Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 4 (2015), pp. 2477-2486

http://www.ripublication.com

An Efficient Audio Steganographic System for MP3 Format using Multi Pattern to Embed Secret Text

Elangovan.B, Srinivasan.B, Senthil Sevan.N, Birundha.T

School of Computing, SASTRA University, Thanjavur, Tamilnadu, India-613 402
Corresponding Author: B.Elangovan,
School of Computing, SASTRA University, Thanjavur, Tamilnadu, India.
Email: elan77@gmail.com

ABSTRACT:

Steganography is the art & science of concealing secret information in a manner that the information cannot be distinguished by others, with the exception of the sender and receiver. All digital files such as audio, video, images and text can be used for concealing the secret data. In this paper, we exhibit steganographic techniques for audio utilizing MP3 files. MP3 (Moving Picture Experts Group1 Audio Layer3) file can give a decent concealing medium as a result of its high speed data transfer and high level of repetition. Audio stego will conceal the information in mp3 files. In the proposed system, the encryption of messages is done and placed with the help of key. The location of the cipher data bits on audio files (MP3) are based on sequence of three patterns. The three patterns are zigzag pattern, spiral pattern, saw-tooth pattern.

Keywords: Audio Steganography, MP3 Format, Pattern, Stego Audio.

Introduction:

Steganography is the methodology of concealing a secure information inside a larger one such that the path to indicate the vicinity or substance of the covered up information is hidden to anybody except for the sender and receiver. Although related, Steganography is not to be mistaken for encryption, which is the methodology of constructing a information ambiguous. Steganography endeavours to shroud the presence of correspondence. The fundamental structure of steganography is comprised of three segments: the transporter, the information and the secret key. The carrier or transporter can be a depiction, a digital image, an mp3 or even a TCP/IP packet in addition to a variety of other things. It is the article which will carry the

concealed message. A secret key is utilized to decipher/find the hidden message. This will be something from a password, a pattern, a dark light or may be lime juice. During this paper, we will specialize in the utilization of steganography among audio (MP3 files).

Audio Steganography may be strategy utilized to transmit hidden transmission by modifying an audio signal in unobservable manner. It is the science of concealing audio information in a host message. The host message (before audio steganography) and stego message (after steganography) have the identical characteristics. Embedding secret informations in digital audio may be a more difficult method. Various techniques for embedding information in digital audio have been established. Audio information stowing away is one of the compelling approach to ensure the protection.

Literature survey:

In the recent years, a few methods for hiding data in audio sequences have been introduced. The majority of the developed techniques exploits the perceptual properties of human audio related framework.

Raffaele Pinardi, Fabio Garzia, Roberto Cusani proposed a steganographic technique for MP3 audio configuration is focused on the peak shaped model algorithm used JPEG images [1]. The proposed method depends on the factual properties of MP3 samples, which are layered by a Modified Discrete Cosine Transform (MDCT). After the conversation of MP3, it's conceivable to shroud some secret data by supplanting the least significant bit of the MDCT coefficients. Those coefficients are picked by factual significance of every coefficient inside the conveyance. They have also discussed the performance analysis of the three steganographic parameters, the embedding capacity, the embedding efficiency and the PSNR.

Yatin Baluja, Shray Mishra, Trilok Singh Saini enforced audio watermarking and it has been incontestible as a attainable resolution to avoid illegal usage of audio files [2]. The projected system will implant the watermark information in estimate constant of distinct wavelet change. Experimental results for distinctive audio signs demonstrate that this watermarking methodology is robust against the essential signal transforming assaults. As an example, resampling, quantization, low pass separating volume scaling and noise expansion.

Muhammad Asad, Junaid Gilani, Adnan Khalid projected a three layered model for audio steganography support on least significant bit replacement [3]. The mystery message to be transmitted is gone through two layers before it is embedded within the third layer. The stego message is transmitted over the system to the receiver aspect and therefore the secret message is recuperated by performing opposite operations in converse request. The aim of the paper is to verify the classifications of secret message. Likewise they talked regarding the usage problems of the three layered model with admiration to distinctive parameters like capability, transparency and robustness. Check results have incontestible that three layer model earned to a sign to commotion degree of 54.78 decibel in correlation to 51.12decibel of customary LSB technique.

