to-Digital Conversion*

E. *Store the sign in most significant bit*

F. *Check first 16 samples to know how many samples contains a secret message*

G. *Extract message*

H. *Change the row vector in nx8 matrix*

I. *Check ASCII*

J. *Show recovered secret image*

K. *End of simulation*

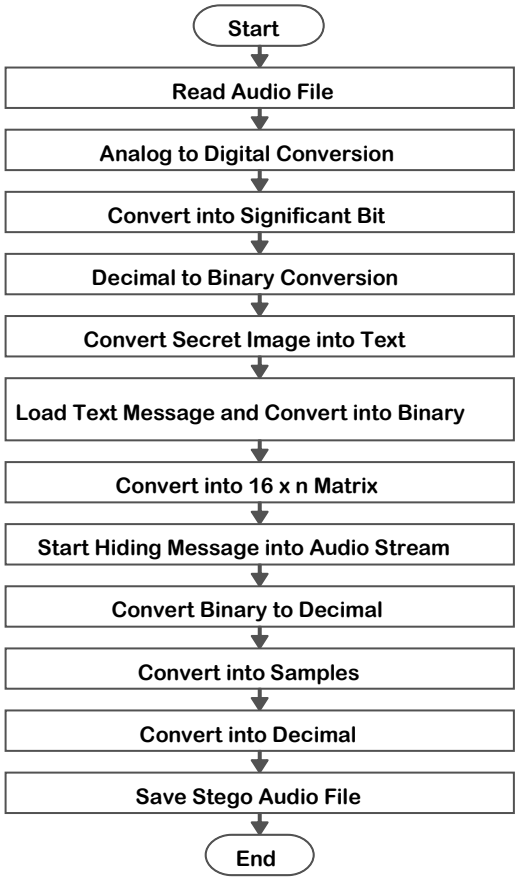

Fig.1.3 Flow Chart of Embedding Process of Secret Image to Get Stego Audio

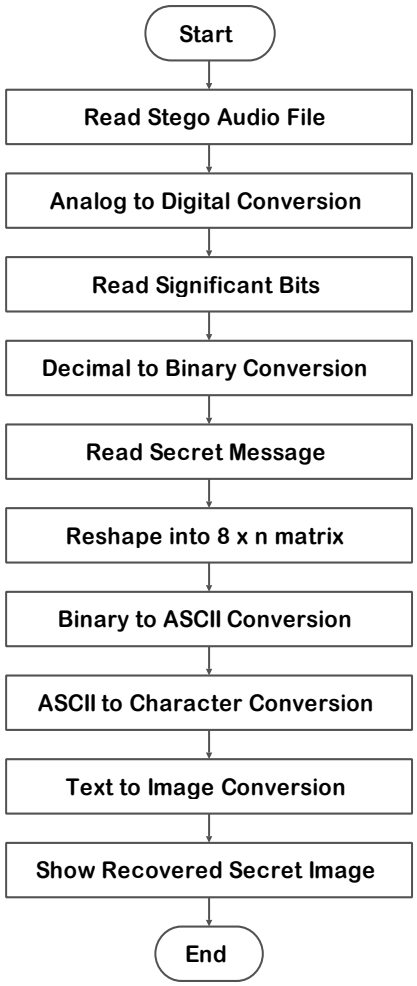

Fig.1.4 Flow Chart of Extraction of Secret Image From Stego Audio

IV. SIMULATION RESULTS

We have implemented the multi-level secure audio steganography method on MATLAB. We can test the performance of the proposed method by comparing both the original audio with embedded audio, and see whether any changes is visible in embedded audio and result of the stego audio is compared by PSNR graph.

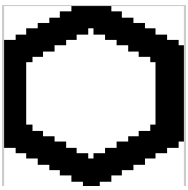

Fig.1.5 Secret Image

ÿÿ————————————————————————ÿ
ÿÿÿÀÿÿÀÀà
————————————————————————————à-
————————————————————————————ðð?
ø> ø~ ü| |ü ~ø >ø ?ð ø ?ø >ü ~| |~
ü> ø? ø ð-
————————————————————————————ð

Fig.1.6 Text Converted From Secret Image

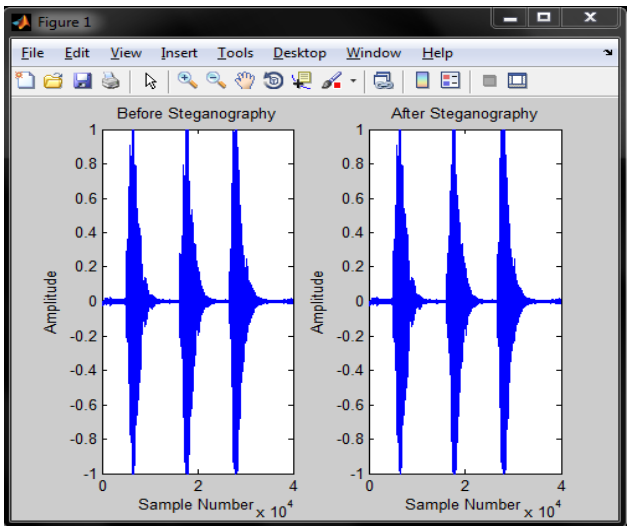

Fig.1.7 Original Cover Audio and After Embedding of Secret Image

As we see in Figure 1.7 there are no visible changes when compared to cover audio with stego audio. There are Mainly two aspects that should be taken into account when discussing the results of the audio steganography. They are higher security, undetectability of secret message. This method satisfies both security aspects and undetectability. This method hides secret messages which are very difficult to detect the original message may be present on any level of the proposed method. So undetectability of the original message is achieved. The security level has increased through the encoding of the secret messages through sender to the receiver he can't find out whether there is any message in the audio. Because there is no visible distortion exists in the audio. Second, when we compare the original audio graph with the embedded one there is no visible difference in both graphs.

ÿÿ————————————————————————ÿ
ÿÿÿÀÿÿÀÀà
————————————————————————————à-
————————————————————————————ðð?
ø> ø~ ü| |ü ~ø >ø ?ð ø ?ø >ü ~| |~
ü> ø? ø ð-
————————————————————————————ð

Fig.1.8 Extracted Text from Stego Audio

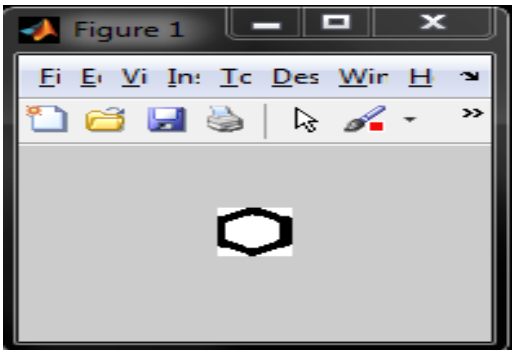

Fig.1.9 Recovered Secret Image

Third, if any, third person finds that there is some message in audio and tries to extract it, then he can't extract it because there are multi-levels in this method and we can hide the secret message in ant level.

Calculate PSNR:

Peak signal-to-noise ratio (PSNR) is most frequently used to measure the quality of reconstruction of Loss compression example: for image compression. A signal, in this case, is the original data, and the noise is the error introduced by compression.

Peak Signal-to-Noise Ratio (PSNR): It is the measure of quality of the audio signal by comparing cover audio with stage audio. PSNR in decibels (dB) is computed by using:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

Figure 1.11 - Peak Signal-to-Noise Equation

Mean Squared Error (MSE): It is defined as the square of the error between cover audio signal & stage audio Signal. The distortion in the audio signal can be measured using MSE. It is calculated as follows.

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

Figure 1.10 - Mean Squared Error Equation

Where f (I, j) represents cover audio signal and F(i,j) represent stego audio signal.

In Table 1 we take different size of audio files with same size of image size (BMP) and get different PSNR values.

Table 1: Comparison of PSNR Values

Audio File	Audio File Size	Secret Image(.bmp) Size	PSNR Value	MSE Value
1.wav	79 KB	1 KB	103.2 dB	0.00
2.wav	435 KB	1 KB	113.45 dB	0.00
3.wav	108 KB	1 KB	62.99 dB	0.00
4.wav	184 KB	1 KB	68.21 dB	0.00
5.wav	71 KB	1 KB	57.48 dB	0.00
6.wav	30 KB	1 KB	53.70 dB	0.00
7.wav	75 KB	1 KB	54.51 dB	0.00
8.wav	41 KB	1 KB	59.40 dB	0.00
9.wav	119 KB	1 KB	65.82 dB	0.00
10.wav	40 KB	1 KB	59.03 dB	0.00

The audio file before and after hiding the secret image into the audio file sounds same. It means there is no deafening difference in an audio file before and after hiding the data into the file.