Bankar Priyanka R., Katariya Vrushabh R., Patil Komal K. planed a completely unique methodology of accommodation of audio steganography utilizing genetic rule message bits are embedded into multiple and better LSB layer qualities transportation concerning enlarged robustness [4]. The robustness would be enlarged against those deliberate attacks that arrange to uncover the concealed message furthermore some inadvertent attacks like noise enlargement.

S.S. Divya, M. Ram Mohan Reddy examined a technique for concealing content in audio utilizing completely different LSB steganography and supply security utilizing cryptography [5]. For sixteen bit every sample audio sequences the utmost range of bits that may be adjusted for LSB audio steganography while not influencing the nature of host audio signal is 4 LSBs. The analysis has projected two novel methodologies of substitution technique of audio steganography that enhances the limit of cover audio for embedding further information. Here message bits are inserted into multiple and variable LSBs. These strategies utilize up to 7 LSBs for embedding data. From the results these methods improves the capability of data hiding of cover audio by 35% to 70% as compared to the standard LSB algorithm which uses 4 LSBs for information implanting.

Proposed System:

Encryption:

Encryption is the methodology of changing information or secret data (referred to as plaintext) utilizing an algorithm (called a cipher) to make it unreadable to anyone exception of those having special knowledge typically referred as a key.

In the proposed system, the encrypted information will be hidden in the audio files which are termed as stego audio. This stego audio contains the original MP3 file as well as the secret information. The characteristics of the original MP3 files and the stego audio remain the same. The block diagram of a encryption is shown in Fig.1.

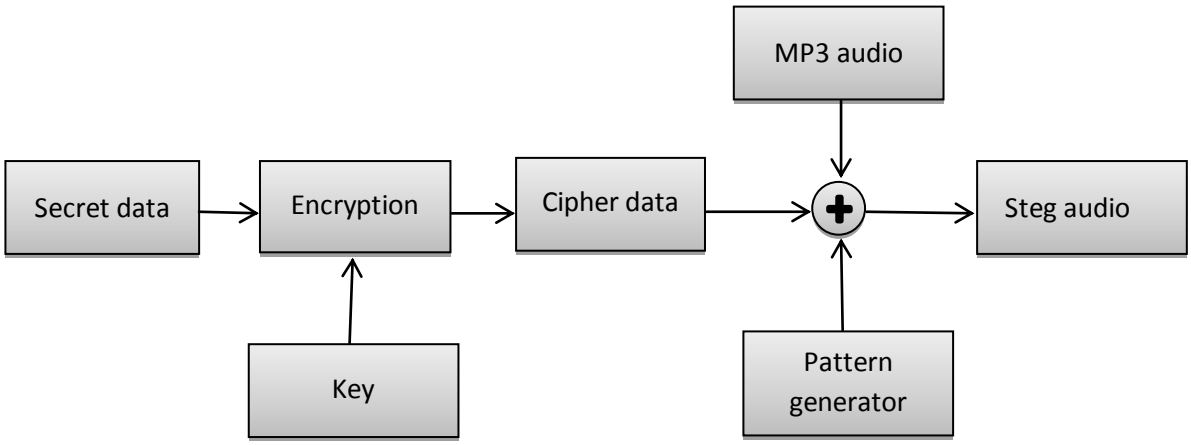


Fig.1.Encryption process

In order to hide the secret information into audio files they must be capable of holding the secret information. To check the capability of audio cover media we use the following formula,

C= (HEADER_SIZE + FOOTER_SIZE + (n bytes *8) + CONST)

Where,

- C is the capability of audio cover media.
- HEADER_SIZE: The MPEG audio file is developed from smaller parts called frames.In common, frames are autonomous things. Each frame has its own header and audio information. There is no document header. In this manner, we can cut any portion of MPEG file and play it accurately. For Layer III, this is not 100% correct. Because of the internal information association in MPEG variant 1 Layer III documents, frames are frequently relied on one another and they can't cut off much the same as that. In order to read information about a MP3 file, it is generally enough to discover the first frame, read its header and except that alternate frames are the same.
- FOOTER_SIZE: End of the file frames is called footer.
- N bytes denoted as number of bytes

Key:

The secret message is hidden the MP3 files with the help of a unique key during the encryption process. In our system, we use a sequence of key based on the number of elements (n) provided for the following formula, 2^{2+n} And hence the corresponding matrix is generated. For example, if n=0; 2^{2+0}= 4. The resultant matrix is,

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

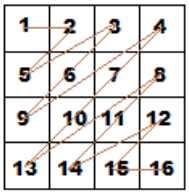
From the generated matrix, we rearrange the key sequence with the help of various pattern, some of these patterns are,

1. Zigzag pattern:

A zigzag is a pattern made up of small corners at variable angles, however constant within the zigzag, following a way between two parallel lines; it can be depicted as both rugged and genuinely consistent. The pattern generator generates a zigzag pattern key sequence based on the following algorithm,

ZigzagForm(a[][],length)
r_idx ->row_index
c_idx ->column_index

While(r_idx<length)
If(r_idx==length-1)
r_idx=c_idx+1;
c_idx=length-1;
else if(r_idx==0)
c_idx=r_idx+1;
r_idx=0;
else
r_idx++;
c_idx--;

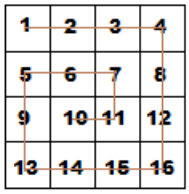


INPUT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
OUTPUT	1	2	5	3	6	9	4	7	10	13	8	11	14	12	15	16

2. Spiral pattern:

A spiral is a curve, which radiates from a central point, escaping as it rotates around the point. The following algorithm used to generate a spiral pattern key sequence.

SpiralForm(a[][],length)
r_ idx ->row_index
c_idx->column_index
For(r_idx=0;c_idx=length-1;r_idx<c_idx;r_idx++;c_idx--)
For(temp=r_idx;temp<c_idx;temp++)
For(temp=c_idx,temp>r_idx;temp--)



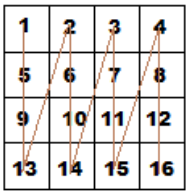
INPUT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
OUTPUT	1	2	3	4	8	12	16	15	14	13	9	5	6	7	11	10

3. Saw-tooth pattern:

The saw-tooth wave (or saw wave) is a sort of non-sinusoidal waveform. It is so named in view of its similarity to the teeth of a saw. To generate a saw tooth pattern key sequence, we can use the following formula,

$$n * (c\_idx - 1) + r\_idx$$

Where,
n is the size of the array.
r_idx– Row of the matrix.
c_idx– Column of the matrix.



INPUT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
OUTPUT	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

For all the patterns we considered in this system we provide the system we provide the same input sequence and the corresponding output of each pattern gives the key sequence for these pattern respectively.
Once we are ready with our key sequences during the encryption and decryption process, the combination of the key sequences are taken in the order got from zigzag, spiral and saw-tooth pattern respectively.

Decryption:

Once the encryption process got over and cipher data has been hidden into the audio files, user should be in a position to understand the context of the cipher data. To decrypt the cipher data and understand its contents we make use of an unique key. The block diagram of a decryption is shown in Fig.2.