After comparing the PSNR values of the proposed technique with Neha Gupta and Nidhi Sharma's [1]

Which having PSNR max range up-to 37 db, And the proposed algorithm having range 53.70 to 113.45 db means it shows the current technique is relatively good.

V. CONCLUSION AND FUTURE SCOPES

The proposed audio steganography technique has certain advantages over previous techniques and these advantages are low complexity, multiple stage security, and accuracy with processing speed. From the results and comparison of PSNR, the stage audio output is nearer to the original audio and listener unable to identify it while listening. From the comparison table, the conclusion can be made as the value of PNSR vary according to the length of secret information as well as the size of cover audio. The higher PSNR significantly shows the efficiency of the algorithm. For further improvements in the area of audio steganography security methods and stages can be increased so that the robustness of algorithm gets better and better. The encoding techniques for text secret information would be better.

REFERENCES

[1] Gupta, N.; Sharma, N., "Dwt and Lsb based Audio Steganography", Process of IEEE Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on , vol., no., pp.428,431, 6-8 Feb. 2014.

[2] Bugár, G.; Bánoci, V.; Broda, M.; Levický, D.; Dupák, D., "Data hiding in still images based on blind algorithm of steganography" Radioelektronika (RADIOELEKTRONIKA), In proc. 24th IEEE International Conference , vol., no., pp.1,4, 15-16 April 2014.

[3] Geethavani, B.; Prasad, E.V.; Roopa, R., "A new approach for secure data transfer in audio signals using DWT" In Proc. IEEE Advanced Computing Technologies (ICACT), 15th International Conference on , vol., no., pp.1,6, 21-22 Sept. 2013.

[4] Khademi, Mahdi; Tinati, M.A., "Audio steganography by using of linear predictive coding analysis in the safe places of discrete wavelet transform domain" In Proc. IEEE Electrical Engineering (ICEE), 19th Iranian Conference on , vol., no., pp.1-5, 17-19 May 2011.

[5] Zhang Kexin, "Audio steganalysis of spread spectrum hiding based on statistical moment" In Proc. IEEE Signal Processing Systems (ICSPS), 2nd International Conference on , vol.3, no., pp.V3-381,V3-384, 5-7 July 2010.

[6] Cairong Li; Wei Zeng; Haojun Ai; Ruimin Hu, "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM" In Proc. IEEE Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09. International Conference on, vol.1, no., pp.240, 243, 25-26 April 2009.

[7] Wang Junjie; Mo Qian; Mei Dongxia; Yao Jun, "Research for Synchronic Audio Information Hiding Approach Based on DWT Domain" In Proc. IEEE E-Business and Information System Security. EBISS '09. International Conference on, vol., no., pp.1,5, 23-24 May 2009.

[8] Johnson N &Jajodia S, Steganalysis: the investigation of hidden information. In: Proc. IEEE Information Technology Conference, Syracuse, NY, p 113–116, 3 Sept. 1998.

[9] Katzenbeisser S &Petitcolas F, Information Hiding Techniques for Steganography and Digital Steganography. Artech House, Norwood, MA. 1999.

[10] Bender W, Gruhl D & Morimoto N, Anthony lu, “Techniques for data hiding”. IBM Systems Journal 35(3): p 313–336, 1996.

[11] Cox I & Miller M, Electronic steganography: the first 50 years. In: Proc. IEEE Workshop on Multimedia Signal Processing, Cannes, France, p 225–230, 2001.

[12] Hartung F &Kutter M, Multimedia watermarking techniques. Proceedings of the IEEE 87(7), p 1709–1107. 1999.

[13] Tanwar, R. ; Bisla, M., Audio steganography In Proc. IEEE International Conference on Optimization, Reliabilty, and Information Technology (ICROIT), P. 322 – 325, 6-8 Feb. 2014.

[14] Binny, A.; Koilakuntla, M., Hiding Secret Information Using LSB Based AudioStegaography. In Proc. IEEE International Conference on Soft Computing and Machine Intelligence (ISCMI), P. 56 – 59, 26-27 Sept. 2014.

[15] Warkar, R.; More, P.; Waghole, D., Digital audio watermarking and image watermarking for information security. In proc. IEEE International Conference on, pp. 1-5, 8-10 Jan. 2015.