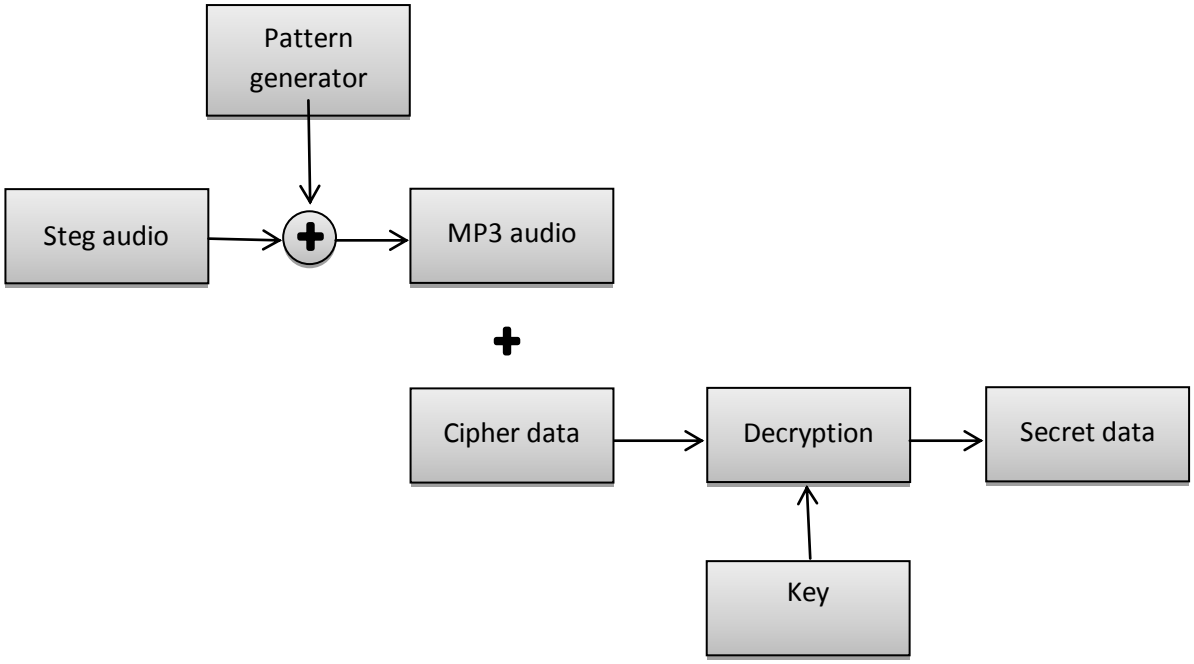


Fig.2.Decryption process

PSNR (Peak Signal Noise Ratio):
PSNR quantifies the nature of the audio signal. It compare the unique audio signal with stego signal. PSNR is measured in decibels (db).

$$\text{PSNR} = 10\log_{10}\frac{\sum_{n=0}^{N} x(n)2}{\sum_{n=0}^{N}[x(n)-y(n)]2}$$

where,
x(n) – Audio cover signal
g(n) – Stego signal
In our system, the noise ratio found out from the PSNR value is less,when we do the same methodology performed in MATLAB.

Embedding Process:
Secret data is encrypted to get the cipher text in order to store them in MP3 file. In this embedding process, to store 1byte letter of the secret text, we need 8 bytes memory space. Similarly all the other bytes of the data are placed on the next corresponding 8 bytes space. Our next step is to convert each 1 byte letter of the secret text to 8 bit binary number and the resultant values are stored in memory. These resultant binary numbers are then passed into pattern generator which generates a unique pattern Zigzag, Spiral, Saw-tooth. Hence are binary numbers are rearranged according to the pattern generated. This rearranged binary output is an cipher text that

is to be hidden in MP3 file.Fig:3 shows an embedding process for 2byte word. For example, consider a word **ok** which has 2 bytes to store a 2byte in mp3 file we need 16bytes memory space. A Binary number of the first letter stored in first 8 bytes. Similarly, the second letter stored in second 8 bytes memory space. Based on the zigzag pattern, binary values are rearranged. Then, the cipher text is hidden into mp3 file.

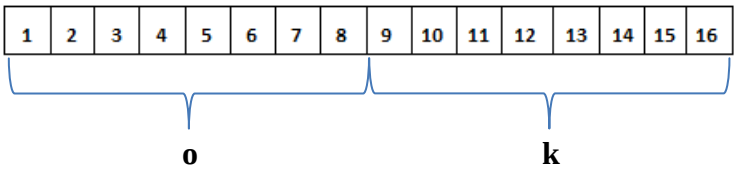


Fig.3.1 shows the memory space allocated for 2 bytes.

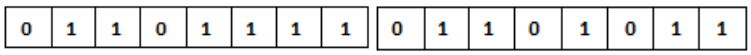


Fig.3.2 :Binary form of secret word (ok).

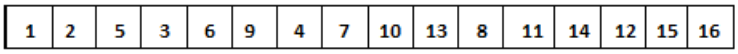


Fig.3.3: Arrangement of elements in zigzag pattern

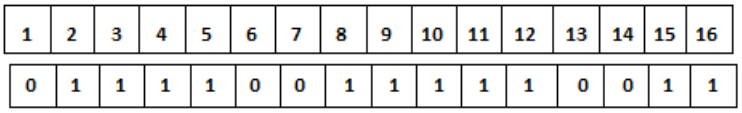


Fig.3.4: Cipher bytes which has stored in mp3

Data table:

S.no	Audio byte	value	Binary value	Embedded bits	pattern	Audio stego
1	51	2	00000010	0	1	00000010
2	52	5	00000101	1	2	00000101
3	53	13	00001101	1	5	00001101
4	54	12	00001100	0	3	00001101
5	55	49	00110001	1	6	00110001
6	56	77	01001101	1	9	01001100
7	57	39	00100111	1	4	00100110
8	58	85	01010101	1	7	01010101
9	59	64	01000000	0	10	01000001
10	60	99	01100011	1	13	01100011
11	61	101	01100101	1	8	01100101

12	62	84	01010100	0	11	01010101
13	63	113	01110001	1	14	01110000
14	64	126	01111110	0	12	01111110
15	65	125	01111101	1	15	01111101
16	66	127	01111111	1	16	01111111

Conclusion:

This paper presents a audio steganography using mp3 files. The new methodology that we have found in this paper is that we use various pattern in order to hide the secret data into mp3 files. To transfer information securely in this method into helpful as we findout the key sequence from various pattern and then pass it to the key generator which gives the corresponding secret key. Because of this process third party will not be able to findout the secret key. Another feature of this methodology is that the noise frequency is less compared to the result of various other software.In future, the proposed system can be extended further to even hide digital files.

References

[1] Raffaele Pinardi, Fabio Garzia, Roberto Cusani, Peak-Shaped-Based Steganographic Technique for MP3 Audio, Journal of Information Security Vol.4 No.1,2013.

[2] YATIN BALUJA, SHRAY MISHRA, TRILOK SINGH SAINI, M.V.PATIL,Frequency Domain Based Data Hiding Technique For Audio Signal, International Journal of Innovative Research in Science, Engineering and Technology,Volume: 2; Issue: 5; p:1564;2013;

[3] Muhammad Asad, Junaid Gilani, Adnan Khalid, Three Layered Model for Audio Steganography, 2012 International Conference on Emerging Technologies (ICET)

[4] Bankar Priyanka R., Katariya Vrushabh R, Patil Komal K, "Audio Steganography using LSB'', International Journal of Electronics, Communication and Soft Computing Science and Engineering, March 2012, pp 90-92

[5] S.S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography", International Journal of Scientific &Technology Research, Vol. 1, pp. 68-70, July 2012

[6] Nedeljko Cvejic, Tapio Seppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

[7] W. Bender, D. Gruhl, N. Morimoto and A.Lu, "Techniques for data hiding, " IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

[8] Kekre, H. B., Athawale, a, Rao, B. S., & Athawale, U.(2010). Increasing the Capacity of the Cover Audio Signal byUsing Multiple LSBs for Information

Hiding. 2010 3rdInternational Conference on Emerging Trends in Engineeringand Technology, 196-201. IEEE.doi:10.1109/ICETET.2010.118

[9] Elangovan, B., Rajesh, K., Venkateswari, An efficient method for high secured image steganography using image segments, International Journal of Applied Engineering Research (12), 1395-1403, 2013